Health and Life Sciences Security Readiness Program

Global Industry Report

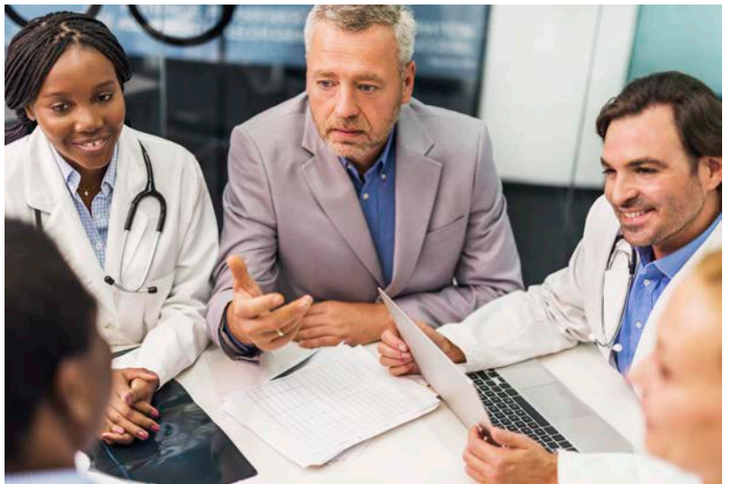
(Global Scope, N=150)

Contents

Executive Summary

Reported On Monday, 16 Oct 2017 15:24 PDT

Comparison Global Scope, N=150



Breaches are the top privacy and security concern in health and life sciences organizations, according to global research conducted by Intel in 2016. This report highlights industry level, aggregate, anonymous results of Security Readiness Workshops conducted with a specific group of health and life sciences organizations, and subsequent analysis of security maturity, priorities, and capabilities. This program is running throughout 2017, led by Intel in collaboration with a broad range of partners working in the health and life sciences industry globally. We welcome your feedback both on the program in general and on this report.

For an introduction to this program see Introduction to the Security Readiness Program.

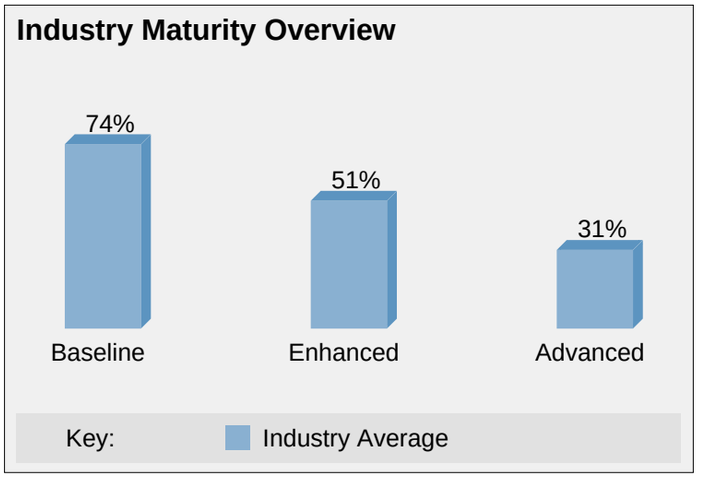
This health and life sciences security readiness program involves a high-level survey of potential security issues. It is intended to inform participants about where they stand on selected security practices in relation to other similar participants in this study. It is not intended to replace participants' other compliance or security due diligence activities. It is also different from and complementary to risk assessments that are required by several regulations and security standards. It provides an opportunity to look at gaps and next steps that can be taken to improve security posture. Improvements to security based on this assessment may also help with compliance with privacy and security regulations, data protection laws, and standards. Please consult publicly available information on your applicable regulations, laws and standards for further information.

For help interpreting this report see Overview of a Security Readiness Industry Report.

Thank you for your interest in the Intel® Health and Life Sciences Security Readiness Program. We welcome your feedback on the overall process, and on this report. For further information about this program, please see the Intel Security Readiness Program website.

1. Maturity Overview

The maturity is shown as the percentage of security capabilities that the benchmark set have implemented in the Baseline, Enhanced, and Advanced maturity levels. As the security posture for the benchmark set improves, the assessment at each of these maturity levels will approach 100%. These are high-level results for a broad overview of the maturity of the benchmark set. See subsequent sections of this report for details on security priorities, readiness, and capabilities of the benchmark set. See Maturity Details for a detailed view of the level of implementation of each of the 42 security capabilities.



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

2. Priorities and Readiness

These results show the priority, or level of concern, and readiness averages for the benchmark set across 8 breach types. Readiness for each breach type is the percentage of relevant security capabilities the benchmark set currently has implemented. Statistics for readiness show the minimum, average, maximum, and standard deviation scores for the benchmark set. Click on the associated breach type link for more details.

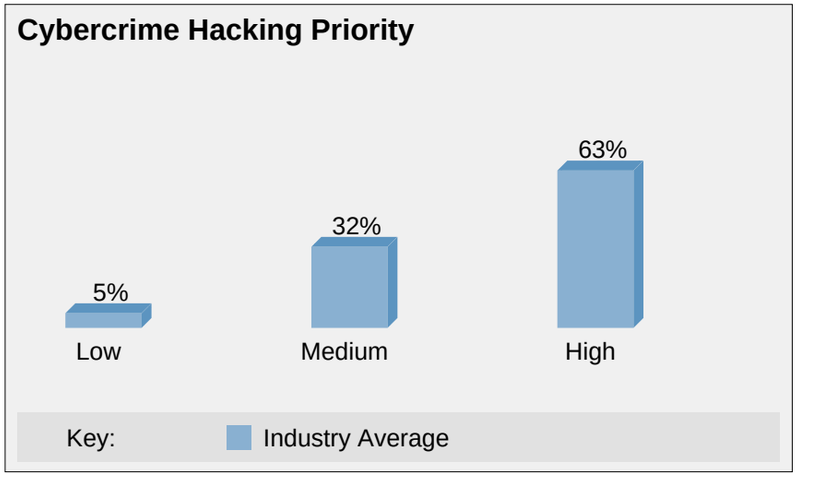
Health and Life Sciences Industry Priorities and Readiness

#	Breach Type	Average Priority	Readiness			
			Min	Mean	Max	Std Dev
2.1	Cybercrime Hacking	Medium / High (79%)	21%	58%	93%	15%
2.2	Loss or Theft of Mobile Device or Media	Medium (51%)	14%	51%	90%	15%
2.3	Insider Accidents or Workarounds	Medium / High (65%)	15%	54%	90%	16%
2.4	Business Associates	Medium (51%)	6%	62%	100%	21%
2.5	Malicious Insiders or Fraud	Medium (45%)	15%	52%	89%	15%
2.6	Insider Snooping	Medium (49%)	13%	51%	89%	16%
2.7	Improper Disposal	Low / Medium (35%)	0%	49%	92%	18%
2.8	Ransomware	High (86%)	17%	60%	91%	16%

Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

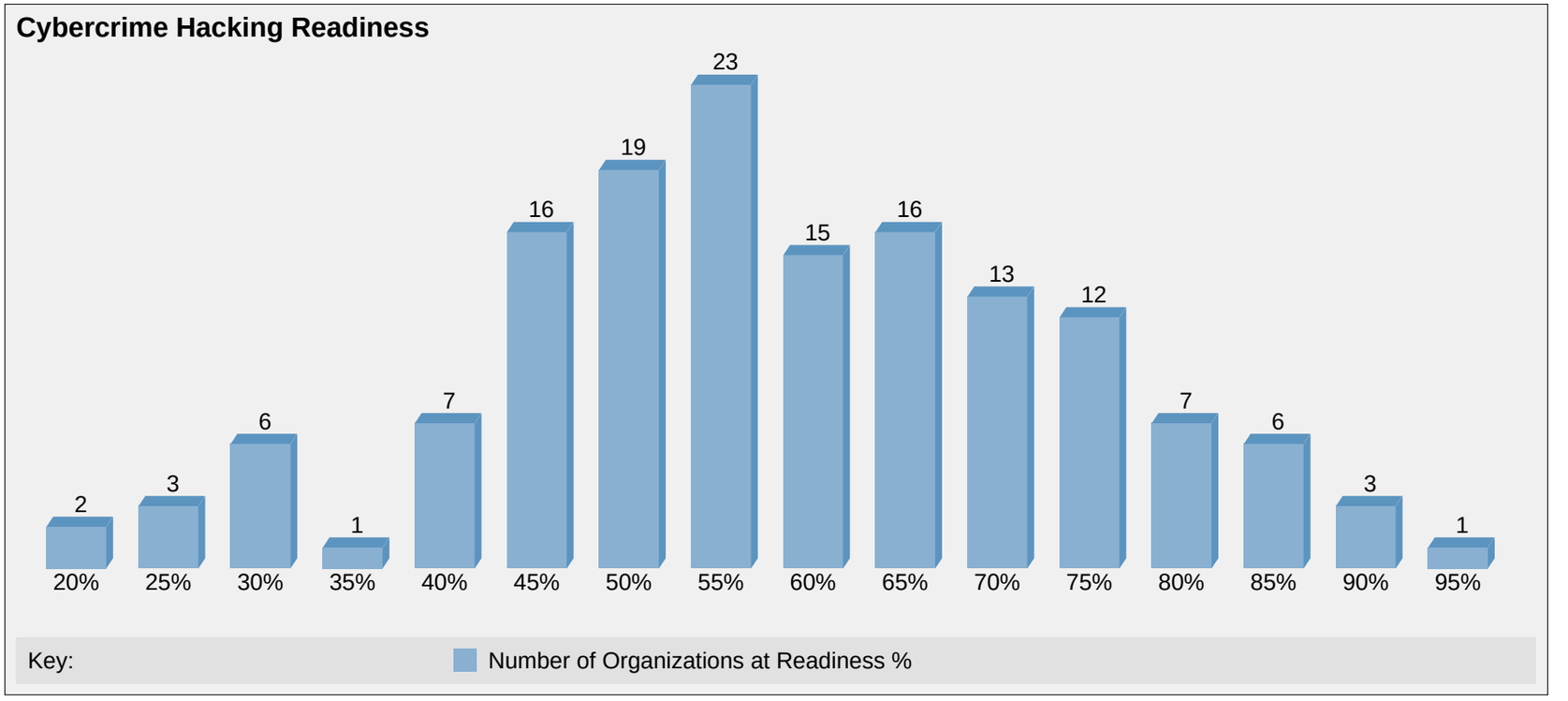
2.1 Cybercrime Hacking

In this type of breach, an external hacker accesses your organization's network and obtains unauthorized access to sensitive information. A common example of this type of breach starts with the hacker spear phishing a worker in your organization, resulting in that worker clicking on a malicious link, which leads to drive-by download of malware. The malware then proliferates inside your intranet and key-logs the database administrator database credentials, at which point it turns into a bot that logs into your database containing sensitive information and exfiltrates this data “low and slow” to evade detection.



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

The following graph shows the distribution of organizations in terms of readiness for Cybercrime Hacking breaches. Horizontal axis percentages reflect the readiness for this type of breach in terms of the percentage of relevant capabilities implemented. The height of each bar is proportional to the number of organizations at that percentage of readiness.



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

The capabilities below are relevant to mitigating risk of Cybercrime Hacking type breaches. The percentage next to each capability indicates the current state of implementation of the capability in the industry.

Cybercrime Hacking Maturity Details - Health and Life Sciences Industry

Baseline

- 77% Policy
- 72% Risk Assessment
- 60% Audit and Compliance
- 71% User Awareness Training
- 93% Anti-Malware
- 82% Identity and Access Management, Single-Factor Access Control
- 92% Firewall
- 89% Email Gateway
- 85% Web Gateway
- 73% Vulnerability Management, Patching
- 63% Security Incident Response Plan
- 89% Backup and Restore

Enhanced

- 67% Penetration Testing, Vulnerability Scanning
- 29% Network Data Loss Prevention (Discovery Mode)
- 43% Multi-Factor Authentication with Timeout
- 83% Secure Remote Administration
- 67% Network Segmentation
- 63% Network Intrusion Prevention System

Advanced

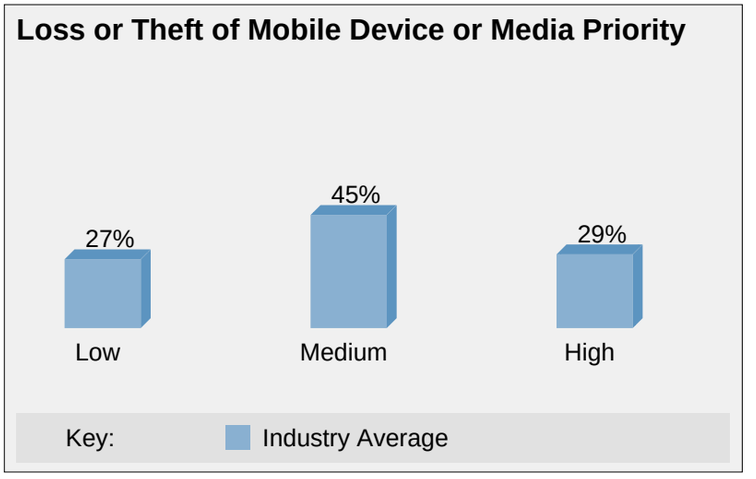
- 20% Network Data Loss Prevention (Prevention Mode)
- 29% Database Activity Monitoring
- 42% Digital Forensics
- 41% Security Information and Event Management
- 50% Threat Intelligence
- 13% Multi-Factor Authentication with Walk-Away Lock
- 18% Server Application Whitelisting
- 34% De-Identification / Anonymization
- 12% Tokenization
- 68% Business Continuity and Disaster Recovery

(⊕ = most have it, ~ = some have it, ⊖ = few have it)

Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

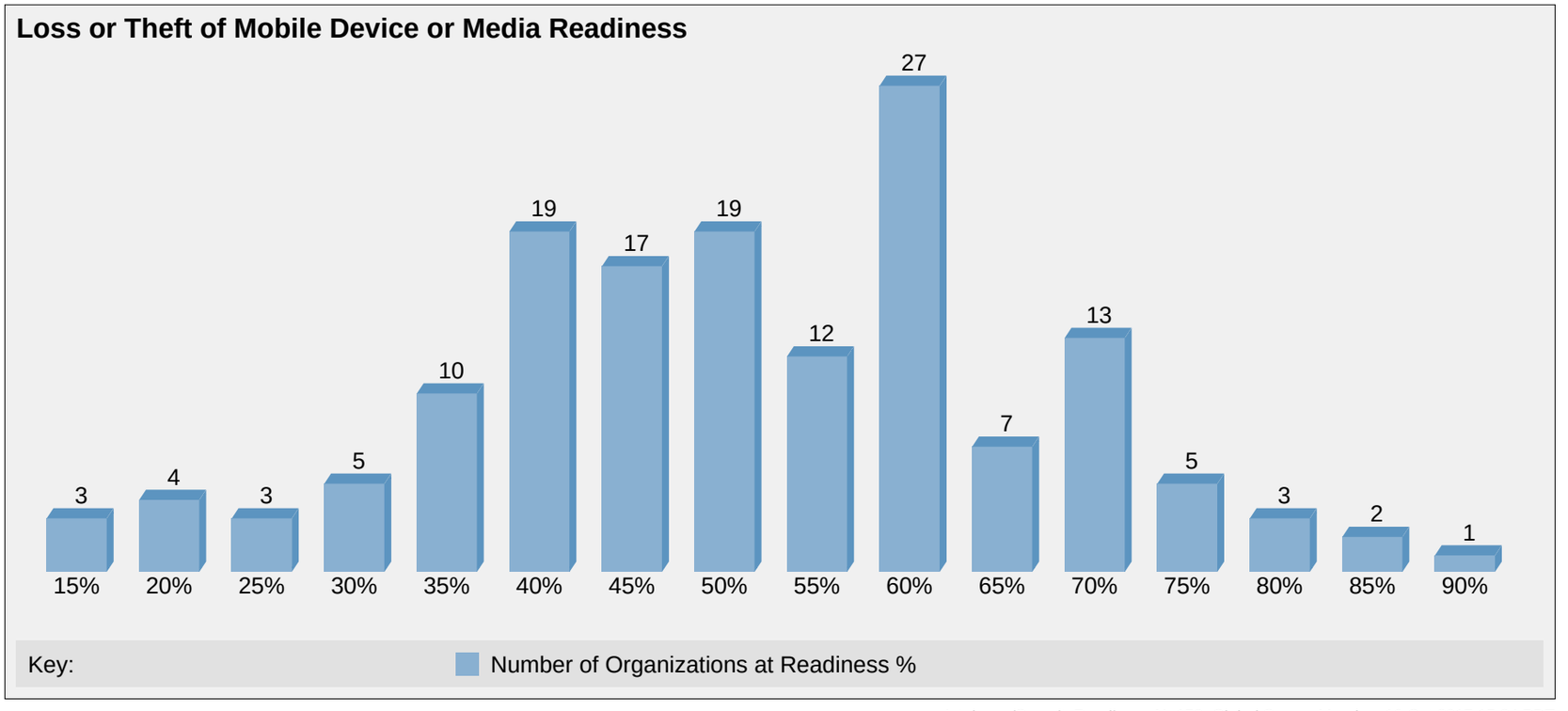
2.2 Loss or Theft of Mobile Device or Media

In this type of breach, a worker either loses or has stolen a mobile device or media containing sensitive information, resulting in potential unauthorized access to that data and a breach. A common example of this is loss of a smartphone, tablet, or laptop containing sensitive information.



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

The following graph shows the distribution of organizations in terms of readiness for Loss or Theft of Mobile Device or Media breaches. Horizontal axis percentages reflect the readiness for this type of breach in terms of the percentage of relevant capabilities implemented. The height of each bar is proportional to the number of organizations at that percentage of readiness.



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

The capabilities below are relevant to mitigating risk of Loss or Theft of Mobile Device or Media type breaches. The percentage next to each capability indicates the current state of implementation of the capability in the industry.

Loss or Theft of Mobile Device or Media Maturity Details - Health and Life Sciences Industry

Baseline

- 77% Policy
- 72% Risk Assessment
- 60% Audit and Compliance
- 71% User Awareness Training
- 63% Endpoint Device Encryption
- 62% Mobile Device Management
- 20% Endpoint Data Loss Prevention (Discovery Mode)
- 82% Identity and Access Management, Single-Factor Access Control
- 73% Vulnerability Management, Patching
- 63% Security Incident Response Plan
- 86% Secure Disposal
- 89% Backup and Restore

Enhanced

- 31% Client Solid State Drive (Encrypted)
- 51% Anti-Theft: Remote Locate, Lock, Wipe
- 43% Multi-Factor Authentication with Timeout
- 83% Secure Remote Administration
- 15% Policy-Based Encryption for Files and Folders
- 41% Server / Database / Backup Encryption
- 64% Virtualization

Advanced

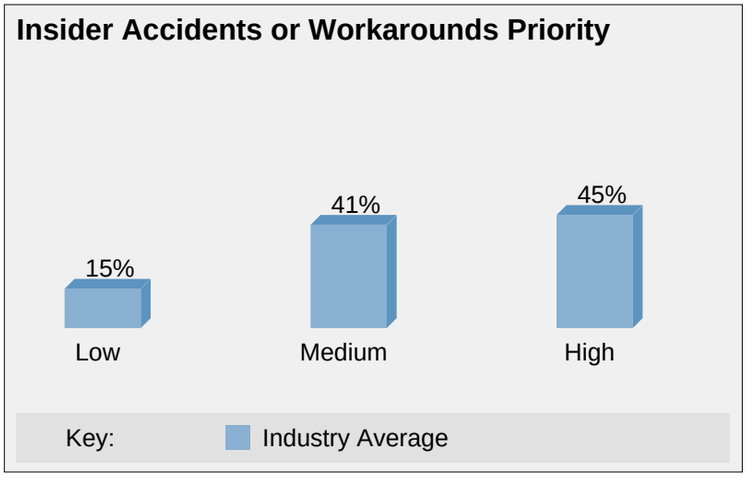
- 15% Server Solid State Drive (Encrypted)
- 42% Digital Forensics
- 13% Multi-Factor Authentication with Walk-Away Lock
- 24% Client Application Whitelisting
- 34% De-Identification / Anonymization
- 12% Tokenization

(⊕ = most have it, ~ = some have it, ⊖ = few have it)

Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

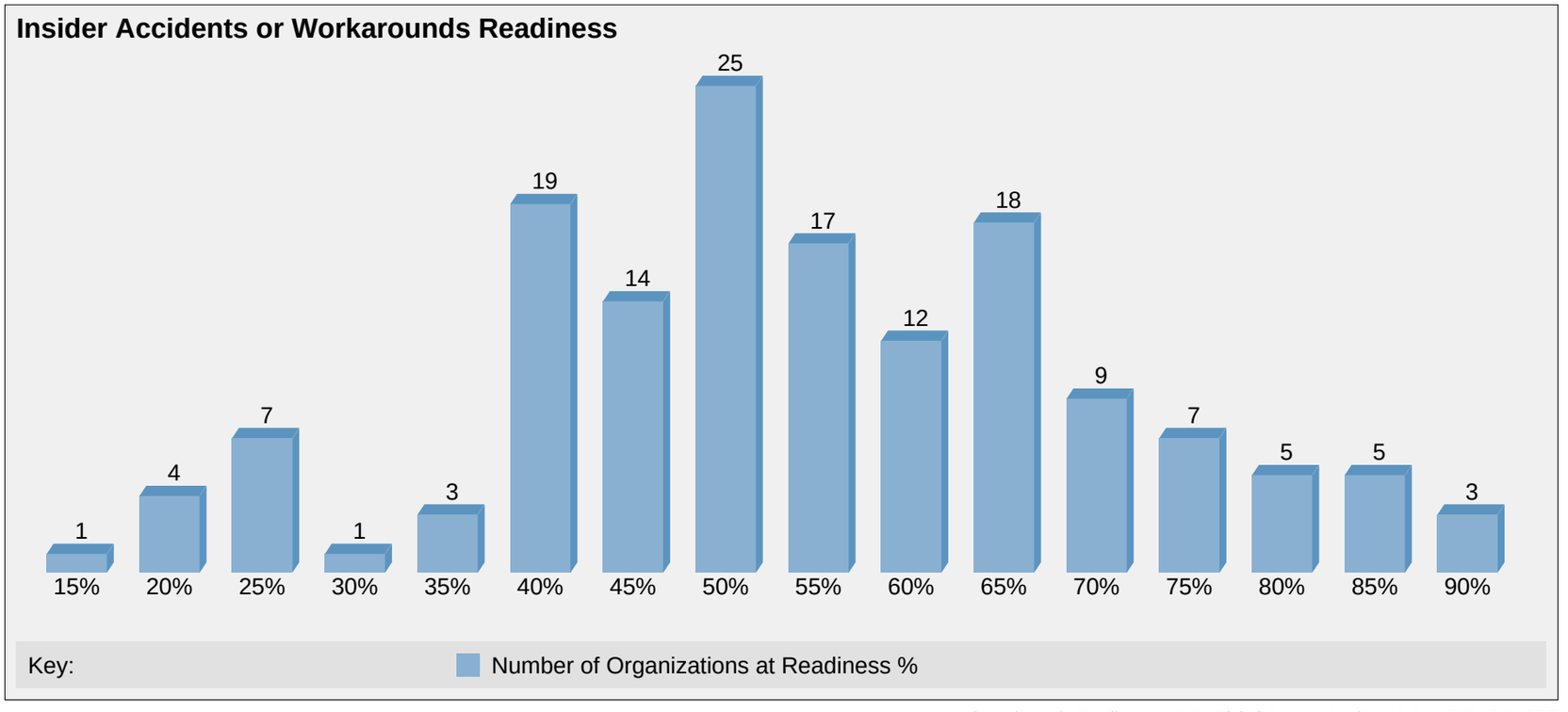
2.3 Insider Accidents or Workarounds

In this type of breach, a worker performs an action that results in unauthorized access to sensitive information. A common example of this type of breach involves a worker emailing unsecured sensitive information, resulting in potential unauthorized access to this information and a breach. This type of breach can involve the use of either corporate or BYOD devices by workers.



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

The following graph shows the distribution of organizations in terms of readiness for Insider Accidents or Workarounds breaches. Horizontal axis percentages reflect the readiness for this type of breach in terms of the percentage of relevant capabilities implemented. The height of each bar is proportional to the number of organizations at that percentage of readiness.



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

The capabilities below are relevant to mitigating risk of Insider Accidents or Workarounds type breaches. The percentage next to each capability indicates the current state of implementation of the capability in the industry.

Insider Accidents or Workarounds Maturity Details - Health and Life Sciences Industry

Baseline

- 77% Policy
- 72% Risk Assessment
- 60% Audit and Compliance
- 71% User Awareness Training
- 62% Mobile Device Management
- 20% Endpoint Data Loss Prevention (Discovery Mode)
- 93% Anti-Malware
- 89% Email Gateway
- 85% Web Gateway
- 73% Vulnerability Management, Patching
- 63% Security Incident Response Plan
- 86% Secure Disposal

Enhanced

- 54% Device Control
- 17% Endpoint Data Loss Prevention (Prevention Mode)
- 29% Network Data Loss Prevention (Discovery Mode)
- 83% Secure Remote Administration
- 15% Policy-Based Encryption for Files and Folders
- 67% Network Segmentation

Advanced

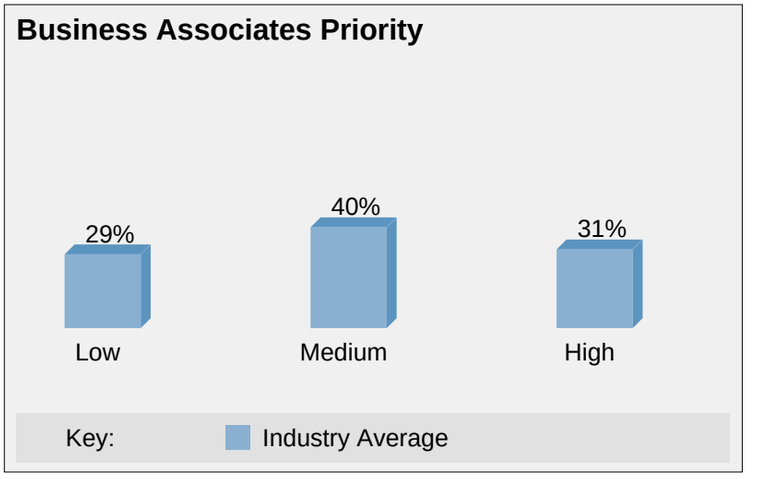
- 20% Network Data Loss Prevention (Prevention Mode)
- 42% Digital Forensics
- 50% Threat Intelligence
- 24% Client Application Whitelisting
- 34% De-Identification / Anonymization
- 12% Tokenization

(⊕ = most have it, ∿ = some have it, ⊖ = few have it)

Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

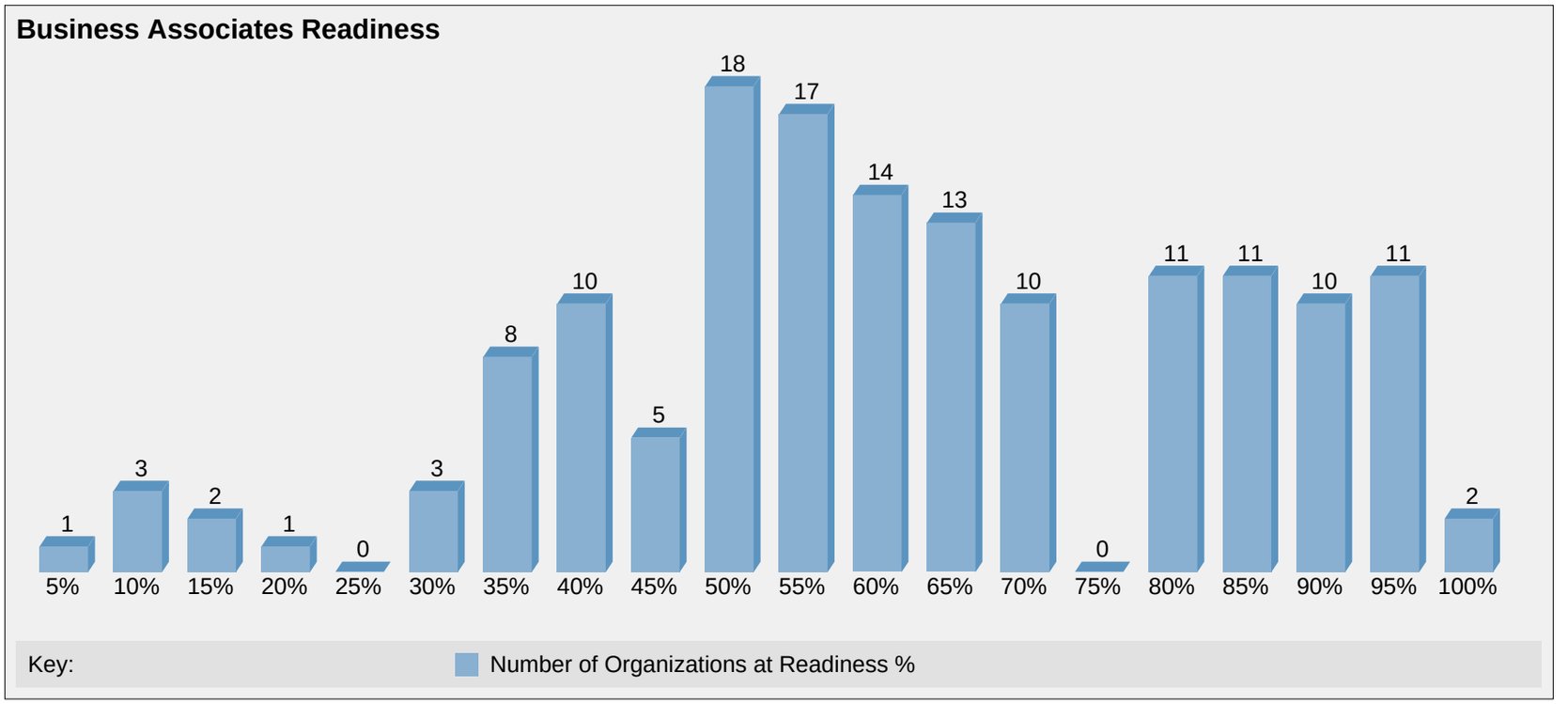
2.4 Business Associates

In this type of breach, a third-party organization contracted by your organization experiences a breach event involving unauthorized access to sensitive information. In this case the sensitive information impacted originates from your organization and was previously shared for the purpose of the third-party organization fulfilling its contractual obligations. In the United States these entities are known as Business Associates, while in Europe they are typically referred to as Data Processors.



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

The following graph shows the distribution of organizations in terms of readiness for Business Associates breaches. Horizontal axis percentages reflect the readiness for this type of breach in terms of the percentage of relevant capabilities implemented. The height of each bar is proportional to the number of organizations at that percentage of readiness.



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

The capabilities below are relevant to mitigating risk of Business Associates type breaches. The percentage next to each capability indicates the current state of implementation of the capability in the industry.

Business Associates Maturity Details - Health and Life Sciences Industry

Baseline

- 77% Policy
- 72% Risk Assessment
- 60% Audit and Compliance
- 71% User Awareness Training
- 63% Security Incident Response Plan

Enhanced

- 86% Business Associate Agreements

Advanced

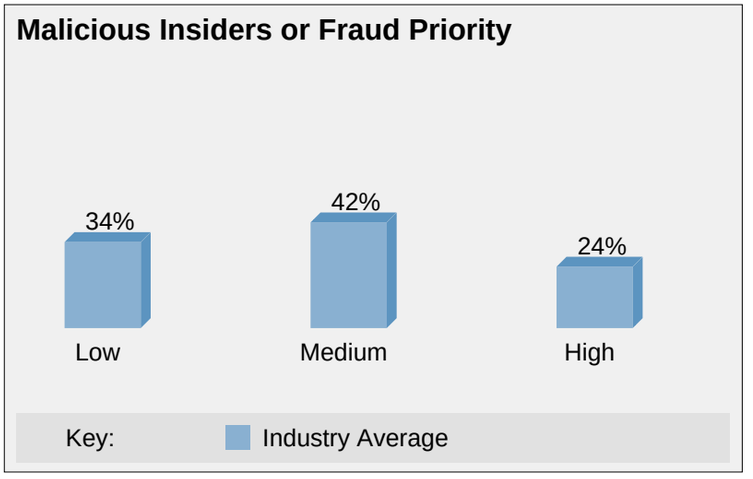
- 42% Digital Forensics
- 50% Threat Intelligence
- 34% De-Identification / Anonymization

(⊕ = most have it, ~ = some have it, ⊖ = few have it)

Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

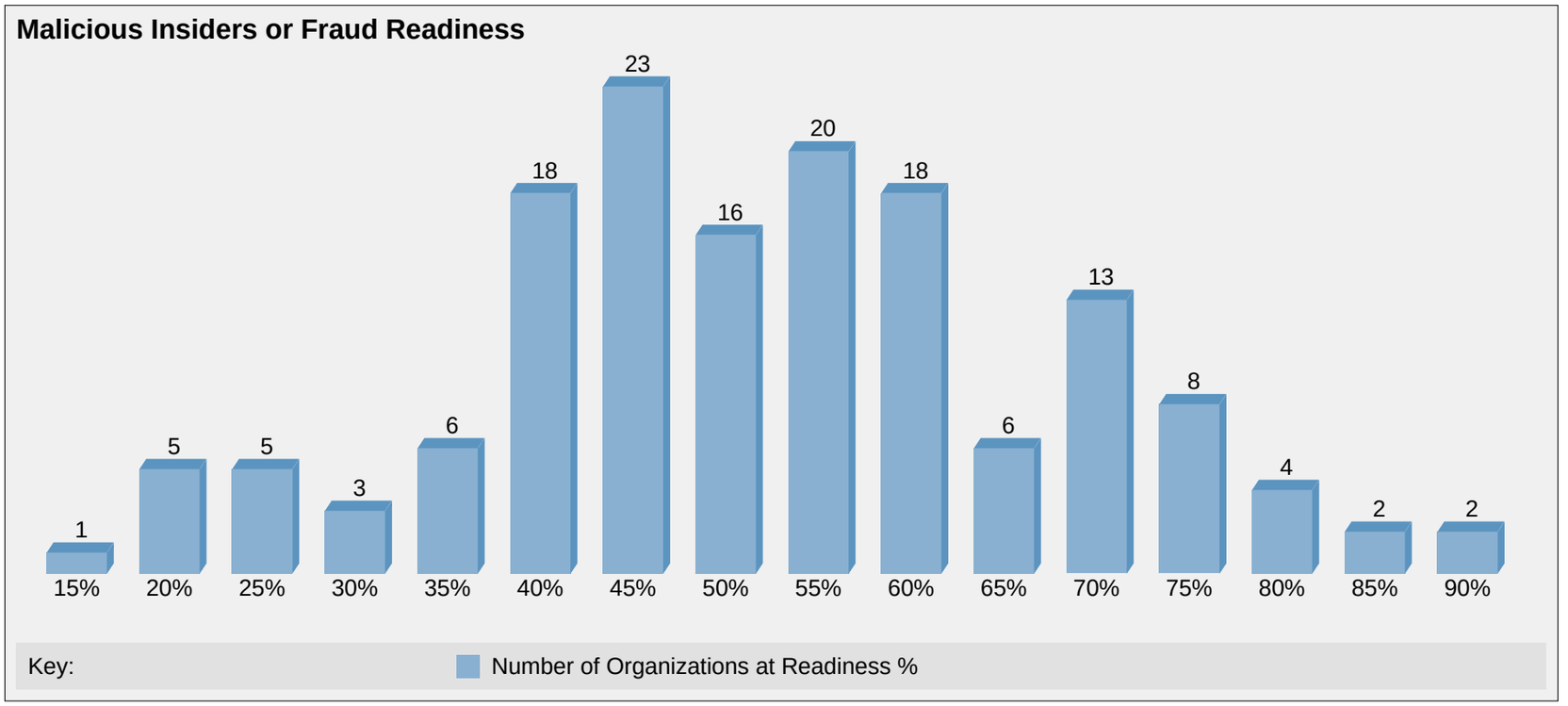
2.5 Malicious Insiders or Fraud

In this type of breach, a worker performs a malicious action that results in unauthorized access to sensitive information. This could be a disgruntled worker or one attempting to commit fraud.



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

The following graph shows the distribution of organizations in terms of readiness for Malicious Insiders or Fraud breaches. Horizontal axis percentages reflect the readiness for this type of breach in terms of the percentage of relevant capabilities implemented. The height of each bar is proportional to the number of organizations at that percentage of readiness.



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

The capabilities below are relevant to mitigating risk of Malicious Insiders or Fraud type breaches. The percentage next to each capability indicates the current state of implementation of the capability in the industry.

Malicious Insiders or Fraud Maturity Details - Health and Life Sciences Industry

Baseline

- 77% Policy
- 72% Risk Assessment
- 60% Audit and Compliance
- 71% User Awareness Training
- 63% Endpoint Device Encryption
- 62% Mobile Device Management
- 20% Endpoint Data Loss Prevention (Discovery Mode)
- 82% Identity and Access Management, Single-Factor Access Control
- 92% Firewall
- 89% Email Gateway
- 85% Web Gateway
- 73% Vulnerability Management, Patching
- 63% Security Incident Response Plan
- 86% Secure Disposal
- 89% Backup and Restore

Enhanced

- 54% Device Control
- 67% Penetration Testing, Vulnerability Scanning
- 31% Client Solid State Drive (Encrypted)
- 17% Endpoint Data Loss Prevention (Prevention Mode)
- 29% Network Data Loss Prevention (Discovery Mode)
- 51% Anti-Theft: Remote Locate, Lock, Wipe
- 43% Multi-Factor Authentication with Timeout
- 83% Secure Remote Administration
- 15% Policy-Based Encryption for Files and Folders
- 41% Server / Database / Backup Encryption
- 67% Network Segmentation

Advanced

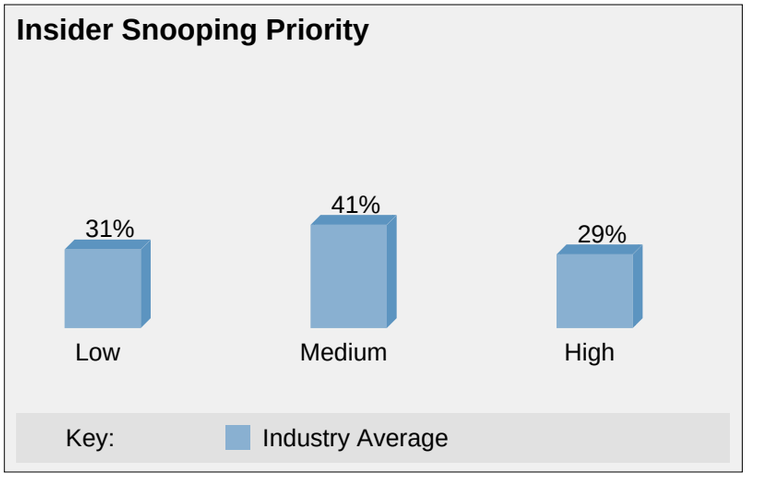
- 15% Server Solid State Drive (Encrypted)
- 20% Network Data Loss Prevention (Prevention Mode)
- 29% Database Activity Monitoring
- 42% Digital Forensics
- 41% Security Information and Event Management
- 50% Threat Intelligence
- 13% Multi-Factor Authentication with Walk-Away Lock
- 24% Client Application Whitelisting
- 18% Server Application Whitelisting
- 34% De-Identification / Anonymization
- 68% Business Continuity and Disaster Recovery

(⊕ = most have it, ~ = some have it, ⊖ = few have it)

Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

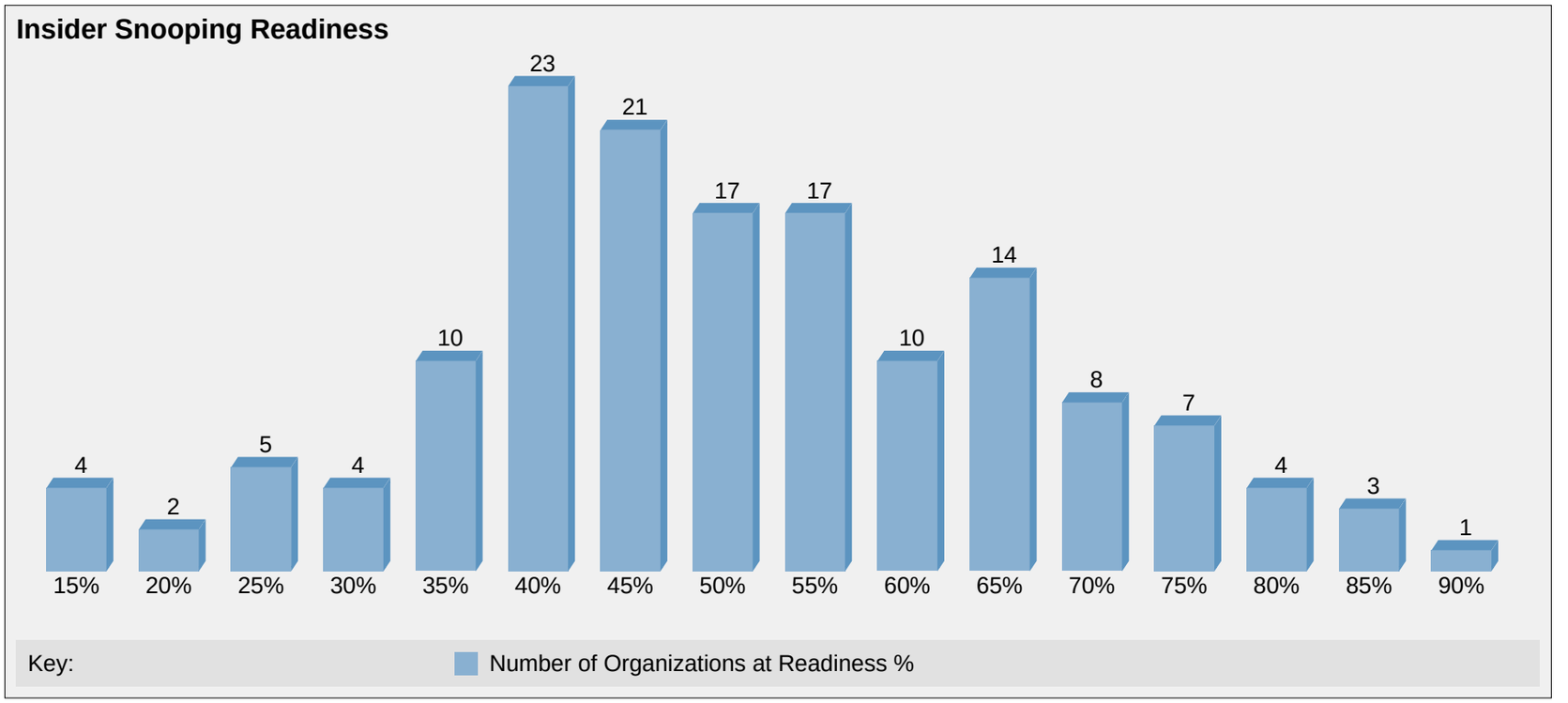
2.6 Insider Snooping

Insider snooping involves a worker accessing sensitive records of your organization without any legitimate need to do so.



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

The following graph shows the distribution of organizations in terms of readiness for Insider Snooping breaches. Horizontal axis percentages reflect the readiness for this type of breach in terms of the percentage of relevant capabilities implemented. The height of each bar is proportional to the number of organizations at that percentage of readiness.



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

The capabilities below are relevant to mitigating risk of Insider Snooping type breaches. The percentage next to each capability indicates the current state of implementation of the capability in the industry.

Insider Snooping Maturity Details - Health and Life Sciences Industry

Baseline

- 77% Policy
- 72% Risk Assessment
- 60% Audit and Compliance
- 71% User Awareness Training
- 63% Endpoint Device Encryption
- 62% Mobile Device Management
- 20% Endpoint Data Loss Prevention (Discovery Mode)
- 82% Identity and Access Management, Single-Factor Access Control
- 92% Firewall
- 85% Web Gateway
- 73% Vulnerability Management, Patching
- 63% Security Incident Response Plan
- 86% Secure Disposal

Enhanced

- 54% Device Control
- 67% Penetration Testing, Vulnerability Scanning
- 31% Client Solid State Drive (Encrypted)
- 17% Endpoint Data Loss Prevention (Prevention Mode)
- 29% Network Data Loss Prevention (Discovery Mode)
- 43% Multi-Factor Authentication with Timeout
- 83% Secure Remote Administration
- 15% Policy-Based Encryption for Files and Folders
- 41% Server / Database / Backup Encryption
- 67% Network Segmentation

Advanced

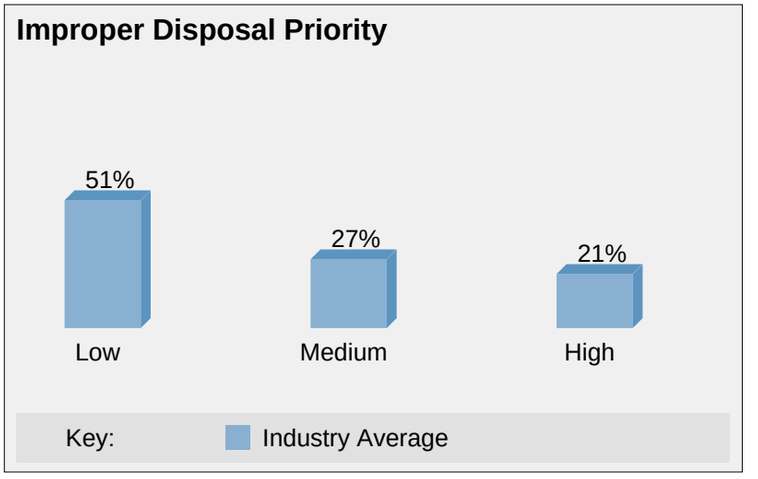
- 20% Network Data Loss Prevention (Prevention Mode)
- 29% Database Activity Monitoring
- 42% Digital Forensics
- 41% Security Information and Event Management
- 50% Threat Intelligence
- 13% Multi-Factor Authentication with Walk-Away Lock
- 24% Client Application Whitelisting
- 18% Server Application Whitelisting
- 34% De-Identification / Anonymization

(⊕ = most have it, ~ = some have it, ⊖ = few have it)

Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

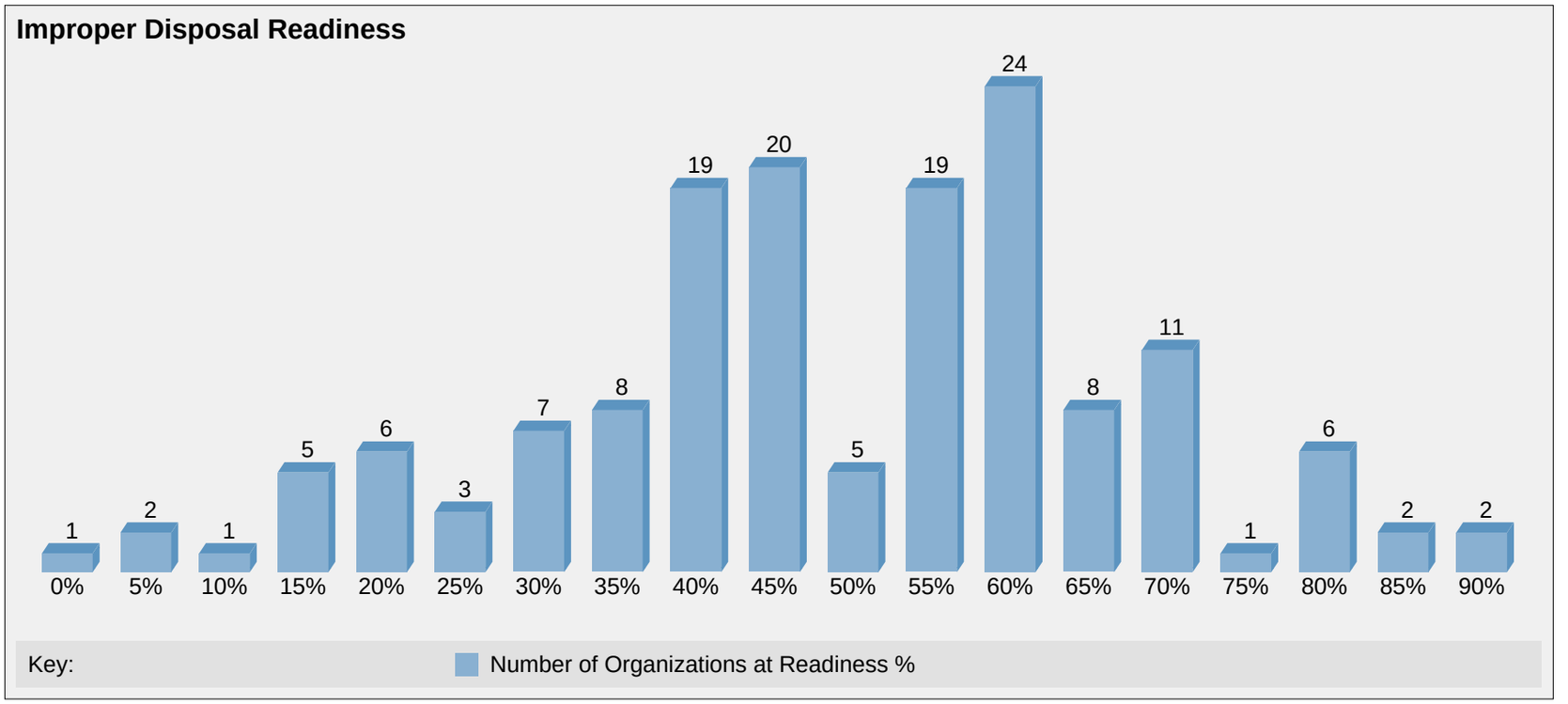
2.7 Improper Disposal

Improper disposal of electronic storage devices or media containing sensitive information. Examples of this could include dumping of paper-based sensitive records in a dumpster, or selling electronic devices with stored sensitive information without first securely wiping them.



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

The following graph shows the distribution of organizations in terms of readiness for Improper Disposal breaches. Horizontal axis percentages reflect the readiness for this type of breach in terms of the percentage of relevant capabilities implemented. The height of each bar is proportional to the number of organizations at that percentage of readiness.



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

The capabilities below are relevant to mitigating risk of Improper Disposal type breaches. The percentage next to each capability indicates the current state of implementation of the capability in the industry.

Improper Disposal Maturity Details - Health and Life Sciences Industry

Baseline

- 77% Policy
- 72% Risk Assessment
- 60% Audit and Compliance
- 71% User Awareness Training
- 63% Endpoint Device Encryption
- 62% Mobile Device Management
- 20% Endpoint Data Loss Prevention (Discovery Mode)
- 73% Vulnerability Management, Patching
- 63% Security Incident Response Plan
- 86% Secure Disposal

Enhanced

- 31% Client Solid State Drive (Encrypted)
- 51% Anti-Theft: Remote Locate, Lock, Wipe
- 15% Policy-Based Encryption for Files and Folders
- 41% Server / Database / Backup Encryption

Advanced

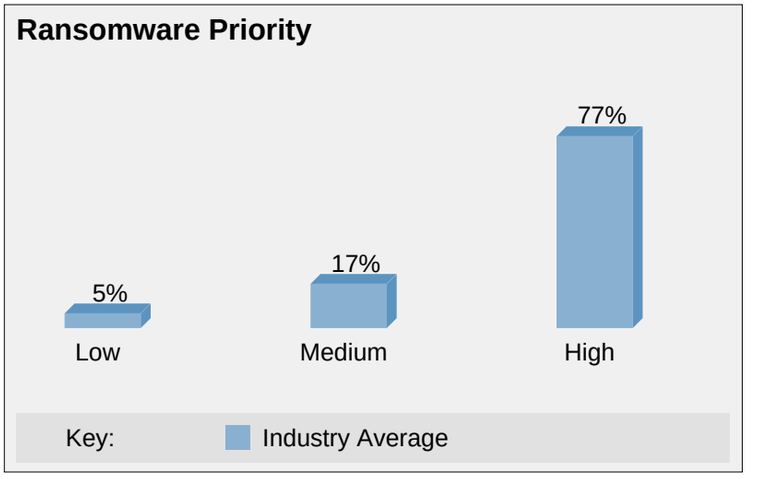
- 15% Server Solid State Drive (Encrypted)
- 42% Digital Forensics
- 34% De-Identification / Anonymization
- 12% Tokenization

(⊕ = most have it, ∿ = some have it, ⊖ = few have it)

Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

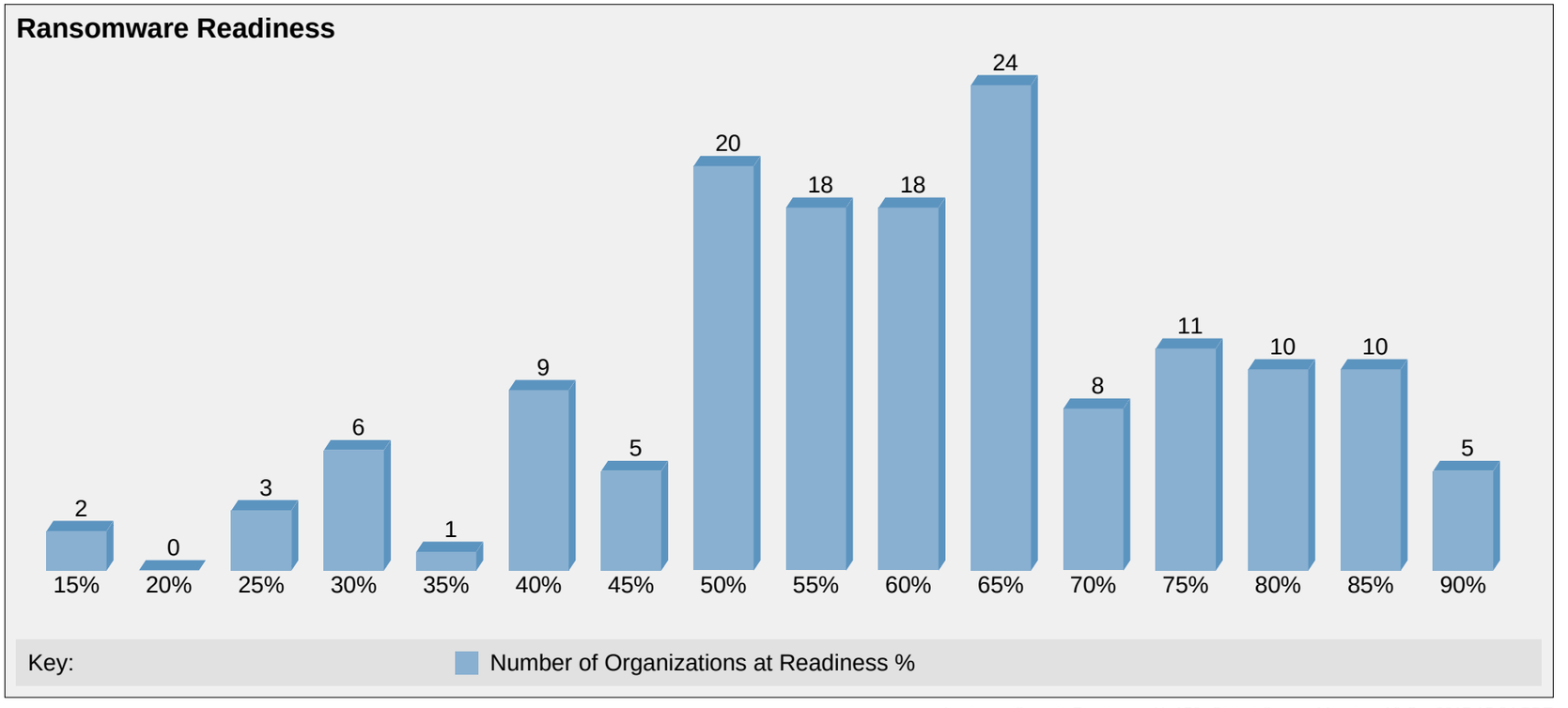
2.8 Ransomware

Ransomware breaches involve malware infections, often through phishing and drive-by download, where the malware encrypts sensitive information in electronic form and the hackers behind it withold the decryption keys, typically demanding a ransom. This type of breach compromises the availability of the sensitive records. It can also involve unauthorized access to sensitive information, depending on the malware and hacker access to the internal network and data of the organization.



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

The following graph shows the distribution of organizations in terms of readiness for Ransomware breaches. Horizontal axis percentages reflect the readiness for this type of breach in terms of the percentage of relevant capabilities implemented. The height of each bar is proportional to the number of organizations at that percentage of readiness.



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

The capabilities below are relevant to mitigating risk of Ransomware type breaches. The percentage next to each capability indicates the current state of implementation of the capability in the industry.

Ransomware Maturity Details - Health and Life Sciences Industry

Baseline

- 77% Policy
- 72% Risk Assessment
- 60% Audit and Compliance
- 71% User Awareness Training
- 93% Anti-Malware
- 82% Identity and Access Management, Single-Factor Access Control
- 89% Email Gateway
- 85% Web Gateway
- 73% Vulnerability Management, Patching
- 63% Security Incident Response Plan
- 89% Backup and Restore

Enhanced

- 54% Device Control
- 67% Penetration Testing, Vulnerability Scanning
- 17% Endpoint Data Loss Prevention (Prevention Mode)
- 67% Network Segmentation
- 63% Network Intrusion Prevention System

Advanced

- 20% Network Data Loss Prevention (Prevention Mode)
- 42% Digital Forensics
- 41% Security Information and Event Management
- 50% Threat Intelligence
- 24% Client Application Whitelisting
- 18% Server Application Whitelisting
- 68% Business Continuity and Disaster Recovery

(⊕ = most have it, ∿ = some have it, ⊖ = few have it)

Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

3. Maturity Details

The capabilities in the maturity model below are directly relevant to mitigating risk of various types of breaches. This view presents a comprehensive overview of all 42 assessed breach capabilities. To see the subset of capabilities relevant to a particular breach type see the previous section for that breach type. Each capability is classified into the Baseline, Enhanced or Advanced security maturity levels. The percentage next to each capability indicates the current state of implementation of that capability in the industry.

Security Maturity Details - Health and Life Sciences Industry

Baseline

- ⊕ 77% Policy
- ⊕ 72% Risk Assessment
- ∿ 60% Audit and Compliance
- ⊕ 71% User Awareness Training
- ∿ 63% Endpoint Device Encryption
- ∿ 62% Mobile Device Management
- ⊖ 20% Endpoint Data Loss Prevention (Discovery Mode)
- ⊕ 93% Anti-Malware
- ⊕ 82% Identity and Access Management, Single-Factor Access Control
- ⊕ 92% Firewall
- ⊕ 89% Email Gateway
- ⊕ 85% Web Gateway
- ⊕ 73% Vulnerability Management, Patching
- ∿ 63% Security Incident Response Plan
- ⊕ 86% Secure Disposal
- ⊕ 89% Backup and Restore

Enhanced

- ∿ 54% Device Control
- ⊕ 67% Penetration Testing, Vulnerability Scanning
- ⊖ 31% Client Solid State Drive (Encrypted)
- ⊖ 17% Endpoint Data Loss Prevention (Prevention Mode)
- ⊖ 29% Network Data Loss Prevention (Discovery Mode)
- ∿ 51% Anti-Theft: Remote Locate, Lock, Wipe
- ∿ 43% Multi-Factor Authentication with Timeout
- ⊕ 83% Secure Remote Administration
- ⊖ 15% Policy-Based Encryption for Files and Folders
- ∿ 41% Server / Database / Backup Encryption
- ⊕ 67% Network Segmentation
- ∿ 63% Network Intrusion Prevention System
- ⊕ 86% Business Associate Agreements
- ∿ 64% Virtualization

Advanced

- ⊖ 15% Server Solid State Drive (Encrypted)
- ⊖ 20% Network Data Loss Prevention (Prevention Mode)
- ⊖ 29% Database Activity Monitoring
- ∿ 42% Digital Forensics
- ∿ 41% Security Information and Event Management
- ∿ 50% Threat Intelligence
- ⊖ 13% Multi-Factor Authentication with Walk-Away Lock
- ⊖ 24% Client Application Whitelisting
- ⊖ 18% Server Application Whitelisting
- ∿ 34% De-Identification / Anonymization
- ⊖ 12% Tokenization
- ⊕ 68% Business Continuity and Disaster Recovery

(⊕ = most have it, ∿ = some have it, ⊖ = few have it)

Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

4. Capabilities

This program assesses the presence of 42 security capabilities in the Health and Life Sciences Industry . This section defines each capability and shows the current state of implementation of the capability in the Health and Life Sciences Industry.

4.1 Policy

Accurate, complete, and up-to-date privacy & security policy. This is the internal document used to govern employee responsibilities with regard to privacy and security of sensitive information.

Workshop Overview More Info

HIPAA: 45 CFR 164.308(a)

ISO: 27001:2013 Section 5.2 Policy

NIST: SP 800-53 Rev. 4 PS-1, PS-7

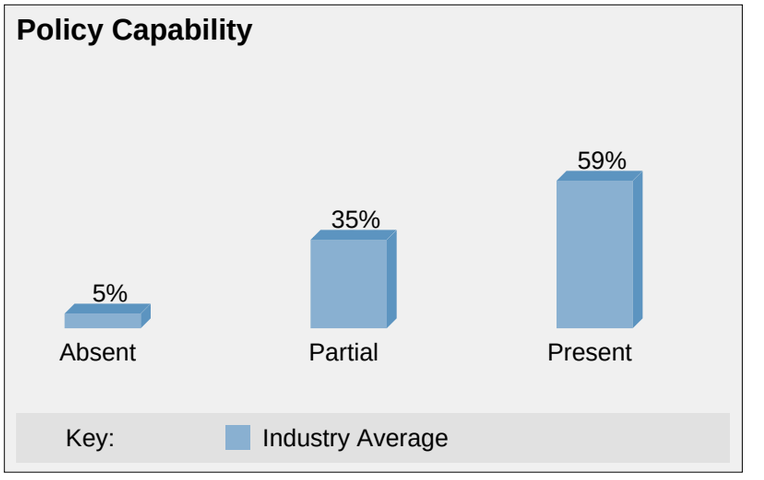
PCI DSS: v3.1 Section 12.1

CIS: v6.1 CSC Governance Item #4: Policies

GDPR: Regulation 78 internal policies

ISO: IEC 80001-1:2010:(4.2.1), IEC/TR 80001-2-2:2012: (5.15)

EU MDR: 2017/745 (19)



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Policy is relevant to the following breach types:

- Cybercrime Hacking
- Business Associates
- Improper Disposal
- Loss or Theft of Mobile Device or Media
- Malicious Insiders or Fraud
- Ransomware
- Insider Accidents or Workarounds
- Insider Snooping

4.2 Risk Assessment

Documented risk assessments done annually.

Workshop Overview More Info

HIPAA: 45 CFR 164.308(a)(1)

ISO: 27001:2013 Section 8.2 Information Security Risk Assessment

NIST: SP 800-53 Rev. 4 RA-1 to RA-3

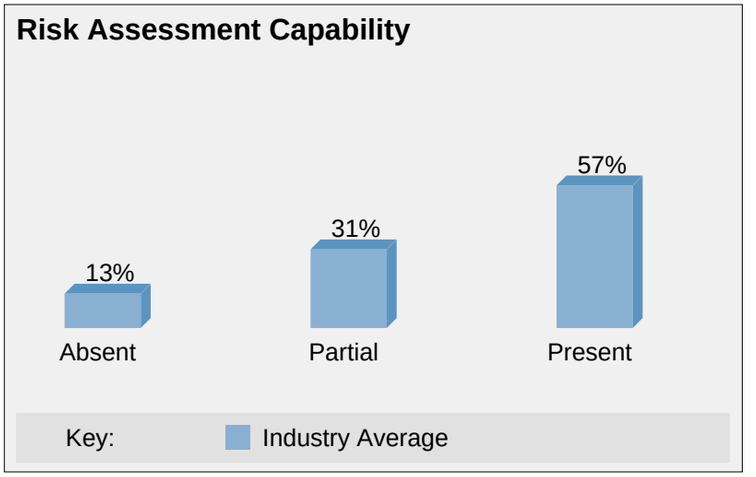
PCI DSS: v3.1 Section 12.2

CIS: v6.1 CSC 13.1

GDPR: Regulation 76 risk assessment

ISO: IEC 80001-1:2010:(4.3,4.4), IEC/TR 80001-2-1:2012

EU MDR: 2017/745 Annex I:(14.2(d),17.2)



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Risk Assessment is relevant to the following breach types:

- Cybercrime Hacking
- Business Associates
- Improper Disposal
- Loss or Theft of Mobile Device or Media
- Malicious Insiders or Fraud
- Ransomware
- Insider Accidents or Workarounds
- Insider Snooping

4.3 Audit and Compliance

Audit and compliance technology and processes in place to detect and remedy non-compliance with policy.

Workshop Overview More Info

HIPAA: 45 CFR 164.312(b)

ISO: 27001:2013 Section 9.2 Internal Audit

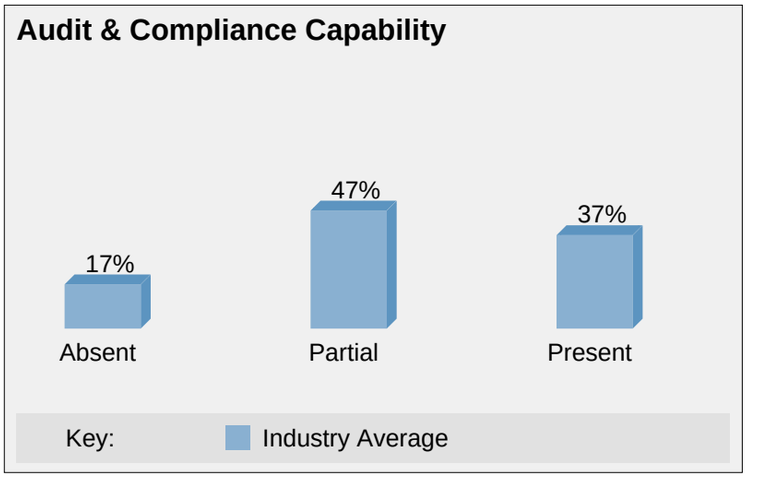
NIST: SP 800-53 Rev. 4 AU-1 to 16

PCI DSS: v3.1 Requirement 10

CIS: v6.1 CSC 6

GDPR: Regulation 74 demonstrate compliance

ISO: IEC 80001-1:2010:(4.4.4,4.6.1), IEC/TR 80001-2-2:2012:(5.2), ISO/TR 80001-2-7:2015



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Audit and Compliance is relevant to the following breach types:

- Cybercrime Hacking
- Business Associates
- Improper Disposal
- Loss or Theft of Mobile Device or Media
- Malicious Insiders or Fraud
- Ransomware
- Insider Accidents or Workarounds
- Insider Snooping

4.4 User Awareness Training

Training of workers on security and privacy. May be implemented at time of hire, change of role, annually, or more frequently. May also be triggered by specific events. More advanced training may use gamified techniques, for example for spear phishing, to help train workers on the job.

Workshop Overview More Info

HIPAA: 45 CFR 164.308(a)(5)

ISO: 27002:2013 Section 7.2.2 Information Security Awareness, Education and Training

NIST: SP 800-53 Rev. 4 AT-1 to 4

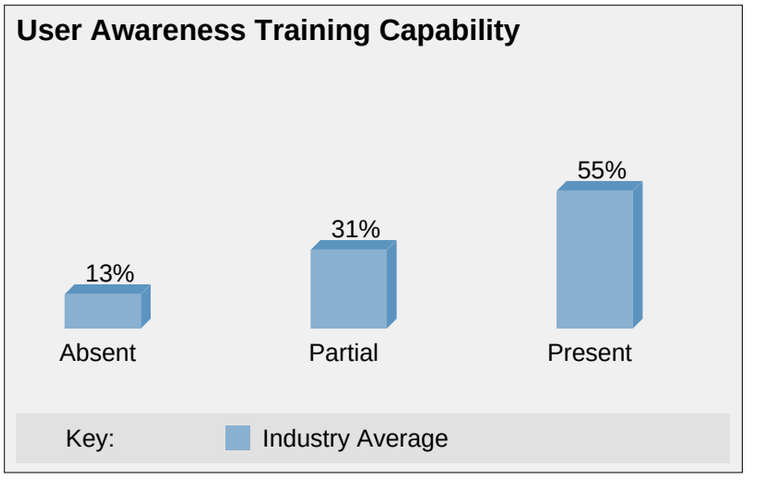
PCI DSS: v3.1 Section 9.9.3

CIS: v6.1 CSC 17

GDPR: Article 39 awareness raising and training of staff

ISO: IEC 80001-1:2010:(4.4.4.1), IEC/TR 80001-2-2:2012:(5.12,5.16)

EU MDR: 2017/745 Annex I:(23.4(f),(ab))



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

User Awareness Training is relevant to the following breach types:

- Cybercrime Hacking
- Business Associates
- Improper Disposal
- Loss or Theft of Mobile Device or Media
- Malicious Insiders or Fraud
- Ransomware
- Insider Accidents or Workarounds
- Insider Snooping

4.5 Endpoint Device Encryption

Client devices storing sensitive information have encryption of data at rest.

Workshop Overview More Info

HIPAA: 45 CFR 164.312

ISO: 27002:2013 Section 10 Cryptography

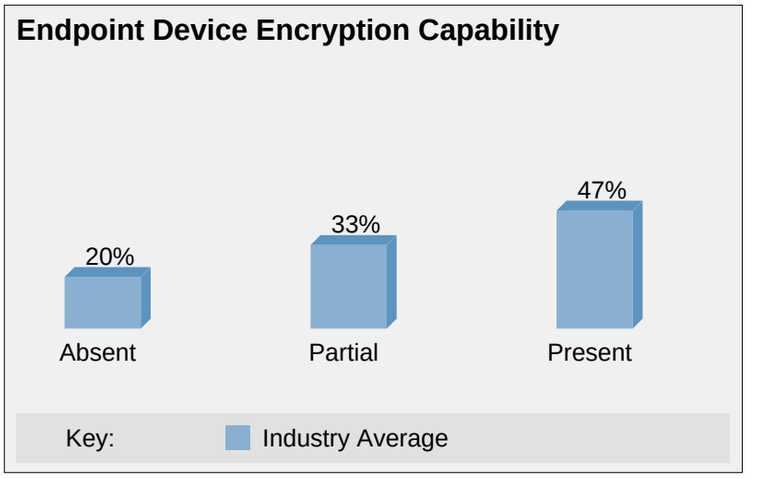
NIST: SP 800-53 Rev. 4 SC-28

PCI DSS: v3.1 Section 3.4.1

CIS: v6.1 CSC 13.2

GDPR: Article 32 1a encryption of personal data

ISO: IEC 80001-1:2010:(4.3.2), IEC/TR 80001-2-2:2012: (5.17)



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Endpoint Device Encryption is relevant to the following breach types:
- Loss or Theft of Mobile Device or Media - Malicious Insiders or Fraud - Insider Snooping
- Improper Disposal

4.6 Mobile Device Management

Management of mobile client devices including smartphones and tablets. Often used with BYOD devices. Functionality may include secure container for whitelisted business apps and data with access control and encryption, as well as remote management including remote lock and wipe.

Workshop Overview More Info

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: 27002:2013 Section 6.2 Mobile Devices and Teleworking

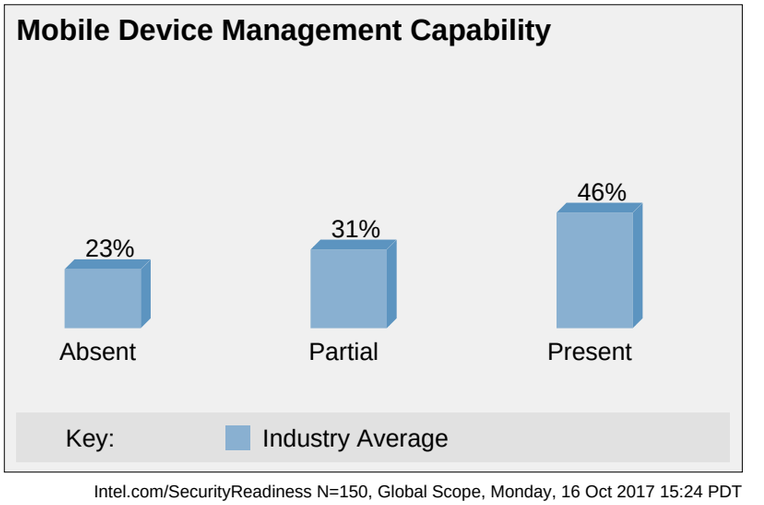
NIST: SP 800-53 Rev. 4 AC-19

PCI DSS: v3.1 Section 1.4

CIS: v6.1 CSC 13

GDPR: Regulation 83 accidental or unlawful loss of personal data

ISO: IEC 80001-1:2010:(4.3.2), IEC/TR 80001-2-2:2012: (5.17)



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Mobile Device Management is relevant to the following breach types:
- Loss or Theft of Mobile Device or Media - Insider Accidents or Workarounds - Malicious Insiders or Fraud
- Insider Snooping - Improper Disposal

4.7 Endpoint Data Loss Prevention (Discovery Mode)

Endpoint Data Loss Prevention (EDLP) ability to discover and possibly also classify sensitive information at rest on clients or servers. In this mode EDLP is only monitoring, logging and alerting, not blocking user actions.

Workshop Overview More Info

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

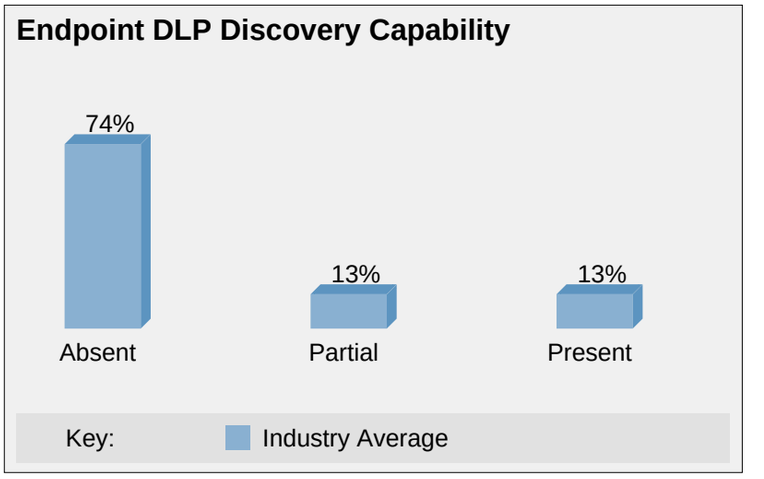
ISO: 27002:2013 Section 18.1.3 Protection of Records

NIST: SP 800-53 Rev. 4 AU-13 to AU-14

PCI DSS: v3.1 Requirement 3

CIS: v6.1 CSC 13.9

GDPR: Regulation 83 accidental loss of personal data



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Endpoint Data Loss Prevention (Discovery Mode) is relevant to the following breach types:

- Loss or Theft of Mobile Device or Media
- Insider Accidents or Workarounds
- Malicious Insiders or Fraud
- Insider Snooping
- Improper Disposal

4.8 Anti-Malware

Ability to detect and remediate blacklisted executables. May be signature based or heuristics / behavior based. Remediation may include quarantine or removal of any malware detected.

Workshop Overview More Info

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: 27002:2013 Section 12.2 Protection from Malware

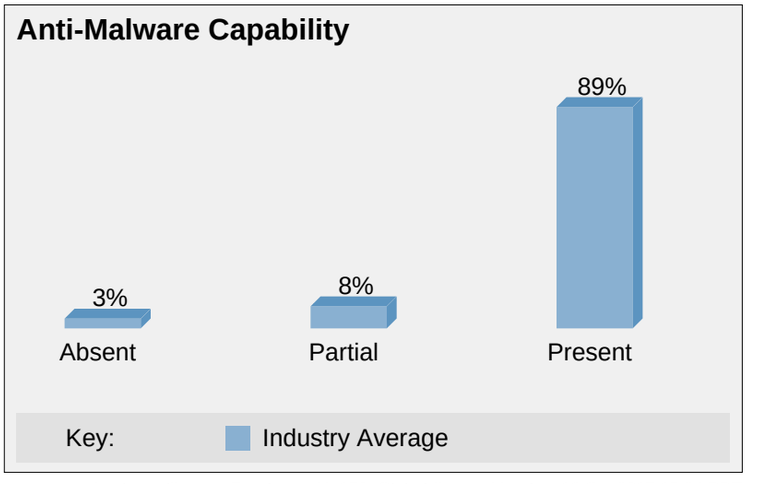
NIST: SP 800-53 Rev. 4 SI-3

PCI DSS: v3.1 Requirement 5

CIS: v6.1 CSC 8

GDPR: Regulation 49 prevent malicious code distribution

ISO: IEC/TR 80001-2-2:2012:(5.5,5.10)



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Anti-Malware is relevant to the following breach types:

- Cybercrime Hacking
- Insider Accidents or Workarounds
- Ransomware

4.9 Identity and Access Management, Single-Factor Access Control

This capability includes both technology and processes covering full IAM (Identity and Access Management) lifecycle such as authentication and authorization / privilege management. Access control using a single factor, either "what you know," "what you have," or "what you are" / biometrics. Username / password is a very common form of "what you know" single factor authentication. There may be multiple sets of credentials across different domains, applications, and solutions.

Workshop Overview More Info

HIPAA: 45 CFR 164.312

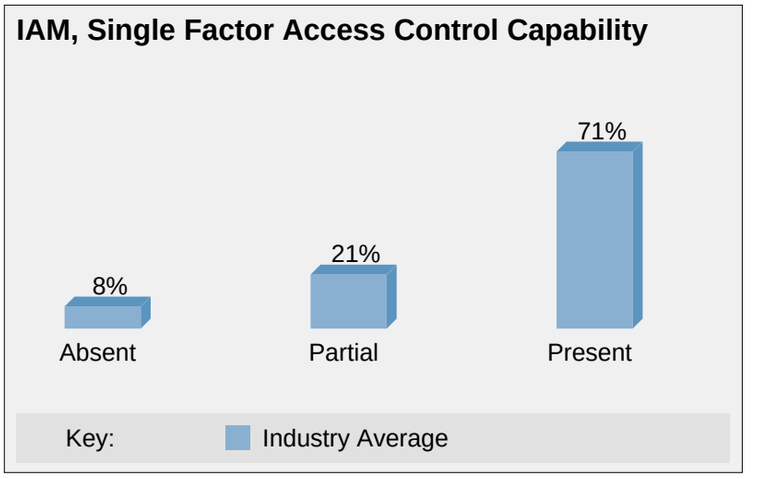
ISO: 27002:2013 Section 9 Access Control

NIST: SP 800-53 Rev. 4 AC-1 to 3

PCI DSS: v3.1 Requirement 7

CIS: v6.1 CSC 14, CSC 5

GDPR: Regulation 39 security and preventing unauthorised access



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Identity and Access Management, Single-Factor Access Control is relevant to the following breach types:

- Cybercrime Hacking
- Loss or Theft of Mobile Device or Media
- Malicious Insiders or Fraud
- Insider Snooping
- Ransomware

4.10 Firewall

The external firewall provides network perimeter defense against unauthorized access to organizations systems and sensitive information. This capability also includes internal host-based firewalls. Services may include provisioning / deployment, upgrade, patching, policy / configuration updates, network traffic monitoring, etc.

Workshop Overview More Info

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: 27002:2013 Section 13.1.2 Security of Network Services

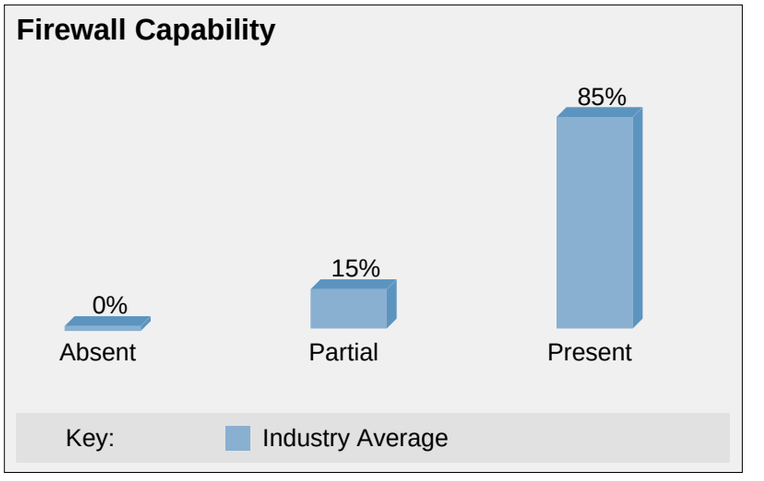
NIST: SP 800-53 Rev. 4 SC-7

PCI DSS: v3.1 Requirement 1

CIS: v6.1 CSC 9.2, CSC 9.6, CSC 12, CSC 18.2

GDPR: Regulation 39 security and preventing unauthorised access

ISO: IEC/TR 80001-2-2:2012:(5.11)



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Firewall is relevant to the following breach types:

- Cybercrime Hacking
- Malicious Insiders or Fraud
- Insider Snooping

4.11 Email Gateway

Safeguard for email and may include inbound threat protection, outbound encryption, compliance, data loss prevention, and administration.

Workshop Overview More Info

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

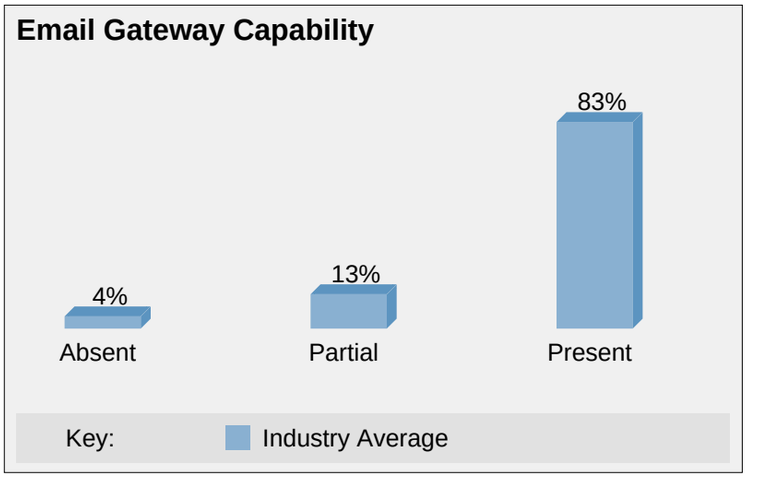
ISO: 27002:2013 Section 13.1 Network Security Management

NIST: SP 800-53 Rev. 4 SC-7

PCI DSS: v3.1 Requirement 5

CIS: v6.1 CSC 7

GDPR: Regulation 49 resist accidental events that compromise confidentiality



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Email Gateway is relevant to the following breach types:

- Cybercrime Hacking
- Insider Accidents or Workarounds
- Malicious Insiders or Fraud
- Ransomware

4.12 Web Gateway

Safeguard for web requests and content returned in responses, and may include analysis of the nature and intent of all content and code entering the network from requested web pages to provide protection against malware and other hidden threats.

Workshop Overview More Info

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

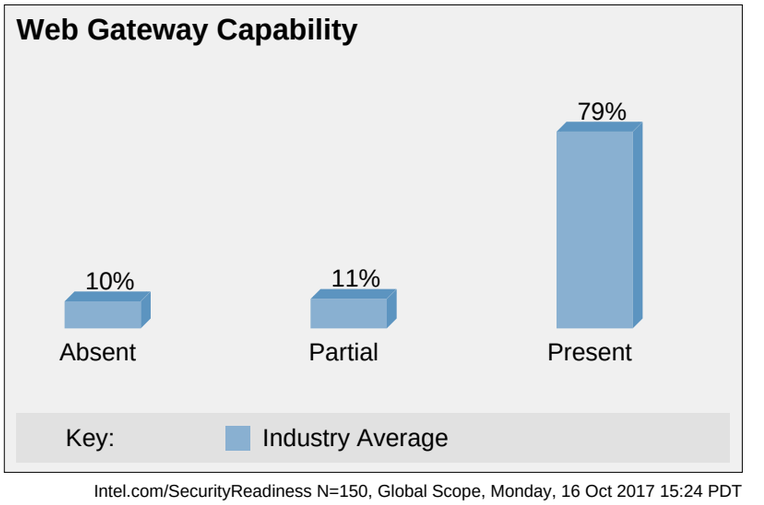
ISO: 27002:2013 Section 13.1 Network Security Management

NIST: SP 800-53 Rev. 4 SC-7

PCI DSS: v3.1 Requirement 5

CIS: v6.1 CSC 7, CSC 12

GDPR: Regulation 49 resist accidental events that compromise confidentiality



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Web Gateway is relevant to the following breach types:

- Cybercrime Hacking
- Insider Accidents or Workarounds
- Malicious Insiders or Fraud
- Insider Snooping
- Ransomware

4.13 Vulnerability Management, Patching

Ability (technology and processes) to manage vulnerabilities on endpoint devices through configuration updates, signature updates, patching, and so forth. This can include patching of operating systems, security solutions, as well as office and business applications to ensure they are up to date and secure.

Workshop Overview More Info

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: 27002:2013 Section 12.6 Technical Vulnerability Management

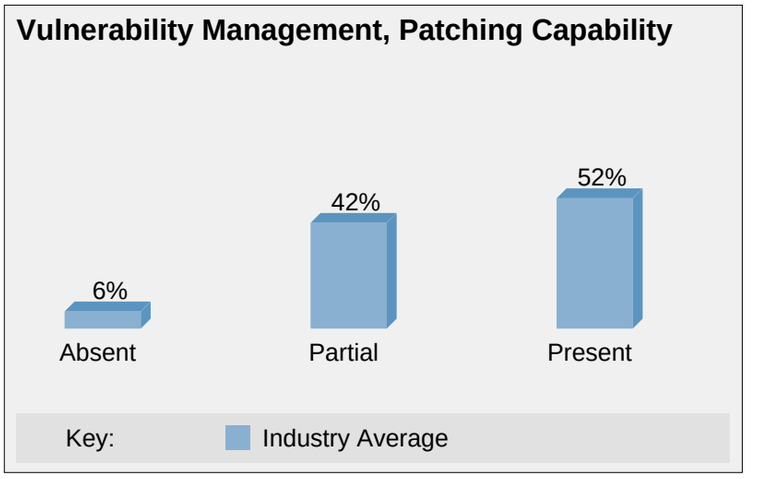
NIST: SP 800-53 Rev. 4 CM-1 to 11, MA-1 to 6

PCI DSS: v3.1 Requirement 6

CIS: v6.1 CSC 3, CSC 11, CSC 15, CSC 18, CSC 4.5

GDPR: Regulation 83 implement state of the art measures

ISO: IEC/TR 80001-2-2:2012:(5.5)



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Vulnerability Management, Patching is relevant to the following breach types:

- Cybercrime Hacking
- Loss or Theft of Mobile Device or Media
- Insider Accidents or Workarounds
- Malicious Insiders or Fraud
- Insider Snooping
- Improper Disposal
- Ransomware

4.14 Security Incident Response Plan

Plans in place covering what do to in the event of a suspected information security incident or breach.

Workshop Overview More Info

HIPAA: 45 CFR 164.308(a)(6)

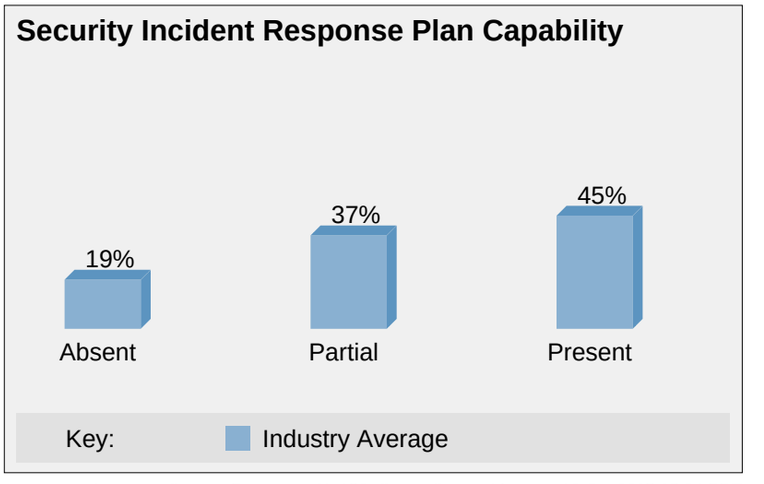
ISO: 27002:2013 Section 16 Information Security Incident Management

NIST: SP 800-53 Rev. 4 IR-1 to 10

PCI DSS: v3.1 Section 12.10

CIS: v6.1 CSC 19

GDPR: Article 32 1 protect confidentiality, integrity, availability of personal data



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Security Incident Response Plan is relevant to the following breach types:

- Cybercrime Hacking
- Loss or Theft of Mobile Device or Media
- Insider Accidents or Workarounds
- Business Associates
- Malicious Insiders or Fraud
- Insider Snooping
- Improper Disposal
- Ransomware

4.15 Secure Disposal

Technology and processes to securely dispose of devices and media containing sensitive information. This can include secure wipe of disk drives, shredding of paper records, and so forth.

Workshop Overview More Info

HIPAA: 45 CFR 164.310(d)(2)(i)

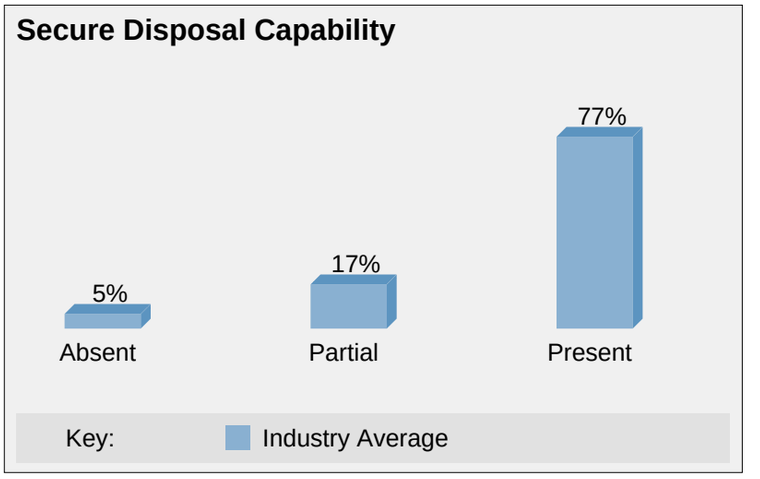
ISO: 27002:2013 Section 8.3.2 Disposal of Media, 11.2.7 Secure Disposal or Re-Use of Equipment

NIST: SP 800-53 Rev. 4 MP-6

PCI DSS: v3.1 Section 9.8

CIS: v6.1 CSC Privacy Impact Assessment: Disposal

GDPR: Regulation 83 protect confidentiality of personal data



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Secure Disposal is relevant to the following breach types:
- Loss or Theft of Mobile Device or Media - Insider Accidents or Workarounds - Malicious Insiders or Fraud
- Insider Snooping - Improper Disposal

4.16 Backup and Restore

Ability to securely back up systems and data, store versioned backups in a secure, managed backup system. At least one version should be air-gapped / offline. This also includes the ability to restore systems that become corrupt or infected. For this capability to be considered fully implemented, it should be regularly tested through a full backup and restore cycle.

Workshop Overview More Info

HIPAA: Security Rule - Protect Availability - Technical Safeguard

ISO: 27002:2013 Section 12.3 Backup

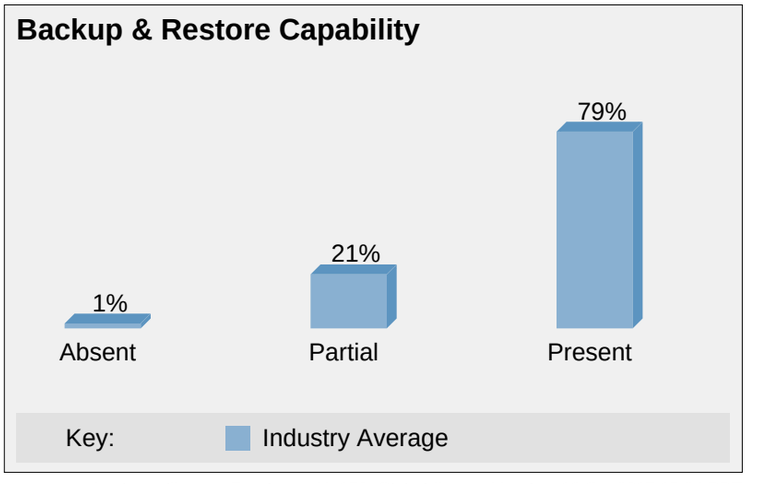
NIST: SP 800-53 Rev. 4 CP-9, 10

PCI DSS: v3.1 Section 9.5.1

CIS: v6.1 CSC 10

GDPR: Article 32 1c restore availability and access to personal data

ISO: IEC/TR 80001-2-2:2012:(5.7)



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Backup and Restore is relevant to the following breach types:
- Cybercrime Hacking - Loss or Theft of Mobile Device or Media - Malicious Insiders or Fraud
- Ransomware

4.17 Device Control

Ability to enforce an organization's policy regarding removable storage devices that may be connected by workers to endpoint client devices. Typically includes representation of policy rules as well as technology and processes to enforce such rules. Examples include USB sticks or other removable storage.

Workshop Overview More Info

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: 27002:2013 Section 8.3.1 Management of Removable Media

NIST: SP 800-53 Rev. 4 MP-7, SC-18, SC-41

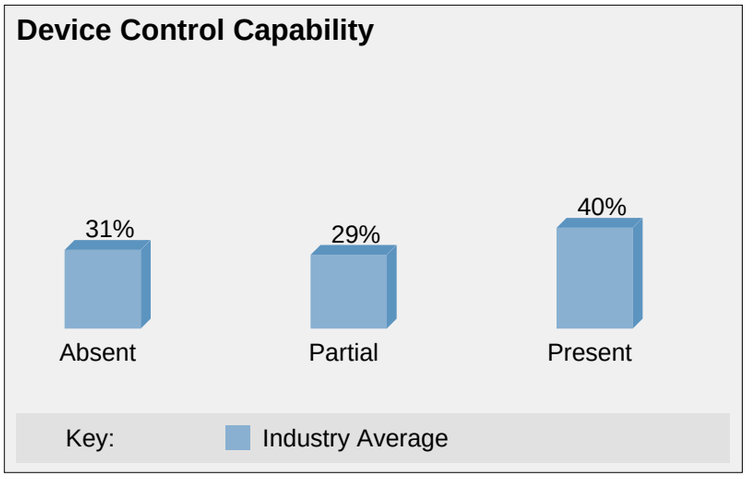
PCI DSS: v3.1 Requirement 5

CIS: v6.1 CSC 13.5

GDPR: Regulation 39 security and preventing unauthorised access

ISO: IEC 80001-1:2010:(4.3.2), IEC/TR 80001-2-2:2012:(5.13)

EU MDR: 2017/745 25(a,b,c),26(a,b,c)



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Device Control is relevant to the following breach types:
- Insider Accidents or Workarounds
- Malicious Insiders or Fraud
- Insider Snooping
- Ransomware

4.18 Penetration Testing, Vulnerability Scanning

Penetration testing and vulnerability scanning has been conducted within the last year to discover vulnerabilities in an organization's IT infrastructure or applications.

Workshop Overview More Info

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

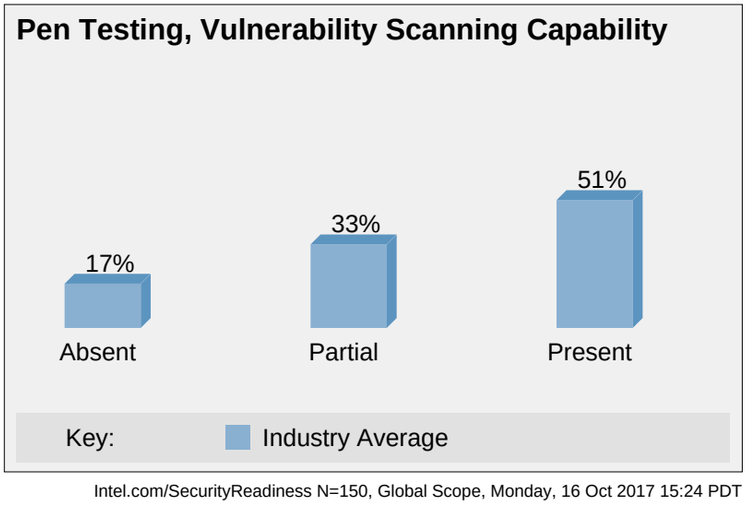
ISO: 27002:2013 Section 18.2.3 Technical Compliance Review

NIST: SP 800-53 Rev. 4 CA-8, RA-5, RA-6

PCI DSS: v3.1 Section 11.3

CIS: v6.1 CSC 9, CSC 4, CSC 15.2, CSC 18.4

GDPR: Article 32 1d regular testing, assessing, evaluating effectiveness of security



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Penetration Testing, Vulnerability Scanning is relevant to the following breach types:
- Cybercrime Hacking
- Malicious Insiders or Fraud
- Insider Snooping
- Ransomware

4.19 Client Solid State Drive (Encrypted)

Self-encrypting solid state drives are used on client / endpoint devices to protect sensitive information at rest, with high performance.

Workshop Overview More Info

HIPAA: 45 CFR 164.312

ISO: 27002:2013 Section 10 Cryptography

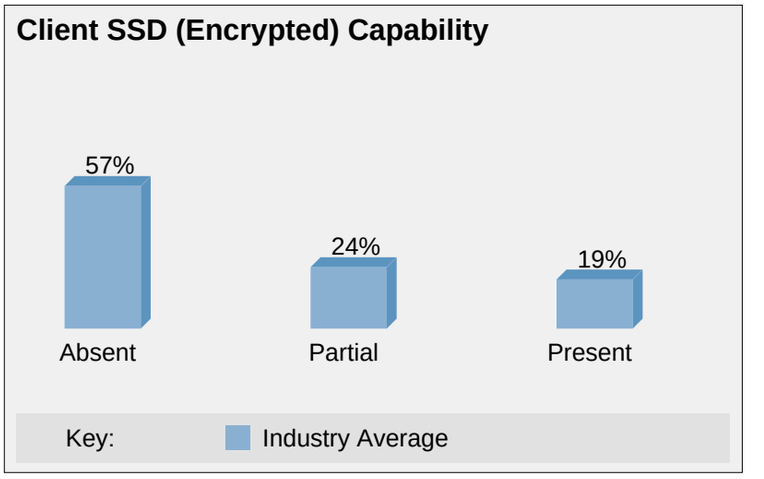
NIST: SP 800-53 Rev. 4 SC-28

PCI DSS: v3.1 Section 3.4.1

CIS: v6.1 CSC 13.2, CSC 14.5

GDPR: Article 32 1a encryption of personal data

ISO: IEC 80001-1:2010:(4.4.4)



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Client Solid State Drive (Encrypted) is relevant to the following breach types:
- Loss or Theft of Mobile Device or Media - Malicious Insiders or Fraud - Insider Snooping
- Improper Disposal

4.20 Endpoint Data Loss Prevention (Prevention Mode)

Data Loss Prevention for endpoint / client devices. Enforces rules derived from the policy of the organization that are intended to protect sensitive information. Includes capability to monitor user actions, detect potential non-compliance, and take action according to policy rules. Actions may include notifying the user, logging information in an audit log, preventing an action, or protecting data used in an action (for example, using encryption).

Workshop Overview More Info

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: 27002:2013 Section 18.1.3 Protection of Records

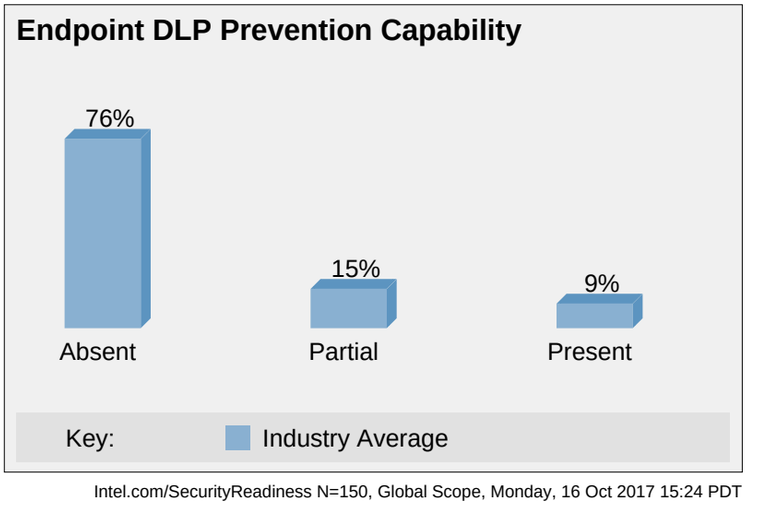
NIST: SP 800-53 Rev. 4 SC-7

PCI DSS: v3.1 Requirement 3

CIS: v6.1 CSC 13.9, CSC 13.4

GDPR: Regulation 49 resist accidental events that compromise confidentiality

ISO: IEC 80001-1:2010:(4.4.4,4.6.1)



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Endpoint Data Loss Prevention (Prevention Mode) is relevant to the following breach types:
- Insider Accidents or Workarounds - Malicious Insiders or Fraud - Insider Snooping
- Ransomware

4.21 Network Data Loss Prevention (Discovery Mode)

Network-based Data Loss Prevention (NDLP) ability to monitor (scan and analyze) network traffic in real time, detect and classify sensitive information, and discover unknown risks. In this mode NDLP is only monitoring, logging, and alerting, not blocking network traffic.

Workshop Overview More Info

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: 27002:2013 Section 13.1 Network Security Management

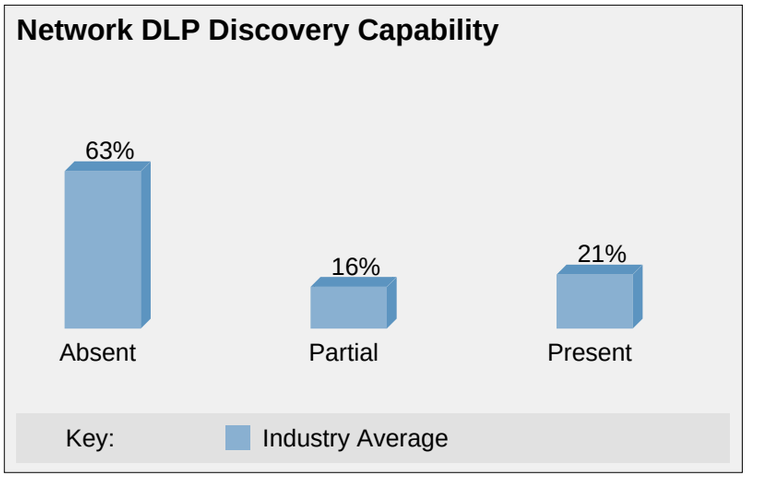
NIST: SP 800-53 Rev. 4 AU-13, 14

PCI DSS: v3.1 Requirement 3

CIS: v6.1 CSC 13.6

GDPR: Regulation 83 accidental loss of personal data

ISO: IEC 80001-1:2010:(4.6.1)



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Network Data Loss Prevention (Discovery Mode) is relevant to the following breach types:
- Cybercrime Hacking - Insider Accidents or Workarounds - Malicious Insiders or Fraud
- Insider Snooping

4.22 Anti-Theft: Remote Locate, Lock, Wipe

Ability for IT Administrators in the organization to remotely locate lost or stolen mobile client devices, lock them, or wipe them to remove sensitive information and thereby reduce risk of breach.

Workshop Overview More Info

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: 27002:2013 Section 6.2 Mobile Devices and Teleworking

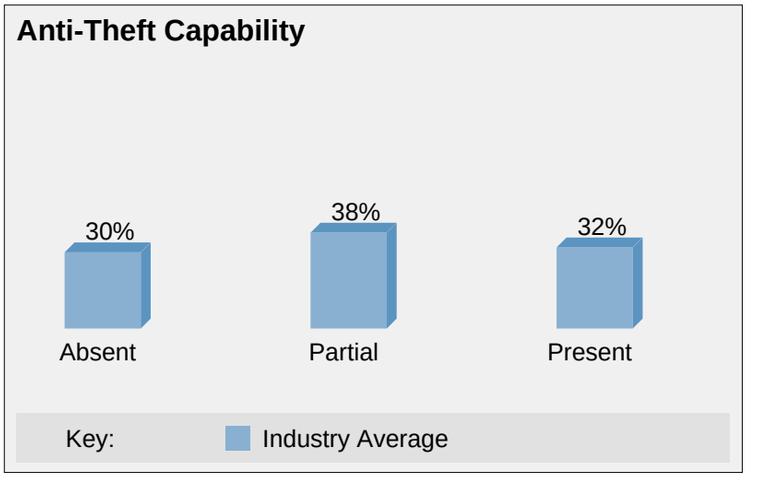
NIST: SP 800-53 Rev. 4 AC-7, AC-19

PCI DSS: v3.1 Section 9.8

CIS: v6.1 CSC 3.4

GDPR: Regulation 39 security and preventing unauthorised access

ISO: IEC 80001-1:2010:(4.3.2,4.4.4), IEC/TR 80001-2-2:2012:(5.13)

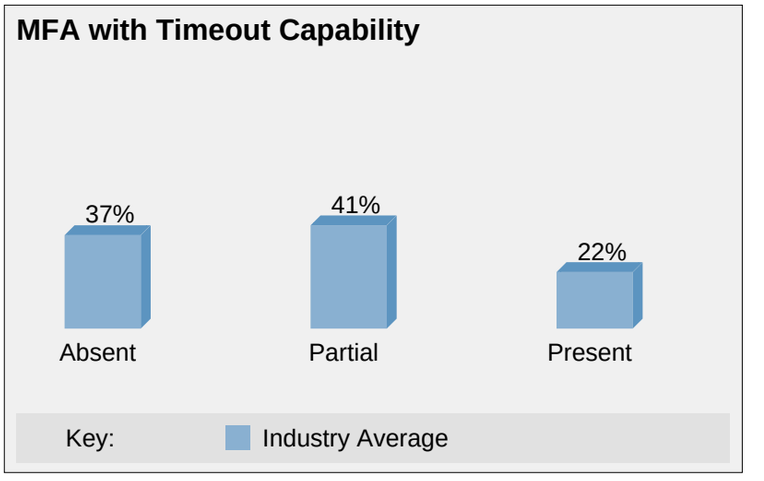


Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Anti-Theft: Remote Locate, Lock, Wipe is relevant to the following breach types:
- Loss or Theft of Mobile Device or Media - Malicious Insiders or Fraud - Improper Disposal

4.23 Multi-Factor Authentication with Timeout

Access control with multiple factors: what you know (e.g., username / password), what you have (e.g., security hardware token), or what you are (biometrics). Timeout functionality automatically locks access after a policy-defined period of inactivity. This is intended to reduce risk of an unauthorized access and breach that may result from an unauthorized person accessing an abandoned secure session.



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Workshop Overview More Info

HIPAA: 45 CFR 164.312

ISO: 27002:2013 Section 9 Access Control

NIST: SP 800-53 Rev. 4 IA-2, AC-2, AC-11, AC-12

PCI DSS: v3.1 Requirement 8

CIS: v6.1 CSC 5.6, CSC 11.4, CSC 12.6, CSC 16.11

GDPR: Regulation 39 security and preventing unauthorised access

ISO: IEC 80001-1:2010:(4.4.4)

Multi-Factor Authentication with Timeout is relevant to the following breach types:
- Cybercrime Hacking - Loss or Theft of Mobile Device or Media - Malicious Insiders or Fraud
- Insider Snooping

4.24 Secure Remote Administration

Ability for IT Administrator in the organization to securely and remotely administer client devices containing sensitive information. This can include diagnostics, remediation of issues, patching, updates (e.g., anti-malware signatures, configurations, upgrades, and so forth).

Workshop Overview More Info

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: 27002:2013 Section 12.6 Technical Vulnerability Management

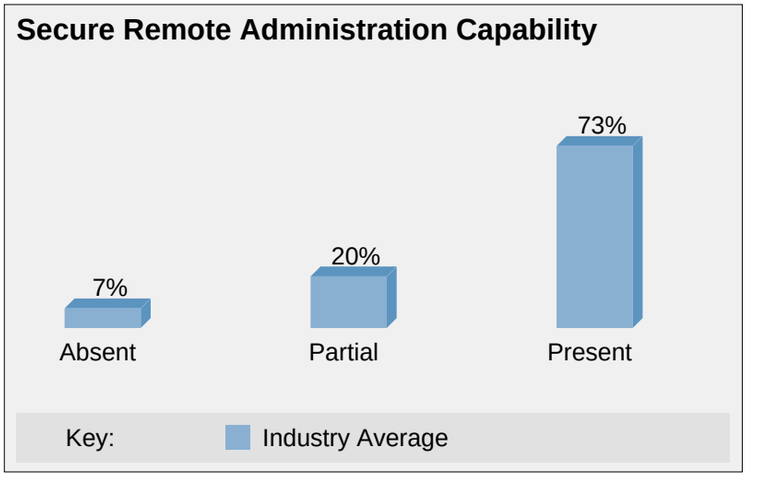
NIST: SP 800-53 Rev. 4 MA-4

PCI DSS: v3.1 Section 10.8.1

CIS: v6.1 CSC 3.4

GDPR: Article 32 1c restore availability and access to personal data

ISO: IEC 80001-1:2010:(4.5)



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Secure Remote Administration is relevant to the following breach types:

- Cybercrime Hacking
- Loss or Theft of Mobile Device or Media
- Insider Accidents or Workarounds
- Malicious Insiders or Fraud
- Insider Snooping

4.25 Policy-Based Encryption for Files and Folders

Encryption of specific files or folders based on policy of the organization, and classification of files, in order to ensure only authorized access to files and folders containing sensitive information. This reduces risk of unauthorized access and mitigates the risk of breach.

Workshop Overview More Info

HIPAA: 45 CFR 164.312

ISO: 27002:2013 Section 10 Cryptography

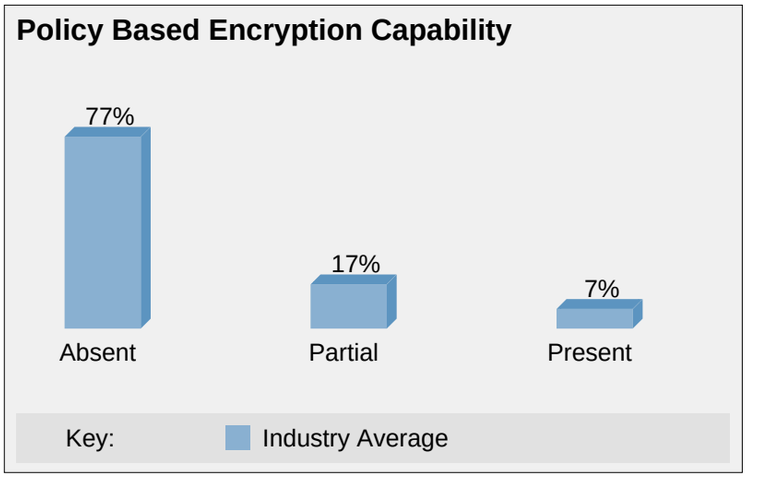
NIST: SP 800-53 Rev. 4 SC-28

PCI DSS: v3.1 Requirement 3

CIS: v6.1 CSC 13.2, CSC 14.5

GDPR: Article 32 1a encryption of personal data

ISO: IEC 80001-1:2010:(4.4.4), IEC/TR 80001-2-2:2012:(5.17)



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Policy-Based Encryption for Files and Folders is relevant to the following breach types:

- Loss or Theft of Mobile Device or Media
- Insider Accidents or Workarounds
- Malicious Insiders or Fraud
- Insider Snooping
- Improper Disposal

4.26 Server / Database / Backup Encryption

Encryption of servers, databases running on servers, SAN's, and backup archives.

Workshop Overview More Info

HIPAA: 45 CFR 164.312

ISO: 27002:2013 Section 10 Cryptography

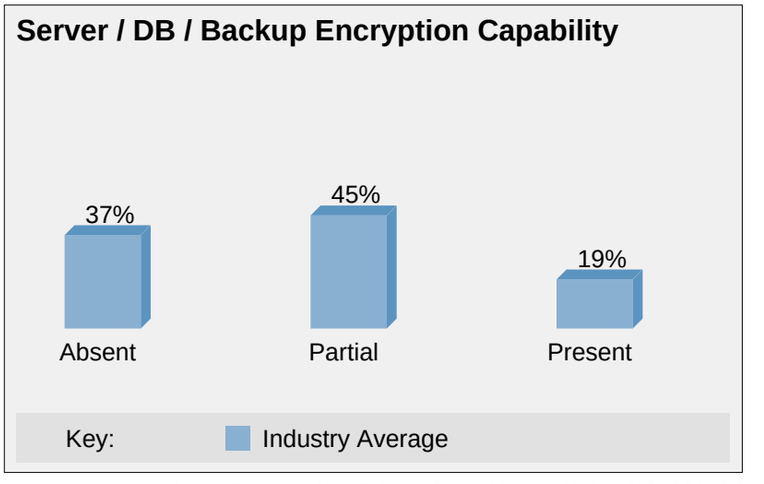
NIST: SP 800-53 Rev. 4 SC-28, CP-9

PCI DSS: v3.1 Requirement 3

CIS: v6.1 CSC 10.3, CSC 13.2, CSC 14.5

GDPR: Article 32 1a encryption of personal data

ISO: IEC 80001-1:2010:(4.4.4)



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Server / Database / Backup Encryption is relevant to the following breach types:

- Loss or Theft of Mobile Device or Media
- Malicious Insiders or Fraud
- Insider Snooping
- Improper Disposal

4.27 Network Segmentation

Network is segmented to protect critical assets. This can include use of DMZ, guest network, and other segmentations to isolate vulnerabilities.

Workshop Overview More Info

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: 27002:2013 Section 13.1.3 Segregation in Networks

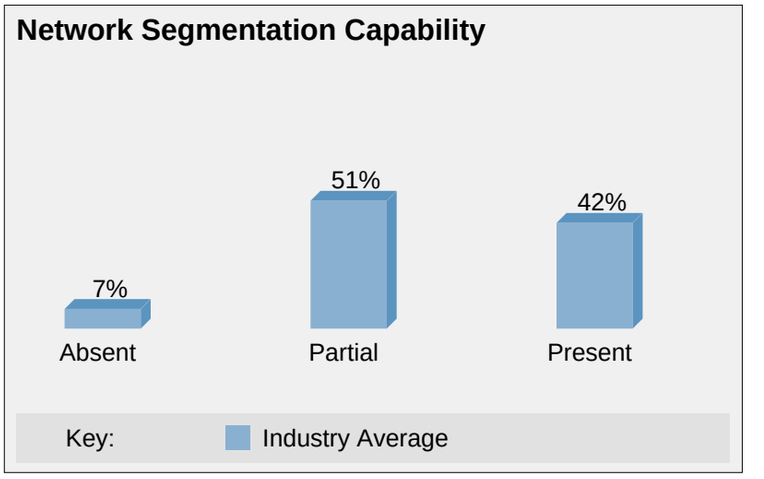
NIST: SP 800-53 Rev. 4 SC-7, SC-32

PCI DSS: v3.1 Requirement 1

CIS: v6.1 CSC 14.1, CSC 12, CSC 15.9

GDPR: Regulation 49 resist unlawful or malicious actions

ISO: IEC 80001-1:2010:(4.4.4)



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Network Segmentation is relevant to the following breach types:

- Cybercrime Hacking
- Insider Accidents or Workarounds
- Malicious Insiders or Fraud
- Insider Snooping
- Ransomware

4.28 Network Intrusion Prevention System

Technology and processes to detect and prevent intrusions into the organization's network.

Workshop Overview More Info

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: 27002:2013 Section 13.1 Network Security Management

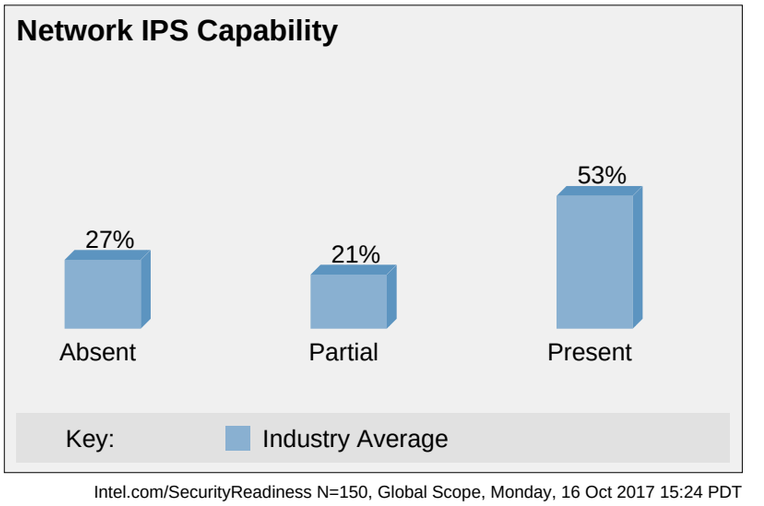
NIST: SP 800-53 Rev. 4 SI-4, SC-7

PCI DSS: v3.1 Requirement 1

CIS: v6.1 CSC 12, CSC 15.3

GDPR: Regulation 49 resist unlawful or malicious actions

ISO: IEC 80001-1:2010:(4.4.4)



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Network Intrusion Prevention System is relevant to the following breach types:

- Cybercrime Hacking
- Ransomware

4.29 Business Associate Agreements

Contractual agreements covering the security and privacy of sensitive information with all third-party sub-contractors or data processors that work with sensitive information.

Workshop Overview More Info

HIPAA: 45 CFR 164.308(b)(1)

ISO: 27002:2013 Section 13.2.4 Confidentiality or Non-Disclosure Agreements

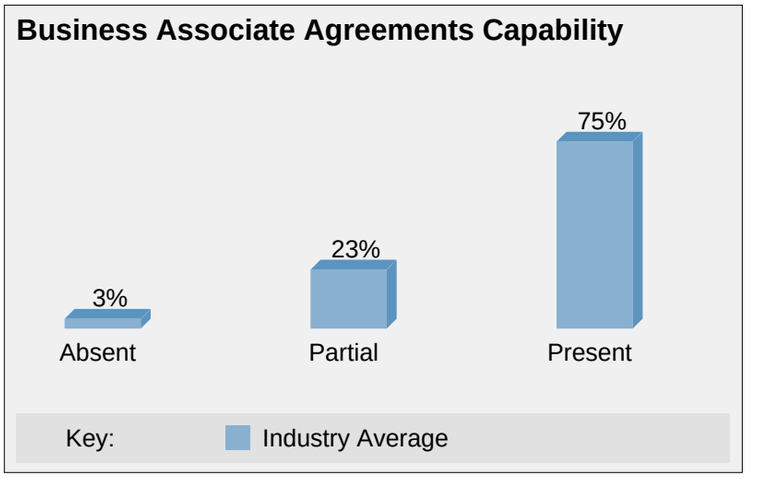
NIST: SP 800-53 Rev. 4 SA-9

PCI DSS: v3.1 Section 12.8.2

GDPR: Article 32 4 controller and processor ensure compliance

ISO: IEC 80001-1:2010:(3.5,3.6,4.3.4), IEC/TR 80001-2-2:2012:(5.14), ISO/TR 80001-2-6:2014

EU MDR: 2017/745 Annex I:(17.4)



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Business Associate Agreements is relevant to the following breach types:
- Business Associates

4.30 Virtualization

Virtualizing clients so that sensitive information exists only on strongly managed and secured servers and not on clients and mobile devices that are at higher risk of loss or theft.

Workshop Overview More Info

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: 27002:2013 Section 11.2.1 Equipment Siting and Protection

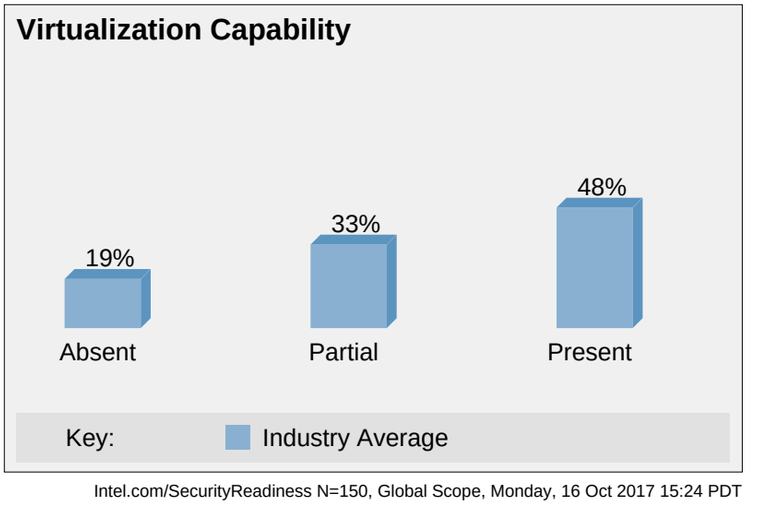
NIST: SP 800-53 Rev. 4 SC-2, SC-7, SI-14

PCI DSS: v3.1 Section 2.2.1

CIS: v6.1 CSC 2.4

GDPR: Regulation 83 protect confidentiality of personal data

ISO: IEC 80001-1:2010:(4.4.4)



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Virtualization is relevant to the following breach types:
- Loss or Theft of Mobile Device or Media

4.31 Server Solid State Drive (Encrypted)

Self-encrypting solid state drives used on servers to protect sensitive information at rest, with high performance.

Workshop Overview More Info

HIPAA: 45 CFR 164.312

ISO: 27002:2013 Section 10 Cryptography

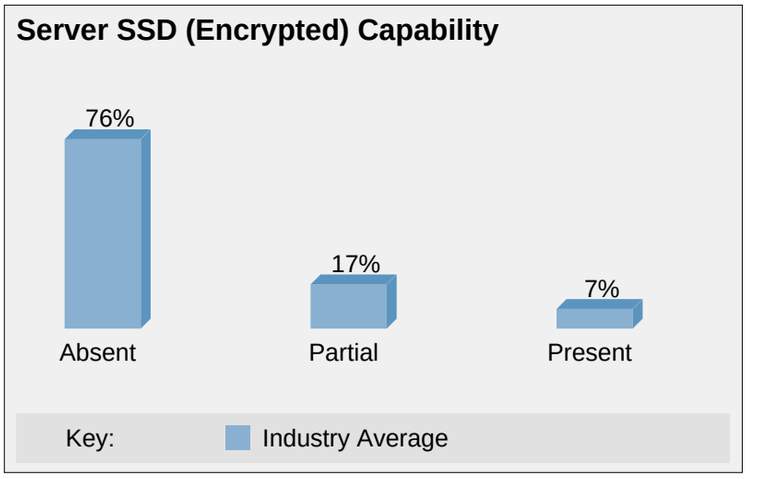
NIST: SP 800-53 Rev. 4 SC-28

PCI DSS: v3.1 Section 3.4.1

CIS: v6.1 CSC 13.2, CSC 14.5

GDPR: Article 32 1a encryption of personal data

ISO: IEC 80001-1:2010:(4.4.4)



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Server Solid State Drive (Encrypted) is relevant to the following breach types:
- Loss or Theft of Mobile Device or Media - Malicious Insiders or Fraud - Improper Disposal

4.32 Network Data Loss Prevention (Prevention Mode)

Network Data Loss Prevention ability to prevent non-compliance with the policy of the organization regarding network traffic. For example, if an organization has a policy against sending sensitive information attached to emails, NDLP can detect and block such emails and notify the sender to reduce risk of recurrence.

Workshop Overview More Info

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

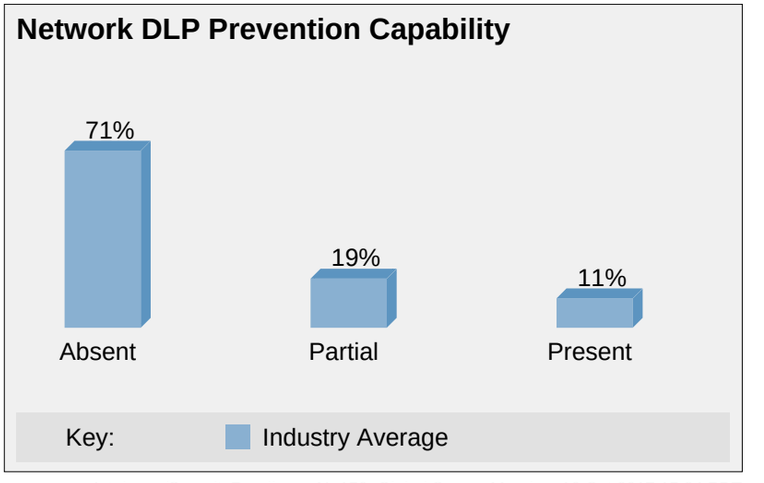
ISO: 27002:2013 Section 13.1 Network Security Management

NIST: SP 800-53 Rev. 4 SC-7

PCI DSS: v3.1 Requirement 3

CIS: v6.1 CSC 13.6

GDPR: Regulation 49 resist accidental events that compromise confidentiality



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Network Data Loss Prevention (Prevention Mode) is relevant to the following breach types:
- Cybercrime Hacking - Insider Accidents or Workarounds - Malicious Insiders or Fraud
- Insider Snooping - Ransomware

4.33 Database Activity Monitoring

Monitoring of database activity in order to detect possible intrusion, for example in a case where database administrator credentials may have been compromised and used for covert unauthorized access to sensitive information in the database.

Workshop Overview More Info

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: 27002:2013 Section 12.4 Logging and Monitoring

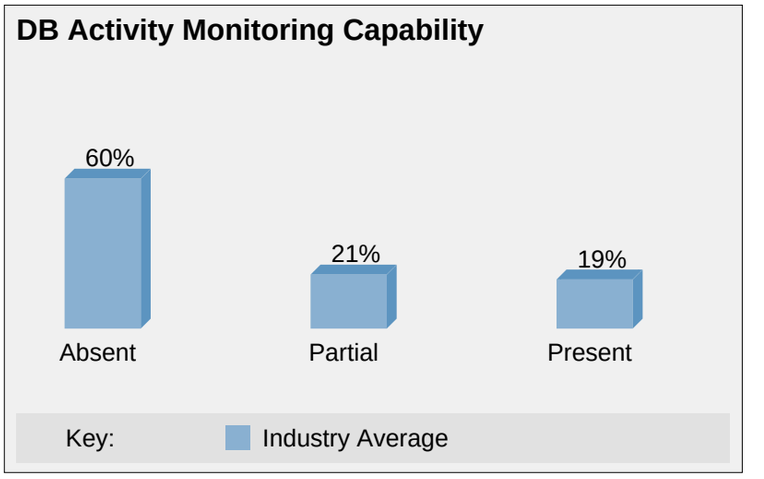
NIST: SP 800-53 Rev. 4 AC-23

PCI DSS: v3.1 Requirement 10

CIS: v6.1 CSC 5.1

GDPR: Regulation 39 security and preventing unauthorised access

ISO: IEC 80001-1:2010:(4.6.1)



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Database Activity Monitoring is relevant to the following breach types:

- Cybercrime Hacking
- Malicious Insiders or Fraud
- Insider Snooping

4.34 Digital Forensics

Ability to conduct forensic analysis of IT infrastructure, often in the event of a suspected security incident, to detect unauthorized access to sensitive information, and establish whether a breach occurred and, if so, characteristics such as timing and extent.

Workshop Overview More Info

HIPAA: Incident Management - Forensics

ISO: 27002:2013 Section 16.1.7 Collection of Evidence

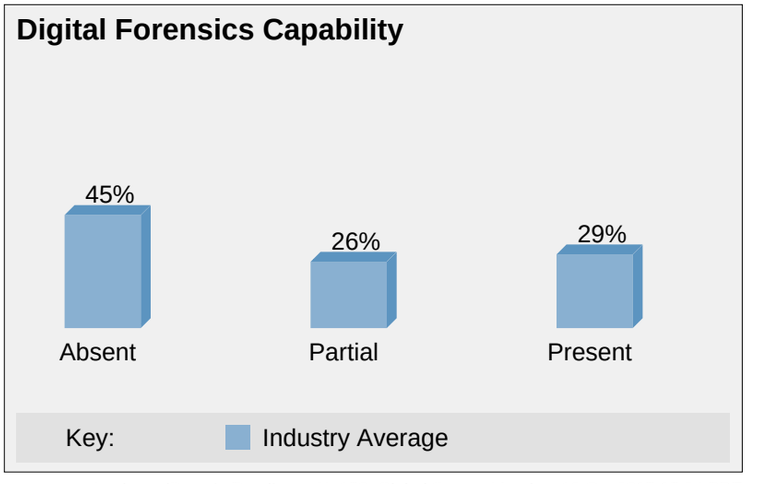
NIST: SP 800-53 Rev. 4 IR-7, 10

PCI DSS: v3.1 Sections 10.3 and A1.4

CIS: v6.1 CSC 17

GDPR: Regulation 83 protect confidentiality of personal data

ISO: IEC 80001-1:2010:(4.6.1)



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Digital Forensics is relevant to the following breach types:

- Cybercrime Hacking
- Business Associates
- Improper Disposal
- Loss or Theft of Mobile Device or Media
- Malicious Insiders or Fraud
- Ransomware
- Insider Accidents or Workarounds
- Insider Snooping

4.35 Security Information and Event Management

Security Information and Event Management includes real-time analysis of logs and security alerts generated by network hardware and applications.

Workshop Overview More Info

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: 27002:2013 Section 12.4 Logging and Monitoring

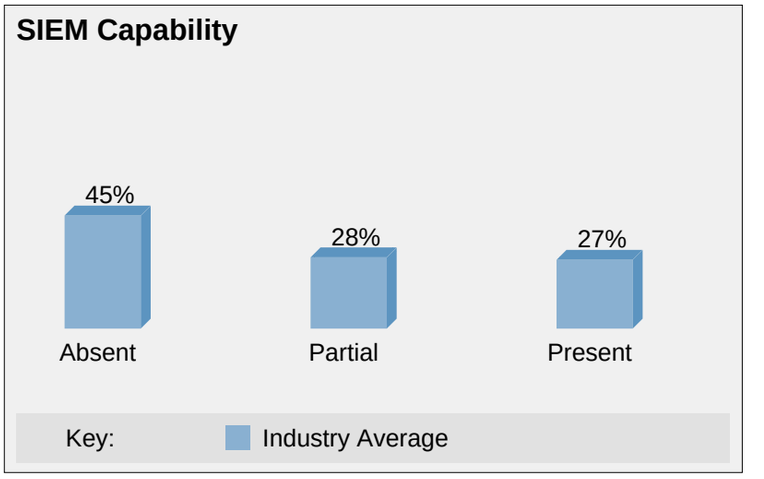
NIST: SP 800-53 Rev. 4 SI-4

PCI DSS: v3.1 Section 10.6

CIS: v6.1 CSC 6.6

GDPR: Regulation 39 security and preventing unauthorised access

ISO: IEC 80001-1:2010:(4.6.2)



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Security Information and Event Management is relevant to the following breach types:

- Cybercrime Hacking
- Malicious Insiders or Fraud
- Insider Snooping
- Ransomware

4.36 Threat Intelligence

Acquisition of threat intelligence information, such as where suspicious activities or intrusions have occurred, the nature of the incidents, and appropriate safeguards and actions to mitigate, and sharing this information across security infrastructure in near-real time to improve defense and minimize recurrence / extent of future intrusions / breaches. Threat intelligence can include information acquired through cybersecurity information sharing forums, reputational information, sandboxing and static or dynamic analysis of suspect executables, or behavioral analytics.

Workshop Overview More Info

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: 27002:2013 Section 12.6 Technical Vulnerability Management

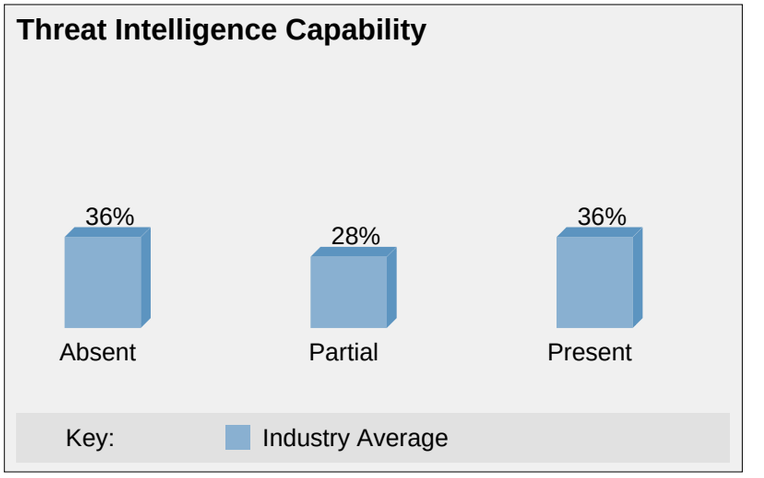
NIST: SP 800-53 Rev. 4 SI-4, SI-5, SC-7, SC-44

PCI DSS: v3.1 Requirement 5

CIS: v6.1 CSC 8.5, CSC 12, CSC 16.10

GDPR: Regulation 39 security and preventing unauthorised access

ISO: IEC 80001-1:2010:(4.6.1)



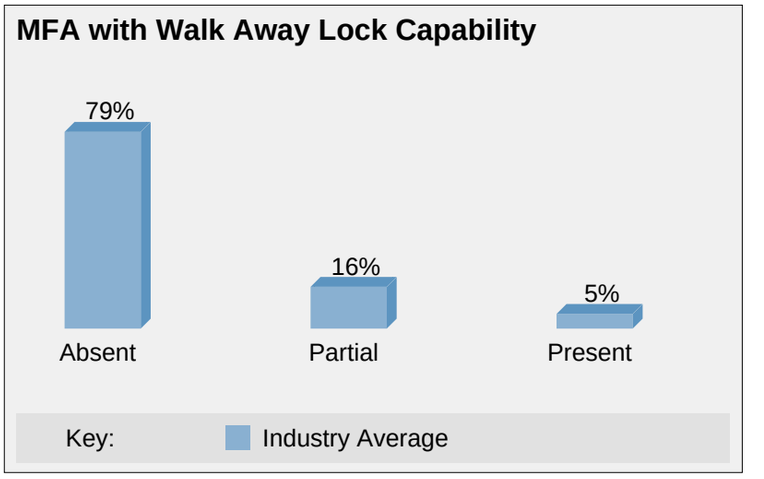
Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Threat Intelligence is relevant to the following breach types:

- Cybercrime Hacking
- Insider Accidents or Workarounds
- Business Associates
- Malicious Insiders or Fraud
- Insider Snooping
- Ransomware

4.37 Multi-Factor Authentication with Walk-Away Lock

Multi-Factor Authentication including multiple factors such as what you know (e.g., username / password), what you have (e.g., security hardware token), and what you are (e.g., biometrics). Walk-away lock is the ability to automatically lock a secure session the moment a worker walks away from the endpoint device being used to access that session. Intended to mitigate risk of an unauthorized individual hijacking a secure session that an authorized user established and has abandoned, and before timeout lock has occurred.



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Workshop Overview More Info

HIPAA: 45 CFR 164.312

ISO: 27002:2013 Section 9 Access Control

NIST: SP 800-53 Rev. 4 IA-2, AC-2, AC-11, AC-12

PCI DSS: v3.1 Requirement 8

CIS: v6.1 CSC 5.6, CSC 11.4, CSC 12.6, CSC 16.11

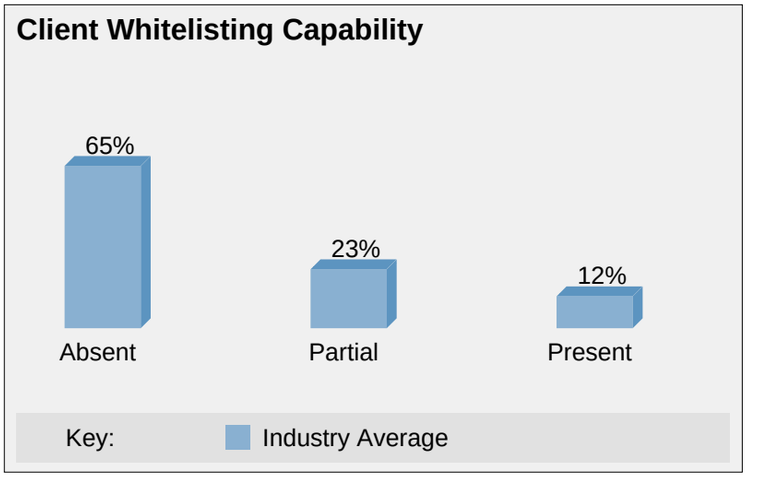
GDPR: Regulation 39 security and preventing unauthorised access

ISO: IEC/TR 80001-2-2:2012:(5.1)

Multi-Factor Authentication with Walk-Away Lock is relevant to the following breach types:
- Cybercrime Hacking - Loss or Theft of Mobile Device or Media - Malicious Insiders or Fraud
- Insider Snooping

4.38 Client Application Whitelisting

Ability to control what applications run on a client device, and block unauthorized applications from running. Typically, signature-based detection and enforcement. Includes secure processes for provisioning, managing, and updating whitelists.



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Workshop Overview More Info

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: 27002:2013 Section 12.2.1 Controls Against Malware

NIST: SP 800-53 Rev. 4 CM-7

PCI DSS: v3.1 Requirement 5

CIS: v6.1 CSC 2.2

GDPR: Regulation 49 resist unlawful or malicious actions

ISO: IEC/TR 80001-2-2:2012:(5.3)

Client Application Whitelisting is relevant to the following breach types:
- Loss or Theft of Mobile Device or Media - Insider Accidents or Workarounds - Malicious Insiders or Fraud
- Insider Snooping - Ransomware

4.39 Server Application Whitelisting

Ability to control what applications run on servers and block unauthorized applications from running. Typically, signature-based detection and enforcement. Includes secure processes for provisioning, managing, and updating whitelists.

Workshop Overview More Info

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: 27002:2013 Section 12.2.1 Controls Against Malware

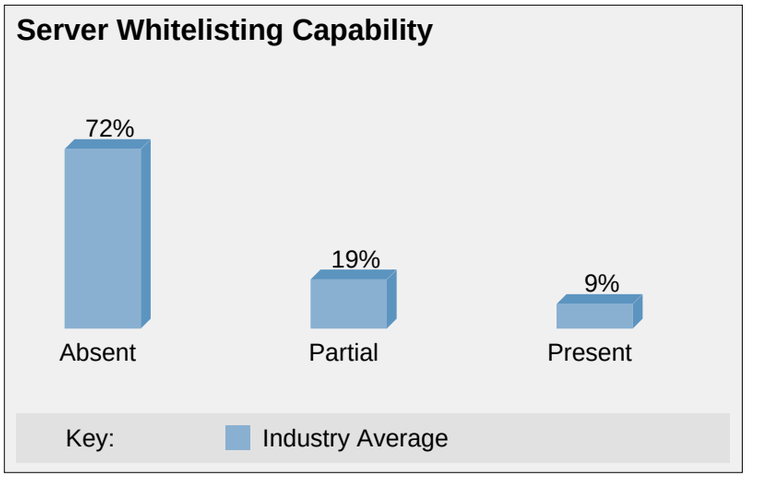
NIST: SP 800-53 Rev. 4 CM-7

PCI DSS: v3.1 Requirement 5

CIS: v6.1 CSC 2.2

GDPR: Regulation 49 resist unlawful or malicious actions

ISO: IEC 80001-1:2010:(4.4.4), IEC/TR 80001-2-2:2012:(5.11)



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Server Application Whitelisting is relevant to the following breach types:

- Cybercrime Hacking
- Malicious Insiders or Fraud
- Insider Snooping
- Ransomware

4.40 De-Identification / Anonymization

The ability to remove or mask personally identifiable information fields in sensitive information in order to enable the subsequent limited use of such information while minimizing risk of breach. These fields can include any information that may be used to identify, locate, or contact individuals associated with the sensitive information records.

Workshop Overview More Info

HIPAA: HHS Guidance

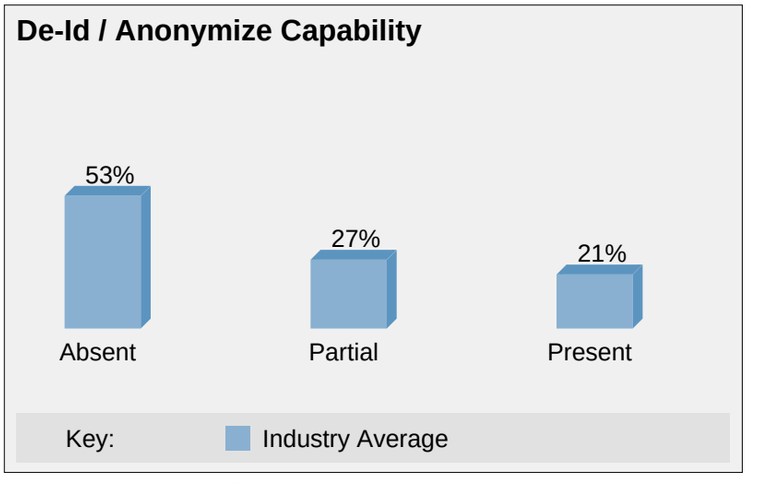
ISO: 27002:2013 Section 9.4.1 Information Access Restriction

NIST: SP 800-53 Rev. 4 MP-6, DM-2, DM-3

PCI DSS: v3.1 Requirement 3

GDPR: Regulation 26 anonymous information

ISO: IEC/TR 80001-2-2:2012:(5.6)



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

De-Identification / Anonymization is relevant to the following breach types:

- Cybercrime Hacking
- Loss or Theft of Mobile Device or Media
- Insider Accidents or Workarounds
- Business Associates
- Malicious Insiders or Fraud
- Insider Snooping
- Improper Disposal

4.41 Tokenization

Replacing personally identifiable information fields in sensitive information records with opaque, unique tokens and storing the mappings from these tokens back to the real data values in a secure, access-controlled database.

Workshop Overview More Info

HIPAA: HHS Guidance

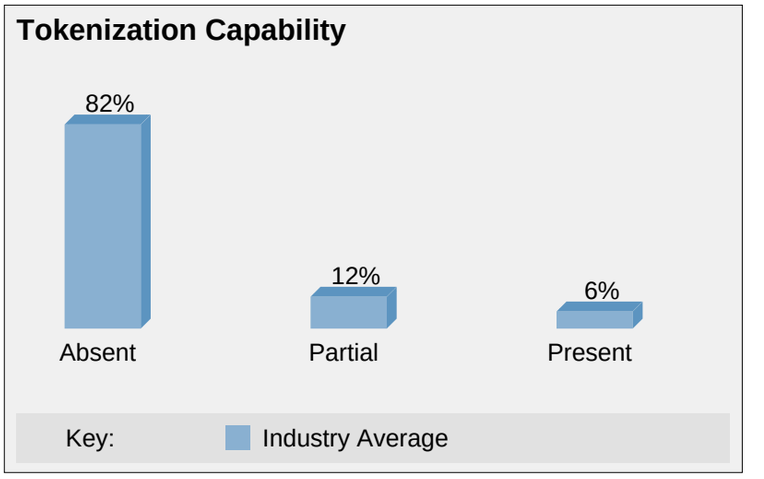
ISO: 27002:2013 Section 9.4.1 Information Access Restriction

NIST: SP 800-53 Rev. 4 MP-6, DM-2, DM-3

PCI DSS: v3.1 Requirement 3

GDPR: Article 32 1a pseudonymisation of personal data

ISO: IEC 80001-1:2010:(4.4.4)



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Tokenization is relevant to the following breach types:

- Cybercrime Hacking
- Loss or Theft of Mobile Device or Media
- Insider Accidents or Workarounds
- Improper Disposal

4.42 Business Continuity and Disaster Recovery

People, process, and technology to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster or disruption. This includes having a plan, as well as failover capabilities to support continuity of critical business processes in the event of a disruption.

Workshop Overview More Info

HIPAA: Security Rule - Protect Availability

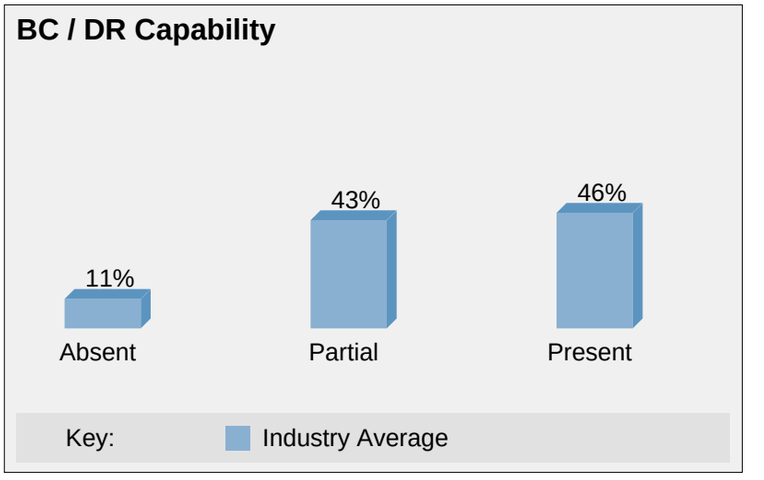
ISO: 27002:2013 Section 11.1.4 Protecting Against External and Environmental Threats

NIST: SP 800-53 Rev. 4 CP-1 to 13

PCI DSS: v3.1 Section 12.10.1

CIS: v6.1 CSC Governance Item #4: Business Continuity and Disaster Recovery

GDPR: Article 32 1c restore availability and access to personal data



Intel.com/SecurityReadiness N=150, Global Scope, Monday, 16 Oct 2017 15:24 PDT

Business Continuity and Disaster Recovery is relevant to the following breach types:

- Cybercrime Hacking
- Malicious Insiders or Fraud
- Ransomware