CtHiMA

AHIMA Affiliate

Connecticut Health Information Management Association

Information Governance: A Best Practices Approach to Mitigating Risks and Improving Resilience

John Moynihan, CPHIMS

May 22, 2019

IRON MOUNTAIN®

re·sil·ience

/rəˈzilyəns/

noun

1. the capacity to recover quickly from difficulties; toughness.
   "the often remarkable resilience of so many British institutions"
2. the ability of a substance or object to spring back into shape; elasticity.
   "nylon is excellent in wearability and resilience"

Session Objectives

- The Current Healthcare Landscape
- What is a Data Breach?
- What happens when the worst happens?
- Let’s talk about Resilience
- Information Governance and why you need it.
- How to get there
- Q&A

The Current Healthcare Landscape

IRON MOUNTAIN®

The Current Landscape: Key Focus Areas

STRATEGIC TARGETS

- Quality outcomes
- Reduced compliance & privacy risks
- Savings targets
- Achieve margin improvement
- Leverage technology

OPERATIONAL EFFICIENCY

- Enhance labor efficiency/ productivity
- Reduce redundancies/ rework
- Improve workflow

COMPLIANCE RISKS

- Advance proactive data and information management
- Improve defensible disposition
- Minimize breach & cybersecurity risks

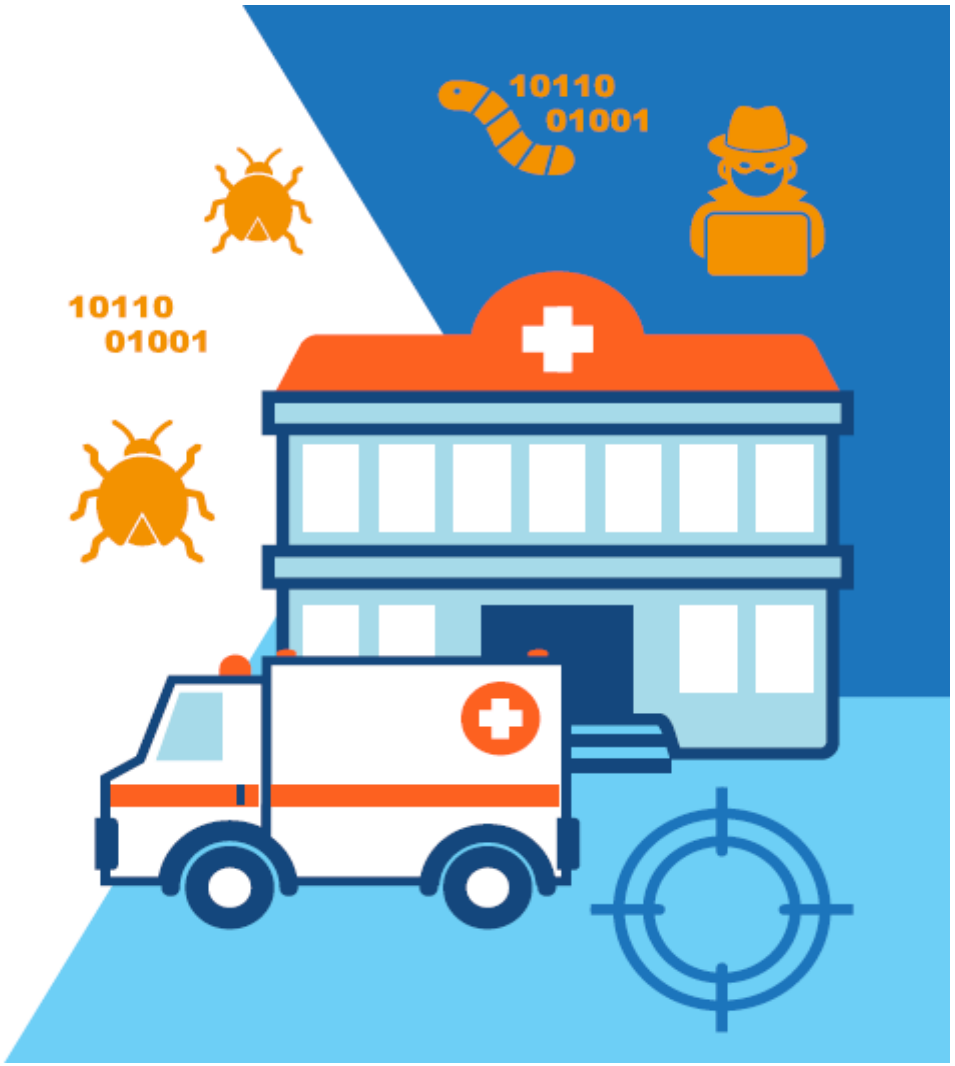
MERGERS & ACQUISITIONS

- Integrate systems
- Address data discrepancies/ source of truth defined
- Integrate hospitals, physician practices, clinics, & other business units
- Manage cultural shifts

What is a Data Breach?

- *According to Techopedia,*

- “A data breach is an incident that involves the unauthorized or illegal viewing, access or retrieval of data by an individual, application or service. It is a type of security breach specifically designed to steal and/or publish data to an unsecured or illegal location.”



https://www.techopedia.com/definition/13601/data-breach

IRON MOUNTAIN®

Your hospital will be targeted.

- Healthcare organizations remain the most vulnerable of any industry because of a lack of investment in infrastructure security
- Hospitals remain the most targeted sector among cyber criminals because health records are worth 20 times the value of credit card

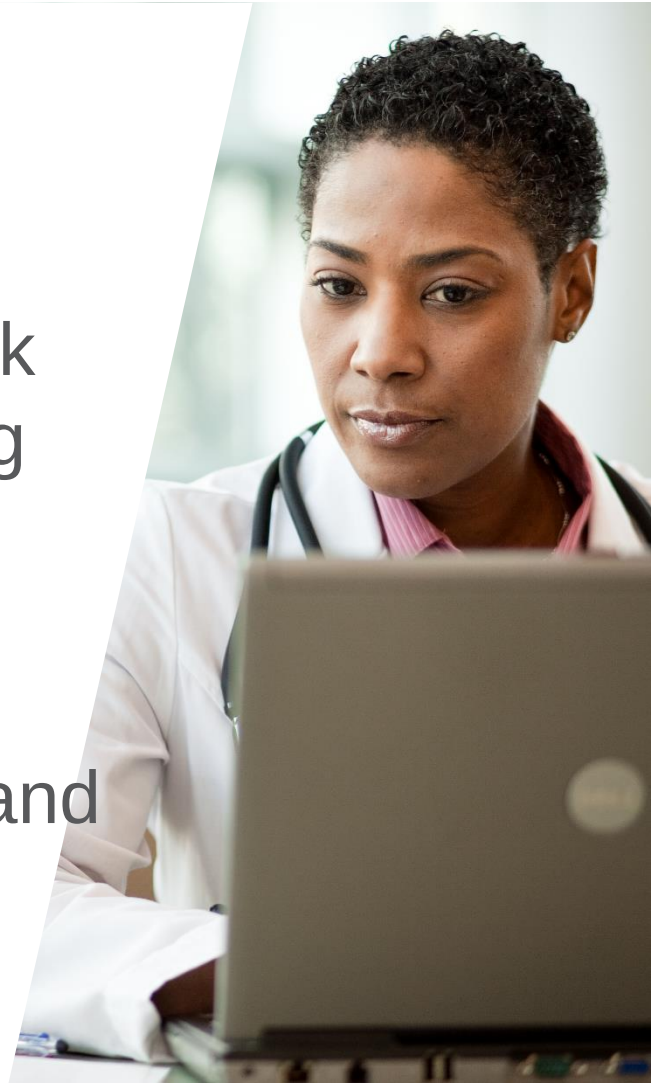
Modern Cyber-Attack Threats

Malware	**Zero-Day & Well-Known**
Destruction	**Wiping**
Ransomware	**Encrypted data held hostage Encrypting/decrypting pre & post processors in app path**
Slow Moving Crawlers	**Subtly encrypt and wipe small pieces of data**
Records Tampering	**Alteration & extraction of data**
Insider Attacks	**Trusted insiders steal proprietary information for personal, financial or ideological reasons**

IRON MOUNTAIN®

Types of Cybersecurity Attacks

- Malware
- Phishing
- SQL Injection Attack
- Cross-Site Scripting (XSS)
- Denial-of-Services (DoS)
- Session Hijacking and Man-in-the-Middle Attacks
- Credential Reuse



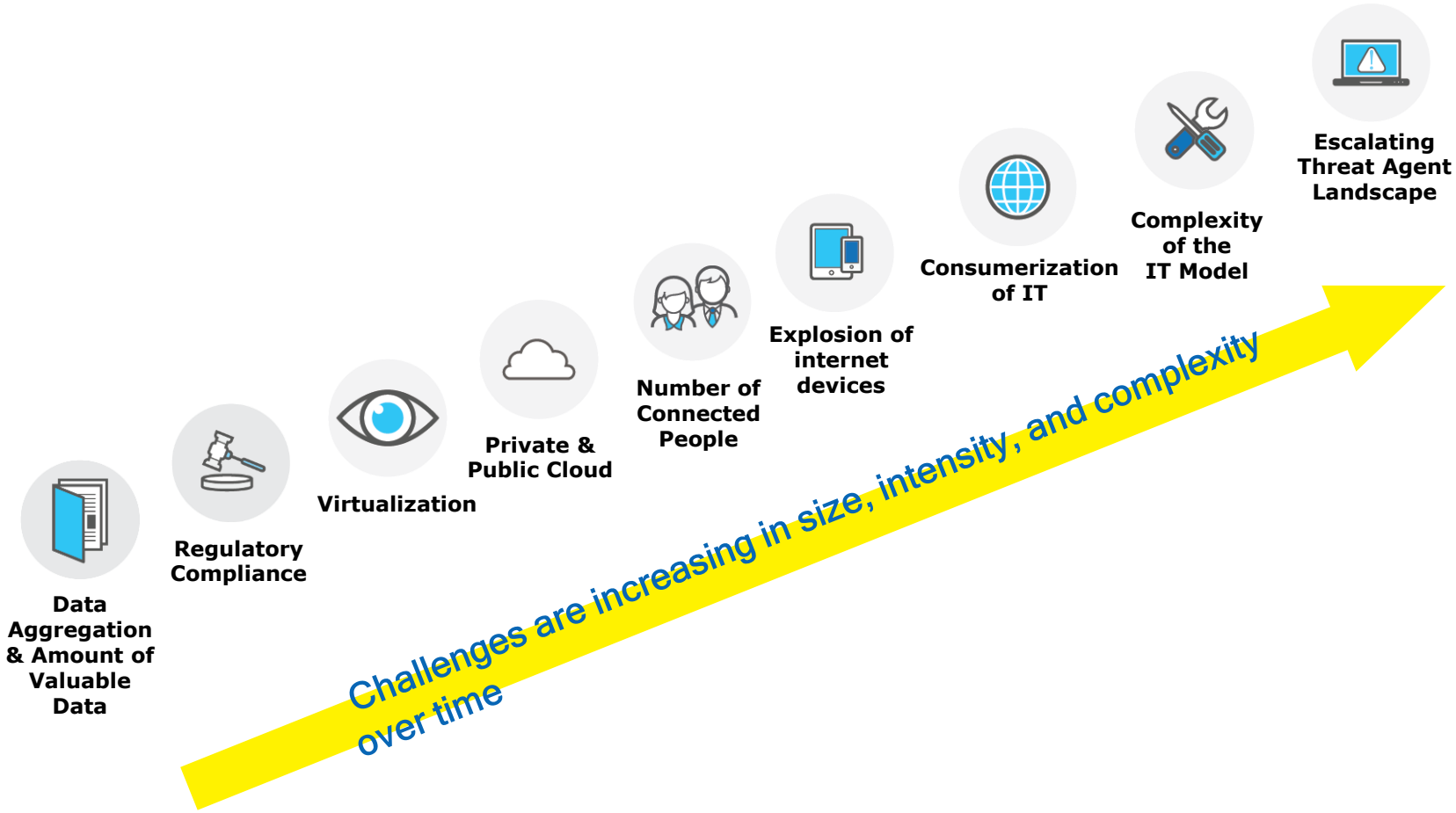
https://www.rapid7.com/fundamentals/types-of-attacks/

The Real Costs of a Ransomware Attack

Sample Ransom: $30,000

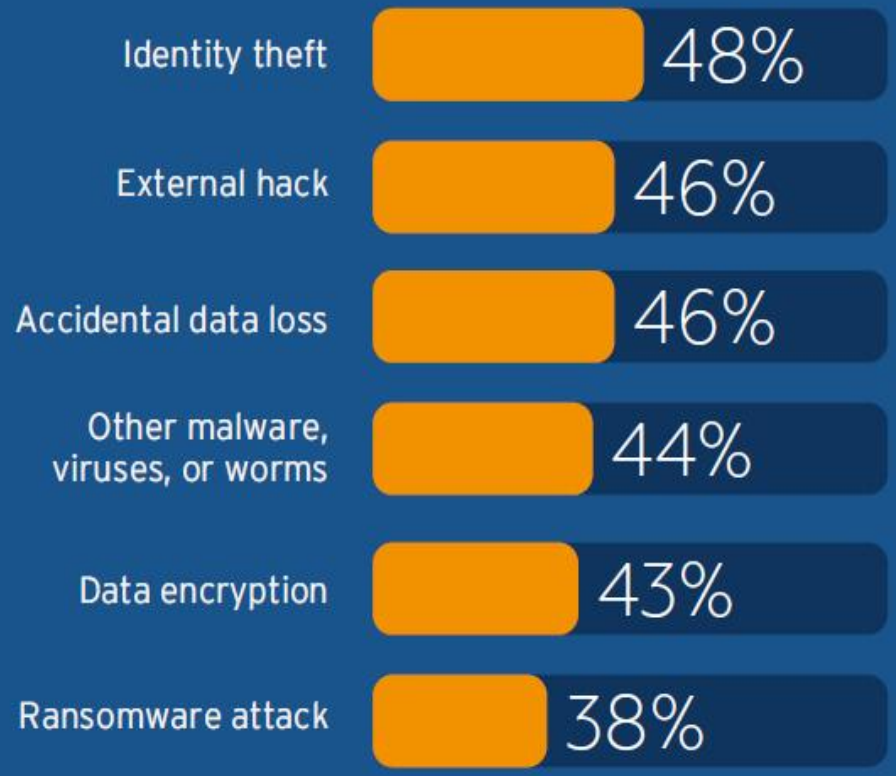
Lost Revenue	2,500,000
Incident Response	75,000
Legal Advice	70,000
Lost Productivity	250,000
Forensics	75,000
Recovery & Re-Imaging	60,000
Data Validation	25,000
Brand Damage	500,000
Litigation	200,000
Data Loss	3,000,000
Total Costs of Attack	**$6,755,000**

Digital Transformation Has Created a Complex Information Landscape

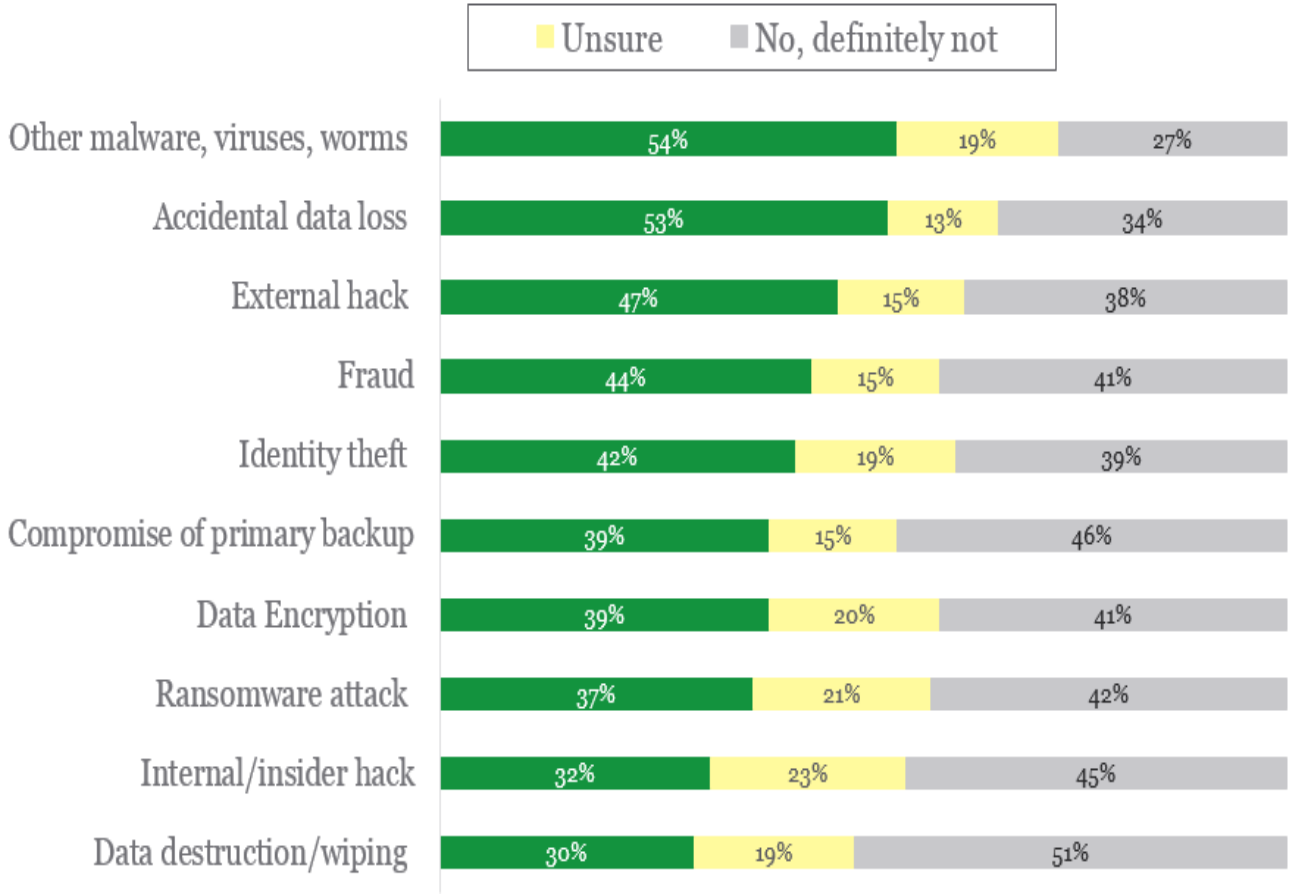


WHICH CYBERSECURITY RISKS ARE THESE ORGANIZATIONS MOST WORRIED ABOUT?

THE SHORT ANSWER: A BUNCH OF THEM.



Experience with Cybersecurity Events



86% of healthcare organizations report they've experienced one or more of these cybersecurity events.

IRON MOUNTAIN®

MORE THAN

HALF

(58%) OF THESE ORGANIZATIONS TOOK "DAYS, WEEKS, OR LONGER" TO GET AFFECTED DATA BACK TO A GOOD STATE AFTER THEIR MOST SERIOUS SECURITY EVENT.

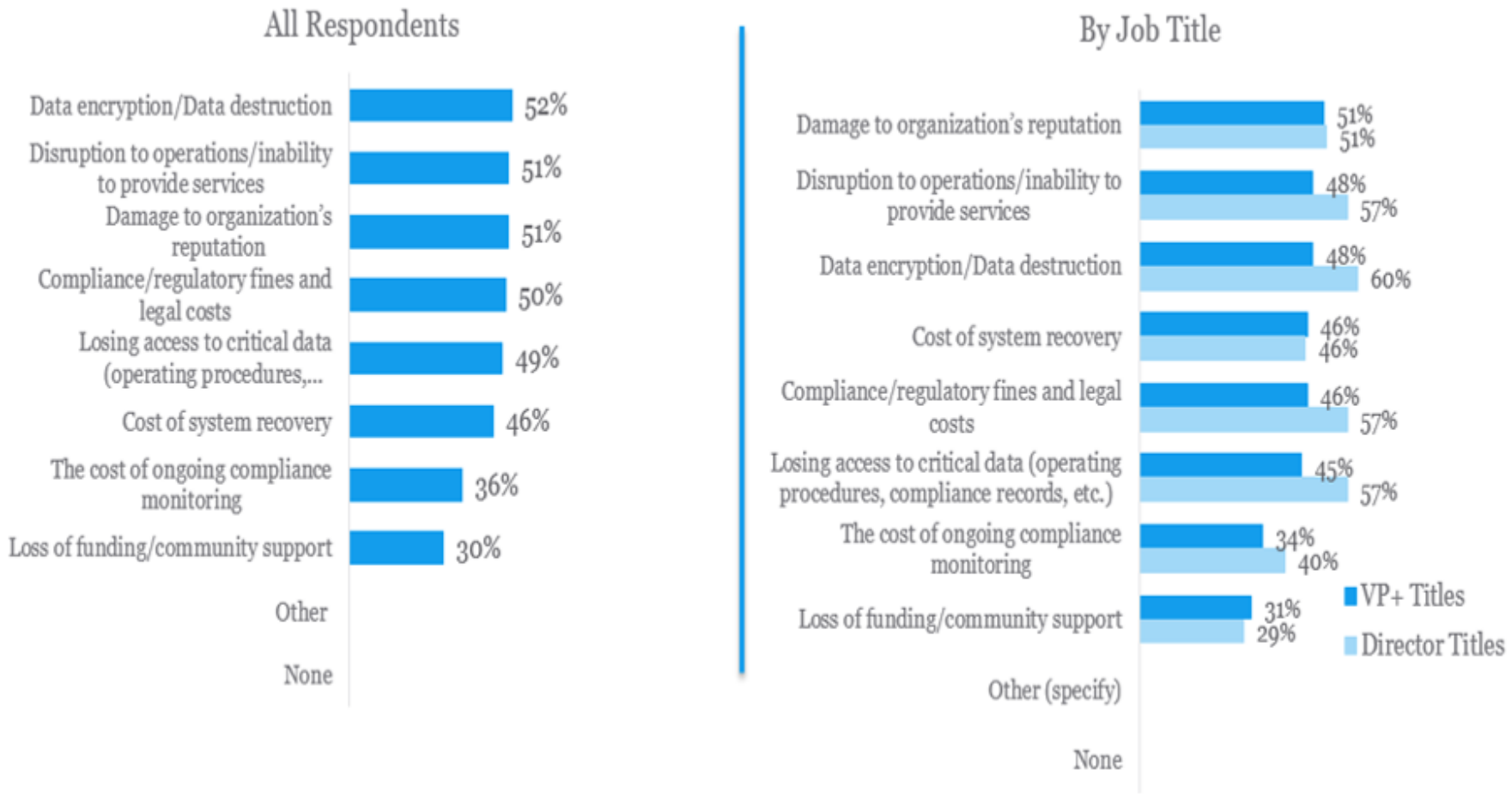
AND

65%

HAD TO REVERT TO DATA VERSIONS THAT WERE "DAYS OR WEEKS" OLD.

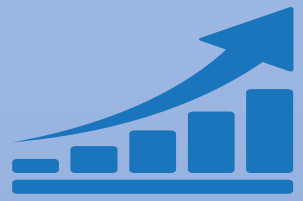
IRON MOUNTAIN®

Most Concerning Potential Business Impacts of Cybersecurity Attacks



Healthcare Industry Cyber Challenges

Explosive Data Growth



Healthcare represents a significant percentage of the overall Digital Universe, and is growing at **48% per year** — faster than the rest of the Digital Universe.

IDC/EMC Digital Universe 2015

Increased Cost of Breach

The cost per lost or stolen record in Healthcare is the highest of any industry, $408 and continues to increase, up $28 from $380 per record in the 2017 report.

2018 Cost of Data Breach study
IBM Security and the Ponemon Institute

Budget Pressures

Healthcare provider IT spending is experiencing decline – yet health systems need planning, modernization, implementation and ongoing threat monitoring

Gartner WW IT Spending Report 9/15

"The healthcare sector is the most targeted yet underprepared genre within our Nation's critical infrastructures."

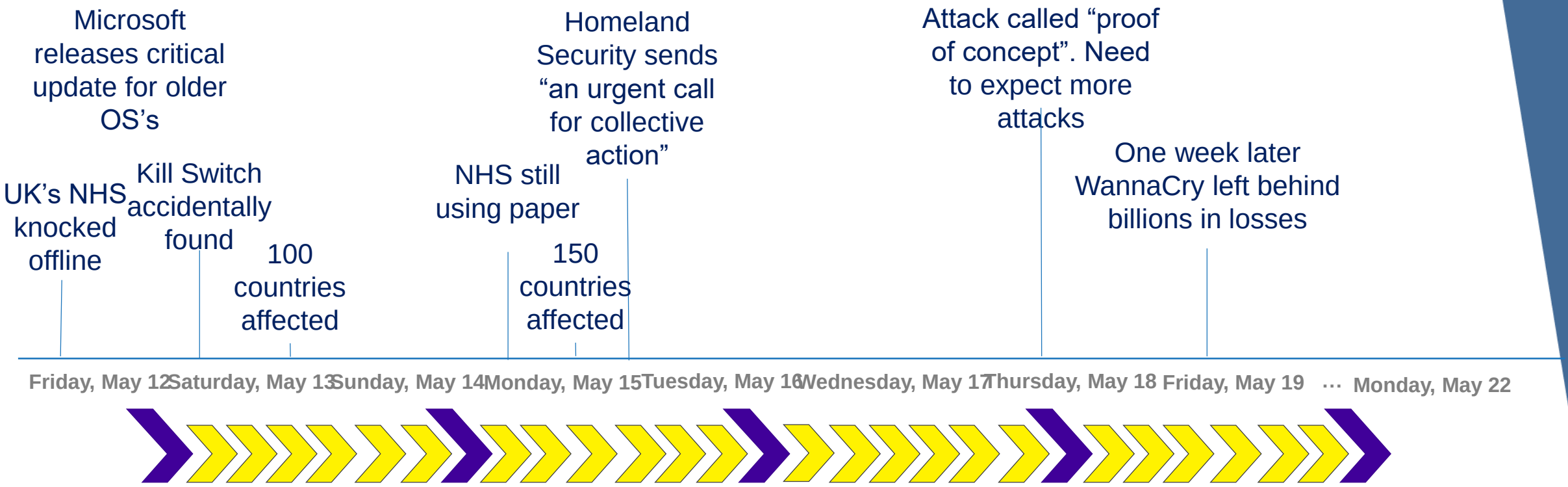
– ICIT "Hacking Healthcare IT in 2016"

Healthcare Regulatory Cybersecurity Guidance

Agency	Data Protection Focus
HIPAA	§ 164.308.7.(ii) Administrative Safeguards – *Required to Establish and Implement:* ✓ **Data backup plan** to create and maintain retrievable copies of ePHI ✓ **Disaster recovery plan** to restore any loss of data ✓ **Emergency mode operation plan** to **enable continuation of critical business processes** for protection of the security of ePHI while operating in emergency mode ✓ **Guidance** Issued for Ransomware as Breach – ***Be Prepared!***
	✓ "... Test restorations should be periodically conducted to verify the integrity of backed up data and provide confidence in an organization's data restoration capabilities…. … **As some ransomware variants have been known to remove or disrupt online backups, entities should consider maintaining backups offline and unavailable from their networks."** ✓ **"The presence of ransomware (or any malware) is a security incident under HIPAA** *that may also result in an impermissible disclosure of PHI in violation of the Privacy Rule and a breach…"* July 2016, US Department of Human and Health Services
CyberCrime Task Force	✓ Back up data regularly, and regularly verify the integrity of those backups. ✓ Secure your backups ✓ **Ensure backups are not connected to the computers and networks they are backing up**. Examples might be securing backups in the cloud or physically storing offline. … Backups are critical in ransomware; if you are infected, this may be the best way to recover your critical data.

IRON MOUNTAIN®

WannaCry Ransomware Cyberattack Timeline & Response, May 2017



IRON MOUNTAIN®

Ransomware Attack Disrupts Emergency Services at Ohio Hospital

What Is Information Governance?

IRON MOUNTAIN®

An organization-wide framework for **managing information throughout its lifecycle** and for supporting an organization's strategy, operations, regulatory, legal, risk, and environmental requirements.

SOURCE: 2014 Information Governance in Healthcare Benchmarking Survey by Cohasset Associates and AHIMA and underwritten by Iron Mountain.

Why Adopt Formal Information & Security Governance in Healthcare?

- Necessary to meet the requirements of a complex Healthcare ecosystem
- Realigns the focus of information management from being solely on technology and physical records to the people and policies around the information
- Required to ensure safe high quality care
- Differentiator that demonstrates a Healthcare organization's commitment to treating information as a valued strategic asset

Aligning IG With Strategic Objectives

Quadruple Aim
Improve patient experience
Improve health of populations
Reduce per capita expense
Reduce clinician & staff burnout

Top Healthcare Regulations
HCQIA Act of 1986
Medicare / Medicaid
CHIP
HRRP
HIPAA Act of 1996
PSQIA of 2005
Affordable Care Act of 2010

Value-Based Care
Payment based on health outcomes vs. fee-for-service or capitated approach

Interworking Gears of Governance

Information Governance:

- Accountability framework & decision rights to ensure effective & efficient us of information across the enterprise to achieve its goal
- Responsibility of executive leadership
- Focus on strategic goals

IT Governance:

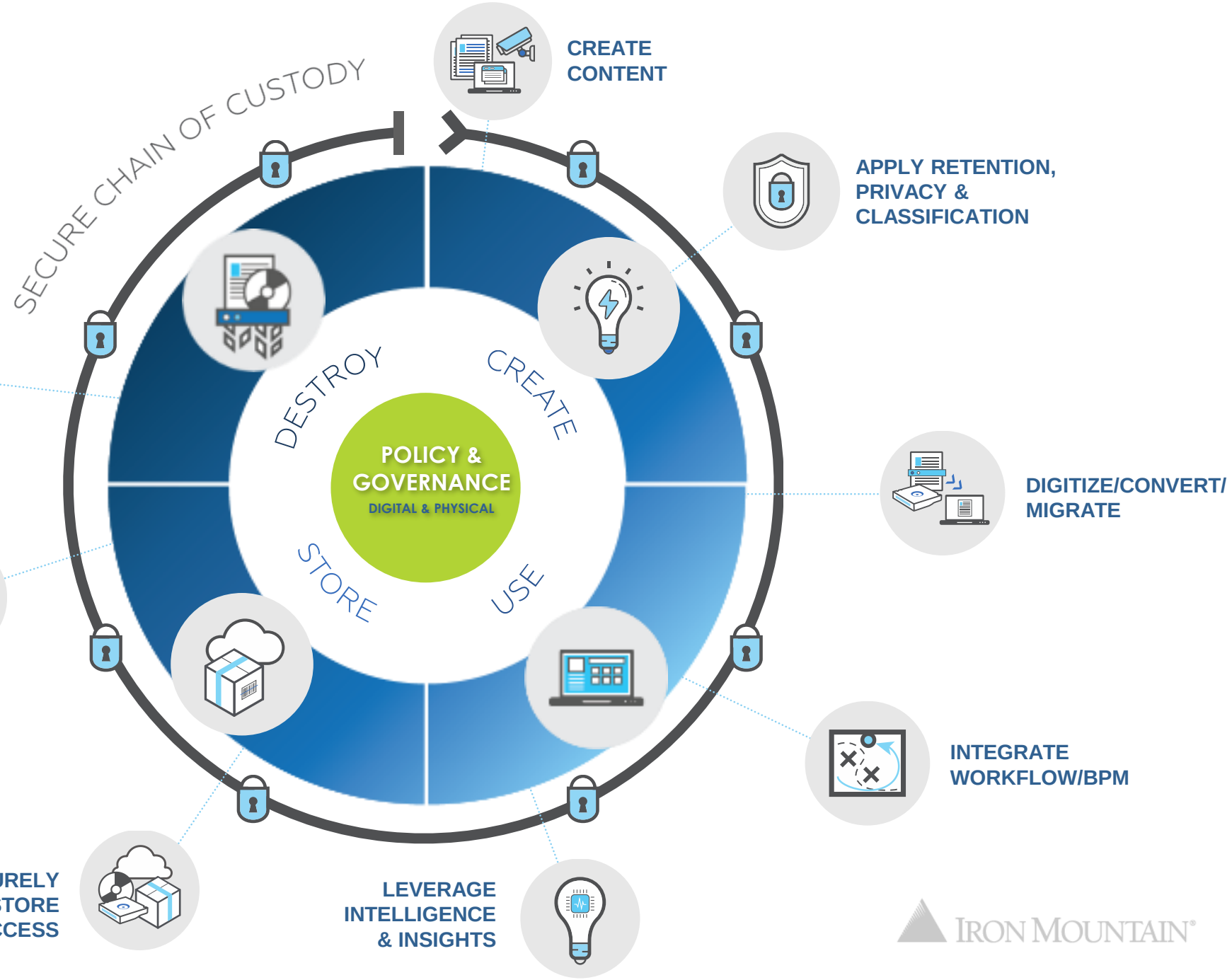
- Policies & procedures to ensure the effective evaluation, selection, prioritization, & funding of competing IT investments
- Oversee implementation & extract business benefits
- Led by the CIO

Data Governance:

- Policies, processes & practices that address the accuracy, validity, completeness & integrity of data (data quality)
- Operational focus (i.e., metadata, classifications, data standards, auditing, risk management, versioning, etc.)
- Business unit stewardship responsibility

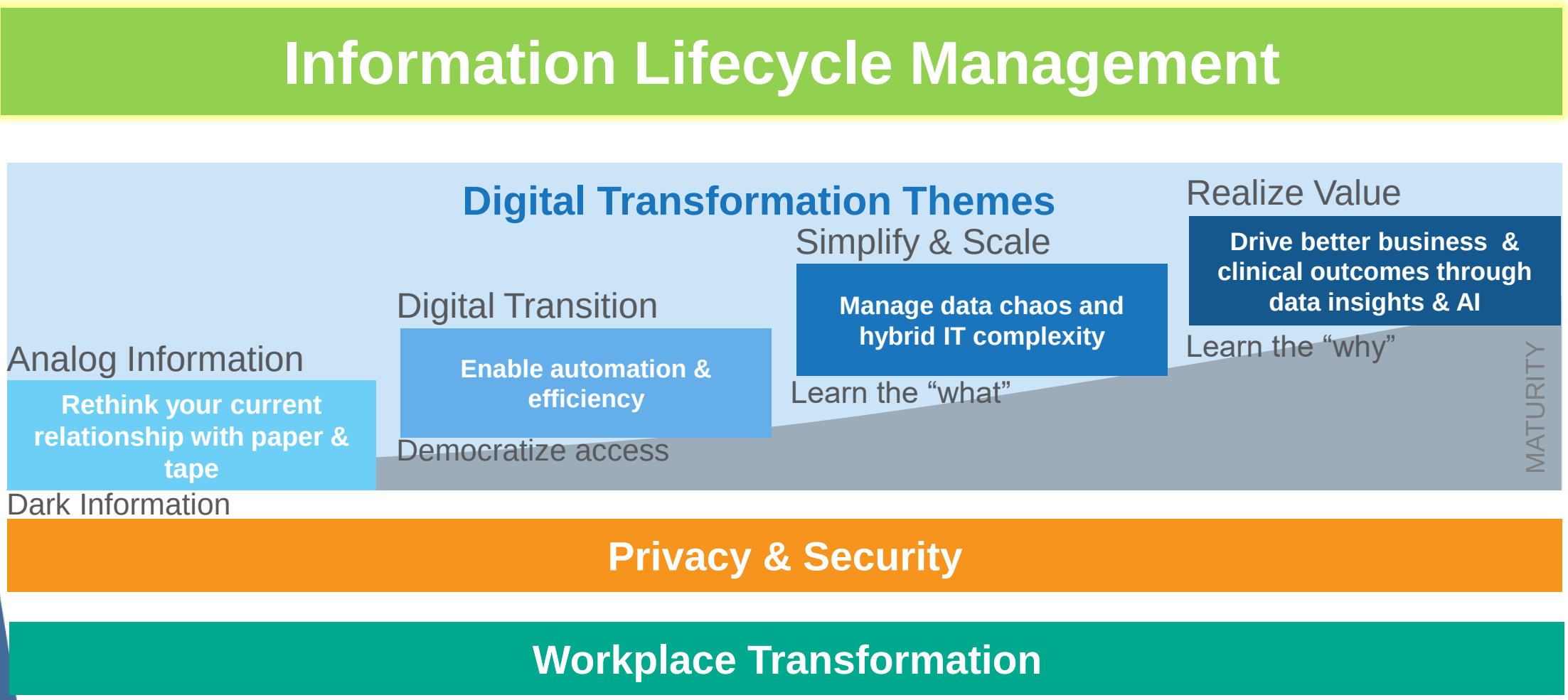
Source: Journal of AHIMA November-December 13

The Information Lifecycle



IRON MOUNTAIN®

Digital Transformation Maturity Model



IRON MOUNTAIN®

Information & Security Governance ensures information quality and integrity by creating a clinical and operational baseline for an organization's infrastructure from which to track changes over time

Information & Security Governance in Healthcare

- Healthcare information is a strategic asset
- Healthcare is a highly regulated industry where organizations must demonstrate compliance with a myriad of laws and standards
- The protection of Personal Healthcare Information (PHI) through Information & Security Governance (IG) from breach, loss, or corruption is critical in order to maintain trust

Let's Talk About Paper…

Hospitals account for
1/3 of all healthcare breaches

Results varied by hospital type

Paper and films most often breached

- Theft
- Improper disposal
- Unauthorized access

Resource: https://www.healthcare-informatics.com/news-item/cybersecurity/paper-records-films-most-common-type-healthcare-data-breach-study-finds

69%

DID YOU KNOW?

Did you know that 69 percent of the information in most companies serves no regulatory, legal or business purpose?

70%

FAST FACT:

In a typical company, as much as 70 percent of paper documents and 60 percent of unneeded electronic information can be defensibly disposed of in a compliant manner.

Resource: https://www.ironmountain.com/resources/general-articles/d/defensible-disposition-and-risk-mitigation-keep-everything-is-not-a-strategy

Key IG Concept: Privacy & Cybersecurity

- Administrative Safeguards
  - Data and information inventories
  - Record retention policies and schedules
  - Defensible disposition practices
- Physical Safeguards
  - Buildings
  - Access
- Technical Safeguards
  - Systems
  - Appropriate access
  - Encryption, firewalls, cloud storage, data centers & redundancy

Resource: https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment

Health Care Industry Cybersecurity Task Force

"In health care, security and cyber risk has historically fallen to IT. ***Information governance*** *is a relatively new concept in the industry and should include not just IT and security stakeholders, but also information stakeholders. Governance structures should also include clinical and non-clinical leaders. Governance of information shifts the focus from technology to people, processes, and the policies that generate, use, and manage the data and information required for care."*

https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf

Defensible Disposition – A Critical Component of IG and Risk Avoidance

"It is natural that information – data and records in all formats – will have an *end of life* at some point in time. Defensible disposition comes into play at this juncture and relates to making decisions about what can be disposed of based on an official policy, and that may mean either moving it to a secure archive or destroying it in a compliant way."

Resource: https://www.ironmountain.com/support/information-economics-academy/our-courses/defensible-disposition

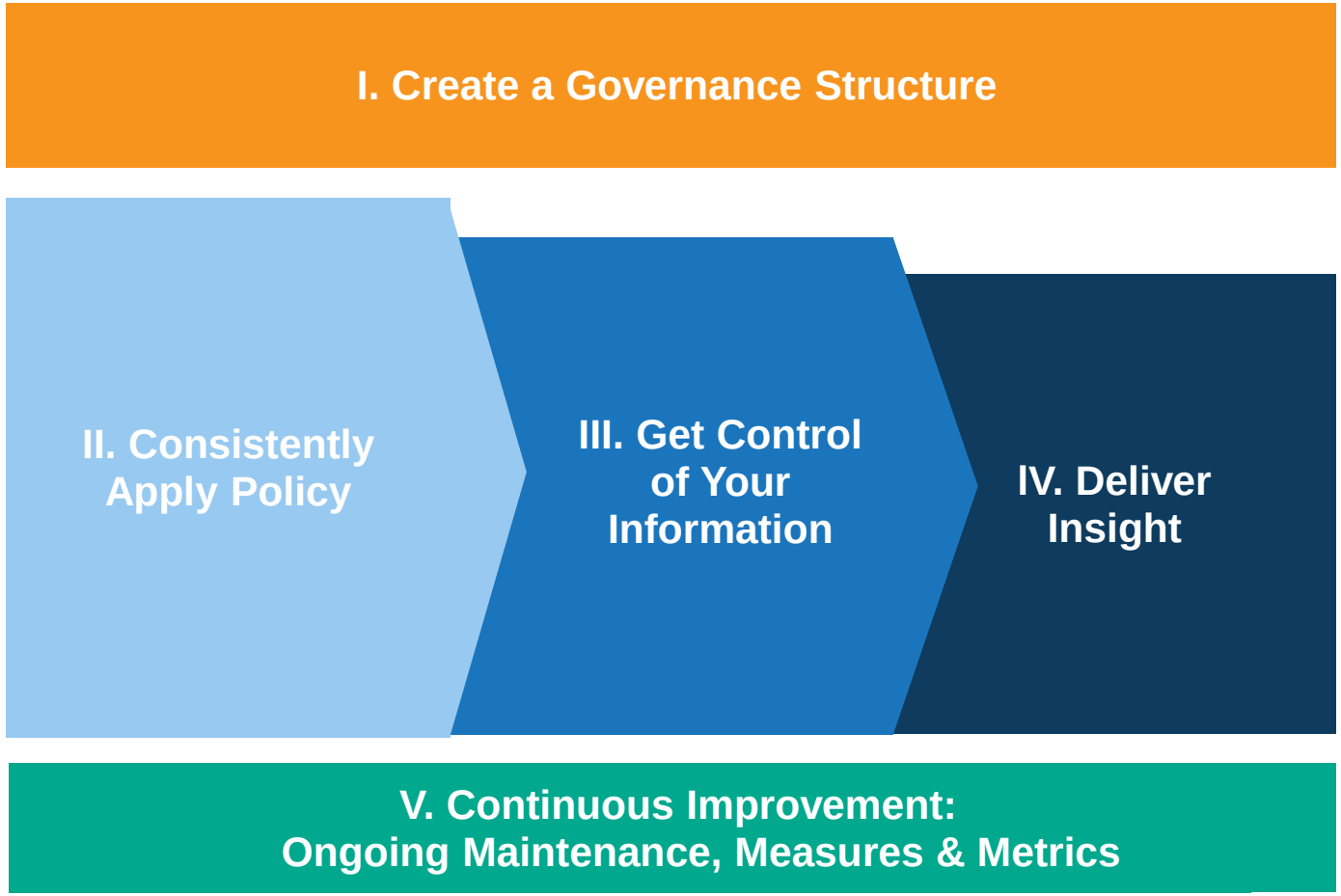
Challenges with Defensible Disposition

1. Not knowing where to start
2. Ill-defined process or execution plan
3. Legal and operational considerations
4. Limited technology
5. Missing or inadequate controls

Resource: A Practical Guide to Records and Information Management Destruction, https://www.ironmountain.com/resources/whitepapers/d/defensible-disposition-report

"The best defense is a good offense."

Roadmap to Achieve Compliance & Enable Enterprise-Wide IG



The Positive Impact of an IG Program

STRATEGIC TARGETS

- Quality outcomes
- Reduced compliance risks
- Savings targets
- Achieve margin improvement

OPERATIONAL EFFICIENCY

- Enhance labor efficiency/ productivity
- Reduce redundancies/ rework
- Improve workflow

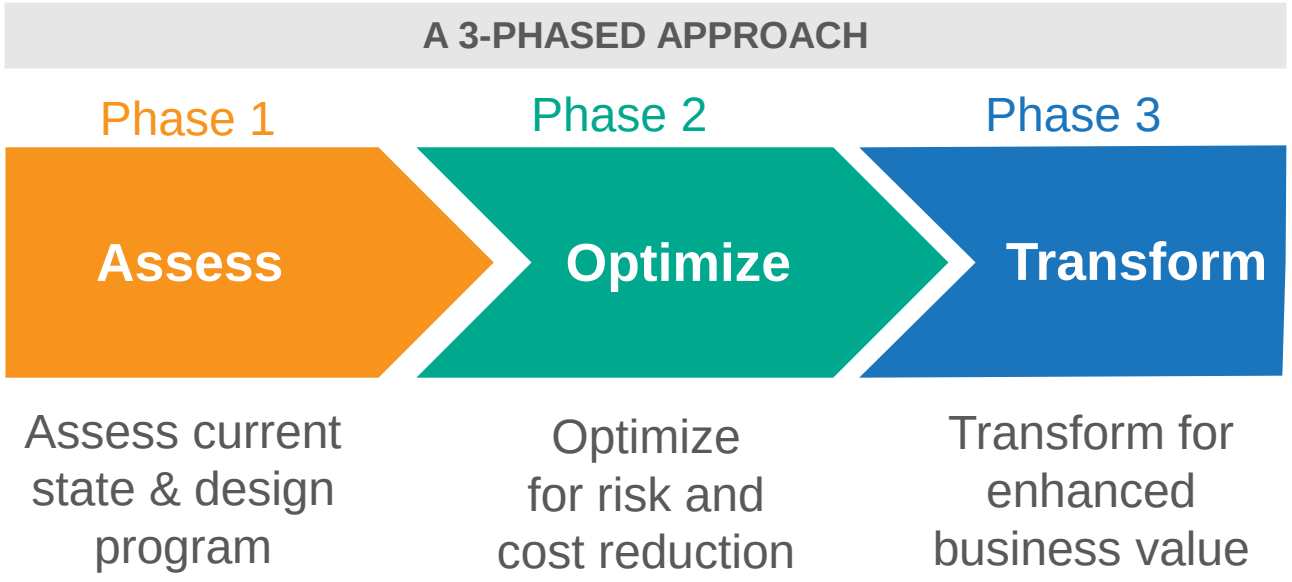
COMPLIANCE RISKS

- Advance proactive data and information management
- Improve defensible disposition
- Minimize breach & cybersecurity risks

MERGERS & ACQUISITIONS

- Integrate systems
- Address data discrepancies/ source of truth defined
- Integrate hospitals, physician practices, clinics, & other business units
- Manage cultural shifts

A Multi-Phased Approach to Defensible Disposition



Defensible disposition is dependent on a solid policy around information/data/IT assets retention and disposition

Breaking It Down – Manageable Next Steps

Phase 1 – Assess

- ✓ Develop a record retention policy & schedule or refresh your current one
- ✓ Ensure it is manageable
- ✓ Educate across the workforce, including location of policy/schedule & establish accountabilities

Phase 2 – Optimize

- ✓ Look for a record retention policy & schedule
- ✓ Evaluate it for currency & thoroughness
- ✓ Ask staff if they are aware of a retention policy/schedule & where it is located

Phase 3 – Transform

- ✓ Develop an enterprise-wide plan for defensible disposition
- ✓ Put policy into action
- ✓ Monitor & report metrics & continuously improve

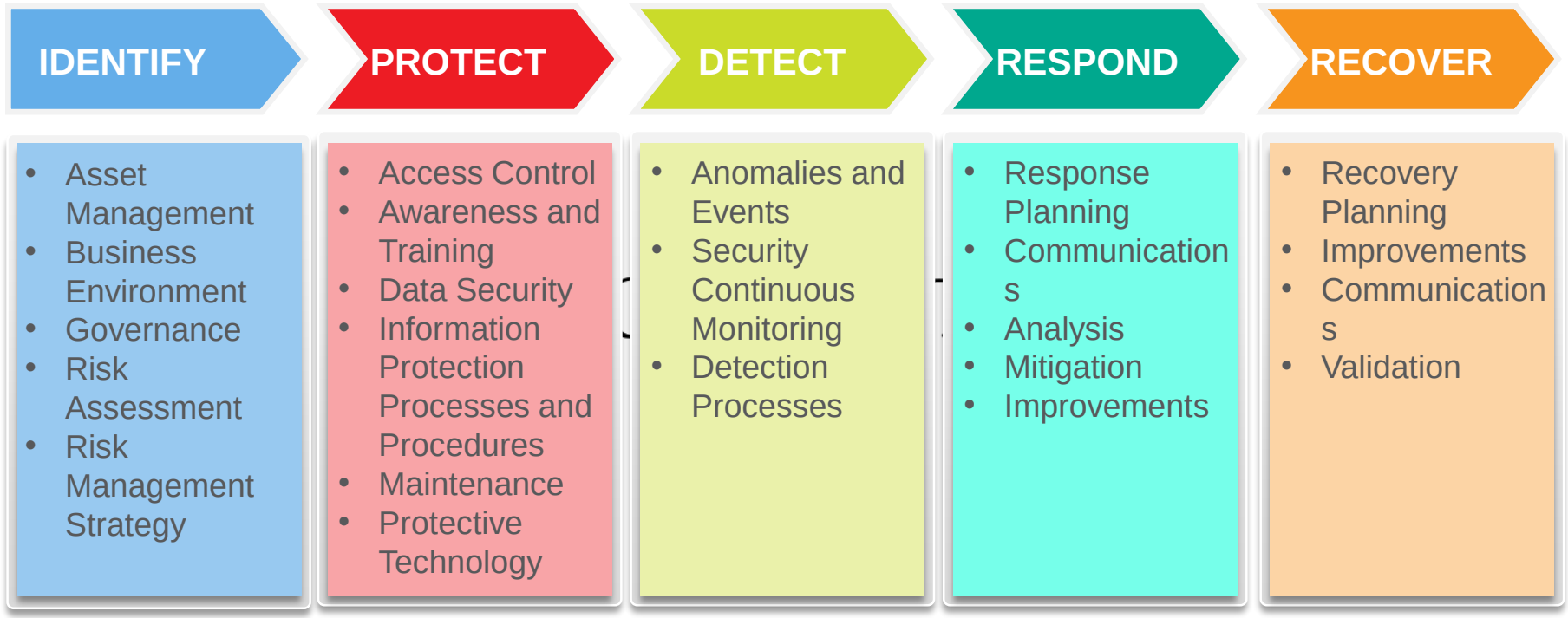
Establishing a Good Offense

1. **ASSESS** current state
2. **OPTIMIZE** for risk and cost reduction
3. **TRANSFORM** for long term, enhanced business value

NIST Cybersecurity Framework

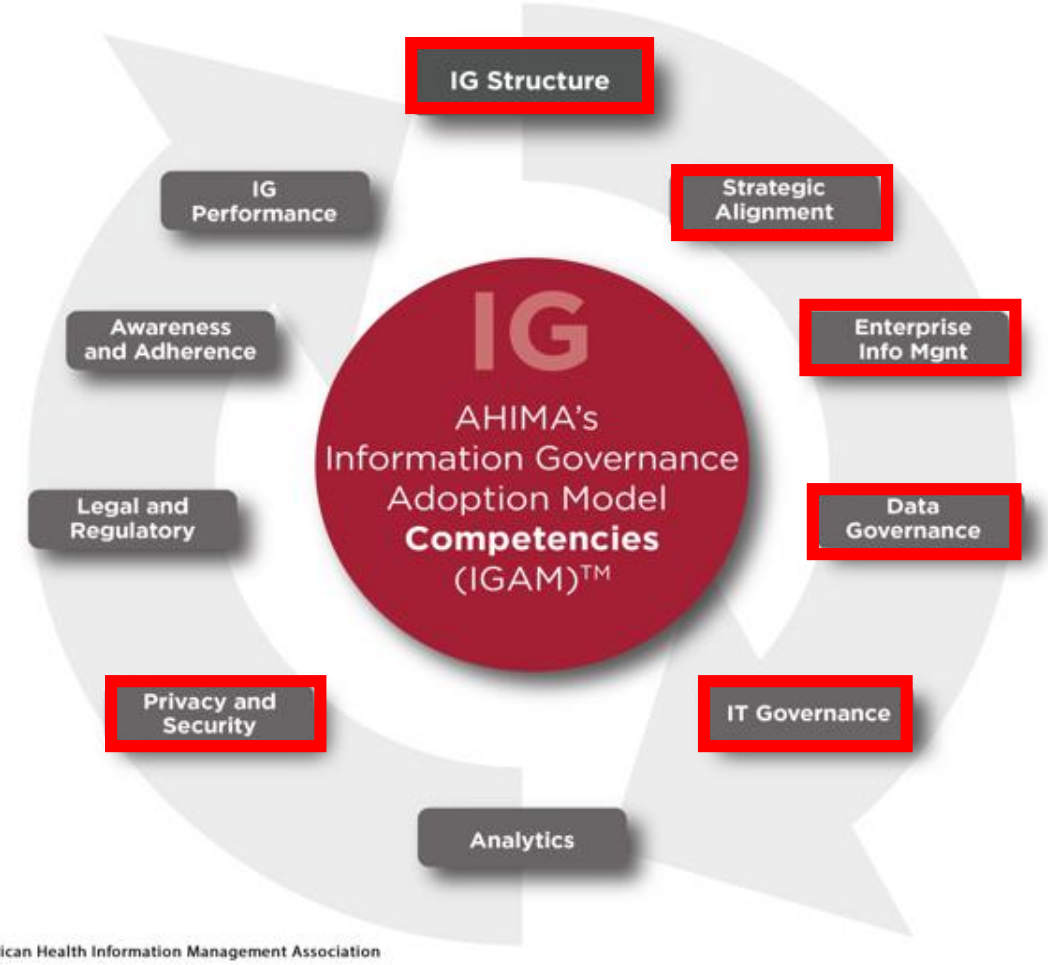
Credit: N. Hanacek/NIST

IRON MOUNTAIN®


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

- Governance
- Asset Management
- Business Environment
- Risk Assessment
- Risk Management Strategy



Clinical systems	Consumer and patient health systems	Core transaction systems	Decision support systems (DSS and CPOE)
Electronic medical record (EMR)	Managed care systems	Medical management systems	Materials management systems
Clinical data repository	Patient relationship management	Imaging	Integrated medical devices
Clinical trials systems	Telemedicine systems	Workflow technologies	Workforce enabling technologies

Security Risk Assessment

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires that covered entities and its business associates conduct a risk assessment of their healthcare organization. A risk assessment helps your organization ensure it is compliant with HIPAA's administrative, physical, and technical safeguards. A risk assessment also helps reveal areas where your organization's protected health information (PHI) could be at risk. Watch the Security Risk Analysis video to learn more about the assessment process and how it benefits your organization or visit the Office for Civil Rights' official guidance.

Read the HHS Press Release.

Download the SRAT event files from the April 29 Webinar [ZIP - 4 MB]

Security Risk Assessment Tool
ONC, in collaboration with the HHS Office for Civil Rights (OCR) and the HHS Office of the General Counsel (OGC), developed a downloadable Security Risk Assessment Tool (SRA Tool) to help guide you through the process.

Download Tool

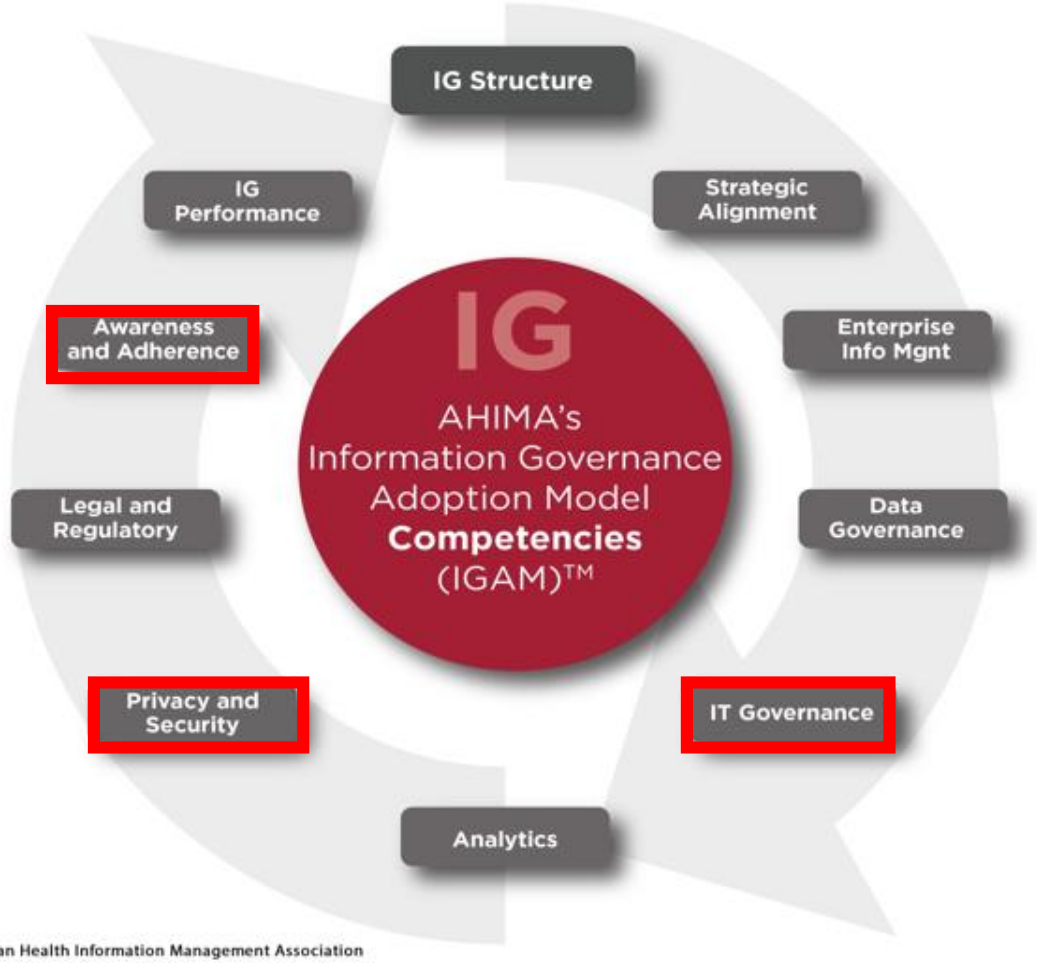
SRA Tool Videos
Watch videos on what a risk assessment may involve, and learn how to use the SRA Tool by watching the SRA Tool Tutorial video.

Watch Videos

https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment

PROTECT

- Access Control
- Data Security
- Information Protection Processes and Procedures
- Maintenance
- Protective Technology
- Awareness and Training



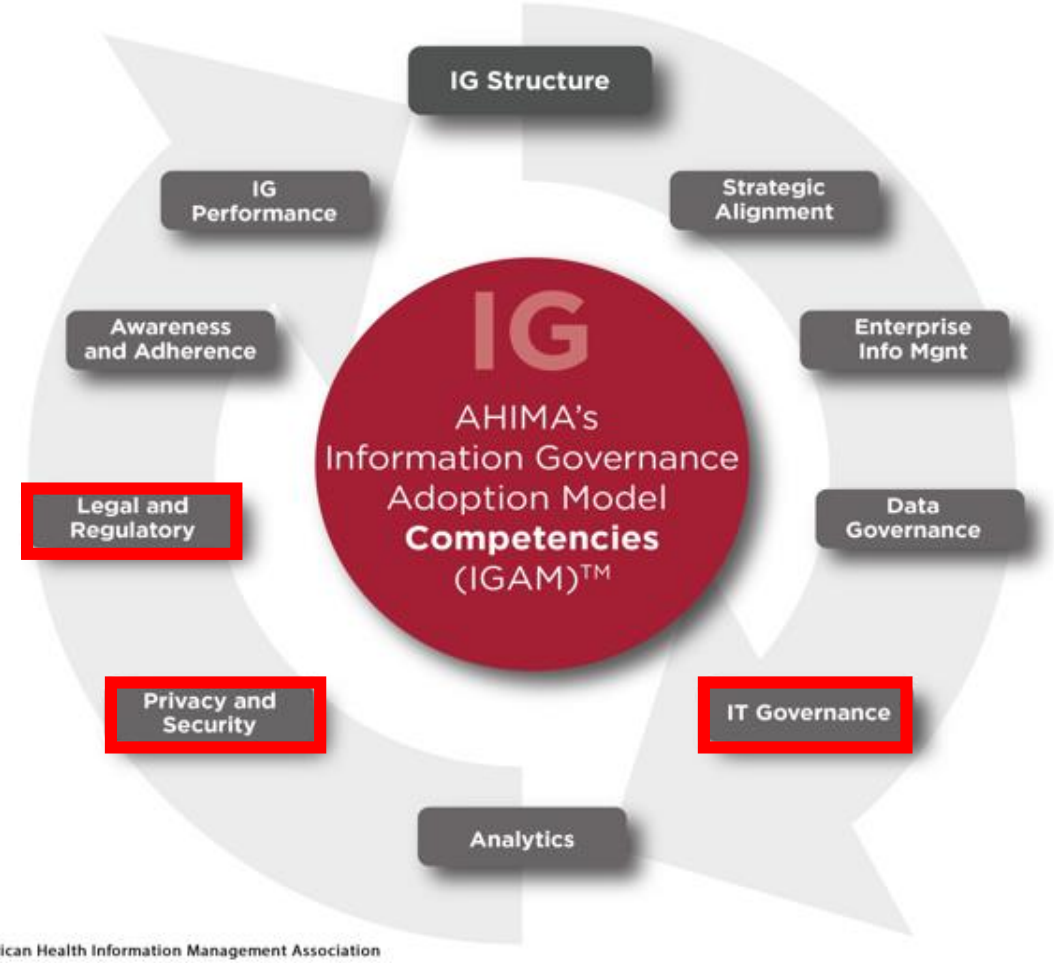
Steps to Protect

- User Password Policies
- Appropriate Access and Use Policies
- Information Sharing Policies and Procedures
- Mobile Device Policies
- Social Media Policies
- eMail Policies
- Advanced Controls, such as encryption, intrusion detection
- Data Center Locations and Security
- Cloud Storage

IRON MOUNTAIN®

DETECT

- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes



RESPOND

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

RECOVER

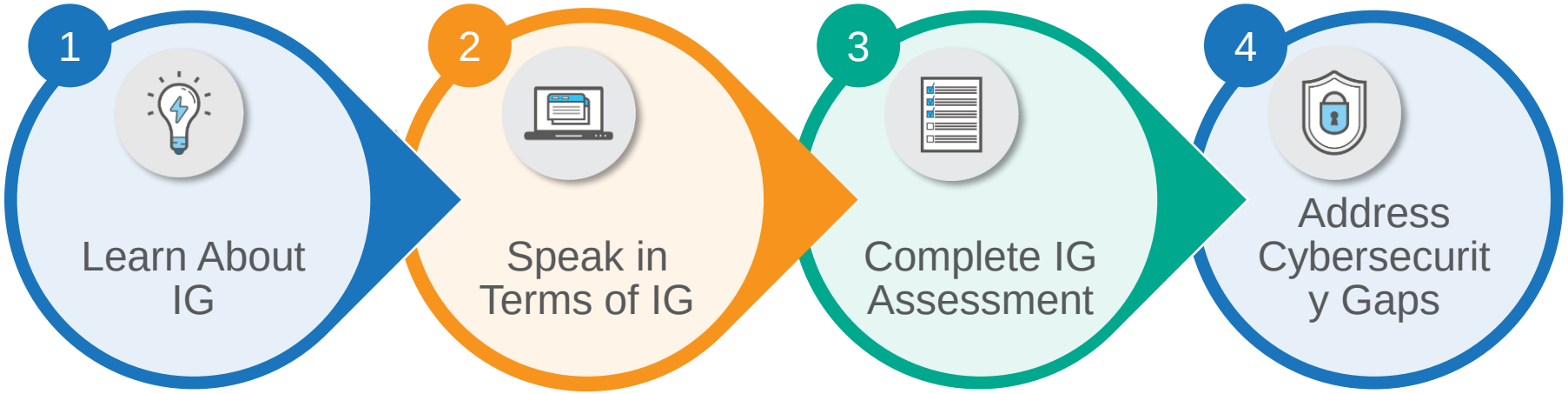
- Recovery Planning
- Improvements
- Communications
- Validation

IG - The Wrapper Around Cybersecurity

An IG Program

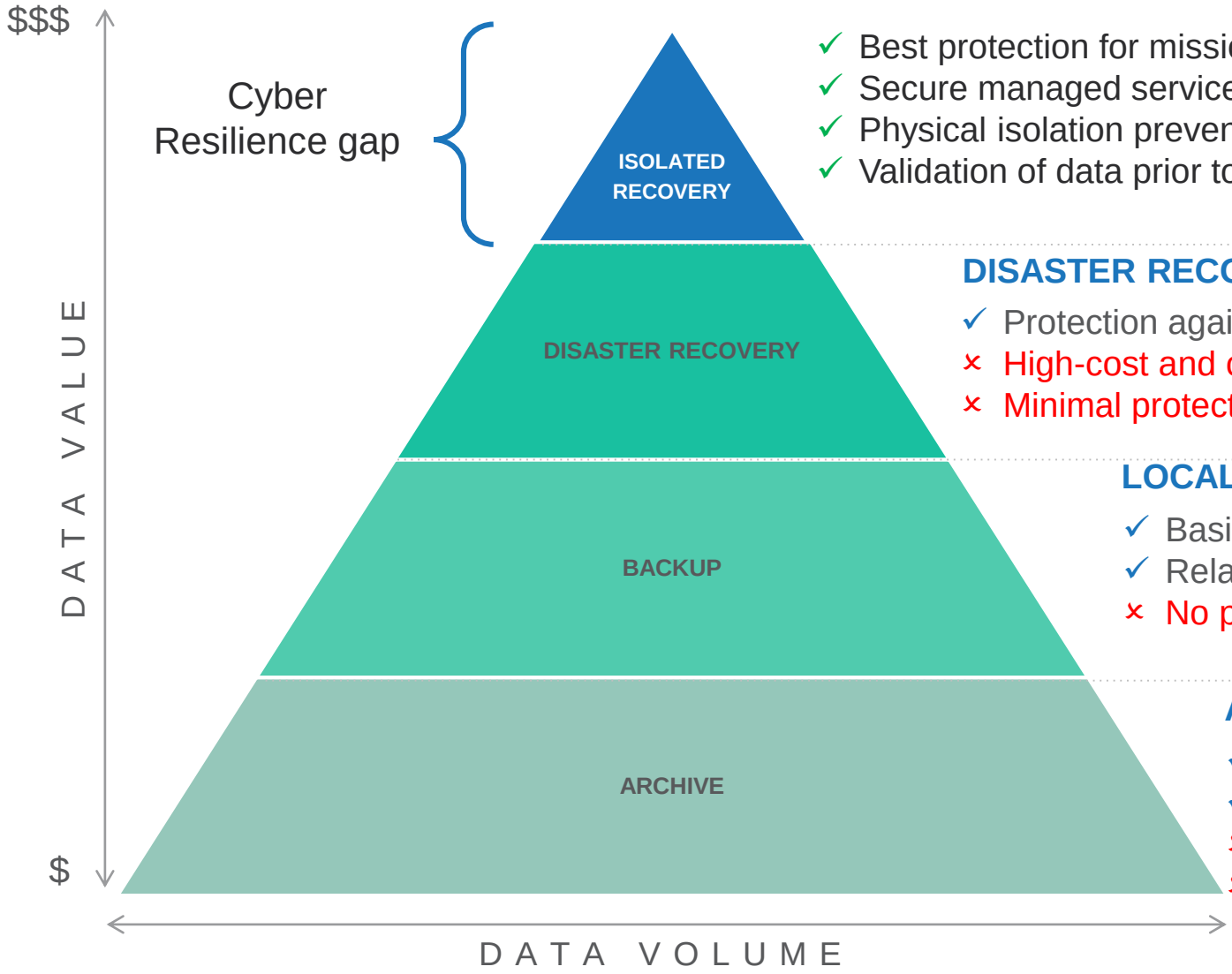
- Ensures well vetted, defined and documented policies, procedures, and processes
- Guarantees key stakeholder engagement and input
- Addresses all decisions about data and information, including the security of electronic data, across the organization in its entirety
- Aligns information decisions and protections with the organization's strategic goals and objectives

What should you do?



IS YOUR MOST CRITICAL DATA REALLY PROTECTED & RECOVERABLE?

The Traditional Pyramid of Protection



ISOLATED RECOVERY

- ✓ Best protection for mission critical data against cyberattack
- ✓ Secure managed service protects from internal attacks
- ✓ Physical isolation prevents network access, ensures rapid recoverability
- ✓ 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 protection & recovery for production & large data sets
- ✓ Relatively fast, low-cost recovery
- × No protection from data loss or corruption from cyber attack

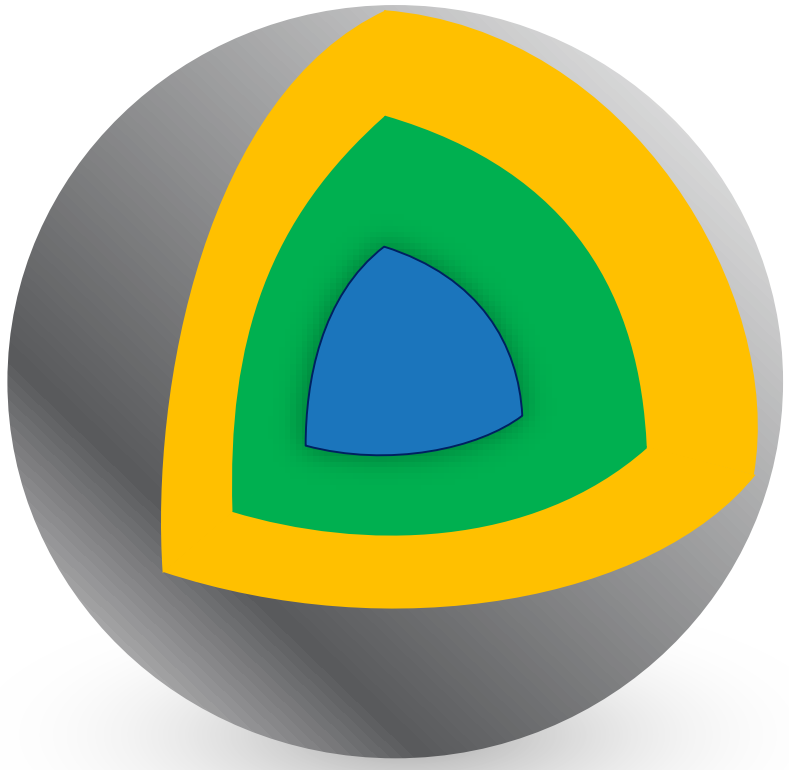
ARCHIVE

- ✓ Long-term protection & retention historical or “cold” data sets
- ✓ Low-cost option to meet compliance and regulatory mandates
- × Slow recovery of mission-critical data
- × No protection from data loss or corruption from cyber attack

Cyber Protection Expert Guidance

- Cyber security experts and regulators recommend "…***physical segregation of networks….and regular testing of critical data recovery procedures***"
- Address the threat of **insider attacks** with managed services
- **Remote data protection** through automated, randomized network disconnection to reduce risk of planned attacks
- **Encryption of data** in-flight and at-rest with key management by customer
- Dedicated secure isolated environment for **offline data testing & validation**
- Understand the **full TCO of managed services** including egress fees, recovery procedures and additional "hidden costs"

Modern Cyber Resilience for Critical Data



BEST

Cloud Cyber Resilience Services (CPR for Data Domain)

- Ultra-secure cloud-based managed service to protect vital digital assets
- Network and physical isolation of CPR Vault in Iron Cloud data centers
- Iron Cloud Cleanroom for off-line isolated analytics and recovery testing
- Rapid, assured restoration to get business-critical systems running again

BETTER

Cloud Disaster Recovery Services

- Secure Immutable Cloud-based storage
- Reduced CAPEX, Lower TCO for better DR
- Industry-leading Resilience, 3-site Geo-redundancy

GOOD

Cloud Archive Services

- Secure Immutable Cloud-based storage
- Industry-leading Security, Resilience and Availability
- Dedicated, Private & encryption in-flight and at-rest

Cyber Resilience Key Takeaways

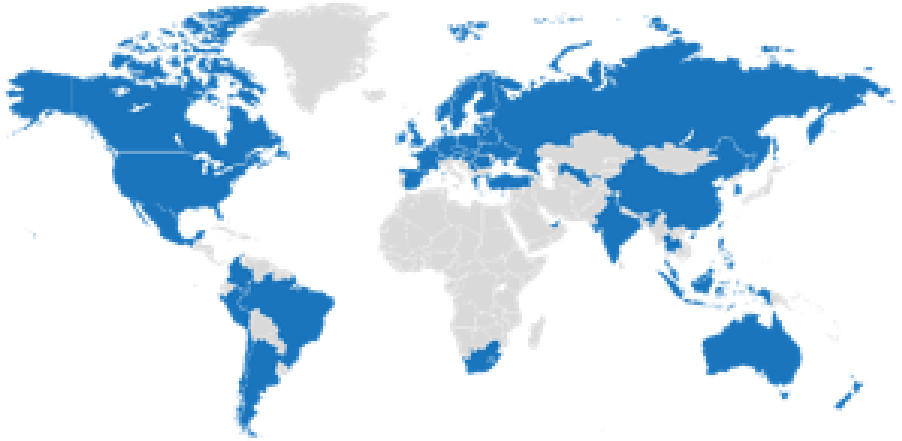
- Cyber Resilience helps mitigate unplanned operational downtime, data loss, & destruction.
- Cyber resilience has been elevated to the executive level, prompting senior level groups charged with designing and testing systemwifde recovery plans.
- Isolated recovery is a critical component of a layered data protection plan.
- To be effective, recovery plans should be updated and tested regularly.
- Best practices for Healthcare include the use of dedicated private networks, encryption of in-flight and at rest data and physical isoloation of critical data from the network

Questions?

JOHN MOYNIHAN, CPHIMS
HEALTHCARE BUSINESS DEVELOPMENT
IRON MOUNTAIN

+1 978-954-8361 – mobile
John.Moynihan@ironmountain.com
www.IronMountain.com/heatlhcare

Iron Mountain



54 COUNTRIES | **6 CONTINENTS**

- **Over 68 Exabytes** of customer data under management
- **89 million** pieces of media stored in highly secure data protection vaults
- **675 million** cubic feet of hardcopy records stored
- **S&P 500 Member** $15B Enterprise Value
- **65+ years** of protecting, preserving and managing critical information and assets
- **Over 850 million** patient records
- **Over 1 billion** medical images

225,000+	95%	90MM	1,400+	25,000+
Customers	Fortune 1000 companies	SF of secure real estate in 54 countries	Facilities	Employees

IRON MOUNTAIN®