Hospital Cybersecurity:

Evolving Threats Require New Approaches

An Information Brief

October 2016

Craig P. Tanio, M.D., MBA, Chair
Ben Steffen, Executive Director

Maryland Health Care Commission

This page intentionally left blank

MARYLAND HEALTH CARE COMMISSION

Commissioners

Craig P. Tanio, MD, MBA, Chair
CEO and Founder, Rezilir Health

Frances B. Phillips, RN, MHA, Vice Chair
Health Care Consultant

John E. Fleig, Jr.
Chief Operating Officer
UnitedHealthcare
MidAtlantic Health Plan

Elizabeth A. Hafey, Esq.
Associate
Miles & Stockbridge P.C.

Jeffrey Metz, MBA, LNHA
President and Administrator
Egle Nursing and Rehab Center

Robert Emmet Moffit, PhD
Senior Fellow
Health Policy Studies
Heritage Foundation

Gerard S. O'Connor, MD
General Surgeon in Private Practice

Michael J. O'Grady, PhD
Principal, Health Policy LLC, and
Senior Fellow, National Opinion Research Center (NORC) at the University of Chicago

Andrew N. Pollak, MD
Professor and Chair
Department of Orthopaedics
University of Maryland School of Medicine
Chief of Orthopaedics
University of Maryland Medical System

Randolph S. Sergent, Esq.
Vice President and Deputy General Counsel
CareFirst BlueCross BlueShield

Diane Stollenwerk, MPP
President
StollenWerks, Inc.

Stephen B. Thomas, PhD
Professor of Health Services Administration
School of Public Health
Director, Maryland Center for Health Equity
University of Maryland, College Park

Cassandra Tomarchio
Business Operations Manager
Enterprise Information Systems Directorate
US Army Communications Electronics Command

Adam J. Weinstein, MD
Medical Director
Nephrology and Transplant Services
Shore Health System

Maureen Carr-York, Esq.
Public Health Nurse and Health Care Attorney
Anne Arundel County

Table of Contents

This information brief was completed by Nikki Majewski, Program Manager, within the Center for Health Information Technology & Innovative Care Delivery under the direction of the Center Director, David Sharp, Ph.D. For information on this brief, please contact Nikki Majewski at 410-764-3839 or by email at nicole.majewski@maryland.gov .

Overview

Cyber-attacks against health care organizations are growing increasingly frequent and complex.[1, 2] Criminals who once targeted retailers and financial firms are now going after medical records. Medical records, which typically contain patient Social Security numbers, addresses, insurance identification numbers, and other medical information, can sell on the black market for as much as 20 times the cost of a stolen credit card number.[3, 4] The threat of cyber-attacks has grown as health care organizations become increasingly dependent on electronic systems to manage patient medical records and perform billing and other administrative functions. Hospitals are just one of many health care organizations that are prime targets for cyber-attacks. Hospitals cannot afford to be paralyzed from a cyber-attack for too long as they provide critical health care services and often have a greater reliance on electronic systems to coordinate care delivery.

The transition from paper-based records to electronic health records (EHRs) places patient information at greater risk of intrusion. The health care industry is not as resilient to cyber-attacks as compared to other sectors.[5] The impact of a cyber-attack can be catastrophic for a hospital in terms of the loss of sensitive or proprietary information, disruption to regular operations, financial losses incurred to restore systems and files, and the potential harm to an organization's reputation.[6] The impact to patients can be just as harmful, impeding the safe and timely delivery of their care and diminishing trust once their privacy is compromised. Nationally, cyber-attacks in health care are estimated to have increased by 125 percent since 2010 and are now considered the leading cause of data breaches.[7] As of June 2016, about 41 percent of breaches were the result of hacking.[8] The surge in cyber-attacks has put pressure on hospitals to refine their cybersecurity strategies.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)[9] requires the regular review of administrative, physical, and technical safeguards for protected health information. Hospitals conduct security risk assessments to understand their vulnerability to threats and identify

---

[1] Ponemon Institute, *The State of Cybersecurity in Healthcare Organizations in 2016*, February 2016. Available at: cdn2.esetstatic.com/eset/US/resources/docs/white-papers/State_of_Healthcare_Cybersecurity_Study.pdf.

[2] Cyber-attacks can be referred to as criminal-attacks and consist of deliberate attempts to gain unauthorized access to sensitive or proprietary information, usually through a computer system or network.

[3] Bloomberg Technology, *Rising Cyber Attacks Costing Health System $6 Billion Annually*, May 2015. Available at: www.bloomberg.com/news/articles/2015-05-07/rising-cyber-attacks-costing-health-system-6-billion-annually.

[4] A medical record sells for about $50 as compared to credit card information that sells for about $1. Among other things, criminals use medical records to fraudulently bill insurance; use patients' identities for free consultations; or pose as patients to obtain prescription medications that can later be sold on the street.

[5] FBI Cyber Division, *Private Industry Notification*, April 2014. Available at: www.aha.org/content/14/140408--fbipin-healthsyscyberintrud.pdf.

[6] Department of Homeland Security, *Ransomware and Recent Variants*, March 2016. Available at: www.us-cert.gov/ncas/alerts/TA16-091A.

[7] Ponemon Institute, *Criminal Attacks Are Now Leading Cause of Data Breach in Healthcare, According to New Ponemon Study*, May 2015. Available at: www.ponemon.org/news-2/66.

[8] The remaining breaches account for insider threats and errors (41 percent) and theft or loss of paper copies of patient protected health information (PHI) or devices containing electronic PHI (17 percent).
HIPAA Journal, *Major 2016 Healthcare Data Breaches: Mid Year Summary*, July 2016. Available at: www.hipaajournal.com/major-2016-healthcare-data-breaches-mid-year-summary-3499/.

[9] Pub. L. 104-191, Aug. 21, 1996, 110 Stat. 1936.

ways to mitigate risks and potentially prevent data breaches or other adverse security events. These assessments identify and prioritize critical cyber assets, which inform the development of strategies for protecting those assets across the enterprise. Critical cyber assets generally consist of electronic devices and communication networks, including hardware, software, and data that are essential to clinical and operational information systems.[10, 11] Hospitals' ability to plan, design, and implement effective cybersecurity controls is critical in preparing for and managing emerging threats.[12]

About the Assessment

The Maryland Health Care Commission (MHCC) conducted a Cybersecurity Assessment (assessment) of Maryland acute care hospitals (hospitals) in the spring of 2016 inquiring about their efforts in preparing for and managing cyber risks. All 48 hospitals in the State contributed to the assessment. This information brief details key findings from the assessment.

Limitations

Hospital Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) self-reported data used in this assessment. The MHCC did not audit the data for accuracy. Interpretation of the survey questions may vary among CIOs and CISOs, which could influence survey findings.

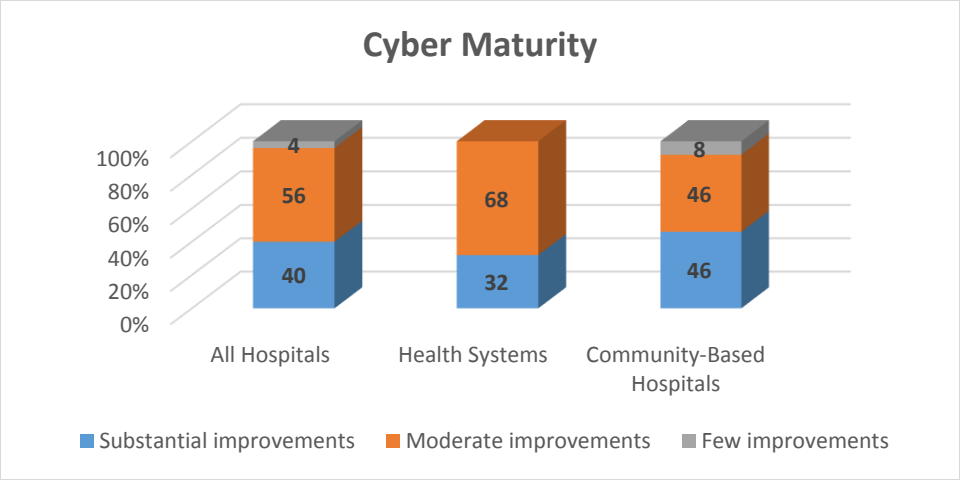
Key Findings

Presented below in aggregate are key findings from the hospital cybersecurity assessment. Note: Acute care hospitals (N=48); health systems (N=22); and community-based hospitals (N=26).

Cyber Maturity

Cyber maturity is generally viewed as a hospital's ability to protect critical cyber assets and adequately detect and respond to a cyber incident. An increase in cyber threats is propelling hospitals to evaluate and refine their cybersecurity programs[13] to improve how they manage cyber risks.[14, 15] Almost all hospitals in the State report making at least moderate improvements to their cybersecurity programs over the past two years. While health systems are generally viewed as having more resources to deploy robust strategies, nearly one half of community-based hospitals report making substantial improvements within the last two years.

[10] Examples of critical cyber assets include, but are not limited to, systems that contain electronic protected health information and financial transactions, mobile devices, and devices that infuse medicine.
[11] A variety of information systems deployed by hospitals support specific departmental needs (e.g., clinical, finance, laboratory, pharmacy, etc.).
[12] Ibid., 7.
[13] A cybersecurity program is a shared responsibility and requires a wide-ranging view of people, processes, and technologies to understand areas of vulnerability and identify and prioritize areas for remediation.
[14] University of Illinois at Chicago, *Healthcare Cybersecurity: Plan must be Enacted*, Accessed August 2016. Available at: healthinformatics.uic.edu/resources/articles/health-informatics-security/.
[15] See Appendix A for information on cybersecurity controls implemented by hospitals.



Cybersecurity Readiness

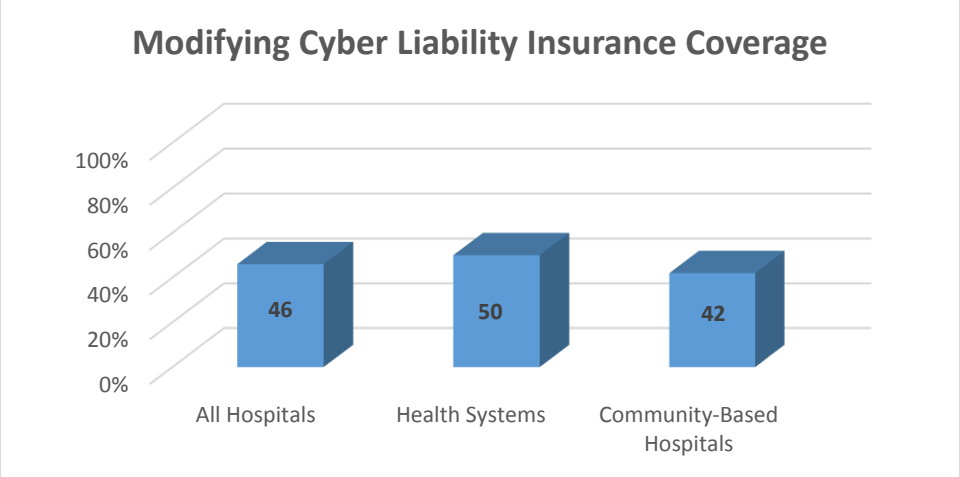
Hospitals deploy a variety of activities to assess risks, which enables them to uncover potential weaknesses in their security policies, processes and systems. This allows hospitals to plan appropriate cyber response and recovery protocols.[16] Nearly all hospitals that are part of a health system conduct more than one security risk assessment annually as compared to about a quarter of all community-based hospitals. Conducting a security risk assessment is a key component of HIPAA and required by hospitals that participate in the Centers for Medicare & Medicaid Services EHR Incentive Programs. More than half of all hospitals report modifying their emergency preparedness and incident response plans; enhancing cyber policies and procedures; and testing cyber incident response plans.

Cybersecurity Readiness			
Activity	All Hospitals	Health Systems	Community-Based
	%		
Conducting more than one security risk assessment annually	58	95	27
Modifying emergency preparedness/incident response plans to include more specific procedures for cyber incidents	69	86	54
Integrating more robust and/or new cyber incident response policies and procedures with existing disaster recovery and business continuity plans	69	82	58
Conducting mock exercises to practice and test hospital capabilities to respond timely and minimize the impact of a cyber incident	73	86	62

[16] HIPAA Journal, *Cyberattacks Simulation Exercise Tests Incident Response Readiness*, December 2015. Available at: www.hipaajournal.com/cyberattack-simulation-exercise-tests-incident-response-readiness-8204/.

Cyber Liability Insurance

Cyber liability insurance[17] is an essential part of risk management, providing protections for any costs associated with a breach, loss of data, or ransomware incident.[18] Electronic systems that create, maintain, or transmit patient data are a source of risk. In 2015, the health care industry was 21 percent more likely to experience a breach as compared to other sectors.[19] Growth in the adoption of EHR systems and interoperability has caused hospitals to reevaluate their cyber liability insurance policies. In general, hospitals weigh their preparedness for a cyber-attack against the cost of cyber liability insurance and the potential cost of a breach.[20] About half of hospitals report plans to modify their cyber liability insurance coverage. In 2015, the largest cyber liability claim nationally was filed by a health care organization in the amount of $15M. Small to mid-sized organizations[21] filed almost half (46 percent) of all claims. The cyber liability insurance market is estimated to reach $5B by 2018 and exceed $7.5B by 2020.[22]

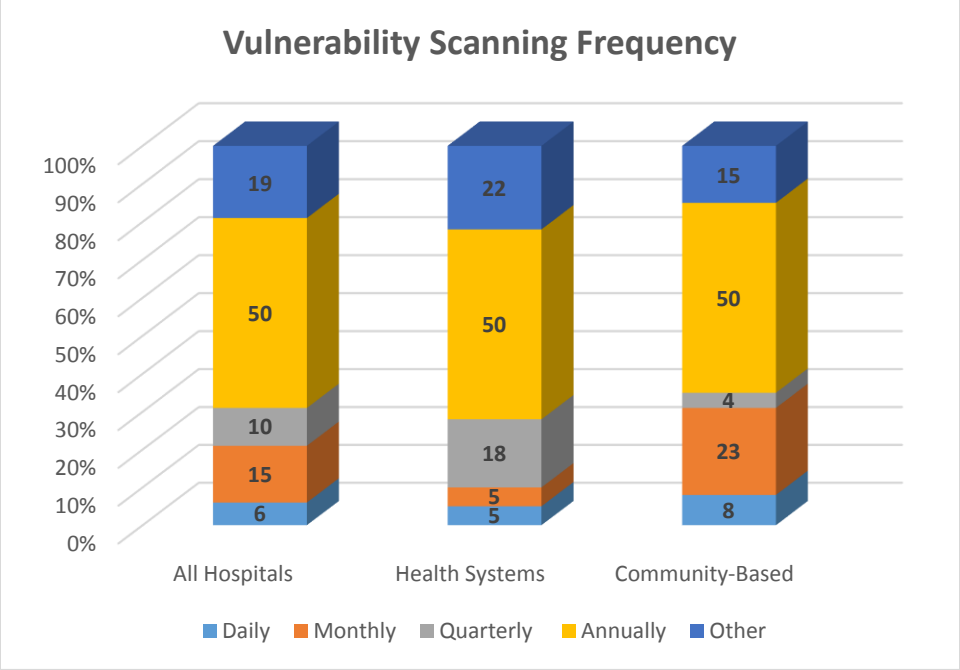


Vulnerability Scanning

Hospitals perform vulnerability scanning (scanning) with varying degrees of frequency. Scanning enables hospitals to identify security gaps in their network. In general, this process uses off-the-self

[17] Also referred to as "Cyber Risk Insurance" or "Data Breach Insurance."
[18] Cyber liability consist of two defined risks: (1) security liability––unauthorized access or use of a network, and (2) privacy liability––violation of privacy laws and regulations that permit unauthorized access to and use of sensitive information. For more information visit: beechercarlson.com/wp-content/uploads/2011/11/Healthcare-Newsletter-Cyber-Liability1.pdf.
[19] NetDiligence, *2015 Cyber Claims Study*, 2015.
[20] HIT Consultant Media, *Should Hospitals Consider Getting Cybercrime Insurance?*, May 2016. Available at: hitconsultant.net/2016/05/09/hospitals-cybercrime-insurance/.
[21] Small to mid-sized organizations are those having annual revenues under $3M.
[22] The Council of Insurance Agents & Brokers, *PwC Report: Cyber Insurance Market Will Triple By 2020*, September 2015. Available at: cyber.ciab.com/2015/09/16/pwc-report-cyber-insurance-market-will-triple-by-2020/.

software[23] to scan for known vulnerabilities[24] and then produces a report indicating the severity of the vulnerabilities found and recommended steps for remediation.[25, 26] Vulnerabilities consist of errors in software code that provide an adversary with direct access to a hospital's network.[27] Common vulnerabilities can include un-patched or out-of-date software or use of default and weak passwords, among other things. HIPAA does not explicitly require scanning; however, it is an essential step in understanding the risks posed to a health care organization.[28] Hospitals typically conduct scans on at least an annual basis. Less than a third of community-based hospitals and hospitals associated with a health system conduct scans on a monthly or quarterly basis. A few hospitals conduct scans on an ad hoc basis.

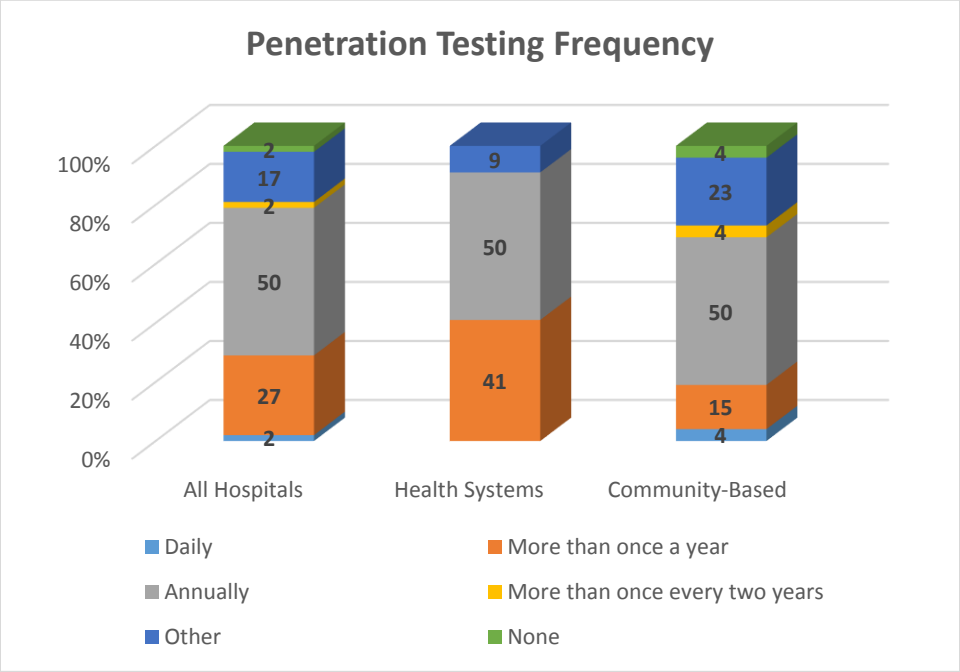


Penetration Testing

Half of hospitals perform penetration testing (or "pentesting") on an annual basis. Pentesting takes the output of scanning and attempts to exploit certain vulnerabilities found to determine if unauthorized access to a network or other malicious activity is possible. This process typically

[23] Off-the-shelf software packages include Nessus or OpenVas among others.
[24] Known vulnerabilities have been identified by the security community and software vendors (e.g., the Heartbleed bug). There are vulnerabilities unknown to the public at large and scanning software will not find them.
[25] CSO, *What's the difference between a vulnerability scan, penetration test and risk analysis?*, May 2015. Available at: www.csoonline.com/article/2921148/network-security/whats-the-difference-between-a-vulnerability-scan-penetration-test-and-a-risk-analysis.html.
[26] Scans are conducted internally (inside the network) and externally (outside the network).
[27] TechTarget, *Common Vulnerabilities and Exposures (CVE)*, April 2015. Available at: searchfinancialsecurity.techtarget.com/definition/Common-Vulnerabilities-and-Exposures.
[28] HITECH Answers, *HIPAA Q&A on Penetration Testing and Vulnerability Scanning*, September 2015. Available at: www.hitechanswers.net/hipaa-qa-on-penetration-testing-and-vulnerability-scanning.

involves mock hackers but may be performed using automated tools.[29] Frequency of pentesting depends on the risk profile of the critical assets a hospital is attempting to protect. Successful pentesting requires a hospital to make changes based on the findings, such as enhancing their security policies and procedures to prevent future exploitations of a vulnerability. Several hospitals noted plans to increase their pentesting frequency. A small number of community-based hospitals conduct pentesting more than once a year as compared to almost half of hospitals that are part of a health system.

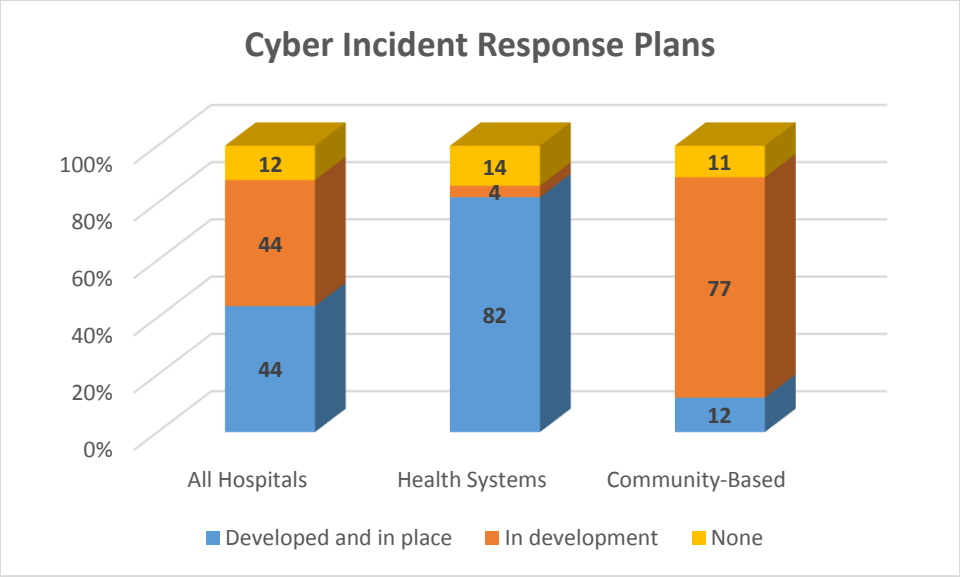


Incident Response Planning

The majority of health systems have established cyber incident response plans (CIRPs) as compared to community-based hospitals where most are under development. A CIRP is a comprehensive plan for responding to a cyber threat or attack. It can be different from a breach response plan as some incidents require rapid response to avoid a breach. Key components of a CIRP are people, processes, and technology extending beyond the IT department and including executive management, human resources, marketing, legal, and vendors with access to data, among others.[30] Included in CIRPs are escalation policies that generally extend up to the board of trustees.[31] The development of a risk profile and CIRP are complimentary activities and part of an evolving cybersecurity strategy for almost all hospitals. Many hospitals have initiatives in place to continually assess opportunities to

[29] CSO, *What's the difference between a vulnerability scan, penetration test and risk analysis?*, May 2015. Available at: www.csoonline.com/article/2921148/network-security/whats-the-difference-between-a-vulnerability-scan-penetration-test-and-a-risk-analysis.html.
[30] Grant Thornton, *Prevention and triage apply in hospital cybersecurity*, 2015. Available at: www.grantthornton.com/~/media/content-page-files/health-care/pdfs/2015/Prevention-and-triage-in-hospital-cybersecurity.ashx .
[31] American Hospital Association, *Cybersecurity and Hospitals, 2014*. Available at: www.aha.org/content/14/14cybersecuritytrustees.pdf.

improve upon incident response planning. A few hospitals report having no plans at the present time to develop a CIRP.



Employee Awareness & Education

All health systems have cybersecurity training programs in place for employees. About three-quarters of community-based hospitals have implemented formal training programs. Employee awareness and education about cybersecurity is one of the greatest defenses against a cyber-attack. Establishing a security-minded culture helps reduce the risk of a cyber-attack. Almost one-half of hospitals send reminder notices to employees about cybersecurity. A primary concern for hospitals today is the rise in ransomware, which holds hospital networks hostage in exchange for money. The most common ransomware attack starts with a phishing scam. Phishing scams are fraudulent e-mail messages appearing to come from a legitimate source that trick employees into disclosing sensitive information. Nationally, it's estimated that ransomware victims have paid $209M in ransom in Q1 2016 as compared to $25M in all of 2015.[32]

Employee Awareness and Education			
Communication Channel	All Hospitals	Health Systems	Community-Based
	%		
Requires formal training for all employees	88	100	77
Provides training to employees regarding their specific responsibility in preventing and responding to cyber-attacks	31	41	23
Distributes cyber tips via newsletters	48	41	54
Conducts campaigns designed to engage and educate employees about cyber security	75	91	62

[32] Barkly, *Ransomware by the Numbers: Must-Know Ransomware Statistics 2016*, Accessed August 2016. Available at: blog.barkly.com/ransomware-statistics-2016.

Remarks

Managing the multi-faceted complexities of cyber threats amid an increased use and reliance on technology is becoming increasingly challenging, yet remains a strategic imperative in health care. Health care organizations are not immune to these threats and with a greater reliance on technology, the potential impact of a cyber-attack increases. The disruption caused by a cyber-attack can have a significant impact on hospitals' capacity to provide patient care. A cyber-attack can also inflict losses in patient privacy and create financial hardships for hospitals. It is essential that hospitals include cybersecurity into their existing governance, risk management, and business continuity framework. Hospitals' approach to cybersecurity must remain flexible and extend beyond the technology infrastructure to include mobile devices, portable media, and medical devices. Through increased vigilance, hospitals can minimize their risks and improve their cybersecurity posture.

The Maryland Health Care Commission thanks hospital Chief Information Officers and Chief Information Security Officers for their contributions to this information brief.

Appendix A

Hospitals implement a number of tactics to help mitigate risks. Controls are security measures that can be applied across an enterprise to improve cyber defenses. Two-factor authentication is an example of one control that uses a variety of methods, including smart cards, one-time password tokens, and biometric devices, to validate a user's identify.[33] About half of Maryland hospitals have implemented two-factor authentication, consistent with hospitals nationally.[34] Other controls implemented by hospitals are detailed in the table below.

Risk Mitigation Tactics			
Control	**All Hospitals**	**Health Systems**	**Community-Based**
	%		
Security Measure for Authorized Users			
Two-factor authentication	46	59	35
Automatic logoff of system users	79	59	96
Require use of strong passwords	88	100	77
Unsuccessful log-in attempt lock-out procedures	90	100	81
Security Technologies			
Up to date firewall configurations	98	100	96
Passcodes for mobile devices	69	55	81
Encryption technologies	79	59	96
Security Protection and Detection Measures			
Internal segmentation of systems	65	45	81
Continuous patch management process that modifies policies/procedures based on previous successes and failures	67	59	73
Intrusion detection or prevention systems	90	100	81

[33] VASCO Data Security, *Two Factor Authentication and Digital Identity Management*.
[34] AIS Health, *Passwords May Never Die, but Authentication Will Keep Evolving*, May 2016. Available at: aishealth.com/archive/hipaa0516-07?utm_source=Real%20Magnet&utm_medium=Email&utm_campaign=96630934.

David Sharp, Ph.D.
Director
Center for Health Information Technology
and Innovative Care Delivery

4160 Patterson Avenue
Baltimore, MD 21215
410-764-3460
www.mhcc.maryland.gov