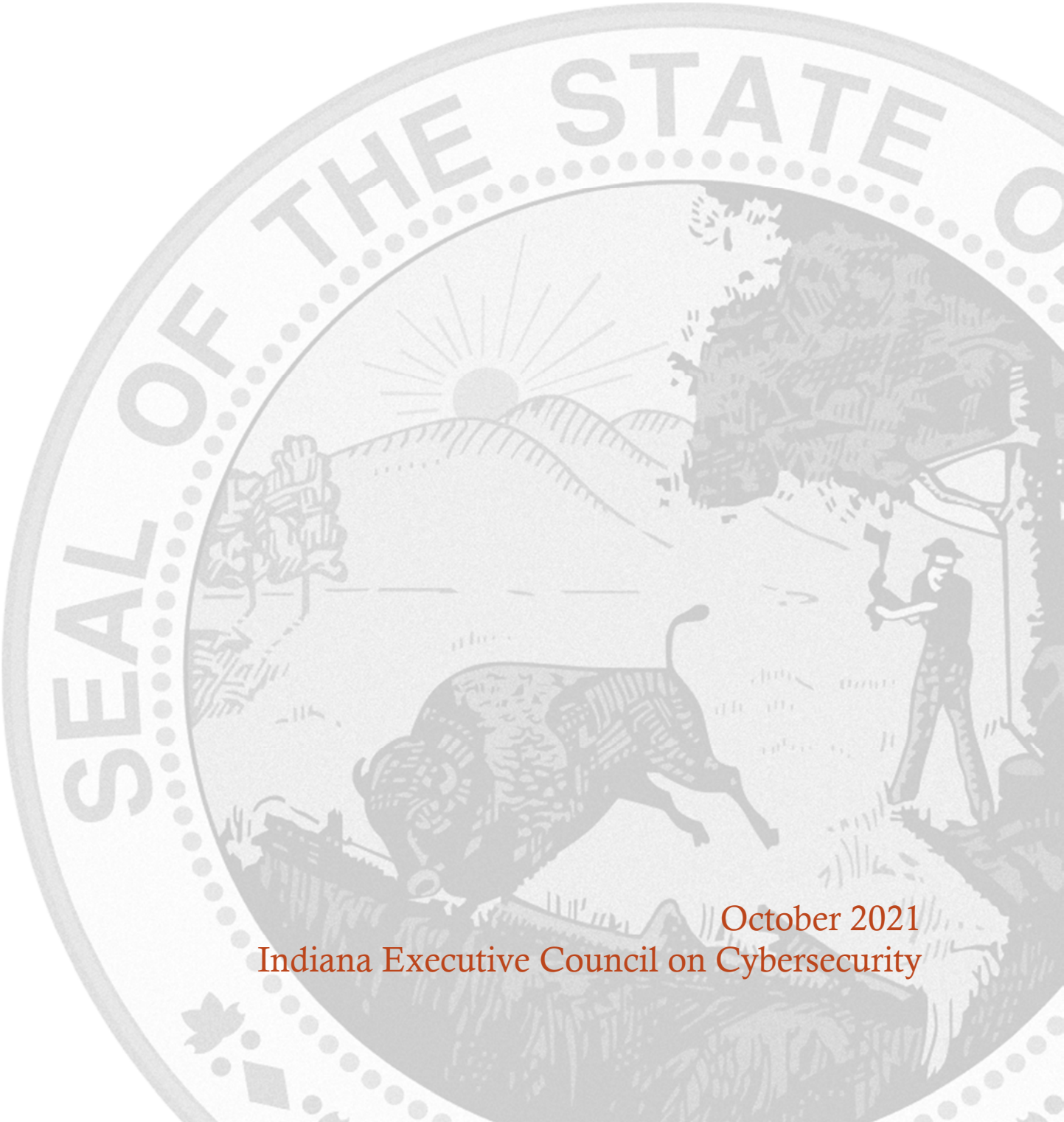
FINANCE COMMITTEE STRATEGIC PLAN

Chair: Angie Ritchey
Co-Chair: Tom Fite



October 2021
Indiana Executive Council on Cybersecurity

Finance Committee Plan

Table of Contents

Committee Members

Committee Members

Last Name	First Name	Organization	Organizational Title	Member Type (Chair/Co-chair/Full-time, As needed)
Cloud	Matthew	Ivy Tech Community College of Indiana-Lake County Campus	Director of Cybersecurity Grants, Asst. Prof. of Data Analytics, and Dept. Chair School of IT and Criminal Justice.	Full Time
Fite	Tom	Indiana Department of Financial Institutions	Director	Co-Chair
Goodlink	George	Lake City Bank	Director	Full Time
Hochstetler	Jay	Qumulus Solutions	Vice President, Security Operations	Full Time
Leetz	Tanya	People's Bank	Executive VP, Chief Information and Technology Officer	Full Time
Lodin	Steve	Sallie Mae Bank	Senior Director, Cybersecurity Operations	Full Time
Merkner	Karl	United Federal Credit Union	Security Engineer	Full Time
Ritchey	Angie	Lake City Bank	Senior Vice President, Chief Technology Officer	Co-Chair
Stouder	Kevin	Indiana Department of Financial Institutions	IT Examiner, IT Program Lead	Co-Chair Proxy
Wuellner	Mark	Indiana Bond Bank	Executive Director	As Needed

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**
  - Determined the need for additional hands-on training and education of industry professionals based on information security best practices and procedures. Committee members also spoke to industry professionals, vendors, and researched common training courses targeted to the financial industry.

- **Research Findings**
  - There is still a need for increased and on-going training and education.

- **Committee Deliverables**
  - Board Leadership Education Plan
  - Disruption Plan
  - Top Security Tips Material 2.0

- **Additional Notes**
  - A network penetration test of selected State systems conducted by members of the IECC and a state-run phishing portal for local and State government employees are being considered as potential deliverables in years two and three.

- **References**
  - Center for Internet Security – Controls
  - European Union – General Data Protection Regulation
  - Federal Deposit Insurance Corporation – Information Technology Risk Examination (InTREx)
  - Federal Deposit Insurance Corporation – Cybersecurity Assessment Tool (CAT)
  - Federal Deposit Insurance Corporation – Security Standards for Customer Information
  - Federal Trade Commission – Gramm-Leach-Bliley-Act
  - FFIEC – Information Technology Booklets
  - Financial Services – Information Sharing and Analysis Center
  - Ivy Tech – Cyber Security / Information Assurance Program
  - National Institute of Standards and Technology – Publications
  - Ponemon Institute – Cost of Data Breach Analysis
  - Ponemon Institute – Megatrends Study in Cybersecurity
  - SANS – CIS Critical Security Controls for Effective Cyber Defense
  - Verizon – Data Breach Investigations Report

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
    a. The cybersecurity landscape has changed significantly over the past five years. As a result, members of the Finance Committee have taken a number of steps to focus on continually educating industry professionals on the basics of cybersecurity. A number of those steps have included educating and training industry professionals through educational opportunities, professional organizations, as well as a number of informal discussions.

2. **What (or who) are the most significant cyber vulnerabilities in your area?**
    a. There have been a number of significant cyber incidents that have affected the financial industry. Among the most notable have been Finastra and Kaseya ransomware attacks, SolarWinds supply-chain attack, Microsoft Exchange server attack, and Windows print spooler zero-day exploit. It is hard to qualify or quantify the most significant cyber vulnerabilities until they have happened. Therefore, it is our responsibility to continually drive conversations within the financial industry towards following information security best practices to avoid risks.

3. **What is your area's greatest cybersecurity need and/or gap?**
    a. The greatest cybersecurity risk in the financial industry is the lack of education about cybersecurity. The risks are real, they do occur, and they have real consequences! We need to remain diligent in how we store, process, and transmit information. We must also hold people accountable for the confidentiality, integrity, and availability of data. One way to remain diligent is to continue to educate people. It is through cybersecurity education that the greatest awareness can be achieved.

4. **What federal, state, or local cyber regulations are your area beholden to currently?**
    a. There are a number of federal and state banking laws that the financial industry is beholden to including the Gramm-Leach-Bliley Act, Sarbanes-Oxley Act, and various Indiana Codes. Beyond domestic law, the European Union recently implemented the General Data Protection Regulation (GDPR). As a result of this new regulation, international corporations based in America will have consequences for data protection issues that arise in Europe.

5. **What case studies and/or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
    a. There are a number of independent annual publications that report on the status of privacy, data protection, and information security policy. The Verizon Data Breach Investigations Report, Poneman's Cost of Data Breach Global Analysis, and Ponemon's Global Megatrends in Cybersecurity are three prominent examples. Each of these are linked on page 9 in the references section of the executive summary.

6. **What research is out there to validate your group's preliminary deliverables? This could be surveys, whitepapers, articles, books, etc. Please collect and document.**
    a. There are a number of banking organizations that collect, document, and report on statistics and trends specifically for the financial industry. The American Bankers Associations (ABA), the Conference of State Bank Supervisors (CSBS), and the Independent Community Bankers Association (ICBA) are industry organizations who have accumulated data pertaining to cybersecurity risks in our area.

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
    a. The Federal Financial Institutions Examination Council (FFIEC) published the Cybersecurity Assessment Tool (CAT) with the most recent version being May 2017. The CAT was released jointly by state and federal regulatory parties as a tool that financial institutions could voluntarily use to identify risks and determine their cybersecurity maturity. Other similar tools include the Financial Services Sector Coordinating Council (FSSCC) Cybersecurity Profile, which is now maintained, updated, and managed by the Cyber Risk Institute "CRI" and was last updated in November 2020. The CRI plans to release a number of new versions by the end of year 2021 that will also include a Cloud Controls version to its profile. The National Institute of Standards and Technology (NIST), under the Department of Commerce, has also created a Cybersecurity Framework (CSF). The framework is a voluntary guidance, based on existing standards, guidelines, and practices for organizations (not just in the financial sector) to better manage and reduce cybersecurity risk.

8. **What does success look like for your area in one year, three years, and five years?**
    a. It is difficult to define "success" within the cybersecurity space. With the advent of zero-day attacks, social engineering, or simple human failure, there are many reasons why cyber incidents continue to plague the financial sector. However, "success" may be achieved through greater education, collaboration, and communication.

9. **What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?**
    a. IT/Cybersecurity focused training is needed both in the corporate world and with individual citizens. Access to this training is key. Training is often targeted at IT/Cybersecurity specialists with minimal training available for non-IT staff. Furthermore, training can be expensive, leaving corporations in a quandary as to who should receive IT/Cybersecurity training and to what depth that training should cover. From a consumer standpoint, financial institutions also recognize that remote access to their customers' data poses a significant risk. To mitigate this risk, financial institutions need to remain diligent in educating customers on IT/Cybersecurity best practices. A customized information security curriculum targeted towards financial sector professionals and customers will increase awareness of IT/Cybersecurity.

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?**
    a. Access to cybersecurity specialists varies greatly across the country, as does the competition and affordability of these resources. Larger metropolitan areas have better access to staffing resources; however, demand for these resources is also greater in metropolitan areas.

11. **What do we need to do to attract cyber companies to Indiana?**
    a. The state of Indiana needs to continue its cybersecurity initiatives leveraging assets like its colleges and universities, research centers of excellence, and business communities. By leveraging these assets, the State can establish an environment that is conducive to attracting more cyber-based companies.

12. **What are your communication protocols in a cyber emergency?**
    a. The financial industry has a number of outlets with which to communicate cyber emergencies. One such outlet is the financial services – information sharing and analysis center (FS-ISAC). The FS-ISAC's mission is to protect the financial services infrastructure and individual firms against acts that could significantly impact the sector's ability to provide services. The FS-ISAC has protocols in place to manage rapid response communications during incidents.

13. **What best practices should be used across the sectors in Indiana? Please collect and document.**
    a. Several different industry resources and best practices are available; however, none serves a one size fits all solution. Among the most notable non-industry specific IT/Cybersecurity and Risk resources include the National Institute of Standard and Technology (NIST); Cybersecurity and Infrastructure Security Agency (CISA); Center for Internet Security (CIS); and Information Systems Audit and Control Association (ISACA). Given the wide range of complexity and risks across the financial industry, it would be unlikely that any one set of best practices would fulfill the needs of all financial businesses.

Deliverable: Board Leadership Education Plan

Deliverable: Board Leadership Education Plan

General Information

1. **What is the deliverable?**
    a. To provide formal cybersecurity training at a management or board membership level, outlining responsibilities associated with oversight within their organization. This formal training could and likely will be beneficial to all sectors of the IECC.

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. Executives/Leaders are better prepared to address the challenges presented to their organizations as a result of cyber threats.

6. **What metric or measurement will be used to define success?**
    a. Attendance and completion of the program.

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 who participated in the training program.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. None of which we are aware.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Possibly all other critical infrastructures committees of the IECC.

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. To be determined. There has been previous program development with Ivy Tech and that may be necessary or appropriate here as well.

12. **Who should be main lead of this deliverable?**
    a. IECC Member, George Goodlink

13. **What are the expected challenges to completing this deliverable?**
    a. Advertising this program to leadership across the state and gaining interest in participation.

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
Identify Curriculum	Committee		12/31/2021	
Identify Instructor/Agency	Committee		3/31/2022	
Advertise Program	IECC		6/30/22	

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
3	6-10	Role = ISO or CISSP	Volunteers		CISSP certification requires CPE hours, which can include serving as an instructor for these types of courses, benefiting this deliverable as well as the CISSP.

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/ Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Materials	Training materials to be used as Guides	$2500	$5000	Grant funding	Could charge a fee to the attendees of their place of business.	Could potentially identify sponsors for the program

Benefits and Risks

17. What is the greatest benefit of this deliverable?

a. Proper education of board members and leadership on the perils of cybersecurity and steps to take if impacted by an event.

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

a. Much of this depends on the extent of the event and costs associated with addressing the threat and recovery.

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

a. Same response as question 18.

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

a. Participation and completion rates.

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. Unsure as to where other programs exist.

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. Unsure as to any other programs that exist, but there are increasing threats associated with cybersecurity consistently reported by media. An assumption that boards are receiving this type of education, but only internally. This effort, however, would be sector wide.

Other Implementation Factors

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

a. Lack of engagement, interest, or resource availability

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. Consistent review of materials included in the program, updates to curriculum and a supply of CISSPs to present.

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

a. This is a new deliverable, so no outside contact or discussion has occurred.

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. IECC and financial institutions in Indiana through associations and communication efforts

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. An awareness campaign will be critical to the success of this program, including social media, news media, and local chambers.

Evaluation Methodology

Objective 1: 1: IECC Finance Committee will develop a curriculum and identify an instructor(s) to be used for the Board and Executive Leadership Education Plan 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: The Board and Executive Leadership Education will be provided to a pilot group of finance institutions by December 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: Disruption Plan and Communication Evaluation

Deliverable: Disruption Plan and Communication Evaluation

General Information

1. **What is the deliverable?**
    a. Like all businesses, financial service providers are subjected to ongoing cyberattack attempts. Albeit rare, successful attacks present substantial risk of a disruption in consumer services, and awareness of this disruption could lead to panic for consumers. This distress could even lead to public safety concerns, such as a deposit run on an institution. Within this deliverable the committee will research the risk of financial services disruption. Any barriers to communication will be explored in effort to outline a communication plan institutions could deploy if/when they need support during and after a cyberattack.

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?**
    ☐ 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 deliverable hopes to increase services and communication available should a cyberattack occur.

6. **What metric or measurement will be used to define success?**
    a. Success will be achieved with the creation of a disruption communication and support strategy primarily. However, it is anticipated that there will be many barriers to communication as well and mapping these barriers will likely become a secondary benefit of this deliverable.

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

8. **Who or what entities will benefit from the deliverable?**
    a. Financial service providers, financial services consumers, and government leadership.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. Unknown. This is one of the questions that could be answered. A list of such resources may not presently exist.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. It is anticipated coordination may be necessary with other groups that involve security and emergency response.

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. Unknown. This question will be answered while completing this deliverable.

12. **Who should be main lead of this deliverable?**
    a. The Indiana Department of Financial Institutions in coordination with partners like the Indiana Bankers Association, the Indiana Credit Union League, and Indiana based federal regulators.

13. What are the expected challenges to completing this deliverable?

a. Confidentiality rules will be a substantial barrier for at least two reasons. Various laws and regulations protect financial service provider information and regulatory findings, and appropriately/importantly so. Revealing details about a cyber attack on a financial institution can make matters worse by revealing certain facts that assist cyber terrorists in further expanding the attack at the affected and/or additional institutions.

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
Begin mapping out the connections to the various partners in the finance sector at a federal, state, and local level	Indiana Department of Financial Institutions	-	2022	
Determine the proper channels and limitations of information sharing of key stakeholders	Indiana Department of Financial Institutions in coordination with partners like the Indiana Bankers Association, the Indiana Credit Union League, and Indiana based federal regulators	-	Qtr 3 2022	
Develop a disruption plan for sharing information with key stakeholders including the State Emergency Operations Center	IECC Finance Committee with Cybersecurity Program Director	-	Qtr 4 2022	
Circulate the disruption plan with all stakeholders	IECC Finance Committee with Cybersecurity Program Director	-	Qtr 3 2023	

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
None					

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 at this time.						

Benefits and Risks

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

a. The largest benefit is preparedness. Upon completion of this deliverable, there will be better understanding of access to public/private coordination during a cyber attack and more awareness of the impediments to communication following a successful attack.

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

a. This deliverable will not reduce the risk of a cyber incident. It will however assist with risk mitigation following any disruption that may occur stemming from a cyber attack.

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

a. Undetermined

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

a. Undetermined

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. The ongoing pandemic continues to demand significant resources from the parties that will be involved with this deliverable. Many unknowns are still ahead for the financial services community, and any pandemic driven recessionary pressures would take human resources away from this deliverable.

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

☒No ☐ Yes

a. The response to question 24 is unknown at this time. No regulatory/policy change is anticipated, but this will become clearer during the work of this project.

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

a. Unknown.

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

a. No contact has been made as of yet, deliverable has not been started.

27. Can this deliverable be used by other sectors?

☒No ☐ Yes

Communications

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

a. Regulatory leadership, financial services association leadership, and governmental leadership.

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

Evaluation Methodology

Objective 1: IECC Finance Committee will develop a Finance Sector Disruption Plan for the State of Indiana by Qtr. 3 of 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

Objective 2: The IECC Finance Committee will evaluate communication opportunities and identify associated barriers by Qtr. 4 of 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: Top Security Tips Material 2.0

Deliverable: Top Security Tips Material 2.0

General Information

1. **What is the deliverable?**
    a. The IECC finance committee developed top security tips as a deliverable from the prior three-year strategic plan (see supporting documentation for Top Security Tips Material 1.0). The committee will now review these tips to be sure that they remain current and applicable. As with the first version of this material, the committee will distribute training material relevant to explaining information security tips that could be implemented in a technology environment on an extremely limited budget that could help secure the environment's data from compromise.

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. Better end-user information security posture, education, awareness, reporting, and response.

6. **What metric or measurement will be used to define success?**
    a. Release of updated security tips that can be utilized by entities with limited IT resources.

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

8. **Who or what entities will benefit from the deliverable?**
    a. Local and State governmental entities throughout Indiana.
    b. Entities with limited IT resources

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. There are other information security resources available from various sources.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. The material will be distributed to all working groups and committees, but their involvement will not be necessary.

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. To Be Determined (TBD), but overseen by the IECC Finance Committee

12. **Who should be main lead of this deliverable?**
    a. IECC Member Jay Hochstetler

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
Revise & circulate "Top Information Security Tips" to IECC for mass distribution	Jay Hochstetler	25%	December 2022	Review of original information with notes and additional content added.

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
No Response					

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

a. None

Resource	Justification/ Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
No Response						

Benefits and Risks

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

a. Better end-user information security posture, education, awareness, reporting, and response. A reduction of information security incidents overall.

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

a. Better end-user information security posture, education, awareness, reporting, and response.

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

a. Educating the workforce of critical infrastructure regarding information security best practices is a necessity and should be considered a priority.

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

a. Circulation of the material to a large audience. No baseline will be measured.

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. Information security best practice documents are widely available. This document explains current attack techniques and potential mitigations. This document should be used in conjunction with other available resources.

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. Periodic review by several resources (i.e. team members) to ensure content is relevant and updated.

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

a. The deliverable will be circulated internally to the committee to distribute as deemed necessary. This could include posting on a state website.

27. Can this deliverable be used by other sectors?

☐No ☒ Yes

a. Information security best practices are not industry specific.

Communications

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

a. IECC feels is appropriate.

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. Currently unknown.

Evaluation Methodology

Objective 1: IECC Finance Committee will review and distribute the Top Information Security Tips 2.0 training material for Indiana businesses by December 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

- Top Security Tips Material 1.0

IECC Finance Committee
Top Security Tips Material 1.0

Information Security Tips - 2019

Harden Interior/Exterior

- Assess risk based on current threat environment and impact.
- Limit externally facing access to data.
  - VPN, email, servers, etc. Enable two-factor authentication (2FA).
- Limit ingress/egress points. Control local network access. Network segmentation.
- Change detection for new open ports, regular automated vulnerability scans.
- Enable host-based firewalls.
  - Do workstations need to talk to each other?
- Enable 802.1x.

Proxy Traffic

- Implement network traffic filters.
- Intrusion Detection / Intrusion Prevention (internal & external).
- Full packet capture and net flow data is a necessity to determine if an incident occurred and what / how much data was transmitted.
- Don’t forget about SSL/TLS.
  - Where is your network packet visibility limited?
- Data Loss Prevention.
  - USB/CD blocking, webmail, email alerts.

Know Where Your Data Lives

- Cloud, onsite, ancillary accounts for business purposes? Does your data auto-sync?
- 2FA wherever possible.
- Strong & unique passwords.
  - Password managers.
- If it doesn’t need to be stored online, don’t.

Disable/Control Ancillary Services

- Services/applications that could be used in an attack. How are attacks occurring? Can we mitigate/prevent?
- Severely limit PowerShell, cmd, etc.
  - Enable PowerShell logging and alerting.
- Use Software Restriction Policies & Group Policies to your advantage.

Group Policy

- Turn off access to USB/CD.
- Limit number of cached logons and don’t let wdigest store passwords in clear text.
- Harden UNC paths.
- Disable/severely limit macros in Office products and other commonly used scripting attacks methods.
- Block scripting in PDFs.

Control Authentication

- Service / local account password randomization and very complex.
- User passwords with complex 12+ characters. Admins 15+.
- Disable WPAD.
- Enable SMB signing.
- Disable NetBIOS & LLMNR.
- Limit admin accounts. Many current threats can execute as standard user.

Control Authentication

- Vendor Accounts
  - How do they have access to your network?
    - Site-to-site VPN / Remote access VPN?
  - Principle of Least Privilege.
  - Disable when not in use.
- Very few admins need Domain Admin.

Examine Phishing Attempts

- They are letting you know how they are trying to attack you, why just delete that message.
- NOT advisable to do this on your corporate network.
- Dedicated phishing email account and virus network/VM for testing user submissions.
- Have the ability to post process internal corporate network traffic.
- Train users on current phishing/social engineering trends.
- Enable DMARC and SPF inspection.

Watch/Archive Logs

- Setup thresholds to auto email when anomalies are detected.
- In addition to the obvious failed logons and other potential indicators of compromise, set thresholds for too many successful logon attempts from one account.
  - Why did one user just log onto 100 machines successfully?
  - What other ways can you detect an attacker’s lateral movements?
- Set useful and relevant retention periods for logs.

Control Mobile Users

- Force VPN when off the network for mobile users. 2FA.
  - Built into most VPN applications.
- We want to have visibility into our machines, no matter their physical location.
- Encrypt all devices.

Patch & Assess

- Set schedules, as often as possible. Patch and assess your environment via vulnerability scanning to ensure patches are being deployed.
  - Nessus, Qualys, OpenVAS, etc.
- Respond to the vulnerability scan results.
  - What is not getting patched? If it can’t be patched, document why and implement mitigating controls.
  - If necessary, establish a manual patching process.

Backups

- Are they stored for long enough?
- Restore testing.
- Is your tertiary backup system online, on the same domain as your primary, use the same backup software?
  - Air-gap your backups.
- Data retention policy?