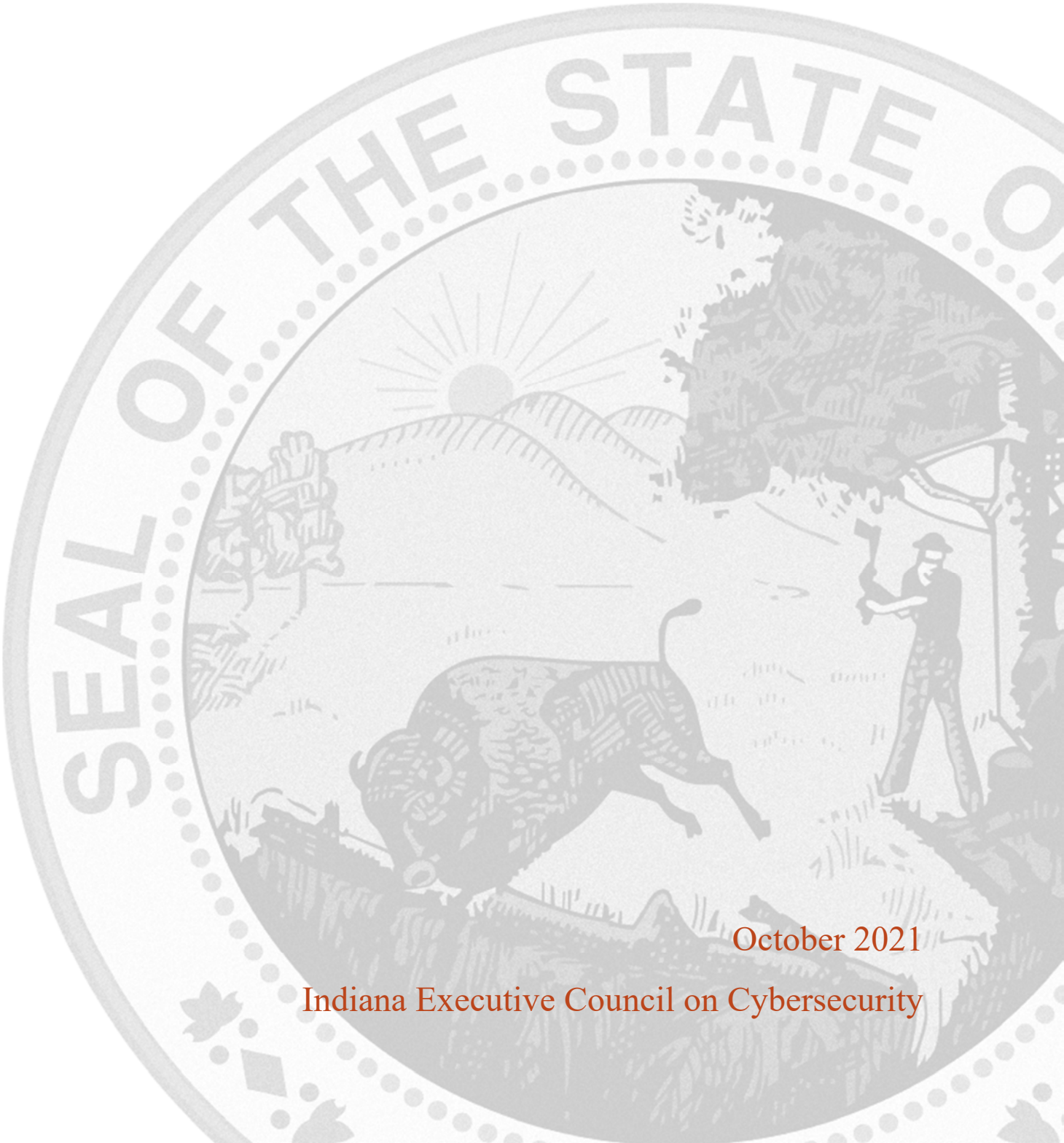
HEALTHCARE COMMITTEE STRATEGIC PLAN

Chair: Mitchell Parker
Co-Chair: Jacob Butler



October 2021

Indiana Executive Council on Cybersecurity

Healthcare 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)
Bailey	George	Purdue University / cyberTAP	Assistant Director, cyberTAP / Professional Services	As Needed
Berryman	Glenn	Community Health Network	Chief Information Security Officer	Advisory
Butler	Jacob	Parkview Health	Manager of Enterprise Systems	Co-Chair
Davis	Philip	Community Health Network	Director, IT Risk and Compliance	Full Time
Fredland	Valita	Community Health Network	Senior General Counsel	Full Time
Hobgood	Lisa	Deaconess Health System	Chief Information Officer	As Needed
Johnson	Jason	Parkview Health	IS Manager	Full Time
Linder	Jared	Family and Social Services Administration	Chief Information Officer	As Needed
Lyle	George	Purdue University	Senior IT Security Risk Analyst	As Needed
Mabry	Kevin	Sentree Systems, Corp.	Chief Executive Officer	Full Time
Martz	Jeff	Health and Hospital Corporation	Chief Information Security Officer	Full Time
Ndow	Emmanuel	Marion General Hospital	Chief Information Officer	As Needed
Odum	Matt	Briljent, LLC	President	Full Time
Parker	Mitchell	IU Health	Executive Director, Information Systems	Chair

Last Name	First Name	Organization	Organizational Title	Member Type (Chair/Co-chair/Full-time, As needed)
Schmidt	Eric	Eskenazi Health	Information Security Officer	Full Time
Sturgeon	Nick	IU Health	Director, Information Security	Full Time
VanZee	Andrew	Indiana Hospital Association	Vice President of Regulatory and Hospital Operations	Full Time
Wichlinski	Robert J.	Great Lakes Labs, LLC	Executive Vice President and General Manager	As Needed
Nevers	Frank	Franciscan Alliance, Inc.	Security Program Manager	Full Time
Vuppalanchi	Deepika	Syra Health	Chief Executive Officer	Full Time
Whitmore	Erica	Anthem, Inc.	Senior Security Risk and Intelligence Analyst	As Needed

Introduction

Introduction

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

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

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

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

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

Executive Summary

Executive Summary

- **Research Conducted**
  - We conducted interviews with three people and summarized questions and findings from the Indiana Medical Device Manufacturer's Council (IMDMC) annual meeting,and two discussions with government officials.
    - Jim Routh, Chief Information Security Officer (CISO), Aetna, board member of National Health Information Sharing and Analysis Center (NH-ISAC), andFinancial Services Information Sharing and Analysis Center (FS-ISAC) member.
    - Suzanne Schwartz, Doctor of Medicine (MD), Master of Business Administration (MBA), Director, Medical Device Security, U.S. Food andDrug Administration (FDA)
    - Jennings Aske, Juris Doctor (JD), CISO, Columbia/New York PresbyterianHealth.
    - Ralph Hall, Leavitt Partners. The committee spoke with him and summarized findings from the IMDMC annual meeting, including discussions from Eli Lilly, Roche, Hill-Rom, and the Mako Group. Mitch Parker chaired the Cybersecurity panel with members of Lilly, Hill-Rom, Mako Group, and Dr.Schwartz and gave all research notes to the group.
    - Deven McGraw, Former Deputy Director of Enforcement, U.S. Department ofHealth and Human Services (HHS) Office for Civil Rights.
    - Iliana Peters, Acting Deputy Director of Enforcement, HHS Office For CivilRights.
    - Nebraska Hospital Association.
    - Josh Singletary, NH-ISAC.
      - The committee has also utilized several papers and presentations from Mitch Parker and IU Health to provide further research. The papers supplied have 100+ sources each andwere submitted as part of graduate school programs.
      - The committee has continued to research actual attacks and vulnerabilities that have led to attacks. We have examined root causes of numerous ransomware and malware attacks that have led to system downtimes across the world.

- **Research Findings**
  - There is high awareness of cybersecurity being an issue in the State of Indiana and nationally.
  - There has been very little practical guidance given to providers that they can use. While HHS has started to give guidance, there is little practical guidance that appliesto small to medium size providers.
  - Currently, in Washington, the Health Information Trust Alliance (HITRUST), a private organization, is actively attempting to usurp the NH-ISAC to be the providerof threat intelligence and reporting to healthcare organizations in the U.S.
    - Many providers will not adopt this framework as it is costly and requires full-time investment to be successful.
      - Full HITRUST adoption also requires vendors to buy into it and use the framework.

        - Lessons learned from Department of Defense (DOD) include special frameworks did not work for them. Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) and Department of Defense Information Assurance Certification and Accreditation Process (DIACAP), and organizations end up falling back to using National Institute of Standards and Technology (NIST) as it is practical and what the rest ofthe federal government has standardized.
- The H-ISAC is providing all providers with information; however, it is overly technical in nature.
    - While H-ISAC does have the Threat Intelligence Committee, which is composed of members from the larger providers, and does provide intelligence to other members, it is highly technical in nature most of the time.
- According to the Nebraska Hospital Association, 75% of their hospitals are in ruralareas and do not have full-time IT staff.
- According to the American Hospital Association, in 2012, approximately 25% of all hospitals had negative operating margins. The average operating margin was 7.04%for the same time period.
- Electronic Medical Records (EMR) systems require significant initial and ongoing investments. The core EMR system, when purchased initially, requires 25% of the lifetime costs paid up front.
- Even with cloud computing, organizations are required to complete information security risk assessments and document them yearly.
    - There has been a growing perception in healthcare that certain systems that contain protected health information do not need involvement from the formalInfo Services e.g. security. This is because the system specific "shadow IT" ends up not waiting for security, doing work, and negating the required security controls necessary to keep them protected.
- Organizations are required, as per the Health Information Technology for Economicand Clinical Health (HITECH) Act, to complete risk assessments of vendors.
- Healthcare organizations are dealing with lower margins, not enough IT staff, and alack of cohesive guidance.
    - The number of vendor risk assessments that medical device manufacturershave to deal with, and the high variety are causing issues with vendors. Jennings Aske is leading an effort to standardize these assessments.
    - While NH-ISAC has the Cyberfit program, which focuses only on applications, licensed by Prevalent, it is also costly at $4,000 per assessment. With the number of vendors and applications that a health system can have, ifused extensively the program can cost more than staff. Smaller providers typically use the Cyberfit program for a few applications. However, according to Iliana Peters, smaller providers still have to conduct their own organizational risk assessments, even if they do risk assessments of applications.
- The FDA is expecting organizations to include security in their legal contracts. Theseneed to be shared to set global expectations.

- The FDA understands that current medical device security efforts are losing peopleover unclear explanations and not listening to customers.
- According to the FDA, vendors need to be educated on how to present security. Many smaller startups are more willing to listen to customers and present a better security plan to their customers. According to Jennings Aske, some large vendors know how to communicate about their own solutions, while many others do not,
  - Standardization and information sharing in this area would provide benefits, according to Jennings, as vendors would be more willing to work with collaborative groups. Binding together groups of organizations, with aggregate market value commensurate with the size of larger medical devicecompanies, is considered incentive enough, indicates Jennings.
- The metrics published did not either refer to Bureau of Labor Statistics data on the workforce or only referred to cybersecurity as part of an overall percentage. There is very little empirical data on staffing metrics for cybersecurity as either a subset of IT or healthcare. Only surveys published by Big 4 firms indicate a relative increase in positions, as opposed to a metrics-based approachrelative to either organizational size, number of assets managed, or number of applications. The only metrics found specifically related to the number of data breaches themselves.
- According to Jim Routh, Midwestern organizations are less likely to take advice from national organizations based on his six years as a CISO in Minnesota.
- The NH-ISAC will be offering discounted endpoint security for all healthcare providers at a very reasonable cost of $10 per machine per year. This addresses a critical need and costs significantly less than other solutions.
- A number of smaller providers are willing to collaborate. However, not all health systems in Indiana have their security managed locally. St. Vincent's, which is part of Ascension, has security managed by an operations center in Troy, Michigan. The issue of collaboration across state lines has to be addressed.
- According to our research, the practical approaches to implementing cybersecurity need to be communicated better to the medical provider community in a way they can use.
- According to our research, the dwell time of attacks within healthcare networks is measured in months, and these attackers are taking their time to identify network assets. They are using this information to specifically target backups and other critical information to increase their chances of payment.
- Attacks have occurred locally, including at Eskenazi Health, that have crippled networks at multiple levels.

- **2021 Plan Working Group Deliverables**
  - Long-Term Education
  - Healthcare "Cyber in a Box"
  - Vendor Management Resources
  - Statewide Cybersecurity Exercises
  - Cyber Sharing Platform

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

- **References**
  - None at this time.

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
   a. Centers for Medicare and Medicaid Services (CMS) has released several guidance documents and programs on cybersecurity.
   b. The Healthcare Information and Management Systems Society (HIMSS) currently offers a comprehensive cybersecurity education program, as does the American Hospital Association (AHA), and American Health Information Management Association (AHIMA). In addition, the National Health Information Sharing and Advisory Center (NH-ISAC) and InfraGard also offers guidance to organizations. HITRUST, which is a for-profit organization, is also popular with many large healthsystems and payers. They have been providing guidance and a security framework.
   c. Much of this education is focused on either the basics or is aimed at highly sophisticated organizations, which is not the majority of healthcare.

2. **What (or who) are the most significant cyber vulnerabilities in your area?**
   a. Currently, the continuing maintenance and upgrading of systems to protect against new and emerging threats, the abundance of legacy systems, the continuing issues with workflows, the lack of consistent training and education, and the economic pressures causing a de-emphasis on cyber due to havingto keep the lights on in many organizations.

3. **What is your area's greatest cybersecurity need and/or gap?**
   a. The need is to provide basic education that is relevant to organizations to show them how to protect, as opposed to the constant emphasis on data breaches. CMS has directly indicated that education has been a weak point, and our research shows that the current approach of having one dedicated subject matter expert (SME) in each regional office isolates security responsibilities to that one person. Whereas, the institutionalization of security standards that the Federal Financial Institutions Examination Council (FFIEC) has accomplished in finance, is a much more comprehensive cybersecurity program model.

4. **What federal, state, or local cyber regulations is your area beholden to currently?**
   a. Those in healthcare are required to follow the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules, HITECH Act, Stark Act, and a number of state and local laws. In addition, the organizations that have not outsourced their payment processing have to follow Payment Card Industry and Data Security Standards. The organizations who actively recruit international patients from the European Union (EU) or advertise in the EU must follow the EU General Data Protection Regulation (GDPR).

5. **What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
   a. The committee has highlighted the H-ISAC Threat Intelligence Committees (TIC) and Cyberfit programs as great examples as for how multiple organizations can work together to identify, classify, and mitigate threats across a large population. We have also discussed how organizations are already self-organizing, specifically with Jennings Aske's work at Columbia/New York-Presbyterian (NYP).

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. Included are two papers written by Mitch Parker, and interviews with Jim Routh, CSO of Aetna; Suzanne Schwartz, MD, MBA, Director of Medical Device Security for the FDA; Ralph Hall from Leavitt Partners at the Indiana Medical Device Manufacturer's Council annual meeting; and Jennings Aske, CISO of Columbia/NYPHealth System in New York City (NYC). We have also researched NH-ISAC, Research Education Networking Information Sharing and Analysis Center (REN- ISAC), and a number of other sources.

7. **What are other people in your sector in other states doing to educate, train, prepare,etc. in cybersecurity?**
   a. Others in the medical sector are currently utilizing the same sources Indiana does. There are also self-organizing as part of emergency management to address these issues. This self-organization includes working with H-ISAC, REN-ISAC, InfraGard, and through contacts in hospital emergency management, including existing regional organizations.

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

   <u>One year:</u>
   - Begin developing a pilot program modeled after H-ISAC's Threat Intelligence Committees (TICs)
   - Collaborate across multiple institutions to address security issues
   - Provide a means for healthcare organizations to contact and to report potential issues.
   - Beginnings of a communication plan designed to reach out to healthcare providers.

   <u>Three years:</u>
   - Expansion of the program to have more dedicated staff and interactionwith providers.
   - More proactive education
   - Collaboration with other states and organizations such as H-ISAC, Infragard, and Department of Homeland Security (DHS) to provide cybersecurity awareness

   <u>Five Years:</u>
   - Having this program as part of normal business of the State.

9. **What is the education, public awareness, and training needed to increase the State'sand your area's cybersecurity?**
   a. There needs to be a concerted effort to reach out to particular medical providers to specifically address what is needed to increase security. Although the awareness of the need for cybersecurity is high, the specific guidance as to what is needed to be secure has been either too specific or not enough.

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. According to the 2020 U.S. Bureau of Labor Statistics, 13 percent of the total workforce in Indiana is in the healthcare sector.
    b. There are no clear statistics as to how much of that section workforce is cybersecurity related.
    c. IU Health employs approximately 35,000 people. Approximately 750 of which work in IT, which is approximately 2% of the workforce. Of that, 20 staff members are dedicated to cybersecurity full-time, which is approximately 0.07% of the total workforce at IU Health.
    d. According to a Frost & Sullivan report, 30% of healthcare hiring managers plan to increase staff by 20% or more, and 9% of managers want to increase hiring to between 16-20%.
    e. According to the May 2017 HealthCare Industry Cybersecurity Task Force report, coupled with the statistics from the BLS 2016-2026 report. The Cybersecurity vacancies for Indiana Healthcare would be around one dedicated Cybersecurity professional for every 10,000 staff with a minimum of one.
    f. The issue is not cybersecurity jobs, it is getting people to understand cybersecurityand use due diligence.

11. **What do we need to do to attract cyber companies to Indiana?**
    a. Advertise and leverage the educational advantage that Indiana has with IU, Purdue, IUPUI, Rose-Hulman, and Notre Dame. Two of the best and most well-connected Cyber programs in the country are here, and there are already a number of tech companies, specifically Salesforce, taking advantage. Facilitating business development and encouraging companies to locate offices and/or staff in Indiana based on the availability of top-level graduates, quality of living, and low cost of living would attract and retain talent.

12. **What are your communication protocols in a cyber emergency?**
    a. Hospital Incident Command System (HICS) is followed to escalate incidents. There is now a coordinated communication with multiple agencies and will follow the same protocols as a standard multi-site incident. Ultimately, a multidisciplinary approach in healthcare is needed that utilizes HICS as patient safety has to be paramount.

13. **What best practices should be used across the sectors in Indiana?**
    a. Focus on assessing risk and helping people understand what to do to address it would be a best practice. There needs to be a focus on the fundamentals of cyber hygiene and privacy measures. Focusing on the cybersecurity as a separate entity independent of overall patient privacy is making it more difficult to attack the root causes of information breaches.

Deliverable: Long-Term Education

Deliverable: Long Term Education

General Information

1. **What is the deliverable?**
   a. The deliverable is Indiana-focused versions of security education targeted at small to medium-sized providers. Most of the guidance given out by CMS to providers assumes that providers either have an IT staff or someone with the requisite level of expertise within the organization to interpret guidance and give staff instruction. While working on several other projects, CMS discovered that most small to medium sized providers and critical access hospitals do not have the staff needed to implementsolutions nor have been educated on how to address threats. Most importantly, manydo not know where to report data breaches or cyber-attacks.
   b. The goal of this solution is to give actionable items to these organizations to implement reasonable security solutions and help prevent common security issues with basic targeted education. We have spoken with the Water committee and discovered we had the same issue where most small to medium-sized organizationsdo not have security staff needed to implement solutions, lacking/no security education, and don't know how to handle breaches.

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.**
   ☐ 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. Providers at all levels will be able to utilize actionable information to protectthemselves against emerging threats.
   b. Better community awareness of threats and, more importantly, actionable steps that providers can take to protect themselves using communications they can understand.

6. **What metric or measurement will be used to define success?**
   a. Number of providers utilizing the service and actively protecting themselves.
   b. Number of organizations receiving intelligence (time period comparisons).

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

8. **Who or what entities will benefit from the deliverable?**
   a. Small to medium healthcare entities across the state who do not currently receive thistype of actionable intelligence.

9. **Which state or federal resources or programs overlap with this deliverable?**
   a. This currently partially overlaps with the work NH-ISAC, REN-ISAC, and InfraGard are currently doing. However, they are not reaching to the level we intend.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. The Health Sector Coordinating Council (HSCC), American Hospital Association (AHA), InfraGard, H-ISAC, REN-ISAC, and the State and Local Government committees.We also will hopefully be working with the Water committee as we share the same challenges.

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. InfraGard, H-ISAC, REN-ISAC, Indiana IOT, Indiana Hospital Association,Indiana Health Information Exchange (IHIE), and Health Sector Coordinating Council (HSCC)

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

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

a. Communicating to the providers and utilizing multiple avenues to do so.
b. Threat Complexity. Having to deal with multiple threat variants affecting providers.
c. Bad patches from vendors (Meltdown/Spectre). Red Hat, Microsoft, and numerous other vendors have released bad patches for vulnerabilities. We don't want to causemachines to malfunction because of non-functional patches.

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
Work with supporting subgroup	JB/Team/Communication Subgroup	15%	9/15/2021	
Gather resources	JB/Team	25%	10/1/2021	
Define Message Formatting	JB/Team	0%	11/1/2021	
Build Delivery Methods	JB/Team	0%	2/1/2022	
Implement 2022 LTE/Release	Mitch Parker	0%	4/1/2022	
Review Effectiveness of Training, Surveys, and Customer Feedback	Mitch Parker	0%	2/1/2023	
Plan 2023 Training	Mitch Parker	0%	3/1/2023	
Deliver 2023 LTE	Mitch Parker	0%	4/1/2023	

Resources and Budget

15. Will staff be required to complete this deliverable?

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
0.5	0.5	Marketing / Communications	IOT	Grant	Need to have someone help with communication and distribution under proper branding

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
Web Site Space	Space on Indiana Cybersecurity Portal to host data – needed for data sharing and accessibility					

Benefits and Risks

17. What is the greatest benefit of this deliverable?

a. This will provide Indiana healthcare providers the training materials and information they need to educate themselves about cybersecurity risks, threats, best practices, and strategies.

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

a. This deliverable will educate providers about the cyber risks and what they can do to mitigate those risks /with a minimum of resources. It will provide healthcare providers with information to aid in their understating of security risks and how to leverage strategies to lower their risks.

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

a. Healthcare providers will continue to be not cognizant about how to mitigate their business risks. Small to medium-sized Healthcare providers will not have information they need to continue to grow knowledge of security topics.

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

a. Success is quantitatively defined as the number of providers who download and utilize the education in their practices. The baseline is zero practices using it now. In addition, a customer satisfaction survey is planned to review effectiveness along with feedback. Having ten providers use this would be considered a success.

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

☒No ☐ Yes

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

☒No ☐ Yes

Other Implementation Factors

---

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

a. The largest factor is the resources from larger providers and IECC to be able to complete these deliverables effectively given numerous other resource constraints.

b. The other major factor is making sure we have enough coverage from members to address covering the news and intelligence sources to develop communications.

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. This will need the continual attention of IECC members to plan, develop, and evaluate effectiveness of the deliverables, especially as topics change.

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

a. This committee has decided to leverage resources from CISA, the Health Sector Coordinating Council, and H-ISAC as a base. Continue work with the communication subgroup is needed to ensure consistent communication plans.

27. Can this deliverable be used by other sectors?

☒No ☐ Yes

a. The long-term education could be used by all other sectors. However, the data will be constant with healthcare needs.

Communications

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

a. All healthcare providers and practices in the state of Indiana will need to be informed of its availability using existing notification systems, the state portal, and appropriate communications mechanisms for the website updates.

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. Making several conference presentations about its development and community involvement will be considered.

Evaluation Methodology

Objective 1: IECC Healthcare Committee will update Indiana-focused versions of security education in 2022.

Type: ☒ Output ☐ Outcome

Evaluative Method:

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

Objective 2: IECC Healthcare Committee and partners will provide updated Indiana-focused versions of security education to 80 percent of Indiana healthcare providers in 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 3: IECC Healthcare Committee and partners will collect customer effectiveness, usage, and/or feedback survey for future development in 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: Healthcare Cyber in a Box

Deliverable: Healthcare Cyber in a Box

General Information

1. **What is the deliverable?**
   a. Repackaging and organizing the Health Sector Coordinating Council and Healthcare Information Sharing and Advisory Council (H-ISAC) materials for Indiana health care providers to give them a more focused and clear approach to solving health care problems.

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.**
   ☐ 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?** (Chose 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. This will provide templates and base information healthcare providers can use to protect themselves against cyberattacks. This information will also be used to help providers understand their risks and take action to address their gaps.

6. **What metric or measurement will be used to define success?**
   a. The number of providers that utilize this toolkit or parts of it after its creation will define its success.

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

8. **Who or what entities will benefit from the deliverable?**
   a. Small to medium-sized healthcare providers that do not have their own security staff or a security firm available to assist will benefit from this.

9. **Which state or federal resources or programs overlap with this deliverable?**
   a. The work from H-ISAC, CISA, and the HSCC overlaps, which is why the focus changed from original content to utilizing much of theirs and repackaging it for healthcare providers.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. We will be coordinating with the Cyber Sharing group, along with multiple other subcommittees to incorporate their materials into the deliverable.

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 Health Sector Coordinating Council (HSCC), Health ISAC (H-ISAC), CISA, and IECC would all need to be involved.

12. **Who should be main lead of this deliverable?**
    a. Mitch Parker or Jeff Martz.

13. **What are the expected challenges to completing this deliverable?**
    a. Continued healthcare IT resource availability given the number of cyber events that have occurred in the past 18 months.

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
Gather resources	MBP/JM	25%	12/31/2021	Delayed due to Eskenazi cyber event
Organize/Select resources	MBP/JM	0%	1/1/2022	
Define format for toolkit	MBP/JM	0%	2/1/2022	
First draft of toolkit	MBP/JM	0%	4/1/2022	
Second Draft	MBP/JM	0%	5/1/2022	
Release	MBP/JM	0%	6/1/2022	
Communication Plan	MBP/JM	0%	6/1/2022	Info available from IHA, state portal, and through state communications mechanisms about this toolkit

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

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
Web Hosting	Need to host for providers	$0	$0			Can use existing IECC web site and Indiana resources

Benefits and Risks

17. What is the greatest benefit of this deliverable?

a. Provide the small and medium, low-staffed providers with templates to assess and address risks without having to spend significant dollars doing so.

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

a. This deliverable will provide healthcare providers with information they can use to self-assess and understand their risk profile from a good starting point. A basic risk assessment can cost $20,000. This can save providers at least that by giving them the info they need to do one of these on their own.

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

a. Small to Medium-sized Healthcare providers will not have information they need to properly assess and address risks to their environment. This will put them in a position of continuing to put patient data and personal information at risk.

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

a. We define success as the number of providers that successfully download and utilize this toolkit in their own practices to help address risks. The baseline for it is that right now 0 of them are doing so. Even 10 providers using this toolkit significantly improves security and is considered a success.

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

☐No ☒ Yes

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

☐ No ☒ Yes

Other Implementation Factors

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

a. The prevalence of cyberattacks in the state of Indiana can impact the resources needed to complete this deliverable.

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. This will require IECC Healthcare Committee members to periodically update these documents and the toolkit as regulations and policies change, specifically at the Federal level. They would also need to coordinate to upload them to the Cybersecurity portal.

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

a. The Health Sector Coordinating Council (HSCC).

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. We would need to notify healthcare providers across the state of Indiana using existing notification systems, the state portal, and appropriate communications mechanisms for web site updates.

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. We would want to involve IHA and potentially IPLA to notify their constituents of this toolkit.

Evaluation Methodology

Objective 1: IECC Healthcare Committee will create a "Healthcare Cyber in a Box" of security education designed for small- to medium-size offices and systems in 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: Healthcare Committee and partners will distribute Healthcare Cyber in a Box of security education information to 80 percent of Indiana healthcare providers.

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 3: IECC Healthcare Committee and partners will measure feedback/usage of the toolkit by 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:

Vendor Management - Healthcare IT Security, Risk & Compliance Handbook

Deliverable: Healthcare IT Security, Risk & Compliance Handbook

General Information

1. **What is the deliverable?**
   a. A short document resourcing Indiana healthcare practices and organizations of all sizes with needed information to ensure their security programs fit the most up-to-date regulatory requirements, especially with vendors.

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. To inform Indiana healthcare providers of recent updates in law and to provide accurate resources for practical implementation advice regardless of size.

6. **What metric or measurement will be used to define success?**
   a. An increasing number of Indiana businesses who assess their cybersecurity risks and make informed business decisions based on that review (whether they insure or not).

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

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

9. **Which state or federal resources or programs overlap with this deliverable?**
   a. The Health Sector Coordinating Council's Health Industry Cybersecurity Supply Chain Risk Management Guide (HIC-SCRiM) overlaps and will be included (https://healthsectorcouncil.org/HIC-SCRiM-v2/).

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Policy working group and possibly Strategic Resources working group

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

12. **Who should be main lead of this deliverable?**
    a. Cybersecurity Council office

13. **What are the expected challenges to completing this deliverable?**
    a. Continued resource allocations given current cybersecurity challenges.

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
Draft the initial document including key outline of processes and procedures Indiana providers need to implement	IECC Healthcare Committee – Mitch Parker, Philip Davis	0%	December 2021	
Circulate the document among the IECC Healthcare Committee for revisions and edits	IECC Healthcare Committee	0%	January 2022	
Implement Committee feedback and finalize document	IECC Healthcare Committee – Mitch Parker, Philip Davis	0%	March 2022	
Publish final draft on the Indiana Cybersecurity website	IECC Healthcare Committee – Mitch Parker, Philip Davis	0%	April 2022	

Resources and Budget

15. Will staff be required to complete this deliverable?

☐No ☒ Yes

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
1/8 FTE	1/8 FTE	Indiana Attorney General staff member skilled in healthcare/HIPAA Security Rule compliance actions	Cybersecurity Council Office	Indiana General Assembly	

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

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

Benefits and Risks

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

a. By publishing details on what Indiana providers need to know regarding their security and risk management programs and practices, state providers will more easily understand federal and state requirements, see fewer fines and compliance penalties, and be able to create more investment in their healthcare services serving Indiana residents.

b. By implementing the security program guidance contained within the document, Indiana healthcare businesses will be more prepared to respond to cyber-attacks and downtimes. As a noted critical infrastructure sector by federal agency Cybersecurity and Infrastructure Security Agency (CISA), Indiana will be contributing to the overall national increased readiness encouraged by the federal government.

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

a. It has been estimated that up to 60% of small and medium sized businesses fail within six (6) months of a cybersecurity attack. By encouraging small and medium sized businesses to protect against cybersecurity risks, Indiana companies will be better protected.
b. The average cost of a healthcare data breach in 2021 has risen to $9.23 million, up from $7.13 million in 2020 (IBM Security 2021 Cost of a Data Breach Report)
c. The average ransomware attack costs businesses $4.62 million (IBM Security 2021 Cost of a Data Breach Report).

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

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

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

a. The Cybersecurity Council could set a baseline of Indiana healthcare entities that have had a reportable breach and/or compliance penalties assessed in the year(s) leading up to the guideline publication, and a drop in both areas of breaches and compliance penalties would measure a successful effort.

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

☒No ☐ Yes

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

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

☒No ☐ Yes

a. We are not aware of initiatives in other states.

Other Implementation Factors

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

a. None known

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

☒No ☐ Yes

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

a. The ongoing effort will likely be monitoring Indiana healthcare entities who have suffered a reportable healthcare breach and/or received compliance penalties as a result.

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

a. No one outside of working group as of yet.

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 stakeholders would benefit from this information.

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

☐No ☒ Yes

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

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

b. The deliverable could be marketed at various healthcare-centric conferences and professional events

Evaluation Methodology

Objective 1: IECC Healthcare Committee will draft the initial document including key outline of processes and procedures Indiana providers need to implement by Qtr. 1, 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: Circulate the document among the IECC Healthcare Committee for revisions and edits by Qtr. 2, 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 3: Implement Committee feedback and finalize document by Qtr. 2 of 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 4: Publish final draft on the Indiana Cybersecurity website by Qtr. 3 of 2022.

Type: ☐ Output ☒ Outcome

Evaluative Method:

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

Deliverable: Exercise

Deliverable: Exercise

General Information

1. **What is the deliverable?**
   a. The Healthcare Committee will stage two tabletop exercises a year to simulate disasters and cyber-attacks across Indiana. These will be open to IECC members and Indiana healthcare organizations. The first exercise will be run by the IECC, and may include members of the Healthcare ISAC, CISA, Health Sector Coordinating Council, and American Hospital Association. The second exercise will be run with the National Guard at Fort Muscatatuck and will involve real-life simulations using their facility.

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. The goals of these exercises are to:
      - Simulate current cyber-attacks within a safe environment to determine opportunities for improvement
      - Provide information on current capabilities and strengths
      - Give a gap analysis of where to improve and why

6. **What metric or measurement will be used to define success?**
   a. Completion of the exercises
   b. After-action report with areas for improvement

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

8. **Who or what entities will benefit from the deliverable?**
   a. The IECC, participating healthcare organizations, recipients of the report, the Indiana National Guard, and other participating organizations would and have benefitted from this.

9. **Which state or federal resources or programs overlap with this deliverable?**
   a. The cybersecurity resources from the IECC, IOT, HSCC, and National Guard overlap.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. The IECC committee at large on planning, along with the National Guard, CISA, and HSCC to plan an exercise.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. We will need to work with IOT, the National Guard, CISA, and HHS/HSCC to complete this. The AHA and IHA are optional.

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

13. **What are the expected challenges to completing this deliverable?**
    a. Based upon the 2021 challenges with delivering both tabletops, it comes down to resource and time availability to plan out the scenarios. We also need time at Muscatatuck to effectively plan out the scenarios using their resources and planning.

Implementation Plan

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

☐ One-time deliverable

☒ Ongoing/sustained effort

Tactic Timeline

INCyber CISA Exercise – August 11, 2021

Tactic	Owner	% Complete	Deadline	Notes
Prepare with planning partners in initial, mid, and final planning meetings	USDHS CISA and IECC partners	100	Jan-July 2021	
Hold Exercise	USDHS CISA and IECC partners	100	Aug. 11, 2021	
Review AAR	Cybersecurity Program Director and USDHS CISA	100	October 2021	

INNG Homeland Defender Exercise – August 13, 2021

Tactic	Owner	% Complete	Deadline	Notes
Prepare with planning partners in initial, mid, and final planning meetings	INNG and IECC partners	100	Aug. 2021	
Initiate cyber IR component	INNG and IECC partners	100	Aug. 2021	
AAR	INNG	50	TBD	
Develop a W/WW workshop to hold virtually	IECC Partners	100	October 2021	

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
0.1	0.1	Planning				

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
Web Conferencing Platform	Needed to host the first tabletop exercise					
Fort Muscatatuck Computing Resources	Needed for real-life simulations of IoT					

Benefits and Risks

17. What is the greatest benefit of this deliverable?

a. The greatest benefit is the production of quantitative results and action plans that detail opportunities for improvement and areas where organizations can take steps to improve.

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

a. This deliverable reduces the risk and impact of a cyber-attack by providing exact steps and processes organizations can take to reduce them immediately based on the exercise. This can potentially save organizations thousands of dollars, if not more, by allowing them to focus on more immediate threats to their people, processes, and technologies.

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

a. We will not be able to simulate current cyber threats in an environment designed to identify issues for remediation. Organizations within Indiana would not be able to identify and address these threats and dependencies, and not be able to appropriately act if one of these events occurs.

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

a. Success is the completion of the exercise itself. The metrics used to measure success will be the after-action items that are needed to follow up on to address issues discovered during the exercises themselves. The baseline is based on the issues discovered, and the number is proportional to the degree of the success.

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

☒No ☐ Yes

a. Indiana is the only state that we are aware of that has involved federal and non-profit agencies, along with the National Guard, to the degree that we have in these exercises.

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

☒No ☐ Yes

a. There are not currently.

Other Implementation Factors

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

- Availability of resources at Fort Muscatatuck to help plan and develop the exercises
- Availability of IECC resources to help plan and develop the IECC exercise

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. We will need at least one IECC member and 2 Healthcare Committee members to work on planning these exercises on an annual basis.

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

a. We have been working with Chetrice Mosley, David Ayers, the HSCC, H-ISAC, Indiana National Guard, and American Hospital Association

27. Can this deliverable be used by other sectors?

☐No ☒ Yes,

a. In 2021 we worked with the Water sector on these. Based on the scenario picked for 2022 we will work with other sectors as identified by the exercise.

Communications

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

a. The entire IECC community and all Indiana healthcare organizations would be notified to see if they wish to observe or participate.

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. Since this is such a unique event for the state of Indiana, there will be media and conference opportunities to present this. This includes television and print media, along with security conferences such as RSA or Black Hat.

Evaluation Methodology

Objective 1: Working with partners, participate in a statewide cyber exercise that affects healthcare industry by August 2021.

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: Working with partners, participate in an exercise with the National Guard at Muscatatuck by August 2021 that addresses a known cyber vulnerability.

Type: ☒ Output ☐ Outcome

Evaluative Method:

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

Deliverable: Cyber Sharing Platform

Deliverable: Cyber Sharing Platform

General Information

1. **What is the deliverable?**
   a. Cyber Sharing Platform

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

4. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns.**
   ☐ 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.

5. **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

6. **What is the resulting action or modified behavior of this deliverable?**
   a. The goal of this cyber sharing platform is to facility sharing of cybersecurity information (i.e., Indicators of Compromise (IOCs), cyber observables, threats, intelligence, tactics, techniques, and procedures) among the healthcare sector at a tactical/technical level. The Healthcare WG will work with the Cyber Awareness and Sharing WG to leverage the IECC Cyber Sharing Community Slack channel to facilitate this deliverable. The resulting action is a grass roots sharing of cyber information in real time.

7. **What metric or measurement will be used to define success?**
   a. Number of IECC members in the IECC Slack Channel.

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

9. **Who or what entities will benefit from the deliverable?**
   a. All IECC healthcare members and their organizations

10. **Which state or federal resources or programs overlap with this deliverable?**
    a. DHS HSIN, H-ISAC Threat Intelligence Committee, HSCC

Additional Questions

11. **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

12. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable**?
    a. Representation from as many healthcare organizations will be necessary.

13. **Who should be main lead of this deliverable**?
    a. Nick Sturgeon

14. **What are the expected challenges to completing this deliverable**?
    a. Getting involvement from healthcare organizations.

Implementation Plan

15. **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
Beta Test	Nick Sturgeon	50%	October 31, 2021	
Go Live	Nick Sturgeon	0%	November 31, 2021	

Resources and Budget

16. Will staff be required to complete this deliverable?

☒No ☐ Yes.

17. 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
Slack Channel	This application is the medium in which the sharing will take place.	Free	$8/person	N/A	N/A	To get additional capabilities and features from the slack channel we would need to move up to the Pro plan. Additionally, Salesforce's purchase of Slack may mean additional costs.

Benefits and Risks

18. What is the greatest benefit of this deliverable? What are the estimated costs associated with that risk reduction?

a. By utilizing the IECC Cyber Sharing Community Slack Channel, it will provide a medium in which the technical cyber security staff of healthcare organizations can share cyber information in real time.

b. This Slack Channel will provide the means of our healthcare organizations and their cyber security/IT staff to share cyber information in real time. This will also allow them to connect with their peers in other organizations at a level they determine is sufficient. This also removes a choke point in sharing information out by elimination the need to rely on one person to share out information. Additionally, individuals can determine what information to share and what information to consume. The biggest cost reduction is time.

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

a. That critical cyber information will not get shared as broadly as needed.

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

a. The definition of success will be the total participation and engagement of the IECC members.

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. Unknown.

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. Unknown

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. We will need engagement from the IECC member organizations to keep this going.

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

a. IECC Cyber Awareness and Sharing Working Group

27. Can this deliverable be used by other sectors?

☐No ☒ Yes

a. This deliverable is something that can be used by all sectors.

Communications

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

a. The healthcare member organizations

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: IECC Healthcare Committee will Beta Test with the Cyber Awareness and Sharing Working Group by Qtr. 1 2022.

Type ☐ Output ☒ Outcome

Evaluative Method:

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

Supporting Documentation

Supporting Documentation

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

- Vendor Management – Best Practices
- Long-Term Education Materials
- Exercise News Release and Information Sheet

Vendor Management – Best Practices

GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

Best Practices – Vendor Management

IECC Partner IU Health has shared the following vendor policies and instructions for other organizations to use as a template for their own.

For their entire vendor management program, visit
https://iuhealth.org/about-our-system/vendor-relations

Indiana University Health, Inc. Standard Information Security Requirements and Demonstration of Compliance for Interfaces

These are minimum requirements required by IU Health's Information Security Program. We recognize that sound practices require continual assessment of evolving risks, technology and relevant issues related to information security. For the purposes of below, (i) each reference to "Agreement" shall be defined to include the BAA and Service Agreement, (ii) each reference to "Provider" shall be defined to include Business Associate, and (iii) each reference to "IU Health" shall be defined to include Covered Entity.

Any information technology system, application, or interface implemented as part of this Agreement that processes, stores, transmits, or receives information classified as Restricted or Critical by the IU Health Data Classification Policy is subject to the regulatory provisions regarding these data classifications, which include the Health Information Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act (FERPA), and the HITECH Act. Therefore, any such system implemented as part of this Agreement must:

i. Demonstrate that it is able to securely transmit and receive data in compliance with the HIPAA Security Rule, or HITECH Act, by utilizing Approved hashing and encryption algorithms from the NIST Cryptographic Algorithm Validation Program (CAVP) (https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program). Transport Layer Security (TLS) version 1.2 or greater and 256-bit Advanced Encryption Standard (AES-256) are IU Health's accepted standards for transmission security, and AES-256 is the accepted standard for encryption of data at rest. SHA-2 and SHA-3 are IU Health's accepted standards for cryptographic hashing algorithms.

ii. Demonstrate that data access requires a unique username/password or two-factor authentication (e.g., username and password, along with a personal identification number, certificate, software or hardware token, or smart card).

    1. If stored, login credentials will be hashed and salted using at least SHA-256 or encrypted using at least AES-256 encryption using FIPS 140-2 compliant encryption. At no time will plaintext credentials will be stored unprotected.

    2. For administrative access to the system to make configuration or security changes, two-factor authentication utilizing a secure application or physical token generating a cryptographically-generated key, or federation to a platform that performs it will be required.

    3. For services running on Microsoft Windows, utilization of Group Managed Service Accounts to run Windows Services will be required when possible.

    4. Authentication utilizing OAuth2 for customer-facing and authenticated Application Programming Interfaces (APIs) is required.

    5. User authentication needs to utilize OAuth2, SAML v2, Azure Active Directory, or similar federation technologies whenever possible.

iii. Demonstrate overall systems compliance by providing the following for mandatory review by IU Health's Information Security Team:

    1. An overall system architecture diagram, which includes a demonstration of logical separation of client data that prevents commingling of data.

2. A recommended network architecture implementation, including recommended segmentation, firewall rules, and network protection such as Data Loss Prevention to allow only applicable ports & protocols to protect data.
3. If this is a cloud-based or hosted system, a documented network architecture showing the security controls in place (e.g., firewalls, IDS/IPS, authentication, Data Loss Prevention, etc.).
4. Demonstrated reviews of firewall and Web Application Firewall (WAF) configurations to validate and verify minimum necessary rules are in place and that misconfigurations which can allow unauthorized access are avoided.
5. Demonstrated security scanning of the environment that includes credentialed and non-credentialed vulnerability scans of the internal and external environments, with a specific focus on addressing Server-Side Request Forgery (SSRF) and Cross-Site Request Forgery (CSRF) issues.
6. Demonstrated security scanning and vulnerability remediation of Application Programming Interfaces (APIs) that includes credentialed and non-credentialed vulnerability scans internally and externally, and full testing of APIs to the Open Web Application Security Project (OWASP) API Security Top 10 Security Project and OWASP Top 10 vulnerability types.
    a. Usage of Web Application Firewalls, API Gateways, or similar mitigation mechanisms to address vulnerabilities will not be considered valid vulnerability remediations by IU Health.
7. Static code analysis utilizing a verified third-party tool to ensure provided source code does not have any known security issues.
8. Security mechanisms on Source Code Control systems to track commits, pulls, or check-ins for potential security issues including trojan horses, malicious code, or backdoors inserted into source code using software supply chain toolsets such as in-toto (https://github.com/in-toto).
9. Digital signing of code and executables developed for the IU Health environment utilizing at least SHA-2 hashing algorithms and checksums.
10. Continual security monitoring of developer workstations, build environments, test machines, servers, and source code control systems.
11. Endpoint Detection and Response (EDR) software on developer workstations, build environments, test machines, source code control systems, and other systems used in the product development environment.
12. Periodic vulnerability testing of the environment to discover and remediate potential vulnerabilities.
13. If the product or service sends email on behalf of IU Health to team members or customers, the systems used to send email on behalf of IU Health must comply with Domain-based Message Authentication, Reporting, and Conformance (DMARC), DomainKeys Identified Mail (DKIM), and Sender Policy Framework (SPF). This is to protect against fraudulent emails being sent to recipients.

iv. Provide support for the application(s) or interface(s) running on a defined set of:

1. Operating Systems and supporting system services (e.g., OpenSSH, OpenSSL, Apache, Systemd).
2. Relational Database Management System Software (e.g., Oracle, SQL Server, MySQL).
3. Third-party software such as Application Servers, Web Servers, Security Software, Support Libraries, and other software required for daily operation of the application(s)

v. If there are discovered security vulnerabilities in the previously described items and/or the application(s)/interface(s), the following need to be provided within 48 hours to IU Health:

1. Mitigation steps that IU Health can undertake to mitigate the reported vulnerabilities.
2. A timeline for any application patches that need to be applied to the environment to mitigate vulnerabilities.
3. A timeline for testing and approval of patches to any of the supporting items described above.

vi. If there are discovered security vulnerabilities in the previously described items and/or the application(s)/interface(s), the following need to be provided within seven (7) days to IU Health:

1. Instructions for patching the supported items to restore the security posture of the environment.
2. Instructions for patching the application to restore the security posture of the environment.

vii. Ensure that the Operating System, any Relational Database Management System Software, and Third-Party software is supported by both the system and/or software vendors for the system lifecycle with system updates and security patches. If any of these components become unsupported, the Provider needs to address this before the system has an unsupported component.

Indiana University Health

Information Security

Indiana University Health, Inc. Guidelines on International Data Usage

The purpose of this exhibit is to set the requirements and guidelines by which IU Health data can be accessed by foreign third parties outside the United States and Canada. Due to the increased risk of data exfiltration and low enforceability of agreements across borders, IU Health has put these requirements and guidelines into place to protect stakeholders.

i. Data Hosting Location. IU Health data must be hosted in the United States, Canada, or a mutually agreeable location where data will be protected under appropriate privacy laws. IU Health will approve the ultimate destination(s) of data.
   a. If data is stored in a mutually agreeable location, the appropriate supervisory authorities will be contacted and advised. Appropriate documentation, such as a Data Protection Impact Analysis and supporting documentation under the European Union General Data Protection Regulation (GDPR) will be filed with them and shared with IU Health.
   b. Whenever possible, data stored outside the United States will be verified and validated using distributed technologies and cryptographic hashing used to keep copies of the hashes in multiple locations, including locations within the United States, even if the data itself resides outside the US.
      i. Distributed systems used to store these hashes must meet IU Health security requirements, detailed in the Indiana University Health Verification and Validation using Distributed Computing Requirements appendix.

ii. Data Access. Access to data outside the United States, Canada, or the agreed-upon location will be via remote or virtual desktop technology using two-factor authentication based upon strong cryptography using technology agreed upon by the vendor and IU Health.
   a. Text message-based authentication is not allowed due to interception risk.
   b. Devices used to access data must meet or exceed IU Health Security Standards

iii. Data Processing. IU Health data must be processed and/or have analytics performed on it in the United States, and the results of the analytics must be stored there.

iv. Data Security. Data stored outside the United States must be stored in facilities that are ISO 27001 certified.

v. Cloud Security. Data stored outside the United States with Cloud providers must be stored with ISO 27017/27018 certified providers. The provider must be certified for the region(s) the data will be stored in.

vi. Restricted Countries and Entities. IU Health forbids Business Associate or any of its subcontractors or subservice providers from directly employing resources or contracting for services on its behalf from countries on the US Department of the Treasury Office of Foreign Asset (OFAC) Control Sanctions Programs list, available at https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx. IU Health also forbids Business Associate or any of its subcontractors or subservice providers from directly employing resources or contracting for services on its behalf from people or companies on the US Commerce Department Bureau of Industry and Security Consolidated Screening List, available at: https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern

Information Security

Medical Device Security and Responsible Vulnerability Disclosure

1. **Medical Device Security Standards**
    a. Medical Devices in the scope of this agreement that are required to meet IU Health Security Standards include devices that have:
        i. Serial (RS-232, RS-485, etc.), Ethernet, Wireless Ethernet, Bluetooth, ZigBee, Cellular data, or other technologies that allow the wired or wireless transmission of data or signals over radio frequencies to another device or computer.
        ii. Persistent storage on the device itself such as a hard drive, solid state disk (SSD), or flash memory.
        iii. Universal Serial Bus (USB) ports.
        iv. Secure Digital (SD) or other forms of removable storage.
        v. A Central Processing Unit (CPU) and Random Access Memory (RAM) used for performing its essential functions.
        vi. A computing device attached to assist the device in performing its intended function.
    b. Applicable devices need to meet the requirements stipulated in the IU Health Standard Information Security Requirements and Demonstration of Compliance exhibit.
    c. Additionally, applicable devices need to demonstrate compliance with either the FDA Content of Premarket Submissions for Management of Cybersecurity in Medical Devices guidance, and/or the Underwriters Laboratories (UL) Standards for Software Cybersecurity for Network-Connectable Products (UL 2900-1).
2. **Responsible Vulnerability Disclosure Policy**
    a. Vendor hereby agrees to permit Indiana University Health (“IU Health”) and its subcontractors to conduct product and application security testing of devices in the scope of this agreement without limitation or restrictions and with the intent to identify potential security vulnerabilities in the software, hardware, devices, antennae, related configurations, and other properties available (“potential vulnerabilities”) on the devices in scope of this agreement.
    b. IU Health agrees equipment upon which any security testing is performed will not be placed in patient care operations. IU Health agrees to disclose potential vulnerabilities to Vendor at no unreasonable day and within 90 days of IU Health identification.
    c. Vendor agrees to provide a vulnerability mitigation plan to IU Health within 7 days of report and make product enhancements available within 90 days should IU Health, according to its own definition, determine the vulnerability prevents safe device utilization.
    d. Furthermore, Vendor agrees to publicly disclose potential vulnerabilities as soon as reasonably possible and at least within 90 days of receipt from IU Health.
3. **Medical Device Security Incident Costs**
    a. In the event of a Security Incident which Covered Entity or other entity with Privacy and Security Rules enforcement jurisdiction determines was proximately caused by nonconformance with the terms and conditions described in Indiana University Health, Inc. Standard Information Security Requirements and Demonstration of Compliance, Business Associate shall be responsible for all costs associated with the incident, including but not limited to: (i) Updating of device firmware and software to mitigate the vulnerability which caused the Security Incident to a current, non-vulnerable version; (ii) Updating of software on associated computing devices, servers, and supporting technology infrastructures to current, non-vulnerable versions; (iii) Remuneration for time spent by internal or contracted IU Health resources to mitigate the vulnerability; (iv) Reconfiguration of the Medical Device environment to conform to the Terms and Conditions in the Security Exhibit; (v) Retesting of the environment by IU Health Information Security or a third party to verify and validate that the Medical Device environment conforms to the requirements of the Standard Information Security Requirements and Demonstration of Compliance exhibit.

Indiana University Health

Information Security

Indiana University Health, Inc. Payment Card Industry – Data Security Standards Requirements

These are minimum requirements required by IU Health's Information Security Program for technologies used on behalf of IU Health for processing payment, credit, or debit cards in accordance with the Payment Card Industry – Data Security Standards (PCI-DSS) set by the PCI Security Standards Council. These are minimum acceptable security standards for protecting this information.

Any information technology system implemented as part of this Agreement that processes, stores, transmits, or receives payment, credit, or debit card information is subject to these requirements. Therefore, any system implemented as part of this agreement must:

i. Demonstrate full compliance with the PCI-DSS standards and associated amendments, available at https://www.pcisecuritystandards.org/ by demonstrating how IU Health will be able to achieve a successful Attestation of Compliance (AOC) by a Qualified Security Assessor (QSA) with the proposed solution.
ii. Work with IU Health to maintain full compliance, verifiable with successful Attestations of Compliance (AOC) with PCI-DSS security standards throughout the product lifecycle by developing an operational management plan to ensure currency of all in-scope components, including operating systems, supporting software, and third-party libraries.
iii. When the PCI-DSS standards update to a new version, provide an operational plan to ensure IU Health's compliance with it before the retirement date of the previous standard.
iv. If any part of the PCI-DSS solution is outsourced, provide the following for review by both the Enterprise Architecture and Information Security teams on an annual basis or upon update of the systems in scope to the current standards version:
    a. A PCI-DSS Attestation of Compliance (AOC) for the current standards version completed by a certified Qualified Security Assessor (QSA). We will not accept self-attestations or any substitute documentation.
        i. We will accept a verified successfully completed AOC in lieu of an IT Risk Assessment (ITRA).
    b. A Service Organizations Control Level 2 (SOC 2) report and HITRUST Common Security Framework (CSF) certification letter or ISO 27001/27018 certification by a certified accountancy for remote or cloud-based hosting facilities.
    c. A data flow diagram showing payment card data flow from entry to ultimate disposition of data.
    d. A network architecture implementation diagram demonstrating required segmentation, firewall rules, and network protection including firewalls, Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS), Data Loss Prevention/Cloud Access Security Broker technologies (DLP/CASB), Security Incident and Event Management Event Logging (SIEM), and strong cryptography.
    e. Demonstrated reviews of firewall and Web Application Firewall (WAF) configurations to validate and verify minimum necessary rules are in place and that misconfigurations which can allow unauthorized access are avoided.
    f. Demonstrated security scanning of the environment that includes credentialed and non-credentialed vulnerability scans of the internal and external environments, with a specific focus on addressing Server-Side Request Forgery (SSRF) and Cross-Site Request Forgery (CSRF) issues.
    g. Ensure that third parties that provide scripts or services to support the credit card processing environment have sufficient security controls, including PCI-DSS Attestation of Compliance where appropriate, to prevent malicious hijacking of their scripts. This is to help prevent Magecart-type attacks where credit card data is sent not only to its legitimate destination, but also to malicious third parties.
    h. Storage of Restricted or Critical data behind a stateful network firewall, ideally logically segmented and not stored on a device with a directly Internet-accessible Internet Protocol (IP) or Internet Protocol v6 (IPv6) address.
    i. Demonstrated two-factor authentication for administrative system access utilizing system(s) compliant with the NIST Special Publication 800-63B standards.
    j. Demonstrated provisioning and identity validation/proofing processes that are compliant with NIST Special Publication 800-63B standards.
    k. If the Business Associate or Third Party will not be compliant with the above, a documented explanation must be provided in a timely manner along with associated risk mitigation strategies.

v. If the PCI-DSS solution involves the collection of credit, debit, or payment card data over phone or voice telecommunication services, the standards in the PCI Standards Security Council Information Supplement, Protecting Telephone-Based Payment Card Data, must be followed for the most current version of the document available.
    a. The solution must be validated and certified by a certified QSA before production operations.
vi. Ensure that all in-scope devices promptly remediate discovered vulnerabilities in the operating system, applications, cryptographic subsystems, and third-party support software within seven (7) days.
vii. Enforce, utilizing network-based and logical controls, that only authorized parties can read, write, or otherwise access PCI-DSS data.
viii. Actively block traffic from malicious sources identified by the Financial Services Information Sharing and Advisory Center (FS-ISAC) and its member institutions.
ix. Enforce, utilizing network-based, logical, and physical controls, that the assets participating in the scope for PCI-DSS are only allowed to connect to systems or services required for authentication, disaster recovery, minimum necessary data interchange, administration, or maintenance.
x. Enforce, utilizing a combination of network-based and contractual controls, the following security controls and practices to address network-based spoofing and interception attacks, including BGP Hijacking and DNS Hijacking:
    a. Participant(s) will make sure that the internetworking infrastructure hosting distributed computing services in the scope of this agreement have Autonomous Service Numbers (ASNs) registered with the American Registry for Internet Numbers (ARIN – www.arin.net) or the equivalent for their geographic area(s).
    b. Participant(s) will make sure that all networking prefixes advertised by the ASNs for routing are properly registered with ARIN or its equivalent(s).
    c. Participant(s) will make sure that all networking providers that exchange traffic through peering arrangements filter announcements of their registered and advertised network address space by non-registered ASNs.
    d. Participant(s) will make sure that the provider(s) providing the internetworking infrastructure hosting their services have staffed Network Operations Center(s) operating 24 hours a day, 7 days a week.
    e. Participant(s) will make sure that the following service level agreements are in place with their provider(s):
        i. 5 minute alerting on network failures or issues with Border Gateway Protocol (BGP) or Domain Name Services (DNS).
        ii. 30 minute escalation to an on call network engineer who can make changes to Border Gateway Protocol (BGP) policies or DNS configurations in real time.
xi. Allow IU Health to audit information systems in the scope of the system(s) in scope of this agreement, including mutually agreed-upon penetration tests and vulnerability scans by the IU Health Information Security team or a certified Qualified Security Assessor.
xii. Allow IU Health to monitor the health of and system connectivity of information systems in the scope of the system(s) in scope of this agreement.
xiii. Allow IU Health to monitor the security posture of information systems in the scope of the system(s) in scope of this agreement, including operating system vulnerabilities, application vulnerabilities, network vulnerabilities, and cryptographic system vulnerabilities.
xiv. Provide strong, mutually agreeable, documented, and auditable processes for provisioning, validating, and verifying the identities of all parties with access to PCI-DSS data in accordance with NIST Special Publication 800-63B standards.
xv. Destroy all data no longer in use or required to be retained using a National Association for Information Destruction (NAID – www.naidonline.org) certified provider for PCI-DSS data.

Indiana University Health, Inc. Smart Contract Security Requirements

These are minimum requirements required by IU Health's Information Security Program for technologies used on behalf of IU Health to provide intelligent contracts, colloquially known as Smart Contracts, on behalf of IU Health. We recognize that this is a technology that can provide significant benefits to IU Health through their use to provide both contracts and automated responses to changes. The purposes of these requirements are to ensure that the underlying technologies utilized on behalf of IU Health are properly assessed and monitored for vulnerabilities that may compromise their integrity, that the contracts work as intended and designed, that IU Health has verification and validation that they are able to work in their intended environment, and that IU Health has reasonable and appropriate controls and measures to prevent intentional or unintentional misuse. For the purposes of below, (i) each reference to "Agreement" shall be defined to include the BAA and Service Agreement, (ii) each reference to "Provider" shall be defined to include Business Associate, and (iii) each reference to "IU Health" shall be defined to include Covered Entity.

i. Each Smart Contract needs to have a defined written use case, preferably in Unified Modeling Language (UML) format or a similar format that defines:
    a. Sender(s)
    b. Recipient(s)
    c. Input(s)
    d. Output(s)
    e. Actor(s)
        i. Blockchain/Distributed Ledger Technology (DLT) system that it will execute on
        ii. Other Contract(s)
        iii. Oracles, which are external resources that can trigger contract execution
        iv. Interfacing systems and methods
        v. Externally accessible media or files.
    f. Execution Conditions
    g. Preconditions
    h. Postconditions
    i. Programming Language Used
ii. All Smart Contracts need to be validated by a third-party Smart Contracts Validation Service which performs security and integrity testing on contracts to ensure that the contracts perform as intended. Of note, EY is specifically excluded due to their conducting financial services audits for IU Health.
    a. Contracts need to be tested by a neutral third party that does not have an interest in the contract or its outcomes or performs audit services for IU Health.
    b. Contracts need to be tested in a separate environment from the production environment.
        i. Both Business Associate and IU Health will provide non-production systems to the third-party validator to test use cases.
    c. As part of the validation testing, contracts need to be tested for the following:
        i. Race Conditions. This is when multiple concurrently executing contracts achieve different results based on timing and execution, and execution becomes dependent upon the timing, not the instructions within of the contract.
        ii. Reentrancy Attacks. This is when a smart contract can be interrupted in the middle of its execution and instructions to be used for the purpose of exploiting code vulnerabilities to transfer assets or resources outside the bounds of the contract to another party.
        iii. Concurrency Testing. Contracts need to be tested to ensure that multiple simultaneous running copies do not cause race conditions, reentrancy attacks, or behavior outside intended conditions.

iv. Timestamp Dependencies. Contracts need to be tested to ensure they are not dependent upon timestamps for conditions of execution, as this can potentially cause a Race Condition, Reentrancy Attack, or Concurrency issue leading to execution outside of defined bounds and exploitable vulnerabilities.
v. Resource Usage. Contracts will be tested to ensure that they execute instructions consistently and use a defined range of resources.
vi. Access to external resources and Oracles must be tested as part of the validation process.
vii. Upstream and downstream data interchange that occurs as part of the contract must be validated.
viii. Contracts must use validated Application Program Interfaces (APIs) and methods to communicate with upstream and downstream systems.

d. Media or files associated with Smart Contracts need to be stored on globally accessible media using InterPlanetary File System (IPFS).
    i. Pinning, which is the permanent storage of resources on IPFS, needs to be enabled for the lifetime of the contract for all associated media or files.
    ii. DNSLink, which uses Domain Name Services to map a domain name to an IPFS resources, needs to be configured and enabled for resources utilized in Smart Contracts.
    iii. When the hashing algorithm used on IPFS is changed, which changes the resource name, the DNSLink name must be updated.
    iv. Sensitive files must be encrypted using the public key(s) of the recipient(s).
e. Audit logging of all activities must occur, preferably using a Blockchain-based system to ensure their integrity.
    i. The audit log system utilized must meet the requirements in the Indiana University Health Verification and Validation using Distributed Computing Requirements appendix.
f. Zero-knowledge proofs must be utilized for Smart Contracts that contain sensitive or regulated information.
g. Blockchain systems and networks that host and execute these contracts must follow the security requirements in the Indiana University Health Verification and Validation using Distributed Computing Requirements appendix.

Indiana University Health

Information Security

Third Party Information Security Practices Due Diligence

Service Organization Control Reports, HITRUST Common Security Framework (CSF) certification, or Annual Risk Assessments.

Due to the increased security, availability, processing integrity, confidentiality, and privacy risks of using Business Associate and associated subservice providers to deliver Services to or on behalf of Covered Entity, Business Associate agrees to provide to CE an attestation of its and its applicable subservice providers that handle IU Health Confidential Information security risk assessments via an IT Risk Assessment (ITRA), ISO 27001/27017/27018 certifications, or Data Protection Impact Analyses and associated documentation, and Service Organizations Control Level 2 (SOC2) reports every year. A Health Information Trust (HITRUST) Common Security Framework (CSF) certification to the current framework will be accepted for every other year. For the purposes of this BAA, IU Health Confidential Information shall mean all non-public information, including, but not limited to, PHI, limited data sets, payment information, personally identifiable information (PII), nonpublic personal information (NPI), Covered Entity proprietary information, sensitive data or information, such that unauthorized access to such data may result in serious financial, legal or operational impact to Covered Entity.

i. *Health Information Trust (HITRUST) Common Security Framework (CSF) Certification.* If Vendor has provided proof of HITRUST certification, allow IU Health the right to review their HITRUST assessment certification letter in lieu of an IT Risk Assessment and SOC2 report.
    a. The HITRUST certification must be kept current within 1 year of review and be conducted by a certified assessor.
    b. The version of the CSF attested to must be current within 1 year of review.
    c. Vendor must provide a copy of the certification letter to IU Health, which has the name of the assessor and the version of the HITRUST Common Security Framework (CSF) that has been attested to and certified.
    d. If the certification lapses or is not to a reasonable current framework version as described in (2), IU Health will immediately require a SOC 2 report and full IT Risk Assessment (ITRA).

ii. *Service Organization Control Reports.* Due to the increased security, availability, processing integrity, confidentiality, and privacy risks of using Business Associate to deliver Services to or on behalf of Covered Entity, Business Associate agrees to annually provide a Service Organization Control 2 (SOC 2) Type 2 report to Covered Entity if (1) it provides Service Organization services to Covered Entity involving IU Health Confidential Information that Covered Entity would otherwise perform such as medical record services, data centers, IT managed services, software as a service (SaaS) vendors, and many other technology and cloud-computing based businesses, or (2) it is required as more particularly described in Exhibit A attached hereto. For the purposes of this, "IU Health Confidential Information" shall mean all non-public information, including, but not limited to, PHI, limited data sets, payment information, personally identifiable information (PII), nonpublic personal information (NPI), Covered Entity proprietary information, sensitive data or information, such that unauthorized access to such data may result in serious financial, legal or operational impact to Covered Entity.

iii. *ISO 27001/27017/27018 Certification.* If Vendor has provided proof of ISO 27001/27017/27018 certification, allow IU Health the right to review their ISO certification in lieu of an IT Risk Assessment and SOC2 report.
    a. The ISO certification must be kept current within 1 year of review and be conducted by an accredited certification body (e.g. ANSI-ASQ National Accreditation Board [ANAB]) or a certified accountancy.
    b. Vendor must provide a copy of the certification letter to IU Health, which has the name of the assessor and the ISO standards that have been attested to and certified.
    c. If the certification lapses or is not to a reasonable current framework version as described in (2), IU Health will immediately require a SOC 2 report and full IT Risk Assessment (ITRA).

Information Security

iv. *European Union General Data Protection Regulation (GDPR) or similar governmental level privacy regulations.* If Vendor has provided proof of compliance with the below, IU Health will review in lieu of an IT Risk Assessment and SOC2 Report. The deliverables need to be in the form of:
    a. A completed Data Protection Impact Assessment (DPIA) or equivalent, including risk assessment and risk management plan.
    b. An assigned Data Protection Officer who has oversight and responsibility for execution of the DPIA, and the review and remediation processes.
    c. Evidence of communication with supervisory authorities about the DPIA, risk assessment, and risk management plan.

v. *Manufacturer Disclosure Statement for Medical Device Security (MDS2) – 2019 revision.* If vendor has provided a completed MDS2 statement for their medical device (not supporting hardware or software), and the MDS2 form submitted is using the 2019 revision of it or later, IU Health will accept this in lieu of an IT Risk Assessment. Older versions do not address current and emerging risks.

vi. *Information Technology Risk Assessment (ITRA).* If the Business Associate cannot provide evidence of HITRUST or ISO certification, sufficient evidence of compliance with GDPR or similar applicable regulations, or a valid MDS2 2019 form for their medical device, the Business Associate needs to Provide IU Health responses to the provided Vendor Risk Assessment and Security Questionnaire.

Any misrepresentation on any of these documents may result in contract termination.

Indiana University Health, Inc. Verification and Validation Using Distributed Computing Requirements

These are minimum requirements required by IU Health's Information Security Program for technologies used on behalf of IU Health to provide verification and validation services utilizing distributed computing. Such technologies include Blockchain, which is its current and most common usage. We recognize that this is a technology that can provide significant benefits to IU Health through their use to validate and verify transactions. The purpose of these requirements is to ensure that the underlying distributed computing technologies utilized on behalf of IU Health are properly assessed and monitored for vulnerabilities that may compromise their integrity, and the data and systems they are meant to provide integrity for. For the purposes of below, (i) each reference to "Agreement" shall be defined to include the BAA and Service Agreement, (ii) each reference to "Provider" shall be defined to include Business Associate, and (iii) each reference to "IU Health" shall be defined to include Covered Entity.

Any information technology system implemented as part of this Agreement that processes, stores, transmits, or receives information that utilizes distributed computing technologies to provide verification and validation services to ensure the integrity of IU Health data is subject to these requirements. Therefore, any system implemented as part of this agreement must:

i. Demonstrate that no data that can be classified as Protected Health Information (PHI), Payment Card Industry-Data Security Standards (PCI-DSS), Family Educational Rights and Privacy Act (FERPA), or Privacy Act data will be stored as part of these systems.
ii. Demonstrate that only minimum necessary data from source systems is used to generate cryptographic hashes using a SHA-256 or greater hashing algorithm which will be stored on said Distributed Computing Service.
iii. Demonstrate that no single entity will have control of more than 50% of the total computing power available to process transactions for distributed computing services. This is because if one entity has control of more than 50% of the computing power, they will be able to alter transactions and compromise system integrity.
iv. Ensure that all participants in the distributed computing service promptly remediate discovered vulnerabilities in the operating system, applications, cryptographic subsystems, and third-party support software that directly interfaces with it or produces data to be utilized by the service within seven (7) days.
v. Ensure that all participants in the distributed computing service have a security management program in place to cover not only the assets involved in the distributed computing service, but also all other assets in the purview of the organization.
vi. Enforce, utilizing network-based and logical controls, that only authorized parties can read, write, or otherwise access the Distributed Computing services.
vii. Enforce, utilizing network-based, logical, and physical controls, that the assets participating in the distributed computing service are only allowed to connect to systems or services required for authentication, disaster recovery, minimum necessary data interchange, administration, or maintenance.
viii. Enforce, utilizing a combination of network-based and contractual controls, the following security controls and practices to address network-based spoofing and interception attacks, including BGP Hijacking and DNS Hijacking:
    a. Participant(s) will make sure that the internetworking infrastructure hosting distributed computing services in the scope of this agreement have Autonomous Service Numbers (ASNs) registered with the American Registry for Internet Numbers (ARIN – www.arin.net) or the equivalent for their geographic area(s).
    b. Participant(s) will make sure that all networking prefixes advertised by the ASNs for routing are properly registered with ARIN or its equivalent(s).
    c. Participant(s) will make sure that all networking providers that exchange traffic through peering arrangements filter announcements of their registered and advertised network address space by non-registered ASNs.
    d. Participant(s) will make sure that the provider(s) providing the internetworking infrastructure hosting their services have staffed Network Operations Center(s) operating 24 hours a day, 7 days a week.
    e. Participant(s) will make sure that the following service level agreements are in place with their provider(s):

   i. 5 minute alerting on network failures or issues with Border Gateway Protocol (BGP) or Domain Name Services (DNS).
   ii. 30 minute escalation to an on call network engineer who can make changes to Border Gateway Protocol (BGP) policies or DNS configurations in real time.

ix. Allow IU Health and other members of the Distributed Computing services to audit information systems in the scope of the system(s) in scope of this agreement.
x. Allow IU Health and other members/users of the Distributed Computing services to monitor the health of and system connectivity of information systems in the scope of the system(s) in scope of this agreement.
xi. Allow IU Health and other members/users of the Distributed Computing services to monitor the security posture of information systems in the scope of the system(s) in scope of this agreement, including operating system vulnerabilities, application vulnerabilities, network vulnerabilities, and cryptographic system vulnerabilities.
xii. Allow IU Health and other members/users of the Distributed Computing services to terminate all access to any information systems which have not been patched or remediated for vulnerabilities within seven (7) days as they pose a risk to the integrity of the system.
xiii. Provide strong, mutually agreeable, documented, and auditable processes for validating and verifying the identities of all participants in the Distributed Computing system.
xiv. Provide verifiable Public Key Infrastructure digital certificates and identities to identify all participants that are issued by a mutually agreeable third party. Self-signed certificates are not acceptable.
xv. Ensure that all data elements utilized as part of the distributed verification and validation system undergo data quality checks. This is to make sure that we only utilize verified and validated data as inputs.
xvi. Ensure that transactions recorded as part of the distributed verification and validation system can be reconciled against transactions from the source computing resources.
xvii. Ensure that identities used to publish transactions to the distributed verification and validation system can be verified, and the cryptographic identities of the series of transactions said identities made can be validated.
xviii. Demonstrate third-party risk management processes by mapping cryptographically verified identities involved in transactions to legal entities, and identifying and reconciling all legal entities in the transaction chain.
xix. Ensure that there is a documented method and process for appending records to the system to amend existing records in case of a correction.
xx. Ensure that there is a governance process by which disputed transactions can be arbitrated and amendments posted to the distributed verification and validation system.

Indiana University Health

Information Security

Indiana University Health, Inc. Wireless, Cellular, Real Time Location System (RTLS), Radio Frequency Identification (RFID), and Near Field Communications (NFC) Requirements

These are minimum requirements required by IU Health's Information Security Program for technologies used on behalf of IU Health for the implementation or usage of Real Time Location Systems (RTLS), Radio Frequency Identifier (RFID), or Near Field Communication (NFC) systems. As these technologies have the potential to be used to support patient tracking, supply chain operations, patient engagement, and tracking of equipment and assets, IU Health needs to ensure that the data and algorithms used by these systems is demonstrably accurate and protected.

Any information technology system implemented as part of this Agreement that implements these technologies is subject to these requirements. Therefore, any system implemented as part of this agreement must:

i. Define exactly what use cases the solution(s) will be utilized for in the IU Health environment.
ii. Ensure that this system will not store Protected Health Information (PHI), Personally Identifiable Information (PII), Payment Card Industry-Data Security Standards (PCI-DSS), or Family Educational Rights and Privacy Act (FERPA) data.
    a. Payment Solutions that utilize Near Field Communications, such as Apple Pay, are covered by the PCI-DSS security requirements and are exempt from these requirements.
iii. Only utilize minimum necessary data to achieve the desired use cases.
iv. Use system-generated numbers or identifiers that are not based on PHI, PII, PCI-DSS, or FERPA data.
v. Utilize mapping and location information supplied by Design & Construction and Telecommunications.
vi. Ensure that there is adequate wireless coverage for the areas and defined use cases for successful operation of the solution.
vii. Ensure that there is no interference with existing wireless solutions.
viii. Whenever possible, provide enclosures or mechanisms to reduce the potential for signal interception.
ix. Follow cabling and installation standards as defined by the IU Health Telecommunications team in their standards documentation.
x. Systems must be able to be segmented from the main corporate network and communicate over a defined set of network addresses, ports, and protocols to a defined set of IP addresses.
xi. Systems used to send and receive collected data and transmit/receive said data to and from official systems of record, including Enterprise Resource Planning (ERP), Electronic Medical Record (EMR) systems, or other designated IU Health applications, must run vendor-supported operating systems, databases, and supporting libraries, and be patched against known vulnerabilities.
xii. If the solution contains Bluetooth 4.0 or greater or Bluetooth Low Energy (LE):
    a. Security Levels 2, 3, or 4 must be enabled using at least 128-bit Advanced Encryption Standard (AES-128) and Elliptic Curve Diffie-Hellman Key Exchange (ECDHE).
    b. Bluetooth LE Privacy Mode must be enabled to prevent eavesdropping of individual Media Access Control (MAC) addresses.
xiii. If the solution utilizes Near Field Communications (NFC):
    a. Change the encryption keys from the default settings.
    b. Follow the security standards in the ECMA-385 standard, NFC-SEC-NFCIP-1 Security Services and Protocol.
xiv. If the solution supports Wireless Internet utilizing Wi-Fi:
    a. Support the latest standards that IU Health supports.
    b. Support WPA2 or WPA3 authentication to encrypt data in transit and protect against improper alteration of data.
xv. If the solution supports cellular technologies, either Long Term Evolution (LTE/4G) or IMT-2020 (5G):
    a. Solution must be deployed using 5G network slicing to isolate application traffic to a defined segment if using direct device connectivity whenever possible.

b. If the solution utilizes site to site connectivity, Software Defined Wide Area Networking (SD-WAN) technologies must be used to protect communications.
c. All transit utilizing LTE or 5G networks must be actively monitored for security events.
d. Demonstrated reviews of firewall and Web Application Firewall (WAF) configurations to validate and verify minimum necessary rules are in place and that misconfigurations which can allow unauthorized access are avoided.
e. Demonstrated security scanning of the environment that includes credentialed and non-credentialed vulnerability scans of the internal and external environments, with a specific focus on addressing Server-Side Request Forgery (SSRF) and Cross-Site Request Forgery (CSRF) issues.
f. Periodic vulnerability testing of the environment to discover and remediate potential vulnerabilities.
g. All equipment utilized in the transit of data from the access points to the termination point at the IU Health network must be kept current and protected against security vulnerabilities.
    i. Any equipment utilized in the transit of data must not be from a prohibited vendor covered under Section 889 of the National Defense Authorization Act (NDAA) of 2019.
h. Enforce, utilizing a combination of network-based and contractual controls, the following security controls and practices to address network-based spoofing and interception attacks, including BGP Hijacking and DNS Hijacking:
    i. Participant(s) will make sure that the internetworking infrastructure hosting distributed computing services in the scope of this agreement have Autonomous Service Numbers (ASNs) registered with the American Registry for Internet Numbers (ARIN – www.arin.net) or the equivalent for their geographic area(s).
    ii. Participant(s) will make sure that all networking prefixes advertised by the ASNs for routing are properly registered with ARIN or its equivalent(s).
    iii. Participant(s) will make sure that all networking providers that exchange traffic through peering arrangements filter announcements of their registered and advertised network address space by non-registered ASNs.
    iv. Participant(s) will make sure that the provider(s) providing the internetworking infrastructure hosting their services have staffed Network Operations Center(s) operating 24 hours a day, 7 days a week.
    v. Participant(s) will make sure that the following service level agreements are in place with their provider(s):
        1. 5 minute alerting on network failures or issues with Border Gateway Protocol (BGP) or Domain Name Services (DNS).
        2. 30 minute escalation to an on call network engineer who can make changes to Border Gateway Protocol (BGP) policies or DNS configurations in real time.

xvi. Provide a monitoring system, model processes, and support in detecting the following fraudulent usage scenarios:
    a. Unauthorized tag or device cloning.
    b. Multiple instances of tag or device IDs.
    c. Unauthorized alteration of stored values on devices or tags.

xvii. Provide structured asset management data on all devices or tags that can be imported into an enterprise asset management system, including but not exclusive to:
    a. Serial Number
    b. Device Name
    c. Device Type
    d. Media Access Control (MAC) Addresses
    e. Firmware Version.
    f. Date of Manufacture.
    g. Warranty Dates.

Long-Term Education Materials

How to develop and execute a patch management routine (CMMC L1)

Mitchell Parker, IU Health

Indiana University Health

Why are we here?

- Any software application including operating systems, firmware, or plugin installed on a system could provide the means for an attack
- Many software vendors provide patches and updates to their supported products in order to correct security concerns and to improve functionality
- This session will ensure that you know how to update and patch software on each device you own

What is the requirement/control?

- From NIST 800-171/CMMC L1 3.4.2e
- Employ automated mechanisms to detect the presence of misconfigured or unauthorized system components and remove the components or place the components in a quarantine or remediation network that allows for patching, re-configuration, or other mitigations.

Why is it important?

- This helps us protect against known vulnerabilities
- It also is item #1 in any DOD Security Technical Implementation Guide
  - Right before configuring least privilege
- You can't have least privilege if you can get around it easily
- It also is a massive issue if you don't patch

How Does it Protect My Information?

- According to Tripwire [1]: 27% of data breaches caused by unpatched vulnerabilities
- Patching security vulnerabilities measurably protects information from known issues that can be used to exfiltrate data

- [1] https://www.tripwire.com/state-of-security/vulnerability-management/unpatched-vulnerabilities-breaches/#:~:text=Unpatched%20Vulnerabilities%20Caused%20Breaches%20in%2027%25%20of%20Orgs%2C%20Finds%20Study,-Ray%20Lapena&text=In%20May%202019%2C%20Verizon%20Enterprise,Breach%20Investigations%20Report%20(DBIR).

What are the consequences of not implementing this control?

- Data Breaches
- Security Issues
- Reputational Harm
- Regulatory Issues/Fines
- Loss of Credibility
- Lack of Ability to Keep Environment Current

OK, what do I really need to do?

- Assume that I don't know IS management well however understand how to run a business – not going to assume you are clueless or inferior

Inventory

- Get an inventory of all the devices in your environment
  - Including Network Devices!

- Also get an inventory of what software you have both on premises and the cloud
- You want to refer to the 7/30/2020 presentation on Methods to inventory and document organizational hardware and software from TCC Solutions – available at: https://mep.purdue.edu/news-folder/20-cyber-topics-in-20-weeks-series-schedule-free/
  - This goes into much greater detail!

Assign someone to keep track

- Assign someone to keep track of them – they do not have to be technical – just keep it updated – manage like a business!
  - Name
  - Description
  - Vendor
  - Contract term
  - Responsible user
  - Sw version
  - Purchase date
  - Number of copies
  - End of support date

What are free or low-cost options to implement the control?

- Make sure you are running a supported operating system
  - If you're running Raspbian, Ubuntu, or Debian, open up a terminal window and type:
    - Sudo apt update;sudo apt upgrade
  - If you're running Red Hat or CentOS, open up a terminal window and type:
    - yum update –security

Include all devices

- Include HVAC, embedded systems, and your facilities management systems
- Too often we ignore these and have critical business functions running on obsolete hardware and software

Determine Support Dates

- Determine software dates for software packages and libraries:
  - Check Vendor Web Sites for software separately bought and installed
  - If it comes with Windows, MacOS, or Linux, will be updated by the OS update programs
  - For the OSes themselves, we've provided instructions for the most popular ones:

Devices Covered

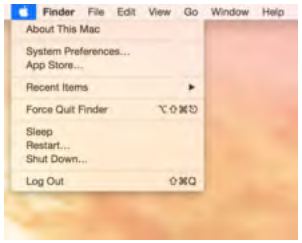
- How do we know if a device is supported?
- Linux:
  - Ubuntu: https://wiki.ubuntu.com/Releases
  - Red Hat: https://access.redhat.com/support/policy/updates/errata
  - Debian: https://wiki.debian.org/DebianReleases
  - Raspberry Pi: https://www.raspberrypi.org/downloads/
- MacOS:
  - https://support.apple.com/en-us/HT201222
- iOS/iPadOS:
  - Only the current version gets updates

Devices Covered

- Android: Generally only within the past year
- Windows:
  - https://support.microsoft.com/en-us/help/13853/windows-lifecycle-fact-sheet
- Chromebooks:
  - https://support.google.com/chrome/a/answer/6220366?hl=en

MacOS

- Click Here:



- Click About This Mac
- Click Software Update:

MacOS

- You will then get this screen. Click Update Now to update

iOS/iPad OS

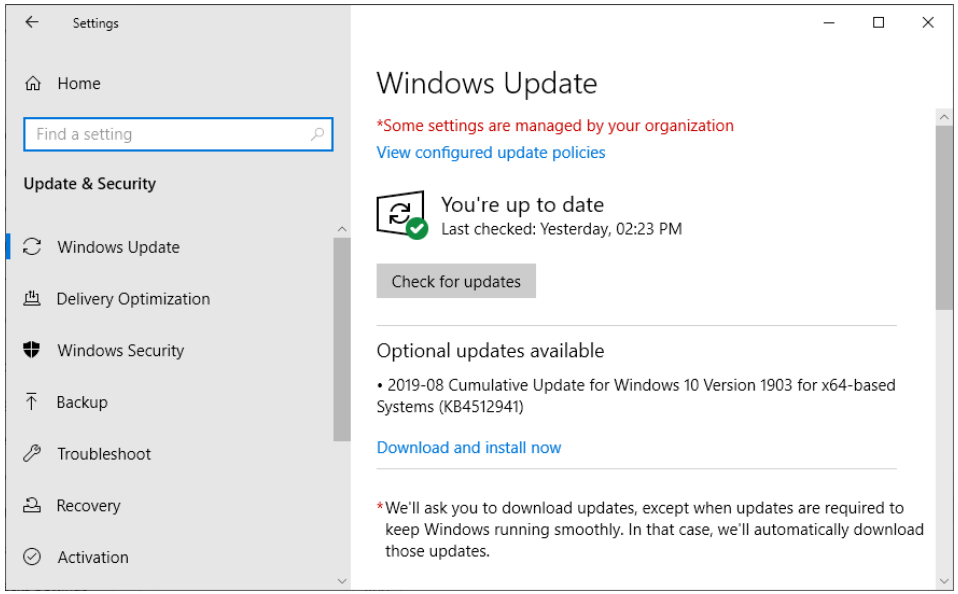
- Go to Settings From the Home Screen:

iOS/iPad OS

- Go to General -> Software Update -> Download and Install

Windows

- Go to Settings -> Windows Update and click on Check for Updates:



Android

- Since this is complex, we just point to the instructions here:
- https://www.lifewire.com/check-updates-for-android-1616953

Chromebook

- Google provides a link to instructions in one place
- https://support.google.com/chromebook/answer/177889?hl=en
- If your device is supported, this should work

What else do I need to patch?

- Operating Systems
- Applications
- Database Systems and Services
- Supporting Libraries

Additional Caveat

- If you have a Zebra industrial device, you will need to contact them to get software updates under a software support contract!

Planning to Update

- If something is 1-2 years out for not receiving patches, plan to replace it
- If you have a smartphone, plan for 2 years for a Samsung, 3-4 for an Apple, and everything else replace within a year
  - Because patches don't come for older Android devices
- If you have older devices, build plans to update/upgrade them

How do I do that?

- Build a monthly schedule to:
  - Check for patches
  - Communicate with customers and let them know what's going on
  - Test patches
  - Apply Them in Production

What do I do if I can't patch something?

- How do I isolate it with wired network equipment?
  - Create a separate Virtual Local Area Network (VLAN)
  - Use your firewall to only allow communications to/from this network to only ports and protocols your application explicitly needs
  - Only allow administrators access to ports needed for remote administration and systems management
  - This may slow performance however is the best alternative for wired equipment

What if I can't patch something?

- How do I isolate it with a Raspberry Pi or older PCs?
  - Configure a firewall on the device using IPFire (www.ipfire.org)
  - Only allow incoming ports for what's absolutely needed
  - Configure Secure Shell or VPN to access ports for what else is needed

What if I can't patch something?

- How do I isolate older WiFi?
  - Get a secondary wireless access point or SSID broadcasting on a different channel
  - What are the effects on WiFi I need to consider?
    - Slower speed for all devices
    - Less security for newer devices
    - If you don't manage, less security for all devices
  - They can't take advantage of newer security and lower the security to the lowest common denominator – so keep them isolated!

What if I can't patch something?

- There's effects on data interchange
- Less secure newer systems
- Less secure data interchange – potential for interception and alteration of data
- We need to keep systems patched and updated so we can secure data interchanges
- That old FTP doesn't "just work". It can be intercepted and your data can be taken!

Let's recap…

- Inventory
- Assign someone to keep track and manage it like a business
- Include All Devices
- Keep track of support dates
- Patch OSes, Applications, Databases, and Supporting Devices
- Plan to Update
- Have a plan for when you can't patch to isolate
  - Especially Wireless!

Thank you!

- Thank you for your time!
- Email: mparker17@iuhealth.org
- Twitter: @mitchparkerciso

Proactive and Preventative Vendor Security Management

Mitchell Parker, Executive Director, Information Security, Indiana University Health

Indiana University Health

Agenda

- Statement of Issue
- Background on Security
- Mergers and Acquisitions
- Background on Devices and Systems
- Business Drivers
- What has happened?
- Where do we start?
- The five key areas of technology management
- Conclusion

Learning Objectives

- Recognize the requirements for implementing an effective vendor management program for technology
- Apply knowledge learned from this presentation to proactively improve vendor relations
- Analyze existing vendor agreements and outsourcing contracts and be able to modify them to support information security initiatives
- Develop effective requirements and goals for Clinical Engineering to accomplish either via statements of work or program management to support security requirements
- Define and measure the effectiveness of an enterprise-wide preventive security program and demonstrate metrics to senior management

Statement of Issue

- We have too much vendor technologies and not enough guidance on how to effectively manage security for them
- In the past decade, as we've increased the usage of Electronic Medical Records, and have automated manual processes, we've connected a significant number of new technologies to the network
- There has not been a corresponding increase in expertise with cybersecurity on many fronts

Background on Security

- Medical Providers are not all large academic healthcare institutions
  - According to the American Medical Association, in 2014, 60.7% of the medical providers out there are small practices with 10 or fewer physicians.
    - Source: https://www.ama-assn.org/press-center/press-releases/ama-study-finds-majority-physicians-still-work-small-practices
  - According to the American Hospital Association in 2016, the average operating margin was 6.7%, with 30.6% of hospitals having negative operating margins
    - Source: https://www.aha.org/system/files/2018-05/2018-chartbook-table-4-1.pdf

Background on Security

- Medical Providers are not all large academic healthcare institutions
  - According to the Nebraska Hospital Association in a personal interview, 75% of the hospitals in their state are rural and in small towns
    - These hospitals don't have IT departments. They have outside consultants or someone doing IT as a side job
    - Rural and Critical Access Hospitals, as a rule, have people that have multiple skills or jobs

Background On Security

- Many of these providers and hospitals do not have the staff to maintain security
- They are lucky if they have staff to maintain the EMR
- We are at an inflection point with new technologies where the security world is going to get turned upside down on providers again
  - New WiFi standards (WiFi 6, 802.11ay)
  - 5G/Reliance on Cellular Service
  - Sunsetting of legacy technologies such as Pagers
  - Shift to Consumerism

Mergers and Acquisitions

- There has been significant acquisition activity with health services companies actively making deals changing the system landscape
  - Pennsylvania alone has had UPMC, Jefferson, Penn Medicine, and Tower Health reshape the landscape since 2014
  - New Jersey has had Hackensack Meridian and Barnabas Health do the same
  - Advocate/Aurora in the Midwest has also had impact
  - CHS has had both significant acquisitions and divestures nationally
  - According to PwC's US Health Services Deals Insights Q3 2018, there were 261 transactions in Q3 2018, and over 200 in each quarter since Q4 2014
    - Source: https://www.pwc.com/us/en/health-industries/publications/pdf/pwc-us-health-services-deals-insights-q3-2018.pdf

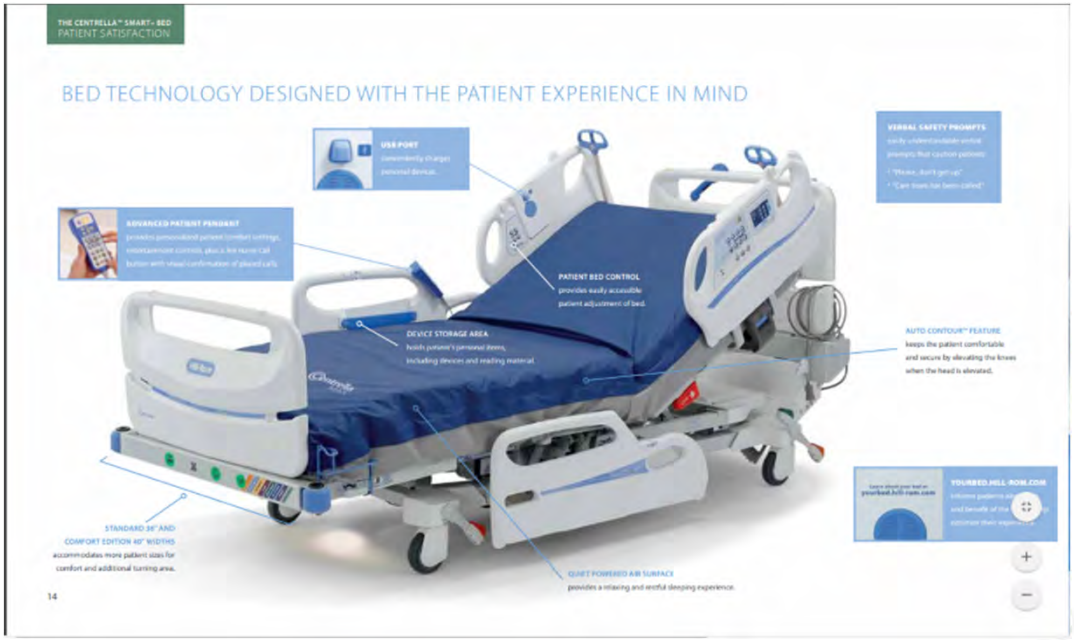
Background on Devices and Systems

1. How does this all relate to them?

- We have had to get very smart about cybersecurity as part of the "M&A Playbook" very quickly for both
- Medical devices, which at one time were considered a capital expense like a bed or supplies, are computer systems in themselves
  - Scratch that part about the bed…the new ones are full-fledged systems in themselves!
  - Not having a plan as you acquire/divest will lead to risks later

Background on Devices and Systems

- Smart Bed Example:



Background on Devices and Systems

2. More about devices…

- They are pervasive
- They are now part of the care process
- They originally were never meant to be networked in a TCP/IP network
  - Serial devices, yes, where a continual data stream could be sent uninterrupted
  - Ethernet and TCP/IP are very different than Serial
  - Wireless is even more difficult to account for (no lines)
  - 5G/Cell-based technologies have to take more into account
  - PACS/DICOM is an exception to this
- This change is still a major challenge that vendors are working on as it greatly increases complexity!

Background on Devices and Systems

3. Appliances

- These were mainly designed as appliances that require basic upkeep
- We've managed them the way we always have, which is by either:
  - A small Clinical Engineering Team
  - Outsourced Third-Party Contractors
  - Consultants
  - The Vendors themselves

Background on Devices and Systems

4. Networking

- We've put them on the same networks as other devices
  - This is not out of ignorance – people willing to accept risk
  - Not everyone understands networking or security well
  - Not everyone has resources to have a full security program
  - This exposes devices that were never meant to be put on large networks with lots of traffic to exactly that
    - Manufacturers are still grappling with the change from serial to TCP/IP
    - Upcoming FDA guidance speaks of encryption and key management
    - We are increasing complexity significantly!

Background on Devices and Systems

5. Smaller Offices = Consumer/Small Office Devices

- Connectivity to a lot of smaller offices is done using consumer equipment
  - Think Linksys, Belkin, Netgear, or what the local store carries
  - Consumer equipment doesn't have the long support lifecycles of gear from Palo Alto, Cisco, or Fortinet
  - It also is a lot easier to set up for non-IT professionals
  - When you have limited resources, you're not going to put something in that has a high chance of breaking and can't quickly fix or replace. You're going to go to Wal-Mart or someplace within a 30 minute drive
    - When you need something quickly and have patients waiting, you are not going to wait

Background on Devices and Systems

6. Vendor Support

- This is also done for vendor support purposes. It's easier for a tech to remote into a PC and then connect to a device or system either over USB or the network if it's on the same segment than to put in a persistent VPN connection
  - VPN connections open up additional risk
  - We can't expect medical offices that run on consumer grade equipment to even know what IPSec is
  - It's hard for software developers to grasp the nuances of networking and PKI
    - Numerous breaches caused by insecure security implementations prove that
      - **Heartbleed and variants**

Background on Devices and Systems

7. Aftermarket Devices

- We have a very large aftermarket of used devices across the world
  - Smaller facilities and those in non-First World countries buy these devices used
    - They are not always cleaned off or secured
    - They likely aren't getting updates
    - Many of these devices are older and won't get updates

7. Aftermarket Devices

Maastricht University donated an MRI to the Cuban Neurosciences Center:

Background on Devices and Systems

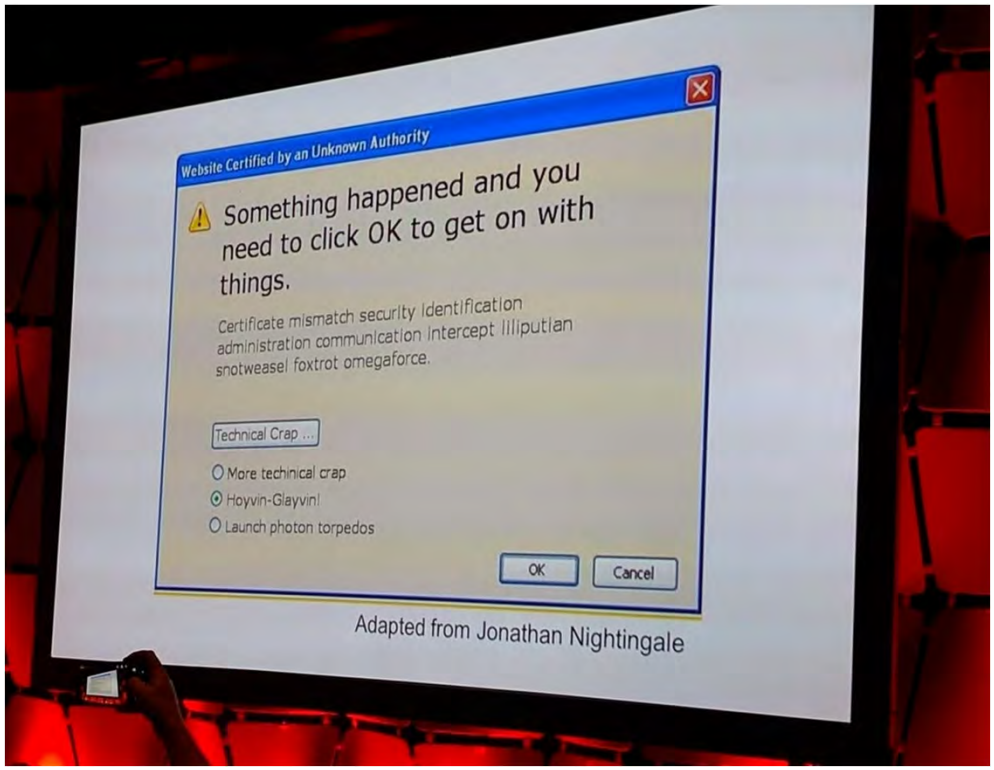
7. Aftermarket Devices

- We also need to account for these in M&A and Divestures
  - Do they meet the new corporate standard?
  - Have they been assessed for risk?
  - Most important – if the facility has had financial difficulties, did they cut support?

Business Drivers

- We have business drivers driving the Internet of Medical Things (IoMT)
  - Shift from Inpatient to Outpatient
  - Need for Monitoring of chronic patients (COPD, diabetes) and compliance
  - Patient Satisfaction/Clinician Communication
  - Population Health
  - Smartphones and Health Apps
  - Fitbits and Consumer Devices

What does the business see?



One Weird Trick…

- We're seeing a lot of "one weird trick" marketing from companies offering to sell us equipment to do all the work for us.

What has happened?

- A number of high-profile incidents have occurred that have demonstrated that medical devices are not secure, and are not meant to be secure.
  - WannaCry
  - Pfizer/Hospira Pumps security issue
  - Ransomware attacks on Windows-based systems
- There is now draft legislation and guidance from the FDA to address these issues that focuses on the development process and vulnerability management
- There are companies and people attempting to resolve these issues using new technologies
  - Blockchain-based tech to verify and validate security and safety of devices across owners by device (Spiritus Partners)

What has happened?

- There is technology, but there are also business issues to address
- The technology issue is obfuscating the management of devices, and how we can practically plan and manage to have them in the environment
  - Make it so that we have a playbook that non-technical staff can follow and understand and why
- Bridge that last mile with everyone

Where do we start?

- It starts with a plan
  - Even if you don't have a security team, develop a plan to manage your vendor technology in five areas:
    - Contracts and Language – the rules of engagement
    - Preparation
    - Acquisition
    - Maintenance
    - Disposition

The five key areas of technology management

1. Contracts and Language

- You need to have six core sets of terms in your contracts to address potential security issues:
  - Minimum Security Standards for encryption and supported components
  - Identify how you will be notified of vulnerabilities
  - SLA for notification time/workarounds
  - SLA for patch availability
  - BAA that covers security logging and auditing
    - Who reviews the logs?
  - Identify responsible parties in the contract in writing!

The five key areas of technology management

2. Preparation

- Identify Vendors
- Establish relationships (external)
  - Include other organizations that run this product.
  - Get to know your vendors well and have a relationship.
  - Even if you buy from a GPO, get to know the team
- Establish relationships (internal)
  - Clinical Engineering – esp outsourced managers
  - Consultants
  - Legal/Contract Management
  - Supply Chain (esp. if outsourced!)

The five key areas of technology management

2. Preparation

- Plan to Manage
- Plan for Emergencies/Issues/Downtime/Recovery
- Build standard work that includes service levels
  - Nothing gets done for a CE contractor without a work order (one contract had 6 places that specified this!)
  - Make sure you have a good relationship with the people in charge of CE so you can get work orders issued.
  - Plan for good network security to buy time.
    - **It takes a long time to patch CE equipment due to resource issues.**
    - **Segmenting these devices helps spread the work and make it predictable.**

The five key areas of technology management

2. Preparation

- Identify how you will be notified of vulnerabilities and changes
  - If you are buying used, make sure you can get the patches in the first place and have a reliable resource (read: Not the Pirate Bay) to get them
    - **ECRI, FDA, vendor themselves, etc.**
- Identify testing/downtime processes
- Identify vendor contacts
- Identify resources
- Identify network requirements and how to meet them
  - Build out how to manage segments and devices.
  - Build out how to monitor networks for anomalies

The five key areas of technology management

2. Preparation

- If you're small, consider a managed service to monitor security so you can collect device logs and be alerted to issues.
  - I do not expect most offices to have a SIEM but they have devices. A managed service helps turn those alerts into plans
  - We made recommendations to draft FDA guidance for log files for this reason
  - We look at the SIEM as being critically important as no human being is going to look at log files.
    - **Let AI, ML, and other tech do this for you**
- Get templated statements of work for product security updates and product maintenance

The five key areas of technology management

3. Acquisition

- If you're acquiring used devices, make sure that you still have a plan to manage as if they were new
  - You may have to pay a little extra to reestablish maintenance contracts
  - If you're going through M&A you need to have this in the playbook!
- Follow through on your processes from Preparation

The five key areas of technology management

4. Maintenance

- Develop and execute Standard work for devices as you need to be able to measure staffing levels and manage these devices
- Log and register maintenance/sec updates on these devices
- Wireless Security is going to be key as standards evolve
- Log and register maintenance on your networks just like CE devices
  - We expect that Joint Commission, based on statements that the loss of a wireless network is a patient safety issue, to ask similar questions
- Make sure you have a documented change management program and follow through with it
  - Log device changes to a central registry

The five key areas of technology management

4. Maintenance

- For large-scale upgrades, use Failure Mode and Effects Analysis to map out potential process failures.
- Make sure you involve all parties and communicate well with them when you perform maintenance.
- Yearly risk assessments and risk management plans to discover and address security issues.
- If you bring in tools, make sure they address a real and identified risk!

The five key areas of technology management

5. Disposition

- Erase devices
- Build erasure/refit costs into sale price
- Consider registering devices in a centralized registry so buyer has history

What have we learned?

- There is a lot more to the backstory of medical devices than just insecure development
- It takes a lot to change multiple decades of development and evolution from serial ports and dedicated lines to 5G
- Even then, we have to manage these devices differently than we have before
- It's not impossible if you have a plan
- A 5 step plan (Contracts, Preparation, Acquisition, Maintenance, Disposition) can help you immensely

Thank you!

- Questions?
- Contact Info:
  - Mitchell Parker
  - Executive Director, Information Security and Compliance
  - Indiana University Health
  - Email: Mitchell.parker@iuhealth.org
  - Twitter: @mitchparkerciso
  - LinkedIn: https://www.linkedin.com/in/mitch-p-95a9a04/
  - Cell: 215 519 1053

A

- W

A

- W

Strategically Improving Medical Device Security

Mitchell, Parker, IU Health

Indiana University Health

Purpose of Presentation

- To show how providers are incorporating security into their strategies and using it to improve their security posture

Background

- I am the Executive Director of Information Security & Compliance (CISO) at Indiana University Health
  - 17 hospitals
  - Hundreds of clinics across the state
  - 34,000+ team members
  - ~600 person IS department

Team Makeup

- Our team focuses on six key areas:
  - HIPAA/PCI Compliance (Kevin St. Laurent)
  - Third Party Risk Management (Rachel Money)
  - Penetration Testing (Chris Gibson)
  - Standards Compliance (Mitch Parker)
  - Program Management (Noidric Davis)
  - IU School of Medicine (Nick Sturgeon)

Interfacing

- As part of our strategic focus, we work closely with a number of business partners:
  - Privacy/Legal
  - Government Affairs
  - Compliance
  - Risk Management
  - Regulatory Affairs
  - Emergency Management
  - Physical Security
  - Chief Health Information Officer
  - An ever increasing number of medical device vendors

Goals

- To use our strategic alliances to work across organizations to assess and address risks at different levels
- To prevent items from going onto the floor without proper risk analysis
- To maintain what we have in good repair
- To effectively plan out lifecycle management for all items on the network
- To effectively communicate our security requirements
- To continue to have great relationships with medical device vendors

Notes and Words

- Strategic Goals
- Explaining and fitting together items for vendors using common language
- De-mystifying security for vendors – let them know what to do
- Take the confusion out of security – explain what we need
- Explain the goal of a constant review process
- Explain our focus on the processes, not on checking boxes
- Build a virtuous cycle to assess and address risk

What is our approach?

- We want to work with our vendors to develop security as part of the overall business process
- We don't want to overwhelm you with questionnaires and checkboxes
- We want to be very clear about what we need to demonstrate that you meet our organizational standards and requirements
- We want to work with you and build partnerships – no adversarial relationships
- We don't want to scare our customers, or you – that does nothing to help us
- We want to avoid preventable issues that can affect our patients

What processes do we use to address this?

- Governance/Intake
- Enterprise Architecture Review
- IT Risk Assessment/Information Security Review
- Privacy Impact Assessment
- Business Associate Agreement
- Internal Policies and Processes
- Internal Review

What do we expect from medical device vendors?

- Security Contacts
- Realistic Operational Management Tasks and Expectations
- Explanations of Security Management Processes
- Openness into your product development processes
- Vulnerability Management Processes with Excellent Communication
- Privacy and Security by Design
- Network Security by Design

Governance

- Organizations need to have a gate for purchases that represents a business unit
- Need to make sure that purchases are consistent across organization – reduce variety
- Need to make sure that purchases meet strategic requirements
- Buy only what we need to – efficient spend and allocation of limited resources

Enterprise Architecture Review

- Yes, this meets our strategic needs, but…
- Does it integrate with what we have?
- Does it integrate with the key systems we use?
- Can we do enterprise provisioning?
- Does it use standard data formats?
- Do we have to reinvent the wheel to fit this in our environment?
- Most Important: Can we implement security standards at the beginning?
  - Can we segment and run your devices as isolated as possible?

Information Security Review

- The IT Risk Assessment is only part of this
- We designed it for several main goals:
  - Vulnerability Management – do you do this in a timely manner?
  - Do you continually assess and address issues?
  - Do you incorporate security and privacy by design?
  - Do you update all components, not just your software?
    - I have seen vendors update software and leave the operating systems, database systems, and web servers obsolete
- Comprehensive Review of security practices and procedures
- We will interview CISOs and key security and management leaders
- Do you protect our patients' information to our standards or better?

Privacy Impact Assessment

- Do you only collect minimum necessary information?
- What data will you be collecting?
- What format is the data in?
- Where will you be storing it?
- How will you be accessing the data?
- Will you be doing any aggregation or de-identification?
  - If so, what is the reason?
- Do you have plans to use our data for any other purposes, even if de-identified?

Business Associate Agreement

- Legal document that covers requirements, liability, and security details
- We address breach response, data handling, expected insurance amounts, and responsibilities
- We also have Appendix A to discuss security requirements
- As part of that, we broke ours out in detail
  - We discuss certificate management, logging, auditing, provisioning, risk assessments, network design, and vulnerability management
  - Instead of addressing HIPAA as one statement, 14 separate statements in plain language with explanations that are most important

Business Associate Agreement

- We do this to put these items up front when you sign a deal with us
- We want it well known what we are looking for
- We also want to let people know that we are looking for compliance with the HIPAA Security Rule in detail
- We've found that many of our vendors were not aware of specific requirements, e.g. Cloud Computing, and we need to be detailed in spelling them out

Internal Policies and Procedures

- Organizations need to have strong policies and procedures
- Need to spell out exactly what responsibilities are and who needs to do them
- Need to be no longer than necessary
- Should have corresponding training with question instrument
- Need to be updated as needed, which may be more than some people are used to
- Need to be well communicated throughout the organization
  - With recorded training instrument answers – OCR looks for this

Internal Review

- According to the 2017 Online Threat Report, 93% of the data breaches out there were caused by people not taking due care or patching
- According to Phil LaDuke in Entrepreneur Magazine, November 8, 2016:
  - If 80 Percent of Success Is Showing Up Then 20 Percent Is Following up
  - *The excuses are many, but the solution is surprisingly simple*
- We need to make sure that we and our customers follow up and do what is needed to address security issues
- When we present stories of data breaches to leadership, ultimately every case has root causes in lack of preparation or due care

Internal Review

- We address this by following up
- However, to do this, you need to lay everything out for people to know
  - Clear policies and procedures
    - Explain all requirements and what is needed
  - Good education plan
  - Good intake process
  - Supporting governance
  - Realistic financial expectations and planning
  - ASSET MANAGEMENT - know what you have!

Internal Review

- As part of these requirements, you design controls tests, just like Internal Audit does
- You review and follow up with your customers
- Get documented evidence of compliance
- Escalate to leadership if not being followed
- If you do this, you address the largest risk

Now we come to expectations from vendors…

- This is where we discuss what we need to see from medical device companies
- We look at this as going both ways
- If we can get some small improvements here we can greatly improve security

Security Contacts

- We want to have direct contact with product security teams
- Instead of having a general customer service number, direct lines to security professionals who can address issues
- The goal is to address potential security issues without having to go through several levels of staff members to explain an issue
- This has been a major frustration as security researchers or customers have had to track down people to report vulnerabilities or issues

Realistic Operational Management Tasks and Expectations

- Time is Money, especially when you have a large operational tail for product maintenance
  - Security work is preventive maintenance
  - We need to budget for time per device to maintain it
  - We need to be realistic as healthcare has limited budgets
    - Either we pay to do it or we pay someone else as part of a work order
    - Large Clinical Engineering outsourcing firms require detailed work orders
    - The front-line staff who implement security remediations do not necessarily need to know

Realistic Operational Management Tasks and Expectations

- The people who write the work orders or manage Clinical Engineering staff normally do not understand what to do for security
  - If you're lucky, they will call you when they get recall notices
- Therefore, we need to be very clear and circumspect and spell out everything that needs to be done as regular tasks
- Make it so that someone who does not know technology or security can copy and paste them into task lists or work orders
  - Explain that you are being realistic about operational costs and reducing risk
  - This also allows us to design controls tests for following up!

Explanations of Security Management Processes

- We need to understand how you manage security, prioritize risk, and develop security fixes
- We also need to understand how you expect us to manage them
- As part of managing these devices, we need to understand how to design security in our environments around them
- We need this information to plan security responses based on how you work

Openness into Product Development Processes

- We want to help you avoid issues or make mistakes
- You also need to understand how the environments you are deploying into will work
- We want you to take these issues into consideration when developing products
- It's our goal to make deployments easy

Vulnerability Management Processes with Excellent Communication

- It's sometimes really hard to sometimes ascertain what is in a patch and what it does
- We are up against change management where we have to understand what a patch changes and what it does
- We need to understand how long per device remediation will take (remember, non-technical people apply these patches)
- We need to know all that and have it documented for us so that we can communicate the urgency to our stakeholders

Privacy and Security By Design

- We would like to see you only collect information you absolutely need to do your job and nothing more
  - Think European Union General Data Protection Regulation (GDPR)
    - GDPR requires this!
- We also want security designed in
  - Don't use default passwords
  - Use secure connections
  - Allow us to install our own SSL/TLS certificates and crypto keys
  - Make it easy to manage them

Privacy and Security By Design

- Security Designed in
  - Make it simple to patch and maintain
  - If it involves a command line, you increase time to maintain and the probability of error
  - Make documentation for patching and maintaining devices as simple as possible
  - Provide human-readable error messages and warnings for issues
    - Codes are for auto mechanics – we need to act quickly and if we have to look up something it leads to confusion
    - Reduce acronyms!

Network Security By Design

- We need to keep your devices as segmented as possible
- We can no longer assume the risk of having medical devices on the same network as PCs – esp. if running Windows
  - Yes, we are aware of medical devices that have had ransomware
- Segmentation buys us time to patch
- It also can reduce risk from insiders and outsider attacks by only allowing access based on role
- We need to extend this to wireless as well
  - However, we need you to support WPA2-Enterprise to fully support this!

Conclusions

- We want to work with manufacturers to improve security
- However, the solutions with the highest return are not entirely technical
- Better communication, understanding of processes, and making sure that the right processes exist goes a long way
- Security is about involving the whole organization in resolving business issues

Thank you!

- Mitchell Parker
- Executive Director, Information Security and Compliance
- IU Health
- Mitchell.parker@iuhealth.org

What is a Security Information and Event Manager (SIEM), and do I really need one?

Mitchell Parker, IU Health

Indiana University Health

Purpose of Presentation

- Security Information and Event Manager (SIEM) software works by collecting log and event data that is generated by host systems, security devices and applications throughout an organization's infrastructure and collating it on a centralized platform.
- This session will cover the information provided by basic SIEMs, and if you need a SIEM, what are low-cost solutions.

Agenda

- History of the SIEM
- What does it stand for?
- Why do we need them?
- What's the Staffing Requirements
- SIEM Features
- Major SIEM Products/Vendors
- Advantages/Disadvantages
- Example Logs/Reports
- Low-Cost/Free Solutions
- Final Tips

History

- In the beginning, there were logs
- And there were many of them
- UNIX and Windows generate a lot them
- So do web servers
- And they can send them over serial ports or port 514
- Windows can also send them to remote servers
- People wanted to aggregate and analyze them together to understand security events
- They also wanted to store and retain them

What does it stand for?

- Security
- Information

And

- Event
- Management

System

- A place for your logs and to analyze them

Why do we need them?

- Log retention of events
- PCI-DSS requirements for log retention
  - PCI requires audit log analysis
  - Retention is state by state on financial data that doesn't have credit cards
- HIPAA requirements for accounting of disclosures and log analysis
  - Six years for Accounting of Disclosures
  - OCR wants logs stored with data
    - Even though states have different retention laws, logs have to be retained as long as data

Why do we need them?

- DOD requirements for log retention
  - 1 year minimum, 5 for Sources and Methods intelligence (DODi 8500.01 control ECRR-1)
- FedRAMP control AU-11 – The organization retains audit records to provide support for after-the-fact reporting
- FedRAMP control AU-9 – The information system protects audit information and audit tools from unauthorized access, modification, and deletion
- FedRAMP control AU-3(2) - This control enhancement requires that the content to be captured in audit records be configured from a central location (necessitating automation). Organizations coordinate the selection of required audit content to support the centralized management and configuration capability provided by the information system.

Why do we need them?

- DFARS Regulation 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting requires:
  - (b)(2)(D) – For external cloud services, the contractor must use cloud service providers compliant with FedRAMP requirements
  - FedRAMP controls AU-6 1-10 require the use of automated mechanisms to integrate audit review, analysis, and reporting processes, analyze and correlate audit records, centrally review and analyze audit records, and integrate analysis of audit records with vulnerability scanning info, performance data, and information system monitoring information

Why do we need them?

- NIST Special Publication 800-171 Revision 2 for non-Cloud services procured under DFARS Regulation 252.204-7012 (b)(2)(i)
- Section 3.3 – Audit and Accountability
  - 3.3.3 – Review and update logged events
  - 3.3.4 – Alert in the event of an audit logging process failure
  - 3.3.5 - Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity
  - 3.3.8 – Protect audit information and audit logging tools from unauthorized access, modification, and deletion

Why do we need them?

- You cannot meet DOD requirements doing this manually
- Given event volumes and requirements, there is no way to accurately do this manually as it requires normalizing and analyzing events
- There is also no way to do this given the volume of events that servers can generate, which are in the millions
- By the time you do one type of analysis, you will have spent enough resources to buy a SIEM and have them do more
  - Not cost-effective!

Why do we need them?

- Most platforms overwrite logs when they hit a certain size like Windows or Active Directory
- Need to correlate events across multiple platforms
  - Correlation is often the only time that you can detect intrusions
- Need to be able to trace paths of events
  - People can forge one set of logs
  - They normally don't make the effort to forge all of them
  - Find errors and inconsistencies to identify possible events

Very practical reasons why we need them

- Need to be able to see when people logged in and out
  - Your HR department will love you for this one
- Ransomware and other advanced attacks rely on blindness to actions
  - Attacks such as UHS, Blackbaud, and numerous others had time between initial intrusion and attacks measured in months
  - No one was watching
- Visibility means that the probability of discovery is much higher
  - If you see something going on you're going to do something
  - If no one is watching or the alarms then you might as well have nothing because you do

What's the staffing requirements?

- Despite what many vendors will tell you, you will need someone monitoring its health at least part-time
  - There is no such thing as set and forget. Whoever tells you this lies.
- You will also need to make sure to set timelines to resolve issues and events
- You need to check to make sure all your log sources work and get alerted if they do not
- You also need to check to make sure logs are being ingested and processed correctly
  - One wrong log file and you're out

What's the staffing requirements?

- You need to check to make sure that you are not getting too few or too many alerts
  - Don't let default settings overload you and cause alarm fatigue
  - Large attacks have succeeded by hiding in millions of events that default SIEM settings have covered up
- Also need to keep the SIEM and underlying systems secure
  - Despite it being a security tool, it's a one-stop shop for information
  - And intelligence on what really runs or doesn't on your network

SIEM Features

- Integrate logs from many sources
  - AV
  - EDR
  - Active Directory
  - Windows Event Logs
  - Linux/UNIX Syslog
  - Network security devices such as firewalls and IDS/IPS
  - Authentication Logs
  - Storage Area Network
  - Virtual Private Networks
  - Applications

SIEM Features

- Normalize logs and formats so you can query them and perform analytics
- Integrate threat intelligence feeds to determine if network traffic or stored events match patterns of known attackers
- Match patterns, sequences, and identify specific events that indicate erroneous or malicious behavior
- Identify anomalies
- Report on anomalies
- Store records of logs and potential findings

SIEM Features

- Feed IDS/IPS and other security systems information on known bad events
  - Be that central hub to centrally arbitrate and distribute
- Ability to develop custom reports on data
- Provide dashboarding and analytics on security events
  - Help you avoid overload and give quick views on events that matter

What are some of the major SIEM products/vendors?

- ELK Stack (Elastic)
  - Largest Open Source/Free solution
- ARCSight
- McAfee (former Nitro Security)
- Alienvault (AT&T)
- LogRhythm
- QRadar (IBM)
- SolarWinds
- Splunk
  - Probably the largest and most full-featured

What makes them special? Why do people pay?

- The algorithms
  - Many of the commercial offerings are tuned and come pre-set for different environments
- The data storage
  - They make it easy to expand them
- How they present dashboards of info to people
  - Many have very polished user interfaces
- Ease of use
- The vendor support system
  - Good with less staff

How do people deploy them?

- On-premises in a rack (people do still have data centers)
- Virtual Machine Image (very common)
- Container (starting to see more of)
- Managed Security Services Provider (MSSP)
  - Let them do most of the work or labor for you
  - Even though they do the hard work you still need to make sure that the systems can send them data
  - They will still deploy Virtual Machines or machines to send events
- In the cloud
  - MSSP's will usually deploy in the cloud

What are the advantages/disadvantages?

- On-premises advantages
  - Local connection to servers on the same network
  - Disk storage is cheap
    - You pay once for the storage, not recurring like the cloud
  - Can be deployed as a virtual machine or container
  - Don't have to worry about cloud storage charges
  - Don't have to have a continual Internet connection or forwarding server - less complex architecture
  - You don't have metered charges for additional services like firewalls

What are the advantages/disadvantages?

- On-premises disadvantages
  - Vendors may charge for additional storage
    - This is “special” storage at a 10x markup even though you can buy that drive on Newegg for $200
  - You must buy additional hardware to scale up
  - You may have to buy additional software licenses to scale up
  - You may have to buy licenses to store software
  - You must upgrade and patch yourself
  - Connecting Cloud apps is difficult and opens up potential network holes
    - Many cloud vendors have insecure APIs and don’t use VPNs

What are the advantages/disadvantages?

- Cloud Advantages
  - Easy to scale out and up
    - Cloud is designed to be elastic
  - Easy to set up
    - Takes 10 minutes to set up in Amazon Web Services
  - Easy to update/upgrade
    - Pushbutton upgrades
  - Ease of connecting Cloud applications
    - No need to set a lot of firewall rules

What are the advantages/disadvantages?

- Cloud Disadvantages
  - Many of the cloud firewall and IPS systems have metered charges
  - You can get hit by additional costs for processing, memory, additional services, and storage if not careful
    - Storage especially will kill your bottom line if you do not forecast correctly
  - You must upgrade on their schedule
    - Cloud vendors have no interest in having a security system becoming a vulnerability and liability
    - If you don't test upgrades I guarantee future issues

What are some example logs and reports we need?

- According to the SANS publication, Top 5 Essential Log Reports, Version 1.0 (Source: https://www.sans.org/security-resources/top5-logreports.pdf)
  - Attempts to Gain Access Through Existing Accounts
  - Failed File or Resource Access Attempts
  - Unauthorized Changes to Users, Groups, and Services
  - Systems Most Vulnerable to Attack
  - Suspicious or Unauthorized Network Traffic Patterns

Attempts to Gain Access Through Existing Accounts

- This report type focuses on several types:
  - Unauthorized logins from outside the network and the number of times they attempted to log in
  - Repeated unauthorized logins from inside the network
  - Logins from workstations or outside by service accounts
  - Logins from foreign countries or different geographic areas
    - Esp. good for finding users using VPNs to log in
  - Logins by normal user accounts to servers other than file servers

Failed File or Resource Access Attempts

- This is good for finding several types of access patterns:
  - Failed Domain Name System (DNS) transfers
  - Failed DNS recursion attempts
    - May be a sign of cache poisoning
  - Failed accesses to non-existent or restricted web site directories
    - May be a sign of someone trying to probe your systems
  - Failed mail relay events
    - Someone trying to impersonate you and send mail
  - Failed file access
    - Why do they want to see salaries.xlsx?

Unauthorized Changes to Users, Groups, and Services

- Accounts that have been added
  - Why is the new user r00ted on our file servers?
- Users added to groups
  - R00ted is now a member of Enterprise Admins
- Services added, changed, or deleted
  - R00ted turned off Antivirus
  - R00ted restarted sshd in a new location
  - R00ed added a new service called pwned.exe as SYSTEM

Systems Most Vulnerable to Attack

- Systems that have not reported in through Event Log that patches were successful
- Systems that have reported in that patches failed
- Vulnerability scanner reports showing vulnerable systems
- Systems that have reported in recent updates/upgrades

Suspicious or Unauthorized Network Traffic Patterns

- Inbound and outbound pings to non-existent or blocked sites
- Initiated outbound traffic from outside-accessible servers
- Outbound traffic to sites identified by threat intelligence
- Outbound traffic to mail servers, Internet Relay Chat, Virtual Private Networking, or file sharing sites
- Outbound Secure Shell/Secure FTP/FTP traffic
- High bandwidth utilization

What are some low-cost/free solutions?

- ELK Stack - Open Source (https://www.elastic.co/start)
- Elastic + LogStash + Kibana
- OSSIM (https://cybersecurity.att.com/products/ossim)
- OSSEC (https://www.ossec.net/)
- Splunk Free (https://docs.splunk.com/Documentation/Splunk/7.2.6/Admin/MoreaboutSplunkFree)
- Apache Metron (http://metron.apache.org/)

What are the most friendly solutions for non-IT professionals?

- There are numerous user-friendly front ends to ELK Stack
  - The paid version also has great support
- Splunk has a significant community that provides support and code for specific applications

Final Tips

- If you can't think of who can manage this effectively in 30 seconds, or do not have the budget to hire someone, get a Managed Security Services Provider
  - They can also help you configure/manage your servers
  - Well worth it for smaller businesses that need DOD or HIPAA-level compliance
  - You will need one that is a FedRAMP authorized vendor to do business with DOD according to DFARS Regulation 252.204-7012
    - MSSPs are offsite and can be considered cloud-based
    - GuidePoint, CrowdStrike, and Qualys are authorized

Even if you go with an MSSP….

- Even though the solution is low-cost, it needs care and feeding like any other IT system
  - Even if its cloud-based you still need to check on and feed source systems
  - You need to forecast your storage needs
  - Calculate how much storage you will need based on the data you have to retain
    - Double it
    - Make sure you have budget for the option you have chosen
    - And that your MSSP contract allows you to expand without killing it!

Thank you!

- Thank you for your time today
- You can reach out at:
  - Email: mparker17@iuhealth.org
  - Phone/Signal: +1 317 719 5531
  - Twitter: @mitchparkerciso

Exercise News Release and Information Sheet

Indiana's Cyber Readiness Advancing Rapidly

Friday, October 1, 2021

If you think about it, protecting a school, hospital, or a city's water supply from a cyberattack is a lot like a football coach drawing up a game plan for playing against the #1 team in the country – every day.

There's game film, playbooks and you always have to account for how you're going to stop the other team's best player from scoring; all the while trying to figure out what else the coach might have up his sleeve. And there's no halftime show to try and adjust to stage a comeback.

That's the challenge facing the State of Indiana in its efforts to continue rapidly moving forward in its mission to further strengthen its cybersecurity resiliency and response.

The progress that's been achieved comes as the State of Indiana and the Indiana National Guard recently hosted two cyber exercises in a partnership with several federal agencies, health care providers, and technology companies, water utility service providers, state, and local government officials, as well as state and federal emergency and law enforcement agencies.

"Conducting these exercises highlights the strength of the cybersecurity structure that exists within the state and underscores the work that's been accomplished over the past three years by

Indiana Governor Holcomb's Executive Council on Cybersecurity with our partners in the military, academic, public and private sectors," said Indiana Department of Homeland Security Executive Director Stephen Cox. "Most importantly, it represents the progress with cyber that's been achieved on behalf of all Hoosiers when we approach cybersecurity as something that is not solved by one entity alone, but by everyone at all corners of the state."

Having a playbook is especially crucial, given the fact there are not only a seemingly endless number of situations in which a cyberattack or incident can occur, but there are all kinds of circumstances and variables that can interfere with a cyber team's strategy for protecting its systems.

When Water Runs Out…

A water utility being attacked is not only scary to every city in America, but the reality of it also happening is real.

The Cybersecurity and Infrastructure Security Agency (CISA) has partnered with the State of Indiana and the City of Fort Wayne to exercise how state, federal, mutual aid, and local government would work together in a long-term cyberattack that eliminates the supply of water from the city, with a special emphasis on the secondary effects for the city's hospitals.

As the Cybersecurity Program Director for the State of Indiana, there's no question cybersecurity impacts every aspect of our daily lives. As we've seen with recent cyber incidents – everything from pipelines to water utilities to schools and hospitals – a cyberattack can create substantial effects and damage to our community and our critical infrastructure, disrupting our daily lives and safety.

When Natural Disasters Hit…

Following the completion of the tabletop exercise, a second cyber exercise as part of a full-scale functional exercise hosted by the Indiana National Guard for first responders and several military branches as well as search and rescue teams at the Muscatatuck Urban Training Center.

The grounds of the 1,000-acre facility, located in Southern Indiana, is a real city that includes a built-in physical infrastructure, a well-integrated cyber-physical environment, an electromagnetic effects system and human elements. There are more than 190 brick-and-mortar structures with roughly 1.5 million square feet under roof, 1.8 miles of subterranean tunnels, a cave complex, more than nine miles of roads, managed airspace, a 185-acre reservoir, and a cyber live-fire range.

The focus of the Indiana National Guard exercise centered on measuring how federal, state, local and private sectors respond to a devastating earthquake.

"We really need to prepare now for these acts which we've already seen here in Indiana and across the world," said Ron Pelletier, founder and chief customer officer at Pondurance, a cyber security company. "When natural disasters hit all parts of the world, we are seeing more and

more targeted cyberattacks in those affected areas. Investing now in preventative measures is the best way to avoid situations like that from becoming worse. It comes down to planning to avoid cyber breaches but being prepared to respond."

As emergency and military teams respond to the effects of the earthquake, the Indiana National Guard also tested the additional response of its incident command leadership while the cyber experts from IU Health, Citizens Energy Group, and Pondurance made the efforts more difficult by attacking the water supply in the aftermath.

It's Not "If" But "When"...

Pelletier added that Pondurance hopes disaster drills, such as these two, will raise awareness among policy makers to help fund security programs and protocols. "National, state, and community security is truly at risk here, and we need to take action now to preserve it. Waiting for the dam to burst before you repair it is a terrible maintenance strategy, and that's exactly the situation we have here across power grids, water supplies, healthcare, you name it."

Having the ability to draw on the resources and expertise required at a moment's notice to keep people safe in the event of a cyber incident or attack relies on making certain that the state and its partners have a line of communications that's always open to make sure the State of Indiana provides a response that's most effective, regardless of the circumstances.

Many of those who are participated in both state exercises also serve on the Indiana Executive Council on Cybersecurity (IECC). As defined in Executive Order 17-11 from Indiana Governor Eric Holcomb, the IECC is a first-of-its-kind collaboration, whose work as an organization within state government, is responsible for guiding the state's cybersecurity policy, It is comprised of 35 Council members and 250 advisory members, all of whom are subject matter experts represent a wide range of businesses, industries and professions, including education, finance, utilities and insurance, among many others.

The State of Indiana and its partners offer best practices, guides, toolkits, and resources to allow all organizations and critical infrastructures to mitigate, but also prepare for a cyberattack. For more information about the IECC or the State of Indiana's Cyber Strategy, visit www.in.gov/cyber.

For more information about CISA's cybersecurity services and resources, visit www.cisa.gov.

INDIANA NATIONAL GUARD

Homeland Defender 2021

Exercise Director: LTC Robert Brake (INNG)

Executive Council: Chief Tom Neal (IN TF1) & LTC Robert Brake (INNG)

Safety Director: CSM Ty Benham (INNG)

Operations Director: Chief Jay Settergren (IN-TF1)

Operational Support: CPT Pemberton (INNG)

MSEL Directors: DC Steve Coover (MFD & IN-TF1) & LTC Robert Brake (INNG)

UNCLASSIFIED

INDIANA NATIONAL GUARD

HOMELAND DEFENDER 2021

POC: LTC Rob Brake

Exercise Mission

INNG host a Full Scale Exercise from 13-15AUG21 vic MUTC involving local and state resources in order to (IOT) reinforce existing relationships, create new ones and share best practices within the 1st responder community.

Exercise Purpose

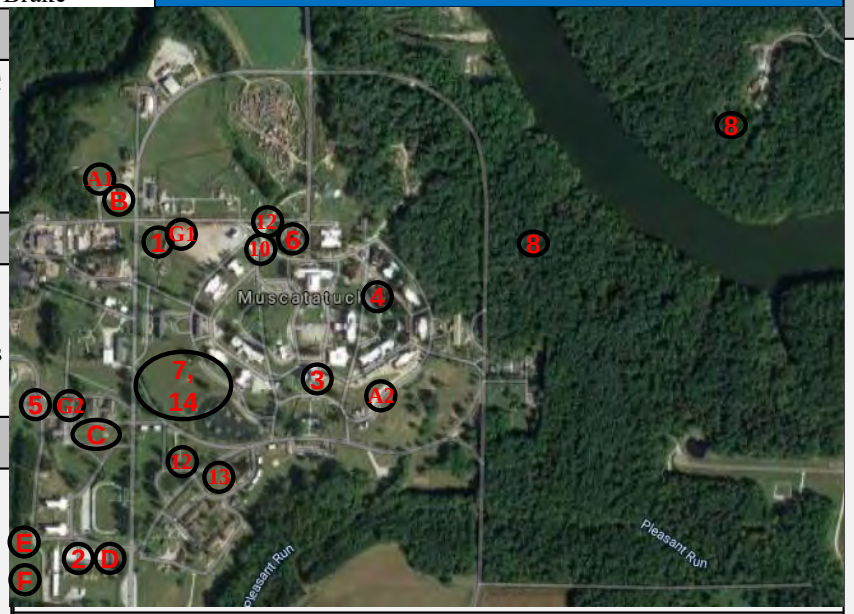
Conduct a joint training event that includes local, state & military partners, focused at the Team level, in order to increase unit/team proficiencies and integration with other 1st responders within the State of Indiana Response Forces.

Exercise Intent

Exercise Commander Intent: Provide a realistic training opportunity for units to collectively train together IOT increase readiness and share tactics, techniques, and procedures via a scalable and nested exercise over a 2 day, weekend exercise. Once completed units, can receive a facilitated AAR based on individual unit training requirements.

Key Tasks: Alert & Mobilize, Deploy, Site Occupation, Joint /combined Operations & Redeploy all IAW NIMS.

End State: Create a realistic collective exercise from H-hour – OP3, that supports Local and State Inter Agency Integration followed by after action reviews IOT ensure State Partners meet individual and team training objectives, increase readiness and share techniques between Agencies.



Concept of Operation

A series of earthquakes occur that quickly exceeds local resources requiring assistance from Regional and State Agencies in order to meet lifesaving operational requirements.

As a result multiple agencies and units receive an Alert Orders to Deploy to staging locations. O/O units will move forward IOT conduct Site Occupation & link up with the Incident Management Team (IMT) IOT receive missions for Full Scale Operations. Once units are Mission Complete, they will begin recovery operations and redeploy to home station.

Operational Lanes:

Lane #1: Initial Command Post & Rail Yard
Lane #2: Unified Command / IMT CMD Post
Lane #3: Hospital Chemical & Radiation
Lane #4: Round Robin Skills Training
Lane #5: Cafeteria Collapse
Lane #6: School Collapse
Lane #7: TF1 Air Load Operations
Lane #8: Lost Personnel WAS
Lane #9: CYBER Ransom
Lane #10: Chaplain Teams
Lane #11: NGRF Alert and Staging Operations
Lane #12: Area Security Operations
Lane #13: Crowd Control Activities
Lane #14: Lifeline Operations

Site A: Staging (Sites 1 & 2)
Site B: MFD & CST CMD Post
Site C: CERFP & TF1 CMD Post
Site D: NGRF CMD Post
Site E: White Cell Team
Site F: Ravenswood Support site
Site G: DECON Sites (1& 2)

Participants/Enablers: 369 (82) BOG -501

CST – 20 (2)
TF1 IN – 6 (15)
CERFP – 208 (5)
CAP – 2
NGRF – 40 (5)
38th CAB – (4)
Ravenswood – (24)
IDHS Dist 8 IMT – 12
127th CB – (2)

MFD – 16 (6)
81st TC – (10)
IOT – 15 (3)
JCSD – 40
UPAD – 6 (2)
ASOS – 4
JFHQ-IN – (4)

( ) = non-participant / support role

Additional:
Role Players – (50)

IPR #1 10SEP20 → **CDC** 06-08OCT20 CAIN/MUTC → IPR #2 1NOV20 → IPR #3 4DEC20 → **IPC** 2-3MAR21 MS Teams → **MPC** 16-17MAR21 MUTC → **FPC** 11-12MAY21 MUTC → IPR #4 21JUN21 → IPR #5 19JUL21 → **Execution** 13-15AUG21 MUTC

UNCLASSIFIED

Homeland Defender Key Events Timeline

1-12 AUG 21 Local media reports increased cyber activity to local municipalities

0330 13 AUG 21 – 4.3 MAG Earthquake

13 AUG 21 – HAZMAT call out initiates Rail Yard and Hospital Scenarios (Lanes 1 and 3)

13 AUG 21 – Second Earthquake Occurs causing multiple structure collapses (Lanes 5 and 6)

13 AUG 21 – IC Requests additional resources from JC-EMA (Lanes 2)

13 AUG 21 – State EOC assigns INNG Forces to IC

13 AUG 21 – NGRF arrives to secure govt. center (Lane 12)

14 AUG 21 – Search and Extraction of structure collapses (Lanes 5 and 6)

14 AUG 21 – Cyber ransom attack at water treatment facility (Lane 9)

14 AUG 21 – Increase civil unrest at govt. center (Lane 13)

14 AUG 21 – Wide area search for lost personnel (Lane 8)

INDIANA NATIONAL GUARD

Task ORG