

Western Region Conference



Healthcare Security Readiness and Maturity Assessment

Janice Ahlstrom and Ken Zoline

Your presenters



Janice Ahlstrom
DIRECTOR

35+ years experience
FHIMSS, CPHIMS, CCSFP, RN, BSN
phone: 612-876-4761
email: janice.ahlstrom@bakertilly.com



Ken Zoline
SENIOR MANAGER

35+ years experience
CISSP
phone: 312-729-8346
email: ken.zoline@bakertilly.com

Agenda

1. Overview of healthcare cybersecurity news
2. Discuss security maturity in healthcare industry
3. Share security frameworks available
4. Discuss the various security frameworks
5. Wrap up

Learning Objectives

- Understand the impact of ransomware attacks in healthcare
- Identify the reported security maturity of the healthcare industry
- Recognize available frameworks and tools to assess security maturity and compliance

What do you need to protect?

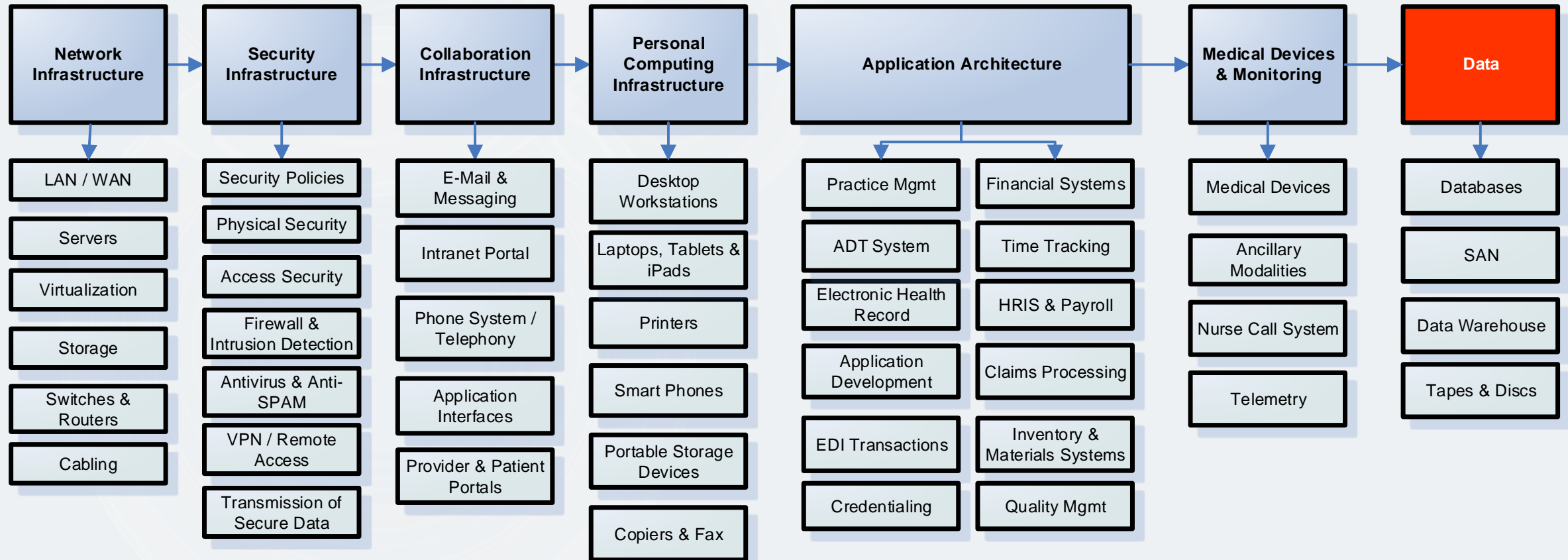
HIPAA Security Rule says: Anyone who maintains or transmits health information shall:

- Maintain reasonable and appropriate administrative, technical and physical safeguards

These safeguards are needed to:

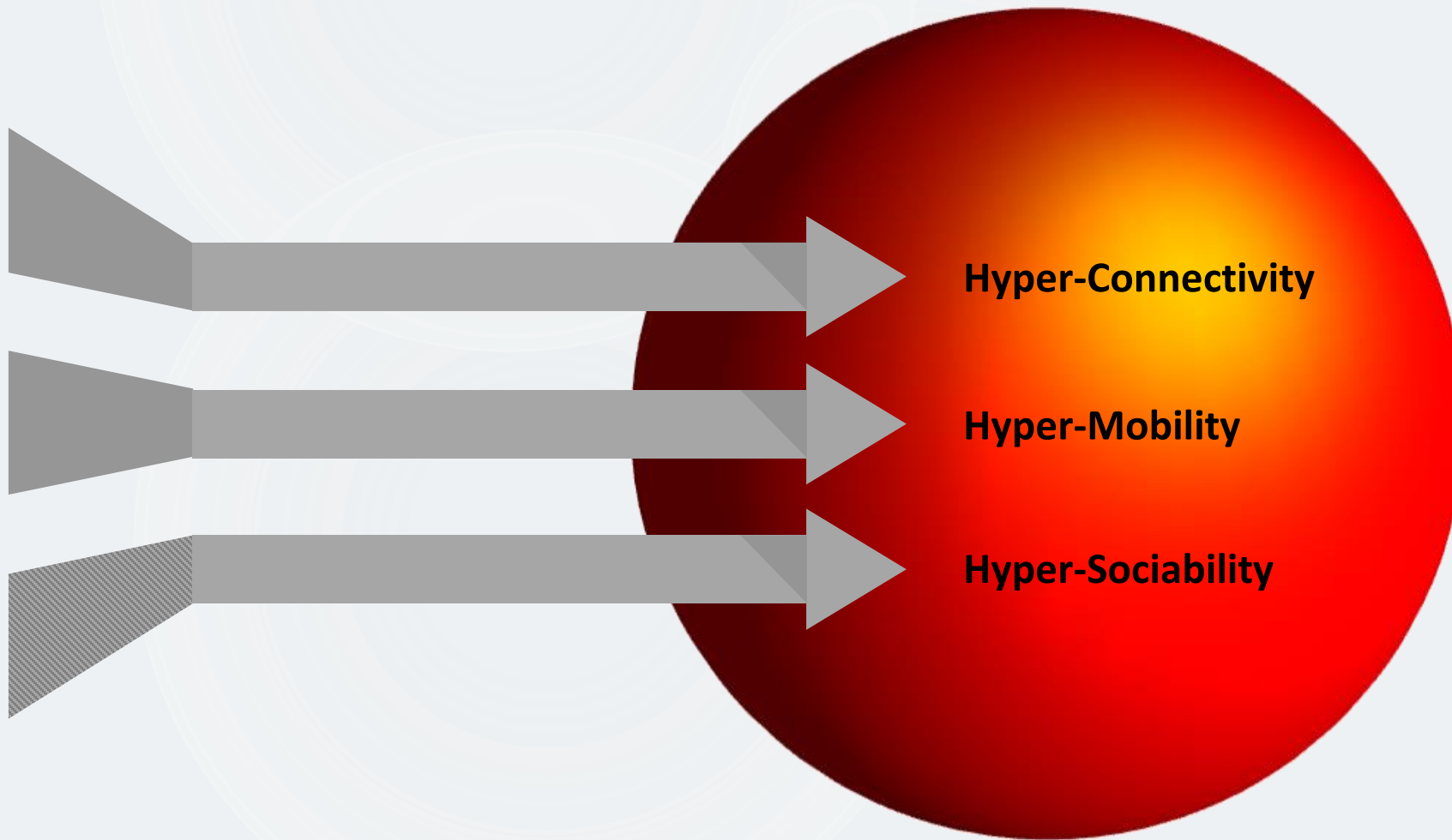
- Ensure the integrity and confidentiality of information
- Protect against any:
 - Anticipated threats
 - Hazards to the security or integrity of the information
 - Unauthorized use or disclosure of the information

What do you really need to protect?



Key risks we face

Society is highly digital...



Unintended
consequence:
A growing
attack surface
ripe for
plundering

HHS Publication of Cybersecurity Practices

- December 28, 2018 (HHS) released **voluntary** cybersecurity practices to the healthcare industry
- Goal: Provide practice guidelines to cost-effectively reduce cybersecurity risks
 - ✓ The “Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients” report
- A two year effort in response to a mandate set forth by the Cybersecurity Act of 2015 Section 405(d)
- Over 150 cybersecurity and healthcare experts and the government contributed to the publication’s development

Jan 2, 2019

Source: <https://www.phe.gov/Preparedness/planning/405d/Pages/reportandtools.aspx>

HHS Cybersecurity Practices Report

- Examines current cybersecurity threats affecting healthcare
- Identifies specific weaknesses that make organizations more vulnerable to the threats
- Provides selected practices that cybersecurity experts rank as the most effective to mitigate the threats

Jan 2, 2019

Source: HHS Healthcare Industry Cybersecurity Practices Report:

<https://www.phe.gov/Preparedness/planning/405d/Pages/reportandtools.aspx>

HHS Cybersecurity Practices Report

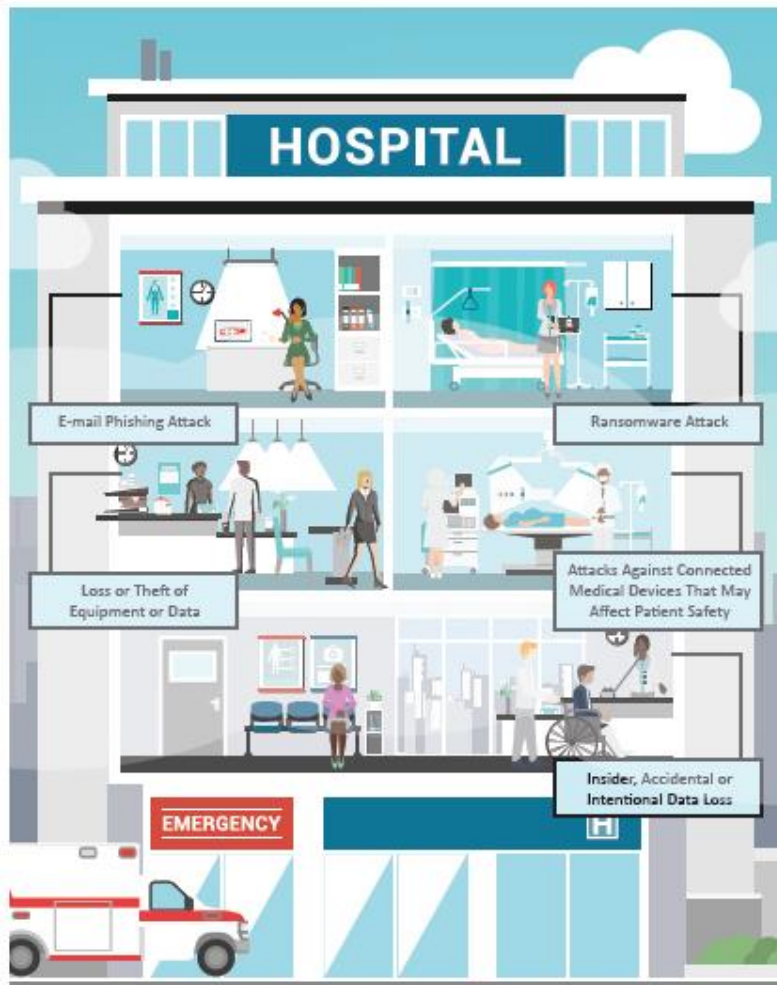
- HHS report indicates that the average breach costs a healthcare organization \$2.2 million dollars
- 4 in 5 physicians in the U.S. have experienced a cybersecurity attack
- Provides practical education regarding the management of threats and vulnerabilities

Jan 2, 2019

Source: HHS Healthcare Industry Cybersecurity Practices Report:

<https://www.phe.gov/Preparedness/planning/405d/Pages/reportandtools.aspx>

Most Common Healthcare Cyber Threats



1. Email phishing attack
2. Ransomware attack
3. Loss or theft of equipment or data
4. Attacks against connected medical devices that may affect patient safety
5. Insider attack: accidental or intentional data loss

Jan 2, 2019

Source: HHS Healthcare Industry Cybersecurity Practices Report:

<https://www.phe.gov/Preparedness/planning/405d/Pages/reportandtools.aspx>

Recent Breach

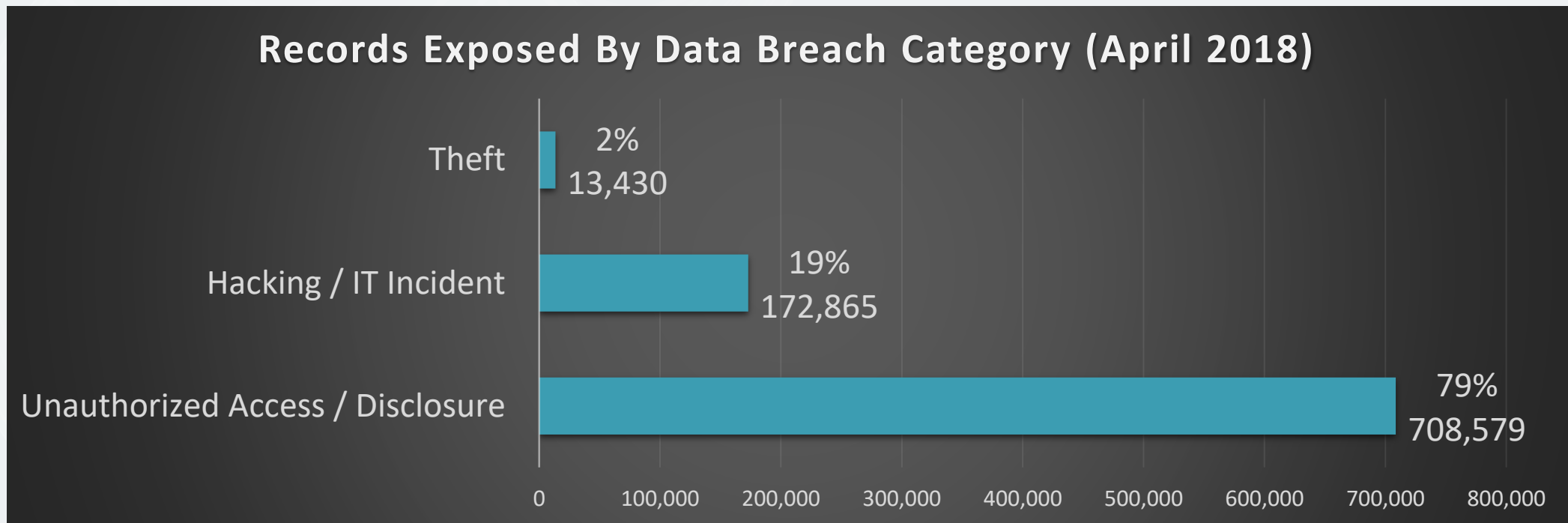
- San Diego Unified School District Data Breach (December 21, 2018)
- Personal data for more than 500,000 students and staff, including health information, may have been compromised
- The hacker gained access to staff credentials using a targeted phishing attack that used emails that appeared to be authentic, but redirected users to fake login pages where hackers collected the credentials
- Hackers had access to the network for nearly a year Jan to Nov 2018
 - ✓ Stole the data from as far back as the 2008-2009 school year
 - ✓ Discovered in October 2018

Dec 26, 2018

Source: <https://healthitsecurity.com/news/san-diego-school-distract-phishing-hack-includes-health-data>

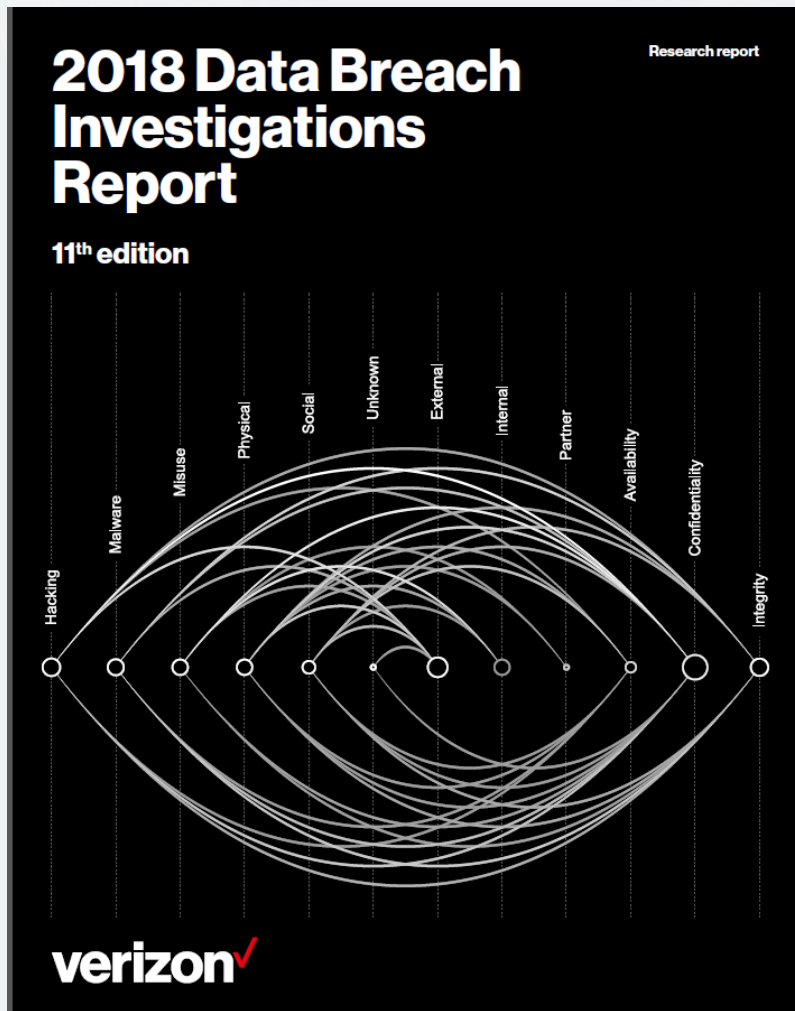
Poorly managed access and access monitoring

- 41 data breaches were reported to OCR in April 2018
 - 894,874 electronic health records were exposed or stolen



Source: May 18, 2018 <https://www.hipaajournal.com/category/healthcare-cybersecurity/>

Key risks are not well documented and managed



Who's behind the breaches?

73% perpetrated by outsiders

28% involved internal actors

2% involved partners

2% featured multiple parties

50% of breaches were carried out by organized criminal groups

12% of breaches involved actors identified as nation-state or state-affiliated

Who are the victims?

24% of breaches affected healthcare organizations

15% of breaches involved accommodation and food services

14% were breaches of public sector entities

58% of victims are categorized as small businesses

What tactics are utilized?

48% of breaches featured hacking

30% included malware

17% of breaches had errors as causal events

17% were social attacks

12% involved privilege misuse

11% of breaches involved physical actions

What are other commonalities?

49% of non-POS malware was installed via malicious email¹

76% of breaches were financially motivated

13% of breaches were motivated by the gain of strategic advantage (espionage)

68% of breaches took months or longer to discover

MediPro Survey

State of Privacy and Security Awareness Report

70% of employees in numerous industries lack awareness to stop preventable cybersecurity attacks

However, 78% of healthcare employees lack preparedness with common privacy and security threat scenarios

Feb. 6, 2018

Source:<https://healthitsecurity.com/news/78-of-healthcare-workers-lack-data-privacy-security-preparedness>

78% of Healthcare Workers Lack Data Privacy, Security Preparedness

Employee training programs are potentially lacking, with research showing healthcare workers do not have strong data privacy and security preparedness.



Polling Question

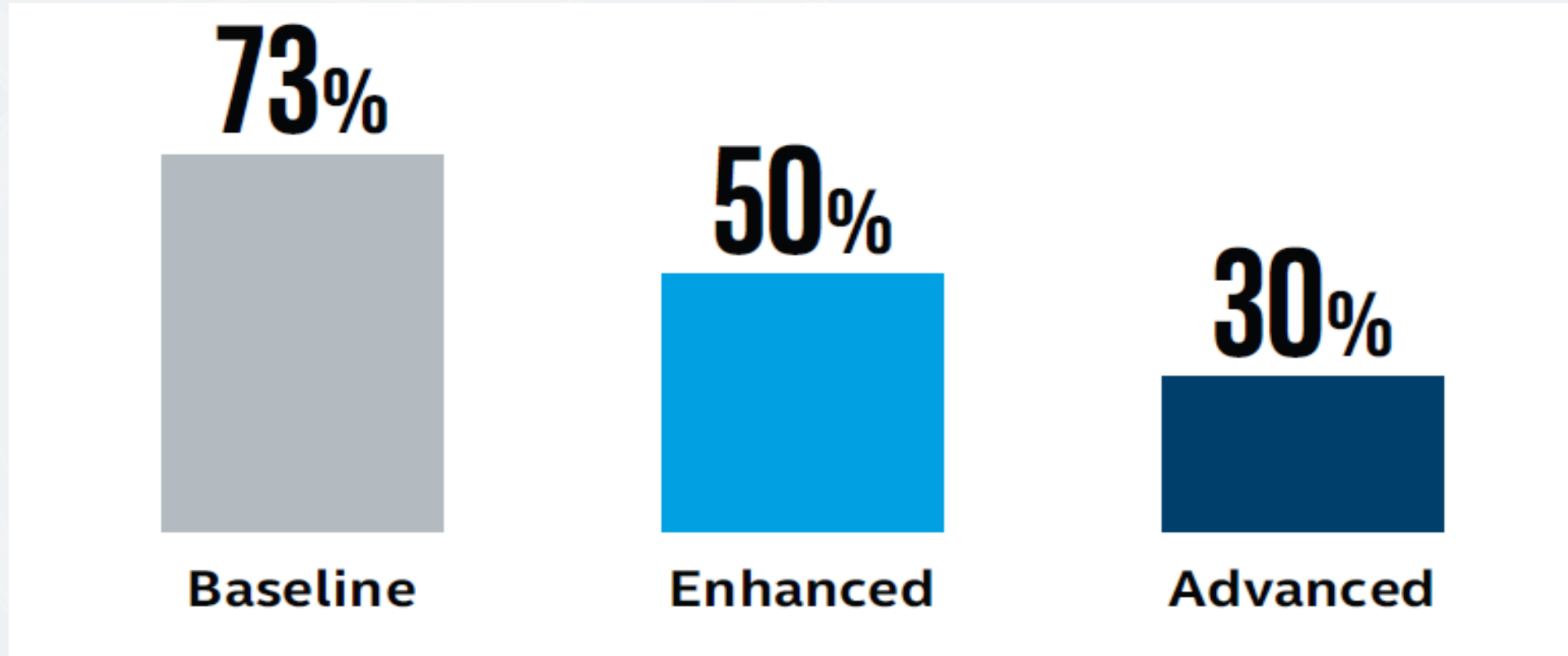
Of the nearly 900,000 health records exposed or stolen that were reported to OCR in April 2018, what was the top cause?

1. Theft
2. Hacking / IT Incident
3. Unauthorized Access / Disclosure

Security Maturity in Healthcare

Healthcare Security Maturity – Intel Study (2017)

Percent of organizations with baseline, enhanced and advanced security measures implemented



See appendix for detailed results.

Security Maturity Measurement Challenges

- How should security maturity be measured?
- What are key metrics? For example,
 1. Is a policy or standard in place?
 2. Is there a process or procedure to support the policy?
 3. Has the process or procedure been implemented?
 4. Is process or procedure being measured and tested by management to ensure effective operation?
 5. Are the measured results being managed to ensure corrective actions are taken as needed?

Security Frameworks

Security Frameworks

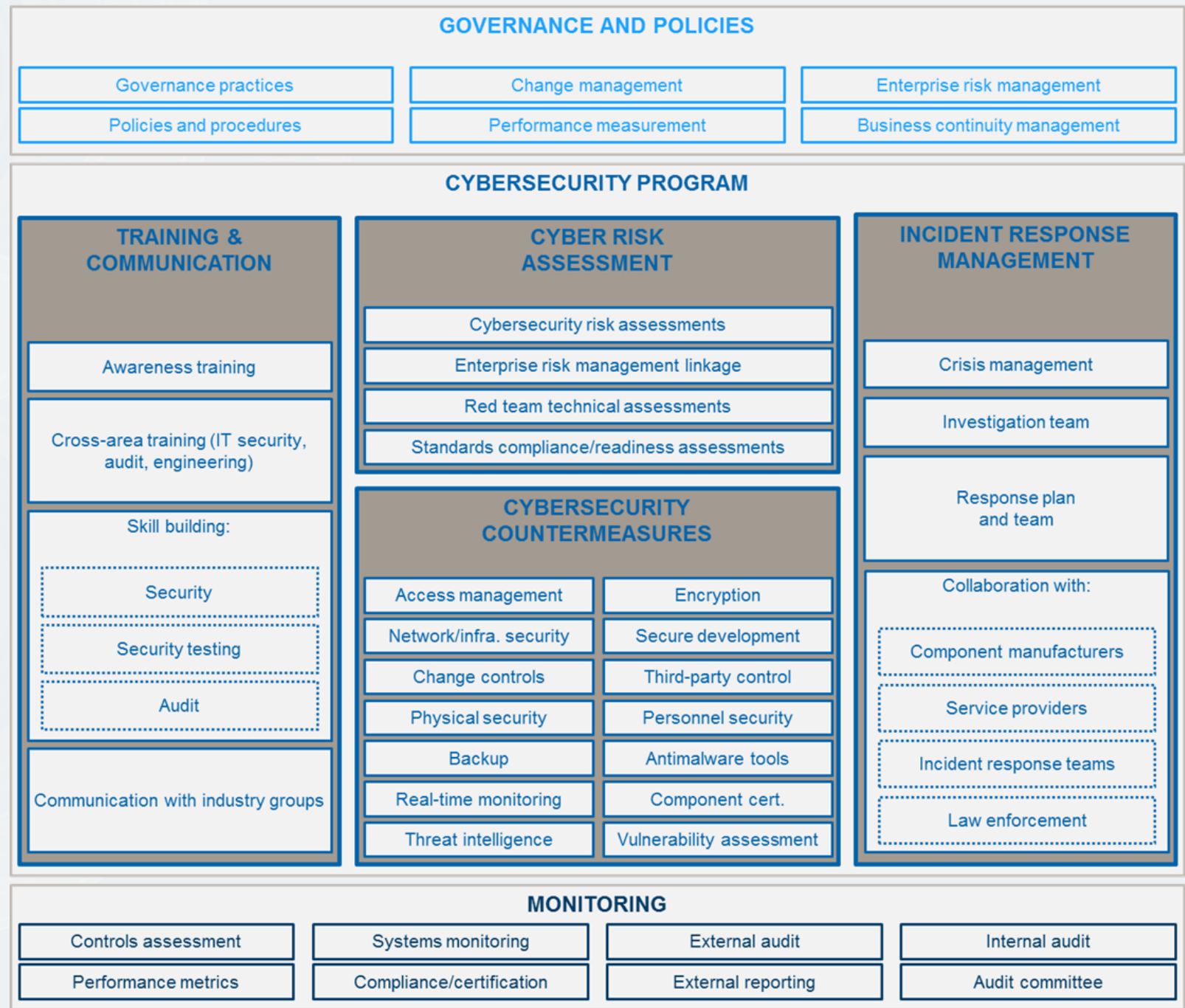
What are they?

- The essential supporting structure for enterprise (cyber)security that enables the consistent definition of policies, standards and procedures, and the implementation of supporting controls and processes

Why are they important?

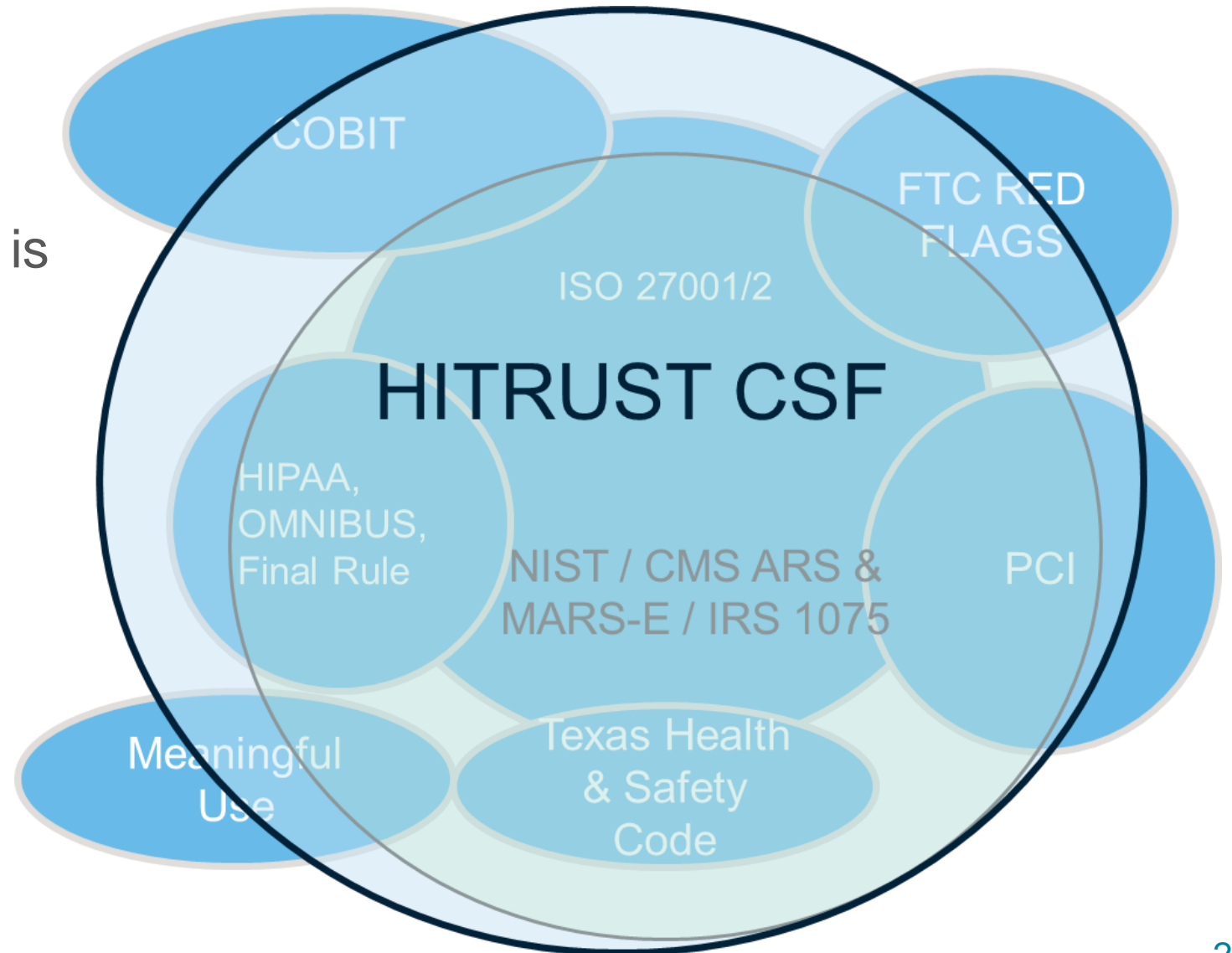
- Security frameworks strive to address the full gamut of risk areas that need to be identified and controlled
- They help an organization create their security program

Security Frameworks enable Security Programs



HITRUST Common Security Framework

- Risk based definition of what is reasonable and appropriate
- Healthcare industry focus
- Evolves as the industry changes
- Provides certification



NIST Cybersecurity Framework

- Discusses cybersecurity functions, activities and outcomes in plain English; provides informative references
- Enables organizations to do the following:
 - 1) Describe their current cybersecurity posture
 - 2) Describe their target state for cybersecurity
 - 3) Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process
 - 4) Assess progress toward the target state
 - 5) Communicate among internal and external stakeholders about cybersecurity risk

Source: <https://www.nist.gov/cyberframework>

NIST 800-53 Framework

- Security controls for federal information systems and organizations
- Documents security controls for all federal information systems, except those designed for national security
- Controls are the management, operational, and technical safeguards to protect the confidentiality, integrity, and availability of a system and its information
- Addresses security control selection for federal information systems in accordance with the security requirements in the Federal Information Processing standard (FIPS) 200

Source: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>

Center for Internet Security (CIS) Critical Security Controls (CSC) Framework

- The CIS Critical Security Controls are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks
- The framework defines a prioritized set of actions to protect organization and their data from known cyber attack vectors
- Defines basic, foundational and organizational controls to implement

Source: <https://www.cisecurity.org/controls/>

ISO 27001 and 27002

- ISO 27001 is an international specification for the establishment and operation of an information security management system (ISMS)
 - The ISMS is a framework of policies and procedures that includes legal, physical and technical controls involved in an organization's information risk management processes
- ISO 27002 provides best practice recommendations on information security controls for initiating, implementing and maintaining an ISMS

Source: <https://www.iso.org/isoiec-27001-information-security.html>

COBIT

- COBIT (Control Objectives for Information and Related Technologies) is a “good-practice” framework created by ISACA for information technology management and governance
- High level framework focused on
 - Audit and assurance
 - Risk management
 - Information security
 - Regulatory and non-regulatory compliance
 - Governance of enterprise IT

Source: <http://www.isaca.org/cobit/pages/default.aspx>

Summary

Polling Question

As you consider your organization's security program, which areas are you most concerned about?

- Governance and policies
- Training and communication
- Cyber risk assessments
- Cybersecurity counter measures
- Incident response and management
- Monitoring

Areas of a Robust Security Program

- Governance and policies
- Training and communication
- Cyber risk assessments
- Cybersecurity counter measures
- Incident response and management
- Monitoring

Cyber principles leaders should consider

- I The need to understand and approach cybersecurity is an enterprise-wide risk management issue, **not just an IT issue**
- II **Understand the legal implications** of cyber risks as they relate to an organization's specific circumstances
- III Adequate access to **cybersecurity expertise** as well as discussions about cyber-risk management should be given regular and adequate time on board meeting and executive agendas
- IV The expectation that management will establish an enterprise-wide cyber-risk management program with **adequate staffing and budget**
- V Board level discussion of cyber risk should include the identification of risk treatment options - **avoid, accept, mitigate or transfer** as well as specific plans associated with each risk treatment option




Questions

Appendix: Intel Security Maturity Study

















Healthcare Security Maturity Intel Study Baseline Measures

Source: 2017

<https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/healthcare-security-readiness-global-industry-highlights-white-paper.pdf>

KEY  Most have it  Some have it  Few have it

BASELINE




 77% Policy
 71% Risk Assessment
 59% Audit and Compliance
 70% User Awareness Training
 62% Endpoint Device Encryption
 61% Mobile Device Management
 20% Endpoint Data Loss Prevention (Discovery Mode)
 92% Anti-Malware
 81% Identity and Access Management, Single-Factor Access Control
 92% Firewall
 89% Email Gateway
 85% Web Gateway
 72% Vulnerability Management, Patching
 61% Security Incident Response Plan
 85% Secure Disposal
 89% Backup and Restore

Healthcare Security Maturity Intel Study















Enhanced Measures

Source: 2017



<https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/healthcare-security-readiness-global-industry-highlights-white-paper.pdf>

KEY  Most have it  Some have it  Few have it













ENHANCED

	53%	Device Control
	66%	Penetration Testing, Vulnerability Scanning
	29%	Client Solid State Drive (Encrypted)
	17%	Endpoint Data Loss Prevention (Prevention Mode)
	29%	Network Data Loss Prevention (Discovery Mode)
	51%	Anti-Theft: Remote Location, Lock, Wipe
	42%	Multi-Factor Authentication with Timeout
	83%	Secure Remote Administration
	15%	Policy-Based Encryption for Files and Folders
	40%	Server/Database/Backup Encryption
	67%	Network Segmentation
	61%	Network Intrusion Prevention System
	85%	Business Associate Agreements
	64%	Virtualization

Healthcare Security Maturity Intel Study Advanced Measures

KEY  Most have it  Some have it  Few have it

ADVANCED

	15%	Server Solid State Drive (Encrypted)
	20%	Network Data Loss Prevention (Prevention Mode)
	28%	Database Activity Monitoring
	41%	Digital Forensics
	40%	Security Information and Event Management
	49%	Threat Intelligence
	13%	Multi-Factor Authentication with Walk-Away Lock
	23%	Client Application Whitelisting
	19%	Server Application Whitelisting
	34%	De-Identification/Anonymization
	12%	Tokenization
	67%	Business Continuity and Disaster Recovery

Source: 2017

<https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/healthcare-security-readiness-global-industry-highlights-white-paper.pdf>