Cyber Security Panel Discussion

Dee Cantrell
US Retina CIO
dcantrell@usretina.com

Ransomware Attack Forces Michigan Practice to Close its Doors

DATA BREACHES APRIL 4, 2019

Report: Cyber Attackers Could Add Fake Cancerous Nodules to Medical Imaging Scans

CYBERSECURITY APRIL 4, 2019

UCLA Health Reaches Settlement over Massive 2015 Data Breach

The agreement includes free credit monitoring, $2 million to reimburse settlement class members, and $5.5 million for a cybersecurity enhancement fund

DATA BREACHES MAR 22, 2019

LabCorp Hit by Same Breach as Quest; 19M Patient Records Exposed in Total

Lab test results were not exposed in either breach, though other personal information m have been

CYBERSECURITY JUNE 6, 2019

Premera Reaches Proposed $74M Settlement for 2014 Data Breach

The insurer has agreed to guarantee a minimum of $42 million in funding for its information security program over the next three years

DATA BREACHES JUNE 5, 2019

Nearly 12M Patients Potentially Affected in Quest Diagnostics Data Breach

A third-party billings collections vendor is the specific company that was breached

CYBERSECURITY JUNE 3, 2019

Baystate Health Hit with Class-Action Lawsuit Following Phishing Attack

DATA BREACHES APRIL 26, 2019

UConn Health Falls Victim to Phishing Attack

The Farmington, Conn.-based University of Connecticut Health is acknowledging a data breach in which officials say an unauthorized third party illegally accessed employee email accounts.On Dec. 24, 2018, officials from the academic medical center...

DATA BREACHES FEB 26, 2019

UCLA Health Reaches Settlement over Massive 2015 Data Breach

The agreement includes free credit monitoring, $2 million to reimburse settlement class members, and $5.5 million for a cybersecurity enhancement fund

DATA BREACHES MAR 22, 2019

Chicago's Rush Health System Reaches Out to Patients Following Data Breach

Chicago's Rush Health System is responding to a data breach that was revealed this week, explaining to its patients what happened

DATA BREACHES MARCH 5, 2019

Current State

* Verizon 2019 Data Breach Investigations Report,
  * Second year in a row the healthcare market is the only industry to show a greater number of insider attacks (59 percent) than external (42 percent).
  * Trend to share and store information within cloud-based solutions is exposing additional security risks.
  * Has been a shift toward compromise of cloud-based email accounts via the use of stolen credentials.
  * Publishing/misconfiguration errors in the cloud are increasing year-over-year.

https://enterprise.verizon.com/resources/reports/dbir/

Current State

* Protenus Breach Barometer for the third quarter of 2018 reported
  * 4.4million patient records compromised in 117 health data breaches.
  * Average cost of a healthcare data breach is $408 per record
  * Highest cost of any industry for eight straight years.
  * Cost is almost triple the cross-industry average of $148 per record

https://www.protenus.com/2019-breach-barometer

Current State

* Carbon Black's survey of healthcare CISOs
  * 83% report seeing attacks increase with the attacks getting more sophisticated
  * Increased adoption of medical and IoT devices has created even larger surface area for attacks
  * Limited cybersecurity staffing and stagnant cybersecurity budget increases challenges

https://www.hcinnovationgroup.com/cybersecurity/news/21085047/cyberattacks-on-healthcare-institutions-continue-to-increase-survey-finds

Current State

* Cynergistek 2019 Report - took a deeper look into the 5 Core Functions of the NIST framework—identify, protect, detect, respond, and recover.
  * 74% of unauthorized insider access to patient records was users' household members; second most common was accessing high profile (VIP/confidential) patient data.
  * Over 60% privacy assessments found gaps in maintaining written policies/procedures
  * Most common gaps among third-party vendors included risk assessment, access management, and governance.
  * The average rating for the "respond and recover" function was 2.5 (on a scale of 0 to 5), indicating the healthcare industry is still not as prepared to respond to a cyber incident as should be.

https://insights.cynergistek.com/reports/2019-healthcare-cybersecurity-privacy-report

Shifting Focus

* Regulatory compliance and Security are not one-in-the-same.
* After 14 years, healthcare is achieving 72% compliance on the HIPAA Security Rule, a C-level grade at best.
* From a technical security perspective, the rule is no longer as relevant - it is about checking boxes for compliance – this is NOT a measure of risk posture or actual security.
* Growing need for healthcare organizations to make serious investments in cybersecurity readiness
* Incidents will occur no matter how well you prepare.
* More important focus is the ability to respond and recover.

https://insights.cynergistek.com/reports/2019-healthcare-cybersecurity-privacy-report

NIST Framework Core Functions

ID

Protect

Detect

Recover

Respond

NIST - the cybersecurity framework created by the National Institute of Standards and Technology in the U.S. Department of Commerce. https://www.nist.gov/cyberframework

NIST Functions

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

https://www.nist.gov/cyberframework

Active Threats

- Form Jacking
- Crypto Jacking
- Ransomware
- Targeted Attacks
  - Supply Chain
  - Cloud Services
  - IoT
  - Phishing … Spear or otherwise
  - Destructive Malware (comprise operational systems)
  - Living off the Land

https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf

Best Practices

- The task group, called for in Section 405(d) of the Cybersecurity Act of 2015, published their recommendations at the end of 2018 in the *Health Industry Cybersecurity Practices (HICP) - Managing Threats and Protecting Patients report.*
- HICP lists 10 overarching cybersecurity practices that the task group determined organizations of all sizes, from local clinics to large healthcare systems, should follow:
  - email protection systems
  - endpoint protection systems
  - access management
  - data protection and loss prevention
  - network management
  - vulnerability management
  - incident response
  - medical device security
  - cybersecurity policies

Recent KLAS/CHIME Report

* KLAS and CHIME recently released a white paper from their analysis of the 2018 Healthcare's Most Wired survey (600+ healthcare organizations).
  * Provides a view of the current landscape around cybersecurity practices, focusing on the HICP set of cybersecurity practices.
  * Bottom line take away – while many providers have adopted guidelines outlined in HICP, there was room for improvement, especially among smaller organizations.

How Aligned Are Provider Organizations with the Health Industry Cybersecurity Practices (HICP) Guidelines – KLAS/CHIME

Findings KLAS/CHIME Report

* Regardless of size, most organizations have deployed email and endpoint protection systems, establishing an initial layer of defense against internal and external threats.
* Many organizations are transitioning from homegrown identity and access management (IAM) solutions to commercial solutions to support their identity policies.
* Multifactor authentication (MFA) remains a gap for half of small organizations.
* Data-loss prevention (DLP) solutions have been widely adopted, though deployment of on-premises DLP solutions has slowed, as organizations have transitioned to the cloud.
* Today's security requirements are challenging historical asset management practices.
* Most organizations have network access control (NAC) solutions to monitor devices that connect to their networks; however, less than half of small organizations are using network segmentation to control the spread of infections.
* Large organizations report more sophisticated and more frequent vulnerability scanning and application testing.
* Small organizations more frequently turn to penetration testing to identify vulnerabilities.

Best Practices Guidance - Preparation

* Educate senior management about the nature, scope and severity of cyber threats; take an enterprise risk management and governance approach.
* Identify the critical assets and mission-critical needs of the organization, assess risks, establish cybersecurity priorities and determine how to manage the risks.
* Adopt risk management practices, such as the NIST Cybersecurity Framework
* Follow the HIPAA Security Rule for risk assessment and management standards which requires HIPAA covered entities and business associates to perform and update risk analysis to identify risks to the privacy, security and availability of protected health information and implement safeguards to reduce the identified risks and vulnerabilities.
* Evaluate vulnerabilities relating to the use of contractors and vendors.
* Ensure that those with incident response roles have access to the incident response plan.
* Incident response plan should be ingrained through regular exercises/practice runs.

https://www.justice.gov/criminal-ccips/file/1096971/download

Best Practices Guidance - Preparation

- Implement incident response plans with specific, up-to-date procedures to handle cyber incidents, provide direction on how to continue operating while managing an incident, and work with law enforcement and incident response firms.
- Essential issues to address in an incident response plan:
  - Who has decision-making responsibility for each incident response element
  - How to contact critical incident response personnel and, if unable to contact them, how to proceed
  - What mission-critical data, networks, assets or services warrant priority attention
  - How to contact and interact with third parties (e.g., data centers or cloud service providers) who host the organization's affected information
  - How to contact the organization's incident response firm and obtain assistance in responding
  - When and how to restore and insure the integrity of backed-up data
  - Criteria to determine who to notify, including when and how to notify law enforcement and government agencies.

https://www.justice.gov/criminal-ccips/file/1096971/download

Best Practices Guidance - Preparation

* Develop relationships with law enforcement agencies, legal counsel familiar with cyber incident management, cybersecurity firms and others who can contribute to incident response.
* Implement appropriate workplace policies to ensure that personnel are familiar with the incident response plan and help prevent cyber threats and mitigate potential damage.
* Maintain basic cybersecurity policies and procedures, including patch management programs, access controls, network segmentation, password management programs, perimeter defense (e.g., firewalls), and server logs.
* Adopt technology solutions and service arrangements for response and recovery.
* Establish procedures for lawful monitoring of systems and devices for cybersecurity threats.
* Work to keep up with cyber threats by accessing information from public and private sector organizations, such as government agencies, information sharing and analysis centers (ISACs), and information sharing and analysis organizations (ISAOs).

https://www.justice.gov/criminal-ccips/file/1096971/download

Best Practices Guidance – During and After an Incident

- Immediately assess the nature and scope of the incident
- Implement measures to minimize continuing damage
- Record and collect information
- Notify appropriate points of contact within the organization, as well as law enforcement, regulators and other victims.
- Follow these steps after a cyber incident appears to be resolved:
  - Continue to monitor the system for signs of compromise
  - Adopt measures to prevent similar attacks
  - Conduct a post-incident review of the organization's performance and assess the strengths and weaknesses of the organization's incident response plan
  - Note and discuss any deficiencies and gaps in the response and take remedial steps as needed.
  - In addition, the security incident should be analyzed to determine what notifications (if any) are required under relevant contracts and law, such as the HITECH Breach Notification Rule if protected health information (PHI) is involved, and state law.

https://www.justice.gov/criminal-ccips/file/1096971/download

Best Practices

* Recommended for Small Healthcare Entities
  * https://www.phe.gov/Preparedness/planning/405d/Documents/tech-vol1-508.pdf
* Recommended for Medium and Large Healthcare Entities
  * https://www.phe.gov/Preparedness/planning/405d/Documents/tech-vol2-508.pdf