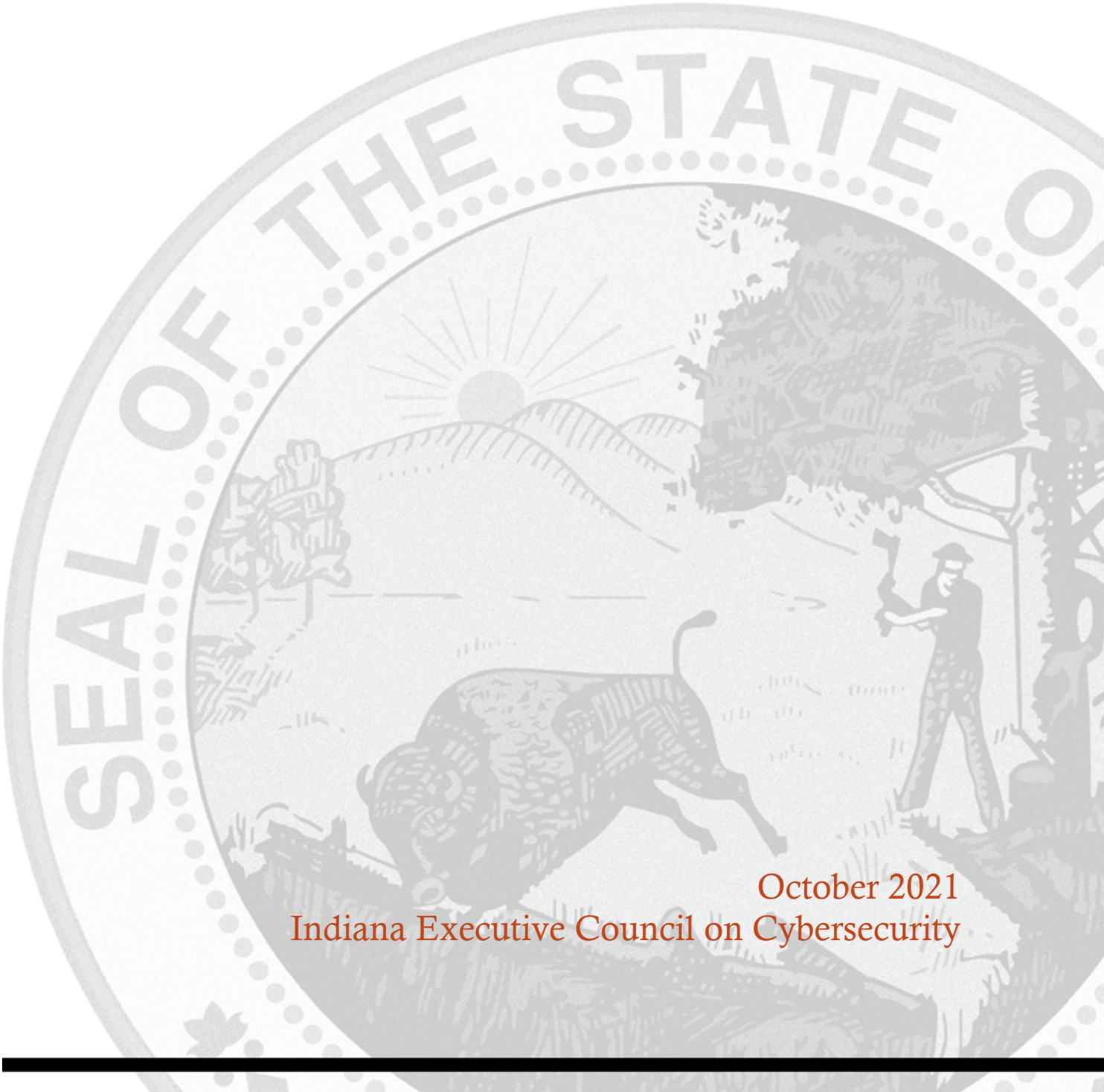
LEGAL AND INSURANCE WORKING GROUP STRATEGIC PLAN

Chair: Todd Rokita
Co-Chair: Stephen Reynolds



October 2021
Indiana Executive Council on Cybersecurity

Legal and Insurance Working Group Plan

Table of Contents

Committee Members

Committee Members

Last Name	First Name	Organization	Organizational Title	Member Type (Chair/Co-chair/Full-time, As needed)
Ehrenberg	Jim	Indiana Office of Technology	General Counsel	Full Time
Harper	Meredith	Eli Lilly and Company	Vice President, Chief Information Security Officer	Full Time
Howell	Michele	Aon Risk Services Central	Vice President, Business Development	Full Time
Ira	Adam	Frost Brown Todd	Attorney	Full Time
Putnam	Reid	Gregory & Appel Insurance	Vice President, Commercial Insurance	Full Time
Reynolds	Stephen	Baker McKenzie	Partner, IPTech	Co-Chair
Rokita	Todd	Indiana Attorney General	Attorney General	Chair
Souza	Diego	Cummins, Inc.	Global Chief Information Security Officer	Full Time
Swearingen	Mark	Hall, Render, Killian, Heath & Lyman, P.C.	Shareholder	Full Time
Swetnam	Douglas	Indiana Office of Attorney General	Section Chief – Data Privacy and Identity Theft Unit	Chair Proxy
Torres	Lori	Indiana Attorney General	Chief Deputy	As Needed
Vare	Todd	Barnes & Thornburg LLP	Partner	Full Time
Berry-Tayman, JD	Lisa	Kevel	Director of Security and Privacy	Full Time

Introduction

Introduction

The world of cybersecurity is highly complex and cluttered with information, misinformation, and disinformation. As a consequence, it is important to approach it strategically and create simplicity.

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) continues its mission to move efforts and statewide cybersecurity initiatives to the "Next Level." With the ever-growing threat of cyberattacks, protecting Indiana's critical infrastructure is the focus of the IECC. Cybersecurity cannot be solved by one entity alone. The IECC works with private, public, academic, and military partners from all over the state to develop and maintain a strategic framework that establishes goals, plans, and best practices for cybersecurity.

The IECC is comprised of fifteen committees and working groups who have worked together to implement the statewide strategy of 2018 while developing an updated comprehensive strategic plan.

The following implementation plan is one of the fifteen specific plans that encompass the complete *2021 Indiana Cybersecurity Strategic Plan.*

For more information, visit www.in.gov/cybersecurity.

Executive Summary

Executive Summary

- **Research Conducted**
  - General Liability insurance exclusions
  - Cybersecurity-related insurance products
  - National Association of Insurance Commissioners Standards
  - OHIO Safe Harbor Bill
  - New Jersey Cybersecurity Bill
  - New York (NY) Financial Services
  - New York Shield law
  - United Kingdom (UK) Cybersecurity Policy
  - Wisconsin (WI) Broadband Bill
  - Indiana Office of Technology (IOT) Consumer TIPS ACT of 2017
  - Washington (WA) Biometric Bill
  - Small Business Cybersecurity Act 2017
  - New York Shield Law & NY Financial Services
  - Virginia HB 679 personal information
  - Verizon 2017 Data Breach report
  - Washington (HB 1493)
  - Cybersecurity insurance presentation by CHUBB
  - Cybersecurity insurance presentation by Travelers
  - Cybersecurity insurance presentation by Evolve MGA
  - State UDAP statutes, state Personal Information Protection Acts, state Data Breach of Security Acts for all 50 states plus District of Columbia
  - Federal statutes
  - General Data Protection Regulation (GDPR)

- **Research Findings**
  - Cybersecurity incidents are generally excluded from General Liability coverage.
  - A variety of companies are currently competing to serve the burgeoning market for insurance products covering cybersecurity-related services and risks.
  - There is no consistency between the cybersecurity policies currently offered in the marketplace.
  - There are approximately 12 different types of cybersecurity-related coverages.
  - There is no central collection of applicable state, federal and international laws with which Indiana businesses and local governments comply.

- **2021 Plan Working Group Deliverables**
  - Cyber Insurance Toolkit
  - Policy Review
  - Cyber Insurance Survey – Post-Covid
  - Funds Transfer Fraud Fact Sheet

- **Additional Notes**
  - None at this time

- **References**

Research

Research

1) What has your area done in the last five years to educate, train, and prepare for cybersecurity?

INDIANA DEPARTMENT of INSURANCE

a) There are now state laws governing cybersecurity breaches and reporting those breaches to the Indiana Department of Insurance. Indiana has enacted HB 1372 based on the National Association of Insurance Commissioners (NAIC) Insurance Data Security Model Law (MDL-668). The law requires state-regulated insurance entities to implement written information security programs, investigate and provide notification of cybersecurity events within a prescribed time, and maintain procedures for the secure disposal of nonpublic information.

b) As of July 1, 2021, Indiana law requires insurance companies and related entities in the insurance industry to report cybersecurity incidents and data breaches to the Indiana Department of Insurance.

i) HEA 1372 establishes a comprehensive regulatory framework requiring licensees to implement information security programs and report data breaches. HEA 1372 also empowers the Indiana Insurance Commissioner (IIC) to make related regulations and enforce the law.

ii) The law requires licensees to:

iii) Develop, implement, and maintain a comprehensive written information security program that:

iv) contains administrative, technical, and physical safeguards to protect nonpublic information;

v) is based on a risk assessment conducted by an employee, affiliate, or outside vendor;

vi) mitigates identified risks according to the licensee's size and complexity, the nature of its activities, and the sensitivity of the nonpublic information it controls; and

vii) defines and periodically reevaluates a retention schedule for nonpublic information and a procedure for its destruction when no longer needed.

viii) Establish a written incident response plan to promptly respond to and recover from cybersecurity events.

ix) Respond to a cybersecurity event by:

x) conducting a prompt investigation;

xi) performing or overseeing reasonable mitigation and restoration activities;

xii) notifying the IIC within three business days after determining that an event has occurred, under certain conditions; and

xiii) notifying affected consumers according to Indiana's consumer data breach notification law.

xiv) Notably, in contrast to the model law, HB 1372:

xv) Limits nonpublic information by excluding licensees' business-related information and focusing instead on consumers' personal data.

xvi) Does not include provisions regarding third-party service provider oversight or testing for externally developed applications.

xvii) Limits reportable cybersecurity events to those that have a reasonable likelihood of materially harming a consumer or any part of the licensee's normal operations.

xviii) Does not explicitly require program adjustments based on business or technical changes, and limits required program reporting to a licensee's executive management rather than its board of directors.

c) Offer and attending trainings both in person and virtually regarding how other state departments of insurance have handled cybersecurity breach notices.
d) Engaging in ongoing conversations with other state regulators with regards to cybersecurity enforcement and training.
e) The National Association of Insurance Commissioners (NAIC) formed an executive committee on cybersecurity and the IDOI/Indiana will serve as a committee member.
f) All cybersecurity insurance policies and rates offered by admitted insurers in the State of Indiana must first be filed with the Indiana Department of Insurance. The IDOI reviews the policy form and rate filings. Most commercial property and general liability policies do not cover cyber risks, and cyber insurance policies are highly customized for clients. In 2019, premiums were estimated at around $3.15 billion, a slight decrease of .22% from the prior year. This number reflects both stand-alone cybersecurity insurance products as well as those writing cybersecurity insurance as part of a package policy. The total Admitted Market for cybersecurity insurance coverage was about $2.03 billion and included both standalone and package policy coverage. The NAIC's notes that this amount represents a 6.81% increase over 2017 numbers.
g) The National Institute of Standards and Technology (NIST) has provided a framework for improving critical infrastructure cybersecurity. The framework provides a structure of standards, guidelines, and practices to aid organizations, regulators, and customers with critical infrastructures in effectively managing their cyber risks., most recently updated in 2018. The framework provides a structure of standards, guidelines, and practices to aid organizations, regulators and customers with critical infrastructures in effectively managing their cyber risks.
h) State insurance regulators serve on the U.S. Department of the Treasury's (Treasury Department) Financial Banking and Information Infrastructure Committee (FBIIC) where they work with federal regulators to address cyber threats in the United States. State insurance regulators continue to monitor cybersecurity in the insurance sector closely. In addition, regulators work with insurers to resolve immediate concerns when a data breach occurs at an insurance company. State insurance regulators are also in the unique position of regulating and monitoring the solvency and market activities of insurance carriers underwriting cybersecurity policies.
i) The IDOI led a national multi-state examination of Anthem following its data breach, which was the largest reported breach at the time, along with 49 states participating in the exam process.

INSURANCE INDUSTRY

a. Cyber Insurers and Brokers/Agents in the space have worked to educate the user-buyer community regarding the exposures, controls, and evolving landscape of Cyber Insurance through various forms. This has been an aggressively expanding and challenging area of Insurance so the marketing collateral and material publicly available is robust.
b. There have been numerous opportunities to educate and train on cybersecurity in the community through webinars, and training sessions that have been held. The IECC's cybersecurity guide that has resided on the state's cybersecurity hub, the Cybertech conferences that have been held in Indiana.

INDIANA ATTORNEY GENERAL

a. The Office of Indiana Attorney General worked with the Indiana State Chamber of Commerce to create a seminar on Cybersecurity
b. The Office of Indiana Attorney

2) What (or who) are the most significant cyber vulnerabilities in your area?

INDIANA DEPARTMENT of INSURANCE

a) The reasons the financial services sector is susceptible to cyberthreats are multifaceted. Financial firms receive, maintain and store substantial amounts of personally identifiable information (PII); however, insurers, in many cases, receive personal health information in addition to personal financial information from both policyholders and claimants.
b) Healthcare breaches continue to grow each year. Research indicates that personal health information continues to be more valuable to hackers than other types of financial records, such as credit cards. Personal health information generally provides more information regarding PII than a financial record. A report authored by Trustwave suggests that a health care record may be worth up to $250 per record on the dark web; a credit card record holds a value of $5.40 per person, per card.

INSURANCE INDUSTRY

a. The biggest vulnerability continues to be under-educated user-buyers not leveraging Cyber Insurance as a piece/part of a robust overall Cyber Risk Management program. With the rapid changes occurring in the market, insureds can be underprepared for the Underwriting Requirements for certain Cyber controls, programs, and protocols necessary to procure good coverage.
b. Healthcare systems, small to middle-market companies that do not have the resources to implement controls, as well as municipalities and rural towns that lack resources.

INDIANA ATTORNEY GENERAL

a. IT vendors and cloud-based software as service providers who manage the transfer and storage of data.

3) What is your area's greatest cybersecurity need and/or gap?

INDIANA DEPARTMENT of INSURANCE

a) Additional training pertaining to how state departments of insurance handle cybersecurity breach notices.

INSURANCE INDUSTRY

a. Connecting technical Cyber Risk Management (Like from the IT or CISO's perspective) with the risk transfer of Cyber Insurance, so the decision makers are making an informed buying decision on Insurance aligned with their strategic growth objectives.
a. Continued education that cybersecurity is important to every size company.

INDIANA ATTORNEY GENERAL

a. Education/Outreach to local governments, schools, and small businesses

4) To what federal, state, or local cyber regulations is your area beholden currently?

INDIANA DEPARTMENT OF INSURANCE

a) Indiana Codes §§ 27-2-27-1 – 27-2-27-32 (Chapter 27, Insurance Data Security)
b) The Computer Fraud and Abuse Act ("CFAA") 18 U.S.C. § 1030
c) Electronic Communications Protection Act ("ECPA") 18 U.S.C. § 2702; 18 U.S.C. § 2511
d) The Gramm-Leach-Bliley Act
e) The NAIC Financial Examination Handbook, incorporated by reference into Indiana Code
f) HIPAA exemption allowed under Indiana Law IC § 27-2-27

INDIANA ATTORNEY GENERAL

a. Ind. Code §4-1-6 Fair Information Practices
b. Ind. Code §4-1-10 Release of Social Security Number
c. Ind. Code §4-1-11 Notice of Security Breach
d. Ind. Code § 5-14-1.5-1 et seq. IN Driver's Privacy Protection Act
e. Ind. Code § 4-13.1-2-9 – Cyber Incident Report
f. Health Insurance Portability and Accountability Act (HIPAA) of 1996
g. Genetic Information Nondiscrimination Act ("GINA") of 2008

<u>The Indiana Attorney General Enforces:</u>

a. Ind. Code §4-1-10 Release of Social Security Number
b. Ind. Code §4-1-11 Notice of Security Breach
c. Ind. Code §4-6-13-1 et seq. Abandoned Records
d. Ind. Code §24-4.7-1-1 et seq. Telephone Solicitation of Consumers
e. Ind. Code §24-5-0.5-1 et seq. Deceptive Consumer Sales Act
f. Ind. Code §24-5-12-1 et seq. Telephone Solicitations Registration
g. Ind. Code §24-5-14-1 et seq. Regulation of Automatic Dialing Machines (Rococall)

h. Ind. Code §24-5-14.5-1 et seq. False or Misleading Caller Identification (Spoofing)
i. Telephone Consumer Protection Act of 1991 (TCPA) 47 U.S.C. § 227
j. Federal Regulations on Telemarketing, Telephone Solicitation and Facsimile Advertising 47 CFR § 64.1200
k. Telemarketing and Consumer Fraud and Abuse Prevention Act 15 USC §6103(e)
l. Telemarketing Sales Rule 16 CFR § Part 310
m. CAN-SPAM Act 15 USC ch. 103
n. CAN-SPAM Rule 16 CFR Part 316
o. Health Insurance Portability and Accountability Act (HIPAA) of 1996, 42 USC §1320d
p. HIPAA Privacy, Security, Breach Notice and Enforcement rules 45 CFR parts 160, 162, 164

INSURANCE INDUSTRY

a. Understanding the various State Breach Statutes, and Federal Regulations and Compliance requirements that impact a given insured in a specific industry is critical incorporation to the structuring, selection of an appropriate Cyber Insurance program.

5) What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?

INDIANA DEPARTMENT of INSURANCE

a) The IDOI has many resources and information developed both internally, from other states' departments of insurance, and from the NAIC.

INSURANCE INDUSTRY

a. Cyber Insurers and Agents/Brokers are constantly and consistently release Claim Scenarios documents and other material to inform the buying decisions.
b. There are many companies, such as AON, that have a very large cybersecurity practice, with a myriad of white papers available to publish and will continue to be thought leaders in the cybersecurity space.

INDIANA ATTORNEY GENERAL

a. White House memo from Anne Neuberger, Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology

6) What research is out there to validate your group's preliminary deliverables?

INDIANA DEPARTMENT of INSURANCE

a) The IDOI materials include studies from other states' departments of insurance, the federal government, and the NAIC.

INSURANCE INDUSTRY

a. No Response

INDIANA ATTORNEY GENERAL

a. State of Hoosier Cybersecurity 2020

7) What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?

INDIANA DEPARTMENT of INSURANCE

a) Attending trainings both in person and virtually regarding how other state departments of insurance have handled cybersecurity breach notices.
b) Drafted a cybersecurity model law (#668) for states to use as a drafting model for their respective legislation.
c) There is now an NAIC executive committee on cybersecurity. Previously, several working groups under NAIC to discuss cybersecurity: Innovation and Technology (EX) Task Force and Cybersecurity (EX) Working Group
    i) These working groups have adopted:
    (1) Principles for Effective Cybersecurity: Insurance Regulatory Guidance. Attached here.
    (2) Roadmap for Cybersecurity Consumer Protections. Attached here.
    (3) Updated the Financial Condition Examiners Handbook for revised cybersecurity protocols.
    (4) Made recommendations to update the Market Regulation Handbook
d) NAIC membership adopted a Cybersecurity Insurance and Identity Theft Coverage Supplement for the property/casualty annual financial statement to collect information about cybersecurity insurance markets.
e) Cybersecurity risks should be incorporated and addressed as part of an insurer's or an insurance producer's enterprise risk management (ERM) process. Cybersecurity transcends the information technology department and must include all facets of an organization.

INSURANCE INDUSTRY

a. No Response

INDIANA ATTORNEY GENERAL

b. State Attorneys General have recommended businesses follow the minimum examples outlined in the Memo by Anne Neuberger on June 2, 2021.

8) What does success look like for your area in one year, three years, and five years?

INDIANA DEPARTMENT of INSURANCE

a) Following state and federal statutes with regards to enforcement and regulation of cybersecurity within the insurance industry.

INSURANCE INDUSTRY

a. Cyber Insurance should now be considered a Duty-of-Care coverage that any/all business should include in their Insurance portfolio – Hopefully by connecting the dots between prudent Cyber Security postures and appropriate Cyber Insurance programs, we can begin to turn the tide of Ransomware and associated Insurance claims (which then impact the cost and structure of the policies to the insured).
a. That, at a minimum, every organization would understand the importance of implementing MFA as a fundamental control. That there is knowledge around the importance of cyber insurance and what it covers and how it can help organizations in the face of a breach.

INDIANA ATTORNEY GENERAL

a. At least weekly outreach events to local governments, schools, and small businesses throughout Indiana to discuss cyber threats and steps to prevent and protect against cybercrime.

9) What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?

INDIANA DEPARTMENT OF INSURANCE

a) The IDOI will post on its website cybersecurity resources available to consumers and industry.

INSURANCE INDUSTRY

a. Should the state through the Indiana Department of Insurance (or various Insurance organizations like the Big I) push additional Cyber Insurance education/training CE requirements as part of the Bi-annual Insurance License renewal?

INDIANA ATTORNEY GENERAL

a. Understanding the ways in which personal information is misused to harm consumers, through identity theft, fraud, and unfair practices.

10) What is the total workforce in your area in Indiana? How much of that workforce is cybersecurity related? How much of that cybersecurity-related workforce is not met?

INDIANA DEPARTMENT of INSURANCE

a) No Response

INSURANCE INDUSTRY

a. While the Insurance workforce in Indiana is robust, how much expertise/specialization in Cyber Insurance is undetermined.

INDIANA ATTORNEY GENERAL

a. No Response.

11) What do we need to do to attract cyber companies to Indiana?

INDIANA DEPARTMENT of INSURANCE

a) Consistency in regulation

INSURANCE INDUSTRY

a. No Response

INDIANA ATTORNEY GENERAL

a. Communications infrastructure.

12) What are your communication protocols in a cyber emergency?

INDIANA DEPARTMENT of INSURANCE

a) If there is a violation of Chapter 27 under Title 27, pursuant to Indiana Code § 27-2-27-27, the Commissioner may after notice and hearing suspend or revoke the license, certificate of authority, or registration of the licensee.

INSURANCE INDUSTRY

a. No Response

INDIANA ATTORNEY GENERAL

a. No Response

13) What best practices should be used across the sectors in Indiana?

INDIANA DEPARTMENT of INSURANCE

a) The cybersecurity financial examination and reporting requirements developed with the NAIC and implemented by state insurance departments could be adopted across sectors.

INSURANCE INDUSTRY

a. No Response

INDIANA ATTORNEY GENERAL

a. NIST Cybersecurity Framework

Deliverable: Insurance Toolkit

Deliverable: Insurance Toolkit

General Information

1. **What is the deliverable?**
   a. Using the Insurance Guide 1.0, develop a toolkit that will provide education and awareness for organizations regarding cyber insurance policies and best practices.

2. **What is the status of this deliverable?**
   ☐ Completed ☐ In-progress 25% ☐ In-progress 50% ☒ In-progress 75% ☐ Not Started

3. **Which of the following IECC goals does this deliverable meet?**
   ☐ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☒ Strengthen best practices to protect information technology infrastructure.
   ☐ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☒ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. A toolkit for Indiana residents describing the different types of coverages and services available in “cybersecurity policies”

6. **What metric or measurement will be used to define success?**
   a. Completed documents made publicly available through state websites.

7. **What year will the deliverable be completed?**
   ☐ 2021 ☒ 2022 ☒ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
    a. All Indiana businesses.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. None.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Strategic Resource and Cyber Awareness and Sharing Working Group
    b. State and Local Government

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. We have a sub-committee comprised of insurance brokers, corporations, and attorneys working on the content.
    b. Indiana Business Resource Council
    c. Indiana University

12. **Who should be main lead of this deliverable?**
    a. Michele Howell in conjunction with the Legal and Insurance Working Group

13. **What are the expected challenges to completing this deliverable?**
    a. Cyber risk and liability insurance is a new and fast-changing marketplace, so the information will likely change each year for the next five to ten years.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    ☐ One-time deliverable
    ☒ Ongoing/sustained effort
    a. This will require periodic updates, at least annually.

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Continued meetings with sub-committee to finalize content.	Michele Howell	75	December, 2021	
Review outline of toolkit for website	Legal and Insurance Working Group	25	Feb. 2022	
Layout and test web-based toolkit	Program Communications Manger	0	March 2022	
Finalize and launch toolkit	working group and communications manager	0	April 2022	

Resources and Budget

15. Will staff be required to complete this deliverable?

☐No ☒ Yes

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
¼ FTE	¼ FTE	Cybersecurity insurance broker	Cybersecurity Council office	Indiana General Assembly appropriation	
¼ FTE	1/16 FTE	Communications	Cybersecurity Council office	Indiana General Assembly	
¼ FTE	¼ FTE	Survey	Cybersecurity Council office	Indiana General Assembly	Secretary of State may need to be involved

16. What other resources are required to complete this deliverable?

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Website space	Making documents available for review or download	May be within scope of current IN website maintenance	unknown	IECC state support	Indiana Legislature	

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. By publishing details on types of services and insurance coverages commercially available, Indiana businesses and local governments will increase awareness and understanding of cyber risks and the products available to manage those risks.
b. By increasing the number of businesses protected against cybersecurity loss, Indiana's economy will be more resilient in the face of increasing cyber threats.

18. How will this deliverable reduce the cybersecurity risk or impact? What are the estimated costs associated with that risk reduction?

a. It has been estimated up to 60% of small and medium-sized businesses fail within 6 months of a cybersecurity attack. By encouraging small and medium-sized businesses to protect against cybersecurity risk, Indiana companies and local governments will be better protected.

19. What is the risk or cost of not completing this deliverable?

a. Up to 60% of small and medium-sized businesses fail within 6 months of a cybersecurity attack, and the risk of being targeted by an attack is rising exponentially. Indiana's economy could be damaged as the result of cyber-attacks against Indiana businesses and local government.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. A completed list of currently available cybersecurity coverages and services would mean success.
b. The Legal and Insurance working group collaborated with IU, ASU, IBRC, and the Indiana Attorney General to produce the first survey of Indiana businesses on Cybersecurity risk. The survey was conducted prior to the Pandemic. A follow up survey needs to be conducted to measure progress of businesses understanding of cyber risks compared to January 2020.
c. A toolkit placed on the website that allows users to quickly access specific information needed to better understand how to safeguard their business relative to cybersecurity.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

☒No ☐ Yes

a. Other states or jurisdictions are likely analyzing similar information, but we are not currently aware of concrete examples.
b. We are not aware of initiatives in other states.

22. Are there comparable jurisdictions (e.g. other states) that do not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

☒No ☐ Yes

a. We are not aware of similar initiatives in other states, but cybersecurity is a hot topic and there has been a flurry of activity at the state level.

Other Implementation Factors

---

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Availability of committee members.
b. Scheduling conflicts among committee members.
c. Lack of budget to conduct follow up study.

24. Does this deliverable require a change from a regulatory/policy standpoint?

☐No ☒ Yes

a. Making insurance coverage and specifically cybersecurity insurance coverage part of a corporation's annual or semi-annual filing with Secretary of State would require legislative and administrative change.

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. The list of applicable laws will require continual updating.
b. The types of coverages available under cybersecurity insurance policies are changing as cybersecurity risks change and will require continuous updating.
c. Surveys of businesses will require annual surveys or coordination with Indiana Chamber of Commerce or Secretary of State.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. Insurance policy coverages:
   i. American International Group (AIG)
   ii. Chubb
   iii. Travelers Insurance
   iv. CNA insurance
   v. AON

27. Can this deliverable be used by other sectors?

☐No ☒ Yes

a. All sectors

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. All stakeholders would benefit from this information.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

☐No ☒ Yes

30. What are other public relations and/or marketing considerations to be noted?

a. Indiana cybersecurity office could coordinate with the Director of Communications for Indiana University and Director of Communications for Office of Indiana Attorney General and Outreach for Office of Indiana Attorney General.
b. Indiana Chamber of Commerce could help promote.

Evaluation Methodology

Objective 1: IECC Legal and Insurance Working Group will develop a Cyber Insurance Toolkit to be provided to government and businesses by April 2022.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: With an effective communications plan, point more than 1,000 users access the Cyber Insurance Toolkit by December 2023.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☐ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☒ Quantifiable Measurement
☐ Other

Deliverable: Policy Review

Deliverable: Policy Review

General Information

1. **What is the deliverable?**
    a. List of cybersecurity laws and regulations for Indiana businesses and residents

2. **What is the status of this deliverable?**
    ☐ Completed ☐ In-progress 25% ☐ In-progress 50% ☒ In-progress 75% ☐ Not Started

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☒ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☒ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Companies, local governments, and individuals will be better able to comply with relevant laws.

6. **What metric or measurement will be used to define success?**
    a. A completed document that captures all current, applicable laws.

7. **What year will the deliverable be completed?**
    ☒ 2021 ☒ 2022 ☒ 2023 ☒ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
    a. The document will educate Indiana businesses and local government about their responsibilities under existing cyber laws.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. None.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Cyber Awareness and Sharing Working Group; Strategic Resources Working Group, State and Local Government

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Attorney General offices across the United States and data privacy and security attorneys on Legal and Insurance Working Group.

12. **Who should be main lead of this deliverable?**
    a. Doug Swetnam/Todd Vera

13. **What are the expected challenges to completing this deliverable?**
    a. Availability of committee members.
    b. Scheduling committee members.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**

☐ One-time deliverable

☒ Ongoing/sustained effort

a. Cybersecurity laws are rapidly changing, and new lists will need to be compiled at least annually, if not more frequently.

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Review and revise list of laws applicable to Indiana businesses and residents under current landscape	Doug Swetnam/Todd Vera	75	December 2021 and annual after this review	Federal and State legislation should be monitored for changes in existing laws.

Resources and Budget

15. Will staff be required to complete this deliverable?

☐No ☒ Yes

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
¼ FTE	¼ FTE	Legal – legislative – Track legislative updates to cyber laws in all jurisdictions affecting IN	Cybersecurity Council office or Indiana Attorney General	Indiana General Assembly appropriation	
¼ FTE	1/16 FTE	Communications	Cybersecurity Council office	Indiana General Assembly	

16. What other resources are required to complete this deliverable?

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Website space	Making documents available for review or download	May be within scope of current IN website maintenance	unknown	Cybersecurity Council office	Indiana legislature	

Benefits and Risks

17. What is the greatest benefit of this deliverable?

a. Businesses and local governments will have a legal reference to identify the current patchwork of cybersecurity laws, regulations and requirements.

18. How will this deliverable reduce the cybersecurity risk or impact? What are the estimated costs associated with that risk reduction?

a. It has been estimated up to 60% of small and medium sized businesses fail within 6 months of a cybersecurity attack. By making companies more aware of the legal requirements expected of them, and the potential penalties and liability for non-compliance, they will be better motivated to plan and prepare for a cyber emergency.

19. What is the risk or cost of not completing this deliverable?

a. Up to 60% of small and medium sized businesses fail within 6 months of a cybersecurity attack, and the risk of being targeted by an attack is rising exponentially. Indiana's economy could be damaged as the result of cyberattacks against Indiana businesses who are not prepared to respond to an incident.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Completing a review of the cybersecurity laws and regulations and then passing the information on to key leaders in Indiana.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

☒No ☐ Yes

a. Other states or jurisdictions are likely looking at these statistics, but we are not currently aware of concrete examples.
b. We are not aware of initiatives in other states, but there may be.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

☐No ☒ Yes

a. There is a possibility other states have comparable initiatives, though we are not aware of any at this time.

Other Implementation Factors

---

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Availability of legal resources to review and verify applicable laws and regulation.
b. With the fast pace of cybersecurity rules and regulations over the past several years it is possible to omit some.

24. Does this deliverable require a change from a regulatory/policy standpoint?

☒No ☐ Yes

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. The list of applicable laws will require continual updating.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. Applicable laws – Legal and Insurance working group

27. Can this deliverable be used by other sectors?

☐No ☒ Yes

a. All sectors

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. All stakeholders would benefit from this information.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

☐No ☒ Yes

30. What are other public relations and/or marketing considerations to be noted?

a. Cybersecurity Program Director for the IECC could coordinate with Office of Indiana Attorney General communications.

Evaluation Methodology

Objective 1: Legal and Insurance Working Group will review and distribute a list of cyber laws applicable to Indiana businesses and residents under the current landscape every year in December.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Funds Transfer Fraud Fact Sheet

Deliverable: Funds Transfer Fraud Fact Sheet

General Information

1. **What is the deliverable?**
    a. Funds Transfer Fraud Fact Sheet

2. **What is the status of this deliverable?**
☐ Completed ☒ In-progress 25% ☐ In-progress 50% ☐ In-progress 75% ☐ Not Started

3. **Which of the following IECC goals does this deliverable meet?**
☐ Establish an effective governing structure and strategic direction.
☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
☐ Strengthen best practices to protect information technology infrastructure.
☐ Build and maintain robust statewide cyber-incident response capabilities.
☒ Establish processes, technology, and facilities to improve cybersecurity statewide.
☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable?**
☐ Research – Surveys, Datasets, Whitepapers, etc.
☒ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Train people on behaviors that will help save them from sending out funds for fraudulent reasons. Help explain what to look out for in terms of phishing, fraudulent requests, compromised email accounts, and other threats.

6. **What metric or measurement will be used to define success?**
    a. No observable metric. There is no way to track metrics except for anecdotal.

7. **What year will the deliverable be completed?**
   ☒ 2021 ☐ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. Any organization that participates in Electronic Funds Transfer

9. **Which state or federal resources or programs overlap with this deliverable?**
   a. None at this time

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. None

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. None

12. **Who should be main lead of this deliverable?**
    a. Leon Ravenna

13. **What are the expected challenges to completing this deliverable?**
    a. None

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    ☒ One-time deliverable
    ☐ Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Complete Funds Transfer Worksheet	Leon Ravenna	25	10/30/2021	

Resources and Budget

15. Will staff be required to complete this deliverable?

☒No ☐ Yes

16. What other resources are required to complete this deliverable?

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
None						

Benefits and Risks

17. What is the greatest benefit of this deliverable?

a. Specifically, having ways to avoid being caught by fraudulent means to send out company funds that cannot, in many cases, be recovered.

18. How will this deliverable reduce the cybersecurity risk or impact? What are the estimated costs associated with that risk reduction?

a. It will reduce risk be educating people as to what fraudulent funds transfers look like, how to spot and avoid these issues to avoid making fraudulent funds transfers. There are no costs except for the time to read and apply fundamental information.

19. What is the risk or cost of not completing this deliverable?

a. Risk is primarily that people will unknowingly send out funds to fraudulent sites and then (in some cases) having to pay original vendors as well.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Only anecdotal metrics will be available. It would be possible to see if claims to the Attorney General's (A/G) office reduced year over year are, but this may be a stretch.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

☒No ☐ Yes

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

☒No ☐ Yes

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. None

24. Does this deliverable require a change from a regulatory/policy standpoint?

☒No ☐ Yes

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. Occasional (potential bi-yearly updates)

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. Leon Ravenna CISO, KAR Global, Christine Collins Director, Incident Response & Investigations KAR Global and Former FBI Agent

27. Can this deliverable be used by other sectors?

☐No ☒ Yes,

a. Any that perform funds transfers such as Healthcare

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Chetrice Romero, Doug Swetnam

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

☐No ☒ Yes

30. What are other public relations and/or marketing considerations to be noted?

a. None at this time.

Evaluation Methodology

Objective 1: IECC Legal and Insurance Working group will develop a Funds Transfer Fraud Fact Sheet to be provided to government and businesses by January 2022.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Cyber Insurance – Survey Post-Covid

Deliverable: Cyber Insurance Survey – Post-Covid

General Information

1. **What is the deliverable?**
    a. In 2019 the Legal and Insurance Working Group conducted a survey with the assistance of Indiana University of Indiana businesses who have cybersecurity insurance coverage. Since 2020 and the pandemic, the landscape of cybersecurity has changed. The Legal and Insurance Working Group would like to redistribute that survey with the assistance of Indiana University of Indiana businesses who have cybersecurity insurance coverage to see what we as a state can learn from the findings.

2. **What is the status of this deliverable?**
    ☐ Completed ☐ In-progress 25% ☐ In-progress 50% ☐ In-progress 75% ☒ Not Started

3. **Which of the following IECC goals does this deliverable meet?**
    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☒ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable?**
    ☒ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. This will require periodic updates, at least annually. The initial objective is to create a baseline measurement of cybersecurity risk management analyses undertaken by Indiana businesses.

6. **What metric or measurement will be used to define success?**
   a. A steadily increasing number of Indiana businesses who have gone through a process to assess their cybersecurity risks and make an informed business decision as a result of that review. (Whether they choose to insure, or not.)

7. **What year will the deliverable be completed?**
   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. Individual Indiana businesses will benefit from making informed cyber risk assessments, and the Indiana economy as a whole will benefit by being better prepared for cyber risks.

9. **Which state or federal resources or programs overlap with this deliverable?**
   a. The Indiana Department of Insurance gathers annual information on admitted carriers, but we do not believe any entity is currently conducting the survey we are suggesting.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Cyber Awareness and Sharing working Group; Strategic Resources Working Group.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Indiana Secretary of State

12. **Who should be main lead of this deliverable?**
    a. Legal and Insurance Working Group and the Cybersecurity Program Director

13. **What are the expected challenges to completing this deliverable?**
    a. Lack of budget to complete new survey.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    ☒ One-time deliverable
    ☐ Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Conduct a survey of businesses for insurance coverage and cybersecurity insurance coverage.	Chair/Co-Chair with Indiana University	0	Qtr 1 2022	
Analyze findings and report it out to the IECC and state leadership	Chair/Co-Chair with Indiana University			

Resources and Budget

15. Will staff be required to complete this deliverable?

☐No ☒ Yes

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
¼ FTE	¼ FTE	Survey	State of Indiana	Indiana General Assembly	Secretary of State should be involved.

16. What other resources are required to complete this deliverable?

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Website space	Making documents available for review or download	May be within scope of current IN website maintenance	Unknown	Unknown	Unknown	

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. By publishing details on types of services and insurance coverages available, Indiana will increase awareness and understanding of the need for cyber risk coverage.
b. By increasing the number of businesses protected against cybersecurity loss, Indiana's economy will be more resilient in the face of increasing cyber threats.

18. How will this deliverable reduce the cybersecurity risk or impact? What are the estimated costs associated with that risk reduction?

a. It has been estimated that up to 60% of small and medium sized businesses fail within six (6) months of a cybersecurity attack. By encouraging small and medium sized businesses to protect against cybersecurity risks, Indiana companies will be better protected.

19. What is the risk or cost of not completing this deliverable?

a. Up to 60% of small and medium sized businesses fail within six (6) months of a cybersecurity attack and the risk of being targeted by an attack is rising exponentially. Indiana's economy could be damaged as the result of cyberattacks against Indiana businesses.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. There is no current survey of Indiana businesses on this subject. The Cybersecurity Council could work with (1) the Indiana Chamber of Commerce or (2) the Office of the Indiana Secretary of State to conduct a survey of Indiana businesses and use the increase of businesses covered by cybersecurity policies as a measure of success.

21. Are there comparable jurisdictions (e.g., other states) that have similar projects that we can compare this project to using the same metrics?

☒No ☐ Yes

a. Other states or jurisdictions are likely looking at these statistics, but we are not currently aware of concrete examples.

22. Are there comparable jurisdictions (e.g., other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

☒No ☐ Yes

a. We are not aware of initiatives in other states. But there may be.

Other Implementation Factors

---

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Lack of budget to conduct survey.

24. Does this deliverable require a change from a regulatory/policy standpoint?

☒No ☐ Yes

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. Surveys of Indiana businesses will require annual surveys or coordination with the Indiana Chamber of Commerce or the Office of the Indiana Secretary of State.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. Indiana University Scott Shackelford and Cybersecurity Program Director

27. Can this deliverable be used by other sectors?

☐No ☒ Yes

a. All sectors

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. All stakeholders would benefit from this information.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

☐No ☒ Yes

30. What are other public relations and/or marketing considerations to be noted?

a. The Indiana Cybersecurity Office could coordinate with Office of the Indiana Attorney General's communications team.

Evaluation Methodology

Objective 1: Legal and Insurance Working Group with Indiana University will conduct a post-COVID survey of businesses for insurance coverage and cybersecurity insurance coverage by June 2022.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: IECC Legal and Insurance Working Group with Indiana University will provide a report of the findings of the cyber insurance survey to the IECC by September 2022.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☒ Qualitative Analysis
☒ Quantifiable Measurement
☐ Other

Supporting Documentation

Supporting Documentation

This section contains all of the associated documents that are referenced in this strategic plan and can be used for reference, clarification, and implementation details.

- Cyber & Technology Insurance Guide - Version 1
- Survey of Cyber Laws – 2019
- Business Insurance Survey and Report – 2020

Cyber & Technology Insurance Guide - Version 1

IECC Legal and Insurance Working Group

Cyber & Technology Insurance Guide Version 1

August 2018

CYBER & TECHNOLOGY INSURANCE COVERAGE

Today, consumers, businesses, and government agencies use internet-capable devices every day. These high tech devices – from laptops to security systems to medical devices – increase efficiency in the collection and exchange of data, and revolutionize industries. Cyber technology also brings new risks. Large companies subject to data breaches have made headlines, but small and mid-size companies that collect data and private information may also be vulnerable. Businesses may be obligated to protect private information by governing laws and regulations – such as Personally Identifiable Information, Personal Health Information and Confidential Corporate Information. Smaller businesses may not be able to survive the costs associated with a data breach. One of the largest growing financial risks a business must face is a cyber breach. Insurance is a necessary component of a business's risk management and disaster recovery plan. Inadequately insured businesses are unlikely to survive major incidents.

Until recently, most businesses have insured only computer equipment and mobile devices against physical risks such as damage, theft, or fire loss. Electronic equipment was insured on the same basis as furniture and automobiles, with no coverage for lost, stolen or disrupted data. Some organizations may have had wider, more extensive policies that also include coverage for equipment breakdown and limited expenses for reinstatement of data, but most cyber risks are now excluded under traditional commercial general liability policies.

Insurers and businesses have recognized that traditional insurance is inadequate, and there is a need for tailored cyber liability insurance to cover a wide variety of exposures that can result from technology-related activities -- from misplaced company cell phones to cyberattacks. Cyber liability insurance is intended to address an insured's obligation to protect private information from inappropriate access undergoing significant changes and likely will continue to do so as it is linked to the ever-changing world of technology. Therefore, it is important to know the terminology, to review your risks, and to determine your coverage needs. Cyber liability insurance is increasingly becoming an important consideration for conducting business in a high-tech marketplace.

FREQUENTLY ASKED QUESTIONS

Q What is cyber liability?

A Cyber liability is the risk of a data breach as a result of online activities and the use of electronic storage technology.

Q What is cyber liability insurance?

A While policies vary, cyber liability insurance is designed to protect a business or organization from:

- Liability claims involving the unauthorized release of information for which the organization has a legal obligation to keep private or confidential, such as employee, patient or customer records.

- Liability claims alleging invasion of privacy.
- Liability claims alleging failure of computer security that results in alterations of data and defense costs.

- Data Response Services, including legal, computer forensics, notification services, credit and identity monitoring products and crisis management expertise, and the reimbursement to the insured for certain out-of-pocket expenses.

Q What is a data breach?

A A data breach occurs when secured information is released to or accessed by unauthorized individuals. The lost data may be employee personnel records, customer financial accounts, or business trade secrets. The incidents pose serious risks for organizations as well as the individuals whose data has been lost or disseminated.

Q How do data breaches happen?

A Data breaches can occur by accident, such as an employee sends out an unsecured email, or by crime, such as a malicious hacker.

Q What data or information do businesses need to secure?

A Most businesses generate vast amounts of data which is available and stored on their electronic storage network systems, which may be subject to certain privacy laws:

- Personal information:
  - Personally identifiable information (PII): name, address, date of birth, telephone number, email address, Social Security number, zip code, biometric data.
  - Protected health information (PHI): healthcare-based treatment information, medical history, health insurance information, including member identification numbers.

- Corporate information: intellectual property, business, contracts, attorney-client privileged information:
  - Payment cardholder information (PCI): credit/debit card data, including account numbers, security codes, insurance account information, etc.

- Cyber-based data: web browser history, cookie information, metadata, and IP addresses.

Q Why consider cyber liability insurance?

A

There are various reasons why a company may want to consider cyber liability insurance as a way to protect confidential data and insure the risk against financial exposure:

- Frequency of privacy breaches are on the rise;
- Threats are getting dramatically worse;
- Almost all 50 states have enacted privacy laws in response to privacy breaches;
- Consumers expect that their confidential information will be protected.
- Class action litigation is becoming more active as a result of privacy breaches.
- Many business contracts now require cyber insurance.
- Cyber liability insurance products are becoming more widely available.

GLOSSARY OF CYBER INSURANCE TERMS

Breach Response – Investigation. Costs incurred to investigate data breach; investigate potential indemnity.

Breach Response – Notification. Costs incurred to notify individuals of breach.

Breach Response – Public Relations. Costs incurred to hire public relations firm.

Breach Response – Remediation. Costs incurred to remediate data breach (e.g., credit monitoring, call center, etc.).

Business Income (or Business Interruption Income Loss) is defined as net profit or loss before income taxes, as well as the continuing normal operating and payroll expenses.

Claim Expenses include reasonable and necessary legal fees, costs, and expenses incurred in the investigation, adjustment, defense, or appeal of a claim. They also typically include the cost of any bond or appeal bond required in any defended suit.

Computer System means computer hardware and software, and the electronic data stored thereon, as well as associated input and output devices, terminal devices, data storage devices, networking equipment, components, software, and electronic backup facilities, including systems accessible through the internet, intranets, extranets, or virtual private networks.

Cyber Attack (Denial of Service Attack) is action preventing an information system from functioning in accordance with its intended purpose; the inability of an authorized third party to access the company's Computer System; and the inability of an authorized third party to access his or her Computer System, where such inability is directly cause by the company's Computer System.

Cyber Extortion. Losses and expenses arising out of a criminal threat to release sensitive information or bring down a system/network.

Damages/Loss includes the amounts the business is legally obligated to pay as a result of a covered judgment, award, or settlement; costs charged against the business in any suit; or pre-

judgment and post-judgment interest and defense costs. It also includes punitive or exemplary damages where insurable by law.

Data Restoration – Security Failure. Costs to restore lost data caused by security failure.

Data Restoration – System Failure. Costs to restore lost data caused by system failure.

Denial of Service Attack is action preventing an information system from functioning in accordance with its intended purpose (see Cyber Attack).

Extra Expense means any reasonable and necessary expenses in excess of the business's normal operating expenses that the business incurs during the Period of Restoration associated with restoring and resuming operations, including securing temporary third-party Internet Service Provider services, temporary website and/or email hosting services, rental of temporary networks, or other temporary equipment or service contracts.

First Party Claim. A first party claim is brought by an insured under the insured's cyber policy for a loss that occurs because of loss or damage to the insured's business.

Funds Transfer and Computer Fraud – Social Engineering. Loss of money or property arising from *bona fide* wire instructions induced through social engineering.

Funds Transfer and Computer Fraud – Traditional Coverage. Loss of money or property arising from fraudulent wire instructions or fraudulent entries into a computer system.

Identity Restoration Services typically means consultation and assistance to an individual receiving notification services to determine whether identity theft has occurred, and, if so, to restore the individual's identity to pre-theft status.

Media or Electronic Publishing Incident means the actual or alleged unintentional libel, slander, trade libel, or disparagement resulting from the insured electronic publishing. It also includes plagiarism, violation of privacy, infringement of a copyright or trademark, or unauthorized use of titles formats, plots, or other protected material resulting from the insured's electronic or media publishing.

Media Liability. Claim by third party in connection with the insured's media content, which may include claim for trademark infringement, defamation, libel, product disparagement, copyright violation, or invasion of privacy.

Network/Computer System typically includes the computer hardware, software, and electronic data, as well as associated input and output devices, terminal devices, data storage devices, networking equipment, components, software, and electronic backup facilities, including systems accessible through the Internet, intranets, extranets, or virtual private networks.

Network Interruption – Contingent BI. Loss of income arising from business interruption caused by third-party service failure (including mitigation expenses).

Network Interruption – Security Failure. Loss of income arising from business interruption caused by security failure (including mitigation expenses).

Network Interruption – System Failure. Loss of income arising from business interruption caused by system failure (including mitigation expenses).

Network Security Liability. Claim by third party arising from the insured's failure of network security.

Network Security/Cyber Incident typically means any Unauthorized Access/Use of, or introduction of malicious code into, or Denial of Service Attack upon, the company's Computer System, that directly results in an interruption in services; or the corruption of deletion of digital assets.

Notification Services typically mean the preparation and distribution of notice letters from the insured advising individuals of the network security event and the availability of related resources if such notices are required by applicable law, as well as call center support services.

Period of Restoration is the period from which the business first suffered an interruption in service to the date and time it was restored (or could have been restored) with reasonable speed to substantially return to the level of operation that existed prior to the interruption. There is typically a limit on the policy that the period of restoration cannot exceed thirty days.

Personal Identifiable Information (PII) is information not available to the general public from which a person can be identified. This definition should be broad enough to include a person's name, telephone number, Social Security number, medical or healthcare data, driver's license number or state identification number, account number, credit and debit card number, or password.

Privacy Incident is the unintentional and unauthorized disclosure of Personal Identifiable Information or confidential information in the care, custody, or control of the business or service provider; a violation of a Privacy Regulation; or failure to comply with the term's own privacy policies.

Privacy Liability – Business Records Claim. Claim by third party arising from the insured's failure to protect trade secrets or other confidential business information.

Privacy Liability – Privacy Claim. Claim by third party arising from the insured's failure to protect personal information (including PII, PHI and FAI).

Privacy Liability – Regulatory Claims. Third party liability coverage that generally is designed to protect an insured business in connection with certain requests for information, investigative demands and/or civil proceedings often brought by or on behalf of a governmental agency arising from the insured's failure to protect personal information. The coverage often includes civil fines and penalties imposed on the insured, to the extent such fines and penalties are insurable by law.

Privacy Notification Costs are reasonable and necessary costs to hire a security expert to determine the existence and cause of a breach; costs to notify consumers under a breach notification law; or fees incurred to determine the actions necessary to comply with a breach notification law.

Privacy Regulation means statutes associate with the control and use of personally identifiable financial, medical, or other sensitive information.

Public Relations Expense typically means the hiring of a public relations firm or crisis management firm for communication services to explain the nature of the network security/cyber event and any corrective actions taken.

Regulatory Fines includes civil money penalties imposed by a federal, state, local, or foreign government entity pursuant to a regulatory proceeding.

Regulatory Proceeding is an investigation of an insured by an administrative, regulatory, or government agency concerning a Privacy Incident; or an administrative adjudicative proceeding for a privacy Wrongful Act or network security Wrongful Act.

Regulatory Injury means injury sustained by a person due to actual or alleged disparagement of an organization's products or services; libel or slander of natural person; or violation of such person's rights of privacy or publicity result from cyber activities.

Retroactive Date means the date in the declarations section of the policy. If no date is set forth in the declarations page, then the retroactive date is the date of the inception of the policy.

Reward Payment/Expenses/Cyber Extortion Costs means the reasonable amount paid by the business, with prior approval of the insurer, to an informant for information not otherwise available, which leads to the arrest and conviction of persons responsible for a cyber attack or threat covered under the policy.

Service Provider means a business the business does not own, operate or control, but that the insured hires and contracts to perform services related to the business' computer systems, including maintaining the computer system; hosting the business' internet website; handling, storing or destroying information and confidential materials; or providing other IT-related services.

Technology Errors & Omissions. Claim by third party for financial loss arising from errors or omissions in the technology-facing component of the insured's business (tech services or products).

Third Party Claim. A third party claim is a demand against the business for monetary damages or non-monetary relief; a written demand for arbitration; or a civil proceeding brought by the service of a complaint or similar pleading.

Unauthorized Access/Use is the use of, or access to, a computer system by a person unauthorized by the insured to do so, or the authorized use of, or access to, a Computer System in a manner not authorized by the insured.

Wrongful Act typically means the actual or alleged act, unintentional error, omission, neglect, or breach of duty by an insured business or Service Provider that directly results in a breach of the insured's network.

Survey of Cyber Laws – 2019

Survey of Indiana Cyber Laws

Title or Description	Standard Type	Reference	Synopsis	Penalty	Statute of Limitations	Enforcement
IN Senate Bill 221 - E-Prescription Bill	State	SB 221	The bill requires prescribers to have access to and utilize INSPECT, a state-sponsored website database that allows practitioners to check a patient's controlled substance prescription history	https://iga.in.gov/legislative/2018/bills/senate/221		https://iga.in.gov/legislative/2018/bills/senate/221
IN Telephone Solicitation of Consumers ("Do Not Call Law")	State	IC art. 24-4.7	" A telephone solicitor may not make or cause to be made a telephone sales call to a telephone number if that telephone number appears in the most current quarterly listing published by the division." IC § 24-4.7-4-2.	$10,000 for the first call; $25,000 for subsequent calls. IC § 24-4.7-5-2(a)(2).	2 years after the call is made. IC § 24-4.7-5-4.	Attorney General: IC § 24-4.7-5-1.
IN Do Not Text Law	State	IC art. 24-4.7	"A telephone solicitor may not make or cause to be made a telephone sales call to a telephone number if that telephone number appears in the most current quarterly listing published by the division." IC § 24-4.7-4-2. A Telephone sales call can be defined as the "transmission of: a text message . . ." IC § 24-4.7-2-9(b)	$10,000 for the first call; $25,000 for subsequent calls. IC § 24-4.7-5-2(a)(2).	2 years after the call is made. IC § 24-4.7-5-4.	Attorney General: IC § 24-4.7-5-1.
IN Prohibited Spyware	State	IC art. 24-4.8	A person who is not the owner or operator of the computer may not knowingly or intentionally: (1) transmit computer software to the computer; and (2) by means of the computer software transmitted under subdivision (1), do any of the following" including deceptively modify computer settings or collect personally identifying information among other things. IC § 24-4.8-2-2.	Damages or $100,000: IC § 24-4.8-3-1(2).	Undefined by statute.	Private right of action: IC § 24-4.8-3-1.
IN Disclosure of Security Breach Act	State	IC art. 24-4.9	After a data security breach involving "personal information," a "data base owner" may need to alert (1) affected Indiana residents, (2) the attorney general, (3) consumer reporting agencies, and (4) the data base owner (if the breached party is not the data base owner). Must notify without unreasonable delay (likely within 30 days of the breach discovery). IC § 24-4.9.-3-1; IC § 24-4.9.-3-2.	$150,000 per notification type: IC § 24-4.9.-4-2(2)	Likely 2 years from notification of Attorney General. Undefined by the statute.	Attorney General: IC § 24-4.9-4-2
IN Protection of Personal Information	State	IC § 24-4.9-3-3.5(c)	"A data base owner shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any personal information of Indiana residents collected or maintained by the data base owner." "A person that knowingly or intentionally fails to comply with any provision of this section commits a deceptive act . . ."	$5,000 per deceptive act: IC § 24-4.9-3-3.5(c).	Likely 2 years from notification of Attorney General. Undefined by the statute.	Attorney General: IC § 24-4.9-3-3.5(f)
IN Disposal of Personal Information	State	IC § 24-4.9-3-3.5(d)	" A data base owner shall not dispose of or abandon records or documents containing unencrypted and unredacted personal information of Indiana residents without shredding, incinerating, mutilating, erasing, or otherwise rendering the personal information illegible or unusable."	$5,000 per deceptive act: IC § 24-4.9-3-3.5(c).	Likely 2 years from notification of Attorney General. Undefined by the statute.	Attorney General: IC § 24-4.9-3-3.5(f)
IN Disposal of Personal Information	State	IC § 24-4-14-8	"A person who disposes of the unencrypted, unredacted personal information of a customer without shredding, incinerating, mutilating, erasing, or otherwise rendering the information illegible or unusable commits a Class C infraction."	Class C or Class A infraction: IC § 24-4-14-8; 34-28-5-4	2 years: IC § 34-28-5-1(c)(2)	Prosecuting Attorney: IC § 34-28-5-1
IN Disposal of Electronic Waste	State	IC § 13-20.5-10-1	Covered entities cannot dispose of electronic in a landfill or through incineration	None: IC § 13-20.5-10-2	NA	NA
IN Deceptive Consumer Sales Act	State	IC ch. 24-5-0.5	"A supplier may not commit an unfair, abusive, or deceptive act, omission, or practice in connection with a consumer transaction. Such an act, omission, or practice by a supplier is a violation of this chapter whether it occurs before, during, or after the transaction. An act, omission, or practice prohibited by this section includes both implicit and explicit misrepresentations." IC § 24-5-0.5-3(a)	$5,000 per knowingly deceptive act: IC § 24-5-0.5-4(g)	2 years after the occurrence of the deceptive act: IC § 24-5-0.5-5.	Private Right of action and Attorney General: IC § 24-5-0.5-4(c)
IN Regulation of Automatic Dialing Machines	State	IC ch. 24-5-14	Indiana's Auto Dialer law prohibits most prerecorded calls, commonly known as "robo-calls," made via an automatic dialing-announcing device ("ADAD") regardless of the subject matter of the message. IC § 24-5-14-5(b).	$5,000 per knowingly deceptive act: IC § 24-5-0.5-4(g)	2 years after the occurrence of the deceptive act: IC § 24-5-0.5-5.	Attorney General: IC § 24-5-14-13.
IN Do Not Fax Law	State	IC § 24-5-0.5-3(b)(19).	Prohibition on sending unsolicited facsimile ("fax") advertisements . The law applies to advertisements sent to residential and business fax numbers. Unlike the Do Not Call law, the Do Not Fax law does not require people to register their fax numbers.	$5,000 per knowingly deceptive act: IC § 24-5-0.5-4(g)	2 years after the occurrence of the deceptive act: IC § 24-5-0.5-5.	Attorney General: IC § 24-5-14-13.

IN Deceptive Commercial Electronic Mail	State	IC ch. 24-5-22	Prohibition on sending unsolicited commercial electronic mail, when failing to comply with statutory sending standards. IC § 24-5-22-8.	Damages or $500 per email: IC § 24-5-22-10(d)(2).	Undefined by statute.	Private right of action: IC § 24-5-22-10(a).
IN Health Records and Identifying Information Protection	State	IC ch. 4-6-14	Provision relates to the Indiana Attorney General's responsibility related to abandoned health records and other records that contain personal information.	NA	NA	NA
IN Notice of Security Breach Act for State Agencies	State	IC ch. 4-1-11	"Any state agency that owns or licenses computerized data that includes personal information shall disclose a breach of the security of the system following discovery or notification of the breach to any state resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person." IC § 4-1-11-5.	NA	NA	NA
IN Release of Social Security Numbers by State Agencies	State	IC § 4-1-10, et seq.	Details the scope of permissible disclosures of Social Security numbers as well as the consequences for violations of the statute.	Level 6 felony: IC § 4-1-10-8; Class A infraction: IC § 4-1-10-10.		Attorney General: IC §§ 4-1-10-11; 4-1-10-12.
IN Release of Social Security Numbers by State Agencies, Notice to Attorney General: Rules	Rule	10 IAC § 5-4-1	"When a state agency becomes aware of a release of Social Security numbers or other personal identifying information, the state agency or employee shall, within two (2) business days of the disclosure, notify the office of attorney general for the state in writing . . ."	NA	NA	NA
IN Driver's Privacy Protection Act ("DPPA")	State	IC § 9-14-13-2	Prohibits the disclosure of personal information associated with motor vehicle records by the Indiana Bureau of Motor Vehicles.	Class C misdemeanor: IC § 9-14-13-11	2 years: IC § 34-28-5-1(c)(2)	Prosecuting Attorney: IC § 33-39-1-5
IN Criminal Law - Wiretap Statute	State	IC art. 35-33.5	Provision outlines the requirements for the state to obtain a warrant to intercept the telephonic or telegraphic communications of an individual.	Suppression of Evidence: IC § 35-33.5-4-4.	NA	NA
IN Rights of Victims of Identity Deception: Civil	State	IC § 24-5-26-2	Provision outlines the duties of those that conduct trade or commerce concerning the protections for victims of identity theft.	$5,000: IC § 24-5-26-3	2 years from the mistreatment date: IC § 24-5-26-3	Attorney General: IC § 24-5-26-3
IN Rights of Victims of Identity Deception: Criminal	State	IC ch. 35-40-14	Provision outlines the duty of law enforcement agencies concerning identity theft and the protections for victims of identity theft.	NA	NA	NA
IN Criminal Law - Offense Against Intellectual Property	State	IC § 35-43-1-7	A person who knowingly or intentionally and who without authorization: (1) modifies data, a computer program, or supporting documentation; (2) destroys data, a computer program, or supporting documentation; or (3) discloses or takes data, a computer program, or supporting documentation that is: (A) a trade secret (as defined in IC 24-2-3-2); or (B) otherwise confidential as provided by law; and that resides or exists internally or externally on a computer, computer system, or computer network, commits an offense against intellectual property, a Level 6 felony.	Level 6 Felony: IC § 35-50-2-7	5 years: IC § 35-41-4-2(a)(1)	Prosecuting Attorney: IC § 33-39-1-5
IN Criminal Law - Offense Against Computer Users	State	IC § 35-43-1-8	(a) A person who knowingly or intentionally and who without authorization: (1) disrupts, denies, or causes the disruption or denial of computer system services to an authorized user of the computer system services that are: (A) owned by; (B) under contract to; or (C) operated for, on behalf of, or in conjunction with; another person in whole or part; (2) destroys, takes, or damages equipment or supplies used or intended to be used in a computer, computer system, or computer network; (3) destroys or damages a computer, computer system, or computer network; or (4) introduces a computer contaminant into a computer, computer system, or computer network; commits an offense against computer users, a Level 6 felony.	Level 6 Felony: IC § 35-50-2-7	5 years: IC § 35-41-4-2(a)(1)	Prosecuting Attorney: IC § 33-39-1-6
IN Criminal Law - Identity Deception	State	IC § 35-43-5-3.5	(a) Except as provided in subsection (c), a person who knowingly or intentionally obtains, possesses, transfers, or uses the identifying information of another person, including the identifying information of a person who is deceased: (1) without the other person's consent; and (2) with intent to: (A) harm or defraud another person; (B) assume another person's identity; or (C) profess to be another person; commits identity deception, a Level 6 felony.	Level 6 Felony: IC § 35-50-2-7	5 years: IC § 35-41-4-2(a)(1)	Prosecuting Attorney: IC § 33-39-1-7

IN Criminal Law - Synthetic Identity Deception	State	IC § 35-43-5-3.8	(a) A person who knowingly or intentionally obtains, possesses, transfers, or uses the synthetic identifying information: (1) with intent to harm or defraud another person; (2) with intent to assume another person's identity; or (3) with intent to profess to be another person; commits synthetic identity deception, a Level 6 felony.	Level 6 Felony: IC § 35-50-2-7	5 years: IC § 35-41-4-2(a)(1)	Prosecuting Attorney: IC § 33-39-1-8
IN Criminal Law - Fraud	State	IC § 35-43-5-4	Encompasses different types of fraud including obtaining property by use of another's credit card unlawfully.	NA	5 years: IC § 35-41-4-2(a)(1)	Prosecuting Attorney: IC § 33-39-1-9
IN Criminal Law - Unlawful Possession of a Card Skimming Device	State	IC § 35-43-5-4.3	A person who possesses a card skimming device with intent to commit: (1) identity deception (IC 35-43-5-3.5); (2) synthetic identity deception (IC 35-43-5-3.8); (3) fraud (IC 35-43-5-4); or (4) terroristic deception (IC 35-43-5-3.6); commits unlawful possession of a card skimming device. Unlawful possession of a card skimming device under subdivision (1), (2), or (3) is a Level 6 felony. Unlawful possession of a card skimming device under subdivision (4) is a Level 5 felony.	Level 5 Felony: IC § 35-50-2-6	5 years: IC § 35-41-4-2(a)(1)	Prosecuting Attorney: IC § 33-39-1-10
IN Unlawful Recording	State	IC § 35-46-8-4	"A person who knowingly or intentionally uses an audiovisual recording device in a motion picture exhibition facility with the intent to transmit or record a motion picture commits unlawful recording, a Class B misdemeanor."	Class B misdemeanor: IC § 35-50-3-3	2 years: IC § 35-41-4-2(a)(2)	Prosecuting Attorney: IC § 33-39-1-11
IN Unlawful Photography and Surveillance of Private Property	State	IC § 35-46-8.5-1	"A person who knowingly or intentionally places a camera or electronic surveillance equipment that records images or data of any kind while unattended on the private property of another person without the consent of the owner or tenant of the private property commits a Class A misdemeanor." Note: Numerous exceptions enumerated within the statute.	Class A misdemeanor: IC § 35-50-3-2	2 years: IC § 35-41-4-2(a)(2)	Prosecuting Attorney: IC § 33-39-1-12
IN State Insurance Commissioners **Navigators and Application Organizations**	State	760 IAC § 4-5-2	"Navigators and application organizations shall comply with the following safeguards to maintain and protect the confidentiality of personal information:"	Up to $10,000 per violation: 760 IAC § 4-7-1(d)	NA	If a navigator or application organization does not comply with the requirements of this rule, the commissioner may initiate an enforcement action against the navigator or application organization under 760 IAC 4-7.
IN Department of Financial Institutions ("DFI")	State		Enforces FFIEC standards.			

Survey of Federal Cyber Laws

Date	Title	Subtitle	Reference	Information
1914	Executive Order 13571		15 U.S.C. § 45, et seq.	Gave the FTC the authority to enforce rules prohibiting “unfair or deceptive acts or practices in or affecting commerce."
		FTC Section 5 Authority	15 U.S.C. § 45(a)(1), et seq.	The basic consumer protection statute enforced by the Commission is Section 5(a) of the FTC Act, which provides that "unfair or deceptive acts or practices in or affecting commerce...are...declared unlawful."
1966	Freedom of Information Act (FOIA) of 1966		5 U.S.C. § 552, et seq.	Under FOIA, “any person” may request “records” maintained by an executive agency. People or entities requesting records need not state a reason for requesting records. Today, all fifty states have freedom of information laws, many of which are based upon the FOIA.
1968	Wiretap Act of 1968		8 U.S.C. § 2511, et seq.	Broadly prohibits the intentional interception, use, or disclosure of wire and electronic communications unless a statutory exception applies. In general, these prohibitions bar unauthorized third parties (including the government) from wiretapping telephones and installing electronic "sniffers" that read Internet traffic.
1968	Omnibus Crime and Control and Safe Streets Act of 1968		18 U.S.C. §§ 2510–22, et seq.	Extended the reach of wiretap regulations to state officials as well as to private parties. Despite its profound increase in the extent of protection, Title III had important limitations. It applied to the interception of “aural” communications; it did not apply to visual surveillance or other forms of electronic communication.
1970	Fair Credit Reporting Act of 1970		15 U.S.C. § 1681, et seq.	The Fair Credit Reporting Act (FCRA) provides limited protections for individuals. It enables people to access their records, and restricts the manner in which records are disclosed. Individuals can challenge inaccuracies on their reports and can sue to collect damages for violations of the Act. However, FCRA immunizes creditors and credit reporting agencies from lawsuits for “defamation, invasion of privacy, or negligence” except when the information is “furnished with malice or willful intent to injure such consumer.” Although the FCRA allows people to sue for negligent violations of the Act, there is a two-year statute of limitations “from the date on which the liability arises."
1970	Racketeer Influenced and Corrupt Organization (RICO) Act of 1970		118 U.S.C. ch. 96	Passed in 1970, the Racketeer Influenced and Corrupt Organizations Act (RICO) is a federal law designed to combat organized crime in the United States. It allows prosecution and civil penalties for racketeering activity performed as part of an ongoing criminal enterprise. Such activity may include illegal gambling, bribery, kidnapping, murder, money laundering, counterfeiting, embezzlement, drug trafficking, slavery, and a host of other unsavory business practices.

1970	Bank Secrecy Act of 1970		Pub. L. No. 91-508 12 U.S.C. §§ 1730(d), 1829b, 1951-59, et seq. 31 U.S.C. H9 1051-1122, et seq.	The Bank Secrecy Act, enacted in 1970, requires banks to retain records and create reports to help law enforcement investigations. The Act was passed due to concerns that the computerization of records would make white collar crime more difficult to detect. Federally insured banks must record the identities of account holders and maintain copies of each financial instrument. International transactions exceeding $5,000 are subject to reporting, as well as domestic transactions exceeding $10,000. In *California Bankers Ass'n v. Shultz* , 416 U.S. 21 (1974), the Supreme Court upheld the Act against a Fourth Amendment challenge by a group of bankers and account holders. The Court concluded that the bankers lacked Fourth Amendment rights in the data because "corporations can claim no equality with individuals in the enjoyment of a right to privacy." *Id* at 65. The account holders failed to allege that they engaged in transactions exceeding $10,000, and as a result, lacked standing.
1974	Privacy Act of 1974		5 U.S.C. § 552a, et seq.	The Act responded to many of the concerns raised by the United States Department of Health Education and Welfare (HEW) report, "Records, Computers, and the Rights of Citizens." It regulates the collection and use of records by federal agencies, and affords individuals right to access and correct their personal information.
1974	Family Educational Rights and Privacy Act of 1974		20 U.S.C. § 1232g, et seq.	The Family Educational Rights and Privacy Act of 1974 (FERPA), otherwise known as the "Buckley Amendment," regulates the accessibility of student records. FERPA does not apply to records maintained by school law enforcement officials or health and psychological records.
1978	Protection of Pupil Rights Amendment ("PPRA") of 1978		20 U.S.C. § 1232h, et seq.; 34 C.F.R. part 98, et seq.	PPRA is a federal law that affords certain rights to parents of minor students with regard to surveys that ask questions of a personal nature. Briefly, the law requires that schools obtain written consent from parents before minor students are required to participate in any U.S. Department of Education funded survey, analysis, or evaluation that reveals information certain topics.
1978	Foreign Intelligence Surveillance Act of 1978		50 U.S.C. §§ 1801–11, et seq.	The Foreign Intelligence Surveillance Act (FISA) of 1978, created a distinct regime for electronic surveillance to gather foreign intelligence. Whereas Title III regulated electronic surveillance for domestic law enforcement purposes, FISA applied when foreign intelligence gathering was "the purpose" of the investigation. FISA permits electronic surveillance and covert searches pursuant to court orders, which are reviewed ex parte by a special court of seven federal judges.
1978	Right to Financial Privacy Act of 1978		29 U.S.C. § 3407, et seq.	The Right to Financial Privacy Act (RFPA) provided limited protection of financial records to fill the gap left by *United States v. Miller* , 425 U.S. 435, 435 (1976). Pursuant to the RFPA, government officials must use a warrant or subpoena to obtain financial information. There must be "reason to believe that the records sought are relevant to a legitimate law enforcement inquiry." Subject to certain exceptions, the customer must receive prior notice of the subpoena.
1978	Airline Deregulation Act - Preemption of authority over prices, routes, and service		49 U.S.C.A. § 41713, et seq.	"[A] State, political subdivision of a State, or political authority of at least 2 States may not enact or enforce a law, regulation, or other provision having the force and effect of law related to a price, route, or service of an air carrier that may provide air transportation under this subpart."

1979	Drug Abuse Prevention, Treatment, and Rehabilitation Act of 1979		42 C.F.R. part 2, et seq.	Drug Abuse Prevention, Treatment, and Rehabilitation Act (Act) is a federal statute designed to be a practical resource for governments, policy planners, service commissioners and treatment providers against drug abuse. The Act makes provision for federal drug abuse programs and activities. The Act also provides for education, treatment, rehabilitation, research, training, and law enforcement efforts to prevent drug abuse.
1980	Privacy Protection Act of 1980		42 U.S.C. § 2000aa, et seq.	Dissatisfaction over *Zurcher v. Stanford Daily* , 436 U.S. 547 (1978) led Congress to pass the Privacy Protection Act in 1980. The Act restricts the search or seizure of "any work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication." As a result of the Act, a subpoena is needed to obtain work product materials, which permits the party to challenge the request in court and to produce the documents without having law enforcement officials intrude on the premises.
1984	Cable Communications Policy Act of 1984		42 U.S.C. § 551, et seq.	The Cable Communications Policy Act (CCPA) of 1984 protects the privacy of cable records. Cable companies must notify subscribers about the collection and use of personal information. Companies cannot disclose a subscriber 's viewing habits. The Act is enforced with a private right of action.
1986	Computer Fraud and Abuse Act of 1986		18 U.S.C. § 1030, et seq.	A United States cybersecurity bill that was enacted in 1986 as an amendment to existing computer fraud law (18 U.S.C. § 1030), which had been included in the Comprehensive Crime Control Act of 1984. The law prohibits accessing a computer without authorization, or in excess of authorization. The original 1984 bill was enacted in response to concern that computer-related crimes might go unpunished. The House Committee Report to the original computer crime bill characterized the 1983 techno-thriller film WarGames—in which a young Matthew Broderick breaks into a U.S. military supercomputer programmed to predict possible outcomes of nuclear war and unwittingly almost starts World War III—as "a realistic representation of the automatic dialing and access capabilities of the personal computer."
1988	Computer Matching and Privacy Protection Act of 1988		5 U.S.C. § 552a(a)(8)–(13), (e)(12), (o)–(r), (u)), et seq.	A major loophole in the Privacy Act of 1974 has been the "routine use" exception. Under this exception, to detect fraud, the federal government in 1977 began running computer comparisons of employee records with the records of people receiving benefits. In 1988, Congress addressed this practice, known as "computer matching" by passing the Computer Matching and Privacy Protection Act. The law established procedures for computer matchings, but did not halt the practice.
1988	Employee Polygraph Protection Act of 1988		29 U.S.C. §§ 2001-09, et seq.	In 1988, Congress passed the Employee Polygraph Protection Act (EPPA). The EPPA prohibits private sector employers from using polygraph examinations on employees and prospective employees. The Act does not apply to public sector employers. Employers can, however, use polygraphs "in connection with an ongoing investigation involving economic loss or injury to the employer's business, such as theft, embezzlement, misappropriation, or an act of unlawful industrial espionage or sabotage" when "the employer has a reasonable suspicion that the employee was involved in the incident or activity under investigation." Private sector employers who provide security services are exempt.

1988	Video Privacy Protection Act of 1988		18 U.S.C. § 2710(b), et seq.	The confirmation hearings of Supreme Court Justice nominee Robert Bork sparked a law to protect videocassette rental data. Reporters attempted to obtain a list of the videos Bork had rented from his video store. Incensed at this practice, Congress passed the Video Privacy Protection Act (VPPA) of 1988.251 The VPPA forbids videotape service providers from disclosing customer video rental or purchase information.
1986	Electronic Communications Privacy Act of 1986		18 U.S.C. §§ 2510-22, 2701-11, 3121-27, et seq.	In 1986, Congress revisited its wiretapping law by substantially reworking Title III of 1968. The Electronic Communications Privacy Act (ECPA) expanded Title III to new forms of communications, with a particular focus on computers. The ECPA restricts the interception of transmitted communications and the searching of stored communications. Title I of the ECPA, known as the "Wiretap Act," regulates the interception of communications. Title II, referred to as the "Stored Communications Act," governs access to stored communications and records held by communications service providers (such as ISPs). Title III, called the "Pen Register Act," provides limited regulation of pen registers and trap and trace devices.
1991	Telephone Consumer Protection Act of 1991		47 U.S.C. § 227, et seq.	In 1991, Congress enacted the Telephone Consumer Protection Act (TCPA), which permits people to request that telemarketers not call them again. If the telemarketer continues to call, people can sue for damages of up to $500 for each call.
1993	Government Performance and Results Act of 1993		Pub. L. No. 103-62	Requires executive agency heads to submit to the Director of the Office of Management and Budget (OMB) and the Congress a strategic plan for performance goals of their agency's program activities. Requires such plan to cover at least a five-year period and to be updated at least every three years. See: https://www.congress.gov/bill/103rd-congress/senate-bill/20
1994	Driver's Privacy Protection Act of 1994		18 U.S.C. §§ 2721-25, et seq.	In 1994, Congress passed the Driver 's Privacy Protection Act (DPPA), which requires that states first obtain a person's consent before disclosing her motor vehicle record information to marketers.
1995	Paperwork Reduction Act (PRA) of 2005		44 U.S.C. § 3501, et seq.	Designed to reduce the public's burden of answering unnecessary, duplicative, and burdensome government surveys.
1996	Health Insurance Portability and Accountability Act (HIPAA) of 1996		Pub. L. No. 104-191, 110 Stat. 1936	The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is the first federal statute to directly address health privacy. HIPPA required the Department of Health and Human Services (HHS) to draft regulations to protect the privacy of medical records. HHS's regulations, among other things, require that people authorize all uses and disclosures of their health information that are not for treatment, payment, or health care operation (such as for marketing purposes).

		HIPAA Privacy Rule	45 C.F.R. part 160, et seq. and 45 C.F.R. part 164, subparts A and E, et seq.	The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.
		HIPAA Security Rule	45 C.F.R. part 160 and 45 C.F.R. part 164, subparts A and C, et seq.	The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.
		HIPAA Breach Notification Rule	45 CFR part 164, subpart D, et seq.	Requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.
		Uses and disclosures for which an authorization or opportunity to agree or object is not required.	45 C.F.R. § 164.512, et seq.	Provides when covered entities or business associates are nor required to obtain valid authorization to use or disclose protected health information. General exceptions exist for public health activities.
		Uses and disclosures to carry out treatment, payment, or health care operations.	45 C.F.R. § 164.506, et seq.	Provides when covered entities or business associates are nor required to obtain valid authorization to use or disclose protected health information. General exceptions exist for collection of payments for medical services.
		Imposition of Civil Money Penalties	45 CFR, part 160, subpart D, et seq.	Provides guidelines for determining what amount an entity should be penalized for violating HIPAA.
1996	Economic Espionage Act of 1996		8 U.S.C. §§ 1831-39, et seq.	This regulation is intended to protect from disclosure outside the government proprietary information that is provided to the government during a bidding process. Exemption 4 of the Freedom of Information Act exempts from mandatory disclosure information such as trade secrets and commercial or financial information obtained by the government from a company on a privileged or confidential basis that, if released, would result in competitive harm to the company, impair the government's ability to obtain like information in the future, or protect the government's interest in compliance with program effectiveness. The law on Disclosure of Confidential Information (18 U.S.C. § 1905) makes it a crime for a federal employee to disclose such information.

1997	No Electronic Theft Act of 1997		Pub. L. No. 105-147	Provides for criminal prosecution of individuals who engage in copyright infringement under certain circumstances, even when there is no monetary profit or commercial benefit from the infringement.
1998	Children's Online Privacy Protection Act of 1998		15 U.S.C. §§ 6501-06, et seq.	The Children's Online Privacy Protection Act (COPPA) of 1998 governs the collection of children's personal information on the Internet. The law only applies to children under the age of thirteen. Children's websites must post privacy policies and obtain "parental consent for the collection, use, or disclosure of personal information from "children." COPPA applies only to websites "directed to children" or where the operator of the website "has actual knowledge that it is collecting personal information from a child."
1998	Digital Millennium Copyright Act (DMCA) of 1998		Pub. L. No. 105-304; 17 U.S.C. §§ 101, 104, 104A, 108, 112, 114, 117, 701, et seq.; 17 U.S.C. §§ 512, 1201–1205, 1301–1332, et seq.; 28 U.S.C. § 4001, et seq.	A U.S. copyright law that implements two 1996 treaties of the World Intellectual Property Organization (WIPO). It criminalizes production and dissemination of technology, devices, or services intended to circumvent measures that control access to copyrighted works (commonly known as digital rights management or DRM). It also criminalizes the act of circumventing an access control, whether or not there is actual infringement of copyright itself. In addition, the DMCA heightens the penalties for copyright infringement on the Internet.
1999	U.S. Uniform Computer Information Transactions Act (UCITA) of 1999 (Last Amended or Revised in 2002)		Uniform Laws Annotated. Uniform Computer Information Transactions Act (Last Amended or Revised in 2002)	UCITA provides a comprehensive set of rules for licensing computer information, whether computer software or other clearly identified forms of computer information. Computerized databases and computerized music are other examples of computer information that would be subject to UCITA. It would also govern access contracts to sites containing computer information, whether on or off the Internet. UCITA would also apply to storage devices, such as disks and CDs that exist only to hold computer information. Professional services by a member of a regulated profession (doctor, lawyer, accountant, for example) are not within UCITA even though communications about the transaction will be in the form of computer information.
1999	The Gramm-Leach-Bliley Act of 1999		15 U.S.C. § 6802(a)-(b), et seq.	In 1999, Congress passed the Gramm-Leach-Bliley (GLB) Act, which allows financial institutions with different branches or affiliates engaging in different services to share the "nonpublic personal information" among each branch of the company. Affiliates must inform customers of the information sharing, but people have no right to stop the companies from sharing it. However, when financial institutions desire to share customer data with third parties, people have a right to opt-out.

2000	Security and Exchange Commission ("SEC") Privacy of Consumer Financial Information Regulations of 2000		17 C.F.R. part 248, subpart A, et seq.	The SEC adopted Regulation S-P, privacy rules promulgated under section 504 of the Gramm-Leach-Bliley Act. Section 504 of GLBA required the Commission to adopt rules implementing notice requirements and restrictions on a financial institution's ability to disclose nonpublic personal information about consumers. The Regulation implements these requirements of the GLBA with respect to investment advisers registered with the Commission, brokers, dealers, and investment companies, which are the financial institutions subject to the Commission's jurisdiction under that Act.
2000	U.S. Congress Electronic Signatures in Global National ("ESIGN") Commerce Act of 2000		Pub. L. No. 106–229	The ESIGN Act is a landmark federal law in the United States. Passed in 2000, it granted legal recognition to electronic signatures and records in the USA based on the understanding that if all parties to a contract choose to use electronic documents and to sign them electronically, they are legal. The ESIGN Act (along with its precursor UETA) provided the legal foundation for use of electronic records and electronic signatures in commerce. It confirmed that electronic records and signatures carry the same weight and have the same legal effect as traditional paper documents and wet ink signatures.
2001	The U.S. Provide Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act of 2001		Pub. L. No. 107-56	In a very short time after the September 11 terrorist attack, Congress passed the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act" (USA PATRIOT Act) of 2001. The Act made several significant changes to the ECPA and FISA, among other statutes. In one amendment, the USA PATRIOT Act enlarged the definition of pen registers and trap and trace devices to apply to addressing information on emails and to "IP addresses." The Act also provided for new justifications for delayed notice of search warrants, increasing the types of subscriber records that could be obtained from ISPs and communications providers, and allowing for a nationwide scope for pen register orders and search warrants for email. The Act also provided for roving wiretaps under FISA as well as increased sharing of foreign intelligence information between law enforcement entities.
2002	Confidential Information Protection and Statistical Efficiency Act (CIPSEA) of 2002		44 U.S.C. § 101	CIPSEA establishes uniform confidentiality protections for information collected for statistical purposes by U.S. statistical agencies, and it allows some data sharing between the Bureau of Labor Statistics, Bureau of Economic Analysis, and Census Bureau. The agencies report to OMB on particular actions related to confidentiality and data sharing. The law give the agencies standardized approaches to protecting information from respondents so that it will not be exposed in ways that lead to inappropriate or surprising identification of the respondent. By default the respondent's data is used for statistical purposes only. If the respondent gives informed consent, the data can be put to some other use.
2002	Sarbanes-Oxley Act ("SOX") of 2002		15 U.S.C. ch. 2A, 98, et seq.	SOX protects shareholders and the general public from accounting errors and fraudulent practices of organizations. It was also tailored to improve the accuracy of corporate disclosures. SOX compliance has recently shifted to include cybersecurity.

2002	E-Government Act of 2002		44 U.S.C. § 3601, et seq.	Established procedures to ensure the privacy of personal information in electronic records. Section 208 of the E-Government Act of 2002 requires agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. PIAs must be made publicly available, unless the agency determines not to make the PIA publicly available if such publication would raise security concerns, reveal classified (i.e., national security), or reveal sensitive information (e.g., potentially damaging to a national interest, law enforcement effort, or competitive business interest).
2002	The Homeland Security Act of 2002		6 U.S.C. § 222, et seq.	In 2002, Congress passed the Homeland Security Act, which created the Department of Homeland Security (DHS), consisting of twenty-two federal agencies. The Act created a Privacy Office for ensuring compliance with privacy laws.
2002	Federal Information Security Management Act ("FISMA") of 2002		44 U.S.C. § 3551, et seq.	FISMA is United States legislation that defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats. FISMA assigns responsibilities to various agencies to ensure the security of data in the federal government. The act requires program officials, and the head of each agency, to conduct annual reviews of information security programs, with the intent of keeping risks at or below specified acceptable levels in a cost-effective, timely and efficient manner.
2003	Do-Not-Call Implementation Act (National Do-Not-Call Registery) of 2003		15 U.S.C. ch. 87-87A, et seq.	In an effort to address unwanted telemarketing calls, the Federal Trade Commission (FTC) and the Federal Communications Commission (FCC) created a do-not-call registry. People can voluntarily register their telephone numbers, and commercial telemarketers are prohibited from calling the numbers. Telemarketers challenged the do-not-call registry as a violation of their First Amendment rights. In 2004, a federal circuit court concluded in *Mainstream Marketing Services, Inc. v. Federal Trade Commission* , 358 F.3d 1228 (10th Cir. 2004) that the do-not-call registry satisfied the *Central Hudson Gas & Elec. Corp. v. Public Service Commission of New York* , 447 U.S. 557 (1980) balancing test for commercial speech and therefore did not run afoul of the First Amendment.
2003	The CAN-SPAM Act of 2003		15 U.S.C. § 7701, et seq.	The Act establishes requirements for those who send unsolicited commercial email. The Act bans false or misleading header information and prohibits deceptive subject lines. It also requires that unsolicited commercial email be identified as advertising and provide recipients with a method for opting out of receiving any such email in the future. In addition, the Act directs the FTC to issue rules requiring the labeling of sexually explicit commercial email as such and establishing the criteria for determining the primary purpose of a commercial email.
2003	The Fair and Accurate Credit Transactions Act of 2003		Pub. L. No. 108-159	In 2003, Congress passed the Fair and Accurate Credit Transactions Act (FACTA), which amended the Fair Credit Reporting Act and extended its preemption on certain state law provisions addressing identity theft and credit reporting. Among other things, the FACTA provided some limited protections against identity theft. For example, FACTA requires credit reporting agencies to provide people with a free credit report each year. It requires credit reporting agencies to disclose to a consumer her credit score, and it allows victims of fraud to alert just one credit reporting agency, which then must notify the others. These provisions and others were criticized by many as not going far enough to address the problem of identity theft.

2004	The Intelligence Reform and Terrorism Prevention Act of 2004		Pub. L. No. 108-458	In 2004, Congress passed the Intelligence Reform and Terrorism Prevention Act to facilitate greater information sharing between federal agencies. The Act requires that intelligence be “provided in its most shareable form” and it aims to “promote a culture of information sharing.
2005	The Real ID Act of 2005		Pub. L. No. 109-13	Attached to a military spending bill, and passed without debate, the Real ID Act of 2005 mandated that state driver ’s licenses meet federal standards set forth by the DHS. Critics claimed that it would establish a de facto national identification card and that it would be extremely costly for the states to implement.
2006	U.S. SAFE WEB Act of 2006		15 U.S.C. §§ 45-58, et seq.	This Act, amending the FTC Act of 1914, provides the FTC with a number of tools to improve enforcement regarding consumer protection matters, particularly those with an international dimension, including increased cooperation with foreign law enforcement authorities through confidential information sharing and provision of investigative assistance. The Act also allows enhanced staff exchanges and other international cooperative efforts.
2007	Open Government Act of 2007		Public Law No. 110-175; 5 U.S.C. § 552, et seq.	Promotes accessibility, accountability, and openness in Government by strengthening 5 U.S.C. § 552 and codifies several provisions of Executive Order 13,392, "Improving Agency Disclosure of Information."
2007	The Freedom of Information Act (FOIA) of 2007		5 U.S.C. § 552, et seq.	Amended Freedom of Information Act (FOIA) of 1966. Provides that any person has a right, enforceable in court, to obtain access to federal agency records, except to the extent that such records (or portions of them) are protected from public disclosure by one of nine exemptions or by one of three special law enforcement record exclusions.
2008	Genetic Information Nondiscrimination Act ("GINA") of 2008		15 U.S.C. §§ 2000ff - 2000ff(11), et seq.	GINA protects individuals against discrimination based on their genetic information in health coverage and in employment. GINA is divided into two sections, or Titles. Title I of GINA prohibits discrimination based on genetic information in health coverage. Title II of GINA prohibits discrimination based on genetic information in employment.
2009	Health Information Technology for Economic and Clinical Health Act ("HITECH Act")		42 C.F.R. parts 412, 413, 422, and 495, et seq.	Promotes the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules.
		Access to systems and records.	42 C.F.R. § 495.346, et seq.	"The State agency must allow HHS access to all records and systems operated by the State in support of this program, including cost records associated with approved administrative funding and incentive payments to Medicaid providers. State records related to contractors employed for the purpose of assisting with implementation or oversight activities or providing assistance, at such intervals as are deemed necessary by the Department to determine whether the conditions for approval are being met and to determine the efficiency, economy, and effectiveness of the program."

		Combating fraud and abuse.	42 C.F.R. § 495.368, et seq.	"(a) General rule. (1) The State must comply with Federal requirements to— (i) Ensure the qualifications of the providers who request Medicaid EHR incentive payments; (ii) Detect improper payments; and (iii) In accordance with § 455.15 and § 455.21 of this chapter, refer suspected cases of fraud and abuse to the Medicaid Fraud Control Unit. (2) The State must take corrective action in the case of improper EHR payment incentives to Medicaid providers."
2010	Government Performance and Results Modernization (GPRM) Act of 2010 (Amends the Government Performance and Results Act of 1993)		Pub. L. No. 111-352 (Amends the Government Performance and Results Act of 1993)	Amends the Government Performance and Results Act of 1993 to require each executive agency to make its strategic plan available on its public website on the first Monday in February of any year following that in which the term of the President commences and to notify the President and Congress. Requires such plan to cover at least a four-year period and to include a description of how the agency is working with other agencies to achieve its goals and objectives, as well as relevant federal government priority goals. Requires the Director of the Office of Management and Budget (OMB) to coordinate with agencies to develop a federal government performance plan, which shall be submitted with the annual federal budget and concurrently made available on an OMB website of agency programs. Requires such plan to: (1) establish government performance goals for the current and next fiscal years; (2) identify activities, entities, and policies contributing to each goal; (3) identify a lead government official responsible for coordinating efforts to achieve the goal; (4) establish common federal government performance indicators with quarterly targets; (5) establish clearly defined quarterly milestones; and (6) identify major management
2014	Federal Information Security Modernization Act of 2014		44 U.S.C. § 3541, et seq.	This Act amends the Federal Information Security Management Act of 2002, 44 U.S.C. § 3541, and requires agencies to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of an agency.
2017	Social Security Number Fraud Prevention Act of 2017		Pub. L. No. 115-59	This Act: (1) prohibits federal agencies from including any individual's Social Security account number on any document sent by mail unless the agency head determines that such inclusion is necessary; and (2) requires agencies that have Chief Financial Officers to issue regulations, within five years of this bill's enactment, that specify the circumstances under which such inclusion is necessary.
2017	The Protecting Patient Access to Emergency Medications Act of 2017		21 U.S.C. § 823, et seq.	In 1970, the Controlled Substances Act (CSA) was created to regulate substances that have the potential to be abused. At the time, the CSA lacked instructions for the maintenance and use of these substances by emergency medical services (EMS). States, therefore, created their own EMS-related controlled substances requirements. In 2017, the Protecting Patient Access to Emergency Medications Act (PPAEMA) was introduced in the United States Congress to amend the CSA to include EMS requirements and end confusion among states and EMS agencies. The PPAEMA was signed into law on November 17, 2017.

2018	Defense Federal Acquisition Regulation Supplement ("DFARS")		48 C.F.R. § 201.104, et seq.	DFARS Safeguarding riles and clauses, for the basic safeguarding of contractor information systems that process, store or transmit Federal contract information. DFARS provides a set of “basic” security controls for contractor information systems upon which this information resides. These security controls must be implemented at both the contractor and subcontractor levels based on the information security guidance in NIST Special Publication 800-171 “Protecting Controlled Unclassified Information in Non-Federal Information Systems and Organizations.”

FEDERAL AGENCY POLICIES

Date	Title	Subtitle	Reference	Information
1973	Organization of Economic Cooperation and Development (OECD) Fair Information Practices		U.S. Department of Health, Education, and Welfare, Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Comm. On Automated Personal Data Systems 29 (1973)	The OCED Fair Information Practices were articulated by the United States Department of Health Education and Welfare (HEW) in 1973. HEW investigated the issues with increasing computerization of information and growing depositories of personal data. The report recommended the page of a code of Fair Information Practices, which were later codified in the Privacy Act of 1974. The recommended practices included the following: 1. There must be no personal data record-keeping systems whose very existence is secret. 2. There must be a way for an individual to find out what information about him is in a record and how it is used. 3. There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent. 4. There must be a way for an individual to correct or amend a record of identifiable information about him. 5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.

1980	Organization of Economic Cooperation and Development (OECD) Privacy Guidelines		Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available in Marc Rotenburg, Privacy Law Sourcebook (2002)	The OECD Privacy Guidelines built upon the Fair Information Practices articulated by the United States Department of Health Education and Welfare (HEW). The OECD Guidelines contain eight principles: (1) collection limitation—data should be collected lawfully with the individual's consent; (2) data quality—data should be relevant to a particular purpose and be accurate; (3) purpose specification—the purpose for data collection should be stated at the time of the data collection and the use of the data should be limited to this purpose; (4) use limitation—data should not be disclosed for different purposes without the consent of the individual; (5) security safeguards—data should be protected by reasonable safeguards; (6) openness principle—individuals should be informed about the practices and polices of those handling their personal information; (7) individual participation—people should be able to learn about the data that an entity possesses about them and to rectify errors or problems in that data; (8) accountability—the entities that control personal information should be held accountable for carrying out these principles.

Survey of Other States Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement
Alabama Breach Notification Law	Ala. Code § 8-38-5	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 1000 people • Notify Credit Reporting Agencies: Yes, if over 1000 people • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: over 10,000 residents or $500,000 • Credit Monitoring: No	$500,000 and $5,000 per day: Ala. Code § 8-38-9	Attorney General: Ala. Code § 8-38-9
Alabama Personal Information Protection Act	Ala. Code § 8-38-3	"Each covered entity and third-party agent shall implement and maintain reasonable security measures to protect sensitive personally identifying information against a breach of security."	Most likely, this would be considered a deceptive practice under Ala. Code § 8-19-5.	None
Alabama Unfair, Deceptive, or Abusive Acts and Practices	Ala. Code § 8-19-5	"The following deceptive acts or practices in the conduct of any trade or commerce are hereby declared to be unlawful: . . . (27) Engaging in any other unconscionable, false, misleading, or deceptive act or practice in the conduct of trade or commerce."	Up to $2,000 per violation: Ala. Code § 8-19-11	Attorney General: Ala. Code § 8-19-4
Alaska Breach Notification Law	Alaska Stat. § 45.48.010	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if not disclosing to residents • Notify Credit Reporting Agencies: Yes, if over 1000 people • If not data owner, notify data owner: Unclear • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: over 300,000 residents or $150,000 • Credit Monitoring: No	Up to $50,000: Alaska Stat. § 45.48.080(b)(1)	Attorney General: Alaska Stat. § 44.23.020(b)(4)
Alaska Personal Information Protection Act	Alaska Stat. § 45.48.430	"A person doing business, including the business of government, may not disclose an individual's social security number to a third party."	Up to $3,000: Alaska Stat. § 45.48.480	Attorney General: Alaska Stat. § 44.23.020(b)(4)
Alaska Unfair, Deceptive, or Abusive Acts and Practices	Alaska Stat. § 45.50.471	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of trade or commerce are declared to be unlawful."	Between $1,000 and $25,000 per violation: Alaska Stat. § 45.50.537	Attorney General: Alaska Stat. § 45.50.501
Arizona Breach Notification Law	Ariz. Rev. Stat. § 18-545	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 people • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: over 100,000 people or $50,000 • Credit Monitoring: No	$10,000 per breach: Ariz. Rev. Stat. § 18-545(H)	Attorney General: Ariz. Rev. Stat. § 18-545(H)
Arizona Unfair, Deceptive, or Abusive Acts and Practices	Rev. Stat. § 44-1522	"The act, use or employment by any person of any deception, deceptive or unfair act or practice, fraud, false pretense, false promise, misrepresentation, or concealment, suppression or omission of any material fact with intent that others rely on such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise whether or not any person has in fact been misled, deceived or damaged thereby, is declared to be an unlawful practice."	Up to $10,000 per violation: Ariz. Rev. Stat. § 44-1531	Attorney General: Ariz. Rev. Stat. § 44-1524
Arkansas Breach Notification Law	Ark. Code § 4-110-105	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: 500,000 residents or $250,000 • Credit Monitoring: No •	Up to $10,000 per violation: Ark. Code §§ 4-110-108; 4-88-113	Attorney General: Ark. Code Ark. Code §§ 4-110-108;§ 4-88-104

Arkansas Personal Information Protection Act	Ark. Code § 4-110-104(b)	"A person or business that acquires, owns, or licenses personal information about an Arkansas resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure"	Up to $10,000 per violation: Ark. Code §§ 4-110-108; 4-88-113	Attorney General: Ark. Code Ark. Code §§ 4-110-108;§ 4-88-104
Arkansas Unfair, Deceptive, or Abusive Acts and Practices	Ark. Code § 4-88-108	"When utilized in connection with the sale or advertisement of any goods, services, or charitable solicitation, the following shall be unlawful: (1) The act, use, or employment by any person of any deception, fraud, or false pretense; or (2) The concealment, suppression, or omission of any material fact with intent that others rely upon the concealment, suppression, or omission."	Up to $10,000 per violation: Ark. Code § 4-88-113	Attorney General: Ark. Code § 4-88-104
California Breach Notification Law	Cal. Civ. Code § 1798.82	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: Yes, if over 1000 people • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: • Credit Monitoring: • Other:	Up to $3,000 per transaction: Cal. Civ. Code § 1798.84	Private right of action: Cal. Civ. Code § 1798.84
California Personal Information Protection Act	Cal. Civ. Code § 1798.81.5	"A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."	Up to $3,000 per transaction: Cal. Civ. Code § 1798.84	Private right of action: Cal. Civ. Code § 1798.84
California Unfair, Deceptive, or Abusive Acts and Practices	Cal. Bus. & Prof. Code § 17200	"As used in this chapter, unfair competition shall mean and include any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising and any act prohibited by Chapter 1 (commencing with Section 17500) of Part 3 of Division 7 of the Business and Professions Code."	$2,500 per violation: Cal. Bus. & Prof. Code § 17206	Attorney General: Cal. Bus. & Prof. Code § 17206
Colorado Breach Notification Law	Colo. Rev. Stat. § 6-1-716	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 people • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: 250,000 residents or $250,000 • Credit Monitoring: No	"The attorney general may bring an action in law or equity to address violations of this section and for other relief that may be appropriate to ensure compliance with this section or to recover direct economic damages resulting from a violation, or both. The provisions of this section are not exclusive and do not relieve an individual or a commercial entity subject to this section from compliance with all other applicable provisions of law." Colo. Rev. Stat. § 6-1-716(4)	Attorney General: Colo. Rev. Stat. § 6-1-716(4)
Colorado Unfair, Deceptive, or Abusive Acts and Practices	Colo. Rev. Stat. § 6-1-105	"A person engages in a deceptive trade practice when, in the course of the person's business, vocation, or occupation, the person:"	Up to $2,000 per violation: Colo. Rev. Stat. § 6-1-112	Attorney General: Colo. Rev. Stat. § 6-1-103.
Connecticut Breach Notification Law	Conn. Gen. Stat. § 36a-701b	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: 500,000 residents or $250,000 • Credit Monitoring: Yes, 12 months • Other:	Up to $5,000 per violation: Conn. Gen. Stat. §§ 36a-701b(g), 42-110o	Attorney General: Conn. Gen. Stat. §§ 36a-701b(g), 42-110o

Connecticut Personal Information Protection Act	Conn. Gen. Stat. § 42-471	"Any person who collects Social Security numbers in the course of business shall create a privacy protection policy which shall be published or publicly displayed. For purposes of this subsection, "publicly displayed" includes, but is not limited to, posting on an Internet web page. Such policy shall: (1) Protect the confidentiality of Social Security numbers, (2) prohibit unlawful disclosure of Social Security numbers, and (3) limit access to Social Security numbers."	Up to $5,000 per violation: Conn. Gen. Stat. §§ 42-471(h), 36a-701b(g), 42-110o,	Attorney General: Conn. Gen. Stat. §§ 42-471(h), 36a-701b(g), 42-110o,
Connecticut Unfair, Deceptive, or Abusive Acts and Practices	Conn. Gen. Stat. § 42-110b	"No person shall engage in unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce."	Up to $5,000 per violation: Conn. Gen. Stat. § 42-110o	Attorney General: Conn. Gen. Stat. § 42-110o
Delaware Breach Notification Law	Del. Code tit. 6, § 12B-102	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 500 residents • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay, but no more than 60 days • Substitute Notice: Yes, if over 100,000 residents or $75,000 • Credit Monitoring: Yes, if SSN breached, 12 months • Other:	"an action in law or equity to address the violations of this chapter and for other relief that may be appropriate to ensure proper compliance with this chapter or to recover direct economic damages resulting from a violation, or both." 6 Del. C. § 12B-104	Director of Consumer Protection of the Department of Justice: 6 Del. C. § 12B-104
Delaware Personal Information Protection Act	Del. Code tit. 6, § 12B-100	"Any person who conducts business in this State and owns, licenses, or maintains personal information shall implement and maintain reasonable procedures and practices to prevent the unauthorized acquisition, use, modification, disclosure, or destruction of personal information collected or maintained in the regular course of business."	"an action in law or equity to address the violations of this chapter and for other relief that may be appropriate to ensure proper compliance with this chapter or to recover direct economic damages resulting from a violation, or both." 6 Del. C. § 12B-104	Director of Consumer Protection of the Department of Justice: 6 Del. C. § 12B-104
Delaware Unfair, Deceptive, or Abusive Acts and Practices	Del. Code tit. 6, § 2532	"A person engages in a deceptive trade practice when, in the course of a business, vocation, or occupation, that person:. . ."	Up to $10,000 per willful violation: Del. Code tit. 6, § 2533	Attorney General: Del. Code tit. 6, § 2533
Florida Breach Notification Law	Fla. Stat. § 501.171(4)(a)	• Notify Affected Residents: Yes • Notify Department of Legal Affairs: Yes, if over 500 • Notify Credit Reporting Agencies: Yes, if over 1000 people • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: over 500,000 residents or $250,000 • Credit Monitoring: • Other:	Up to $500,000 and more penalties: Fla. Stat. § 501.171(9)	Department of Legal Affairs: Fla. Stat. § 501.171(9)
Personal Information Protection Act	Fla. Stat. § 501.171(2)	"Each covered entity, governmental entity, or third-party agent shall take reasonable measures to protect and secure data in electronic form containing personal information."	Up to $500,000 and more penalties: Fla. Stat. § 501.171(9)	Department of Legal Affairs: Fla. Stat. § 501.171(9)
Unfair, Deceptive, or Abusive Acts and Practices	Fla. Stat. § 501.204	"Unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful"	Up to $10,000 per violation: Fla. Stat. § 501.2075	Department of Legal Affairs: Fla. Stat. § 501.2075
Georgia Breach Notification Law	Ga. Code § 10-1-912	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 10,000 residents • If not data owner, notify data owner: Yes, within 24 hours • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: over 100,000 residents or $50,000 • Credit Monitoring: No	None	None
Unfair, Deceptive, or Abusive Acts and Practices	Ga. Code § 10-1-393	"Unfair or deceptive acts or practices in the conduct of consumer transactions and consumer acts or practices in trade or commerce are declared unlawful."	Up to $5,000 per violation: Ga. Code § 10-1-397(a)(2)(B)	Attorney General: Ga. Code § 10-1-397

Hawaii Breach Notification Law	Haw. Rev. Stat. § 487N-2	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 1000 residents • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 200,000 residents or $100,000 • Credit Monitoring: No	Up to $2,500 per violation: Haw. Rev. Stat. § 487N-3	Attorney General: Haw. Rev. Stat. § 487N-3
Unfair, Deceptive, or Abusive Acts and Practices	Haw. Rev. Stat. § 480-2	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are unlawful."	Up to $10,000 per violation: Haw. Rev. Stat. § 480-3.1	Attorney General or Director of the Office of Consumer Protections: :Haw. Rev. Stat. § 480-3.1
Idaho Breach Notification Law	Idaho Code § 28-51-105	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 50,000 residents or $25,000 • Credit Monitoring: No	Up to $25,000 per breach: Idaho Code § 28-51-107	Attorney General: Idaho Code § 28-51-107
Unfair, Deceptive, or Abusive Acts and Practices	Idaho Code § 48-603	"The following unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared to be unlawful, where a person knows, or in the exercise of due care should know, that he has in the past, or is:"	Up to $10,000 per violation: Idaho Code § 48-606(1)(e)	Attorney General: Idaho Code § 48-606
Illinois Breach Notification Law	815 Ill. Comp. Stat. § 530/10	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,000 residents or $250,000 • Credit Monitoring: No	Up to $50,000: 815 ILCS §§ 530/20; 505/7	Attorney General: 815 ILCS §§ 530/20; 505/7
Personal Information Protection Act	815 Ill. Comp. Stat. § 530/45	"A data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure."	Up to $50,000: 815 ILCS §§ 530/20; 505/7	Attorney General: 815 ILCS §§ 530/20; 505/7
Unfair, Deceptive, or Abusive Acts and Practices	815 Ill. Comp. Stat. § 505/2	"Unfair methods of competition and unfair or deceptive acts or practices, including but not limited to the use or employment of any deception, fraud, false pretense, false promise, misrepresentation or the concealment, suppression or omission of any material fact, with intent that others rely upon the concealment, suppression or omission of such material fact, or the use or employment of any practice described in Section 2 of the "Uniform Deceptive Trade Practices Act", approved August 5, 1965,1 in the conduct of any trade or commerce are hereby declared unlawful whether any person has in fact been misled, deceived or damaged thereby. In construing this section consideration shall be given to the interpretations of the Federal Trade Commission and the federal courts relating to Section 5(a) of the Federal Trade Commission Act.2"	Up to $50,000: 815 Ill. Comp. Stat. § 505/7	Attorney General: 815 Ill. Comp. Stat. § 505/7
Iowa Breach Notification Law	Iowa Code § 715C.2	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 500 residents • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 350,000 residents or $250,000 • Credit Monitoring: No	Up to $40,000 per violation: Iowa Code §§ 715C.2(9), 714.16(7)	Attorney General: Iowa Code §§ 715C.2(9), 714.16(7)

Unfair, Deceptive, or Abusive Acts and Practices	Iowa Code § 714.16	"The act, use or employment by a person of an unfair practice, deception, fraud, false pretense, false promise, or misrepresentation, or the concealment, suppression, or omission of a material fact with intent that others rely upon the concealment, suppression, or omission, in connection with the lease, sale, or advertisement of any merchandise or the solicitation of contributions for charitable purposes, whether or not a person has in fact been misled, deceived, or damaged, is an unlawful practice."	Up to $40,000 per violation: Iowa Code § 714.16(7)	Attorney General: Iowa Code § 714.16(7)
Kansas Breach Notification Law	Kan. Stat. § 50-7a02	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 5,000 residents or $100,000 • Credit Monitoring: No	"an action in law or equity to address violations of this section and for other relief that may be appropriate": Kan. Stat. § 50-7a02(g)	Attorney General: Kan. Stat. § 50-7a02(g)
Personal Information Protection Act	Kan. Stat. § 50-6,139b(b)(1)	" A holder of personal information shall: (1) Implement and maintain reasonable procedures and practices appropriate to the nature of the information, and exercise reasonable care to protect the personal information from unauthorized access, use, modification or disclosure. If federal or state law or regulation governs the procedures and practices of the holder of personal information for such protection of personal information, then compliance with such federal or state law or regulation shall be deemed compliance with this paragraph and failure to comply with such federal or state law or regulation shall be prima facie evidence of a violation of this paragraph; . . ."	Up to $10,000 per violation or $20,000 per willful violation: Kan. Stat. §§ 50-6139b(d, e), 50-636	Attorney General: Kan. Stat. § 50-636
Unfair, Deceptive, or Abusive Acts and Practices	Kan. Stat. § 50-626	"No supplier shall engage in any deceptive act or practice in connection with a consumer transaction."	Up to $10,000 per violation or $20,000 per willful violation: Kan. Stat. § 50-636	Attorney General: Kan. Stat. § 50-636
Kentucky Breach Notification Law	Ky. Rev. Stat. § 365.732	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 people • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: 500,000 residents or $250,000 • Credit Monitoring: • Other:	None	Private Right of Action: Ky. Rev. Stat. § 365.730
Unfair, Deceptive, or Abusive Acts and Practices	Ky. Rev. Stat. § 367.170	"Unfair, false, misleading, or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful."	Up to $2,000 per violation: Ky. Rev. Stat. § 367.990(2)	Attorney General: Ky. Rev. Stat. § 367.990(2)
Louisiana Breach Notification Law	La. Rev. Stat. § 51:3074	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 50,000 residents or $250,000 • Credit Monitoring: No • Other:	"a fine not to exceed $5,000 per violation. Notice to the attorney general shall be timely if received within 10 days of distribution of notice to Louisiana citizens. Each day notice is not received by the attorney general shall be deemed a separate violation." 16 La. Admin. Code Pt III, 701	Attorney General: 16 La. Admin. Code Pt III, 701
Unfair, Deceptive, or Abusive Acts and Practices	La. Stat. § 51:1405	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful."	Up to $5,000 per violation: La. Rev. Stat. § 51:1407(B)	Attorney General: La. Rev. Stat. § 51:1407(A)

Maine Breach Notification Law	Me. Rev. Stat. tit. 10 § 1348	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 1,000 people or $5,000 • Credit Monitoring: No	"[M]aximum of $2,500 for each day the person is in violation:" Me. Rev. Stat. tit. 10 § 1349	Attorney General: Me. Rev. Stat. tit. 10 § 1349
Unfair, Deceptive, or Abusive Acts and Practices	Me. Rev. Stat. tit. 5 § 207	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are declared unlawful."	$5,000 penalty for non-compliance with § 211: Me. Rev. Stat. tit. 5 § 212	Attorney General: Me. Rev. Stat. tit. 5 § 212
Maryland Breach Notification Law	Md. Code, Com. Law § 14-3504	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: Yes, over 1000 • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay and several day requirements • Substitute Notice: Yes, if over 175,000 residents or $100,000 • Credit Monitoring: No • Other:	$1,000 per violation: Md. Code, Com. Law §§ 14-3508, 13-410	Division of Consumer Protection: Md. Code Comm . Law §§ 13-403 and 13-410
Personal Information Protection Act	Md. Code, Com. Law § 14-3503	"To protect personal information from unauthorized access, use, modification, or disclosure, a business that owns or licenses personal information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations."	$1,000 per violation: Md. Code, Com. Law §§ 14-3508, 13-410	Division of Consumer Protection: Md. Code Comm . Law §§ 13-403 and 13-410
Unfair, Deceptive, or Abusive Acts and Practices	Md. Code Comm . Law §13-303	"A person may not engage in any unfair or deceptive trade practice, as defined in this subtitle or as further defined by the Division, in:. . ."	$1,000 per violation: Md. Code, Com. Law § 13-410	Division of Consumer Protection: Md. Code Comm . Law §§ 13-403 and 13-410
Massachusetts Breach Notification Law	Mass. Gen. Laws Ch. 93H § 1	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: Attorney General • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,00 residents or $250,000 • Credit Monitoring: 2 years	Up to $5,000 per violation: Mass. Gen. Laws Ch. 93A § 4	Attorney General: Mass. Gen. Laws § 93H § 1
Unfair, Deceptive, or Abusive Acts and Practices	Mass. Gen. Laws Ch. 93A § 2	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful."	Up to $5,000 per violation: Mass. Gen. Laws Ch. 93A § 4	Attorney General: Mass. Gen. Laws Ch. 93A § 4
Michigan Breach Notification Law	Mich. Comp. Laws § 445.72	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,000 residents or $250,000 • Credit Monitoring: No	$250 per notice failure, or up to $750,000 per breach: Mich. Comp. Laws § 445.72(13)	Attorney General: Mich. Comp. Laws § 445.72(13)
Unfair, Deceptive, or Abusive Acts and Practices	Mich. Comp. Laws § 445.903	"Unfair, unconscionable, or deceptive methods, acts, or practices in the conduct of trade or commerce are unlawful and are defined as follows:. . ."	Up to $25,000: Mich. Comp. Laws § 445.905	Attorney General: Mich. Comp. Laws § 445.905

Minnesota Breach Notification Law	Minn. Stat. § 325E.61,	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: Yes, if over 500 residents. Notification in 48 hours. • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,000 residents or $250,000 • Credit Monitoring: No	Unclear: Minn. Stat. §§ 325E.61(6), 8.31	Attorney General: Minn. Stat. §§ 325E.61(6), 8.31
Unfair, Deceptive, or Abusive Acts and Practices	Minn. Stat. § 325F.69	"Fraud, misrepresentation, deceptive practices. The act, use, or employment by any person of any fraud, false pretense, false promise, misrepresentation, misleading statement or deceptive practice, with the intent that others rely thereon in connection with the sale of any merchandise, whether or not any person has in fact been misled, deceived, or damaged thereby, is enjoinable as provided in section 325F.70."	Unclear: Minn. Stat. § 8.31	Attorney General: Minn. Stat. § 8.31
Mississippi Breach Notification Law	Miss. Code § 75-24-29	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 5,000 residents or $5,000 • Credit Monitoring: • Other:	$10,000 per violation: Miss. Code § 75-24-19	Attorney General: Miss. Code § 75-24-29(8)
Unfair, Deceptive, or Abusive Acts and Practices	Miss. Code § 75-24-5	"Unfair methods of competition affecting commerce and unfair or deceptive trade practices in or affecting commerce are prohibited. Action may be brought under Section 75-24-5(1) only under the provisions of Section 75-24-9."	$10,000 per violation: Miss. Code § 75-24-19	Attorney General: Miss. Code § 75-24-9
Missouri Breach Notification Law	Mo. Rev. Stat. § 407.1500	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 1000 residents • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 150,000 residents or $150,000 • Credit Monitoring: • Other:	Up to $150,000: Mo. Rev. Stat. § 407.1500(3)	Attorney General: Mo. Rev. Stat. § 407.1500(3)
Unfair, Deceptive, or Abusive Acts and Practices	Mo. Rev. Stat. § 407.020	"he act, use or employment by any person of any deception, fraud, false pretense, false promise, misrepresentation, unfair practice or the concealment, suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce or the solicitation of any funds for any charitable purpose, as defined in section 407.453, in or from the state of Missouri, is declared to be an unlawful practice."	Up to $1000 per violation: Mo. Rev. Stat. § 407.100(6)	Attorney General: Mo. Rev. Stat. § 407.100
Montana Breach Notification Law	Mont. Code § 30-14-1704	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: Yes, coordination provision • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,000 residents or $250,000 • Credit Monitoring: • Other:	Up to $10,000 per willful violation: Mont. Code §§ 30-14-1705; 30-14-142(2)	Department of Justice (Attorney General): Mont. Code § 30-14-1705
Unfair, Deceptive, or Abusive Acts and Practices	Mont. Code § 30-14-103	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are unlawful."	Up to $10,000 per willful violation: Mont. Code § 30-14-142(2)	Department of Justice (Attorney General): Mont. Code § 30-14-1705

Nebraska Breach Notification Law	Nebraska Neb. Rev. Stat. § 87-803	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 100,000 residents or $75,000 • Credit Monitoring: No	Direct economic damage: Neb. Rev. Stat. § 87-806	Attorney General: Neb. Rev. Stat. § 87-806
Unfair, Deceptive, or Abusive Acts and Practices	Neb. Rev. Stat. § 59-1602	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce shall be unlawful."	Up to $2,000 per violation: Neb. Rev. Stat. § 59-1614	Attorney General: Neb. Rev. Stat. § 59-1614
Nevada Breach Notification Law	Nev. Rev. Stat. § 603A.220	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,000 residents or $250,000 • Credit Monitoring: No	Injunction: Nev. Rev. Stat. § 603A.290	Attorney General: Nev. Rev. Stat. § 603A.290
Personal Information Protection Act	Nev. Rev. Stat. § 603A.210	"A data collector that maintains records which contain personal information of a resident of this State shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure."	Injunction: Nev. Rev. Stat. § 603A.290	Attorney General: Nev. Rev. Stat. § 603A.290
Unfair, Deceptive, or Abusive Acts and Practices	Neb. Rev. Stat. § 59-1602	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce shall be unlawful."	Up to $2,000 per violation: Neb. Rev. Stat. § 59-1614	Attorney General: Neb. Rev. Stat. § 59-1608
New Hampshire Breach Notification Law	N.H. Rev. Stat. § 359-C:20	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if subject to N.H. Rev. Stat. § 358-A:3(I) • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: As soon as possible • Substitute Notice: Yes, if over 1,000 residents or $5,000 • Credit Monitoring: No	Up to $10,000 per violation: N.H. Rev. Stat. §§ 359-C:20; 358-A:4(III)(b)	Attorney General: N.H. Rev. Stat. §§ 359-C:20; 358-A:4
Unfair, Deceptive, or Abusive Acts and Practices	N.H. Rev. Stat. § 358-A:2	"It shall be unlawful for any person to use any unfair method of competition or any unfair or deceptive act or practice in the conduct of any trade or commerce within this state. Such unfair method of competition or unfair or deceptive act or practice shall include, but is not limited to, the following:"	Up to $10,000 per violation: N.H. Rev. Stat. § 358-A:4(III)(b)	Consumer Protection and Antitrust Bureau, Department of Justice: N.H. Rev. Stat. § 358-A:4
New Jersey Breach Notification Law	N.J. Stat. § 56:8-163	• Notify Affected Residents: Yes • Notify Attorney General: Yes, prior to notification to customers • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,000 residents or $250,000 • Credit Monitoring: No • Other:	Up to $10,000 for the first offense, and $20,000 for subsequent offenses: N.J. Stat. § 56:8-13	Attorney General: N.J. Stat. § 56:8-3.1

Unfair, Deceptive, or Abusive Acts and Practices	N.J. Stat. § 56:8-2	"The act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise or real estate, or with the subsequent performance of such person as aforesaid, whether or not any person has in fact been misled, deceived or damaged thereby, is declared to be an unlawful practice; provided, however, that nothing herein contained shall apply to the owner or publisher of newspapers, magazines, publications or printed matter wherein such advertisement appears, or to the owner or operator of a radio or television station which disseminates such advertisement when the owner, publisher, or operator has no knowledge of the intent, design or purpose of the advertiser."	Up to $10,000 for the first offense, and $20,000 for subsequent offenses: N.J. Stat. § 56:8-13	Attorney General: N.J. Stat. § 56:8-3.1
New Mexico Breach Notification Law	N.M. Stat. § 57-12c-6	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 1000 residents • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: No later than 45 days after the breach discovery date • Substitute Notice: Yes, if over 50,000 residents or $100,000 • Credit Monitoring: No	Up to $150,000: N.M. Stat. § 57-12c-11	Attorney General: N.M. Stat. § 57-12c-11
Personal Information Protection Act	N.M. Stat. § 57-12c-4	"A person that owns or licenses personal identifying information of a New Mexico resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal identifying information from unauthorized access, destruction, use, modification or disclosure."	Up to $25,000: N.M. Stat. § 57-12c-11	Attorney General: N.M. Stat. § 57-12c-11
Unfair, Deceptive, or Abusive Acts and Practices	N.M. Stat. § 57-12-3	"Unfair or deceptive trade practices and unconscionable trade practices in the conduct of any trade or commerce are unlawful."	Up to $5,000 per violation: N.M. Stat. § 57-12-11	Attorney General: N.M. Stat. § 57-12-11
New York Breach Notification Law	N.Y. Gen. Bus. Law § 899-AA, N.Y. State Tech. Law 208	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: Yes, if over 5000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,000 residents or $250,000 • Credit Monitoring: No	Up to $150,000: N.Y. Gen. Bus. Law § 899-AA(6)	Attorney General: N.Y. Gen. Bus. Law § 899-AA(6)
Unfair, Deceptive, or Abusive Acts and Practices	N.Y. Gen. Bus. Law § 349	"Deceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state are hereby declared unlawful."	Up to $5,000 per violation: N.Y. Gen. Bus. Law § 350-d	Attorney General: N.Y. Gen. Bus. Law § 349(f)
North Carolina Breach Notification Law	N.C. Gen. Stat § 75-65	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,000 or $250,000 • Credit Monitoring: No • Other:	Up to $5,000 per violation: N.C. Gen. Stat. §§ 75-65(i), 75-15.2	Attorney General: N.C. Gen. Stat. §§ 75-65(i), 75-15
Unfair, Deceptive, or Abusive Acts and Practices	N.C. Gen. Stat. § 75-1.1	"Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are declared unlawful."	Up to $5,000 per violation: N.C. Gen. Stat. § 75-15.2	Attorney General: N.C. Gen. Stat. § 75-15

North Dakota Breach Notification Law	N.D. Cent. Code § 51-30-02	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 250 people • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,000 or $250,000 • Credit Monitoring: No	Up to $5,000 per violation: N.D. Cent. Code §§ 51-30-07, 51-15-11	Attorney General: N.D. Cent. Code § 51-30-07
Unfair, Deceptive, or Abusive Acts and Practices	N.D. Century Code § 51-15-02	"The act, use, or employment by any person of any deceptive act or practice, fraud, false pretense, false promise, or misrepresentation, with the intent that others rely thereon in connection with the sale or advertisement of any merchandise, whether or not any person has in fact been misled, deceived, or damaged thereby, is declared to be an unlawful practice. The act, use, or employment by any person of any act or practice, in connection with the sale or advertisement of any merchandise, which is unconscionable or which causes or is likely to cause substantial injury to a person which is not reasonably avoidable by the injured person and not outweighed by countervailing benefits to consumers or to competition, is declared to be an unlawful practice."	Up to $5,000 per violation: N.D. Cent. Code § 51-15-11	Attorney General: N.D. Cent. Code § 51-15-07
Ohio Breach Notification Law	Ohio Rev. Code § 1349.19	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: No longer than 45 days following the breach discovery date • Substitute Notice: Yes, if over 500,000 residents or $250,000 • Credit Monitoring: No • Other: Substitute notice exception for small businesses.	Cascading penalties based on delay: Ohio Rev. Code § 1349.192	Attorney General: Ohio Rev. Code § 1349.19(i)
Unfair, Deceptive, or Abusive Acts and Practices	Ohio Rev. Code § 1345.02	"No supplier shall commit an unfair or deceptive act or practice in connection with a consumer transaction. Such an unfair or deceptive act or practice by a supplier violates this section whether it occurs before, during, or after the transaction."	Up to $25,000: Ohio Rev. Code § 1345.07	Attorney General: Ohio Rev. Code § 1345.02(E)(3)
Oklahoma Breach Notification Law	Okla. Stat. tit. 24, § 163	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 100,000 residents or $50,000 • Credit Monitoring: No	Up to $150,000: Okla. Stat. § 24-165	Attorney General: Okla. Stat. § 24-165
Unfair, Deceptive, or Abusive Acts and Practices	Okla. Stat. tit. 15, § 753	"A person engages in a practice which is declared to be unlawful under the Oklahoma Consumer Protection Act when, in the course of the person's business, the person . . ."	Up to $2,000 per violation or up to $10,000 per willful violation: Okla. Stat. tit. 15, § 761.1	Attorney General: Okla. Stat. tit. 15, § 761.
Oregon Breach Notification Law	Oregon Rev. Stat. § 646A.604	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 250 residents • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 350,000 residents and $250,000 • Credit Monitoring: Yes	Or. Rev. Stat. §§ 646A.604(9)(a), 646.642(3)	Director of the Department of Consumer and Business Services: Or. Rev. Stat. § 646A.624
Personal Information Protection Act	Or. Rev. Stat. § 646A.622	"A person that owns, maintains or otherwise possesses, or has control over or access to, data that includes personal information that the person uses in the course of the person's business, vocation, occupation or volunteer activities shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the personal information, including safeguards that protect the personal information when the person disposes of the personal information."	Up to $1000 per violation: Or. Rev. Stat. § 646A.624	Director of the Department of Consumer and Business Services: Or. Rev. Stat. § 646A.624

Unfair, Deceptive, or Abusive Acts and Practices	Or. Rev. Stat. § 646.607	"A person engages in an unlawful trade practice if in the course of the person's business, vocation or occupation the person. . ."	Up to $250,000 per violation: Or. Rev. Stat. § 646.642(3)	Prosecuting attorney: Or. Rev. Stat. § 646.642(3)
Pennsylvania Breach Notification Law	73 Pa. Stat. § 2303	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 175,000 people or $100,000 • Credit Monitoring: No	Up to $1,000 per violation: 73 Pa. Stat. §§ 2308, 201-8	Attorney General: 73 Pa. Stat. § 2308
Unfair, Deceptive, or Abusive Acts and Practices	73 Pa. Stat. § 201-3	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce as defined by subclauses (i) through (xxi) of clause (4) of section 21 of this act and regulations promulgated under section 3.12 of this act are hereby declared unlawful. The provisions of this act shall not apply to any owner, agent or employee of any radio or television station, or to any owner, publisher, printer, agent or employee of an Internet service provider or a newspaper or other publication, periodical or circular, who, in good faith and without knowledge of the falsity or deceptive character thereof, publishes, causes to be published or takes part in the publication of such advertisement."	Up to $1,000 per violation: 73 Pa. Stat. § 201-8	Attorney General: 73 Pa. Stat. § 201-8
Rhode Island Breach Notification Law	R.I. Gen. Laws § 11-49.3-4	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over • Credit Monitoring: • Other:	$100 per reckless violation, $200 per knowing/willful violation: R.I. Gen. Laws § 11-49.3-5	Attorney General: R.I. Gen. Laws § 11-49.3-5
Personal Information Protection Act	R.I. Gen. Laws § 11-49.3-2	"A municipal agency, state agency or person that stores, collects, processes, maintains, acquires, uses, owns or licenses personal information about a Rhode Island resident shall implement and maintain a risk-based information security program that contains reasonable security procedures and practices appropriate to the size and scope of the organization; the nature of the information; and the purpose for which the information was collected in order to protect the personal information from unauthorized access, use, modification, destruction, or disclosure and to preserve the confidentiality, integrity, and availability of such information. A municipal agency, state agency, or person shall not retain personal information for a period longer than is reasonably required to provide the services requested; to meet the purpose for which it was collected; or in accordance with a written retention policy or as may be required by law. A municipal agency, state agency, or person shall destroy all personal information, regardless of the medium that such information is in, in a secure manner, including, but not limited to, shredding, pulverization, incineration, or erasure."	$100 per reckless violation, $200 per knowing/willful violation: R.I. Gen. Laws § 11-49.3-5	Attorney General: R.I. Gen. Laws § 11-49.3-5
Unfair, Deceptive, or Abusive Acts and Practices	R.I. Gen. Laws § 6-13.1-2	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are declared unlawful."	Up to $10,000 per violation: R.I. Gen. Laws § 6-13.1-8	Attorney General: R.I. Gen. Laws § 6-13.1-8
South Carolina Breach Notification Law	S.C. Code § 39-1-90	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 1000 residents • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over • Credit Monitoring: • Other:	$1,000 per resident for knowing or willful violation: S.C. Code § 39-1-90(H)	Attorney General: S.C. Code § 39-1-90(H)
Unfair, Deceptive, or Abusive Acts and Practices	S.C. Code § 39-5-20	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful."	Up to $5,000 per violation: S.C. Code § 39-5-110	Attorney General: S.C. Code § 39-5-110

South Dakota Breach Notification Law	SD SB62	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 250 residents • Notify Credit Reporting Agencies: Yes • If not data owner, notify data owner: Yes • How many days to Notify: Within 60 days of breach discovery date. • Substitute Notice: Yes, if over 500,000 people or $250,000 • Credit Monitoring: • Other:	Enacted on 3/21/2018, effective July 1, 2018	http://sdlegislature.gov/docs/legsession/2018/Bills/SB62ENR.pdf
Unfair, Deceptive, or Abusive Acts and Practices	S.D. Codified Laws § 37-24-6	"It is a deceptive act or practice for any person to: (1) Knowingly act, use, or employ any deceptive act or practice, fraud, false pretense, false promises, or misrepresentation or to conceal, suppress, or omit any material fact in connection with the sale or advertisement of any merchandise, regardless of whether any person has in fact been misled, deceived, or damaged thereby. . . "	Up to $2,000 per violation: S.D. Codified Laws § 37-24-27	Attorney General: S.D. Codified Laws § 37-24-23
Tennessee Breach Notification Law	Tenn. Code § 47-18-2107	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes, within 45 of breach discovery date • How many days to Notify: Within 45 of breach discovery date • Substitute Notice: Yes, if over 500,000 people or $250,000 • Credit Monitoring: No	"civil penalty of whichever of the following is greater: ten thousand dollars ($10,000), five thousand dollars ($5,000) per day for each day that a person's identity has been assumed or ten (10) times the amount obtained or attempted to be obtained by the person using the identity theft.": Tenn. Code § 47-18-2105	Division of Consumer Affairs of the Department of Commerce and Insurance: Tenn. Code § 47-18-2105
Personal Information Protection Act	Tenn. Code § 47-18-2110	"On and after January 1, 2008, any person, nonprofit or for profit business entity in this state, including, but not limited to, any sole proprietorship, partnership, limited liability company, or corporation, engaged in any business, including, but not limited to, health care, that has obtained a federal social security number for a legitimate business or governmental purpose shall make reasonable efforts to protect that social security number from disclosure to the public."	"civil penalty of whichever of the following is greater: ten thousand dollars ($10,000), five thousand dollars ($5,000) per day for each day that a person's identity has been assumed or ten (10) times the amount obtained or attempted to be obtained by the person using the identity theft.": Tenn. Code § 47-18-2105	Division of Consumer Affairs of the Department of Commerce and Insurance: Tenn. Code § 47-18-2105
Unfair, Deceptive, or Abusive Acts and Practices	Tenn. Code § 47-18-104	The following unfair or deceptive acts or practices affecting the conduct of any trade or commerce are declared to be unlawful and in violation of this part:	Up to $1,000 per violation: Tenn. Code § 47-18-108(b)(3)	Division of Consumer Affairs of the Department of Commerce and Insurance: Tenn. Code § 47-18-108
Texas Breach Notification Law	Tex. Bus. & Com. Code § 521.053	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 10,000 people • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: 500,000 people or $250,000 • Credit Monitoring: No	Between $2,000 and $50,000 per violation and up to $150,000 in additional penalties: Tex. Bus. & Com. Code § 521.151	Attorney General: Tex. Bus. & Com. Code § 521.151
Personal Information Protection Act	Tex. Bus. & Com. Code § 521.052	"A business shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business."	Between $2,000 and $50,000 per violation: Tex. Bus. & Com. Code § 521.151	Attorney General: Tex. Bus. & Com. Code § 521.151
Unfair, Deceptive, or Abusive Acts and Practices	Tex. Bus. & Com. Code § 17.45	"False, misleading, or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful and are subject to action by the consumer protection division. . ."	Up to $20,000 per violation: Tex. Bus. & Com. Code § 17.47	Consumer Protection Division, Attorney General: Tex. Bus. & Com. Code § 17.47

Utah Breach Notification Law	Utah Code § 13-44-202	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Not allowed • Credit Monitoring: No	Up to $100,000: Utah Code § 13-44-301	Attorney General: Utah Code § 13-44-301
Personal Information Protection Act	Utah Code § 13-44-201	"Any person who conducts business in the state and maintains personal information shall implement and maintain reasonable procedures to: (a) prevent unlawful use or disclosure of personal information collected or maintained in the regular course of business; and (b) destroy, or arrange for the destruction of, records containing personal information that are not to be retained by the person."	Up to $100,000: Utah Code § 13-44-301	Attorney General: Utah Code § 13-44-301
Unfair, Deceptive, or Abusive Acts and Practices	Utah Code § 13-11-5	"An unconscionable act or practice by a supplier in connection with a consumer transaction violates this act1 whether it occurs before, during, or after the transaction."	Up to $2,500 per violation (administrative fine): Utah Code § 13-11-17	Division of Consumer Protections: Utah Code § 13-11-17
Vermont Breach Notification Law	Vt. Stat. tit. 9 § 2435	• Notify Affected Residents: Yes • Notify Attorney General: Yes, within 14 business days of breach discovery • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 5,000 residents or $5,000 • Credit Monitoring: • Other:	Unclear from statute	Attorney General: Vt. Stat. tit. 9 § 2435(g)
Unfair, Deceptive, or Abusive Acts and Practices	Vt. Stat. tit. 9, § 2453	"Unfair methods of competition in commerce and unfair or deceptive acts or practices in commerce are hereby declared unlawful."	Up to $10,000 per violation: Vt. Stat. tit. 9, § 2461	Attorney General: Vt. Stat. tit. 9, § 2461
Virginia Breach Notification Law	Va. Code § 18.2-186.6	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 1000 residents • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 100,000 residents or $50,000 • Credit Monitoring: • Other: Special provisions for income tax data	Up to $150,000 per breach: Va. Code § 18.2-186.6(I)	Attorney General: Va. Code § 18.2-186.6(I)
Unfair, Deceptive, or Abusive Acts and Practices	Va. Code § 59.1-200	"The following fraudulent acts or practices committed by a supplier in connection with a consumer transaction are hereby declared unlawful . . ."	Up to $2,500 per violation: Va. Code § 59.1-206	Attorney General: Va. Code § 59.1-206
Washington Breach Notification Law	Wash. Rev. Code § 19.255.010	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 500 residents • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: No more than 45 days after the breach discovery • Substitute Notice: Yes, if over 500,000 residents or $250,000 • Credit Monitoring: • Other: Reimbursement from businesses to financial institutions provision	Up to $25,000: Wash. Rev. Code §§ 19.255.010(17), 19.86.140	Attorney General: Wash. Rev. Code § 19.255.010(17)
Unfair, Deceptive, or Abusive Acts and Practices	Wash. Rev. Code § 19.86.020	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful."	Up to $25,000: Wash. Rev. Code § 19.86.140	Attorney General: Wash. Rev. Code § 19.86.080

West Virginia Breach Notification Law	W.Va. Code § 46A-2A-102	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 100,000 residents or $50,000 • Credit Monitoring: No • Other:	Up to $5,000 per violation: W.Va. Code §§ 46A-2A-104, 46A-7-111	Attorney General: W.Va. Code § 46A-2A-104
Unfair, Deceptive, or Abusive Acts and Practices	W. Va. Code § 46A-6-104	Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful."	Up to $5,000 per violation: W.Va. Code § 46A-7-111	Attorney General: W.Va. Code § 46A-7-111
Wisconsin Breach Notification Law	Wis. Stat. § 134.98	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Within 45 days of the breach discovery date • Substitute Notice: Yes, see statute • Credit Monitoring:	None	No one
Unfair, Deceptive, or Abusive Acts and Practices	Wis. Stat. § 100.20	"Methods of competition in business and trade practices in business shall be fair. Unfair methods of competition in business and unfair trade practices in business are hereby prohibited."	From $100 to $10,000 per violation: Wis. Stat. § 100.26(6)	The Department of Agriculture, trade, and consumer protection: Wis. Stat. § 100.20
Wyoming Breach Notification Law	Wyo. Stat. § 40-12-502	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, see statute • Credit Monitoring: No	Damages: Wyo. Stat. § 40-12-502	Attorney General: Wyo. Stat. § 40-12-502(f)
Unfair, Deceptive, or Abusive Acts and Practices	Wyo. Stat. § 40-12-105	"A person engages in a deceptive trade practice unlawful under this act when, in the course of his business and in connection with a consumer transaction, he knowingly. . ."	Up to $5,000 per violation: Wyo. Stat. § 40-12-113	Attorney General: Wyo. Stat. § 40-12-113
District of Columbia Breach Notification Law	D.C. Code § 28- 3852	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 100,000 or $50,000 • Credit Monitoring: No	$100 per Affected Resident: D.C. Code § 28- 3853	US Attorney General: D.C. Code § 28- 3853
Unfair, Deceptive, or Abusive Acts and Practices	D.C. Code § 28-3904	"It shall be a violation of this chapter, whether or not any consumer is in fact misled, deceived or damaged thereby, for any person to: . . ."	Up to $1000 per violation: D.C. Code § 28-3909	Corporation Counsel: D.C. Code § 28-3909
Guam Breach Notification Law	9 GCA § 48.30	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 5,000 residents or $10,000 • Credit Monitoring: No • Other:	Up to $150,000 per breach: 9 GCA § 48.50	The Attorney General: 9 GCA § 48.50

Unfair, Deceptive, or Abusive Acts and Practices	5 GCA § 32201	"False, misleading, or deceptive acts or practices, including, but not limited to those listed in this chapter, are hereby declared unlawful and are subject to action by the Attorney General or any person as permitted pursuant to this chapter or other provisions of Guam law. A violation consisting of any act prohibited by this title is in itself actionable, and may be the basis for damages, rescission, or equitable relief. The provisions of this chapter are to be liberally construed in favor of the consumer, balanced with substantial justice, and violation of such provisions may be raised as a claim, defense, crossclaim or counterclaim."	Up to $5,000 per violation: 5 GCA § 32127	Attorney General: 5 GCA § 32116
Puerto Rico Breach Notification Law	10 Laws of Puerto Rico § 4051	• Notify Affected Residents: Yes • Notify the Secretary of Consumer Affairs: Yes, within 10 days • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 100,000 people or $100,000 • Credit Monitoring: No	Up to $5,000 per violation of the provisions of this chapter: 10 Laws of Puerto Rico § 4055	The Secretary: 10 Laws of Puerto Rico § 4055
Unfair, Deceptive, or Abusive Acts and Practices	10 Laws of Puerto Rico § 259	"Unfair methods of competition, and unfair or deceptive acts or practices in trade or commerce are hereby declared unlawful."	"a civil penalty imposed by the Department of Consumer Affairs up to a maximum of five thousand dollars ($5,000). Each separate violation of said decision shall be considered as continuous noncompliance therewith, in which case, each day the decision is not complied with shall be considered as a separate violation." 10 Laws of Puerto Rico § 259	The Office of Monopolistic Affairs: 10 Laws of Puerto Rico § 259
Virgin Islands Breach Notification Law	V.I. Code tit. 14, § 2208	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 50,000 residents or $100,000 • Credit Monitoring: No • Other:	Actual damages: V.I. Code tit. 14, § 2211	Private right of action: V.I. Code tit. 14, § 2211
Unfair, Deceptive, or Abusive Acts and Practices	V.I. Code tit. 12, § 101	"No person shall engage in any deceptive or unconscionable trade practice in the sale, lease, rental or loan or in the offering for sale, lease, rental, or loan of any consumer goods or services, or in the collection of consumer debts."	Up to $5,000 per violation: V.I. Code tit. 12, § 104	The Commissioner: V.I. Code tit. 12, § 104

Survey of International Cyber Laws

Title	Country	Information	Applies to	Notes
China Cybersecurity Law (CSL)	CHINA	CSL regulates the construction, operation, maintenance and use of networks, as well as network security supervision and management within mainland China. The Cyberspace Administration of China (CAC) is the primary governmental authority supervising and enforcing the CSL.		
General Data Privacy Regulation (GDPR)	EUROPEAN UNION	The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy.	Countries that belong to the EEA include EU + 3. Austria, Belgium, Bulgaria, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom. Non-EU countries in the EEA Norway, Iceland, Liechtenstein	While GDPR is In place as law there is not yet specific country by country adoption of laws to align or go stricter than GDPR. It should be expected that Germany, France and Spain will go above and beyond the standard GDPR language and add more provisions.
International Traffic in Arms Regulations (ITAR)	UNITED STATES	A United States regulatory regime to restrict and control the export of defense and military related technologies to safeguard U.S. national security and further U.S. foreign policy objectives ITAR is the International Traffic in Arms Regulations and requires, in part, that defense-related articles and technical data listed on the United States Munitions List USML only be shared with U.S. citizens absent special authorization or exemption. Furthermore, ITAR is a set of standards that deals with information security involving any parties that handle technical data related to the manufacturing, the exporting and a general involvement with defense articles or services.		
Encryption and Export Administration Regulation (EAR)		The Export Administration Regulations (EAR) is a set of US government regulations on the export and import of most commercial items. The U.S. Department of Commerce is responsible for implementing and enforcing EAR. Specifically, working with items deemed dual-use and having both commercial and military applications. In particular, encryption or Cryptographic Information Security		
Australia		The Privacy Act includes thirteen Australian Privacy Principles (APPs). The APPs set out standards, rights and obligations for the handling, holding, use, accessing and correction of personal information (including sensitive information).		
India	India	India is not a part of any convention on protection of personal data that is equvalent to the GDPR. India has adopted other international declarations and conventions including the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, these acts recognise the right to privacy.		
Japan		European Union (EU)-Japan Economic Partnership Agreement (EPA) is a reciprocal adequacy arrangement that established the equivalence of the EU's General Data Protection Regulation (GDPR) and Japan's Act on the Protection of Personal Information (APPI) and enabling cross-border data transfers between the two. Japan was previously not included in the EU's whitelist of countries considered as having adequate levels of personal data protection.		

Russia		In 2014, Russia adopted personal data localisation rules. These rules required all operators that collect and process Russian citizens personal data to use databases located in Russia. These requirements apply to the personal data of all Russian citizens, regardless of their relation with the company. The new rules do not cross-border transfer of personal data. However, the requirement for primary data processing via Russian databases is considered to be onerous.		
Canada		Canada has adequacy with the EU and GDPR (as of the launch of GDPR) based on the PIPDEA law that covers data privacy in Canada. In general, Canada privacy is not that bad. However, organizations in British Columbia and Nova Scotia that do business with quasi-governmental entities such as banks & transportation are subject to FIPPA. In particualr, article 30. is critical to understand as it prohibits transfer of data outside of Canada.		

Survey of Institutions

Title	Information	URL
Cloud Security Alliance	Offers a number of certifications including: CSA Security, Trust & Assurance Registry (STAR) Certificate of Cloud Security Knowledge (CCSK) Certified Cloud Security Professional (CCSP) Global Consultancy Program	https://cloudsecurityalliance.org/
Commission on Accreditation for Law Enforcement Agencies ("CALEA")	CALEA is intended to preserve the ability of law enforcement agencies to conduct electronic surveillance while protecting the privacy of information outside the scope of the investigation. It requires that telecommunications carriers and manufacturers of telecommunications equipment design their equipment, facilities, and services to ensure that they have the necessary surveillance capabilities to comply with legal requests for information.	http://www.calea.org/
Control Objectives for Information and Related Technologies ("COBIT")	COBIT 5 is the only business framework for the governance and management of enterprise IT. COBIT 5 integrates other major frameworks, standards and resources, including ISACA's Val IT and Risk IT, Information Technology Infrastructure Library (ITIL®) and related standards from the International Organization for Standardization (ISO).	http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx
Federal Energy Regulatory Commission (FERC) Revised Critical Infrastructure Protection (CIP) Reliability Standards	NERC, which FERC has certified as the nation's Electric Reliability Organization, developed Critical Infrastructure Protection (CIP) cyber security reliability standards. On January 18, 2008, the Commission issued Order No. 706, the Final Rule approving the CIP reliability standards, while concurrently directing NERC to develop significant modifications addressing specific concerns. In January 2016, FERC issued a Final Rule revising the CIP reliability standards. Docket No. RM15-14-000. As of December 2017, FERC release a Notice of Proposed Rulemaking to direct NERC to develop and submit modifications to improve mandatory reporting of Cyber Security Incidents. [Docket Nos. RM18-2-000 and AD17-9-000.	https://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity.asp
Federal Financial Institutions Examination Councils ("FFIEC")	The Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB) and to make recommendations to promote uniformity in the supervision of financial institutions. Guidance includes: Online Banking: https://www.ffiec.gov/pdf/authentication_guidance.pdf FFIEC Cybersecurity Assessment Tool: https://www.ffiec.gov/cyberassessmenttool.htm	https://www.ffiec.gov/
Health Insurance Trust Alliance (HITRUST) CSF	HITRUST CSF is a certifiable framework that provides organizations with a comprehensive, flexible and efficient approach to regulatory compliance and risk management.	https://hitrustalliance.net/hitrust-csf/

Indiana Department of Financial Institutions (DFI)	Enforces FFIEC standards.	https://www.in.gov/dfi/
Indiana State Insurance Commissioners Navigators and Application Organizations		https://www.in.gov/idoi/
International Organization for Standardization ("ISO")	ISO creates documents that provide requirements, specifications, guidelines or characteristics that can be used consistently to ensure that materials, products, processes and services are fit for their purpose.	https://www.iso.org/home.html
ISA/IEC 62443 (ISA99)	The ISA-99/IEC 62443 standard is the worldwide standard for security of the Industrial Control Systems in the Operational Technology (OT) domain of organizations. The standard was created by the International Society of Automation, a leading worldwide nonprofit organization. The standard offers organizations handles to improve the digital security and safety of their process and SCADA environments.	https://www.isa.org/isa99/
National Institute of Standards and Technology ("NIST")	NIST is a measurement standards laboratory, and a non-regulatory agency of the United States Department of Commerce.	https://www.nist.gov/
North American Electric Reliability Corporation ("NERC")	The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the bulk power system through system awareness; and educates, trains, and certifies industry personnel.	https://www.nerc.com/Pages/default.aspx
PCI Security Standards Council	Helps merchants and financial institutions understand and implement standards for security policies, technologies and ongoing processes that protect their payment systems from breaches and theft of cardholder data. Also helps vendors understand and implement standards for creating secure payment solutions.	https://www.pcisecuritystandards.org/
SSAE-18/ ISAE 3402	ISAE 3402 was developed to provide an international assurance standard for allowing public accountants to issue a report for use by user organizations and their auditors (user auditors) on the controls at a service organization that are likely to impact or be a part of the user organization's system of internal control over financial reporting.	https://www.ssae-16.com/soc-1-report/the-ssae-18-audit-standard/

Business Insurance Survey and Report – 2020

State of Hoosier Cybersecurity

2020

December 2020

Prepared for

Indiana Executive Council on Cybersecurity

By

Kelley School of Business, Indiana University
Indiana Business Research Center
Anne Boustead JD, PhD (University of Arizona), Scott Shackelford JD, PhD (Indiana University)

Special thanks to Jay Bhatia and Eric Spencer for their invaluable research support in this project. We would also like to thank the anonymous respondents who participated in our survey on behalf of their organizations, and to Stephen Vina, and Professors Asaf Lubin and Angie Raymond for their helpful comments and suggestions.

Table of Contents

Index of Figures

Contact Information

For more information about this report, contact the Indiana Business Research Center at (812) 855-5507 or email ibrc@iupui.edu. Professor Shackelford may be reached at sjshacke@indiana.edu.

Executive Summary

As is the case in many jurisdictions, public and private organizations in Indiana are unfortunately no stranger to cyber attacks. Counties across the state such as Lake,[1] Lawrence,[2] and LaPorte[3] have been targeted by criminals in recent ransomware campaigns, leading to hundreds of thousands in losses. Healthcare providers such as Hancock Memorial Hospital have been similarly breached, as have universities, small business, utilities, and school corporations.[4] Yet it has proven difficult to understand the full scope of these cyber threats, and how Hoosier organizations are attempting to prevent and respond to them.

To get a more complete picture of Hoosier cyber risk planning, the Legal and Insurance working group of the Indiana Executive Cybersecurity Council, in collaboration with researchers at Indiana University and the University of Arizona, conducted this study to help explore how Indiana organizations perceive and manage cyber risks. We pay particular attention to the role of insurance as part of an overarching cyber risk mitigation strategy.

The report is broken down into the following sections. Section 1 offers background on the technical, organizational, and legal dimensions of the cyber threat, along with a policy review highlighting recent primarily state-level efforts in Indiana and beyond to better manage cyber risk. Section 2 reviews the methods used in this study. Section 3 summarizes our results, paying particular attention to such topics as risk perceptions, management, and the evolving role of cyber risk insurance. Section 4 concludes the study with a look at policy opportunities to address the vulnerabilities and governance gaps revealed by the survey.

This goal of this report is to provide business leaders, policymakers, law enforcement professionals, and all Hoosiers with important information about cyber readiness, help organizations of all sizes better understand current cyber threats facing Indiana, and describe current efforts to address them. In the end, cybersecurity is a team sport, and we're all in this together.

---

[1] *See* Anna Ortiz, *Lake County, Ind., Sheriff's Email Online After Cyberattack*, GOVTECH (Sept. 9, 2019), https://www.govtech.com/security/Lake-County-Ind-Sheriffs-Email-Online-After-Cyberattack.html.

[2] *See* Rich Van Wyk, *Cyberattack Knocks out Lawrence County Government Computers*, WTHR (Feb. 13, 2020), https://www.wthr.com/article/news/local/indiana/cyberattack-knocks-out-lawrence-county-government-computers/531-637645fa-2797-416f-b890-e95112333106.

[3] *See* Mike Lowe, *Laporte County Government Pays $130K Ransom to Hackers*, WGNTV (July 18, 2019), https://wgntv.com/news/laporte-county-government-pays-130k-ransom-to-hackers/.

[4] *See* Patrick Howell O'Neill, *Indiana Hospital Shuts Down Systems After Ransomware Attack*, CYBERSCOOP (Jan. 15, 2018), https://www.cyberscoop.com/hancock-hospital-ransomware/.

Key Findings

- The Indiana organizations who responded to this survey generally expressed concern about the risk of a cyber incident. Less than 5% of respondents indicated that they were not at all concerned about the risk of a cyber incident, while over 46% of respondents identified as somewhat concerned and almost 49% identified as very concerned. When asked about the specific types of cyber incidents they were concerned about, respondents most frequently indicated concern about malware attacks (86% of respondents), phishing attacks (76% of respondents), and ransomware attacks (74% of respondents).
- In order to understand Indiana organizations' previous experiences with and responses to cyber incidents, respondents were asked whether their organization had experienced a successful cyber incident in the past three years. Approximately 19% of respondents indicated that they had experienced a successful cyber incident during this timeframe, while 67% of respondents indicated that their organization did not experience a successful cyber incident and 13% were either not sure or declined to provide an answer. Of respondents who indicated that their organization had experienced a successful cyber incident in the past three years, 50% indicated that none of these incidents resulted in data loss and 31% indicated that less than five of these incidents resulted in data loss.
- The vast majority – over 82% – of respondents indicated that their organization had taken steps to prevent a cyber incident; about 7% indicated that their organization had *not* taken steps to prevent cyber incidents, and about 9% indicated that they were not sure. Of respondents who indicated that they had taken steps to prevent cyber incidents, 95% had installed antivirus software, while over 75% had updated/patched software, and over 70% had provided their employees with training to reduce cyber-related risks. Seventeen respondents indicated that they had used mechanisms to prevent cyber incidents other than the options provided by the survey; these respondents described a broad range of alternative mechanisms including installing firewalls and spam filters, adopting multi-factor authentication, and hiring a cybersecurity firm to advise on defenses.
- Respondents who indicated that their organization had not taken steps to prevent cyber incidents were then asked why these steps had not been taken. Of those respondents who indicated that their organization had not taken steps to adopt cyber incident prevention mechanisms, slightly more than half attributed this decision to the organization being unsure what to do, while 40% explained that their organization did not think it was at risk. Perhaps most interestingly, no respondents indicated that their organization did not adopt cyber incident prevention mechanisms because they believed those mechanisms to be ineffective.
- In order to understand how Indiana organizations are protecting their systems and information, respondents were then asked whether their organization had adopted certain cybersecurity practices. Of the 178 respondents who answered the question, slightly less than half indicated that their organization had adopted automatic updating of operation systems and software and implementation of remote backups.
- The development and documentation of incident planning and response is a key cybersecurity practice. About 27% of respondents reported that their organization had written cyber incident planning and response documentation, with more than half indicating that their organization did not have such documentation and the remainder of respondents being uncertain or unresponsive.

- Cybersecurity response is also shaped by the people selected to lead this response. When asked who at their organization was ultimately responsible for managing cyber risk, about 15% of respondents indicated this role was filled by their Chief Information Officer, and about 14% indicated that this role was filled by their Chief Executive Officer. Interestingly, almost half of respondents elected to write in their own response to this question, with a common response being that this role was fulfilled by an information technology manager, director, or department (and several respondents indicating that no one served in this role).
- Organizations concerned about their cybersecurity have a range of external tools and frameworks available to help guide their decision making in this area. Fifty-eight respondents stated that their organization consulted an externally developed tool, framework, or control when making decisions about cyber practices. Among respondents who indicated that their organization used an externally developed framework to guide their cybersecurity decision making, the most commonly used framework was the NIST Cybersecurity Framework, which had been adopted by 58% of those organizations adopting a framework and 36% had adopted the Center for Internet Security (CIS) Critical Security Controls.
- About half of respondents indicated that their organization had cyber risk insurance; 26% indicated that their organization did not have cyber risk insurance; remaining respondents were either unsure or declined to answer. Respondents were next asked why their organization obtained a cyber risk insurance policy. Half of respondents described the decision to obtain cyber risk insurance as a response to news reports on cyber incidents. A large minority (40.82%) of respondents provided another reason for obtaining cyber risk insurance. These reasons included insurance agent recommendations or inclusion of cyber coverage in a general policy, response to cybersecurity trainings by trade organizations or other outside groups, and a perception that obtaining this insurance "just made business sense."

Understanding Cyber Risk

Although many consumers and businesses think of cyber risk in terms of hacked computers and stolen credit card numbers, there is a rapidly expanding universe of vulnerabilities fed in part by the explosion in Internet-connected devices and services comprising the Internet of Things. Even before the COVID-19 pandemic, which shifted many personal and professional activities online, cyber criminals, terrorists, hacktivists, and even foreign nation states were exploiting these vulnerabilities to steal identities, intellectual property, and compromise critical infrastructure. In this section, we begin by outlining the technical, economic, and legal dimensions of the cyber threat landscape currently facing organizations. We then turn to recommendations commonly made to organizations seeking to manage their cyber risk profiles, summarizing these best practices in terms of three steps: being aware, being organized, and being proactive. Finally, we discuss several issues that are currently changing the cyber risk landscape.

A. Cyber Threat Dimensions

Organizations currently face cyber risks across multiple dimensions: the myriad technical threats to information and systems pose serious economic threats across many sectors. Furthermore, the complex, patchwork legal landscape governing cybersecurity and privacy in the United States poses a challenge to businesses seeking to understand the protections that apply to them and the regulations they must comply with.

1. Technical

Technical vulnerabilities pervade modern business, and society. Smart phones can be compromised to be used as microphones even when they appear to be turned off.[5] Internet-connected lights and kitchen appliances can be hijacked to launch cyber attacks.[6] Internet traffic can be rerouted to servers around the world without the user's awareness.[7] Supply chain vulnerabilities and weak encryption can lead to a cascade of failures, yet are hard to identify and address.[8] Each of these cyber risks, as with so many others, require a suite of corporate

[5] *See* Darlene Storm, *New Attacks Secretly Use Smartphone Cameras, Speakers, and Microphones*, COMPUTER WORLD (Aug. 20, 2014), https://www.computerworld.com/article/2598704/new-attacks-secretly-use-smartphone-cameras--speakers-and-microphones.html.

[6] *See* Sarah Murray, *When Fridges Attack*: Why Hackers Could Target the Grid, FIN. TIMES (Oct. 17, 2018), https://www.ft.com/content/2c17ff5e-4f02-11e8-ac41-759eee1efb74.

[7] *See* Zak Doffmann, *Russia and China 'Hijack' Your Internet Traffic: Here's What You Do*, FORBES (Apr. 18, 2020), https://www.forbes.com/sites/zakdoffman/2020/04/18/russia-and-china-behind-internet-hijack-risk-heres-how-to-check-youre-now-secure/#2b936c395b16.

[8] *See* Nate Berg, *Starbudks, PepsiCo, and BMW Partner to Fix a Global Problem Worth Trillions*, FAST COMPANY (Aug. 6, 2020), https://www.fastcompany.com/90536448/starbucks-pepsico-and-bmw-partner-to-fix-a-global-problem-worth-trillions; Caroline Dowling, *How Vulnerable is Your Supply Chain?*, INDUSTRY WK. (Dec. 6, 2012),

governance and policy responses. The problem is vexing given both the complexity and scale of the issue, with reports of novel cyber attacks being launched every thirty-nine seconds.[9]

2. Economic

Successful cyber attacks can cause serious and long-lasting impacts on organizations, including but not limited to financial damages, compromised personally identifiable information, breaches of critical infrastructure, tarnished reputations, and a loss of consumer confidence.[10] Managing the fallout from a data breach can be a challenging and costly endeavor. While this pertains to most organizations, it is especially true for small and midsize businesses (SMBs). Cybercrime has become a significant cost center for these firms, with a 2019 survey revealing that 58% of executives thought that data breaches were a more significant concern than incidents like fires, floods, and physical break-ins combined.[11] This is both true of midmarket firms, as well as larger organizations; indeed, perhaps counterintuitively the bigger the company, the less it spends per employee for cybersecurity owing to economies of scale combined with a lack of focus on cybersecurity issues.[12] For example, a 2019 cybersecurity IBM survey of large firms found that only 16% of respondents considered user security awareness training to be a priority.[13]

In addition to businesses, attacks on local governments are more salient than ever. Governments often misperceive the potential complexity of a cyber attack, which can cause sensitive data like bank information, government processes, municipal employee records to become vulnerable. Just like businesses, local governments have to work within the lack of financial resources to tackle cybersecurity challenges, with average state or local government agencies spending less than 5% of their IT budget on cybersecurity.[14]

Despite these risks, and with a few notable exceptions such as the financial industry where cybersecurity spending is high due to the alignment of incentives through the imposition of

---

https://www.industryweek.com/supply-chain/customer-relationships/article/21959294/how-vulnerable-is-your-supply-chain.

[9] *See Hackers Attack Every 39 Seconds*, SEC. MAG. (Feb. 10, 2017), https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds.

[10] *See Press Release: New Study Reveals Impact of Cyberattacks on Consumer Confidence, Corporate Reputation*, DHM RES. (Oct. 3, 2019), https://www.dhmresearch.com/press-release-new-study-reveals-impact-of-cyberattacks-on-consumer-confidence-corporate-reputation/.

[11] Survey: *Cybercrime More Devastating to SMBs than Other Threats Combined*, GLOBE NEWS WIRE (Feb. 26, 2019), https://www.globenewswire.com/news-release/2019/02/26/1742542/0/en/Survey-Cybercrime-More-Devastating-to-SMBs-than-Other-Threats-Combined.html.

[12] *White Hat, Black Hat and the Emergence of the Gray Hat: The True Costs of Cybercrime* (Osterman Res. White Paper, Aug. 8, 2018), http://resources.malwarebytes.com/files/2018/08/GLOBAL-White-Hat-Black-Hat-and-the-Emergence-of-the-Gray-Hat-The-True-Costs-of-Cybercrime_Sponsored-by-Malwarebytes.pdf.

[13] *IBM Study: More Than Half of Organizations with Cybersecurity Incident Response Plans Fail to Test Them*, IBM (Apr. 11, 2019), https://newsroom.ibm.com/2019-04-11-IBM-Study-More-Than-Half-of-Organizations-with-Cybersecurity-Incident-Response-Plans-Fail-to-Test-Them.

[14] *See Congress Moving Closer Toward Cybersecurity Aid to State and Local Governments*, ST. SCOOP (Sept. 23, 2019), https://statescoop.com/congress-moving-closer-toward-cybersecurity-aid-to-state-and-local-governments/.

liability for breaches, the overall growth in cybersecurity spending remains relatively low according to Gartner Research. Spending on cybersecurity grew at 12% compound annual growth rate (CAGR) in 2018, and it is projected to decline to 7% CAGR by 2023.[15] Part of this decline may be explained by more boards pushing back and asking for improved data and understanding of what increased cybersecurity spending has achieved after years of heavy investment.[16] And, to date, many organizations have not faced significant fines, litigation costs, or incentives to change behavior. A 2018 report from Schinichi Kamiya and colleagues found that "[a]fter suffering a breach of customers' personal data, the average attacked firm loses 1.1 percent of its market value and experiences a 3.2 percentage point drop in its year-on-year sales growth rate."[17] In fact, some firms, such as LinkedIn, saw their stock prices actually rise following significant cyber attacks.[18] As a result, an open debate is underway about whether or not we are experiencing a market failure in cybersecurity and, if so, what role state and federal governments should have in addressing it.

3. Legal

Unlike other jurisdictions such as the European Union, the U.S. government has no comprehensive federal law that regulates information security, cybersecurity, and privacy throughout the country. As a result, many states have passed laws to address these governance gaps. This creates a unique challenge for organizations that conduct business across state lines, as these areas are currently regulated by a piecemeal of sector-specific federal laws and state legislation.

Some states have been more active in adopting cybersecurity laws than others, although some categories of cybersecurity have been commonly adopted. Figure 1 below shows variation in the number of cybersecurity laws adopted by states, taking into account laws that expressly criminalize phishing, distributed denial-of-service (DDoS) attacks, spyware, and ransomware, as well as the creation of a state-wide cybersecurity task force and adoption of the NAIC data security model law for the cyber-insurance industry. Furthermore, even states that have adopted similar laws may have implemented them at different times. For example, Figure 2 summarizes the year each state passed their Breach Notification Law.

Legislative policymaking is ongoing in this area. Thirty-eight states, Washington, D.C., and Puerto Rico have considered nearly 300 bills or resolutions that deal significantly with cybersecurity in 2020,[19] and 31 states enacted new cybersecurity legislation so far this year.

---

[15] *Id*.

[16] *See* Louis Columbus*, Why Cybersecurity is Really a Business Problem*, FORBES (June 25, 2020), https://www.forbes.com/sites/louiscolumbus/2020/06/25/why-cybersecurity-is-really-a-business-problem/#362b6134436c.

[17] Shinichi Kamiya, *What is the Impact of Successful Cyberattacks on Target Firms?*, NAT'L BUREAU OF ECON. RES. (NBER Working Paper No. 24409, 2018), http://www.nber.org/papers/w24409.

[18] *See* Nicole Perlroth, *Lax Security at LinkedIn Is Laid Bare*, N.Y. TIMES, June 10, 2012, at B1.

[19] Cybersecurity Legislation 2020, https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2020.aspx (last visited Aug. 11, 2020).

This marks a significant rise from 2015 when only 26 states considered resolutions and just eight states enacting legislation. Some of the areas seeing the most recent legislative activity include:

- Increasing penalties for cybercrimes.
- Regulating cybersecurity within the insurance industry.
- Regulating government agencies to implement training and security policies and practices to better improve incidence response and preparedness.
- Creating task forces and commissions to study or advise on cybersecurity issues.
- Supporting programs and incentives for cybersecurity training and education.

OBJ

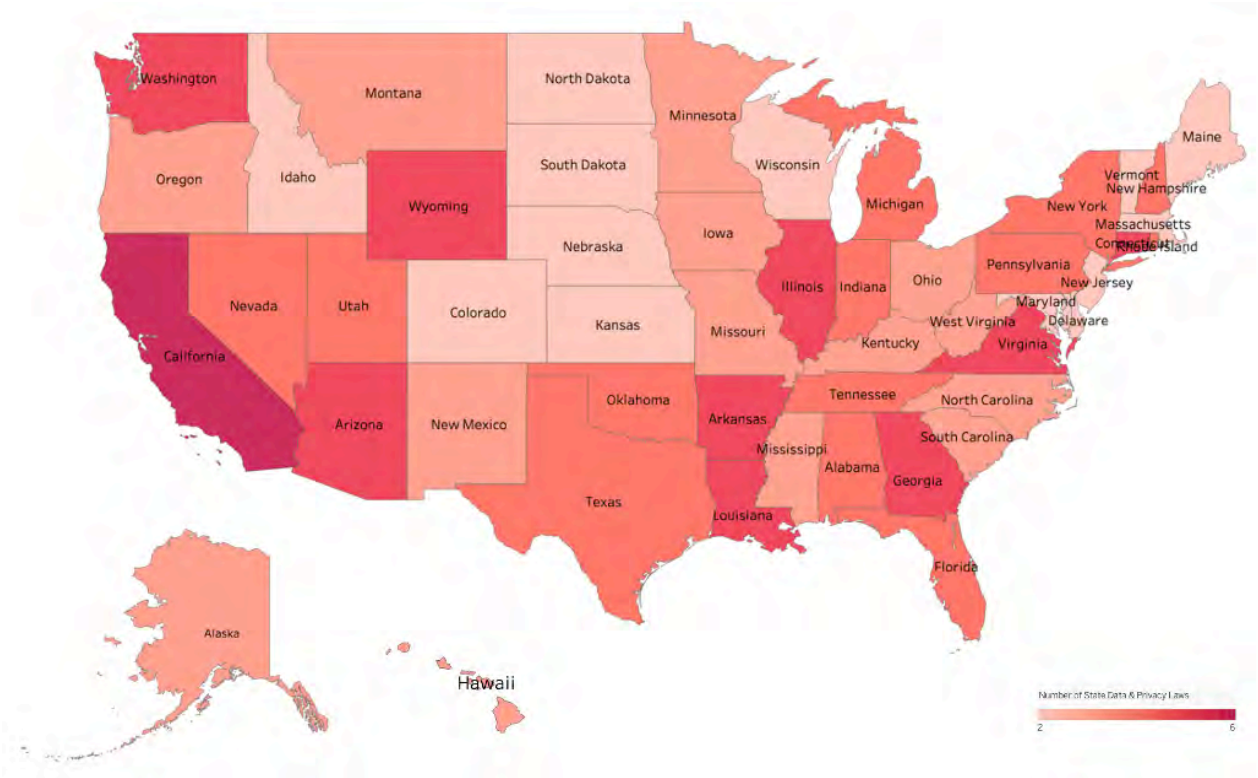


Figure 1: State-Level Cybersecurity Laws (2020)

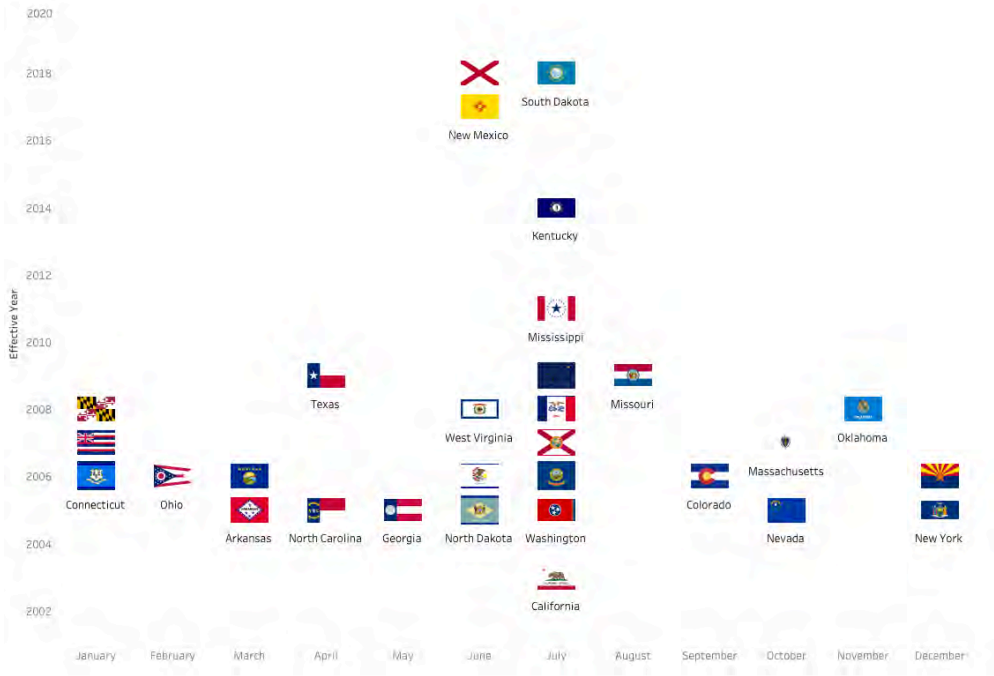


Figure 2: State Breach Notification Laws

B. Steps to Managing Cyber Risks

Analysts have recommended that organizations of all sizes manage cyber risk by (1) being aware, (2) being organized, and (3) being proactive.[20] As we discuss below, each of these steps can potentially include a wide range of technical and business activities.

1. Be Aware

Managers and policymakers need to keep up to date on the growing variety of cyber threats facing their organizations, especially as an increasing number of workers are working remotely. Phishing and ransomware campaigns are especially prevalent during the pandemic.[21] Cybercriminals have taken advantage of the current global health crisis, for example, and the new technical configurations that result from a remote workforce to multiply the number of attacks.[22] In response, organizations of all sizes need to be aware of the variety of cyber threats facing their organizations. A range of cybersecurity best practices can help firms better

[20] Scott J. Shackelford, *The Three 'B's' of Cybersecurity for Small Businesses*, CONVERSATION (Apr. 17, 2017), https://theconversation.com/the-three-bs-of-cybersecurity-for-small-businesses-76259.

[21] *See Understanding and Dealing with Phishing During the Covid-19 Pandemic*, ENISA (May 6, 2020), https://www.enisa.europa.eu/news/enisa-news/understanding-and-dealing-with-phishing-during-the-covid-19-pandemic.

[22] *See* Steve Grobman, *Adjusting to the New Security Realities of a Remote Workforce*, CYBER SCOOP (May 27, 2020), https://www.cyberscoop.com/steve-grobman-new-cybersecurity-realities-remote-workforce/.

understand their vulnerabilities, including network traffic analysis using deep packet inspection.[23]

2. Be Organized

Protecting an organizations' physical infrastructure is only the first step in safeguarding its assets; in many ways, digital assets and information is increasingly the lifeblood of both government entities and private firms. One example of this fact is the extent to which the intangible assets comprising the S&P 500 flipped from the 1970s to 2018, at which point intangibles such as intellectual property and reputation comprised 84% of corporate value.[24] Organization is vital to protect such invaluable digital assets, yet even a computer that is "air gapped," or unplugged from the public Internet may still be accessible via flash drive or rewritable CD introduced by an insider threat. Large companies like Sony did not even have a Chief Information Security Officer until relatively recently. It hired one in the aftermath of its 2011 breach, but that did not save them from being breached again in 2014.[25] As is explored below in the Results section, still in 2020 both leadership structures and accountability remains muddy in too many organizations across Indiana.

3. Be Proactive

In general, the best cyber defense is a healthy skepticism and proactive vigilance backed up by a robust program of cyber hygiene and an updated incident response plan. Employees who do not have appropriate cybersecurity skills can unintentionally create vulnerabilities in a network. For example, it has been reported that 91% of cyber-attacks start with a phishing email – an issue that may be addressable by training.[26] Network security policies ensure that employees have access to the correct and appropriate information, and play a key role in preventing breaches from occurring. However, designing security policies to strike the correct balance between security and convenience is not an easy undertaking. For example, consider the difficulty of monitoring employees who are working remotely. One study found that 78% of IT specialists reported that their end users had set up unapproved services and applications, which increased

---

[23] *See* Duncan Geere, *How Deep Packet Inspection Works*, WIRED (Apr. 27, 2012), https://www.wired.co.uk/article/how-deep-packet-inspection-works. SaaS-based web gateway architecture has also been a proposed solution that can provide essential security controls to safeguard users visiting websites. In addition to protecting businesses from incoming threats and outgoing information exfiltration, it also allows organizations to apply similar corporate internet access policies to the increasing number of remote workers due to the COVID-19 pandemic.

[24] *See* Bruce Berman, *$21 Trillion in U.S. Intangible Assets is 84% of S&P 500 Value*, IP CLOSE UP (June 4, 2019), https://ipcloseup.com/2019/06/04/21-trillion-in-u-s-intangible-asset-value-is-84-of-sp-500-value-ip-rights-and-reputation-included/.

[25] *See* John Gaudiosi, *Why Sony Didn't Learn From its 2011 Hack*, FORTUNE (Dec. 24, 2014), https://fortune.com/2014/12/24/why-sony-didnt-learn-from-its-2011-hack/.

[26] *91% of Cyber Attacks Start with a Phishing Email: Here's How to Protect Against Phishing*, DIGITAL GUARDIAN (July 26, 2017), https://digitalguardian.com/blog/91-percent-cyber-attacks-start-phishing-email-heres-how-protect-against-phishing.

the chance of a potential unmanaged risk.[27] Hiring qualified cybersecurity personnel is another source of concern, as demonstrated by the fact that there are currently more than 3.5 million unfilled cybersecurity jobs.[28] In general, it is essential that organizations have resources and tools in place that allow them to adhere to and manage security policies. Anything that forces people to drastically change the way they work or results in an organization's lack of agility is counterproductive. An ideal solution should offer increased security entwined with business agility, which is an arena where cyber risk insurance can help.

C. Current Trends in Addressing Cyber Risk

Cyber risk evolves as quickly as the technology, social context, and policies underlying information systems. Although this evolution occurs in myriad ways, in this section we focus on three of the most prominent issues in cyber risk management today: the continuing importance of cyber risk insurance, the emergence of Artificial Intelligence (AI) as a tool for identifying and responding to cyber incidents, and the impact of the COVID-19 pandemic on technology practices and risks.

1. Cyber Risk Insurance

Cyber risk insurance has long been thought of as an integral component to managing cyber risk. Insurance firms have been experimenting with cyber risk insurance policies for decades.[29] By some estimates the market is worth more than $2.5 billion in 2020, with projections that it could triple by 2030,[30] a trend that could be reinforced by regulatory developments such as the California Consumer Privacy Act (CCPA) or the EU's General Data Protection Regulation (GDPR).[31] Indeed, U.S. companies are increasingly eyeing cyber insurance as they potentially face millions of dollars in liability under CCPA, under which state residents can seek up to $750

[27] *See The 2020 State of IT*, Spiceworks, https://www.spiceworks.com/marketing/state-of-it/report/ (last visited Aug. 10, 2020).

[28] *See The Dearth of Skilled. Cybersecurity Personnel*, SC MAG. (Jan. 23, 2020), https://www.scmagazine.com/home/advertise/the-dearth-of-skilled-cybersecurity-personnel/. In the absence of trained personnel, network security operations can turn to policy-based automation to reduce incomprehensibility, improve visibility, and focus resources on more complex tasks to improve operational efficiencies that directly impact the upshot of the business.

[29] Jon Swartz, *Firms' Hacking-Related Insurance Costs Soar*, USA TODAY (Feb. 9, 2003), http://usatoday30.usatoday.com/tech/news/computersecurity/2003-02-09-hacker_x.htm.

[30] *Insurance 2020 & Beyond: Reaping the Dividends of Cyber Resilience*, PWC (2020), https://www.pwc.com/gx/en/industries/financial-services/publications/insurance-2020-cyber.html.

[31] *See* Carolyn Cohn, *Europe's New Data Privacy Law Boosts Cyber Insurance Sales*, INSURANCE J. (May 22, 2018), https://www.insurancejournal.com/news/international/2018/05/22/489977.htm ("Insurers say the directive, together with major cyber attacks like last year's WannaCry and NotPetya viruses, is driving demand in Europe for cyber insurance – a sector seen as relatively profitable.").

per data security incident. The CCPA also directs the California Attorney General to take enforcement actions for privacy violations.[32]

In addition to protecting organizations against financial fallout from cyber incidents, organizations can use cyber risk insurance to inform their security practices in other ways. For example, insurers can use tactics like cyber-meteorology to audit companies against cyber risks and help them prioritize their security efforts.[33] The insurance industry has also focused extensively on their own cybersecurity practices. Model laws like the National Association of Insurance Commissioners (NAIC) Insurance Data Security Model Law seek to establish data security standards for regulators and insurers in order to mitigate the potential damage of future data breaches. This Model Law, which has been enacted in at least 11 states as of September 2020, requires insurers and other entities licensed by a state department of insurance to develop, implement, and maintain an information security program based on a recognized risk assessment tool, with a designated employee in charge of the information security program. The model does not create a private cause of action, nor does it limit an already-existing private right of action. As such, it is less a new approach to regulating cyber risk insurance than an encouragement for covered insurance providers to adopt an approved set of cybersecurity tools and frameworks.

However, with 49 states still not mandating cyber insurance, adoption has been slow. Deloitte's 2019 Middle Market Cyber Insurance Survey reported cost and coverage limits being the main deterrent from purchasing cyber risk insurance.[34] However, much is still unknown about how companies decide whether to adopt cyber risk insurance, and the broader role that cyber risk insurance plays in cyber risk mitigation practices, which is a key topic on which this survey focuses.

Moreover, cyber risk insurance does not protect companies against all types of cyber risks. The full impact of some potential risks may be difficult to quantify and thus difficult to fully insure. Insurance policies may exclude coverage of incidents that happen under certain circumstances, such as a cyber-attack that is attributed back to a foreign nation that may be defined as an act of war. Businesses must carefully review policies to ensure that their expectations about what types of incidents are covered aligns with their policies, which can create barriers to adopting policies.

2. Artificial Intelligence

Artificial intelligence (AI) has been sought as the next frontier for protection against cyber threats with some organizations predicting AI-powered technologies to triple by 2021.[35] An

---

[32] *See* Daniel R. Stoller, *Cyber Insurance Purchases Will Surge With California Privacy Law*, BLOOMBERG L. (Feb. 5, 2020), https://news.bloomberglaw.com/privacy-and-data-security/cyber-insurance-purchases-will-surge-with-california-privacy-law.

[33] *See* Vishaal Hariprasad, *Introducing 'Cyber Meteorology:' A New Strategy for Cyber Insurance*, DARK READING (Feb. 3, 2020), https://www.darkreading.com/risk/introducing-cyber-meteorology-a-new-strategy-for-cyber-insurance-/d/d-id/1336924.

[34] Julie Bernard, *Overcoming Challenges to Cyber Insurance Growth*, DELOITTE (Mar. 16, 2020), https://www2.deloitte.com/us/en/insights/industry/financial-services/cyber-insurance-market-growth.html.

[35] *The 2020 State of IT*, *supra* note 27.

automated, zero-time prevention platform can reduce the array of duties typically carried out by a cybersecurity team, which helps mitigate the prevailing cybersecurity workforce shortage, though no piece of software however advanced can replace a well-trained and well-rounded cybersecurity professional. Automated systems can, though, create alerts about anomalous activities that need to be investigated by human analysts, which can turn out to be benign. Moreover, as new threats arise, security solutions that use artificial intelligence must be re-trained to keep up.[36] Deep learning prediction models can produce a far lower level of false positives than traditional AI systems, which typically experience an approximately 1% false positive rate.[37] It is designed to automatically identify the relevant features of a malicious file or vector without engineering from a cybersecurity expert.

3. Cybersecurity During the Pandemic

CIOs and CISOs have been under intense pressure to meet the needs of homebound workers, while concurrently needing to take added steps to safeguard their enterprise networks. Organizations recognize the new risks associated with new types of employees working from home that have not done so prior to the pandemic. Mitigating the risks of a remote workforce largely comes down to ensuring the business is using the right security and that IT leaders are educating their employees on best practices around security as we navigate this crisis.

From an organizational standpoint, it is now more critical than ever to have the right technology in place and to make sure equipment is up to date and secure. It is also crucial for remote employees to exercise good cyber-hygiene. Organizations attempting to decide how to change their cybersecurity practices in light of COVID-19-related changed to work practices may find it helpful to consult decision-making frameworks such as the NIST Cybersecurity Framework or the Indiana University Center for Applied Cybersecurity Research Information Security Practice Principles.

COVID-19 may also change the planned use of cyber risk insurance, potentially for many years to come. The Cowbell Economic Impact of Cyber Insurance reported 65% of small and mid-Size Enterprises in the U.S plan to spend more on cybersecurity insurance over the next two years. More than half believe the cost of insurance is well worth the protection, on average, firms opt for cybersecurity insurance coverage limits of about 0.14% of revenue. By comparison, only 58% of large US-based enterprises plan to spend more on cyber-insurance over the next two years.[38]

---

[36] *Id*.

[37] *See* Abhimanyu S. Ahuja, *The Impact of Artificial Intelligence in Medicine on the Future Role of the Physician*, PEERJ (2019), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6779111/.

[38] *See Survey Results: The Economic Impact of Cyber Insurance*, COWBELL (June 2020), https://cowbell.insure/wp-content/uploads/2020/06/Cowbell-Cyber-data-report.pdf.

Methods

A. Aims of this Study

Given the multifaceted cyber threat landscape and the universality of cyber risk concerns to organizations today, it is to be expected that organizations will adopt different approaches to protecting their information and computer systems. These approaches will frequently be difficult to observe without querying organizations directly, as the steps an organization takes to buttress their cybersecurity postures may not be obvious from the outside. However, policymakers, analysts, and organizations themselves can benefit from a clearer description of this decision-making process. Better identification of the factors that organizations consider when making cybersecurity decisions can help policymakers develop incentives to promote decisions that protect consumers – and identify barriers to good decision-making. Analysts can conduct evaluations of cybersecurity policies in order to help identify which policies can be supported by empirical evidence. Organizations may benefit by better understanding the cybersecurity decision-making of their peers, as this may help them identify the standards of their industry.

In order to contribute to our current understanding of cybersecurity decision-making, we conducted a survey of Indiana organizations to query them about their perceptions of cyber risk, how their organization manages these risks, and the role of cyber risk insurance in this decision-making process. The content and distribution of this survey are described in the remainder of this section; the next section presents a summary of key results.

B. Survey Development and Distribution

We began this study by consulting with a variety of stakeholders on both the general topics that should be addressed by a cyber risk survey, and any specific questions that they would think it necessary to include. We focused in particular on questions that would elicit information that would be most likely to be useful to cybersecurity decision-makers on both the governmental and organizational levels. Through this process, we identified several key topics to focus on, namely cyber risk perceptions, cyber risk management and planning, and cyber risk insurance use/non-use. We drafted questions to address each of these decision-making dimensions. These questions were then vetted for both completeness and clarity by cybersecurity analysts and stakeholders in order to maximize the likelihood that we would obtain useful information and ensure that would be understandable to potential respondents. The finished survey protocol is provided in Appendix B.

This survey was distributed in partnership with the Indiana Executive Cybersecurity Council and the Indiana Business Research Center. A solicitation and link to the survey was sent to an extensive mailing list of more than 3,000 public and private organizations in Indiana. We received 336 responses, including 197 complete responses and 139 incomplete responses. Incomplete responses were dropped for analysis. This left us with an overall response rate of 6%.

Figure 3 below describes the number of employees and geographic scope of respondent organizations. As can be seen, respondents represented a range of organizational sizes, but most commonly reported that their organization employed 1-10 people. Similarly, respondents most commonly reported that their organization was local in geographic scope by a wide margin (82%, N=162).

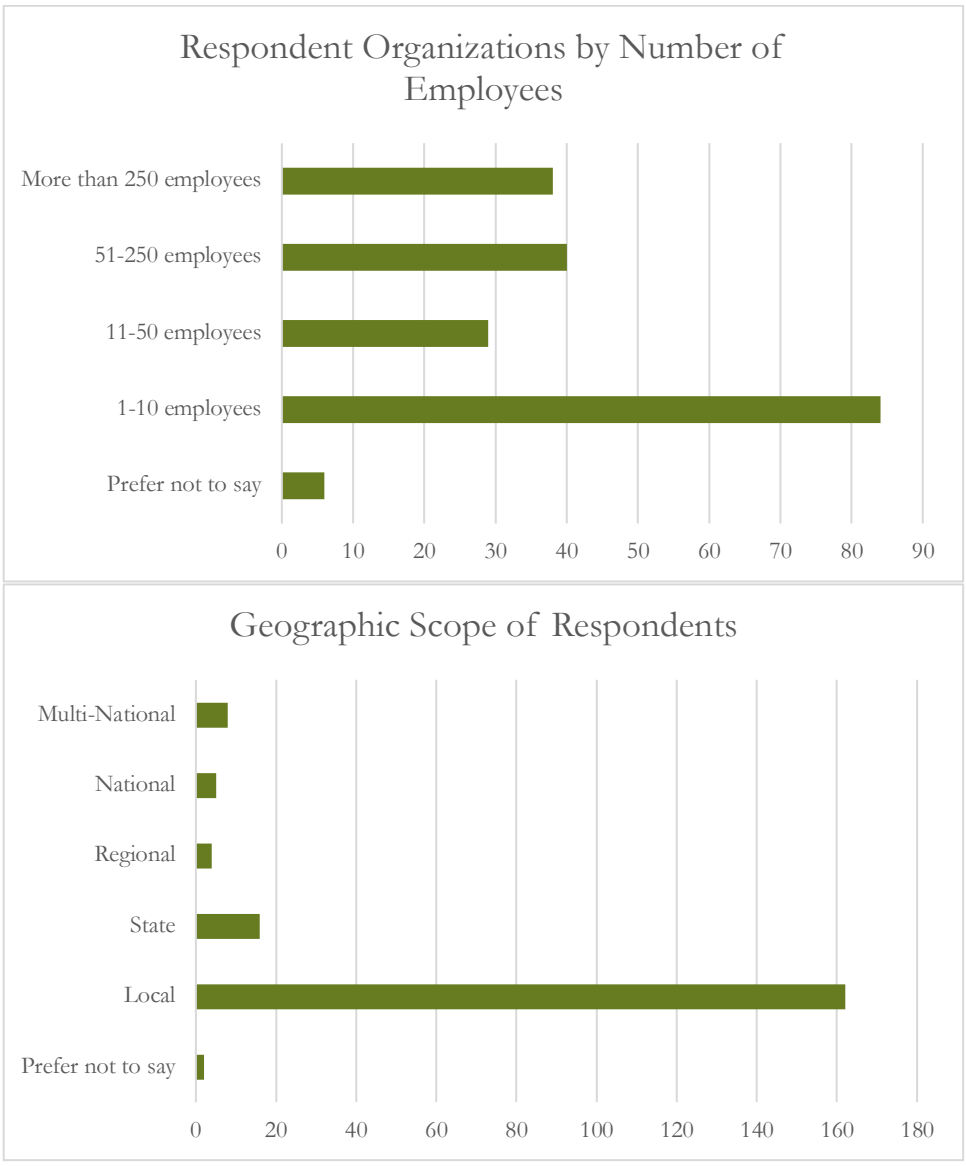


Figure 3: Description of Respondent Organizations

As there are particular concerns about cybersecurity decision-making amongst organizations that comprise critical national infrastructure, respondents were also asked whether their organization fell within one of these categories. As is shown in Figure 4 below, about 58% of respondents indicated that their organization fell within a critical infrastructure sector. In particular, about 36% of respondents reported that their organization fell within the Government Facilities Sector.

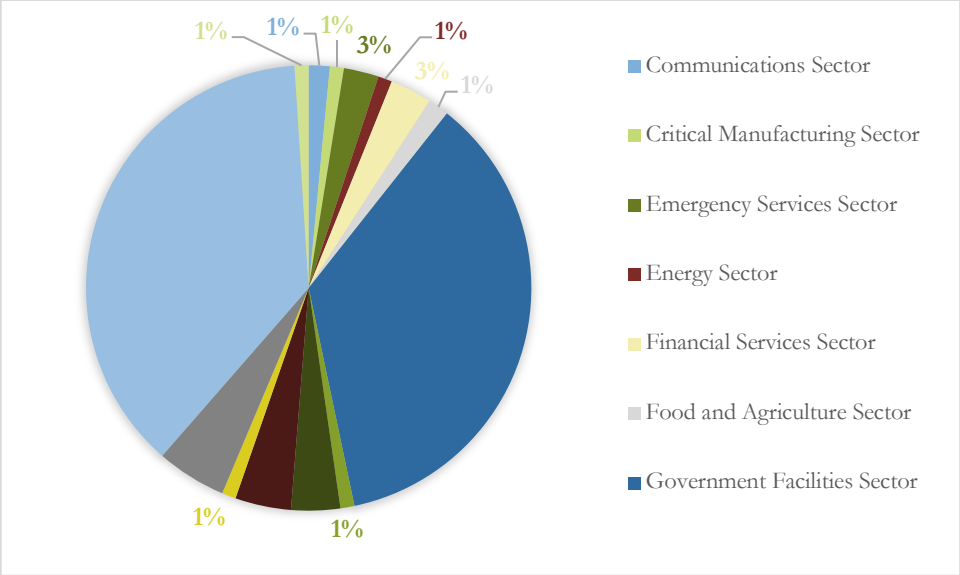


Figure 4: Respondents by Critical Infrastructure Sector

C. Limitations

There are several key limitations to this analysis. It may be that cybersecurity decision-making amongst organizations that chose to respond to this survey may be different from those organizations that did not chose to respond. In particular, representatives from organizations that are more concerned about cybersecurity decision-making may be more likely to respond to the survey, as the issues it raises are more salient to them and their employers. Combined with the relatively low response rate of the survey, this suggests that the results of this analysis should not be seen as representing the exact parameters of cybersecurity decision-making in general. Rather, it should be seen as an exploratory effort to understand the range of factors that might contribute to cybersecurity decision-making in Indiana. Additionally, responses to the survey will be influenced by how respondents interpreted the questions, as well as the scope of their knowledge of their organization's cybersecurity practices and their recollection of these practices. Future, more in-depth qualitative research with organizations could provide additional details and insights that would refine the insights from this paper.

Nevertheless, this analysis can provide key insights to inform cybersecurity policymaking in Indiana today. It provides a description of mechanisms used by organizations to protect their information and mitigate potential attacks, which can be used to identify practices currently employed by organizations in the state. It explores the reasons why these practices have not been adopted, which can provide insights about barriers that governmental organizations may seek to address.

Results

In this section, we summarize and discuss the responses provided by the Indiana organizations that participated in our survey. We focus specifically on describing cyber risk perceptions, planning, and responses. When possible we contextualize these responses with reference to other sources of data.

A. Risk Perceptions & Experiences

1. Potential Events & Consequences

The Indiana organizations who responded to this survey generally expressed concern about the risk of a cyber incident. Almost 49% identified as very concerned and over 46% of respondents identified as somewhat concerned about the risk of a cyber incident, while less than 5% of respondents indicated that they were not at all concerned about the risk of a cyber incident. As shown in Figure 5 below, when asked about the specific types of cyber incidents they were concerned about, respondents most frequently indicated concern about malware attacks (86% of respondents), phishing attacks (76% of respondents), and ransomware attacks (74% of respondents). Of those respondents who indicated that they were concerned about another type of cyber incident, the types of incidents they described included zero-day exploits, attacks through third party vendors, and an attack that resulted in the release of client/patron information.

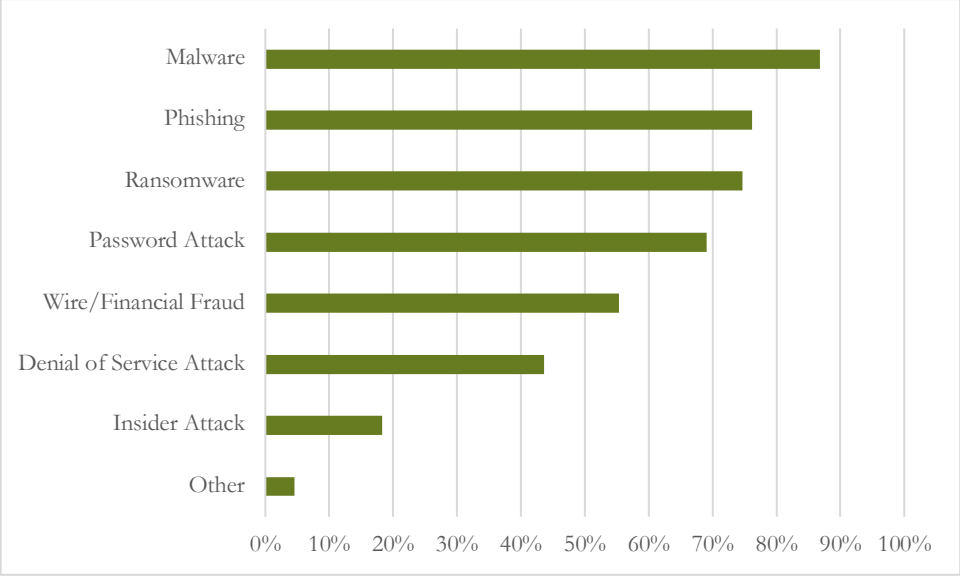


Figure 5: Proportion of Respondents Concerned About Cyber Incidents, By Type

Respondents were also asked to rank the types of cyber incidents they were concerned about in order of how concerned they were. Ransomware attacks were most commonly ranked as the highest concern amongst respondents who provided an answer to this question, while phishing attacks and malware attacks were ranked second and third respectively. Notably, respondents least frequently ranked insider attacks and other types of attacks as their highest source of concern, despite the overall prevalence of these issues.

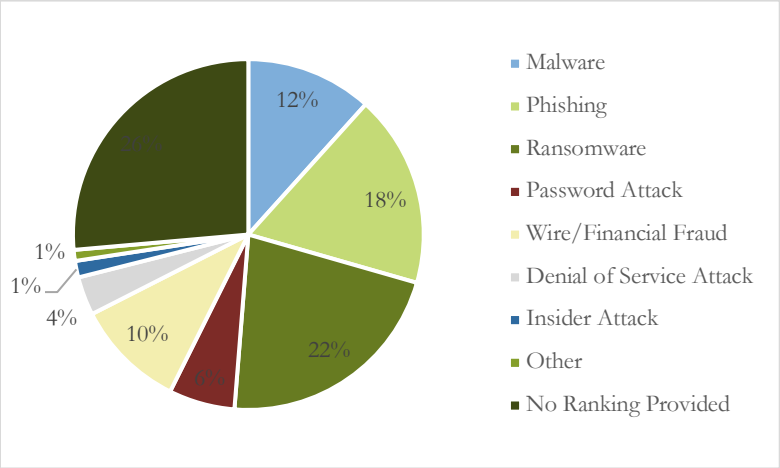


Figure 6: Proportion of Respondents Most Concerned About Each Type of Cyber Incident

In order to situate these results, we can compare them with data on data breaches reported to the Indiana Attorney General's office pursuant to Indiana's data breach notification statute in 2018 and 2019.[39] According to these data, the majority of data breaches reported to the Indiana Attorney General were caused by an external cause, as is shown in Figure 7 below.[40] The next most common cause of a reported data breach – inadvertent disclosure – occurred about a third as often as an external system breach. Reported data breaches were attributed to insider wrong-doing in about 6% of reported data breach. These results roughly align with concerns expressed by our respondents, who both most frequently mentioned external causes of cyber incidents such as malware and phishing attacks as potential sources of concern and ranked these external causes of cyber incidents as their sources of greatest concern.

[39] Ind. Code. Ann. § 24-4.9.

[40] The data used in this figure were obtained from public records of Notice of Security Breach Reports for Indiana. Simplified published versions of these reports are available at Indiana Attorney General, *Identity Theft Protection*, https://www.in.gov/attorneygeneral/2874.htm (last visited Oct. 29, 2020).

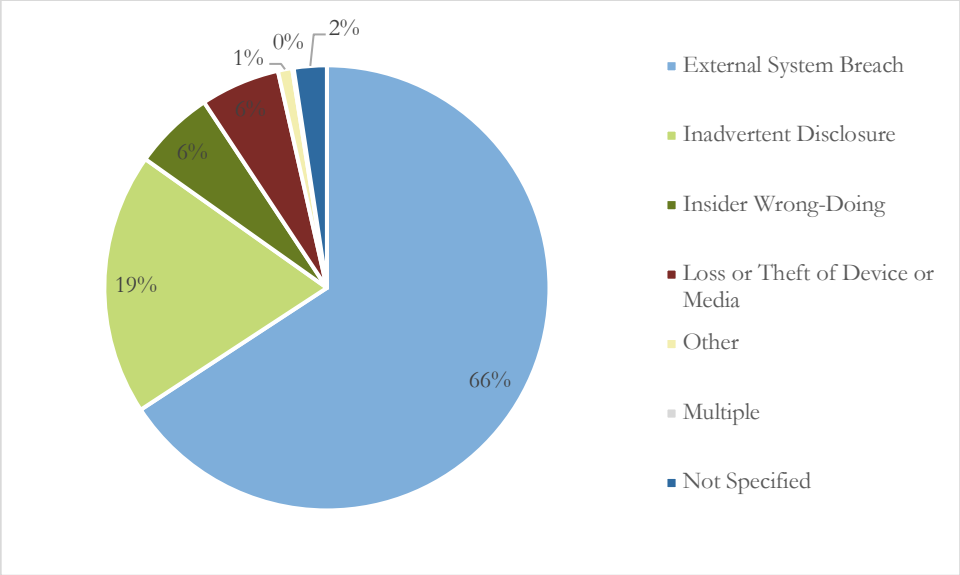


Figure 7: Causes of Data Breaches Reported to the Indiana Attorney General

Respondents were then asked about their concerns regarding the potential consequences of a cyber incident. As is shown in Figure 8 below, respondents most frequently indicated that they were concerned about data being deleted or lost (78% of respondents), data or information being exposed to outsiders (65% of respondents), and identity theft (64% of respondents). Interestingly, only a small proportion of respondents indicated that they were concerned with other potential consequences of a cyber incident. These respondents specifically indicated that they were concerned about personally identifying information being used against their stakeholders, and the loss of resources and staff time incurred in the course of responding to the incident.

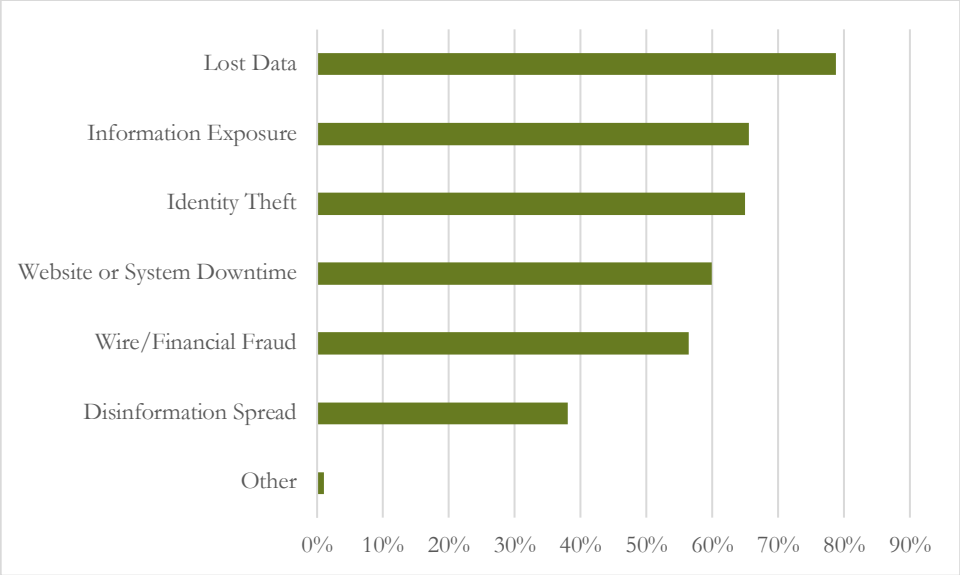


Figure 8: Proportion of Respondents Concerned About Consequences of Cyber Incidents, By Type

Respondents were again asked to rank the potential consequences of cyber incidents based on their level of concern. Of those who provided an answer to this question, respondents most frequently indicated that they were most concerned about data being deleted or lost (22% of respondents), data being exposed to outsiders (16% of respondents), and wire/financial fraud (11% of respondents).

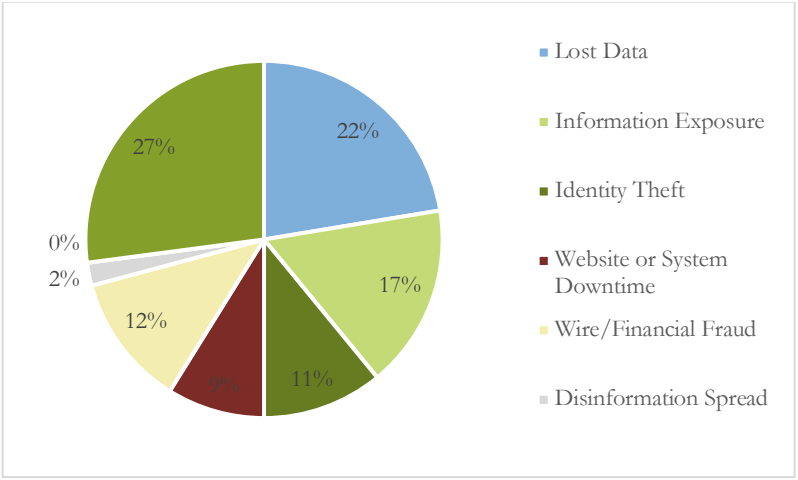


Figure 9: Proportion of Respondents Most Concerned About Consequence of Cyber Incident

2. Previous Events and Responses

In order to understand Indiana organizations' previous experiences with and responses to cyber incidents, respondents were asked whether their organization had experienced a successful cyber incident in the past three years. Approximately 19% (N=38) of respondents indicated that they had experienced a successful cyber incident during this time frame, while 67% (N=132) of respondents indicated that their organization did not experience a successful cyber incident and 13% (N=25) were either not sure or declined to provide an answer. Of respondents who indicated that their organization had experienced a successful cyber incident in the past three years, 50% indicated that none of these incidents resulted in data loss and 31% indicated that less than five of these incidents resulted in data loss. Respondents were then asked to describe the most recent incident experienced by their organization. As is shown in Figure 10 below, the most common types of cyber incidents experienced by respondents were phishing attacks and wire/financial fraud, while no respondents indicated that the most recent incident experienced by their organization was a DDoS attack.

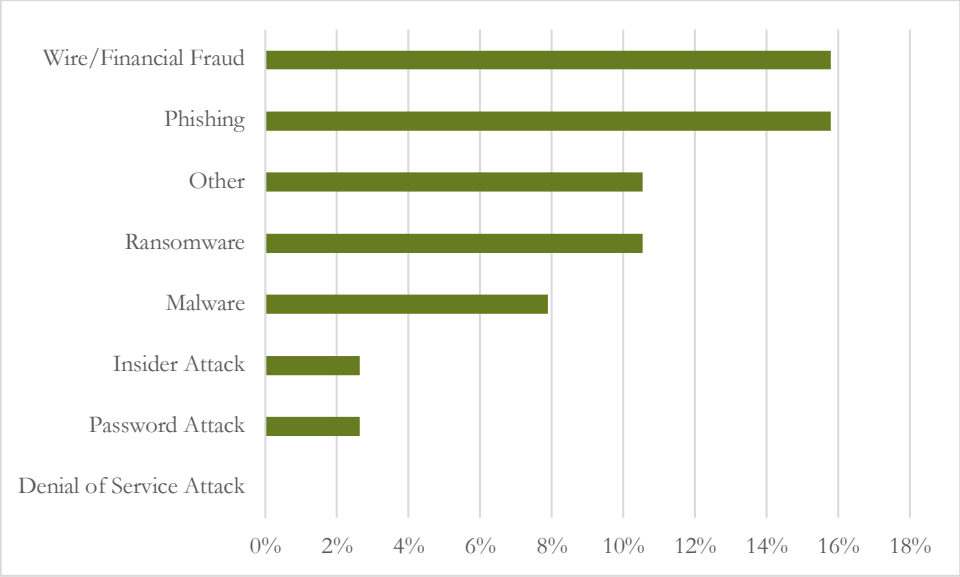


Figure 10: Types of Cyber Incidents Experienced by Respondents' Organizations

Respondents also described the consequences of the most recent cyber incident experienced by their organization; these results are summarized in Figure 11 below. Over 18% (N=7) respondents reported experiencing exposure of information to outsiders as a result of the cyber incident, while over 15% (N=6) reported wire/financial fraud as a result of the cyber incident.

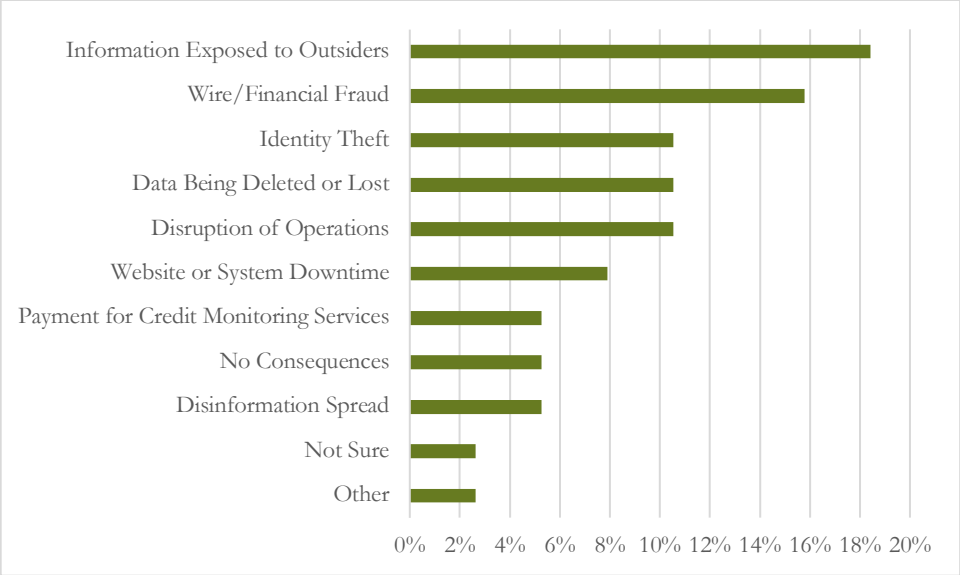


Figure 11: Consequences of Cyber Incidents Experienced by Respondents' Organizations

B. Managing Cyber Risk

1. Prevention and Mitigation of Cyber Incidents

Prevention is a key component of an effective cybersecurity strategy. The vast majority – over 82% – of respondents indicated that their organization had taken steps to prevent a cyber incident; over 7% indicated that their organization had *not* taken steps to prevent cyber incidents, and over 9% indicated that they were not sure. Of respondents who indicated that they had taken steps to prevent cyber incidents, there was a high degree of commonality in the mechanisms adopted. As shown in Figure 12 below, over 95% of respondents who indicated that they had taken steps to prevent cyber incidents installed antivirus software (N=155), while over 75% (N=126) indicated that they had updated/patched software and over 70% (N=114) provided their employees with training to reduce cyber-related risks. Seventeen respondents indicated that they had used mechanisms to prevent cyber incidents other than the options provided by the survey; these respondents described a broad range of alternative mechanisms including installing firewalls and spam filters, adopting multi-factor authentication, and hiring a cybersecurity firm to advise on defenses.

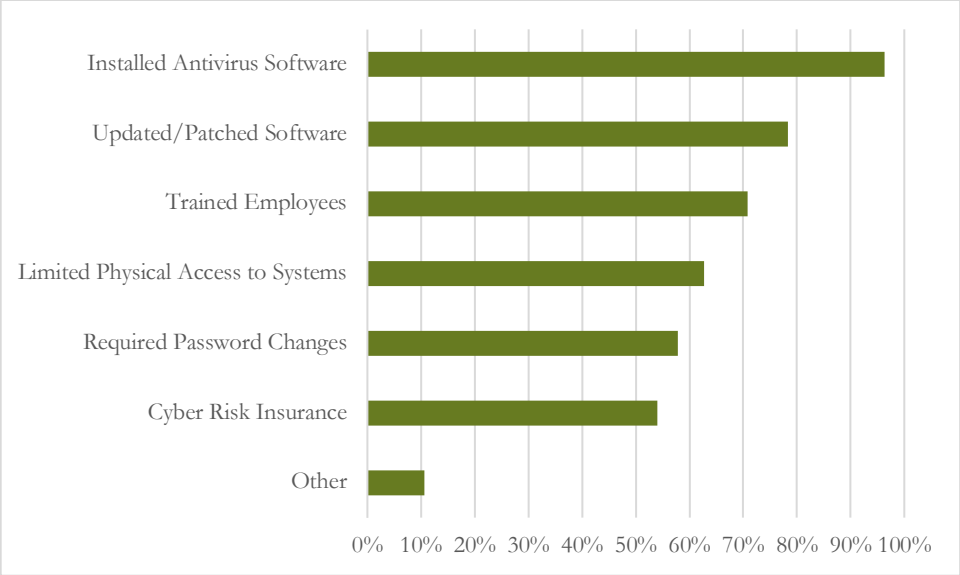


Figure 12: Mechanisms Used to Prevent Cyber Incidents

Respondents who indicated that their organization had not taken steps to prevent cyber incidents were then asked why these steps had not been taken. As shown in Figure 13 below, of those respondents who indicated that their organization had not taken steps to adopt cyber incident prevention mechanisms, slightly more than half (N=8) attributed this decision to the organization being unsure what to do, while 40% (N=6) explained that their organization did not think it was at risk. Twenty percent (N=3) indicated that their organization had reasons other than those provided by the survey for not adopting cyber risk prevention mechanisms; these respondents generally went on to explain that their organization was either too small to engage in prevention mechanisms or did not have their own equipment to protect. Perhaps most interestingly, no respondents indicated that their organization did not adopt cyber incident prevention mechanisms because they believed those mechanisms to be ineffective.

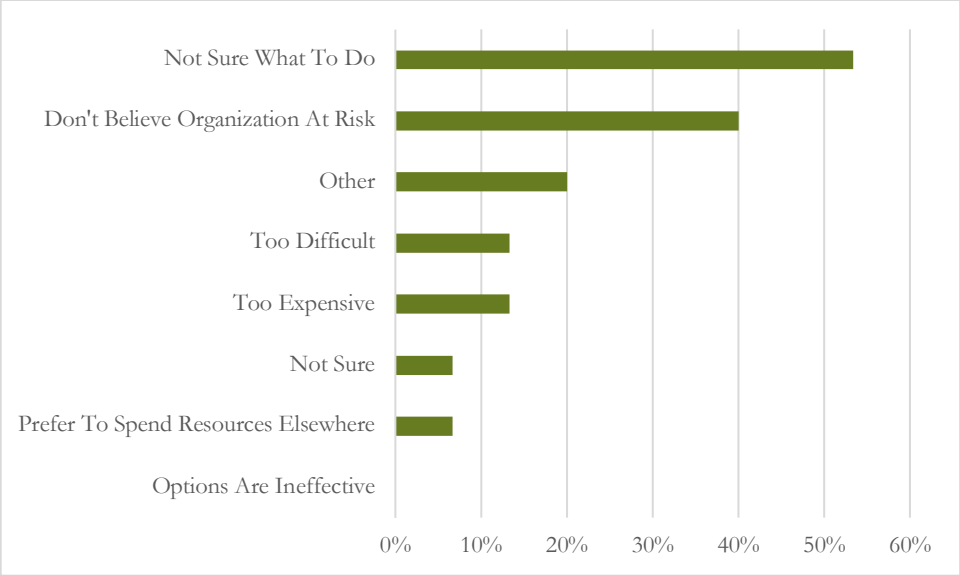


Figure 13: Reasons for Not Adopting Prevention Mechanisms

Almost 70% (N=134) respondents indicated that their organization had taken steps to mitigate the impact of a cyber incident, while about 11% (N=23) indicated that their organization had not taken these steps and about 19% (N=37) were not certain. Respondents who indicated that their organization had adopted mechanisms to mitigate cyber incidents were then asked what mitigation mechanisms their organization had undertaken. As is shown in Figure 14 below, almost 85% (N=113) of respondents indicated that their organization had installed automatic back-up systems, while approximately 60% (N=84) of respondents indicated that their organization had purchased cyber risk insurance. Almost 12% (N=16) of respondents described other cyber incident mitigation mechanisms undertaken by their organization; such mechanisms included upgrading hardware, strengthening firewalls, and testing their network or incident response plan.

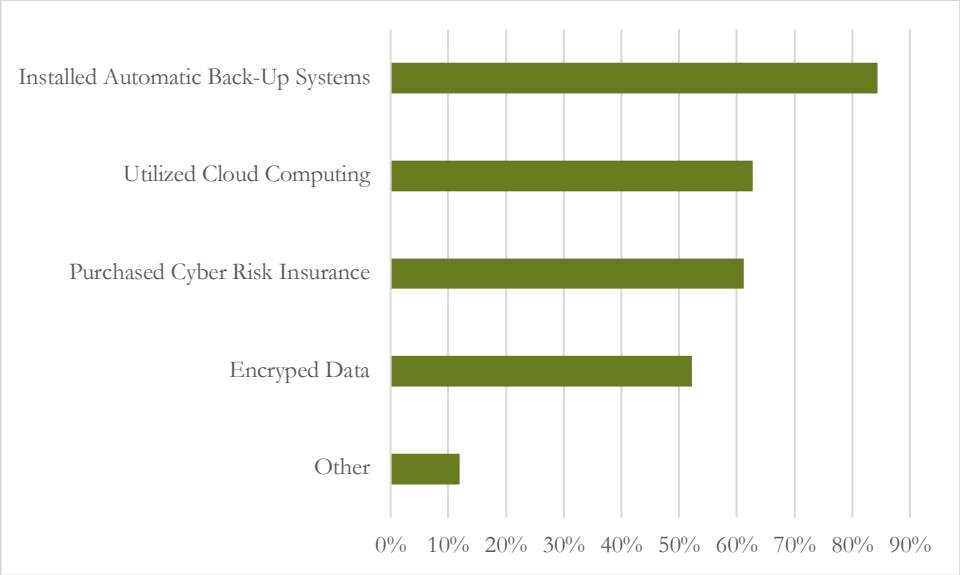


Figure 14: Mechanisms Used to Mitigate Cyber Incidents

Respondents who indicated that their organizations had not adopted mitigation measures were then asked why these measures had not been adopted. Respondents most commonly cited uncertainty about how to accomplish this as the reason their organization had not adopted mitigation mechanisms, with about 47% (N=11) respondents adopting this option. Twenty-six percent (N=6) of respondents indicated that their organization had not adopted mitigation mechanisms because they didn't believe themselves to be at risk. The approximately 17% (N=4) of respondents who characterized their organization as having other reasons for not adopting mitigation mechanisms elaborated that these reasons included not having technical infrastructure to secure or currently being at the stage of investigating mitigation options.

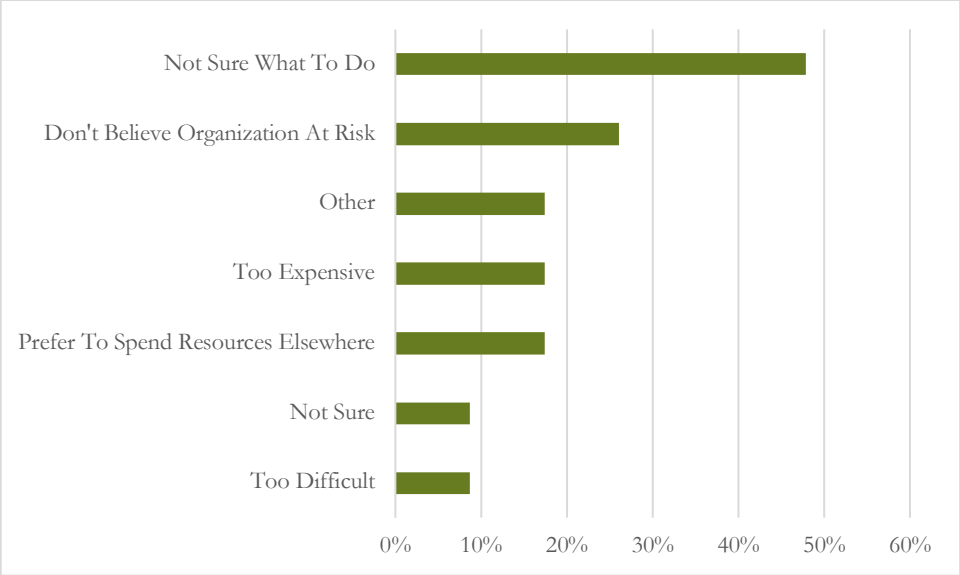


Figure 15: Reasons for Not Adopting Mitigation Mechanisms

2. Cybersecurity Practices, Personnel, and Training

In order to understand how Indiana organizations are protecting their systems and information, respondents were then asked whether their organization had adopted certain cybersecurity practices. As is shown in Figure 16 below, of the 178 respondents who answered the question, slightly less than half indicated that their organization had adopted automatic updating of operation systems and software (N=88) and implementation of remote backups (N=86). The next most commonly adopted practice was use of multi-factor authentication, which about a quarter of respondents had indicated that their organization had adopted.

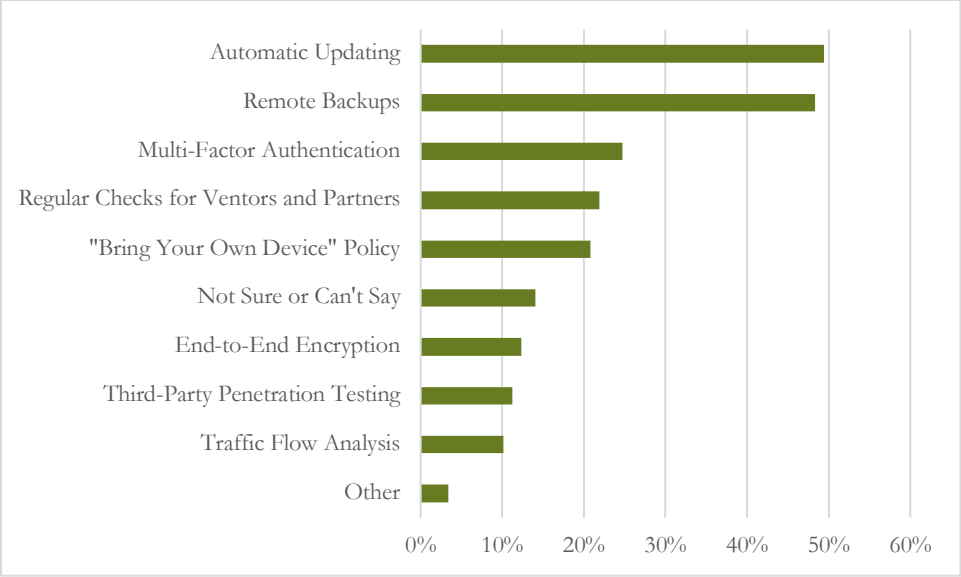


Figure 16: Cybersecurity Practices Adopted

The development and documentation of incident planning and response is a key cybersecurity practice. About 27% (N=55) of respondents reported that their organization had written cyber incident planning and response documentation, with more than half (N=109) indicating that their organization did not have such documentation and the remainder of respondents being uncertain or unresponsive. Respondents who indicated that their organization had written cyber incident planning and response documentation were then asked about their perceptions of the documentation. As shown in Figure 17 below, these perceptions were weakly positive on average, with respondents on average falling between “somewhat agree” and “neither agree or disagree” for all statements. However, there was a degree of polarization in these responses, with “strongly agree” being the most frequently occurring response to all statements.

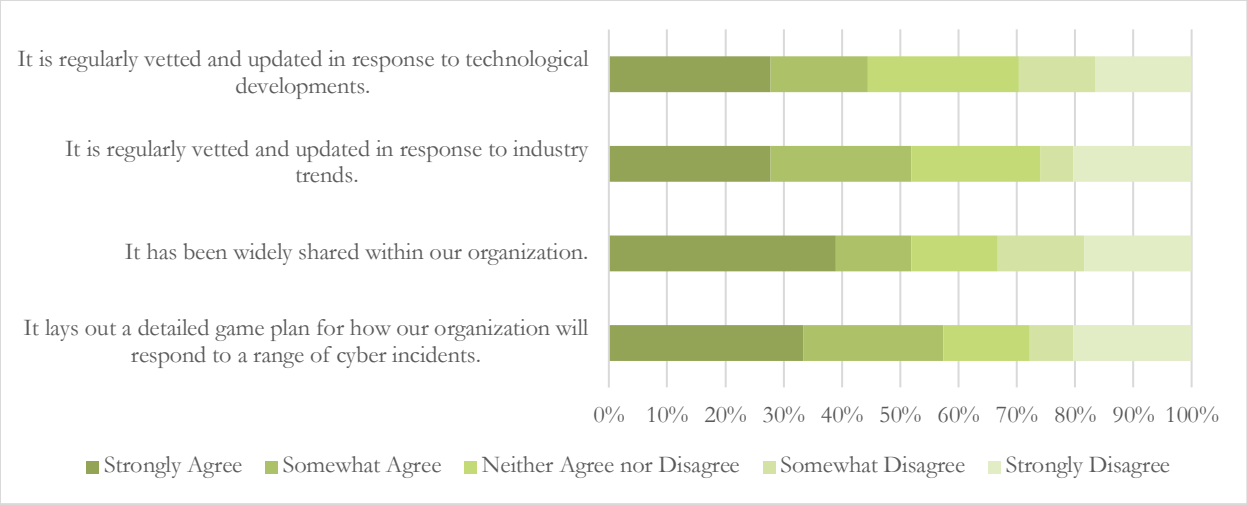


Figure 17: Perceptions of Cybersecurity Documentation

Cybersecurity response is also shaped by the people selected to lead this response. When asked who at their organization was ultimately responsible for managing cyber risk, about 15% (N=30) of respondents indicated this role was filled by their Chief Information Officer, and about 14% (N=28) indicated that this role was filled by their Chief Executive Officer. Interestingly, almost half of respondents elected to write in their own response to this question, with a common response being that this role was fulfilled by an information technology manager, director, or department (and several respondents indicating that no one served in this role). The heterogeneity of these responses suggests that many Indiana organizations seek guidance about corporate governance best practices to ensure that cybersecurity and data privacy are adequately integrated into organizational decision-making.

Respondents were also asked how many cybersecurity professionals were employed at their organization. Sixty-seven percent (N=133) indicated that their organization did not employ a cybersecurity professional, and 23% (N=47) indicated that their organization employed between 1 and 5 cybersecurity professionals. Additionally, as all employees can play a role in ensuring an organization's cybersecurity, respondents were asked about cybersecurity training practices at their organizations. While 58% (N=116) indicated that their organization had provided some employees with cyber risk awareness training, only 29% (N=58) of respondents stated that they themselves had received such training. A plurality of respondents who received such training (44%, N=25) stated that they received yearly training, while a smaller minority (32%, N=18) stated that their received training once a quarter.

3. Usefulness of Standards & Frameworks

A proactive approach to cybersecurity includes preemptively identifying security weaknesses and adding processes to identify threats before they occur. However, a plurality of respondents (37%, N=69) were not sure whether their organization was using specific tools to proactively manage cyber risk. Thirty-four percent (N=32) indicated that their organization had revised or

updated their incident response plan, while 32% (N=60) indicated that their organization had consulted news reports to proactively manage cyber risk. The 8% (N=16) of respondents who stated that their organization had taken other steps to proactively manage cyber risk described that these steps included having their computer system audited and hiring a consultant for monitoring.

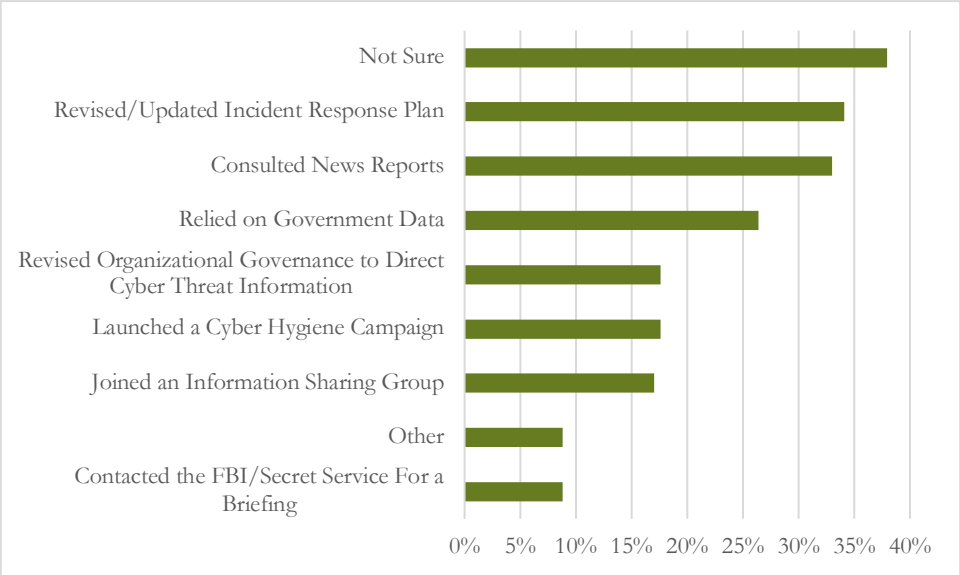


Figure 18: Tools Used to Proactively Manage Cyber Risk

Organizations concerned about their cybersecurity have a range of external tools and frameworks available to help guide their decision making in this area. Fifty-eight respondents (29%) stated that their organization consulted an externally developed tool, framework, or control when making decisions about cyber practices. Among respondents who indicated that their organization used an externally developed framework to guide their cybersecurity decision making, the most commonly used framework was the NIST Cybersecurity Framework, which had been adopted by 58% (N=34) of those organizations adopting a framework and 36% (N=21) had adopted the Center for Internet Security (CIS) Critical Security Controls.

C. Role of Cyber Risk Insurance

About half of respondents (N=98) indicated that their organization had cyber risk insurance; 26% (N=52) indicated that their organization did not have cyber risk insurance; remaining respondents (N=47) were either unsure or declined to answer. In this section, we explore how organizations with cyber risk insurance decided to obtain this insurance coverage, what is covered under these policies, and what is required by these policies.

1. Adoption of Cyber Insurance

Respondents with knowledge of when their organization had obtained cyber risk insurance most frequently indicated that this insurance had been obtained within the last five years, as indicated in Figure 19 below. Interestingly, one respondent indicated that their organization had obtained cyber risk insurance in 2001, almost a decade before any other respondent.

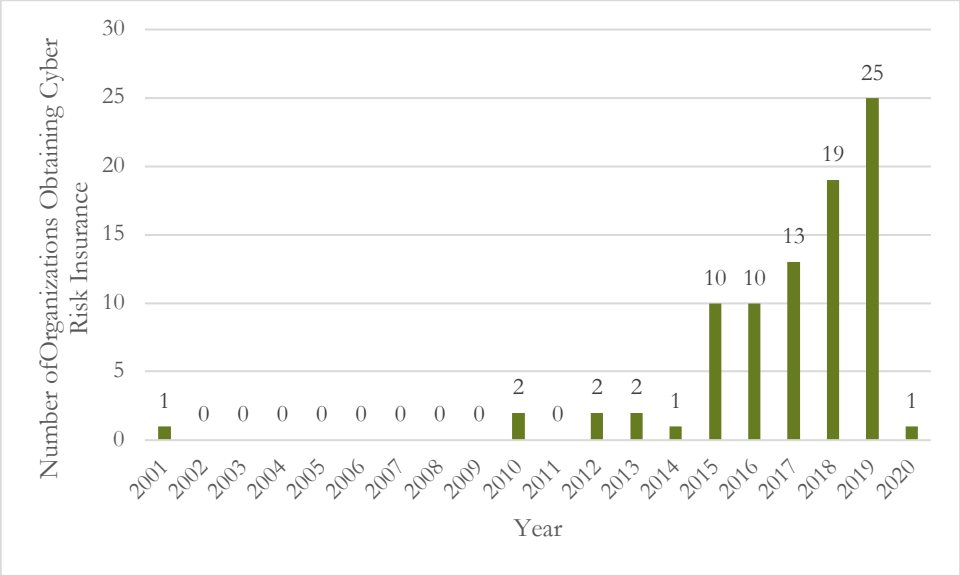


Figure 19: Year Cyber Risk Insurance Was Obtained

Respondents were then asked why their organization obtained a cyber risk insurance policy; the results of this question are described in Figure 20 below. Half of respondents (N=49) described the decision to obtain cyber risk insurance as a response to news reports on cyber incidents. A large minority (40%, N=40) of respondents provided another reason for obtaining cyber risk insurance. These reasons included insurance agent recommendations or inclusion of cyber coverage in a general policy,[41] response to cybersecurity trainings by trade organizations or other outside groups, and a perception that obtaining this insurance "just made business sense."

[41] As coverage provided under a general policy might be different than coverage provided under a cyber-specific insurance policy, these responses could raise concerns about an additional source of insurance policy variation amongst respondents. However, as only three respondents indicated that their organization obtained cyber insurance as part of a more general policy, these responses have probably not had an outsized influence on our overall analysis.

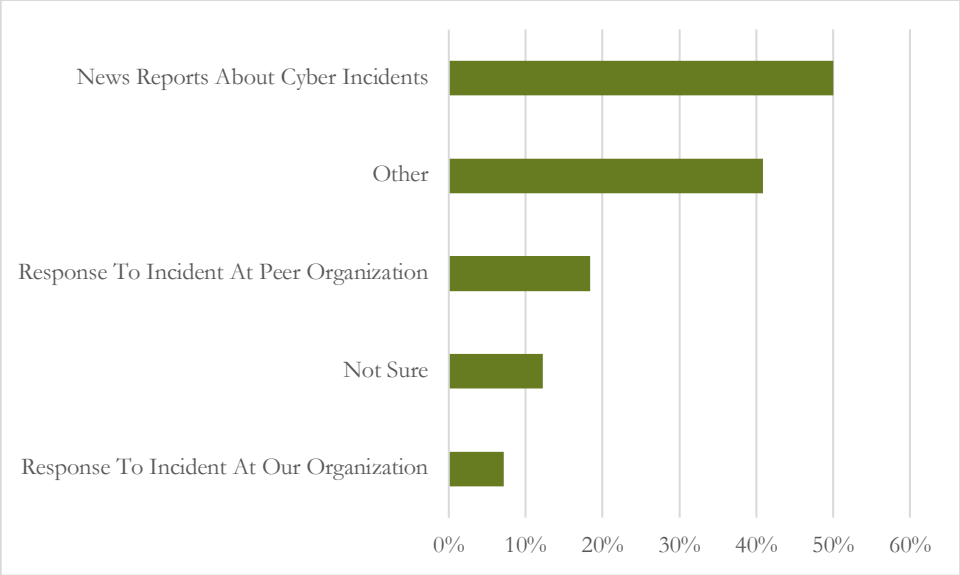


Figure 20: Reasons for Obtaining Cyber Risk Insurance

2. Cyber Insurance Coverage

Cyber insurance plans may offer coverage for incidents that occur under a variety of circumstances, and losses that occur to a variety of people and organizations. Insurance plans commonly cover first-party losses, which are losses that are incurred by the insured. Figure 21 below describes the first-party losses covered by respondent organizations' insurance plans. In particular, respondents whose organizations had cyber risk insurance most commonly reported that their organization's insurance policy covered losses due to damage to computers or information systems (54%, N=53), with a similar but slightly smaller number of respondents indicating that their organization's cyber insurance policy covered expenses related to responding to the breach (52%, N=51).

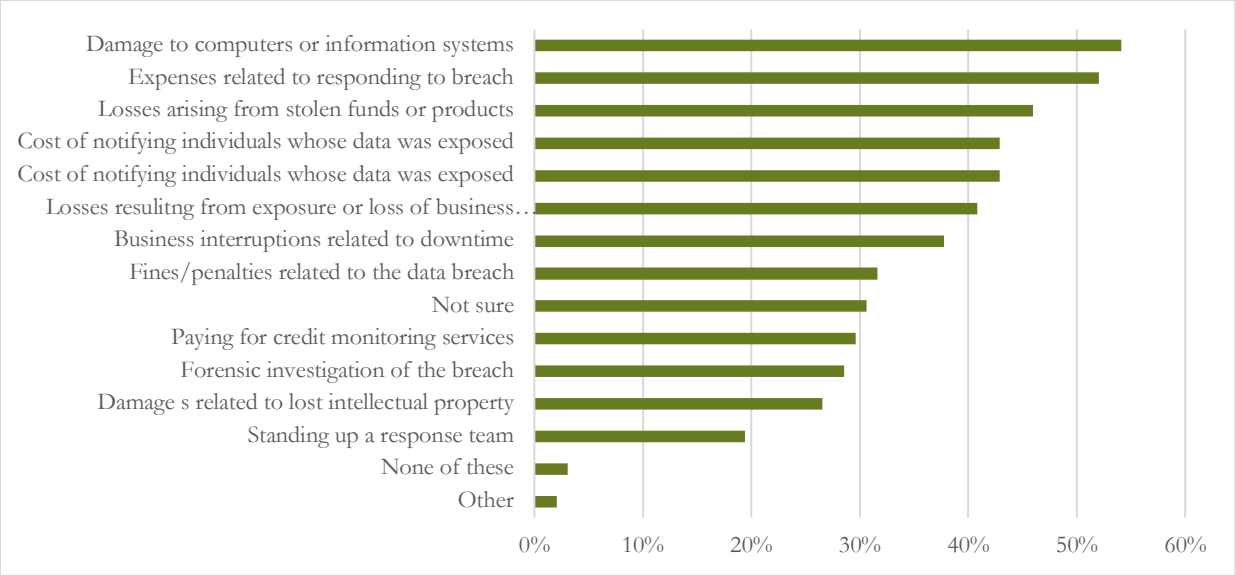


Figure 21: First Party Losses Covered Under Cyber Insurance

In addition to first party losses, cyber insurance plans may also cover third-party losses, which are losses incurred by other parties for which the insured party may nonetheless be liable. As is shown by Figure 22 below, respondents were less sure about the third-party losses covered under their organization's cyber insurance policy. However, about 33% (N=33) of respondents whose organizations have cyber risk insurance policies reported that this policy included costs for legal defenses related to the data breach, while about 26% (N=26) reported that this policy included coverage for claims for damages from those whose information was exposed by the incident.

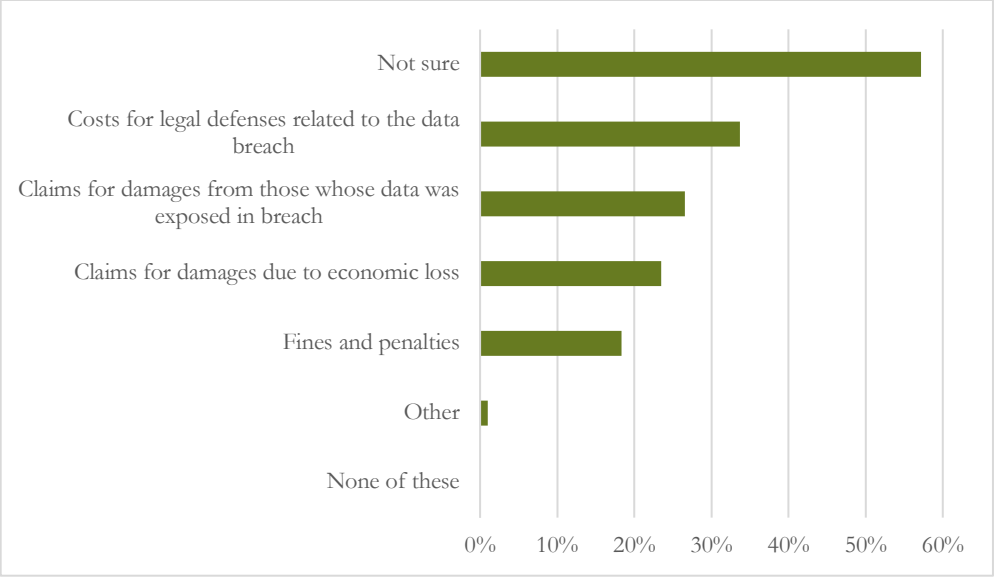


Figure 22: Third Party Losses Covered Under Cyber Insurance

Over 60% (N=59) of respondents with cyber insurance policies reported that these policies included a limit on coverage; the remainder were largely unsure as whether their policy included such a limit. Out of the 35 respondents who reported the amount of their coverage limit, the most commonly reported limit was $1 million; however, some respondents reported a coverage limit in the hundreds of millions of dollars. In addition to limitations on coverage amount, insurers may also exclude certain categories of incidents from coverage under a policy. The majority of respondents who indicated that their organization had insurance coverage were unsure as to whether that insurance policy excluded coverage in certain circumstances, although almost 20% (N=18) of respondents whose organizations had cyber risk insurance reported that this policy had coverage exclusions. Of those respondents who were able to provide information about these exclusions, the most frequently cited reason for exclusion was acts of war or terrorism, with losses that occurred because the organization failed to provide and maintain adequate security.

3. Required Security Measures

As insurers bear risks associated with potential cyber incidents, it is common for cyber risk insurance policies to require the insured organization to undertake certain security practices. Of those respondents who indicated that their organization had a cyber risk insurance policy, 47% of them indicated that this policy required them to undertake certain security measures. As is shown in Figure 23 below, the most commonly required security practices were employee training and cyber hygiene, with about 40% (N=19) of those whose organizations were required to adopt security practices by their insurer indicating that these required practices included employee training. About 34% (N=16) indicated that their insurer required their organization to engage in mandatory, automatic patching of systems. Respondents who indicated that their insurer required other security measures were asked to describe these security measures.

Responses included the development of a cybersecurity plan and compliance with the Payment Card Industry Data Security Standard.

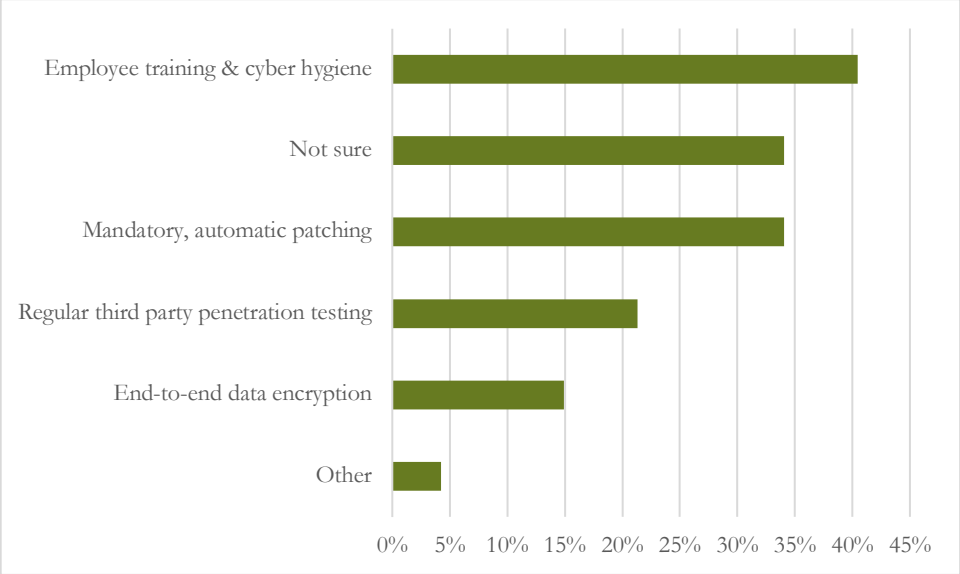


Figure 23: Security Measures Required by Respondents' Insurer

4. Non-Adoption of Cyber Risk Insurance

Policymakers and analysts interested in understanding cyber risk insurance decision-making can learn just as much from organizations that do not have cyber risk insurance as from those who do. Consequently, respondents whose organizations did not have a cyber risk insurance policy were asked whether their organization had ever considered obtaining a cyber risk insurance policy and, if so, why they did not decide to obtain such a policy. Almost half (48%; N=46) of respondents whose organizations did not have a cyber risk insurance policy indicated that their organization had never considered obtaining such a policy, while 38% (N=37) indicated that they were unsure. About 13% (N=12) indicated that their organization had considered obtaining such a policy and had decided against it. These respondents most commonly indicated that cost was a factor in the decision not to obtain cyber risk insurance, either because they believed it to be too expensive or their preferred to spend resources on other policies. One respondent who provided an additional reason that their organization had not adopted a cyber risk insurance policy indicated that their organization may have been "overwhelmed with what exactly we really needed to obtain."

Respondents who did not currently have cyber risk insurance were asked what would encourage their company to obtain a cyber risk insurance policy as an open-ended question. Responses unsurprisingly covered a range of potential factors. Many respondents described the cost of obtaining a policy as a significant factor, frequently mentioning affordability and the need for "a better value proposition." Other respondents indicated that their organization would be more likely to obtain cyber risk insurance if they perceived they were more at risk ("awareness of the treat and the damage that could result"), or if they obtained additional information about their

level of risk either through incidents at peer organizations or general statistics. Finally, some respondents indicated that their organizations were unlikely to ever obtain cyber risk insurance, generally due to the fact that they did not perceive that their organization was ever likely to be at risk.

Policy Opportunities

A. Awareness Training

As was made clear in our results, there is a clear need to help educate organizations about cybersecurity best practices with more than half of respondents being unsure of which techniques and tools to use to best mitigate the particular cyber risks they face. In particular, given concerns over malware, phishing, and ransomware, public-private training sessions would seemingly be well suited to focus on these issues in particular. Indiana has made strides in this regard such as through the Indiana Cybersecurity Hub,[42] and the Indiana Information Sharing and Analysis Center (IN-ISAC).[43] However, greater coordinated outreach by leveraging educational institutions, civil society groups, and law enforcement could address this lack of awareness potentially through a push to promote October as Cybersecurity Awareness Month. Senior leadership in particular, including boards of directors, should be a key area of focus given the diffusion of cybersecurity responsibilities and persistent lack of clarity about accountability at so many Indiana organizations.

A concrete idea that the Executive Council could consider to help address this clear need is by working with universities and community colleges across the state to create a cybersecurity curriculum that local and state leaders could access and would answer these questions, such as best practices for ransomware mitigation. The site could also include model incident response plans, explainers for cyber risk insurance coverage and common exclusions, and other tools. Relatedly, we would encourage a deeper partnership – perhaps in collaboration with regional economic development authorities, the IN-ISAC, and the Indiana Business Research Center – between state and local leaders on quarterly trainings on various cybersecurity hot topics such as ransomware and the need to enable multi-factor authentication, end-to-end encryption for sensitive databases, and BYOD policies.

B. Proactive Cybersecurity

As seen in the results to this survey, while many organizations (82% of respondents) have taken some steps to prevent a cyber incident mostly through investing in antivirus solutions and patching, it is not uncommon to maintain a reactive cybersecurity stance across Indiana organizations. Proactive cybersecurity is an amorphous field, comprising a wide range of active and passive measures that are often commonly, though not always accurately, referred to as "active defense." While "hacking back" is a lightning rod within this field,[44] it is just one data

[42] *See* Indiana Cybersecurity Hub, https://www.in.gov/cybersecurity/ (last visited Oct. 1, 2020).

[43] IN-ISAC, https://www.in.gov/cybersecurity/in-isac/ (last visited Oct. 1, 2020).

[44] *See, e.g.*, Carl Franzen, *Should US companies be allowed to hack China in revenge? New report says yes*, VERGE (May 22, 2013), http://www.theverge.com/2013/5/22/4356196/report-tells-congress-companies-should-hack-back [https://perma.cc/JX7X-FE7X]; *see also* Eric Chabrow, *The Case Against Hack-Back*, BANK INFO. SEC.

point in a larger and more dynamic movement, which includes technological, organizational, and legal best practices deep packet inspection to audits promoting defense-in-depth.[45] Such a "lean in" approach to cybersecurity is essential to help guard against the more reactive mindset that has long bedeviled the field of cybersecurity risk management.[46] There seems to be an opportunity to help educate Indiana organizations about the full range of proactive cybersecurity best practices available to them to help manage various cyber risks. This can include both spreading awareness of, and encouraging the uptake including through government procurement, of leading cybersecurity and privacy frameworks including from NIST. Although this was the dominant option selected by respondents, still more than 40% of Indiana participants are not utilizing it at present. The proposed 2020 IN Attorney General's cybersecurity rule, discussed next, would constitute such a nudge.[47]

C. Defining "Reasonable" Cybersecurity

On September 25, 2020 Indiana Attorney General Curtis Hill proposed a rule that would change the incident response process for Indiana organizations that have experienced a data breach. In brief, the proposal would make two main substantive revisions from the current structure: (1) impose a requirement for database owners to "create, implement and report a corrective action plan (CAP) to the Attorney General within thirty days" of the reported breach; and (2) establish "a 'safe harbor' for what constitutes 'reasonable measures' to safeguard personal information in Indiana."[48] Database owners are those persons or entities that "own or license computerized data that include personal information."[49] Under existing Indiana law, these owners should "implement and maintain reasonable procedures, including taking any appropriate corrective

---

(Jan. 6, 2015), http://www.bankinfosecurity.com/case-against-hack-back-a-7759 [https://perma.cc/9WXW-U7TK]; Tom Field, *To 'Hack Back' or Not?*, BANK INFO. SEC. (Feb. 27, 2013), http://www.bankinfosecurity.com/to-hack-back-or-not-a-5545 [https://perma.cc/7XUH-H8T9] (discussing, among other things, the likelihood of prosecution in the United States for engaging in hacking back).

[45] *See, e.g.*, Orla Cox, *Proactive Cybersecurity — Taking Control Away from Attackers*, SYMANTEC (Apr. 2, 2014), http://www.symantec.com/connect/blogs/proactive-cybersecurity-taking-control-away-attackers [https://perma.cc/3XM6-R369]; Michael A. Davis, *4 Steps for Proactive Cybersecurity*, INFO. WK. (Jan. 18, 2013), http://www.informationweek.com/government/cybersecurity/4-steps-for-proactive-cybersecurity/d/d-id/1108270 [https://perma.cc/8XYL-H3PN]; *Hackback? Claptrap! — An Active Defense Continuum for the Private Sector*, RSA CONF. (Feb. 27, 2014), http://www.rsaconference.com/events/us14/agenda/sessions/1146/hackback-claptrap-an-active-defense-continuum-for ("[A]ctive defense should be viewed as a diverse set of techniques along a spectrum of varying risk and legality.").

[46] MCAFEE, UNSECURED ECONOMIES: PROTECTING VITAL INFORMATION 6 (2009), https://www.cerias.purdue.edu/assets/pdf/mfe_unsec_econ_pr_rpt_fnl_online_012109.pdf [https://perma.cc/N6L4-KAML] (comparing cybersecurity investment rates across countries and concluding that "it appears that decision makers in many countries, particularly developed ones, are reactive rather than proactive").

[47] IN Attorney General Proposal Rule LSA Document # 20-366, https://www.workplaceprivacyreport.com/wp-content/uploads/sites/162/2020/09/IN-AG-Hill-Proposed-Regulations.pdf.

[48] *See* Joseph J. Lazzarotii, *Indiana AG Proposed Regulations Creating Corrective Action Plan Requirement and Cybersecurity Safe Harbor*, WORKPLACE PRIVACY REP. (Sept. 25, 2020), https://www.workplaceprivacyreport.com/2020/09/articles/data-breach-notification/indiana-ag-proposed-regulations-create-corrective-action-plan-requirement-and-safe-harbor/.

[49] *Id.*

action, to protect and safeguard from unlawful use or disclosure any personal information of Indiana residents collected or maintained by the data base owner."[50] As Attorney General Hill said in describing the proposal: "This rule would provide businesses a playbook on how to protect data, and would protect the businesses that follow the playbook. It's a win for both consumers and businesses."[51]

A key piece of this effort is specifying what 'reasonable' cybersecurity entails. To date, that varies across the more than one dozen states with such laws on the books. Under Californian law, for example, organizations are required to implement "reasonable security procedures and practices . . . to protect personal information from unauthorized, access, destruction, use, modification, or disclosure."[52] The California Attorney General's Office defined "reasonable" to include the following list of Center for Internet and Security controls as the *minimum* threshold, which include requiring multi-factor authentication, and end-to-end encryption on portable devices.

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Security Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
4. Continuous Vulnerability Assessment and Remediation
5. Controlled Use of Administrative Privileges
6. Maintenance, Monitoring, and Analysis of Audit Logs
7. Email and Web Browsing Protection
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capability
11. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
17. Security Skills Assessment and Appropriate Training to Fill Gaps
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

---

[50] *Id.*

[51] *Id.*

[52] Paul Otto & Brian Kennedy, "*Reasonable Security" Becomes Reasonably Clear to California Attorney General*, CHRONICLE OF DATA PROTECTION (Mar. 1, 2016), https://www.hldataprotection.com/2016/03/articles/cybersecurity-data-breaches/reasonable-security-becomes-reasonably-clear/.

Instead, the proposed Indiana rule mirrors the efforts from other Midwestern states including Ohio's safe harbor law and offers a list of leading cybersecurity frameworks that, if adopted, are presumptively reasonable. These include: the aforementioned NIST CSF, ISO 27000, along with sector-specific laws depending on the sector and industry in which the covered entity is operating, which could include the Fair Credit Reporting Act, Health Insurance Portability and Accountability Act (HIPAA), and/or the payment card industry data security standard (PCI). There are also proposed requirements for regular improvements, such as by implementing up-to-date versions of the NIST CSF, timely tracking vulnerabilities and applying remediation strategies, and updating incident response plans at least annually.

D. Incident Response Best Practices

Under the proposed 2020 Indiana AG cybersecurity rule, covered entities may need to take steps to amend their incident response plans to submit a CAP within a timely fashion (e.g., within thirty days). This requirement would help address the demonstrated lack of planning as seen in the results of this survey with only 27% of respondents reporting that their organizations had a written incident response plan on file. Requirements built-in to the proposed rule to ensure that such plans are regularly updated (e.g., at least annually) could help address this shortfall. Additional steps to aid in this process, and dovetailing with the need for better cyber awareness, would be to encourage that such plans are widely communicated, and even vetted by third parties including insurance firms. The Executive Council could work with universities and other partners to coordinate regular incident response and tabletop exercises to highlight the importance of this proactive planning. One idea would be to focus on one critical infrastructure sector roughly each month, and then conduct a follow-up survey to see how practices have changed after the trainings have taken place.

E. Cyber Risk Insurance

As is evident from this survey, there remains significant barriers for Indiana organizations accessing this tool, including cost, awareness, and confusion over coverage for both first and third-party losses. Given that only 20% of the survey respondents likewise were aware of exclusions in their policies, it seems clear that the State has a role to play in helping Indiana organizations navigate what types of cyber risks insurance can, and cannot, help mitigate. One tool to help in this regard, which could be folded into Indiana's Cybersecurity Hub offerings, could take the form of a guide modeled after Citizen Lab's *Security Planner* but focused not just on cybersecurity best practices, but also on the navigating cyber risk insurance questions across markets, and sectors.

We plan follow-up surveys to periodically assess how Indiana is improving along these metrics, and hope that these results help convince other states to follow Indiana's example in this regard.

Appendix A: Sources Used for Figure 1

- **State Phishing** - https://www.ncsl.org/research/telecommunications-and-information-technology/state-phishing-laws.aspx
- **Ransomware & DDOS** - https://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx#Ransomware
- **Spyware** - https://www.ncsl.org/research/telecommunications-and-information-technology/state-spyware-laws.aspx
- **Cybersecurity Taskforce** - https://www.ncsl.org/research/telecommunications-and-information-technology/statewide-cybersecurity-task-forces636129887.aspx
- **Cybersecurity interest** - https://www.naic.org/documents/cmte_legislative_liaison_brief_data_security_model_law.pdf

Appendix B: Indiana Cybersecurity Survey Protocol

Start of Block: Cyber Risk Perceptions

Q1.1
Cyber incidents - such as phishing attempts, malware attacks, and ransomware demands - are increasingly an area of concern for both the public and private sectors. Although organizations have options for managing cyber risk, relatively little is currently known about what steps are being taken, including what role insurance is playing in this planning process. Additional information would help identify barriers that prevent effective cyber risk planning, while enabling organizations to better understand how their cyber risk planning compares with that of their peers. To get a more complete picture of Hoosier cyber risk planning, the Legal and Insurance working group of the Indiana Executive Cybersecurity Council, in collaboration with researchers at Indiana University and the University of Arizona, is conducting a study to help explore how Indiana organizations perceive and manage cyber risks. This study will pay particular attention to the role of insurance as part of an overarching cyber risk mitigation strategy. The report resulting from this study will provide policymakers and law enforcement with important information about cyber readiness, and help Hoosier organizations like yours better understand current cyber practices in your industry.

We are asking you to participate in this study by filling out a short survey describing your organization's perceptions of cyber risk and use of cyber risk insurance. This survey will take no more than 25 minutes to complete. The responses you provide will only be reported in the aggregate. Your participation is entirely voluntary, and you would be free to terminate the survey at any point. Thank you very much.

Curtis T. Hill, Jr.
Indiana Attorney General Co-Chair of the Legal and Insurance working group of the Indiana Executive Cybersecurity Council

- I agree to participate in the survey
- I do not agree to participate in the survey

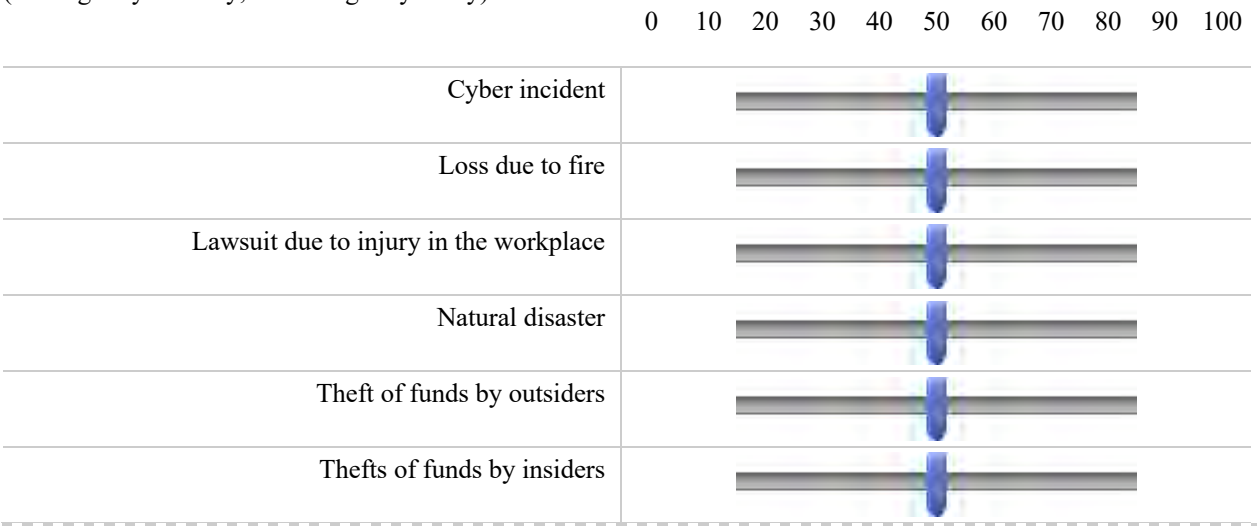
Q1.2 How concerned is your organization about the risk of a cyber incident?

- Not at all concerned
- Somewhat concerned
- Very concerned

Q1.3 Does your organization currently have an insurance policy that provides coverage for any of these events? (Select any that apply)

- Cyber incident
- Loss due to fire
- Lawsuit due to injury in the workplace
- Natural disaster
- Theft of funds by outsider
- Theft of funds by insider
- Not sure

Q1.4 How likely do you think it is that the following events will impact your organization? (0 being very unlikely, 100 being very likely)



Carry Forward All Choices - Displayed & Hidden from "How likely do you think it is that the following events will impact your organization? (0 being very unlikely, 100 being very likely)"

Q1.5 How much harm do you think your organization would face if each of the following events occurred? (0 being very little harm, 100 being a great deal of harm)

	0 10 20 30 40 50 60 70 80 90 100
Cyber incident	
Loss due to fire	
Lawsuit due to injury in the workplace	
Natural disaster	
Theft of funds by outsiders	
Thefts of funds by insiders	

Q1.6 What types of cyber incidents is your organization concerned about? (Select any that apply)

- Ransomware (e.g., extortion)
- Phishing (e.g., targeting key personnel through cyber-enabled means)
- Insider attack (e.g., an employee selling access or secrets)
- Malware (e.g., malicious software)
- Wire/financial fraud (e.g., theft of money through electronic means)
- Password attacks (e.g., someone else breaking your passwords)
- Denial of service attacks (e.g., someone making it impossible for users to access your website)
- Other (Please describe) _____

Carry Forward Selected Choices from "What types of cyber incidents is your organization concerned about? (Select any that apply)"

Q1.7 Please rank the potential types of cyber incidents you identified from most concerning to least concerning.

- Ransomware (e.g., extortion)
- Phishing (e.g., targeting key personnel through cyber-enabled means)
- Insider attack (e.g., an employee selling access or secrets)
- Malware (e.g., malicious software)
- Wire/financial fraud (e.g., theft of money through electronic means)
- Password attacks (e.g., someone else breaking your passwords)
- Denial of service attacks (e.g., someone making it impossible for users to access your website)
- Other (Please describe)

Q1.8 What potential consequences of cyber incidents is your organization concerned about? (Select all that apply)

- Data or information being exposed to outsiders
- Data or information being deleted or lost
- Disinformation about your organization being spread
- Identity theft
- Wire/financial fraud
- Website or system downtime
- Other (Please describe) _____

Carry Forward Selected Choices from "What potential consequences of cyber incidents is your organization concerned about? (Select all that apply)"

Q1.9 Please rank the potential consequences of cyber incidents you identified from most concerning to least concerning.

Data or information being exposed to outsiders
Data or information being deleted or lost
Disinformation about your organization being spread
Identity theft
Wire/financial fraud
Website or system downtime
Other (Please describe)

End of Block: Cyber Risk Perceptions

Start of Block: Cyber Risk Management and Planning

Q2.1 To your knowledge, has your organization experienced a successful cyber incident in the past three years?

Yes
No
Not sure or can't say

Q2.2 How many cyber incidents resulting in data theft did your organization experience in the last three years?

None
1-5
6-10
11-50
51-100
More than 100
Not sure or can't say

Display This Question:
If How many cyber incidents resulting in data theft did your organization experience in the last thr... != None
And How many cyber incidents resulting in data theft did your organization experience in the last thr... != Not sure or can't say

Q2.3 Please think back to the most severe cyber incident resulting in data theft experienced by your organization in the last three years. When did the cyber incident occur?

Month _____
Year _____

Display This Question:
If How many cyber incidents resulting in data theft did your organization experience in the last thr... != None
And How many cyber incidents resulting in data theft did your organization experience in the last thr... != Not sure or can't say

Q2.4 What type of cyber incident did your organization experience?

- Ransomware
- Phishing
- Insider attack
- Malware
- Password attacks
- Denial of service attacks
- Wire/financial fraud
- Other (Please describe) _____
- Not sure

Display This Question:
If How many cyber incidents resulting in data theft did your organization experience in the last thr... != None
And How many cyber incidents resulting in data theft did your organization experience in the last thr... != Not sure or can't say

Q2.5 What were the consequences of the cyber incident experienced by your organization?

- No consequences occurred
- Data or information being exposed to outsiders
- Data or information being deleted or lost
- Disinformation about your organization being spread
- Identity theft
- Wire/financial fraud
- Payment for credit monitoring services
- Website or system downtime
- Disruption of operations
- Other (Please describe) _____
- Not sure

Q2.6 Has your organization taken any steps to prevent potential cyber incidents?

- Yes
- No
- Not sure

Display This Question:
If Has your organization taken any steps to prevent potential cyber incidents? = Yes

Q2.7 What steps has your organization taken? (Select all that apply)

- Installed antivirus software
- Trained employees to spot potential cyber risks
- Invested in cyber risk insurance
- Limited physical access to computer systems
- Required employees to regularly change passwords
- Update and patch software regularly
- Other (Please describe) _____

Display This Question:
If Has your organization taken any steps to prevent potential cyber incidents? = No

Q2.8 Why hasn't your organization taken steps to prevent potential cyber incidents? (Select all that apply)

- Too expensive
- Too difficult
- Not sure what to do
- Prefer to spend resources on other priorities
- Options for preventing cyber incidents are ineffective
- Don't believe our organization is at risk
- Other (Please describe) _____
- Not sure

Q2.9 Has your organization taken any steps to mitigate potential cyber incidents?

- Yes
- No
- Not sure

Display This Question:
If Has your organization taken any steps to mitigate potential cyber incidents? = Yes

Q2.10 What steps has your organization taken? (Select all that apply)

- Installed automatic back-up systems
- Encrypted data
- Purchased cyber risk insurance
- Utilized cloud computing
- Other (Please describe) _____

Display This Question:
If Has your organization taken any steps to mitigate potential cyber incidents? = No

Q2.11 Why hasn't your organization taken steps to mitigate potential cyber incidents?

- Too expensive
- Too difficult
- Not sure what to do
- Prefer to spend resources on other priorities
- Don't believe our organization is at risk
- Other (Please describe) _____
- Not sure

Q2.12
Does your organization use any of the following tools to proactively manage the cyber threats facing your organization? (Select all that apply)

- Joined an information sharing group such as an ISAC
- Consulted news reports
- Relied on government data such as from IN-ISAC or US CERT
- Contacted the FBI/Secret Service for a briefing
- Revised and updated the organization’s incident response plan
- Launched a cyber hygiene campaign
- Revised organizational governance to ensure that cyber threat information was getting where it was needed.
- Other (Please describe) _____
- Not sure

Q2.13 Did your organization refer to any externally developed cyber tools, frameworks, or controls in making decisions about cyber practices?

- Yes
- No
- Not sure

Skip To: Q2.15 If Did your organization refer to any externally developed cyber tools, frameworks, or controls in m... != Yes

Q2.14 If so, which? (Select all that apply)

- NIST Cybersecurity Framework
- ISA
- ISME
- NISTIR 7621 Measure
- ISO 15408
- ISO 27001-02
- ETSI
- Center for Internet Security (CIS) Critical Security Controls
- SP 800-53 R4 Controls
- Australia Top 35 Controls
- Other (Please specify) _____

Q2.15 To your knowledge, has your organization provided anyone with training intended to raise awareness of the potential for cyber threats like hacking, phishing, spamming, or other threats related to stealing or compromising digital?

- Yes
- No
- Not sure

Q2.16 Did you receive training in a formal setting offered by your organization?

- Yes
- No
- Not Sure

Skip To: Q2.18 If Did you receive training in a formal setting offered by your organization? != Yes

Q2.17 How often have you attended trainings designed to improve your awareness of cyber threats?

- Once a quarter
- Once a year
- Every few years
- I have attended only one training

Q2.18 Have others in your organization received training in a formal setting offered by your organization?

- Yes
- No
- Not sure

Q2.19 Who in your organization is ultimately responsible for managing cyber risks?

- CEO
- Board of Directors Committee
- Chief Information Security Officers (CISO)
- Chief Information Officer (CIO)
- Chief Privacy Officer (CPO)
- Chief Information Governance Officer (CIGO)
- Other (Please specify) _____
- Not sure

Q2.20 How many cybersecurity professionals are currently employed at your organization?

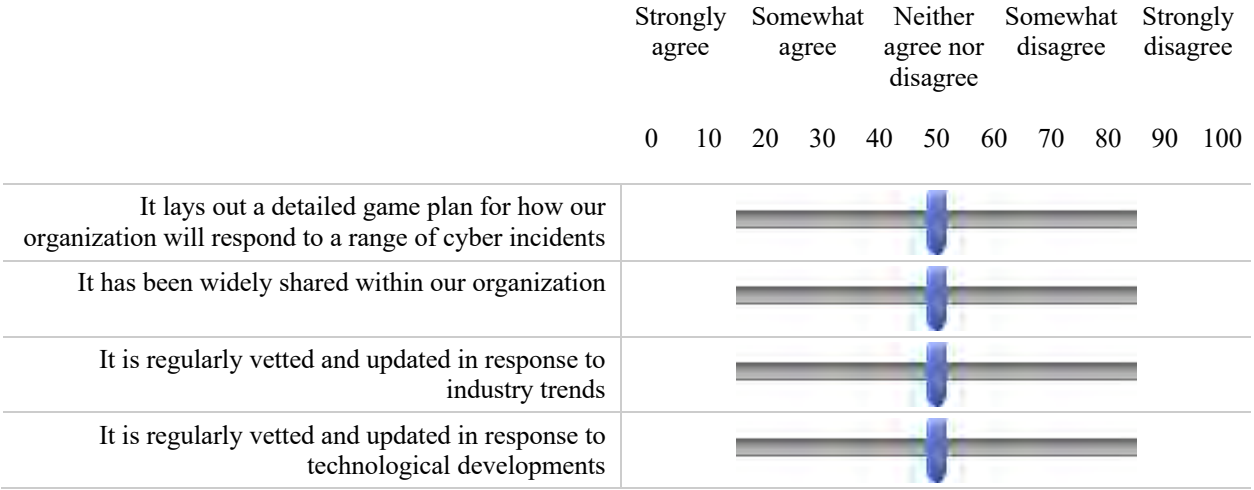
- None
- 1-5
- 6-10
- 11+

Q2.21 Does your organization have written documentation related to cyber incident planning and response?

- Yes
- No
- Not sure

Skip To: Q2.23 If Does your organization have written documentation related to cyber incident planning and response? != Yes

Q2.22 How strongly would you agree or disagree with the following statements about your organization's cybersecurity documentation?



Q2.23 Which, if any, of the following practices does your organization currently employ? (Select all that apply)

- Multi-factor authentication
- End-to-end encryption
- Remote backups
- Automatic updating of operating systems and software
- Traffic flow analysis
- Third-party penetration testing
- Policy on "Bring Your Own Device" (BYOD)
- Regular checks for vendors and partners
- Others (Please describe) _____
- None of the above
- Not sure or can't say

Q2.24 Does your organization currently have insurance specifically tailored to cover cyber incidents?

- Yes
- No
- Not sure

End of Block: Cyber Risk Management and Planning

Start of Block: Cyber Risk Insurance Use

Q3.1 When did your organization obtain a cyber risk insurance policy?

- Year _____
- Month _____

Q3.2 Why did your organization get a cyber risk insurance policy? (Select all that apply)

- Response to an incident at our organization
- Response to an incident at a peer organization
- News reports about cyber incidents
- Other (Please describe) _____
- Not sure

Q3.3 Which (if any) losses to your organization (first-party losses) are covered under this policy? (Select all that apply)

- Expenses related to responding to the cyber breach (such as hiring a firm to secure systems)
- Cost of notifying affected customers or others whose data was exposed in a breach
- Credit monitoring services
- Fines/penalties related to the data breach
- Business interruptions related to denial of service or other downtime
- Losses resulting from exposure or use of confidential business information
- Losses arising from stolen funds or products
- Damage to computer or information systems (including cost of restoring lost data)
- Damages related to lost intellectual property
- Forensic investigation of the breach
- Standing up a call center and response team
- Other (Please describe) _____
- None of the above
- Not sure

Skip To: Q3.5 If Which (if any) losses to your organization (first-party losses) are covered under this policy? (S... = None of the above
Skip To: Q3.5 If Which (if any) losses to your organization (first-party losses) are covered under this policy? (S... = Not sure

Carry Forward Selected Choices from "Which (if any) losses to your organization (first-party losses) are covered under this policy? (Select all that apply)"

Q3.4 Please rank how important it is for your organization to have coverage for the first-party losses you selected, from most important to least important.

Expenses related to responding to the cyber breach (such as hiring a firm to secure systems)
Cost of notifying affected customers or others whose data was exposed in a breach
Credit monitoring services
Fines/penalties related to the data breach
Business interruptions related to denial of service or other downtime
Losses resulting from exposure or use of confidential business information
Losses arising from stolen funds or products
Damage to computer or information systems (including cost of restoring lost data)
Damages related to lost intellectual property
Forensic investigation of the breach
Standing up a call center and response team
Other (Please describe)
None of the above
Not sure

Q3.5 Which (if any) losses to others (third-party losses) are covered under this policy? (Select all that apply)

Claims for damages from customers or others whose information was exposed in the breach
Claims for damages from customers or others who suffered other economic loss due to your security failure (e.g., malware was pushed to their systems)
Costs for legal defenses related to the data breach
Fines and penalties
Other (Please describe) _____
None of the above
Not sure

Skip To: Q3.7 If Which (if any) losses to others (third-party losses) are covered under this policy? (Select all t... = None of the above
Skip To: Q3.7 If Which (if any) losses to others (third-party losses) are covered under this policy? (Select all t... = Not sure

Carry Forward Selected Choices from "Which (if any) losses to others (third-party losses) are covered under this policy? (Select all that apply)"

Q3.6 Please rank how important it is for your organization to have coverage for the third-party losses you selected, from most important to least important.

Claims for damages from customers or others whose information was exposed in the breach
Claims for damages from customers or others who suffered other economic loss due to your security failure (e.g., malware was pushed to their systems)
Costs for legal defenses related to the data breach
Fines and penalties
Other (Please describe)
None of the above
Not sure

Q3.7 Does your cyber risk insurance policy require your organization to undertake certain security measures?

Yes
No
Not sure

Skip To: Q3.9 If Does your cyber risk insurance policy require your organization to undertake certain security mea... != Yes

Q3.8 What security measures are required by your cyber risk insurance policy? (Select all that apply)

Mandatory, automatic patching
End-to-end data encryption
Employee training & cyber hygiene
Regular third party penetration testing
Other (please list) _____
None of the above
Not sure

Q3.9 Does your cyber risk insurance policy have a limit?

Yes
No
Not sure

Skip To: Q3.11 If Does your cyber risk insurance policy have a limit? != Yes

Q3.10 What is the limit?

_____

Q3.11 Does your cyber risk insurance policy exclude coverage in certain circumstances?

Yes
No
Not sure

Skip To: Q3.13 If Does your cyber risk insurance policy exclude coverage in certain circumstances? != Yes

Q3.12 Under what circumstances would your cyber risk insurance policy exclude coverage (Select all that apply)
- Act of war/terrorism
- Internet of Things-related breach
- Losses from unencrypted devices
- Contractual liability
- Criminal or fraudulent acts
- Losses related to unauthorized collection of customer data
- Losses that occurred because your organization failed to provide and maintain adequate security
- Other (Please describe) _____
- None of the above

Q3.13 Is your policy retroactive to cover losses that occurred (in whole or in part) before its start date?
- Yes
- No
- Not sure

Q3.14 Does your company require subcontractors to have cyber risk insurance?
- Yes
- No
- Not sure

Skip To: End of Block If Does your company require subcontractors to have cyber risk insurance? != Yes

Q3.15 What losses must be covered under a subcontractor's cyber risk insurance policy?
- Expenses related to responding to the cybersecurity breach (such as hiring a firm to secure systems)
- Cost of notifying affected customers or others whose data was exposed in a breach
- Fines/penalties related to the data breach
- Business interruptions related to denial of service or other downtime
- Losses resulting from exposure or use of confidential business information
- Not sure

End of Block: Cyber Risk Insurance Use

Start of Block: Cyber Risk Insurance Non-Use

Q4.1 Has your company ever had a cyber risk insurance policy?
- Yes
- No
- Not sure

Skip To: Q4.6 If Has your company ever had a cyber risk insurance policy? != Yes

Q4.2 During what period did your company have a cyber risk insurance policy?
- Date cyber risk insurance coverage began _____
- Date cyber risk insurance coverage ended _____

Carry Forward All Choices - Displayed & Hidden from "Which (if any) losses to your organization (first-party losses) are covered under this policy? (Select all that apply)"

Q4.3 Which (if any) losses to your organization (first-party losses) were covered under this policy? (Select all that apply)

- Expenses related to responding to the cyber breach (such as hiring a firm to secure systems)
- Cost of notifying affected customers or others whose data was exposed in a breach
- Credit monitoring services
- Fines/penalties related to the data breach
- Business interruptions related to denial of service or other downtime
- Losses resulting from exposure or use of confidential business information
- Losses arising from stolen funds or products
- Damage to computer or information systems (including cost of restoring lost data)
- Damages related to lost intellectual property
- Forensic investigation of the breach
- Standing up a call center and response team
- Other (Please describe) _____
- None of the above
- Not sure

Carry Forward All Choices - Displayed & Hidden from "Which (if any) losses to others (third-party losses) are covered under this policy? (Select all that apply)"

Q4.4 Which (if any) losses to others (third-party losses) were covered under this policy?

- Claims for damages from customers or others whose information was exposed in the breach
- Claims for damages from customers or others who suffered other economic loss due to your security failure (e.g., malware was pushed to their systems)
- Costs for legal defenses related to the data breach
- Fines and penalties
- Other (Please describe) _____
- None of the above
- Not sure

Q4.5 Why did you discontinue your former cyber risk insurance policy? (Select all that apply)

- Too expensive
- Couldn't get a policy
- Covered under other insurance policies
- Prefer to spend resources on other priorities
- Options for preventing cybersecurity incidents are ineffective
- Don't believe our organization is at risk
- Other (Please describe) _____
- Not sure

Skip To: End of Block If Why did you discontinue your former cyber risk insurance policy? (Select all that apply) = Too expensive
Skip To: End of Block If Why did you discontinue your former cyber risk insurance policy? (Select all that apply) = Couldn't get a policy
Skip To: End of Block If Why did you discontinue your former cyber risk insurance policy? (Select all that apply) = Covered under other insurance policies
Skip To: End of Block If Why did you discontinue your former cyber risk insurance policy? (Select all that apply) = Prefer to spend resources on other priorities
Skip To: End of Block If Why did you discontinue your former cyber risk insurance policy? (Select all that apply) = Options for preventing cybersecurity incidents are ineffective

Skip To: End of Block If Why did you discontinue your former cyber risk insurance policy? (Select all that apply) = Don't believe our organization is at risk
Skip To: End of Block If Why did you discontinue your former cyber risk insurance policy? (Select all that apply) = Other (Please describe)
Skip To: Q4.6 If Why did you discontinue your former cyber risk insurance policy? (Select all that apply) = Too expensive
Skip To: End of Block If Why did you discontinue your former cyber risk insurance policy? (Select all that apply) = Not sure

Q4.6 Has your company ever considered obtaining a cyber risk insurance policy?
- Yes
- No
- Not sure

Skip To: Q4.8 If Has your company ever considered obtaining a cyber risk insurance policy? != Yes

Q4.7 Why did your company decide not to obtain a cyber risk insurance policy? (Select all that apply)
- Too expensive
- Difficult to obtain
- Covered under other insurance policies
- Prefer to spend resources on other priorities
- Options for preventing cybersecurity incidents are ineffective
- Don't believe our organization is at risk
- Other (Please describe) _____

Q4.8 What would encourage your company to obtain a cyber risk insurance policy?

_____
_____
_____
_____
_____

End of Block: Cyber Risk Insurance Non-Use

Start of Block: Organization and Respondent

Q5.1 What is your job title?

_____

Q5.2 How many employees does your organization have?
- 1-10 employees
- 11-50 employees
- 51-250 employees
- More than 250 employees

Q65 Does your organization fall within one of the following critical infrastructure sectors?

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector
- Defense Industrial Base Sector
- Emergency Services Sector
- Energy Sector
- Financial Services Sector
- Food and Agriculture Sector
- Government Facilities Sector
- Healthcare and Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector
- Transportation Systems Sector
- Water and Wastewater Systems Sector
- No, my organization does not fall within a critical infrastructure sector
- Prefer not to say

Skip To: Q5.4 If Does your organization fall within one of the following critical infrastructure sectors? != No, my organization does not fall within a critical infrastructure sector

Q5.3 What sector is your organization in?

- Accommodation and Food Services
- Administrative and Support Services
- Agriculture, Forestry, Fishing, and Hunting
- Arts, Entertainment, and Recreation
- Construction
- Educational Services
- Finance and Insurance
- Government
- Health Care and Social Assistance
- Manufacturing
- Mining
- Other Services
- Professional, Scientific, and Technical Services
- Real Estate, Rental, and Leasing
- Retail Trade
- Transportation and Warehousing
- Utilities
- Wholesale Trade
- Other (Please specify) _____

Q5.4 Which of the following types of information about individuals does your organization handle? (Select all that apply)

- Personally identifiable information (e.g., home addresses, email addresses, social security numbers)
- Personal financial information (e.g., credit card numbers, banking information, credit scores)
- Personal health information (e.g., allergies, past medications)
- Other (Please describe) _____
- We do not collect any personal data

Q5.5 How would you describe the geographic scope of your organization?

- Local (e.g., city or county)
- State
- Regional (e.g., more than one state)
- National
- Multi-national
- Does not apply

Q5.6 Would you be willing to participate in a follow-up interview to further explore how your company is managing cyber risk?

- Yes
- No

Display This Question:

If Would you be willing to participate in a follow-up interview to further explore how your company... = Yes

Q5.7 Thank you for your willingness to participate in a follow up interview. Please provide your name, affiliation, and email for contact purposes only.

_____

End of Block: Organization and Respondent