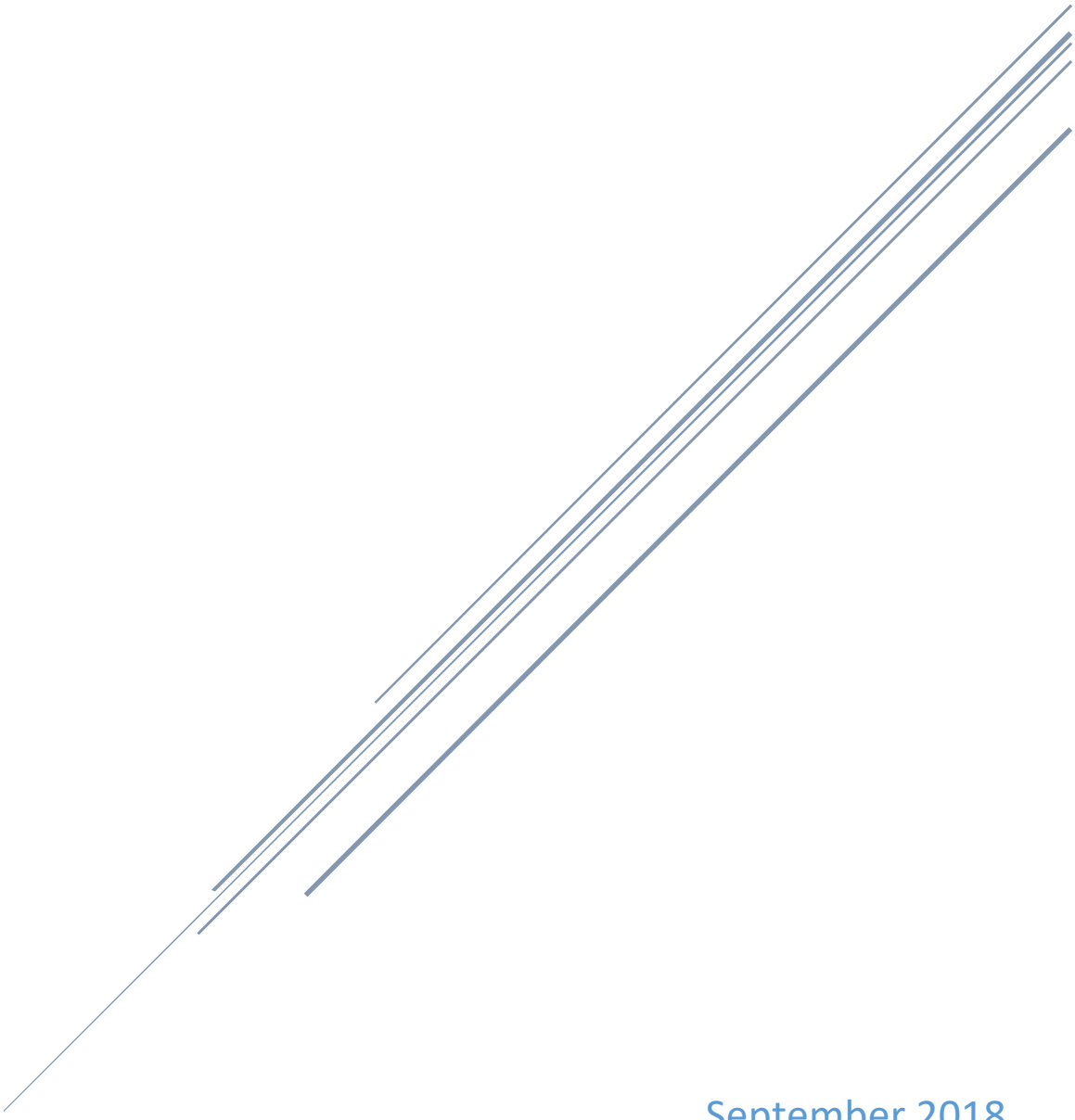
FINANCE COMMITTEE STRATEGIC PLAN

Chair: Owen LaChat | Co-Chair: Tom Fite



September 2018

Indiana Executive Council on Cybersecurity

Finance Committee Plan

Contents

Committee Members

Committee Members

Name	Organization	Title	Committee/Workgroup Position	IECC Membership Type
Owen LaChat	MutualBank	Technology Infrastructure & Security Manager	Chair	Voting
Tom Fite	Indiana Department of Financial Institutions	Director	Co-Chair	Advisory
William Tucek	Navient	Sr Mgr., Network Security	Full Time	Advisory
Brian Vitale	Notre Dame FCU	Chief Risk and Compliance Officer	Full Time	Advisory
Sharon Ferguson	MutualBank	Chief Risk Officer / ISO	Full Time	Advisory
Michael Servas	MutualBank	Sr. Information Security Analyst	Full Time	Advisory
Matthew Cloud	Ivy Tech	Project Director - TAACCCT Grant School of IT	Full Time	Advisory
Brad Stone	Indiana Department of Financial Institutions	Director of Information Technology	Full Time	Advisory
Kevin Stouder	Indiana Department of Financial Institutions	IT Program Lead/IT Examiner	Full Time	Advisory

Introduction

Introduction

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) and its mission was continued. With the ever-growing threat of cyberattacks, the IECC has been tasked with developing and maintaining a strategic framework to establish goals, plans, and best practices for cybersecurity to protect Indiana's critical infrastructure. The IECC is comprised of twenty committees and working groups who worked together to develop a comprehensive strategic plan and implementation plans. This implementation plan is one of the twenty specific plans that make up the complete 2018 Indiana Cybersecurity Strategic Plan.

Executive Summary

Executive Summary

- **Research Conducted**
  - Determined the need for additional hands-on training and education of industry professionals on information security best practices and procedures. Spoke to industry professionals, vendors, and researched common training courses targeted to the financial industry.

- **Research Findings**
  - A need for increased and on-going training and education.

- **Committee Deliverables**
  - Cyber Training Program Pilot
  - Top Information Security Tips Material

- **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. We have been able to educate and train industry professionals through a number of professional organizations as well as through other informal discussions.

2. **What (or who) are the most significant cyber vulnerabilities in your area?**
    a. There have been a number of significant cyber vulnerabilities that have affected financial institutions as well as other industries in the recent past. Among the most notable were the WannaCry ransomware attack, Meltdown/Spectre vulnerabilities, and the Heartbleed and Poodle attacks. 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 around the risks of not following information security best practices.

3. **What is your area's greatest cybersecurity need and/or gap?**
    a. The greatest cybersecurity need and gap in the financial industry, as well as other industries, is to acknowledge and understand that cybersecurity risks are real, that they do occur, and they have real consequences. For example, we have witnessed and may have been impacted by the Equifax, Anthem, and Target breaches. Consequently, we need to remain diligent in the way that information is stored, processed, and transmitted and hold end-user employees and customers accountable for the confidentiality, integrity, and availability of information. Increased cybersecurity education is the greatest need, as it is through education that greater awareness can be achieved. This means educating the end-users, who are often the actual source of a breach. However, it also means more education for the technology specialists who will be continually challenged to identify and protect vulnerabilities as well as respond to and recover after an attack has occurred.

4. **What federal, state, or local cyber regulations is 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 here 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 above 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 Cybersecurity Assessment Tool (CAT 1.0) was developed and released in recent years, and most recently updated in May 2017. CAT 1.0 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. Discussions are ongoing as to what the next version of this tool will look like. It is a challenge to develop such a tool that is sophisticated enough to be used by the larger community and smaller regional banks, yet also simple enough to be used by smaller banks with less complex systems and who also have less IT staff resources. The goal of CAT 1.0 was that the assessment could be completed internally by the institution's own IT staff, meaning it would not require third-party assistance. This philosophy was important, as the associated costs of using outside consultants would have greatly impacted the adoption rate of this assessment methodology.

8. **What does success look like for your area in one year, three years, and five years?**
    a. Without a doubt, complete success in even as much as five years is unlikely. However, the trend of financial attacks, the severity of those attacks, and the loss of data from attacks should all be trending in a positive direction. Cybersecurity management tools will improve, reducing cyber exposure, and increased awareness will result in a greater end-user caution.

9. **What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?**
    - **a.** Diligence and focused training are needed both in the corporate world and also with individual citizens. Access to training is key in a corporate world. Training is often targeted at IT specialists, and there is minimal training available for non-IT staff. Furthermore, access to what training is available can be expensive leaving corporations to decide between who gets access to training and to what extent. From a consumer standpoint, financial institutions recognize that a customer and a customer's access can be one of their greatest points of vulnerability. In response, institutions have started to educate their own customers to partner with their clients to reduce this exposure.
    - b. A customized information security curriculum targeted towards financial sector professionals will increase 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 for and affordability of these resources. Larger metropolitan areas understandably have better access to a staff resource pool; however, demand for these resources is also greater in metropolitan areas. For example, access to and cost of staff would be greater in San Francisco than in Indianapolis, and likewise, access is greater in Indianapolis than it is in any small town in Indiana.

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. This is an expansive question, and probably should be a paper stand alone. Several different tools are available (National Institute of Standards and Technology (NIST) and CAT 1.0 for example); however, no platform serves a one size fits all solution. Given the wide range of complexity and risk variance across the industry, it would seem unlikely than any one set of best practices would fulfill the needs of all financial businesses.

Deliverable: Cyber Training (Ivy Tech)

Deliverable: Cyber Training (Ivy Tech)

General Information

1. **What is the deliverable?**
    a. Provide training on cybersecurity and prerequisite IT instruction for business executives to fully understand the risks and prevention of an active cyberattack.

2. **What is the status of this deliverable?**
    a. In-progress; 75% complete

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

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

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Giving industry professionals a solid, hands-on foundation in information security.

6. **What metric or measurement will be used to define success?**
    a. Certificate of completion of global IT and Cybersecurity Curriculum from CISCO on IT Essentials, Introduction to Networking, and CISCO Certified Networking Associate in CyberOps. Trainees will also be prepared for CompTIA A+, CompTIA Security+, and the CCNA CyberOps Certification. With one additional course they would be prepared for CompTIA Network+ and CISCO Certified Entry-level Network Technician.

7. **What year will the deliverable be completed?**
    a. 2019.

8. **Who or what entities will benefit from the deliverable?**
    a. Ivy Tech and various other public and private entities that attend the training courses.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. Several other state colleges and universities have cybersecurity programs. Ivy Tech has 25 locations throughout the state to provide training. Ivy Tech courses could be taken by professionals for credit or taken in a fast track (one course per month) in a not-for-credit format. However, those who take it in a not-for-credit format obtain college credit by passing the industry certifications. All for-credit coursework or credit obtained by certification crosswalk taken during the cybersecurity program transfers to most Indiana four-year public universities. Additionally, this same coursework was approved by the Indiana Department of Education for students to take in the 9-12th grades in the new Computer Science and IT pathways and are dual credit eligible.
    b. Additional and higher-level cybersecurity training can be obtained through Ivy Tech towards an Associate of Science (AAS) degree in Cybersecurity which transfer as a 2+2 or 3+1 (3 years at Ivy Tech and 1 year at the four-year college) to four-year institutions for a Bachelor's degree focused on cybersecurity including Vincennes University, Purdue Northwest University, and WGU-Indiana.
    c. Through a National Security Agency (NSA)/National Science Foundation (NSF) grant, six students are chosen from the Ivy Tech CSIA program to receive free tuition and a $25,000/year stipend to complete their second year at Ivy Tech and last two years at Purdue Northwest. They are chosen after taken the mentioned three courses in this training program.
    d. Federal resources from the Department of Labor Trade Adjustment Assistance Community College and Career Training (TAACCCT) grant established the initial data centers, IT specific classrooms, supplies and training needed to allow these programs to be available and increased the employment of over 20,000 IT students in three years in cybersecurity and other IT fields.

Additional Questions

---

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. All other committees and working groups are encouraged to participate.

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. The Ivy Tech program already exists and targeting it toward working professionals shouldn't need additional resources.
    b. However, targeting high school instructors so that the cybersecurity specific courses can be fully implemented within them will require $50K/year for two years to pay for trainers to train sufficient high school teachers across the State.

12. Who should be main lead of this deliverable?

a. Matthew Cloud

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

a. The cost of sending a business person (or teacher) through their respective training at Ivy Tech is $1,000 per person per course with a minimum of five people per course. There are several well-known private companies that offer cybersecurity training for industry professionals at a rate of $2,500-5,000 per person per course with a minimum of five to ten people. While Ivy Tech's cost is significantly less and achievable for larger businesses, the cost is too high for many high schools and smaller businesses including community credit unions.

Implementation Plan

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

a. Ongoing/sustained effort.

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Ivy Tech Curriculum & Scheduling	Matthew Cloud	100	July 2018	
Pilot courses & integrate other interested parties	Owen LaChat	30	February 2019	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No.

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
N/A					

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

a. The Ivy Tech program already exists and targeting it toward working professionals shouldn't need additional resources. However, targeting high school instructors for that the cybersecurity-specific courses can be fully implemented within the schools require $50K/year for two years. Funds will pay trainers to instruct a sufficient number of teachers across the state.

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes

17. What are the details of this deliverable?

a. The cost per person per course is $1,000. A minimum of five people per course is needed. MutualBank is funding at least five people for the pilot. Once the pilot is completed, it could be taught at any of the 25 campuses throughout the State in the faster format for business professionals, that is one class per month non-credit.

b. The fast track pilot for businesses began in July 2018 at the Ivy Tech Muncie campus, 345 S High Street Muncie, IN 47305, with one course per month.

c. Three courses are needed to complete the track:
   - Course 1 - IT Essentials.
   - Course 2 - Introduction to Networking.
   - Course 3 - CCNA CyberOps/Security+.

d. These courses have been taught for several years at Ivy Tech. The fastest these courses have been taught with typical college students is 8 weeks. They have been taught in four to six weeks for IT instructors for the past two years. As the pilot goes along, flexibility may be needed to extend the course length and will be given. The students in the pilot course, may talk with the instructor to change the start and end dates to work with any vacation. Classes will be recorded so that they can review later. Trainees will be expected to work online or at the campus 8-12 hours per week, in addition to the formal 4 hours of class time to successfully complete the work.

e. We have a primary instructor chosen who has taught two of the three classes for many years. We also have backup instructors for each of the courses and they have taught the courses for many years as well. Therefore, it will also help to see how well our current train-the-trainer model is working so that improvements can be made before adding high school instructors. Questionnaires will be sent to the trainees before and after on expectations and implementation so that future instruction will be improved.

f. Sustainability can be through grants such as Skill Up, NSF, or CISCO for high school instructors. Larger businesses should be able to afford the training. However, we should investigate a way to subsidize training for smaller businesses where most cybersecurity holes will occur. One possibility is a subsidy be generated by having enough people to be trained in a class through grants or otherwise. This would ensure the basic course costs are met. After that, a larger business could sponsor a "friend" business. As an example, when the minimum threshold for class cost coverage is reached, 10 trainees, then the number of trainees could be doubled at a minimal increased cost. As a maximum to ensure a quality experience, no more than 20 trainees in each class.
g. Additionally, Governor Holcomb recently signed a bill requiring high schools to include at least one Computer Science course for every high school student who starts by 2021.
h. Goal for 2021: Indiana to increase the number of instructors to at least one Computer Science (CS) teacher per Indiana high school. There are over 500, which include private. This would enable Indiana to educate these new CS instructors to teach cybersecurity at the end of a two-year process.
i. Goal for 2023: To have one cybersecurity trained instructor in each K12 school by 2023, so that between an integrated K14 system, Indiana will be reaching out to both K12 and businesses for supporting a statewide initiative. Then, we will have the most secure State in the US.

Benefits and Risks

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

a. See question #6.

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

a. With appropriate training and certifications, professionals working in critical infrastructure should be better prepared to recognize, assess, and respond to cybersecurity incidents within their organization. The average cost of a breached record is approximately $141. This does not include a company's reputational damage. The costs can become staggering for a company that houses personally identifiable information for thousands or millions of customers.

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

a. Unknown. Educating the workforce of critical infrastructure is a necessity and should be considered a priority.

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

a. Certificate of completion of global IT and cybersecurity Curriculum from CISCO on IT Essentials, Introduction to Networking, and CISCO Certified Networking Associate in CyberOps. Trainees will also be prepared for CompTIA A+, CompTIA Security+, and the CCNA CyberOps Certification. With one additional course they would be prepared for CompTIA Network+ and CISCO Certified Entry-level Network Technician.

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

a. **If Yes, please list states/jurisdictions**

i. Several other state colleges and universities have cybersecurity programs. Ivy Tech has 25 locations throughout the state to provide training. Ivy Tech courses could be taken by professionals for credit or taken in a fast track (one course per month) in a not for-credit format. However, those who take it in a not for credit format obtain college credit by passing the industry certifications. All for-credit coursework or credit obtained by certification crosswalk taken during the cybersecurity program transfers to most Indiana four-year public universities. Additionally, this same coursework was approved by the Indiana Department of Education for students to take in the 9-12th grades in the new Computer Science and IT pathways and are dual credit eligible.

ii. Additional and higher-level cybersecurity training can be obtained through Ivy Tech towards an AAS degree in cybersecurity which transfer as a 2+2 or 3+1 (3 years at Ivy Tech and 1 year at the four year college) to four-year institutions for a Bachelor's degree focused on cybersecurity including Vincennes University, Purdue Northwest University, and WGU-Indiana.

iii. Through an NSA/NSF grant, 6 students are chosen from the Ivy Tech CSIA program to receive free tuition and a $25,000/year stipend to complete their second year at Ivy Tech and last two years at Purdue NW. They are chosen after taken the mentioned three courses in this training program. Federal resources from the Department of Labor TAACCCT grant established the initial data centers, IT specific classrooms, supplies and training needed to allow these programs to be available and increased the employment of over 20,000 IT students in three years in cybersecurity and other IT fields.

23. 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?

a. No

b. **If Yes, please list states/jurisdictions**

i. That is a difficult question to answer accurately, as it is often not stated publicly exactly how a security breach occurred. I think it is safe to state that giving the professionals in the industry a solid technical foundation is extremely important.

Other Implementation Factors

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

a. See Question #4

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

a. No

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

a. Ivy Tech or a similar state institution will need to continue offering their courses in a manner that is affordable and efficient for working professionals.

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

a. Ivy Tech, Indiana Department of Financial Institutions, and Indiana Bankers Association.

28. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
    i. Foundational knowledge of information security is not industry specific.

Communications

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

a. Whoever the IECC feels is appropriate.

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

a. Yes

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

a. Planned marketing will occur via:
    i. https://www.ivytech.edu/it/
    ii. https://www.ivytech.edu/cyber-security/
    iii. https://www.ivytech.edu/itacademies/
    iv. Press releases regarding cybersecurity centers in Muscatatuck, Fishers, and Valparaiso.
    v. Directly to high schools and through statewide conferences for educators.
    vi. Campus-based advisory board meetings.

Evaluation Methodology

Objective 1: Ivy Tech will develop a cybersecurity curriculum for business executives by July 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

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

Objective 2: IECC Finance Committee and Ivy Tech will launch a pilot program with 7 participants by August 2018.

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

Deliverable: Top Security Tips Material

General Information

1. **What is the deliverable?**
    a. 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?**
    a. In-progress; 85% complete

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

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

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Better end-user information security posture, education, awareness, reporting, and response.

6. **What metric or measurement will be used to define success?**
    a. A reduction of information security incidents overall.

7. **What year will the deliverable be completed?**
    a. 2018

8. **Who or what entities will benefit from the deliverable?**
    a. Local and State governmental entities throughout Indiana.

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 won't 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. MutualBank, Inc.

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

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?**
    a. One-time deliverable.

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Revise & circulate "Top Information Security Tips" to IECC for mass distribution	Owen LaChat	85	December 2018	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. No

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
N/A					

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
N/A						

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. See question #5.

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?

a. Yes.

b. **If Yes, please list states/jurisdictions**

i. 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?

a. Yes.
b. **If Yes, please list states/jurisdictions**
    i. See question #9

Other Implementation Factors

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

a. See question #4

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

a. No.

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

a. Nothing.

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

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

27. Can this deliverable be used by other sectors?

a. Yes,
b. **If Yes, please list sectors**
    i. Information security best practices are not industry specific.

Communications

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

a. Whoever the 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)?

a. 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 develop the Top Information Security Tips training material for Indiana businesses by December 2018.

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

No Supporting Documentation Provided At This Time