The slide features a blue-to-purple gradient bar on the left side. The Coverys logo is at the top left, with the tagline "Better Intelligence for Better Outcomes™". Below it, the text "Presented by:" is followed by "Sue Boisvert" and her credentials "BSN, MHSA, CPHRM, FASHRM" and title "Senior Risk Specialist". At the bottom of the bar is "Coverys Education". The main title "An Enterprise Look at Cyber Risk" is centered in a large, bold, blue font. The background is a light gray with faint, stylized graphics of a circuit board, binary code, and a person silhouette. The word "COVERYS" is also faintly visible in the background.

COVERYS
Better Intelligence
for Better Outcomes™

Presented by:

Sue Boisvert
BSN, MHSA, CPHRM, FASHRM
Senior Risk Specialist

Coverys Education

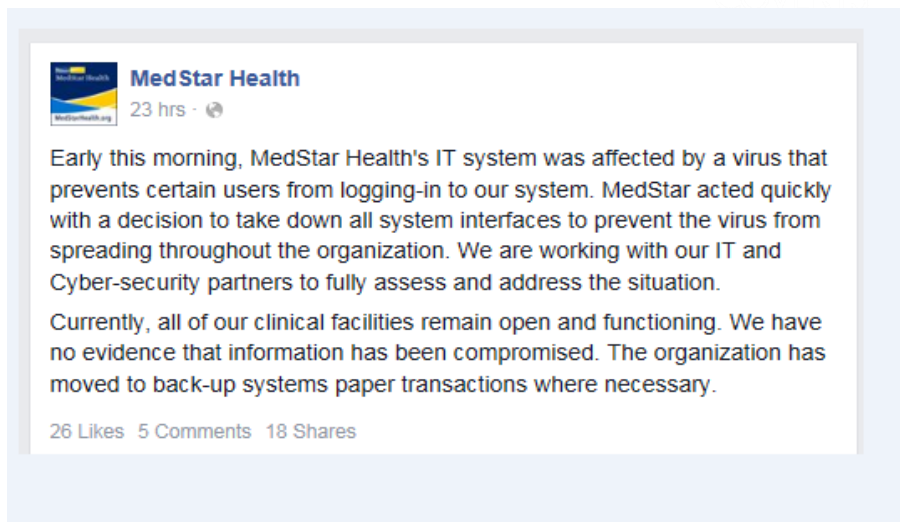
An Enterprise Look at Cyber Risk

Conflict of Interest Disclosure

Sue Boisvert does not have any real or apparent conflict(s) of interests or vested interest(s) that may have a direct bearing on the subject matter of the continuing education activity.

Learning Objectives

- Identify the top 3 cyber risks facing healthcare organizations today
- Define three common cyber risks/attacks
- Discuss risk management's role in mitigating cyber risk



The image shows a screenshot of a Facebook post from MedStar Health. The post is titled "MedStar Health" and is dated "23 hrs · 🌐". The text of the post reads: "Early this morning, MedStar Health's IT system was affected by a virus that prevents certain users from logging-in to our system. MedStar acted quickly with a decision to take down all system interfaces to prevent the virus from spreading throughout the organization. We are working with our IT and Cyber-security partners to fully assess and address the situation. Currently, all of our clinical facilities remain open and functioning. We have no evidence that information has been compromised. The organization has moved to back-up systems paper transactions where necessary." Below the text, it shows "26 Likes · 5 Comments · 18 Shares".

Data Sources



Ponemon Healthcare Data Report 2016

Top 3 Security Concerns

- 65% Employees
- 45% Cyber attacks
- 30% Mobile devices/Cloud

Top 3 Breach Root Causes

- 51% Criminal attack
- 41% Third party error
- 39% Lost or stolen device

Ponemon Healthcare Data Report 2016

Leading Vulnerabilities

Covered Entity

- 51% Lack of 3rd party vigilance
- 44% Lack of skilled IT staff

Business Associates

- 54% Employee negligence
- 50% Lack of mitigation technology

Ponemon. Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data. May 2016

HHS Breaches

By Covered Entity

- 66% Provider
- 19% Business Assoc.

By Misadventure

- 50% Theft
- 23% Unauthorized access
- 11% Hacking
- 10% Loss

By Media Type

- 50% Hardware
- 25% Paper
- 13% "e"

Verizon Data Breach Report 2015

Healthcare Sector Data Breach Causes

- 32% Miscellaneous Errors
- 26% Insider Misuse
- 16% Theft or Loss
- 12% Point of Sale
- 9% Web Application Attacks
- 4% Cyber Espionage
- 1% Crimeware

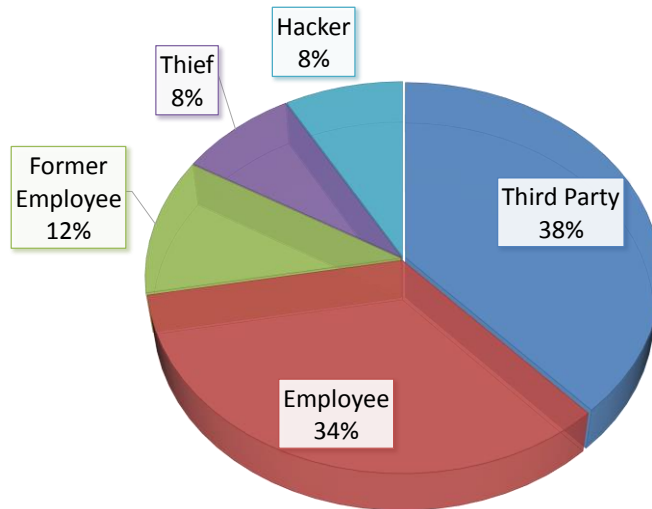


Verizon 2015 Data Breach Investigations Report

Cyber Regulatory Coverage

- Information Security and Privacy
- Privacy Breach Response Services
- Regulatory Defense and Penalties
- Social Media Content
- Cyber Extortion
- First Party Data Protection
- Crisis Management and Public Relations
- First Party Network Business Interruption

Cyber Claims by Source



Top Cyber Risks in Healthcare

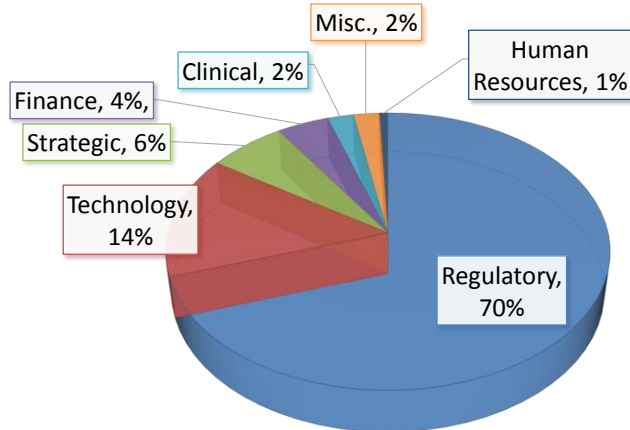
- Employees
- Business Associates
- Theft/Loss
- Cyber attacks (hacking, malware, DDoS etc)



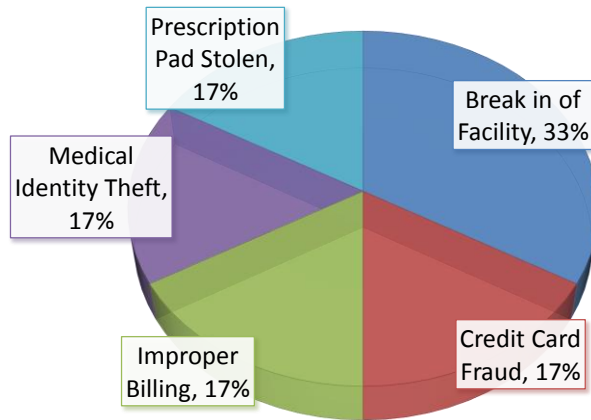
Activity



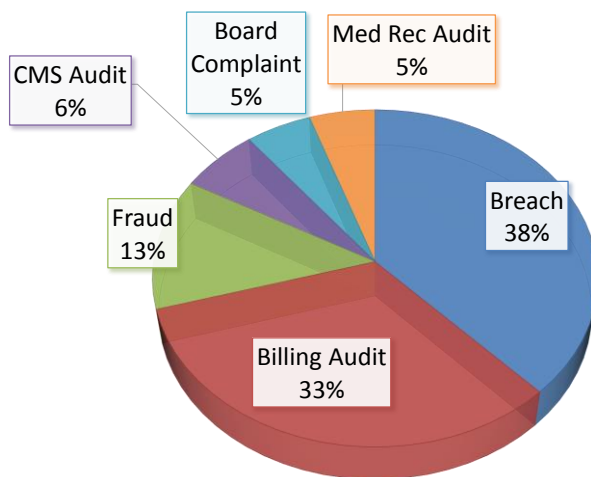
Cyber Claims by ERM Domain



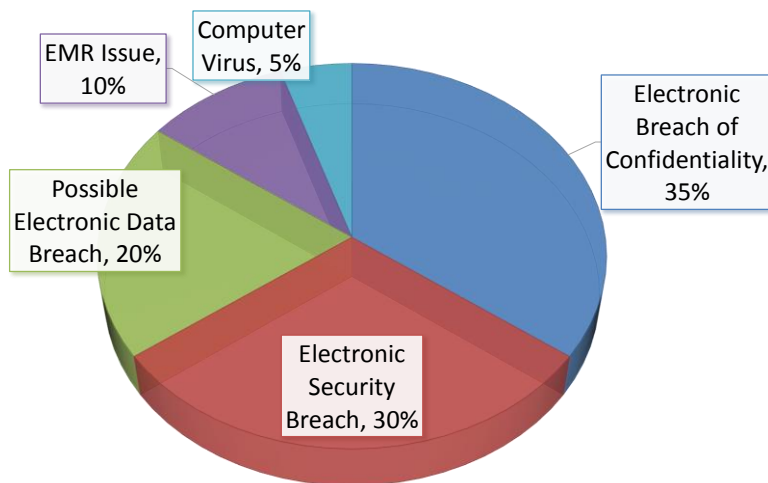
Finance Domain



Regulatory Domain



Technology Domain



Risk Management's Role?

- Participate on health IT committees
 - Collaborate with CIO, CISO, BME
 - Encourage an enterprise risk perspective
- Participate in privacy and security audits
 - Evaluate the Security Risk Assessment for omissions:
 - Networked medical devices
 - PCI Compliance
 - HVAC systems
 - Website/servers
 - Whaling

Risk Management's Role?

- Facilitate health IT and cyber risk event reporting
 - How are reports submitted
 - Who reviews the information
 - How is the investigation conducted
- Participate in significant cyber event analyses
 - Use comprehensive framework such as RCA3

Risk Management's Role?

- Keep up with the “evidence”
 - [NIST Special Publications](#) SP 800 and SP 1800 series
 - [Sociotechnical Model](#) of health IT
- Organize a team and implement one (or more) of the [SAFER Guides](#)



Cyber Resources

Center for Internet Security National Campaign
Cyber Hygiene Toolkits:

Count:

<https://www.cisecurity.org/cyber-pledge/tools/documents/count.pdf>

Configure:

<https://www.cisecurity.org/cyber-pledge/tools/documents/configure.pdf>

Control:

<https://www.cisecurity.org/cyber-pledge/tools/documents/control.pdf>

Patch:

<https://www.cisecurity.org/cyber-pledge/tools/documents/patch.pdf>

Repeat:

<https://www.cisecurity.org/cyber-pledge/tools/documents/repeat.pdf>

NIST Computer Security Division Special Publications SP 800 Series Computer
Security:

<http://csrc.nist.gov/publications/PubsSPs.html#SP 800>

SP 800-160 DRAFT Systems Security Engineering: An Integrated Approach to Building
Trustworthy Resilient Systems (Second Draft).

http://csrc.nist.gov/publications/drafts/800-160/sp800_160_second-draft.pdf

See Software Assurance Tables starting on page 264

SP 1800 Series Cyber Security:

<http://csrc.nist.gov/publications/PubsSPs.html>

Scroll down to 1800s

Sophos Threatsaurus: The A-Z of computer and data security threats:

<https://www.sophos.com/en-us/medialibrary/PDFs/other/sophosthreatsaurusaz.pdf?la=de-DE.pdf>

Thank You!!



COVERYS[®]
Better Intelligence
for Better OutcomesSM

All materials are subject to copyright. Reproduction without prior permission is prohibited.
This information is intended to provide general guidelines for risk management. It is not intended and should not be construed as legal advice.