Cybersecurity Guide to Planning & Evaluating Risks for Indiana Local Officials

March 2021

A publication made possible by the following associations:
Association of Indiana Counties
Accelerate Indiana Municipalities
Indiana Association of County Commissioners

With technical assistance provided by Purdue University

TABLE OF CONTENTS

I. INTRODUCTION

As local government functions have become more automated and computerized, the risk of cyberattacks has become more concerning. From providing emergency response through 911 call centers to safe drinking water through municipal water treatment plants, local governments in Indiana are charged with providing services that are critical to life and living for the general population. Imagine if these critical services were suddenly disrupted by a malicious act – a cyberattack.

A cyberattack can be mounted against digital devices. It is a malicious act that seeks to damage data, steal data, or disrupt digital life in general. Cyberattacks include threats like computer viruses, data breaches, and Denial of Service (DoS) attacks. Depending on the intent of the attacker, a cyberattack can be merely a nuisance or it can be potentially life threatening.[1]

ATTACKS ON GOVERNMENT IN INDIANA

Unfortunately, several Indiana local governments have already fallen victim to cyberattacks. For instance, in 2019, LaPorte County government was forced to pay $132,000 to hackers after a ransomware cyberattack shut down part of the county's computer system.[2] In 2017, in Franklin County, the county's financial software vendor was hit by an attack, which then allowed the county's records to be affected. While the county lost the records of one day's work, other work was saved by virtue of a backup done the night before. The Franklin County Auditor and Treasurer disabled user rights to view information in the financial system as a result of the attack in order to protect the security of the records.[3] In Madison County, 2016, hackers launched a ransomware attack on 600 computers and 75 servers and forced law enforcement officers to use pen and paper when processing inmate information at the local jail. Officers on patrol had to contact other agencies in order access a person's criminal records. On the advice of its insurance carrier, county officials paid the $21,000 ransom. The county later approved spending nearly $200,000 to secure additional IT contracts which included off-site data storage, a backup court system and protections against future infections.[4]

Indiana state government fell victim to attack in 2018. Federal prosecutors issued indictments and financial sanctions against Iranian hackers that illegally accessed Indiana state government computers. The hackers also accessed the computer systems of 144 universities where they stole data and intellectual property across all fields of research including engineering, medicine, science and technology. The hackers pretended to be professors at other schools and sent emails to the victim professors expressing an interest in their academic articles. The emails included a link to other articles that required the victim professors to enter their login information. The hackers then captured the login credentials and used it to access the university computer systems.[5]

WHY TARGET LOCAL GOVERNMENTS

While local governments may not seem like great targets because of the money or the data they collect, local governments are enticing targets to hackers because of their digital connections. Local government computers are digitally connected to state and federal computers. The hackers end goal is to access state and federal databases. While the federal databases have stronger security shields, it is not the same for other connected computers at lower levels of government. Rather than trying to hack straight into the federal system, an easier route might be to go through a local, more vulnerable, computer system that is digitally connected.[6]

There has been an increase in cyberattacks targeting state and local government organizations mainly because these levels of government have fewer resources than the federal government. A report released in late 2019 showed that at least 174 municipal organizations were targeted by ransomware in 2019 – a 60% increase over 2018.[7]

STAY INFORMED AND BE PREPARED

For many people, they don't consider themselves to be Information Technology (IT) or computer savvy, however, because the threats are real and the services provided by locals are critical, all local officials and employees must take the cybersecurity problem seriously. To promote more awareness of the need for cybersecurity planning, the following organizations collaborated on this publication: the Association of Indiana Counties (AIC), Accelerate Indiana Municipalities (Aim), and the Indiana Association of County Commissioners (IACC) to provide an overview of the cybersecurity planning process.

ACKNOWLEDGMENTS

The local government associations would like to thank Purdue University's Technical Assistance Program cyberTAP group, along with Mark Green and Jason Dell from Network Solutions, Inc., and Todd Vare of Barnes & Thornburg for their specific contributions to Part 3 of this publication.

II. STATUS OF LOCAL GOVERNMENT

AWARENESS

While there is little quantifiable data available at the present about the preparedness of local governments in Indiana to guard against cyberattacks, on a nationwide basis, the International City/County Management Association notes that most local governments in the United States don't have a strong grasp of the policies and procedures they should implement to protect their technology systems from attacks.[8] Forty-four percent of local governments nationwide reported that they regularly face cyberattacks on either an hourly or daily basis. More troubling is the high percentage of governments that do not know how often they are attacked (28 percent) or breached (41 percent). Further, a majority of local governments nationwide do not catalog or count attacks (54 percent). [9]

LOCAL GOVERNMENT RESOURCES

In 2019, county governments in Indiana received a boost with their cybersecurity protection efforts. The Indiana Secretary of State's Office entered into an agreement with California-based FireEye Security to provide counties with desktop and email protection, as well as 24/7 live network monitoring. The effort initially focused on county clerk's offices and elections related personnel but broadened to include all end points. Using federal funds purposed for election security, the secretary of state provided FireEye's capabilities to all 92 counties at no cost for three years. Senate Enrolled Act 179 (Public Law 135) passed by the Indiana General Assembly in 2020 *required* counties to enter into an agreement with the Secretary of State to use the FireEye software for specified security purposes.

One thing that is apparent about local governments in general is that there is a varied level of resources available to devote to IT matters in general. While some larger counties may have 25 or more IT professionals[10], other units of local governments such as small towns may not even have outside IT assistance engaged year-round on a contract basis.

III. INITIAL PLANNING FOR CYBERSECURITY

WHERE DO WE START?

Though cybersecurity is different from traditional risks facing local governments, it is fundamentally a risk management challenge centered on the protection of electronic information and systems. The U.S. government standard framework for managing information systems risk is detailed in a series of National Institute of Standards and Technology (NIST) Special Publications (SPs) shown in Figure 1, below.[11]

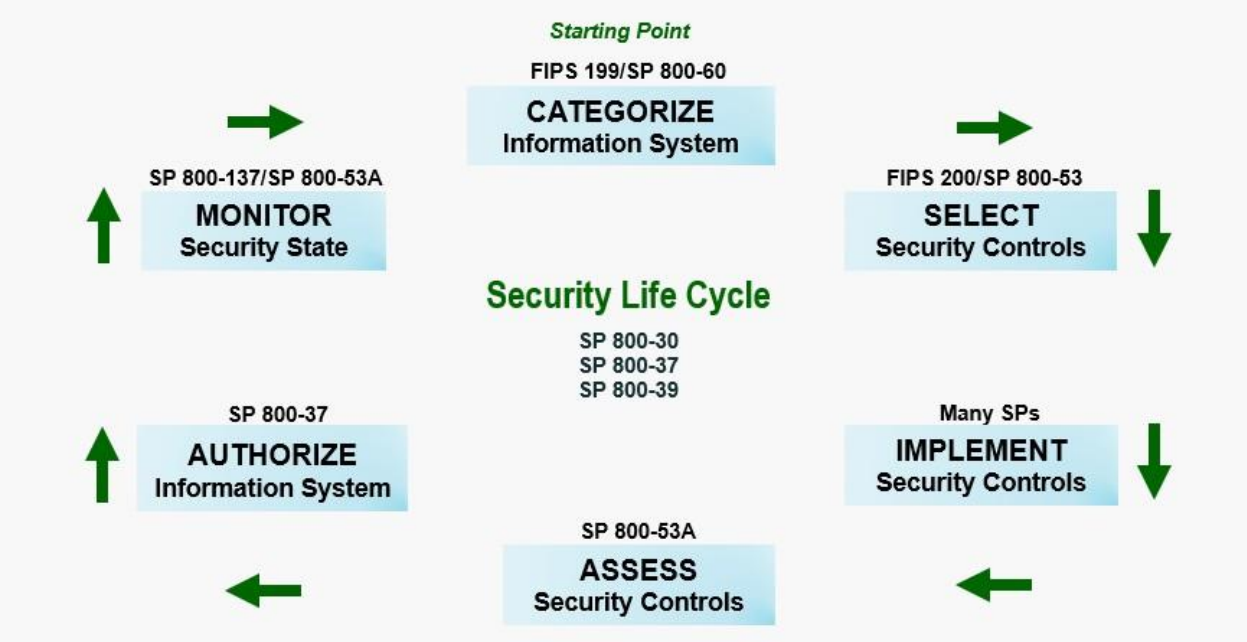

Figure 1: NIST Risk Management Framework

Section V of this guide describes the process for identifying and managing cybersecurity risk in terms of the NIST Risk Management Framework while providing guidance and resources targeted specifically at local governments.

WHO SHOULD BE AT THE PLANNING TABLE

In order to start the cybersecurity planning process, local leaders must create a culture of cybersecurity that imagines worst-case scenarios and explores a range of solutions to mitigate threats to the ecosystem of local government technology. This involves prioritizing funding for cybersecurity, establishing stronger cybersecurity policies and training employees in cybersecurity protocols. Cybersecurity is more than just the IT department's problem. Success will require collaboration with:

- Local elected officials
- Internet-technology and cybersecurity staff members

- Department managers
- End users[12]

PLANNING TIME FRAME / WRITING THE PLAN

Developing your cybersecurity plan is going to involve research and fact finding. Depending on the local unit of government's size, you can expect plan development to take between six months to one year, or longer. While developing a cybersecurity plan is discussed in greater depth under Section IV, it starts with risk assessment which includes knowing what assets you own and finding out what insurance companies will require in order to obtain an insurance policy. Once you have the results of your research regarding risk assessment, you will group your risks into like categories, address those groups as part of a cybersecurity plan, and develop a one to two year plan to address the following: realistic timelines and answers, internal project management and internal resources.[13]

Your plan will need to be written and communicated throughout your unit of government. It is recommended that the plan should include a one to two page executive summary with the main findings, a spreadsheet or table showing the initial plan, along with a 20-25 page document showing the security plan which details timelines, staff needed, money needed and estimated completion time for each item.[14]

Though this guide focuses on the security of electronic information and information systems, your government should ensure that risks related to paper records are categorized, assessed, controlled, and monitored as part of the same process used for electronic information and systems.

IV. CREATING A CYBERSECURITY PLAN

The *state* governments that are currently leading in cybersecurity have adopted and implemented security controls based on nationally recognized frameworks. Two of the leading and most commonly adopted frameworks are the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the International Organization for Standardization.[15] Our recommendations here are based on the NIST Framework, which is intended to be useful to companies, government agencies, and not-for-profit organizations regardless of their focus or size. Because each organization's risks, priorities and systems are unique, the tools and methods used to achieve the outcomes described by the NIST Framework will vary. [16]

The NIST framework recommends a five step approach:

1) Identify
2) Protect
3) Detect
4) Respond
5) Recover

IDENTIFY YOUR ASSETS / RISK MANAGEMENT

First, a local unit of government must develop an understanding of their systems, people, assets, data, and capabilities.[17] At the top of the list is critical infrastructure. The US Patriot Act of 2001 defines "critical infrastructure" as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." NIST recommends that due to the increasing pressures from external and internal threats, organizations responsible for critical infrastructure need to have a consistent and iterative approach to identifying, assessing and managing cybersecurity risks. [18] This approach is necessary regardless of an organization's size, threat exposure, or cybersecurity sophistication today.[19]

Risk management is the ongoing process of identifying, assessing and responding to risk. With an understanding of risk tolerance, local governments can prioritize cybersecurity activities, enabling local officials and staff to make informed decisions about cybersecurity expenditures. A local unit may choose to handle risk in different ways, including mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk, depending on the potential impact to the delivery of critical services.[20]

It is important that local units identify emerging risks and use cyber threat information from internal and external sources to gain a better understanding of the likelihood and impact of cybersecurity events.[21] In addition, it is important for local units to embark on supply chain risk management (SCRM) during the procurement process because outside suppliers of goods and services can introduce vulnerabilities to the local unit's cybersecurity. The primary objective of

cyber SCRM is to identify, assess, and mitigate products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the cyber supply chain. These activities may include determining cybersecurity requirements for suppliers, instituting the requirements through contracts or other formal agreements, communicating with suppliers how the cybersecurity requirements will be verified, and verifying and validating that the requirements have been met.[22]

PROTECT YOUR ASSETS

The second step is to protect your assets by developing and implementing appropriate safeguards to ensure delivery of critical services.[23] Protecting assets requires a multi-faceted approach. It includes identity management and access control, awareness and training, data security, information protection processes and procedures (such as backups and redundancies), maintenance, and using protective technologies (such as firewalls – software that prohibits suspicious information from delivery).[24]

DETECT INCIDENTS

Detection requires development and implementation of appropriate activities to identify the occurrence of a cybersecurity event.[25] Being able to recognize an anomaly or an event is key and this only occurs through continuous security monitoring and institution of detection processes.[26]

RESPOND WITH A PLAN

Investments in planning and exercises support timely response and recovery actions following the detection of a cybersecurity incident, resulting in reduced impact to the delivery of services.[27] It must be contemplated in advance what potential system failures might occur and what plan of action would take place based on each scenario. Prioritization of critical infrastructure and systems is important. For instance, if all systems went down within your local unit of government, it's likely that any support to emergency medical services or 911 would be at the top of the list to be restored.

Testing the viability of your plan is also important. Mock cyberattack exercises should be part of your response planning procedures.

RECOVER NORMAL OPERATIONS

Your end goal is to restore any capabilities or services that were impaired due to a cybersecurity incident.[28] Once operations have been restored, it is important to go back and review the incident to analyze the effectiveness of the response and timing.

V. CYBERSECURITY AS RISK MANAGEMENT

CATEGORIZING INFORMATION SYSTEMS

The goal of categorizing of information and systems is to determine the severity of the impact to your government and its citizens if the *confidentiality, integrity, or availability (CIA)* of the information, or the systems affecting that information, is impaired. Information and systems impact categorization is a crucial first step in the development of your information security plan because these categorizations drive the types and amount of controls used to safeguard the information that your government owns and manages. If too little control is applied to information, your government will face an unacceptable level of information security and privacy risk. If high impact controls are applied to all of your government's information, unacceptable levels of cost will result. So, organizations first need to inventory and categorize information and systems before they can properly apply controls to those data and systems.

In some cases, information risk categorizations are made for your government through regulation. For example, loss of CIA of health information regulated by the HIPAA Security and Privacy Rules is considered high impact because of the ramifications defined in regulation. In other cases, impact categorization is more nuanced. While building plans may not create a high impact of CIA if compromised in most cases, loss of confidentiality of the plans to the county jail or a chemical treatment plant could create a severe, negative impact on several local governments and populations. Emergency dispatch information may not be confidential, but is high-impact data because its availability is critical to the safety and security of your citizens. If your government is new to information impact categorization, or to cybersecurity planning more broadly, you should begin with broad categorizations. As the cybersecurity maturity of your government increases, your categorizations should become more nuanced. Developing more nuanced information impact categorizations is one reason why cybersecurity maturity and planning is an iterative process that requires constant effort.

SELECTING SECURITY CONTROLS

Well-designed security controls provide a level of security and privacy protections to information that match the impact categorizations through a wide range of threats to your environment with minimal impact on the function of the system or information. Because information is increasingly stored and transmitted electronically on systems administered by information technology professionals, controls applied to these data are often technical. However, the most effective controls regimes incorporate physical and administrative controls, as well as technical. For example, preventing malicious actors and/or software from accessing an e-mail system requires technical controls that stop known malicious software types and e-mail from known malicious addresses. But, e-mail security improves when users are required by policy to use strong passwords, change those passwords regularly, and are trained to recognize and respond to phishing e-mail messages that find their way through technical defenses. Layering multiple controls against information security threats is known as "defense in depth" and is the most

effective and resilient way to protect information and information systems. Several resources including: policy templates, controls frameworks, and technical guidance for your systems can help your government select the best controls for your particular environment.

IMPLEMENTING SECURITY CONTROLS

Because information security controls may be administrative, technical, and physical controls in nature, and because all local government employees have more access to the information and systems of their government than regular citizens, *all members of your organization have a role in implementing effective information security controls*. A key information security control is the use of unique access credentials for each individual user. In order to effectively implement this control, human resources or departmental personnel must notify an IT administrator to add a new, unique user to systems impacted by the hire. The IT administrator must add the new user and properly configure the new user's account, and most importantly, all users must keep their credentials secret and unique to themselves. Even when information security controls are limited to specific departments or functions, such as data backups or policies related to specific regulations like HIPAA, multiple people are involved. Therefore, all controls should be well documented and training should be developed that addresses each control and the reason for its use.

Organizational leaders have special roles in implementing information security controls. Once controls are selected, and associated policies and procedures developed are approved, leaders must consistently enforce policies and procedures. Doing so, along with constantly explaining and advocating for the use of the information security-related controls, builds a culture of information security that is a critical component of successful and mature information security programs. Most importantly, leaders must always abide by information security controls that are put in place for their organizations. While cases exist where the application of controls will necessarily differ among groups within your government, these cases must be documented and approved prior to their implementation and should be as close to the standard implementation of the control as possible.

In addition to documentation, training, and enforcement through leadership, successful implementation of controls requires that controls effectiveness be monitored. If, for example, a new acceptable systems use policy is implemented, requiring members of the organization to sign the policy provides a monitoring point that can be used to signify that users have read and understand the policy. If "acceptable systems use" in your environment requires that no non-organization-owned devices are allowed to connect to the organization's internal network, then network logs and audits of those logs may also serve as a monitoring point for the acceptable systems use policy. As with information security controls themselves, monitoring points should be deliberately determined and documented along with the control itself. Results of monitoring activities should also be documented.

ASSESSING SECURITY CONTROLS

Assessing information security controls is an ongoing and continuous process as illustrated in Figure 1 in Section III Because the environment in which local governments operate is continually changing, especially in terms of the use of information and supporting technology, security controls must be regularly re-evaluated. Assessment is a key mechanism for the evaluation of controls and may incorporate several components. As information security policies and procedures are documented, a regular interval for review should be determined. A regular, internal policy/procedure review serves to ensure that these documents continue to meet the controls needs of the organization set during the documents' creation, or if changes are required. Internal, regular, full-scale assessments are also important to evaluate the overall control structure against the overall changes to the use needs of and environment in which information is used. Finally, external, full-scale assessments are necessary to have a robust and full-scale information security program. External assessments are designed to provide a broader view of control structures not subject to internal challenges and viewpoints. These components, when well implemented, provide robust protections against unauthorized release of information, malicious use of systems, and other forms of cyber and non-cyber information attacks.

AUTHORIZING SECURITY CONTROLS

Like policies and procedures within any of the various functions of government, information security-related policies require authorization at each of the levels at which they apply. In functions such as health care and justice, information security controls are required by regulation. In other cases, such as credit card processing, information security best practices are enforced through stringent application of industry best practices. In all cases, effective information security controls programs are driven by executive leadership. A key role played by organizational leaders in information security is to approve controls. Departmental leaders will likely be involved both in drafting and approving controls for use within their departments. The approval process for departmental controls is often less formal than for approval of organization-wide controls; but, regardless of the level of formality of the approval process, all controls changes should be documented, as noted above.

Organization-wide controls face additional challenges to approval because those charged with approving controls will not always sufficiently understand the controls or the environment in which those controls will be implemented. Lack (perceived or real) of understanding by organizational stakeholders of the concepts that underpin technical controls negatively impacts the security life cycle. If stakeholders don't understand how a control works or why it is necessary, they are not likely to support its implementation or approval. Therefore, it is incumbent on the department head, as the liaison between executive level officials and departmental staff, to ensure that both groups understand and support controls recommendations. In some cases when controls face challenges in the approval process, external resources may be helpful in providing information or new perspectives on controlling risk that may be able to bridge divides among stakeholders. Information technology departmental managers and advocates within the organization face particular challenges to building

understanding of required controls for approval, but should focus on creating controls that meet the needs of approvers, can be effectively implemented, monitored, regularly reviewed, and updated as needed.

MONITORING SECURITY STATE

Among the daily challenges of delivering services to citizens, monitoring of internal controls can easily be lost. Keeping track of effective controls can be tedious and the connections among controls monitoring points and the larger mission of the government can seem abstract and distant. Yet, controls monitoring is critical to effective cybersecurity, and more broadly, information security.

Technical controls such as firewalls, switches, authentication systems and workstations have the ability to log activity that can be used to monitor critical functions, which inform the organization's cybersecurity posture and status. By themselves, these devices and logs can be helpful to maintaining information security. But, an effective, organization-wide information security control posture requires integration of various logs and monitoring points so that concerning patterns can be noted and acted upon before an incident occurs. Unfortunately, information technology leaders often find themselves trying to balance between an expensive, integrated, security monitoring solution (manual or technical) and ad-hoc log review that is ineffective at preventing cybersecurity and other attacks on sensitive information. The speed with which the cybersecurity landscape is changing, especially for local governments, prevents any organization from being fully resourced for cybersecurity. Choices must be made. Available resources should be focused on information deemed most critical and sensitive during the information classification step above. When considering the allocation of resources for monitoring of sensitive information, decision makers must take a holistic approach to information and access to it. Information can only be well-secured when the systems and physical locations where it can be accessed are also well-secured. The most effective programs for securing sensitive information integrate cybersecurity controls on systems and technology with broader physical and administrative information security controls. Monitoring security controls, therefore, should focus first on holistic controls coverage for information deemed most critical, and then move to less sensitive information using the same approach.

VI. HELPFUL LINKS

Framework for Improving Critical Infrastructure Cybersurity

National Institute of Standards and Technology (NIST)
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

State and Local Election Cybersecurity Playbook

Harvard Kennedy School Belfer Center for Science and International Affairs
https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook

Glossary of Cybersecurity Terminology

National Initiative for Cybersecurity Careers and Studies
https://niccs.us-cert.gov/about-niccs/glossary

Indiana Advisory Commission on Intergovernmental Relations Cybersecurity Survey Results

http://iacir.spea.iupui.edu/documents/CybersecurityBriefIACIR.pdf

Indiana Cybersecurity Self-Assessment Scorecard Survey

https://www.in.gov/cybersecurity/files/IECC%20Cybersecurity%20Scorecard%20Public%20fillable.pdf

Indiana Executive Council on Cybersecurity (IECC)

https://www.in.gov/cybersecurity/3812.htm

END NOTES

[1] Taylor, Hugh. (2020, January 22). *What are Cyber Threats and What to do About Them.* The Preyproject.com. https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/

[2] Kwiatkowski, Maximilian. (2019, July 17). *County Forced to Pay $132,000 Ransom to Hackers.* Nwitimes.com. https://www.nwitimes.com/news/local/govt-and-politics/county-forced-to-pay-132-000-ransom-to-hackers/article_497cd952-a648-5a72-b280-8254ecd6b229.html

[3] Nolting, Mike. (2017, August 20). *Cyber Attack Reported in Franklin County*. *Wrbiradio.co*m. https://wrbiradio.com/2017/08/20/cyber-attack-reported-in-franklin-county/

[4] Ragan, Steve. (2016, December 8). *After attack, Indiana county will spend $220,000 on Ransomware Recovery*. *Csoonline.com.* https://www.csoonline.com/article/3148274/after-attack-indiana-county-will-spend-220000-on-ransomware-recovery.html

[5] Goudie, Chuck and Christine Tressel. (2018, March 23). *Iranian Cyber Attackers Target State of Indiana and 144 Universities.* Abc7chicgo.com. https://abc7chicago.com/iranian-cyber-attackers-target-state-of-indiana-144-universities/3252887/

[6] Christian, Kurt. (2020, January 3). *Indiana Counties Battle Cyber Attackers with Help from State, Feds, Indianapolis Business Journal.* IBJnews.com. https://www.ibj.com/articles/indiana-counties-battle-cyber-attackers-with-help-from-state-feds

[7] Ibid.

[8] McGalliard, Tad. (2018, March 30). *How Local Governments Can Prevent Cyberattacks*. *Nytimes.com.* https://www.nytimes.com/2018/03/30/opinion/local-government-cyberattack.html

[9] Ibid. Citing the International City/County Management Association and University of Maryland, Baltimore County study.

[10] Christian, Kurt. (2020, January 3). *Indiana Counties Battle Cyber Attackers with Help from State, Feds, Indianapolis Business Journal.* IBJnews.com. https://www.ibj.com/articles/indiana-counties-battle-cyber-attackers-with-help-from-state-feds

[11] National Institute of Standards and Technology Privacy Workshops, https://www.nist.gov/document/nistprivacyriskworkshop6517pptx

[12] McGalliard, Tad. (2018, March 30). *How Local Governments Can Prevent Cyberattacks*. *Nytimes.com.* https://www.nytimes.com/2018/03/30/opinion/local-government-cyberattack.html

[13] Presentation by Mitchell Parker, IU Health.

[14] Ibid.

[15] IT Alliance for Public Sector. *State Cybersecurity Principals and Best Practices*. *Itic.org,* https://www.itic.org/dotAsset/6b96ecc0-53d8-4068-b2a5-4fd79676c9ed.pdf

[16] Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, National Institute of Standards and Technology, p. 2. (2018, April 16). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[17] Ibid, p. 7.

[18] Ibid, p. 1.

[19] Ibid.

[20] Ibid, p. 4.

[21] Ibid, p. 14.

[22] Ibid, p. 16.

[23] Ibid, p. 7.

[24] Ibid, 23.

[25] Ibid, p. 7.

[26] Ibid, p. 23

[27] Ibid, p. 6.

[28] Ibid, p. 8.