ECONOMIC DEVELOPMENT COMMITTEE STRATEGIC PLAN

Chair: Secretary of Commerce Brad Chambers
Co-Chair: Ronald W. Pelletier

October 2021
Indiana Executive Council on Cybersecurity

Economic Development 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)
Jeffers	Chris	Indiana Economic Development Corporation	PTAC Director	Full Time
Lubbers	Teresa	Indiana Commission for Higher Education	Commissioner	Full Time
Ortiz	Jason	Pondurance	Senior. Product Engineer	Full Time
Pelletier	Ronald W.	Pondurance	Founding Partner	Co-Chair
Rapp	Douglas	Cyber Leadership Alliance	President	Full Time
Roberts	David	Indiana Economic Development Corporation	Vice President, Chief Innovation Officer, Business Development	Chair Proxy
Staton	Jim	Indiana Economic Development Corporation	Senior Vice President and Chief Business Development Officer	Full Time
Thompson	JJ	Alpine Start	Founder	As Needed
Wasky	Mark	Indiana Economic Development Corporation	Vice President & Counsel, Government & Community Affairs	As Needed
Watkins	David	Indiana Economic Development Corporation	SBDC State Director	Full Time
Silbaugh	Chris	Rolls Royce	Senior Security Strategy Officer	Full Time

Chambers	Brad	Indiana Economic Development Corporation	Secretary of Commerce	Chair
Langley	Bryan	Indiana Economic Development Corporation	Senior Vice President of Defense	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**
  - The Economic Development Working Group referred to several resources related to the economic impact and projections of cybersecurity employment and corporate growth projections, including report commissioned by the Indiana Economic Development Corporation (IEDC), comparisons with other state's indicated initiatives (e.g., GA, MI, MD, KY, LA, CO, etc.), employment data reported by US Department of Labor, Office of Economic Adjustment, and Emsi Occupation Snapshot Report for Q4 2017 (central Indiana).
    - The State's existing assets, needs of the private and public sector, opportunities for talent and commercial growth, and "threats" related to other states' strategic initiatives in the economic development of cybersecurity in their respective states.

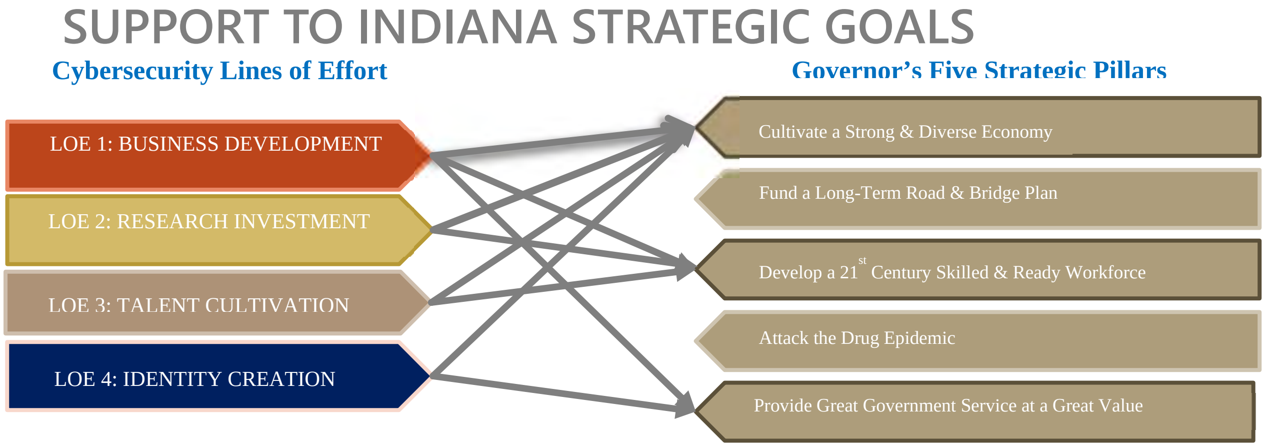
- **Research Findings**
  - Our review of the economic development strengths, weaknesses, opportunities, and threats (SWOT) of cybersecurity led the group to the following conclusions:
    - Cybersecurity should not be thought of as a discrete sector. Rather, all companies must have a cybersecurity awareness and plan in order to win and, in some cases, to even compete for business opportunities.
    - Cybersecurity is one of the fastest growing areas within the technology sector. Based on data from the U.S. Bureau of Labor Statistics' Information Security Analyst's Outlook, cybersecurity jobs are among the fastest-growing career areas nationally. The BLS predicts cybersecurity jobs will grow 31% through 2029; a rate that is over seven times faster than the national average job growth of 4%.
    - Cybersecurity Ventures predicts global spending on cybersecurity products and services will exceed $1 trillion cumulatively over the five-year period from 2017 to 2021.
    - Cybersecurity The global cybersecurity market size is forecast to grow to $345.4 billion U.S. dollars by 2026.
    - Indiana's largest assets are Academia and Innovation and Entrepreneurship (per IEDC report found in supporting documentation section).
    - These conclusions led the working group to establish a preliminary declaration of its group ethos and mission that reads as follows**:**
    - Indiana's vibrant economy is based on a secure, stable environment. Today, in addition to physical security and fiscal stability, individuals and companies must be able to rely on cybersecurity to grow, invest, and prosper.
  - Economic development is advanced by:
    - Attracting and growing companies in all sectors by demonstrating Indiana's technical infrastructure readiness, backed by its commitment to safeguard that infrastructure.
    - Encouraging collaboration amongst companies and institutions on information protection strategies; and
    - Considering and proposing policy recommendations to (a) support the attraction and growth and (b) promote further growth of existing cybersecurity companies.

  - Economic success is defined through both qualitative and quantitative metrics that focus on:
    - New business starts and attractions
    - Support to new start-ups
    - Retention of existing businesses
    - Number of new cybersecurity jobs created
    - Number of non-cyber jobs created to support new cyber business
    - Average salary of jobs created
    - New employee demographics (workforce diversity, education levels, etc.)
    - Retention of cybersecurity professionals who graduate from one of the State's universities or colleges, who accept Indiana-based cyber employment

- **Additional Findings**
  - Among several data points , one important finding during the working group's research showed that Hoosiers believe the most important role of government in cybersecurity business development is positive economic climate, strategic leadership, and business incentives.

- **2021 Committee Deliverables**
  - Incentive Program
  - Cyber Business Attraction Package
  - Cybersecurity Maturity Model Certification (CMMC) Outreach Plan

- **Additional Notes/Way Ahead:**
  - The Economic Development working group will consider the following strategy and make recommendations around at least four discrete lines of effort that align to the Governor's Five Strategic Pillars:


SUPPORT TO INDIANA STRATEGIC GOALS
Cybersecurity Lines of Effort
Governor's Five Strategic Pillars
LOE 1: BUSINESS DEVELOPMENT
LOE 2: RESEARCH INVESTMENT
LOE 3: TALENT CULTIVATION
LOE 4: IDENTITY CREATION
Cultivate a Strong & Diverse Economy
Fund a Long-Term Road & Bridge Plan
Develop a 21st Century Skilled & Ready Workforce
Attack the Drug Epidemic
Provide Great Government Service at a Great Value

- **References**

  - IEDC Cyber Initiative Report 2017
  - Mlitz, Kimberly, Cybersecurity Market Revenues Worldwide, 2021-2026
  - Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed $150 Billion in 2021 - https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem
  - Morgan, Steve, http://cybersecurityventures.com/cybersecurity-market-report/
  - “Cyber Threat: Indiana’s Call to Action,” Anita Nerses (Raytheon), Inside Indiana Business, August 9, 2017. Cyberpoint Technology & Innovation Center proposal to City of Baltimore
  - “Uncharted: New Partners Team up as Georgia Stakes its Claim on Cyberleadership,” Adam Stone, Government Technology, October/November 2017.
  - Canales, Christian, R. Contu, S. Despande, E. Kim, L. Pingree. Forecast Analysis: Information Security, Worldwide, 2Q15 Update, Gartner, September 08, 2015.
  - Turnaround and transformation in cybersecurity: Key findings from the Global State of Information Security® Survey 2016. PwC, www.pwc.com/gsiss.
  - Emsi Occupational Snapshot Report, Q4 2017. www.economicmodeling.com

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
   a. Local nonprofits have supported students with programs
      - Techpoint (XTERN, Tech Fellowship)
      - Nextech (K-12 computer skills support)

   b. Local companies working with Apprentice University for internships
   c. Purdue Polytechnic High School formation
   d. Additional university accreditations and degree options in computer science
   e. International Securities Services Association (ISSA) and Indiana Systems Audit and Control Association (ISACA) chapters remain active as well as Infragard
   f. K-12 requirements as part of Next Level agenda
   g. Indiana Information Sharing and Analysis Center (IN-ISAC)

2. **What (or who) are the most significant cyber vulnerabilities in your area?**
   a. Small and medium-sized businesses
   b. Small local government entities (schools included)
   c. Insufficient infrastructure
   d. Insufficient workforce

3. **What is your area's greatest cybersecurity need and/or gap?**
   a. Education/Awareness of threat, impact, and opportunity
   b. Workforce development/retention

4. **What federal, state, or local cyber regulations is your area beholden to currently?**
   a. Defense Federal Acquisition Regulation Supplement (DFARS) compliance
   b. General Data Protection Regulation (GDPR) based on European Union's General Data Protection Regulation
   c. National Institute of Standards and Technology (NIST)
   d. Health Insurance Portability and Accountability Act (HIPAA)

5. **What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
   a. Baltimore, Maryland, and local cooperation with National Security Agency (NSA)
   b. Michigan Economic Development Corporation
   c. Georgia Cyber Innovation and Training Center
   d. Rhode Island Corporate Cybersecurity Initiative
   e. Cyber California

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. IEDC Cyber Initiatives
   b. Cyberpoint Technology & Innovation Center proposal to City of Baltimore
   c. "Uncharted: New Partners Team up as Georgia Stakes its Claim on Cyber Leadership," Adam Stone, Government Technology, October/November 2017.
   d. "Cyber Threat: Indiana's Call to Action," Anita Nerses (Raytheon), Inside Indiana Business, August 9, 2017.
   e. Kentucky State Research

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
   a. Public Private Partnership (P3) Investment in cybersecurity incubators and accelerators

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

	Year 1	**Year 3**	**Year 5**
New businesses starts and attractions	1	5	10
Support to new start-ups	P3 formed or identified	Innovation Center established	
Number of new cybersecurity jobs created	10	75	250
Average salary of jobs created	$90,000	$100,000	$110,000
Minority & Female Participation	>5%	>10%	>25%
Retention of cybersecurity professionals who graduate from one of the State's universities or colleges, who accept Indiana-based cyber employment	50	150	250

9. **What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?**
   a. Need to define exactly what the State wants to be in cyber (e.g., security of smart mobility, energy grid, defense, manufacturing, agtech, fintech, insurance tech, bio/health) to focus growth and allocation of resources
   b. Public Service Announcements (PSA) for awareness
   c. Educate educators
   d. Cyber clubs K-12 and track talent
   e. Identify current assets and capabilities better (e.g., INFRAGARD, Henry St. DHS)
   f. Publicize this Council and their efforts
   g. Utilize and promote the Information Sharing and Analysis Center (ISAC) as a tool

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. Indiana based cyber-focused companies
    b. Cyber-focused companies with office in Indiana
    c. Companies that do cyber but not as their primary focus
    d. Cybersecurity workforce using the updated tools from DWD using CyberSeek.org

11. **What do we need to do to attract cyber companies to Indiana?**
    a. Recommended Policy and State government considerations:
       - What marketing or branding can be used to coalesce messaging? Digital Crossroads or Cyber Crossroads?
       - Can IN.GOV website note "Tech" or "Cyber" in tandem with Business and Agriculture?
       - What would be the impact of eliminating or narrowing non-compete agreements?

    b. Recommended infrastructure investments:
       - Cybersecurity tech park and/or innovation center, which would include:
         - Sensitive Compartmented Information Facility (SCIF)
         - Co-work area
         - Accelerator aspect
         - Cyber-range
         - K-12 programming
         - Expanded 5G wireless
         - High-speed fiber
         - Small Cells
         - Resilient Grid (strategic location and control of battery and gen-sets for critical infrastructure)

    c. Recommended incentives for consideration:
       - Incentives for companies that move into the state that can demonstrate compliance with NIST standards (theory: secure companies present less burden and risk to the public)
       - Incentives for purchasing products and services from state-based companies
       - Must be Hoosier businesses to bid on state and local government cybersecurity products and service RFQs so long as products and service offerings are substantially similar to other commercially available options
       - Tax deduction for companies that make or have made investments in their digital security structure
       - Subsidize cost of Small and Medium Business (SMB) use of IN-ISAC.
       - Cybersecurity Investment Incentive Tax Credit
         - "A refundable tax credit is available for a minimum investment of $25,000 in a qualified Maryland Cybersecurity Company (QMCC). The credit is claimed by the QMCC. The QMCC may be allowed a tax credit of up to 33% of an eligible investment, up to $250,000."
         - Note: Indiana's Venture Capital Investment Tax Credit (VCI) is 20 percent, up to $1 million.

12. **What are your communication protocols in a cyber emergency?**
    Not applicable.

13. **What best practices should be used across the sectors in Indiana?**
    a. Use NIST standards for definitions
    b. Increase awareness and messaging of threat and opportunity

Deliverable: Investment

Deliverable: Investment

General Information

1. **What is the deliverable?**
   a. Develop a framework of potential economic development support for Indiana businesses seeking to improve their cybersecurity posture and thrive in the federal cybersecurity environment.

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.**
   a. Strengthen best practices to protect information technology infrastructure.
   ☐ 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. It is the goal of this working group deliverable to develop an economic development framework that supports investment in Indiana businesses engaging in the cybersecurity landscape. The resulting action or modified behavior of this deliverable would be the improved cybersecurity posture and success of Hoosier businesses.

6. **What metric or measurement will be used to define success?**
   a. Success will be defined by the deployment of an economic development framework that the IEDC can use to invest in new companies that begin in, or move to, Indiana as well as those existing Indiana companies seeking to improve their cybersecurity preparedness.

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

8. **Who or what entities will benefit from the deliverable?**
   a. Indiana businesses and businesses considering starting or locating in Indiana

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. Defense Industrial Committee, Cyber Awareness and Sharing Working Group, Workforce Development Committee

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. IEDC

12. **Who should be main lead of this deliverable?**
    a. IEDC Chief Innovation Officer

13. **What are the expected challenges to completing this deliverable?**
    a. Funding and legislative priorities

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
Research market needs around cybersecurity	IEDC	0%	June 2022	

Research other successful business investment and support programs	Economic Development committee	0%	June 2022	
Meet with IEDC executive team	Economic Development committee	0%	December2022	
Put together framework recommendation	Economic Development committee	0%	January 2023	

Resources and Budget

15. Will staff be required to complete this deliverable?

☒No ☐ Yes

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
None						

Benefits and Risks

17. What is the greatest benefit of this deliverable?

a. This initiative will encourage cybersecurity investments in the state of Indiana by companies looking to start, grow, or relocate in Indiana.

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

a. By developing a framework for economic development support of businesses in relation to cybersecurity, the cybersecurity of the entire State will be enhanced and business resiliency improved.

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

a. By not developing a framework for economic development support and investment in improvements in the cybersecurity posture of Indiana businesses, the State risks a scattered and uncoordinated approach to cybersecurity development and support.

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

This may be the most challenging piece of this program. There are many frameworks available, but not all companies must subscribe to the same ones. Therefore, it may prove difficult to make direct comparisons across industries. The baseline should be reflective of today’s business environment

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

    a. Further research will be needed to validate the answer to Question #9 above. This research would then also identify potential jurisdictions that could be used as a control.

Other Implementation Factors

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

    a. No common definition of acceptable cybersecurity measures and several frameworks and models

    b. The desire of this subcommittee to not require audits and rely on self-reporting which may not prove to be reliable

    c. Not enough funding to support future investments

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

    ☐No ☒ Yes

    a. Regulation and policy may be required to create and enable potential new support framework.

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

    a. No Response

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

    a. No Response

27. **Can this deliverable be used by other sectors?**

    ☐No ☒ Yes

    a. There could be potential overlap with the Workforce Development Committee and Defense committee.

Communications

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

a. Not known

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. No response.

Evaluation Methodology

Objective 1: The Economic Development Committee with the IEDC will develop an economic development support framework for Indiana companies to thrive in the cybersecurity landscape 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

Objective 2: Companies that move, start, or grow here will have a framework for economic development support 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: Leadership

Deliverable: Leadership

General Information

1. What is the deliverable?

Leverage and raise awareness of the resources available from Indiana academic institutions, defense assets, private sector, and governmental entities to promote Indiana's thought leadership in innovation and cybersecurity.

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. Highlight and support the research and capabilities of Indiana defense assets, private sector partners, governmental entities, and universities such as Purdue, IU, Notre Dame, Rose Hulman, Butler, Ivy Tech, etc. as it relates to cybersecurity to position Indiana as a thought leader on the national stage.
6. **What metric or measurement will be used to define success?**
    a. The best indicator of success will be increased awareness of State programs and interactions with public-private partners, out-of-state cybersecurity influencers, and governmental entities.

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

8. **Who or what entities will benefit from the deliverable?**
    a. New and existing businesses, Indiana universities, and Hoosiers across the State would benefit from a position as a cybersecurity thought leader and convener of discussions around cybersecurity research, innovation, and technology.
9. **Which state or federal resources or programs overlap with this deliverable?**
    a. No response

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

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. Defense development, Homeland security, DOD, Department of Commerce, SBA and others all have a role to play in cybersecurity leadership and awareness building.

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

13. **What are the expected challenges to completing this deliverable?**
    a. Many states and cities are competing in this area. Standing out of the crowd will be difficult for a non-traditional cybersecurity locale such as Indiana.

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
Generate list of highlights and support activities	ED Subcommittee	10%	December 2022	
Lend IEDC backing/support to select initiatives & activities	ED Subcommittee	10%	December 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
1	N/A	IEDC	State	N/A	Existing staff that interact with cybersecurity activities

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

a. No response

Benefits and Risks

17. What is the greatest benefit of this deliverable?

a. Greater awareness of Indiana’s position as a thought leader on cybersecurity issues.

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

a. Risk mitigation is achieved by increasing general public awareness, encouragement of growth in the sector, implementation of remedial and preventative measures by government and business, and promotion of proper cyber hygiene.

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

a. Indiana could be passed by other States seeking to establish a reputation as cybersecurity focused.

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

a. Greater awareness of cybersecurity thought leadership and activities – number of support initiatives tied 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

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. No Response

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. Recommendations from this subcommittee and others through the cyber community are needed for the strategies to remain timely.

26. **Who has the committee/working group contacted regarding implementing this deliverable?**
    a. Indiana academic institutions, private sector partners, and governmental entities.

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. All

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. This list should emphasize cyber-related events and updates

Evaluation Methodology

Objective 1: Indiana Economic Development Corporation and Committee will work to identify potential partners, activities, and initiatives of cybersecurity influencers in the State of Indiana 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

Objective 2: Measure the effectiveness of IEDC supported activities and initiatives in the cybersecurity space 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: Technical Assistance

Deliverable: Technical Assistance

General Information

1. **What is the deliverable?**
   a. Address the growing need for small businesses to deploy cybersecurity best practices by delivering technical assistance programming and services through the IEDC and its partners.

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. Develop a plan for the implementation of technical assistance programs that will assist small businesses with cybersecurity awareness and outreach, assessment tools, training opportunities, and direct support with CMMC Level 1 implementation.

6. **What metric or measurement will be used to define success?**
   a. Clients Assisted or spoken with Level 1- 40-60 – stretch goal (Fully implementing CMMC L1 controls).

   Note: depending on level of assistance needed, the level of companies assisted can fluctuate.

7. **What year will the deliverable be completed?**

   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

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

9. **Which state or federal resources or programs overlap with this deliverable?**
   a. DLA (DoD) manages the CMMC process. Any potential overlap may come from third party vendors or other federal agencies who may provide additional resources that could be applicable to CMMC (i.e., MEP, SBA).

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Defense Industrial Committee and Cyber Awareness and Sharing 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. IEDC and Purdue University

12. **Who should be main lead of this deliverable?**
    a. IEDC: Bryan Langley and Chris Jeffers

13. **What are the expected challenges to completing this deliverable?**
    a. Formulating an outreach plan that will adequately addresses a fluctuating training program, with an increased demand and need for Indiana companies, primarily in the area of defense companies.

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
Process to manage support	IEDC/Purdue	100	October 2021	Program is expected to be active in Dec.
Develop outreach plan	IEDC	50%	January 2022	
Implement outreach plan	IEDC with partners	10%	February 2022	
Evaluate effectiveness of outreach plan	IEDC	0%	February 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
No Response	No Response	Existing staff	IEDC		This process has been built in using existing funds

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
Purdue	Already built in					

Benefits and Risks

17. What is the greatest benefit of this deliverable?

a. Support Indiana small businesses to implement cybersecurity best practices such as becoming Level One(L1) Cybersecurity Maturity Model Compliant (CMMC)

18. **How will this deliverable reduce the cybersecurity risk or impact? What are the estimated costs associated with that risk reduction?**
    a. Will involve having more Indiana small businesses trained and aware of cybersecurity best practices, thereby reducing cybersecurity risk. Based on CMMC compliance, that includes a cost that would normally be charged to the businesses. The support we are providing helps them move to L1 certification, so the cost and support is more around getting companies equipped.

19. **What is the risk or cost of not completing this deliverable?**
    a. Indiana companies not being CMMC compliant and losing defense contracts.

20. **What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?**
    a. Based on how many companies we can support through the process, 40-60 companies.

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. No Response

24. **Does this deliverable require a change from a regulatory/policy standpoint?**
    ☒No ☐ Yes
    a. No, however additional support from the state will help us increase the resources available to companies, although the cost of being cybersecurity prepared falls primarily on the company.

25. **What will it take to support this deliverable if it requires ongoing sustainability?**
    a. Both federal and state funding.

26. **Who has the committee/working group contacted regarding implementing this deliverable?**
    a. Indiana small businesses, the IEDC and Purdue customers and vendors

27. Can this deliverable be used by other sectors?

☐No ☒ Yes

a. Any committee that works with businesses and eventually, government sectors

Communications

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

a. Indiana small businesses and IEDC stakeholder groups, to include the IECC. Purdue will also provide information to their clients and customers.

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. Any training program, while primarily for companies who serve the defense industry, could be suitable for all types of industries. So, the reach of the program may be larger than anticipated.
b. The partnership between IEDC and Purdue is unique among most states because we are leveraging available resources to support companies.

Evaluation Methodology

Objective 1: IEDC and partners will develop a cybersecurity technical assistance plan in Indiana 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

Objective 2: Measure the effectiveness of the Cybersecurity technical assistance plan by the number of participants (40) by February2023.

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

- Indiana Economic Development Corporation Cyber Initiative Report

IECC Economic Development Corporation Cyber Initiative Report

INDIANA ECONOMIC DEVELOPMENT CORPORATION

Indiana

A State that Works®

CYBER INITIATIVE

2017

Prepared by Douglass C. Rapp, CISM, for IEDC with special thanks to:

Nick Goodwin, *Chief Strategy Officer*, Indiana Department of Workforce Development

Walter Grudzinski, *Director of Information Security and Business Continuity*, Vectren Corporation

Brandt Hershman, *State Senator, District 7*, Indiana Senate

Christopher Judy, *Representative, District 83*, Indiana House of Representatives

David Lefever, *Chief Executive Officer*, The Mako Group

Steve Lodin, *Senior Director of Cyber Security Operations*, Sallie Mae

Chetrice Mosley, *Indiana Cybersecurity Program Director*, Indiana Office of Technology and Indiana Department of Homeland Security

Chad Pittman, *Vice President of the Office of Technology Commercialization*, Purdue Research Foundation

Joel Rasmus, *Managing Director*, CERIAS at Purdue University

Leon Ravenna, *Chief Information Security Officer*, KAR Auctions

Stephen E. Reynolds, *Partner, Data Security and Privacy Practice*, Ice Miller Litigation Group

David Roberts, *President*, Battery Innovation Center

Dr. Eugene Spafford, *Executive Director Emeritus*, Purdue CERIAS

Nick Sturgeon, *IN-ISAC SOC Manager*, State of Indiana

Dr. Robert Templeman, *Senior Fellow*, Center for Applied Cybersecurity Research

J.J. Thompson, *Founder/Chief Executive Officer*, Rook Security

Tony Vespa, *Founder/Chief Executive Officer*, Vespa Group

Brad Wheeler, *Chief Information Officer*, Indiana University

THE OPPORTUNITY

The conditions for successful economic development in cybersecurity are incredibly strong in Indiana. Indiana possesses the right resources to become a driving force in the cybersecurity industry and emerge as a recognized world leader in cybersecurity research and innovation.

Indiana advantages include

- A strong talent pipeline stemming from over 50 colleges and universities
- A vibrant entrepreneurship/innovation culture
- A State Executive Counsel on Cybersecurity[1]
- World renowned research facilities and personnel
- A long history of pioneering innovation in the field
- A strong and collaborative cybersecurity community
- Unique military assets and businesses
- Expert training and exercises

Indiana needs only to foster the community and leverage existing strengths to achieve greater success.

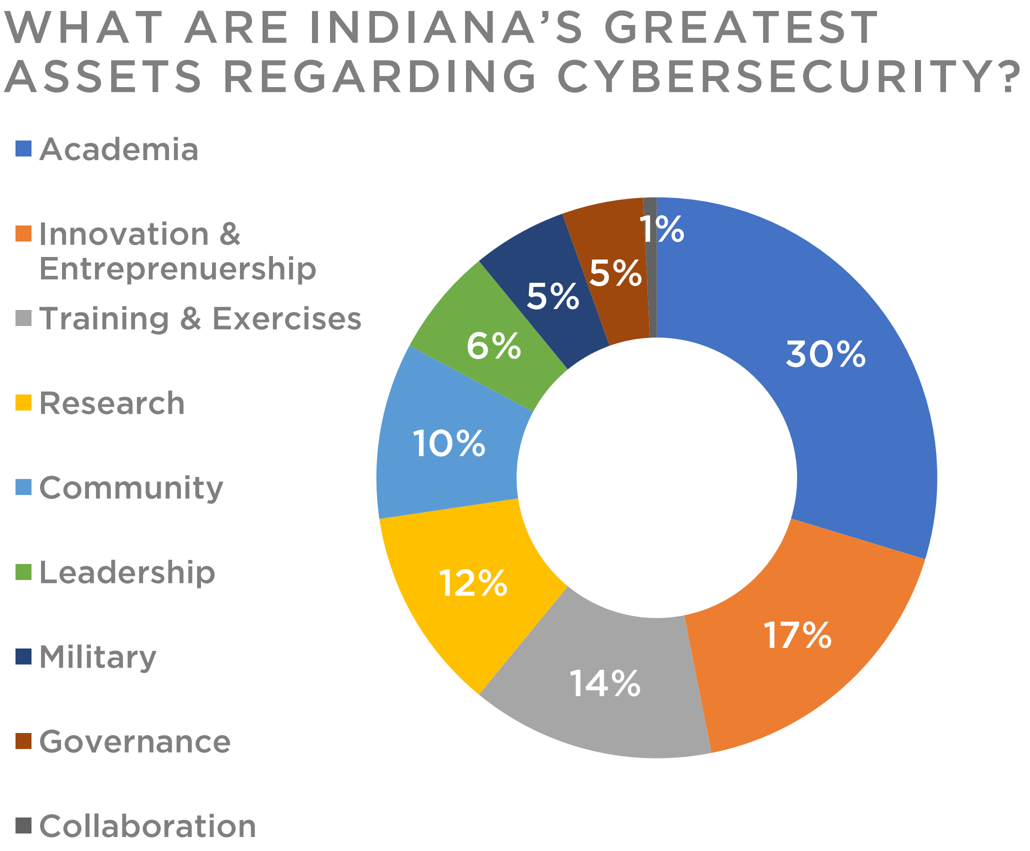


Figure 1. Indiana cybersecurity industry survey results on greatest assets.

[1] See Annex A: Executive Council on Cybersecurity

MARKET OVERVIEW

Cybersecurity is the fastest growing area within the technology sector and one of the fastest growing industries worldwide. The global cybersecurity market has grown roughly 35 times in 13 years going from $3.5 billion in 2004 to $120 billion in 2017[2] and industry experts predict that growth will continue 8-15% each year for the next five years. Global spending on cybersecurity products will eclipse a cumulative $1 trillion in the same period[3]. The market will continue to grow at a comparable rate to the growth of the Internet/Internet of Things.

To combat the ever-expanding number of threats and complexity of off-the-shelf attacks, companies are investing more than ever into Cybersecurity. Worldwide spending on cyber security reached $75.4 billion in 2015 and shows no sign of slowing[4]. The continued proliferation of cyber threats is driving so much spending on cyber security that it has become difficult for industry analysts to keep up. Industry surveys have indicated that respondents are increased their cybersecurity budgets roughly at an average of 24% in 2015[5] and show no signs of slowing down. Many businesses are spending much more. J.P. Morgan & Chase has doubled its budget to a record $500 million and Bank of America has stated publicly that they have no set budget– they will invest what it takes to secure their company. The U.S. Government has committed to a record 35% spending increase to $19 billion in 2017[6].

Challenges

Cybersecurity has only recently been recognized as a market. Research is complicated by the fact that it is neither a defined industry by the North American Industry Classification System (NAICS) nor the Standard Industrial Classification (SIC). Occupation codes by the Standard Occupational Classification (SOC) system are only now starting to be developed[7]. These codes are important because they are used by federal agencies such as the Bureau of Labor Statistics and Census Bureau to classify workers and employers in the vast amounts of public data they publish.

Contributing to industry confusion is the fact that there is no standard definition for cybersecurity, thus past and current reports rely heavily upon the reporter's individual definition and interpretation. A company that specializes in cybersecurity may currently be classified as a software firm, a consulting firm, or a security firm. Organizations routinely employing sizable cybersecurity staff include financial institutions, healthcare organizations, law firms, utilities, educational institutions, retail enterprises, and manufacturers yet are not necessarily considered in reports regarding the cybersecurity industry. A cybersecurity professional may be classified as an information security architect, computer network architect, security consultant, computer and information systems manager, or simply an "IT technician".

[2] Ross, Alec. "Want job security? Try online security". Wired, April 25, 2016.
[3] Morgan, Steve. Cybersecurity Market Report, Q1 2017. http://cybersecurityventures.com/cybersecurity-market-report/
[4] Canales, Christian, R. Contu, S. Despande, E. Kim, L. Pingree. Forecast Analysis: Information Security, Worldwide, 2Q15 Update, Gartner, September 08, 2015.
[5] Turnaround and transformation in cybersecurity: Key findings from the Global State of Information Security® Survey 2016. PwC, www.pwc.com/gsiss.
[6] Morgan, Steve. Cybersecurity Market Report, Q1 2017. http://cybersecurityventures.com/cybersecurity-market-report/
[7] There are currently no NAICS or SIC codes associated with the keywords cybersecurity or information security.

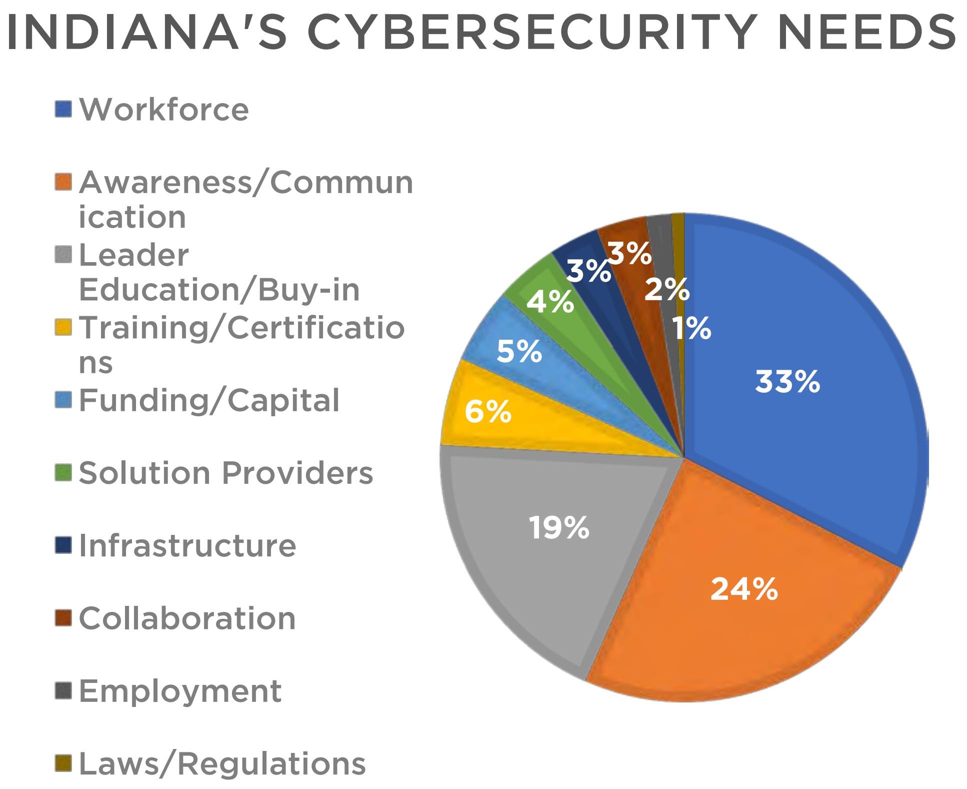


Figure 2. Indiana cybersecurity industry survey results on greatest cybersecurity needs.

Despite numerous advantages, Indiana faces several challenges that will need to be addressed for the State to achieve a dominant position in the marketplace and to accomplish strategic goals. According to a cyber security industry survey conducted by the Indiana Economic Development Corporation (IEDC)[8] in 2016-2017, Indiana challenges include:

» Attraction and retention of cybersecurity talent
» Access to funding/capital
» C-Suite/Executive level education and buy-in
» Increased local solution providers
» Investment in cybersecurity infrastructure
» Local access to training and certifications
» Increased collaboration through public/private partnerships (P3)
» On-going support of existing expertise and resources
» Cybersecurity awareness and communication

[8] See Annex B: Indiana Economic Development Corporation Cybersecurity Survey

The Goal

Indiana's continued economic success in the cybersecurity market lies in its core strengths of creating and applying things or being "a State that Works", its outstanding business climate, and willingness to embrace technology and emerging markets.

Establish Indiana as a world leader in cybersecurity and the nucleus of cybersecurity in the region.

Success will be identified through both qualitative and quantitative metrics that focus on

1) The attraction of new businesses to the State
2) Support to new start-ups within the State
3) The retention of existing businesses within the State who may be exploring moves
4) The number of new cybersecurity jobs created
5) The number of non-cyber jobs created to support new cyber business
6) The salary of jobs created
7) New employee demographics (workforce diversity, education levels, etc.)
8) Lessening the "Brain-Drain" by increasing the number of cybersecurity professionals who graduate from one of the State's universities or colleges, who accept Indiana-based cyber employment

The Strategy

The strategy for Indiana economic development within cybersecurity is grounded in market research at the state, national, and international levels. Through research, industry engagement, asset inventory, and SWOT analysis, four strategic lines of effort were identified.

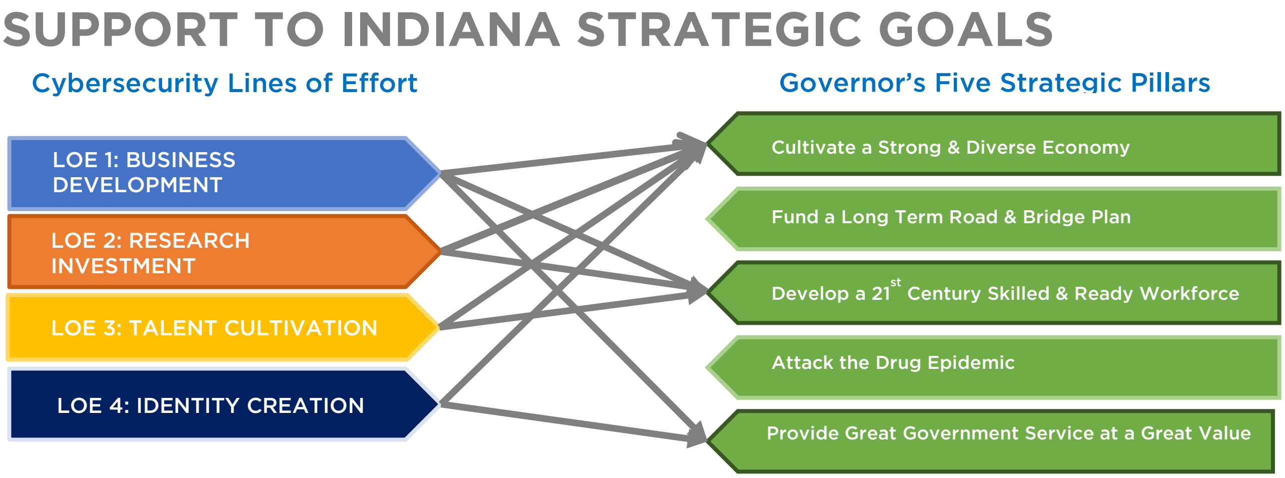

SUPPORT TO INDIANA STRATEGIC GOALS
Cybersecurity Lines of Effort
Governor's Five Strategic Pillars
LOE 1: BUSINESS DEVELOPMENT
LOE 2: RESEARCH INVESTMENT
LOE 3: TALENT CULTIVATION
LOE 4: IDENTITY CREATION
Cultivate a Strong & Diverse Economy
Fund a Long Term Road & Bridge Plan
Develop a 21st Century Skilled & Ready Workforce
Attack the Drug Epidemic
Provide Great Government Service at a Great Value

Figure 4. Cybersecurity lines of effort support to Indiana Strategic Goals

Line of Effort 1: Business Development

The business development line of effort (LOE) is rooted in the fundamentals of business development strategy.

- Business recruitment/attraction
- Business retention/expansion
- Business creation (innovation and entrepreneurship)
- Creativity and talent cultivation
- Place-making

The strategy will focus on defining and developing strategies/plans for industry clusters, developing a regional strategy/plan, creation of demand/retention of wealth, retaining and expanding cybersecurity businesses, leveraging existing military facilities and expertise, and investing in innovation and entrepreneurship.

Immediate progress can be made through investment into Indiana cyber companies with resources allocated under the State of Indiana's $1B innovation and entrepreneurship initiative and other tools. By doing so, Indiana will help relieve banking limitations caused by a lack of physical assets to secure lending[9], reduce risk associated with investors who don't understand cybersecurity, and reduce the barriers in attracting non-pillaging investment from out of state investors to fuel A and B round growth. Additionally, we can increase success of Indiana cybersecurity companies by adopting an "Indiana first" policy in State and local government.

Mid- and long-term strategies for business attraction will focus on large cybersecurity company relocation, and on attracting research and development offices from big companies that are not ready to relocate to Indiana. We will create an environment to unlock intellectual property from these companies that will seed synergistic industry clusters through start-ups[10].

Line of Effort 2: Research Investment

Research and development drives economic growth. These activities allow researchers and scientists to develop and apply new knowledge, techniques, and technologies. As technology evolves, productivity increases and businesses can produce more with fewer resources. Indiana is home to three prominent R1 universities (Indiana University/Bloomington, Notre Dame University and Purdue University/West Lafayette) who have major R&D initiatives in cybersecurity, but active and productive cyber research is also conducted at several other Indiana schools, including Ball State, Indiana State University, Indiana University–Purdue University at Indianapolis, Indiana–Purdue University Fort Wayne and Purdue University/Calumet. Five NSA/DHS Centers for Academic Excellence are headquartered at Indiana-based institutions of higher education.

[9] Traditional company valuation relied on heavily on physical assets. As newer business models evolve, investors are beginning to recognize services, technology creation, and network orchestration as important components in determining value.

[10] Sometimes referred to as a "Cluster Effect". An example of this is the 45+ information security companies that emerged from Internet Security System and SecureIT in Atlanta, GA.

"Leading in cybersecurity requires fast-paced innovation in technology, policy, and practice. Indiana has the deep strengths in its research universities, partnerships, and workforce for firms to thrive in the heartland."
Brad Wheeler, CIO, Indiana University

The strategy in this line of effort will concentrate on

» Support to research consortiums
» Increase contracting capacity to government
» Establish a presence in both national and international strategic markets
» Foster collaboration on grant writing/funding efforts
» Make clear, visible commitments to people and institutions in the field

Line of Effort 3: Talent Cultivation

Cybersecurity is experiencing a significant shortage of practitioners. Conservative estimates indicate over a quarter-million positions currently sit unfilled in the US alone, and a shortage of 1.5 million cybersecurity professionals is predicted by 2019[11]. The ability to produce and retain cybersecurity talent will give Indiana a distinct market advantage. Indiana currently produces a significant number of cybersecurity professionals and possesses the assets to create more. Indiana advantages include:

» 30+ colleges and universities with specific cybersecurity/information security degrees, certificates programs, or course work[12]
» 72 schools in Indiana producing graduates with competencies related to becoming a Cyber Security Analyst over the last 5 years[13]
» 70+ middle and high school Cyber Patriot teams in Indiana[14]

The strategy for this line of effort will focus on collaborating with the Department of Workforce Development, academia, and industry to create a comprehensive cybersecurity talent pipeline strategy, incentives to attract/retain talent, utilizing data to strategically determine workforce needs, and supporting K-12 cybersecurity initiatives.

[11] Morgan, Steve. "Cybersecurity job market to suffer severe workforce shortage." CSO Online, July 2015, http://www.csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html

[12] Asset Inventory conducted by the Indiana Economic Development Corporation.

[13] Emsi Occupation Snapshot Report. Cyber Security Analyst in Indiana. Emsi Q1 2017 Data Set, www.economicmodeling.com

[14] List provided by Cyber Patriot.

"By far, our greatest assets in Indiana are the skilled talent we have access to. There are pockets of highly accomplished individuals who set the tone for the cyber environment in our state, and really the entire mid-west. This also holds true for the potential talent pool that is up and coming due to the dedication of State of Indiana's economic development initiatives."

David Lefever, Chief Executive Officer
The Mako Group

While there is a growing interest in cybersecurity at the 8-12 grade levels, few of Indiana's secondary education districts have relevant computer programming or cybersecurity programs.
An investment in middle and high school level educational initiatives could provide a dramatic payoff by influencing Indiana students to choose to pursue a cyber career path. While Indiana's colleges and universities are at the forefront of cyber education and research, many of its students are non-Indiana citizens who graduate and leave the state. An investment in grade 8-12 CS/Cyber programs would increase the number of future college-educated CS/Cyber professionals seeking career jobs in Indiana. IEDC should work with the Department of Education and the Department of Workforce Development to strengthen Indiana's commitment to preparing students for this growing, high-paying industry.

Understanding and enhancing the work-life culture that is important to the attraction and retention of cybersecurity talent will be a critical component of this LOE.

Line of Effort 4: Identity Creation

The State of Indiana has been very successful at branding itself as "The State That Works." Indiana has long since recognized the value of a strong brand identity. By synchronizing with the current brand campaign, Indiana will create a brand/identity for Indiana economic development efforts in cybersecurity. Key qualities and benefits this brand include:

» Indiana is a State that creates and applies cybersecurity (a "State that Protects")
» Indiana is a state that understands and excels in collaboration between government, academia, and private industry
» Indiana is a State that welcomes and recognizes the value of diversity
» Indiana's business environment creates a competitive advantage for our businesses
» Indiana is a great place to live, work, and play

By synchronizing this messaging and branding strategy within the Indiana cybersecurity sector, Indiana will illustrate a comprehensive approach to demonstrating benefit. Indiana will strategically target regionally (Midwestern states with an economic climate that is less business-friendly than Indiana), nationally and internationally, and leverage relationships with industry, academia, and the military to expand opportunities.

"Driving economic development by bringing together resources from top flight schools, state government and business is but one benefit in the fight against cyber criminals that can impact every person and business. That's what Indiana does!"

Leon Ravenna, Chief Information Security Officer
KAR Auctions

IMPLEMENTATION

Line of Effort 1: Business Development

1.1 Cluster Strategy: Services, Forensics, ICS/SCADA, SIoT (Manufacturing integrity/Sensors)

Managed Security Services

Cybercrime continues to drive the consumer cybersecurity market and high growth areas in managed security services are predicted to be analytics/SIEM (10%); threat intelligence (10%); mobile security (18%); and cloud security (50%)[15]. It is imperative that Indiana attracts, nurtures and sustains companies and offers initiatives that foster cybersecurity solutions for small to midsize businesses as they historically have been the most vulnerable and generated the most risk.

Digital Forensics

The global digital forensics market was worth $2 billion in 2014 and is predicted to reach $4.9 billion by 2021. Market growth is projected to be 12.5% CAGR from 2015 to 2021[16]. Indiana has numerous unique assets in digital forensics including Purdue University's internationally lauded Cyber Forensics Laboratory and a high concentration of digital forensic expertise within the Indiana State Police and other entities.

Industrial Control Systems (ICS)/Supervisory Control and Data Acquisition (SCADA)

Increasing attacks on critical infrastructure such as power, water, oil and gas, manufacturing, transportation, and others is the major force driving the ICS security market. The Industrial Control Systems (ICS) security market size is estimated to grow from $9 billion in 2016 to $12.6 billion by 2021, at a Compound Annual Growth Rate

[15] IDC Report. http://www.idc.com/

[16] Digital Forensics Market - Global Industry Analysis, Size, Share, Growth, Trends and Forecast 2016 – 2026. Transparency Market Research, July 30, 2015, http://www.transparencymarketresearch.com/digital-forensics-market.html

(CAGR) of 7%[17]. With Indiana leading the nation in manufacturing job growth -- home to both the second largest automotive industry in the nation and unique capability facilities such as the Muscatatuck Urban Training Center (MUTC) —Indiana has the environment to increase innovation and its leadership within this market segment.

Securing the Internet of Things (SIoT)

IoT security is continually evolving and is ~~both~~ the responsibility of both the government and the private sector. Indiana's chief roles in the SIoT is to provide tools and resources to businesses that incorporate security into product development, improve security to consumer and vendor-managed devices, and secure the infrastructure that enables these devices. Serving as a catalyst for SIoT efforts in Indiana are the research at Indiana University School of Informatics and Computing, at Purdue's CERIAS, and the high level of expertise Crane Naval Surface Warefare Center.

1.1.1. Action: The IEDC needs to create cluster organizations and solicit cybersecurity action plans by convening economic development entities, industry, academia, military, and innovation/entrepreneurship leaders. Plans should be solicited by region (regional cities) and should be competitive for State resources.

1.2 Create a community and communicate efforts.

1.2.1. Action: Indiana needs an industry organization to organize cluster activity, assist the IEDC in execution of the Strategic Cybersecurity Economic Development Plan, partner with both IEDC and DWD on synchronizing talent development activities, represent industry interests, create and execute industry events, and disseminate industry information.

1.2.2. Action: Indiana needs to build a significant cybersecurity conference that showcases existing talents and assets within the State. This event should be industry driven but supported by the State.

[17] Industrial Control Systems (ICS) Security Market by IT Solution, by IT Service (Risk Management Services, Design, Integration and Consulting, Managed Services, and Audit and Reporting), by Vertical & by Region - Global Forecast to 2021. marketsandmarkets.com, July 2016.

WHERE DO YOU GET YOUR INFORMATION CONCERNING STATE CYBERSECURITY EFFORTS?

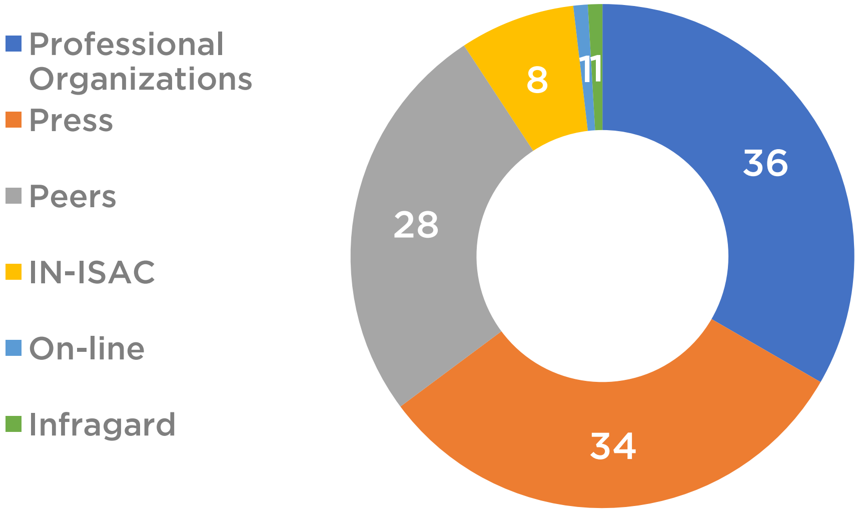


Figure 5. Indiana cybersecurity industry survey results on State information.

1.3 Create Demand/Retain Wealth

1.3.1 Action: Invest in a resource center that provides security solutions to our most vulnerable businesses. According to the National Small Business Association, Indiana small businesses employ 45.5% of our workforce[18]. Small business is the most susceptible business sector to cybercrime as they generally cannot afford to in-house cybersecurity talent and there are fewer providers that offer affordable scaled solutions. Studies have indicated that up to 60% of small business fail within 6 months of a significant cyber incident such as a breach or ransomware[19]. Coupled with the cost of complying with rising information security requirements mandated in regulations such as Defense Federal Acquisition Regulation Supplement (DFARS), the European Union's General Data Protection Regulation (GDPR) and others, many business are accepting risk of and transferring that risk to everyone that they do business with.

Indiana should invest resources available from government, academia, and the private sector to form P3 entities which specifically address the risk to small and mid-sized business. Indiana should fuel demand by educating businesses on vulnerabilities and secure wealth by mitigating costs associated with cybersecurity incidents.

1.4 Innovation and Entrepreneurship

1.4.1. Action: Attract or create a cybersecurity accelerator with a proven business model to become self-sustaining[20]. The accelerator should have partnerships with both academia and private industry to unlock and transfer intellectual property to the market.

[18] Small Business Profile – Indiana. U.S. Small Business Administration, Office of Advocacy, 2017.

[19] National Cyber Security Alliance (NCSA) and Symantec Annual Survey, http://www.staysafeonline.org/stay-safe-online/resources/

[20] Accelerators should specifically be fixed-term, cohort-based programs that include formal educational and mentorship components, facilitate opportunity to access sufficient capital and culminate in public pitch or demo day. Examples can be found at the Seed Accelerators Rankings Project at Rice's Jones Graduate School of Business.

1.5 International Strategy

1.5.1. Action: Create a formal research relationship with key countries (e.g., Israel, India, Singapore, and the "5-Eyes") and develop a strategic plan with quantifiable metrics for cybersecurity business development as part of a larger technology business development plan.

1.6 Regional cluster organization and action plan

1.6.1. Action: Create a formal consortium within the region through partnerships with Illinois, Ohio, Michigan and Northern Kentucky. Conduct a detailed asset inventory and an action plan for attracting cybersecurity talent and businesses to the Midwest to compete against other markets.

1.7 Leveraging Military Assets

1.7.1. Action: Unlock the potential of our statewide military assets by engaging elected and appointed officials to reduce regulatory barriers associated with private industry use. Invest in infrastructure at the Muscatatuck/Atterbury cyber physical range to attract private entity utilization. Invest in infrastructure at Westgate so that NSWC Crane can expand workforce into the technology park. Invest in and enhance infrastructure at Baer Field and Terre Haute Air National Guard Bases to leverage both intelligence and security operations center assets. Invest in other installations and assets as they are identified.

1.8 Identifying Factors Affecting Business Growth and Retention

1.8.1. Action: Determine other factors that would cause businesses to establish in states other than Indiana, and develop strategies to address them. This includes potential negative concerns (e.g., access to coasts, social issues, energy costs), and potential positive issues (cost of living, moderate climate). A plan should be formulated to enhance Indiana's positioning and image in these regards.

Line of Effort 2: Research Investment

2.1 Increase contracting capacity

2.1.1. Action: Support organizations in Indiana that are working to expand or create contracting capacity with priority going to those whose goal it is to leverage Indiana businesses and innovation through the creation of progressive tools such as Other Transaction Authorities. Priority should also be given to consortiums built around tools managed by Indiana entities with minimal facility and administration (F & A) costs.

2.2 Support to research consortiums

2.2.1. Action: Support to cybersecurity research consortiums such as Center for Applied Cybersecurity Research (CACR) at Indiana University and the Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University.

2.3 Establish a stronger presence in Washington, D.C.

2.3.1. Action: Establish a stronger presence in Washington, D.C. to engage the federal Cybersecurity community and facilitate the access of Indiana businesses to the $19B government cybersecurity market.

2.4 Grant Collaboration

2.4.1. Action: Establish leadership by developing grant writing talent that can attract funding from federal sources specifically to support strategic initiatives contained in this plan.

Line of Effort 3: Talent Cultivation

3.1 Cybersecurity talent pipeline strategy.

3.1.1. Action: Support the Department of Workforce Development in utilizing data to strategically determine workforce needs and create a cybersecurity workforce pipeline. Synchronize efforts in research, marketing, and strategy within the cybersecurity sector.

3.2 Incentives to attract/retain talent.

3.2.1. Action: Engage State leadership to create a State Cybersecurity Scholarship. The scholarship could utilize existing education funds and provide ~~a~~ two-year scholarship ($25,000 per year) that stipulates the recipient’s commitment to work in cybersecurity at the State or Indiana local government level for each year the scholarship is accepted[21].

3.2.2. Action: Engage State leadership to create individual tax incentives for cybersecurity professionals living in Indiana, a Federal security clearance cost tax credit, and other creative tools to attract and retain cyber security talent, businesses and research.

3.3 Support to K-12 cybersecurity programs.

3.3.1. Action: Create an organized state-wide cybersecurity competition incorporating other programs such as CyberPatriot and US Cyber Challenge. Establish regional and State level cyber camps leveraging industry organizations, universities, businesses, and military assets[22].

3.3.2 Action: Strengthen the State’s K-12 CS/Cyber educational programs by providing grants to grade 8-12 public schools to implement state-approved CS/Cyber educational programs, and by offering train-the-trainer workshops for K-12 teachers. Offer a state-recognized basic cybersecurity certificate program to all high school students.

Line of Effort 4: Identity Creation

4.1 Collateral

4.1.1. Action: Create cybersecurity economic development web content, single page collateral, multiple page state asset collateral, and branding/display materials.

4.2 Targeted marketing plan

4.2.1. Action: Create a detailed marketing plan targeting cybersecurity businesses in the Washington D.C., Baltimore, San Francisco, New York, Boston, Chicago, Austin,

[21] CyberCorps Scholarship for Service (SFS) has a scholarship targeting federal information assurance professionals. Currently, only Purdue University participates in this program. The Commonwealth of Virginia created the Cybersecurity Public Service Scholarship Program however it is currently unfunded.

[22] Both CyberPatriot and US Cyber Challenge teams exist across the State of Indiana. Indiana should establish a program with camps that utilizes Indiana assets while incorporating teams from these existing programs.

and Atlanta[23]. The plan will be synchronized with other efforts in these geographic areas and will include advertising, industry events, and engagement opportunities.

FUNDING PLAN

Investment strategy for the Indiana Cybersecurity Economic Development Plan is based on core principles:

1. Incentives are tied to the strategic plan.
2. Resources are maximized through industry led initiatives, partnerships, and collaboration.
3. Incentives are performance based with claw back provisions.
4. Supported actions are evaluated on metrics of measured results and outcomes.
5. Supported actions are evaluated on quantitative or qualitative Return on Investment (ROI).
6. An economic and fiscal impact analysis will be conducted on projects as necessary.
7. A cost-benefit analysis will be conducted on projects as necessary.

[23] These cities are generally regarded as having a strong cybersecurity business sector.

Annex A: Executive Council on Cybersecurity

In April 2016, former Governor Mike Pence announced the formation of the Indiana State Executive Council on Cybersecurity (Cybersecurity Council), a comprehensive public-private partnership charged with enhancing Indiana's ability to prevent, respond to and recover from all types of cybersecurity issues, including attacks. The Cybersecurity Council, continued under Executive Order of current Governor Eric Holcomb, includes expertise from public and private partners.

The Cybersecurity Council's goals include formalizing strategic cybersecurity partnerships across the public and private sectors, strengthening best practices to protect information technology infrastructure, and building and maintaining robust statewide cyber incident response capabilities. Indiana is calling on experts in state and federal government, business, Indiana's National Guard, and academia to work together, communicate in a timely manner and share best practices for mitigating cybersecurity threats.

The Cybersecurity Council is currently comprised of 23 members from various public and private sector organizations across the state.

Current Executive Orders can be found at http://www.in.gov/gov/2384.htm.

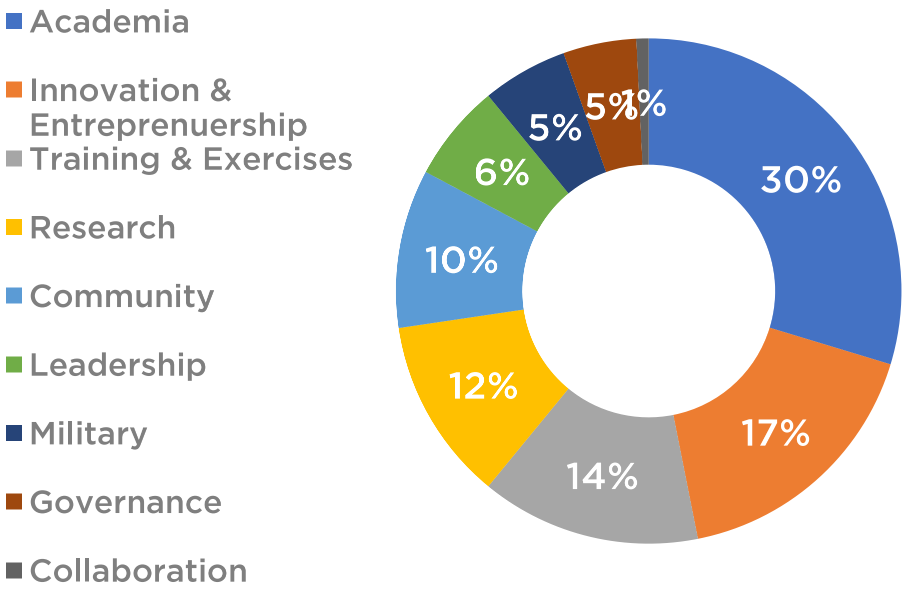
Annex B: Indiana Economic Development Corporation Cybersecurity Survey

The IEDC developed and conducted a cybersecurity industry survey which was distributed in hard copy to participants of the Cybersecurity Town Halls as well as made available online. The purpose of the survey was to

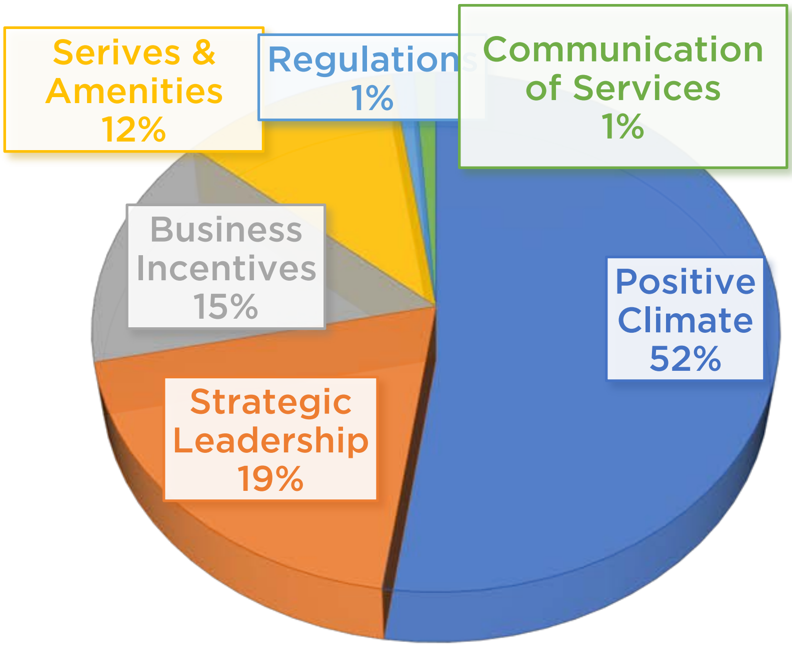
- Determine what motivates and identify issues of concern and interest Indiana's cybersecurity community.
- Receive comments, opinions, and feedback on Indiana cybersecurity environment
- Discuss important topics/issues
- Facilitate an unbiased approach to the development of the Indiana Cybersecurity Economic Development plan
- Conduct an initial asset inventory
    - Create a benchmark to which future results can be compared

Highlights of the survey results that were key to the development of this plan are depicted below.

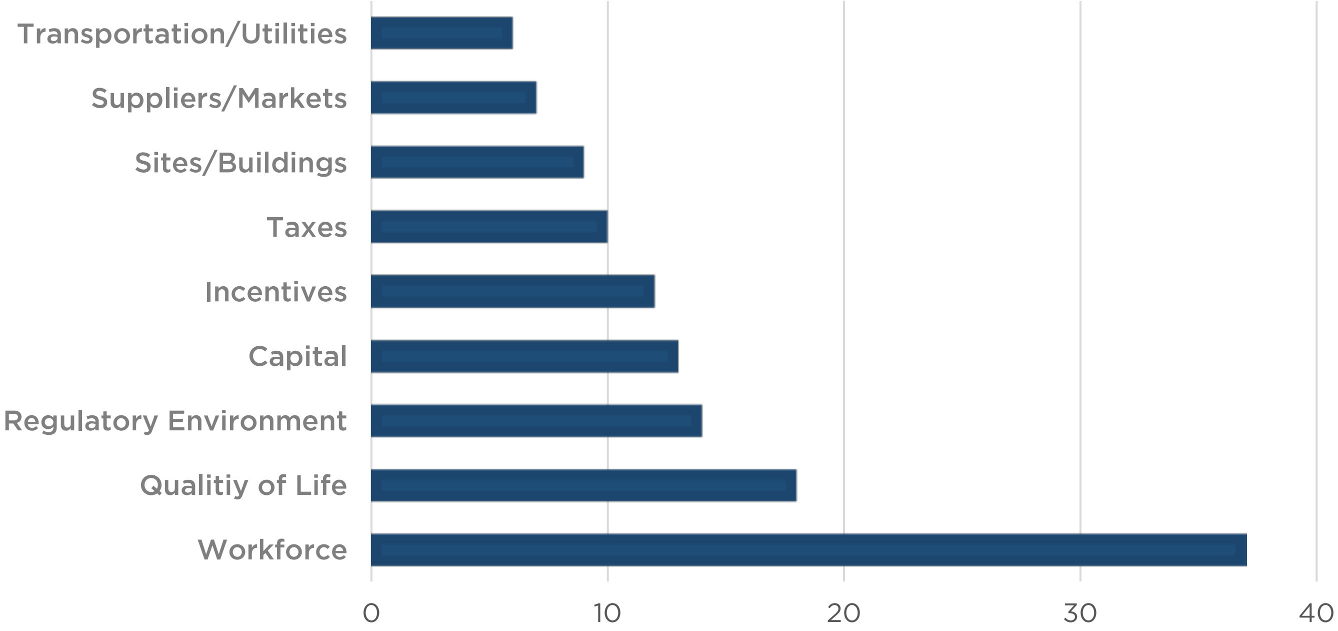
WHAT ARE INDIANA'S GREATEST ASSETS REGARDING CYBERSECURITY?



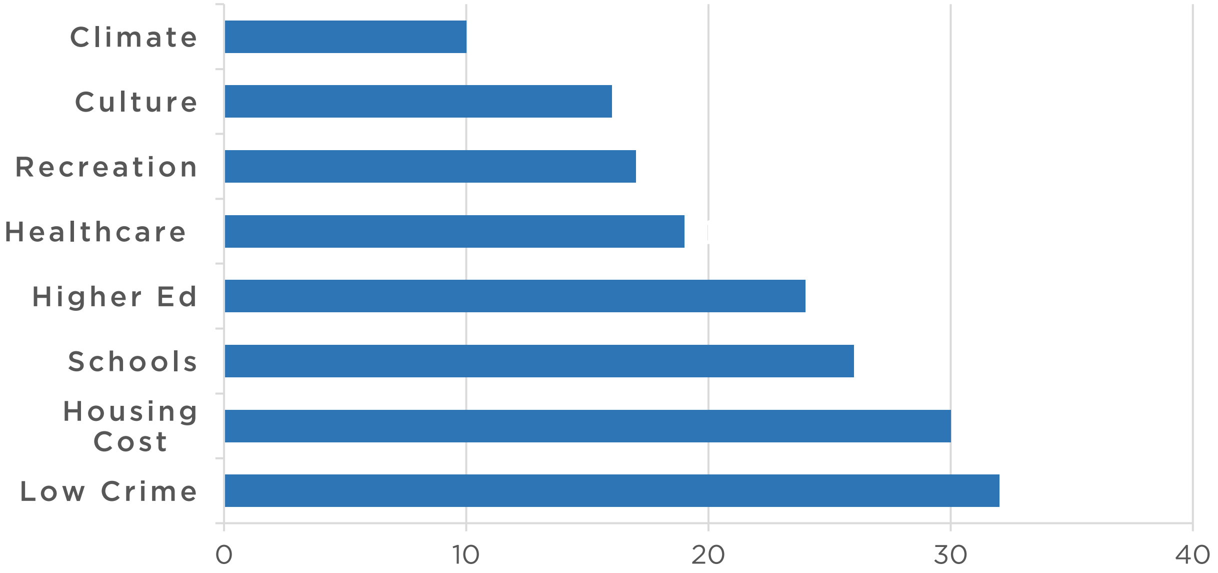
WHAT IS THE MOST IMPORTANT ROLE OF GOVERNMENT IN BUSINESS DEVELOPMENT?



WHAT ELEMENTS ARE MOST IMPORTANT TO YOU IN A BUSINESS ENVIRONMENT?



WHAT ELEMENTS ARE MOST IMPORTANT TO YOU FROM A QUALITY OF LIFE PERSPECTIVE?



Annex C: Indiana Economic Development Cybersecurity Town Hall Series

The Indiana Economic Development Corporation hosted a series of engagements across the State of Indiana known as the "Cybersecurity Town Hall Series." In total, 7 cybersecurity town halls were conducted across the state (Bloomington, Columbus, Evansville, Fort Wayne, Portage, Westgate, and West Lafayette). The stated objectives for these events were:

- To define the cybersecurity market in Indiana through direct engagement with cybersecurity providers and consumers.
- To identify economic development/business development opportunities within cybersecurity/information security.
- To educate cybersecurity providers and consumers about state incentives and programs available through the IEDC, Indiana Procurement Technical Assistance Center, and to Indiana Small Business Development Center.

Additional goals included identifying business to business opportunities for participants, general networking, and conducting an Indiana asset inventory.

Participants included cybersecurity solution providers who provide Identity and Access Management (IAM), risk and compliance management, encryption, Data Loss Prevention (DLP), Unified Threat Management (UTM), firewall, antivirus/antimalware, Intrusion Detection System (IDS)/Intrusion Prevention System (IPS), security and vulnerability management, disaster recovery, Distributed Denial of Service (DDoS) mitigation, web filtering, and other services.

Other participants were cybersecurity service providers specializing in managed services, professional services including consulting, training and education, support and maintenance, design and integration, and risk and threat assessment. Cybersecurity consumers across the following verticals also participated: aerospace and defense, government and public utilities, Banking, Financial Services, and Insurance (BFSI), IT and telecom, healthcare, retail, and manufacturing. Higher education and the military also participated.

Locations	Key Discoveries
Bloomington	• Opportunities to unlock intellectual property from higher education. • An innovation and entrepreneur community that could benefit from economic gardening. • Many assets and individuals that could be more effectively engaged by the state.
Columbus	• A high concentration of cybersecurity expertise and need surrounding advance manufacturing and industrial control systems. • A need for local cybersecurity certification training. • A desire to leverage military assets. • A Shortage of workforce. • A need for small and mid-size business cybersecurity solutions.
Evansville	• A desire for better communication within the state on cybersecurity information and initiatives. • A high concentration of expertise within utilities (energy). • A high concentration of cybersecurity expertise and need surrounding advance manufacturing and industrial control systems. • A need for small and mid-size business cybersecurity solutions. • A shortage of workforce.
Fort Wayne	• A need and desire to develop regional cybersecurity strategies. • A high concentration of expertise in health care, medical devices and advanced manufacturing. • A need for small and mid-size business cybersecurity solutions. • A shortage of workforce.

Portage	• A need for small and mid-size business cybersecurity solutions. • A need and desire to develop regional cybersecurity strategies. • A desire to leverage military assets. • A shortage of workforce.
Westgate	• A desire to leverage military assets. • Many assets and individuals that could be more effectively engaged by the State. • A need for investment in infrastructure. • A shortage of workforce.
West Lafayette	• Many assets and individuals that could be more effectively engaged by the State. • Opportunities to unlock intellectual property from higher education. • An innovation and entrepreneur community that could benefit from economic gardening.

Annex D: Indiana Cybersecurity Engagement Activities

Date	Category	Event	Representative	Location
June 24, 2016	State	Infragard Food and Agriculture Sector Event	Advisor for Cybersecurity	Atlanta, IN
June 26-27, 2016	International	Israel Cybersecurity Delegation	Governor, Secretary of Commerce, Chief Innovation Officer, Advisor for Cybersecurity	Indianapolis, IN
June 30, 2016	State	CXO Conference	Advisor for Cybersecurity	Indianapolis, IN
July 14, 2016	State	Innovation Showcase	Advisor for Cybersecurity	Indianapolis, IN
July 26-27, 2016	National	CSWC Microelectronics Integrity Symposium	Chief Innovation Officer, Advisor for Cybersecurity	Indianapolis, IN
August 2-5, 2016	National	Black Hat	Advisor for Cybersecurity	Las Vegas, NV
August 22, 2016	State	Association for Financial Professionals of Indiana	Advisor for Cybersecurity	Indianapolis, IN
September 1, 2016	State	Indy Big Data Conference	Chief Innovation Officer, Advisor for Cybersecurity	Indianapolis, IN
September 11-15, 2016	National	Infragard National Summit	Advisor for Cybersecurity	Orlando, FL
September 29, 2016	State	Center for Applied Cybersecurity Research Summit	Advisor for Cybersecurity	Indianapolis, IN
October 13, 2016	State	Centric Day of Innovation	Advisor for Cybersecurity	Indianapolis, In
October 24-27, 2016	National	ICS Cybersecurity Conference	Advisor for Cybersecurity	Atlanta, GA
November 22, 2016	State	Indiana Cybersecurity State of the State	Advisor for Cybersecurity	Indianapolis, IN
January 18, 2017	National	Atlanta A-List	Advisory for Cybersecurity	Indianapolis, IN
January 29 – February 3, 2017	International	CyberTech	Secretary of Commerce, Chief Innovation Officer, Advisor for Cybersecurity, Director of Field Operations	Tel Aviv, Israel
February 13-17, 2017	National	RSA	Advisor for Cybersecurity	San Francisco, CA
March 7-9, 2017	International	International Resiliency Conference	Advisor for Cybersecurity	New Orleans, LA
March 30 - April 1, 2017	National	Women in Cybersecurity	Advisor for Cybersecurity	Tucson, AZ
April 17-19, 2017	State	Center for Education and Research in Information Assurance and Security Symposium	Chief Innovation Officer, Advisor for Cybersecurity	West Lafayette, IN
April 21, 2017	State	Indiana Aerospace and Defense Council Breakfast	Governor, Secretary of Commerce, Chief Innovation Officer, Advisor for Cybersecurity	Indianapolis, IN