PELL CENTER
for INTERNATIONAL RELATIONS
and PUBLIC POLICY

Rhode Island Corporate Cybersecurity Initiative

October 2017

SURVIVING A CYBER ATTACK

Preparedness and Resiliency in Action

After-Action Report & Supplemental Material

Francesca Spidalieri
Senior Fellow, Cyber Leadership

Executive Summary

This report is based on content discussed during the "Cybersecurity & Healthcare Tabletop Exercise," conducted by the Salve Regina University's Pell Center in collaboration with PreparedEx, SecureWorks, and the Newport County Chamber of Commerce on May 10th, 2017.[1] The event was attended by senior leaders and security professionals from over 30 healthcare organizations in New England, as well as representatives of the R.I. Department of Health, R.I. Office of the Health Insurance Commissioner, and law enforcement agencies. The primary goal of this cybersecurity tabletop exercise was to provide healthcare organizations and state agencies with greater insight into the specific cybersecurity issues they face and explore possible responses and mitigation strategies that could lead to industry-driven solutions.

The exercise involved a series of cyber intrusion scenarios created to identify weaknesses common in the healthcare industry and addressed real-world cascading effects, including consequences for the provision of healthcare, outcry from patients, and media fallout for the organizations that fall victim to such attacks. The exercise was designed to show how different cyber threat vectors can infiltrate even the most sophisticated computer systems and networks, and also to explore possible remedies, mitigation techniques, and incident responses. Participants worked together on a range of timely and important cyber-related issues, including: ransomware and data breach response and remediation, data leakage considerations, digital forensics investigations, crisis management, legal and regulatory compliance, and cyber liability insurance.

This event was part of the Pell Center's Rhode Island Corporate Cybersecurity Initiative (RICCI), an ongoing effort aimed at bringing together senior leaders from various sectors in Rhode Island who can affect change and make the state more secure and resilient to cyber threats. Congressman Jim Langevin (D-RI) joined this group of senior leaders for a keynote address on the future of the healthcare law and on best practices to strengthen the cybersecurity posture of healthcare organizations.

This report identifies key issues and recommendations in the following categories:

1. Management buy-in: Prioritize cybersecurity as an enterprise-wide responsibility with support and direction from leadership and duties and accountability extending through every level of the workforce.

2. Proactive Risk Mitigation: Take stock of sensitive data in your system and identify, assess, prioritize, and address cyber-related risks before an incident occurs.

3. Policy and Procedures: Establish appropriate policies and procedures for effective incident response and business continuity plans.

4. Cybersecurity Awareness and Education: Develop effective programs to train and educate employees on roles and responsibilities pertaining to cybersecurity.

5. Information Sharing & Partnerships: Join formal and informal networks of information sharing with industry partners (e.g. NH-ISAC) and law enforcement (e.g. InfraGard).

The information provided in this report and the Supplemental Material in the back can be used as a tool for ongoing efforts to review existing plans, update policies, build relationships with other organizations in your community, and strengthen patient safety and data security across your entire enterprise. We have also included recommendations derived from past Pell Center reports, and the "Report on Improving Cybersecurity in the Healthcare Industry" released to Congress by the Health Care Industry Cybersecurity Task Force in June 2017.[2] Senior leaders and management should work together in conjunction with their IT departments to determine applicability of items contained in this report. The information does not constitute legal advice or counsel. Please direct any comments or feedback regarding this report to Pell Center's Senior Fellow, Francesca Spidalieri, at Francesca.spidalieri@salve.edu.

Background

Media headlines in recent years have shown an increased number of cyber attacks targeting the healthcare industry, including hospitals, insurance companies, small practices, and others who manage medical records. Since 2009, over 170 million Americans have had their personal health information breached or accidentally disclosed; a number expected to grow due to the high value compromised data can command on the black market, along with the continuous digitization and sharing of medical records.[3]

According to a May 2016 Ponemon Institute's study on privacy and security of healthcare data, data breaches are costing the healthcare industry a walloping $6.2 billion a year, with an average cost of over $2.2 million per breach for covered entities and more than $1 million for business associates.[4] Nearly 90 percent of the healthcare organizations surveyed in the study had experienced a data breach during the previous two years, and nearly half (or 45 percent) had more than five data breaches in the same time period. A data breach in the healthcare sector can have not only financial and reputational effects on the company targeted by the threat actors, but could have dramatic ramifications for the patients due to the nature of the information disclosed. Electronic medical records are a treasure trove of sensitive – and very valuable – information, from patients' social security numbers to medical histories and insurance billing details. These information can be used for identity theft and fraud or to get medical treatment, medical equipment or prescription drugs in your name. This, in turn, can result in bogus information added to your medical file, changes to your healthcare benefits, and potential life-threatening consequences.

Criminal attacks continue to be the leading cause of data breaches in the healthcare industry, along with insider breaches and internal problems such as employee mistakes, accidental disclosures, third-party snafus, and stolen or lost devices with unencrypted patient information on them. In 2017, the healthcare sector suffered the most security incidents, surpassing the public sector and every other private industry, with an increased number of ransomware, malware, and denial-of-service (DoS) attacks.[5]

In May 2017, one of the largest ransomware attacks on record – "WannaCry" – spread quickly around the world, infecting more than 300,000 computers across nearly 150 countries and disrupting services in multiple industries and especially healthcare organizations. While the WannaCry ransomware attack was certainly not the only internationally scaled cybersecurity threat in recent years, this attack's consequential

impacts served as a stark reminder of the significant vulnerabilities at the intersection of technology and medicine, and especially of the threats the use of legacy equipment, lack of understanding of cyber risks, limited education and awareness programs for healthcare professionals, and hyper-connectivity of medical devices and hospital networks pose to patient safety. Healthcare organizations were hit particularly hard with hospitals in England forced to cancel surgeries and unable to perform even simple x-rays in emergencies.

With an eye towards mitigating similar cyber attacks and increasing preparedness and resilience to cyber risks, the Pell Center conducted a cybersecurity and healthcare tabletop exercise on May 10th, 2017 – just three days before the debilitating WannaCry attack – focusing specifically on the challenges and potential responses to growing cyber threats in the healthcare industry. The exercise included a similar ransomware attack to the WannaCry one, in addition to a series of other cyber intrusion scenarios, such as email spoofing, phishing attacks directed at patients, data exfiltration, system compromise, and other cyber attacks aimed at disrupting service delivery and stealing valuable personal healthcare information (PHI).

Mitigating these risks is a must for operators and insurers of the healthcare industry. Covered entities must also be compliant with the Health Insurance Portability and Accountability Act (HIPPA), which requires to implement physical, technical, and administrative controls to safeguard protected health information (PHI) and to report breaches (including ransomware attacks).[6] Being compliant with existing laws and regulations, however, does not mean a healthcare organization has a good security posture. HIPAA requirements should be viewed as a minimum standard for privacy and security. To prevent data breaches, disruptions of service, and increasingly even deletion or manipulation of data, healthcare organizations need to look beyond compliance.

The Pell Center Cybersecurity and Healthcare Tabletop Exercise addressed these and many other issues currently affecting the healthcare industry, and in particular the security of the sensitive data that has been entrusted to them by their patients and employees. This After-Action Report identified key issues and recommendations in the following categories:

1. Management buy-in

While the healthcare industry has historically viewed cybersecurity as an IT challenge, often approached reactively and not seen as a solution that directly impacts patients' care, this approach is no longer acceptable. Today, no board, senior executive or even owner of small practices and rural hospitals can ignore cybersecurity – it is the source of systemic risk and potential damaging "material effects" that can hurt an organization's profits, value, brand, reputation, and put patients' safety at risk. Leadership support and involvement are fundamental for the success of a comprehensive cybersecurity program. While cybersecurity is a shared responsibility, creating a culture of security that prioritizes addressing cyber risks across the entire organization must start at the top. If management is committed to a culture and environment that embraces honesty, integrity, security, and ethics, employees are more likely to uphold those same values. Cybersecurity must be integrated front and center into daily activities and anchored into the management's decision-making processes in a holistic and comprehensive manner. Making the decision to prioritize and resource cybersecurity in healthcare requires a cultural shift and increased support and direction from leadership, with duties and responsibilities extending through every level of the workforce.

In recent years, senior management and board members across industries have become more involved in cyber risk management activities, and some organizations have started to put in place formal structures to report risk assessment results and cyber preparedness levels back to the board. Some of the best practices and lessons learned from the field include:

- Aligning the business objectives and critical business functions with the security needs of the organization and the patients they serve, and making cybersecurity an organizational issue designed to keep patients safe from digitally-sourced harm – the focus is the patient!
- Identifying critical stakeholders and establishing cybersecurity roles and responsibilities within the organization. This may include performing a gap analysis to identify the roles and responsibilities that are not appropriately filled, and deciding which positions are most critical to the organization's security (e.g. Chief Information Security Officer (CISO)). Smaller healthcare providers (e.g. dental office, small medical practice) that are not be able to afford full-time technical resources should consider outsourcing some of these services or leveraging shared service providers. It is fundamental to match the culture of the organization to the type of workforce needed and understanding the specific human capital needs and resources allocated specifically for cybersecurity.
- People specifically responsible for the organization's cybersecurity posture should be properly deployed across the various functions of the organization, enabled with clear scope of responsibilities, empowered with the appropriate authorities and reporting chains, and supported with ongoing training and development.
- Effectively communicating the organization's values and priorities from the top and throughout the organization to employees and stakeholders, and also to business partners, vendors, and other third parties through training, policies, on-the-job mentoring, memos/codes of conduct, and other awareness programs in order to minimize risks and ensure enterprise-wide adoption.
- Understanding the threat landscape, and staying abreast of the latest techniques and vulnerabilities relevant to your organization and best practices to combat those threats.
- Conducting an in-depth analysis of the potential direct and indirect costs and impacts of cyber incidents to the organization and patients' safety, which may also help justify increased investments to manage specific cyber risk areas.

- Making cybersecurity a regular topic of discussion during executive team and Boards of Directors meetings; and including regular briefings on the cybersecurity risks and threats the organization is facing and the resources (e.g. personnel, capital, material) needed to mitigate and/or manage them in such a manner that supports the mission and future viability of the organization.
- Leveraging available studies and statistics to show where your organization is compared to others in the same industry, and understanding what added value can be brought to the table, and what can be done more proactively and efficiently.
- Deciding whether to purchase cyber liability insurance to moderate the impact of cyber risks, including insider negligence and third party risks.

2. Proactive Risk Mitigation

Boards of Directors, C-suite executives, and senior management ultimately bear the responsibility for cybersecurity issues, and must view cyber risk as a component of their overall enterprise risk management process rather than as a compliance issue. While cyber risks and vulnerabilities cannot be completely eliminated, they can be managed and reduced through informed decision-making processes, careful planning, and appropriate allocation of resources. These are some of the best practices identified in this category:

- Taking stock of sensitive data in your system and knowing where they are stored, who has access to them, and how they are being protected (e.g. encryption, systems segregation, dual-factor authentication) – governance should ensure that access to PHI is limited to those who really need it and that actual access is checked against this list. Small and medium-sized healthcare providers looking for cost-effective solutions to their legacy EHR systems, aging infrastructure, and poorly protected local servers and databases, should evaluate options to migrate patient records and other information to more secure environment (e.g. cloud, shared computer environments).
- Encrypting PHI and other sensitive data on computer systems and portable devices;
- Not collecting data unless needed and getting rid of it as soon as of no use;
- Having a full inventory of all the devices connected to your network and to EHRs (e.g. mobile devices, medical devices, applications), and limiting employee access to resources and devices that aren't necessary for daily workflow and activities.
- Shifting the focus to proactively identify, assess, prioritize, and address cyber-related risks – audits are not sufficient – and developing cyber risk mitigation strategies, including working with management to establish the vision, risk appetite, and strategic direction of the organization.
- Aligning security controls with the risk and impact to the organization.
- Developing a strategy for cybersecurity hygiene for existing and legacy equipment, a systemic approach for patching operating systems and medical devices as soon as updates become available, and for addressing related vulnerabilities in older medical device models (legacy systems);
- Ensuring that all software and anti-virus programs are up-to-date.
- Creating backups of all critical files, which should be frequently updated and kept in a secure location.
- Being able to restore systems from backups in a timely way.
- Putting together a cross-functional crisis and incident response team.

There are also various independently-validated best practices, industry-specific standards, security controls, assessment

tools, and benchmarks that can help healthcare organizations assess their cybersecurity readiness, identify and address weaknesses and shortcomings, and proactively mitigate risks. While no framework fits every organization, the following foundational references should be considered by healthcare organizations to define roles, responsibilities, and activities associated with managing cyber risks, secure store and share PHI, and safely incorporate medical devices in their IT networks:

- The International Organization for Standardization (ISO) IEC 80001: Application of risk management for IT-networks incorporating medical devices on roles, responsibilities, and activities;[7]
- The International Organization for Standardization (ISO) IEC 80001: Application of risk management for IT-networks incorporating medical devices;[8]
- The Health Information Trust Alliance (HITRUST) Common Security Framework (CSF);[9]
- The National Institute for Standards and Technology (NIST) Cybersecurity Framework offers a tool (identify, protect, detect, respond, and recover) that can help understand, manage, and communicate cybersecurity risks. While the Framework is not specific to the healthcare industry, it provides a high-level description of standards and best practices to help organizations manage cybersecurity risks. The FDA provides additional industry specific guidance for medical device risk management through its pre- and post-market guidance for management of medical device cybersecurity. These documents align to and overlay with the NIST Cybersecurity Framework.[10]

3. Policy and Procedures

Policies make clear acceptable and unacceptable actions in an organization and dictate the consequences for negligence or intentional failure to comply with communicated policies, while procedures provide more detailed instructions on how to implement those policies. Together, they help arm personnel within an organization with rules and tools to address issues that may arise and facilitate more informed decision-making leading to more effective resource allocation, operational efficiencies, and the ability to mitigate and rapidly respond to cyber threats. Their core objectives should be to: protect sensitive information; secure critical services and infrastructures; minimize downtime and business disruption caused by a cyber incident; articulate a clear course of action in the event of a cyber incident; preserve brand and reputation; comply with regulations and legal mandates; and maintain good relationships with patients and other partner organizations. These were among the most important takeaways from our exercise:

- Instituting clear cybersecurity policies for employees and third-parties governing the use of organization resources, systems, facilities, and equipment (e.g. computers, smartphones, tablets, medical devices) and access to PHI and other sensitive information.
- Establishing procedures to monitor systems usage; identify potential internal threats; and to remotely wipe information from stolen or lost devices used to store PHI.
- Holding employees accountable for their role in limiting access to only those systems and data that they actually need to do their job, and immediately revoking that access when an employee leaves or changes roles.
- Establishing a safe procedure to report a cyber incident or internal mistake, and ensuring that if employees witness unethical behaviors from other employees or third party vendors that they have a process to report such behavior with guaranteed anonymity and without fear of retaliation. This will also foster a culture and environment that encourages and rewards timely reporting.
- Negotiating clear security requirements for third party vendors and service providers that have access to sensitive and

confidential information or provide critical services, and review them regularly.

- Implementing good patch management policies and procedures to perform weekly checks to ensure software and operating systems are up to date with all patches applied;
- Establishing clear protocols to triage, prioritize, and escalate alerts and responses – know when to declare an incident, who is responsible, and who should be involved from management down;
- Developing well-exercised and regularly updated crisis management, incident response, business continuity, and disaster recovery plans for emergencies and crises, including "playbooks" for all stakeholders within the organization. Response to cyber incidents should be planned and tested like other serious incidents that can affect healthcare organizations, such as fast-spreading viruses or diseases.
- Conducting regular, cross-functional, and impactful exercises and drills that include the senior leadership team from within organizations, and that take into consideration the need to operate in a degraded environment and run business functions on alternate systems (including going back to paper records) in the event of network and/or devices disruptions.
- Devising a good communication plan and having a unified and consistent message both internally and with the public in the event of a cyber incident – common messaging shows confidence and professionality (consider also developing a canned FAQ that they can rely on for interviews and unannounced visits/ calls from the press). General Counsels, human resource, and public relation/ communication departments should also be included in the communication and crisis management planning.
- Having clear reporting and notification procedures in place if a breach happens. HIPPA requirements and the Rhode Island Identity Theft law are reported in the Supplemental Material.

4. Cybersecurity Awareness and Education

While the conventional wisdom in the healthcare industry may still be that cybersecurity is an IT challenge, it is increasingly obvious that it is very much a "people problem" too. Technology solutions can be purchased to make it harder for hackers to gain access to networks and data, but no matter how good any particular technology is, its efficacy is limited if it is not effectively adopted, implemented, and correctly used by skilled employees who follow well-defined processes.[11] Moreover, while technology failures, malware, and medical device vulnerabilities can be blamed for many cyber incidents in the healthcare sector, the "people problem" is often at the core of some of the most damaging cyber attacks we have witnessed in recent years. Indeed, most cybersecurity issues start with ordinary users – from doctors to nurses to billing clerks – who have not received proper training, are not aware of the risks, do not take cybersecurity seriously, or prioritize convenience over security by – consciously or not – sidestepping basic standards of best practices. Increased cybersecurity awareness can be an enabler for healthcare organizations, supporting both business and clinical objectives, as well as facilitating the delivery of efficient, high-quality patient care.[12] Best practices and effective mechanisms that can help healthcare organizations raise cybersecurity awareness and manage a professional cybersecurity workforce include:

- Increasing cybersecurity awareness and engaging the entire workforce in protecting the organization and their most critical assets — patients!
- Educating all employees about malicious content, phishing, scams, and how to identify and avoid it, and ensuring that personnel across the enterprise are regularly trained and tested so that they understand and fully appreciate their role in maintaining a strong cybersecurity posture. People learn and absorb things differently, so make sure to use different means and methods to get the message

out. For instance, if employees understand how to protect themselves and their families at home, they are more likely to uphold the same best practices at work.

- Organizing regular cybersecurity awareness trainings and campaigns across the entire organization to reinforce best practices in cyber hygiene and fostering a culture of cybersecurity. Organizations should leverage existing federal cyber awareness campaign (e.g. DHS Stop.Think.Connect. and the Federal Trade Commission (FTC) OnGuard Online) and resources to create consistent messaging and develop foundational, specific, and actionable tips and takeaways for different stakeholders.[13]
- Encouraging security professionals, especially chief information security officers (CISOs), to understand the business they are in, the problems and risks that a certain security tool or software may be able to address, and how to integrate security into business, and business into security. Their soft skills should include being able to communicate, negotiate, and develop relationships within the executive team and the board, so that they can be present when privacy and security issues are being discussed.
- Recognizing that cybersecurity is a complex subject that requires knowledge and expertise from multiple disciplines (e.g. computer science, information technology, engineering, policy, law, ethics), and fostering a diverse workforce – it takes diverse experiences, different talents, and different ways of thinking to solve complex problems.

5. Information Sharing & Partnerships

Information sharing is an integral part of an effective cybersecurity culture. Effective, timely, and actionable information sharing can improve security and resilience for the organization and the broader community. Sharing information, both internally from and to senior leadership and other members of the organization and externally to industry peers, trusted third parties, law enforcement, and security organizations, can be a force multiplier; it expand capabilities and improves incident response, crisis management, and recovery. Consider the following when making a decision on who to share information with and what may be important to share:

- Identifying the right partners who could benefit from information you may have or who could be of assistance during a cyber incident or on whom you depend for critical services. For instance, consider becoming a member of formal networks of information sharing with industry partners (e.g. NH-ISAC), or getting involved in a consortium, informal partnership (e.g. Pell Center's RICCI initiative), or other forums dedicated to sharing best practices and effective mechanisms to counter cyber threats.[14]
- Establishing relationships with law enforcement (e.g. FBI, RI State Police Computer Crimes Unit, Fusion Center, InfraGard) and other government officials to interdict or investigate cyber crimes (such as fraud, identity theft, data breach, etc.)
- Integrating information sharing into your incident response plan and establishing thresholds and triggers on what, when, and with whom to share information during an incident or crisis.
- Addressing real or perceived barriers given to justify not sharing information (e.g. fear of reputation damage, bad publicity, loss of patients' trust), and addressing those concerns.
- If you think you might be the victim of medical identity theft, contact the Identity Theft Resource Center for more information and resources.[15]

Supplemental Materials

Overview

Regulatory issues present challenges and opportunities, from a governance, legal, IT, audit, and operational perspective. Most, if not all, organizations, regardless of profit vs. non-profit, large vs. small, fall under some state and/or federal regulations that impact the use of information.

The goal of organizations is not to develop a "new" approach for each regulatory requirement, but rather to develop a culture of security and responsible implementation of regulatory requirements. A majority of the regulations do not pursue proactive enforcement, compliance is assessed when a complaint has been lodged or a violation becomes apparent. Having the groundwork in place to undergo an audit or investigation can make all the difference in the findings report or in responding to a major cyber incident. Most of the regulatory requirements stipulate the adoption of a comprehensive information security program, which includes the following:

- Designation of a competent authority—the individual who is responsible and accountable for the implementation of the information security and risk management program for the organization;
- Identification of material internal and external risks to the security, integrity, and confidentiality of personal information stored, collected, processed, maintained, acquired, used, owned or licensed by the organization;
- Reasonable security procedures and practices put in place to control risks associated with information. Obviously specific requirements will vary based on the individual regulation, the company size, etc., but core components can be distilled into very basic, understandable definitions of awareness and action.

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) was enacted as federal law in 1996. There have been numerous amendments and additions to the act since it was originally enacted, including the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act.

HIPAA is best known for its data protection rules. They address the security and privacy of personally identifiable health information.

Title 1 of HIPAA addresses the availability and coverage of group health plans and certain individual health plans while also making provisions for health coverage if a person loses or changes their job. Title II is focused on administrative controls, and is also known as the Administrative Simplification (AS) provisions. Title III sets standards for transactions and codifies national identifiers for major participants in healthcare such as providers, insurance companies, and employers. There are five specific rules that make up the AS portion, namely: the Privacy Rule, the Transactions and Code Sets Rule, the Security Rule, the Unique Identifiers Rule, and the Enforcement Rule.

Under HIPPA, a breach is any impermissible use or disclosure of unsecured Protected Health Information (PHI) that harms its security or privacy. The use or disclosure must cause a significant risk of harm to the affected person (the harm can be financial or reputational). The HITECH Act specifically addresses privacy and security of the electronic transmission of health information, and sets out explicit procedures surrounding breach notification requirements of PHI. In fact, HIPAA Privacy Rule requires all covered entities to mitigate an unauthorized use and disclosure of PHI, and the HITECH Act requires to notify people if their PHI was used or disclosed in an unauthorized manner (PHI must be encrypted through HHS-approved process to be considered secure). If a covered entity or business associates have a breach of unsecured PHI, they must notify the victims within 60 days of the discovery.

More information about HIPAA can be found at https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf.

Rhode Island Identity Theft Protection Act of 2015-General Rules Chapter 11-49.3

The Rhode Island Identity Theft Protection Act of 2015 updated the 2005 version of the same law, and is the main R.I. law on electronic data breaches and notification of breach requirements.[16] According to the new statute, any "municipal agency, state agency, or person that stores, collects, processes, maintains, acquires, uses, owns or licenses personal information about Rhode Island residents" is subject to the law. Contained under the umbrella term "Personal Information" is a Rhode Island resident's Social Security Number, driver's license number, account information regarding financial services, medical and health insurance information, and email addresses with passwords. Entities retaining personally identifiable information (PII) of R.I. residents are forbidden from holding on to them longer then it is required to provide necessary services and must, after a period of time, destroy all held personal information. Should a data breach be discovered by the information holder, the law mandates that a notification of the breach must be made within 45 days and, should that breach affect more than 500 Rhode Islanders, the entity would be required to notify also the attorney general and major credit reporting agencies.

The notification to individuals must include a description of the incident, the type of information subject to the breach, the date of the breach, and any services offered to those affected. Violations of the law are a civil violation bearing a penalty of up to but not more than $100 per record for reckless violations of this law, and up to but not more than $200 per record for knowing and willful violations. The attorney general may bring an action in the name of the state against the business or persons in violation.

More information on the statute can be found at: http://webserver.rilin.state.ri.us/BillText/BillText15/SenateText15/S0134B.pdf.

National Institute of Standards and Technology (NIST) Cybersecurity Framework

The NIST Cybersecurity Framework, created in 2013 through collaboration between industry and government, consists of standards, guidelines, and practices to promote the protection of critical infrastructure, as well as businesses across all industries.[17] The Framework did not introduce new standards or concepts; rather, it leveraged and integrated industry-leading cybersecurity practice from various standards bodies that have proved to be successful when implemented, and could also deliver regulatory and legal advantages that extend well beyond improved cybersecurity for organizations that adopt it early.

The Framework provides an assessment mechanism that enables organizations to determine their current cybersecurity capabilities, set individual goals for a target state, and establish a plan for improving and maintaining cybersecurity programs. This prioritized, flexible, repeatable, and cost-effective approach can help organizations manage cybersecurity-related risk.

NIST has also started a campaign to clarify and highlight how other industry guidelines and standards can be used in concert with the NIST Framework, and offers various tools to organizations to better understand the effectiveness of their cybersecurity efforts, including a self-assessment tool.

More information on the NIST Framework can be found at http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm.

Rhode Island Joint Cyber Task Force (JCTF) - Rhode Island State Police Computer Crimes Unit

The Rhode Island Joint Cyber Task Force (formerly known as the Cyber Disruption Team) is a multi-disciplinary group of cybersecurity professionals available to help organizations respond and assess during the beginning stages of a cybersecurity-related incident. Led by the Rhode Island State Police Computer Crimes Unit, members can provide immediate triage and incident response functions based on their sector and/or specialty. Working in conjunction with its partners, the JCTF can leverage its intelligence capabilities to place your incident in a larger context (if applicable), and can help connect you with more in depth services, as needed.

Think you have all the right policies and procedures in place? Not sure? The JCTF also helps critical infrastructure entities complete confidential self-assessments on their cyber incident response and business continuity plans. If you are interested in learning more about self-assessments or our other outreach missions, please contact us.

Contact: Captain John Alfred, Cyber Crimes Unit and Fusion Center Commander

Tel: 401-921-8148, email: john.alfred@risp.gov

Rhode Island Department of Health Center for Emergency Preparedness and Response (CEPR)

The Center for Emergency Preparedness and Response (CEPR) at the Rhode Island Department of Health (RIDOH) is dedicated to creating and promoting a state of readiness and prompt response to protect the health of Rhode Islanders during catastrophic events and large-scale disasters and emergencies. CEPR accomplishes its mission by coordinating education, assessment, planning, response, and support services involving public health providers, private medical providers, public safety agencies, and government officials. CEPR staff work with all of the Centers within RIDOH as necessary to respond to all hazards, including responding to the consequences of a cyber event that may impact healthcare facilities, drinking water systems, or food establishments. CEPR staff serve as the Emergency Support Function (ESF) 8: Public Health and Medical Services liaisons during activations of the State Emergency Operations Center.

Contact: Alysia Mihalakos, Chief, Center for Emergency Preparedness and Response

Tel: 401-222-8035, email: alysia.mihalakos@health.ri.gov

To report an emergency with healthcare or public health impact 24/7: 401-222-6911

Healthcare Coalition of Rhode Island (HCRI)

The Healthcare Coalition of Rhode Island (HCRI), co-chaired by the Rhode Island Department of Health (RIDOH) and the Hospital Association of Rhode Island (HARI), and their partners work together to strengthen and enhance the capabilities of R.I.'s public health and healthcare systems to respond to evolving threats and other emergencies.

HCRI strives to execute effective responses that can prevent or reduce morbidity and mortality from public health incidents whose scale, rapid onset, or unpredictability stresses the public health and healthcare systems; and ensure the earliest possible recovery and return of the public health and healthcare systems to pre-incident levels or improved functioning. HCRI serves as the 24/7/365 support/response entity for R.I.'s entire healthcare system. Members include all hospitals, health centers, nursing homes, and assisted living communities in R.I. Emergency Management Agencies, Emergency Medical Services (EMS), the Rhode Island Blood Center, and numerous other partners are also engaged. During an emergency, including a cyber event, the co-chairs of HCRI will work with impacted facilities to respond to the consequences of the event and to ensure information sharing across the healthcare sector.

Contact 1: Joseph Reppucci, Healthcare Preparedness Program Coordinator, Center for Emergency Preparedness and Response, HCRI co-chair

Tel: 401-222-4787, email: joseph.reppucci@health.ri.gov

Contact 2: Dawn Lewis, Healthcare Emergency Preparedness Coordinator, Hospital Association of Rhode Island (HCRI co-chair)

Tel: 401-443-2367, email: dawnl@hari.org

Rhode Island Office of the Attorney General

The Rhode Island General Law §11-49.3-4 states that any agency or business, whether Rhode Island-based or not, must notify residents of Rhode Island whose information or identities may have been compromised by a security breach in the most expedient time possible, but no later than 45 calendar days after confirmation of the breach. In an incident in which more than 500 Rhode Island residents may be affected, the Department of Attorney General must be notified as well. In instances in which individuals' health insurance and/or health records are compromised, please inform, as soon as possible, both the Health Care Advocate and the Insurance Advocate within the Department of Attorney General.

Reports should be made by calling 401-274-4400 or email at consumers@riag.ri.gov.

United States Attorney's Office for the District of Rhode Island

The United States Attorney's Office for the District of Rhode Island (USAO) has the primary responsibility for investigating and prosecuting all manner of cybercrime, including violations of the Computer Fraud and Abuse Act (18 U.S.C. sec. 1030), which criminalizes various forms of computer hacking and other cyber intrusions. The USAO works with federal cyber investigators from all law enforcement agencies, including the Federal Bureau of Investigation, Homeland Security Investigations, and the U.S. Secret Service. The USAO also partners with the Rhode Island State Police and the Rhode Island Office of Attorney General to coordinate investigations. The USAO is committed to working with private sector businesses to vigorously pursue cyber criminals in a balanced fashion, with a sensitivity for the needs of victimized businesses.

Contact: William Ferland, Assistant U.S. Attorney, Criminal Chief

Tel: 401-709-5084, email: William.Ferland@usdoj.gov

U.S. Secret Service

The U.S. Secret Service maintains Electronic Crimes Task Forces, which focus on identifying and locating international cyber criminals connected to cyber intrusions, bank fraud, data breaches, and other computer-related crimes. The Secret Service also runs the National Computer Forensic Institute, which provides law enforcement officers, prosecutors, and judges with cyber training and information to combat cyber crime.

Contact: Ted Arruda, Resident Agent in Charge (RAC) – Providence Office

Tel: 401-331-6452, email: ted.arruda@usss.dhs.gov

Federal Bureau of Investigation (FBI)

The FBI leads the national effort to investigate high-tech crimes, including cyber-based terrorism and espionage, computer and network intrusions, and major cyber fraud and identify theft. They also gather and share information and intelligence with public and private sector partners worldwide.

The Boston Division oversees operations in Massachusetts, Maine, New Hampshire, and Rhode Island.

Contact: FBI Boston Division, Tel: 617-742-5533, email: Boston@ic.fbi.gov

FBI Providence, Rhode Island Resident Agency, Tel: 401-272-8310

United States Computer Emergency Readiness Team (US CERT)

www.us-cert.gov

The team is charged with providing response support and defense against cyber-attacks for the Federal Civil Executive Branch (.gov) and information sharing and collaboration with state and local government, industry and international partners. US-CERT interacts with federal agencies, industry, the research community, state and local governments, and others to disseminate reasoned and actionable cybersecurity information to the public.

National Healthcare & Public Health Critical Infrastructure Resilience (NH-ISAC)

www.nhisac.org

Consists of a network of computer security incident response teams that work together to deal with computer security problems and their prevention, enabling incident response teams to more effectively respond to security incidents.

InfraGard

www.infragard.org

InfraGard is a public-private partnership between the FBI and the private sector. It is an association of individuals that facilitates information sharing and intelligence between businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to prevent and respond to computer security problems.

ISACA

www.isaca.org

ISACA's mission is to support enterprise objectives throughout the development, provision and promotion of research, standards, competencies and practices for the effective governance, control and assurance of information systems and technology.

Endonotes

[1] Francesca Spidalieri, "Pell Center Hosts Cybersecurity and Healthcare Exercise Ahead of Real-Life Global Cyber Attack," Pell Center, June 14, 2017, http://pellcenter.org/pell-center-cybersecurity-healthcare-exercise/.

[2] Healthcare Industry Cybersecurity Task Force, "Report on Improving Cybersecurity in the Healthcare Industry," June 2017, https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf.

[3] U.S. Department of Health and Human Services – Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf and "Largest Healthcare Data Breaches of 2016," HIPPA Journal, January 4, 2017, https://www.hipaajournal.com/largest-healthcare-data-breaches-of-2016-8631/.

[4] "Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data," Ponemon Institute LLC, May 2016, https://www.ponemon.org/local/upload/file/Sixth%20Annual%20Patient%20Privacy%20%26%20Data%20Security%20Report%20FINAL%206.pdf.

[5] Christiaan Beek, et al., "Health Warning – Cyberattacks are targeting the health care industry," McAfee Labs, September 2017, https://www.mcafee.com/us/resources/reports/rp-health-warning.pdf.

[6] "Health Insurance Portability and Accountability Act of 1996," https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf.

[7] International Organization for Standardization, "IEC 80001-1:2012 Application of risk management for IT-networks incorporating medical devices – Part 1: Roles, responsibilities and activities," (2016) https://www.iso.org/standard/44863.html.

[8] International Organization for Standardization, "IEC/TR 80001-2-2:2012 Application of risk management for IT-networks incorporating medical devices – Part 2-2: Guidance for the communication of medical device security needs, risks and controls," (2012) https://www.iso.org/standard/57939.html.

[9] For more on the Health Information Trust Alliance (HITRUST) Common Security Framework (CSF), see: https://hitrustalliance.net/understanding-leveraging-csf/.

[10] "A Framework for Improving Critical Infrastructure Cybersecurity," National Institute for Standards and Technology (February 2014), http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm.

[11] Francesca Spidalieri, "Understanding Cyber Threats: Lessons for the Boardroom," Pell Center, (September 2016): 4, http://pellcenter.org/wp-content/uploads/2016/09/Understanding-Cyber-Threats-Lessons-for-the-Boardroom.pdf.

[12] Healthcare Industry Cybersecurity Task Force, "Report on Improving Cybersecurity in the Healthcare Industry," 40, https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf.

[13] Department of Homeland Security, "Stop.Think.Connect." https://www.dhs.gov/stopthinkconnect, and Federal Trade Commission, "OnGuard Online," https://www.consumer.ftc.gov/features/feature-0038-onguardonline.

[14] For more information on the Pell Center's Rhode Island Corporate Cybersecurity Initiative (RICCI), see: http://pellcenter.org/rhode-island-corporate-cybersecurity-initiative/.

[15] Identity Theft Resource Center, http://www.idtheftcenter.org/.

[16] "Rhode Island Identity Theft Protection Act of 2015," http://webserver.rilin.state.ri.us/BillText/BillText15/SenateText15/S0134B.pdf.

[17] "National Institute of Standards and Technology (NIST) Cybersecurity Framework", https://www.nist.gov/cyberframework.

PELL CENTER
for INTERNATIONAL RELATIONS
and PUBLIC POLICY

About the Pell Center

The Pell Center for International Relations and Public Policy at Salve Regina University is a multi-disciplinary research center focused at the intersection of politics, policies, and ideas. Dedicated to honoring Senator Claiborne Pell's legacy, the Pell Center promotes American engagement in the world, effective government at home, and civic particpation by all Americans.

www.pellcenter.org