HIMSS18 The leading health information and technology conference

WHERE THE WORLD CONNECTS FOR HEALTH

Conference & Exhibition | March 5–9, 2018

Las Vegas | Venetian – Palazzo – Sands Expo Center

Cybersecurity Risk Management Strategies at a National Post-Acute Care Org.

Session 294, March 9, 2018

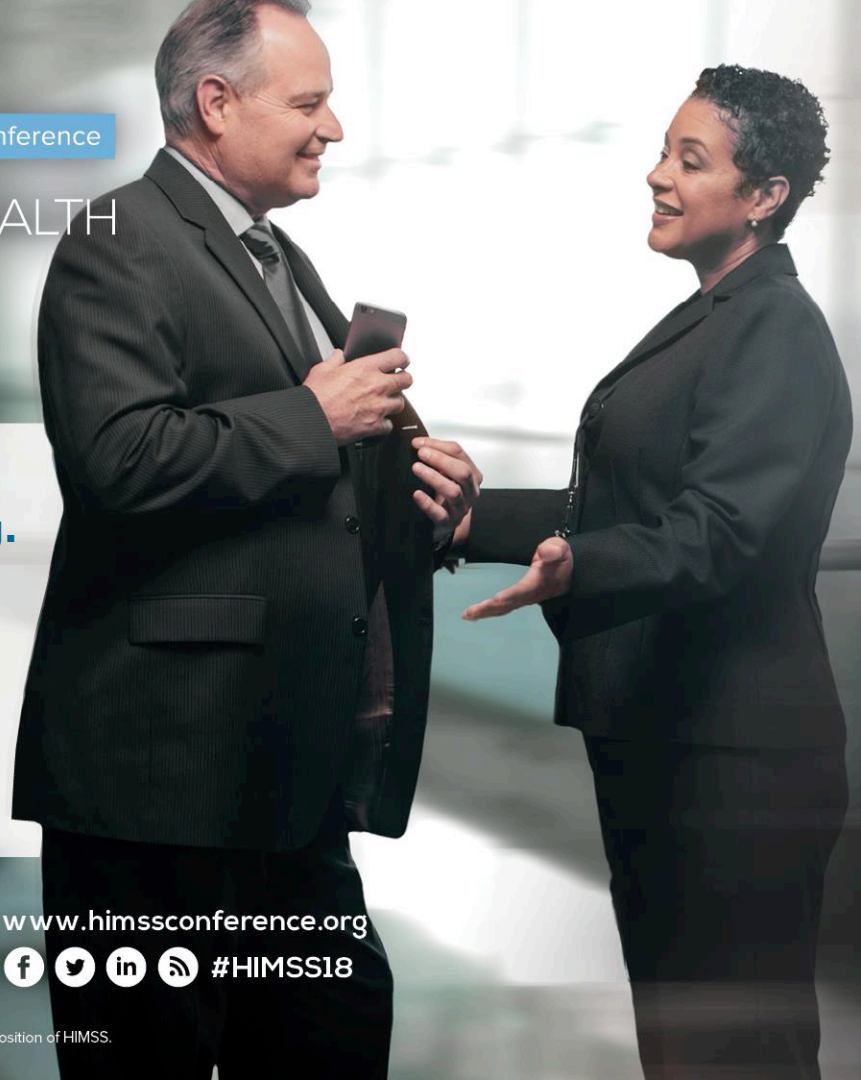
Richard Paul
VP, Information Technology
Covenant Care

Jeff Bell, CISO
CareTech Solutions

COVENANT CARE

CareTech An HTC Global Company

COMMITMENT



www.himssconference.org

#HIMSS18

Conflict of Interest

Richard Paul
BS, MBA

Has no real or apparent conflicts of interest to report.

Conflict of Interest

Jeff Bell, BS	Salary: Receives salary from CareTech Solutions

Agenda

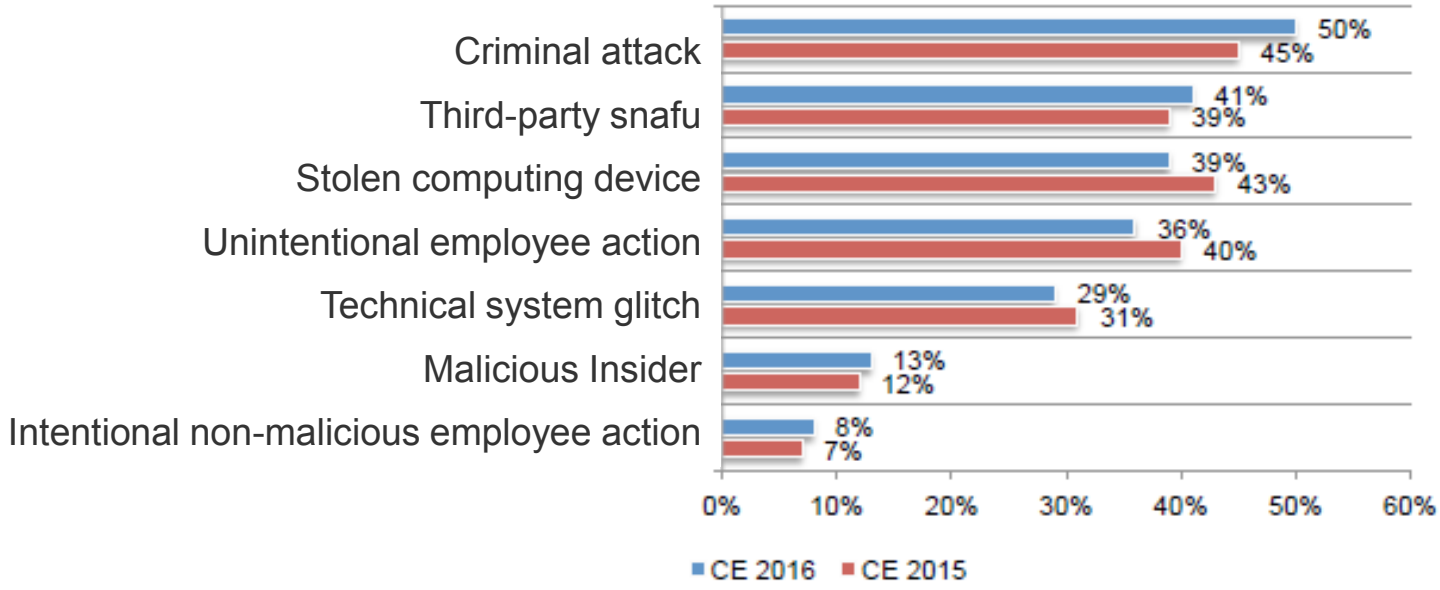
- Top Cybersecurity Threats and Risks
- Cybersecurity Risk Management Strategies
- Identity and Access Management (IAM) – an Essential Foundation
- Communication and Accountability with Vendors
- Looking Forward – Challenges and Opportunities

Learning Objectives

- Identify current healthcare privacy and cybersecurity risks
- Examine the cybersecurity and risk management needs of a national post-acute care organization
- Discuss the key benefits of utilizing a centralized approach to access management
- Describe communication strategies healthcare and outsourcing partners organizations can use to coordinate risk management efforts

Top Cybersecurity Threats and Risks

What was the root cause of the healthcare organizations' data breach?

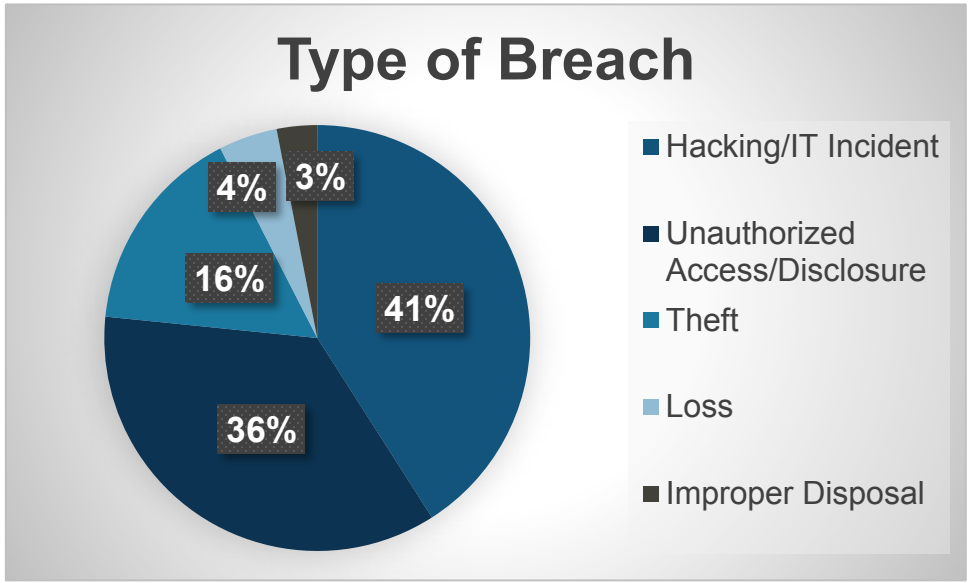


Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data, Ponemon Institute, May, 2016, Sponsored by ID Experts

Top Cybersecurity Threats and Risks

2017 PHI Breaches Reported to the OCR (over 500 records)

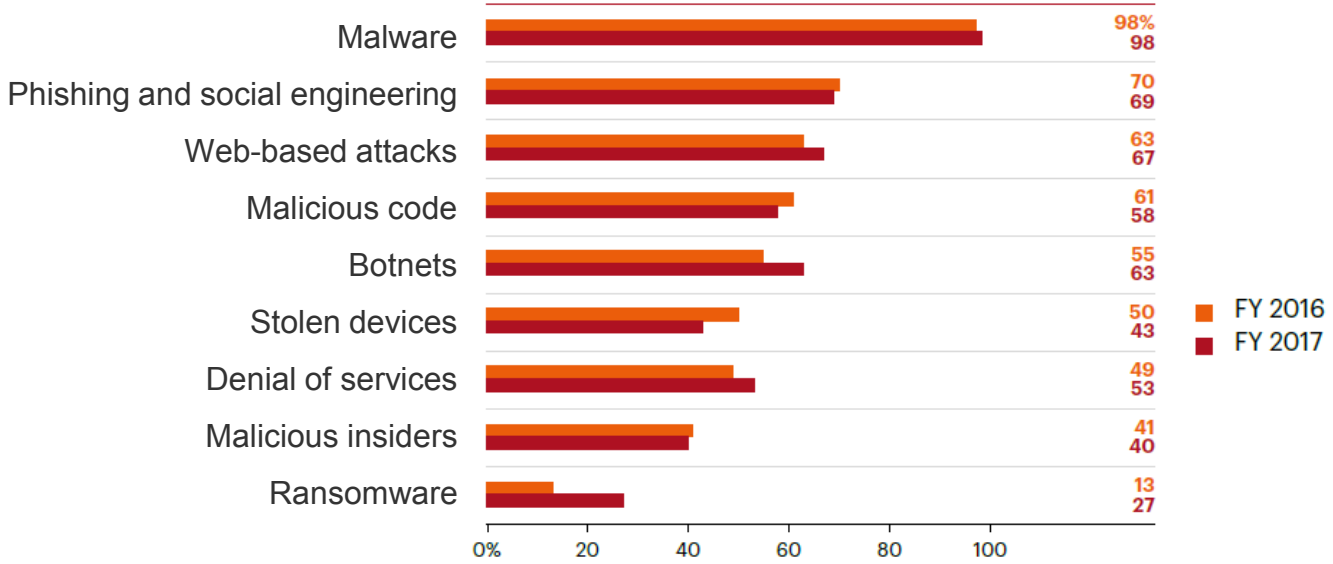
Total: 359



https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf accessed February 27, 2018

Top Cybersecurity Threats and Risks

Types of cyber attacks experienced by companies



2017 Cost of Cybercrime Study, conducted by Ponemon Institute LLC, Jointly Developed by Accenture, 2017
Field research was completed in August 2017. 254 organizations participated. Healthcare was represented in the study.

Top Cybersecurity Threats and Risks

2017 Cost of Cybercrime Study (Global, across all industries)

130	Average number of security breaches per org
$ 11.7M	Average annual cost of cybercrime per org
$ 12.5M	Average annual cost of cybercrime per healthcare org
27.4%	Percentage increase in average annual cost of cybercrime
27.0%	Percentage of orgs reporting ransomware attacks (doubled)
41.0%	Percentage of orgs reporting malicious insider attacks (stable)
$ 2.4M	Average cost of a malware attack
$ 1.06M	Average cost of a ransomware attack
$ 2.33M	Average cost of a malicious insider attack

2017 Cost of Cybercrime Study, conducted by Ponemon Institute LLC, Jointly Developed by Accenture, 2017
Field research was completed in August 2017. 254 organizations participated. Healthcare was represented in the study.

Cybersecurity Frameworks

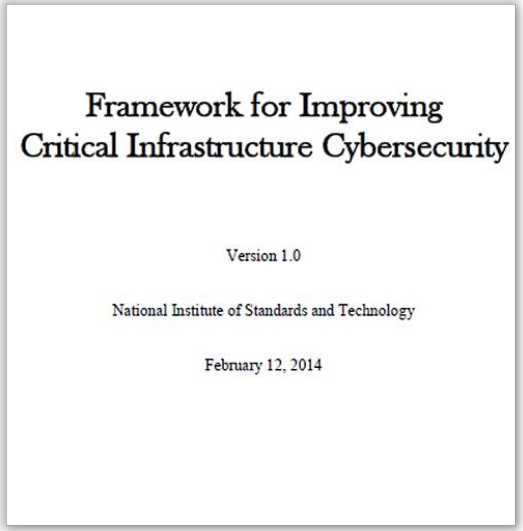
Given the level of Cybersecurity Risk how can an organization:

- Decide on an appropriate cybersecurity program?
- Assure stakeholders, regulators, customers, the public?
- Demonstrate due diligence?

Cybersecurity frameworks are descriptions of a required or recommended set of controls (security safeguards).

Third party validation can provide an additional level of assurance.

NIST Cybersecurity Framework


Framework for Improving Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology

February 12, 2014

* Version 1.1 draft was released January 10, 2017. It provides new details on how to manage cyber supply chain risks, clarifies key terms and introduces measurement methods.

Identify: Asset Management, Business Environment, Governance, Risk Assessment, Risk Management Strategy

Protect: Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures

Detect: Anomalies and Events, Security Continuous Monitoring, Detection Processes

Respond: Response Planning, Communications, Analysis, Mitigation, Improvements

Recover: Recovery Planning, Improvements, Communications

Framework Core

Function	Category	Subcategory	Informative References
PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	· **CCS CSC** 16 · **COBIT 5** DSS05.04, DSS06.03 · **ISA 62443-2-1:2009** 4.3.3.5.1 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 · **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 · **NIST SP 800-53 Rev. 4** AC-2, IA Family
		PR.AC-2: Physical access to assets is managed and protected	· **COBIT 5** DSS01.04, DSS05.05 · **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 · **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 · **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-9
		PR.AC-3: Remote access is managed	· **COBIT 5** APO13.01, DSS01.04, DSS05.03 · **ISA 62443-2-1:2009** 4.3.3.6.6 · **ISA 62443-3-3:2013** SR 1.13, SR 2.6 · **ISO/IEC 27001:2013** A.6.2.2, A.13.1.1, A.13.2.1 · **NIST SP 800-53 Rev. 4** AC-17, AC-19, AC-20
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	· **CCS CSC** 12, 15 · **ISA 62443-2-1:2009** 4.3.3.7.3 · **ISA 62443-3-3:2013** SR 2.1 · **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4 · **NIST SP 800-53 Rev. 4** AC-2, AC-3, AC-5, AC-6, AC-16
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	· **ISA 62443-2-1:2009** 4.3.3.4 · **ISA 62443-3-3:2013** SR 3.1, SR 3.8 · **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1 · **NIST SP 800-53 Rev. 4** AC-4, SC-7

Framework Core:
a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors.

Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, National Institute of Standards and Technology, February 12, 2014

Benefits of using the Cybersecurity Framework

Improves Cybersecurity

- Up to date in terms of cyber threats / risks / effective controls
- Emphasis on Detect, Respond, Recover – not just Protect
- More up to date and comprehensive than the HIPAA Security Rule

Reduces Legal Exposure –

- Demonstrate due care in case of a breach and federal / state investigation or law suit
- Represents a baseline of good cybersecurity practices
- Originated from Presidential Order

Improves Collaboration and Communication

- Common understanding of cybersecurity with management

Cybersecurity Risk Management: Role of IAM

IAM is critical for HIPAA compliance

HIPAA Security Rule:

- Workforce Security: Implement policies and procedures to ensure that all members of its workforce have appropriate access to [ePHI] … and to prevent those … who do not have access ... from obtaining access… 164.308(a)(3)(i)
- Information Access Management: Implement policies and procedures for authorizing access to [ePHI] that are consistent with the applicable requirements…164.308(a)(4)(i)
- Access Control: Implement technical policies and procedures for electronic information systems that maintain [ePHI] to allow access only to those persons or software programs that have been granted access rights… 164.312(a)(1)

Cybersecurity Risk Management: Role of IAM

IAM is critical for cybersecurity risk management

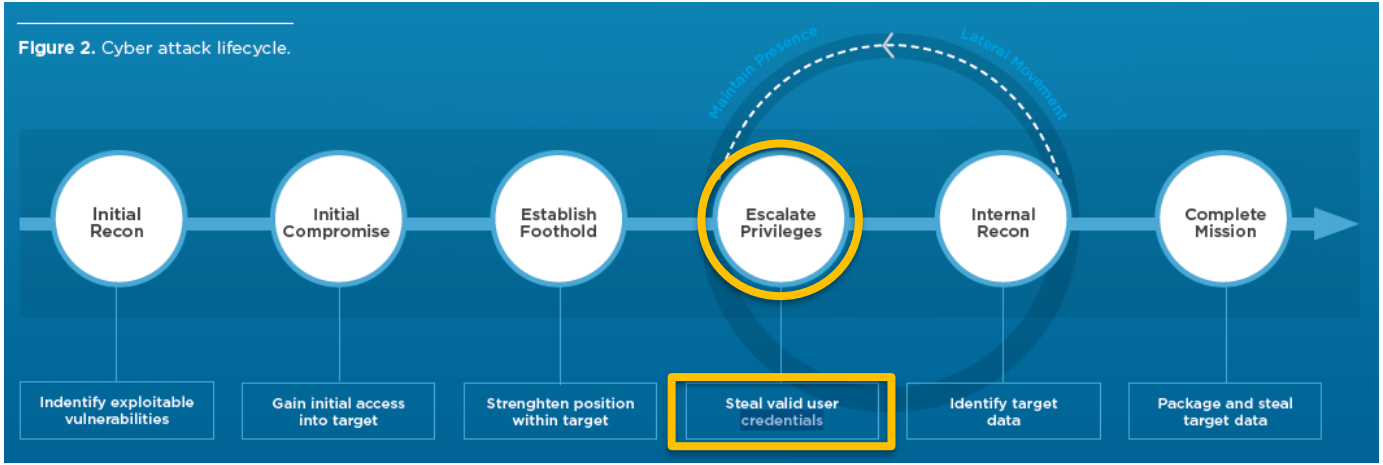
NIST Cybersecurity Framework:

- Identities and credentials are managed for authorized devices and users (PR.AC-1)
- Physical access to assets is managed and protected (PR.AC-2)
- Remote access is managed (PR.AC-3)
- Access permissions are managed, incorporating the principles of least privilege and separation of duties (PR.AC-4)
- Access to systems and assets is controlled, incorporating the principle of least functionality (PR.PT-3)

Cybersecurity Risk Management: Role of IAM

IAM is critical for cybersecurity risk management

Key role of compromised credentials in cyber attacks:



See Microsoft.com/pth

M-Trends 2017, A View From the Front Lines, Mandiant, p 10.

Key components of IAM

- Define access needed per role: least privilege / minimum necessary
- Methods to request and authorize access
- Methods to provision access
- Methods to change and terminate access
- Methods to track access requested/approved/provisioned/de-provisioned
- Methods to review and recertify access
- Audit process
- Credentials provided securely and per policy
- Strong authentication

Common Security Problems

- Shadow IT: Decentralized access management approach leads to inconsistent practices
- Inconsistent configuration of authentication settings (password length, password change period, password complexity, # of failed attempts allowed, etc.)
- Onboarding new users is inconsistent – not all access is done timely or right
- Inconsistent practices for handling terminations – missed or late terminations of access. Terminations may be late, especially for systems managed by third parties and for vendor access
- Weak authentication

Common Security Problems (continued)

- Lack of recertification to confirm authorized users and access levels
- Lack of monitoring and deactivating inactive (stale) accounts
- Inconsistent access levels per role (minimum necessary / least privilege)
- Infrequent users (auditors, surveyors) have year round access
- HIPAA non-compliance (missed terminations, excess privileges, etc.)
- Potential to overpay licensing fees due to missed terminations

- Post Acute Healthcare Organization
- 8,000 healthcare professionals across 54 locations in multiple states
- Private company
- National footprint
- Utilize cloud-based applications
- Rely on managed IT services

Covenant Care's IAM program

- Centralized, managed service model
- IAM solution with the following capabilities:
  - Electronic System Access Request Form (eSARF)
  - Workflow: Management authorization, system owner authorization
  - Access requests are submitted by management today, but system supports requests from the users with workflow for approvals
  - Management of roles and role-based access levels
  - Single source of truth for all identities and access levels / changes

Covenant Care's IAM program

- IAM solution with the following capabilities (continued):
  - Support for periodic recertification of authorized users and access levels
  - Automated terminations upon entry by HR or management
  - Terminations of access are based on IAM database, so terminations are complete and accurate. No need to check individual systems to confirm which systems the individual had access to
  - For infrequent system users system can inactivate access automatically based on end date or inactivity period; and can automatically re-activate all access upon request and approval(s)

Covenant Care's IAM program

Internal Audit Process

- Periodic access review
- Verify terminations are not missed and access levels are correct
- Internal audit for independent assurance

External Risk Assessment and Supplier Risk Management

- Annual security risk assessment of Covenant Care by third party
- Subscribe to security ratings of IT outsource partners & suppliers
- Communicate findings with IT partners & validate remediation

Challenges and Opportunities

- Implement the workflow for system owners to approve access requests which are not supported by pre-approved role-based access
- Support on-demand (rapid) provisioning
- Has 8,000 healthcare professionals across 54 locations in multiple states
  - Some employees move across different locations, requiring access changes
- Organizational changes can require rapid response from provisioning team
- Continue to improve consistency across the organization

Conclusions

- Cybersecurity risks will only increase
- Keep driving to a mature cybersecurity risk management program
- Utilize a cybersecurity framework
- Consider the NIST Cybersecurity Framework
- Invest in your IAM program to reduce risks related to
  - Excess privileges
  - Missed terminations
  - Outliers: external auditors, contractors, shadow IT

Questions

Richard Paul

VP, Information Technology
Covenant Care

Rpaul@CovenantCare.com

COVENANT CARE

Jeff Bell

Chief Information Security Officer
CareTech Solutions

Jeff.bell@CareTech.com

CareTech
An HTC Global Company