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

Survive Ransomware and Thrive in a Digital Environment

Session #240, March 8, 2018

Susie Keeton, Director,

Product Management, Iron Mountain

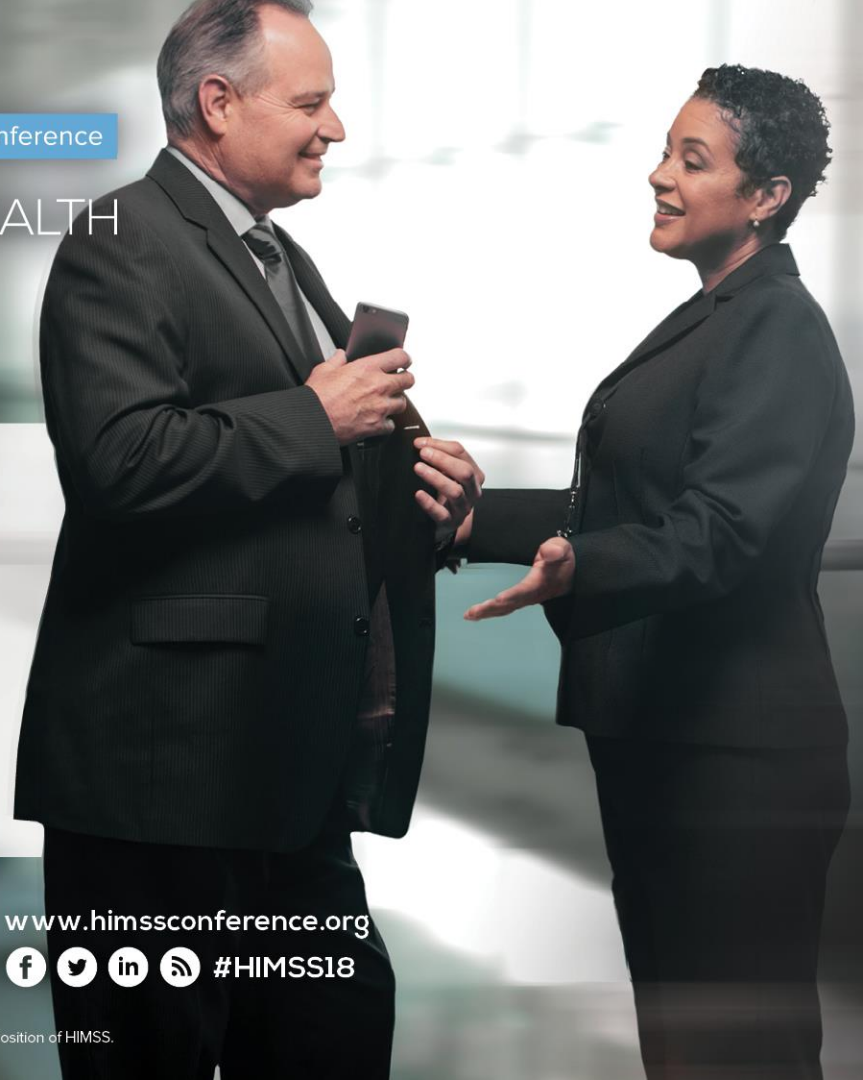
Joshua Clough, Senior Solutions Engineer, Iron Mountain

Jim Shook, DPS Cybersecurity & Compliance Practice, Global Technology Office, Dell EMC

IRON MOUNTAIN®

DELL EMC PARTNER PLATINUM

CLOUD SERVICE PROVIDER & STRATEGIC OUTSOURCER



COMMITMENT

www.himssconference.org

#HIMSS18

Agenda

- Progression of Ransomware Attacks In the Healthcare Industry
- Common Challenges in Combatting This Ever-Evolving Cyber Security Risk
- Best Practices to Limit Your Organization's Vulnerability, Optimize Recovery and Minimize the Fallout
- Questions from the Audience

Learning Objectives

- Learn about the current state of cyber-attacks in the healthcare industry
- Explore why existing solutions are no longer effective
- Identify practices to improve data protection and optimize recovery after an attack

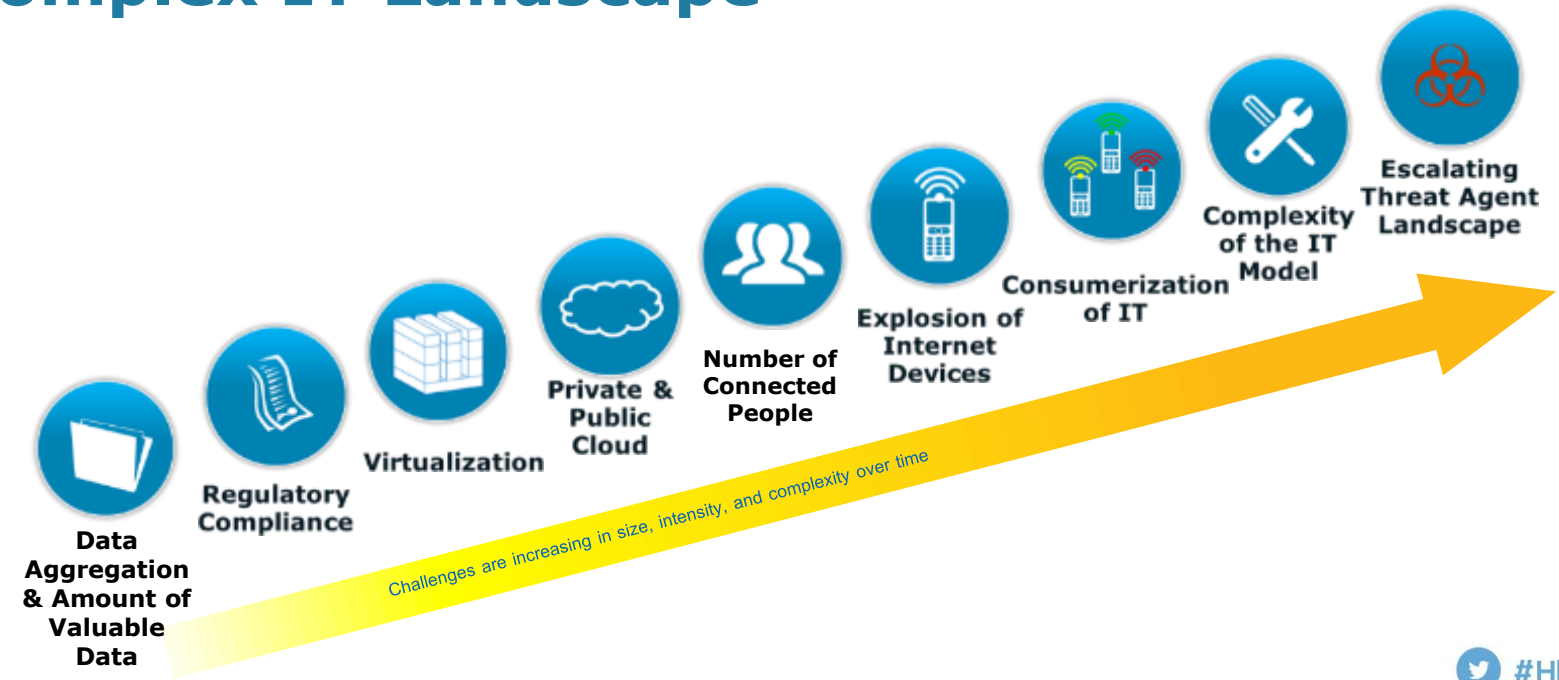
MEET YOUR SPEAKERS

Session Moderator: Susie Keeton, Director of Product Management, Iron Mountain
An accomplished business leader and product manager with extensive experience in the medical and scientific industries, Susie oversees the innovation roadmap and manages a portfolio of cloud products for archival data needs across several verticals including healthcare. Prior to her role at Iron Mountain, Susie held senior product and technology roles at Philips and CareFusion.

Panelist: Joshua Clough, Senior Solutions Engineer, Iron Mountain
Joshua Clough is a visionary IT professional with over a decade of experience in the industry. As Senior Solutions Engineer at Iron Mountain, Joshua is responsible for the design of Cloud, Backup and Disaster Recovery solutions. Prior to his role at Iron Mountain, Josh held technical solution and disaster recovery architect roles at organizations such as IBM, SourceHOV and AvanGrid.

Panelist: Jim Shook, DPS Cybersecurity & Compliance Practice, Global Technology Office, Dell EMC
Jim is a recognized authority on the intersection of law and technology, focusing on cybersecurity and compliance issues including data privacy, retention and eDiscovery. He leverages a diverse background in law and computer science to help Dell EMC's customers understand and solve their issues in these areas.

Digital Transformation Has Created a Highly Complex IT Landscape



Discussion Topic: Emerging and Growing Threats

- How would you describe the threat landscape?
- What threats are you most concerned about today?
- Looking forward, how do you see the threat landscape evolving?

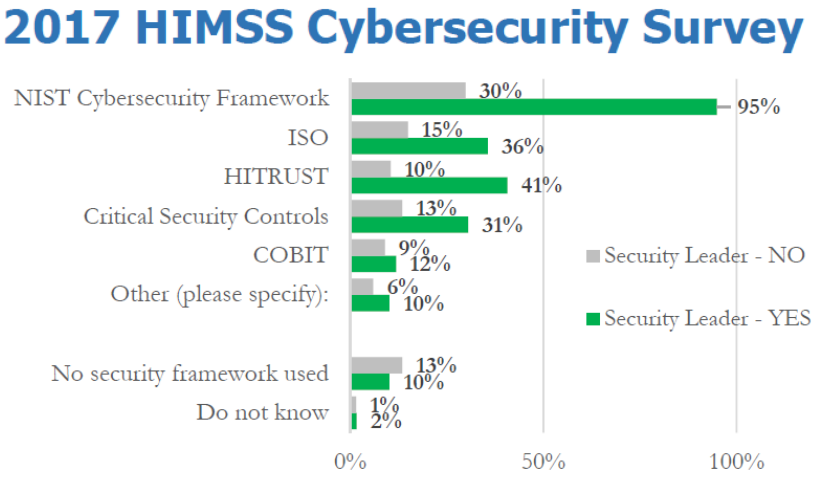
Discussion Topic: The Increasing Value and Vulnerability in Healthcare

- Why is healthcare such a desirable target for cyber-criminals today?
- For healthcare providers, what are the short-term and long-term implications of a ransomware attack?

Best Practices For Surviving A Ransomware Attack

Adopt a Cyber Security Framework

- What are the key differences between NIST and HITRUST?
- Why are organizations with a CISO in place heavily adopting NIST?
- Why is it critical to adopt a framework?



Source: *http://www.himss.org/sites/himssorg/files/2017-HIMSS-Cybersecurity-Survey-Final-Report.pdf*

NIST Cybersecurity Framework

Identify	Protect	Detect	Respond	Recover
• Asset Management • Business Environment • Governance • Risk Assessment • Risk Management Strategy	• Access Control • Awareness and Training • Data Security • Information Protection Processes and Procedures • Maintenance • Protective Technology	• Anomalies and Events • Security Continuous Monitoring • Detection Processes	• Response Planning • Communications • Analysis • Mitigation • Improvements	• Recovery Planning • Improvements • Communications • Validation

Identify	Develop ability to manage risk
Protect	Develop and implement safeguards
Detect	Develop activities to identify events
Respond	Develop ability to contain
Recover	Develop resilience and restore

NIST National Institute of Standards and Technology U.S. Department of Commerce

Identify

- Align with stakeholders across the organization to classify mission critical applications and data to minimize impact to patient care and health system operations in event of attack
- Tier data and backup strategy based on risk profile
- Categorize impact of losing access to data for:
  - Patient outcomes
  - Financial
  - Reputation

Discussion Topic: Identifying Critical Data

- What percentage of enterprise data should be labeled “critical” to business operations?
- What are the tiers of data protection based on risk profile and compliance requirements?

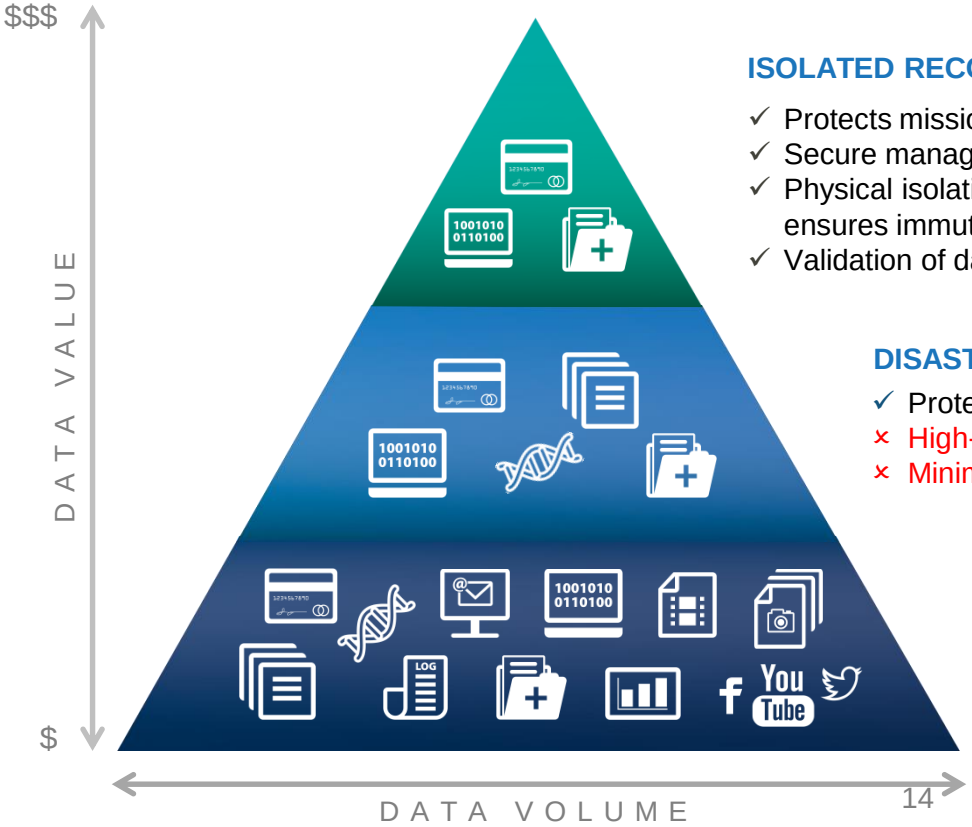
Identify	Develop ability to manage risk
Protect	Develop and implement safeguards
Detect	Develop activities to identify events
Respond	Develop ability to contain
Recover	Develop resilience and restore

NIST National Institute of Standards and Technology U.S. Department of Commerce

Protect

- Assess and validate that critical data is protected
- Evaluate and address gaps in protection strategy and develop roadmap to mitigate risks
- Avoid data loss or corruption from attacks
- Leverage professional services to design, implement, test and maintain data protection environment

The Pyramid of Protection



ISOLATED RECOVERY

- ✓ Protects mission critical data against cyberattack
- ✓ Secure managed service protects against internal attacks
- ✓ Physical isolation prevents network access and ensures immutability of data
- ✓ Validation of data prior to recovery

DISASTER RECOVERY

- ✓ Protection against site loss
- × High-cost and complexity limit effectiveness and scope
- × Minimal protection from data loss or corruption from cyber attack

LOCAL BACKUP

- ✓ Basic lowest-cost protection and recovery for production and large data sets
- ✓ Relatively fast recovery
- × No protection from data loss or corruption from cyber attack

Discussion Topic: Protection

- How can cloud be a part of sound cybersecurity and data protection strategy while maintaining HIPAA compliance?
- What are best practices to identify risks and vulnerabilities in your environment?

Identify	Develop ability to manage risk
Protect	Develop and implement safeguards
Detect	Develop activities to identify events
Respond	Develop ability to contain
Recover	Develop resilience and restore

NIST National Institute of Standards and Technology U.S. Department of Commerce

Recover

- Test the recoverability of your critical data for RTO, RPO and backup
- Validate integrity of backup data in a secure, segregated environment
- Recover production-ready data after the attack lifecycle has been stopped

Discussion Topic: Recovery

- What are critical metrics to measure preparedness and success in the event of an attack?
- What solutions can a health system use to ensure a gold copy of critical data?
- What are best practices for quick recovery to minimize downtime?

Closing Thoughts

Questions

IRON MOUNTAIN®

DELL EMC PARTNER PLATINUM
CLOUD SERVICE PROVIDER & STRATEGIC OUTSOURCER

Please feel free to contact today's speakers with any questions you might have following this session:

Susie Keeton, Director of Product Management, Iron Mountain, Susanna.Keeton@ironmountain.com

Joshua Clough, Senior Solutions Engineer, Iron Mountain, Joshua.clough@ironmountain.com

Jim Shook, DPS Cybersecurity & Compliance Practice, Global Technology Office, Dell EMC, jim.shook@dell.com