Health and Life Sciences Security Readiness Report

For Star Healthcare

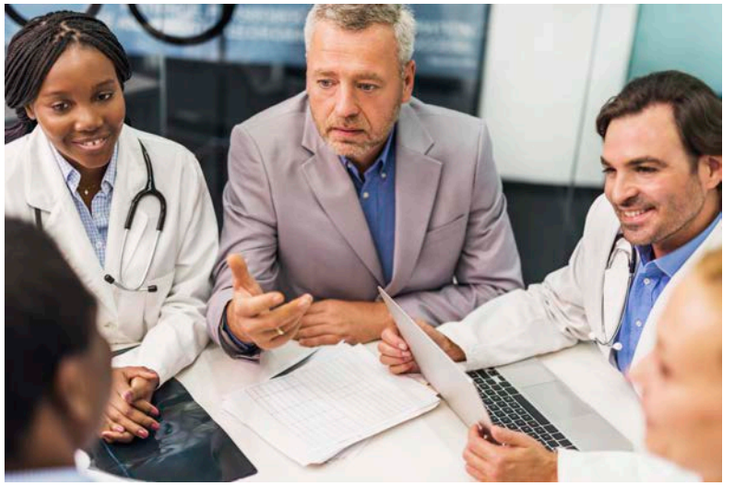
(Global Scope, N=151)

Fictitious organization and assessment data. For demo purposes only.

Draft

Contents

Reported	Monday, 23 Oct 2017 09:04 PDT
Assessed	Monday, 1 Feb 2016 11:18 PST
Organization	Star Healthcare Provider, Large, US
Account Manager	Kathy Trustworthy Senior Account Manager Sage Data Security 123 456 7890 Kathy.Trustworthy@SageDataSecurity.com
Assessor	Joe Whitehat CISSP Senior Security Assessor Sage Data Security Joe.Whitehat@SageDataSecurity.com
Comparison	Global Scope, N=151



Executive Summary

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 the results of a Security Readiness Workshop and subsequent analysis of your organization's security capabilities. It compares your security maturity, priorities across breach types, and your security capabilities with those of other health and life sciences organizations that have also been analyzed up to the time of this report. 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 assessment is 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 Report.

In this engagement, 42 security capabilities were assessed. Star Healthcare has 75% of the capabilities in the Baseline maturity level (1% ahead of average), 46% in Enhanced (5% behind average), and 29% in Advanced (1% behind average). The security maturity level of Star Healthcare peaks in the Baseline level. See Maturity Overview for further details on the assessment of the security maturity level of Star Healthcare and how this compares with the broader health and life sciences industry.

Star Healthcare is leading the industry (upper percentile range) in terms of readiness for the following breach types: Loss or Theft of Mobile Device or Media, Business Associates, Insider Snooping, and Improper Disposal. Star Healthcare is lagging the industry (lower percentile range) in terms of readiness for the following breach types: Cybercrime Hacking. See Priorities and Readiness for further details on Star Healthcare readiness for various breach types and how this compares, in terms of percentile, to the rest of the health and life sciences industry. At Star Healthcare, Cybercrime Hacking, Malicious Insiders or Fraud, and Ransomware are considered High priority. Loss or Theft of Mobile Device or Media, Insider Accidents or Workarounds, Business Associates, and Insider Snooping are considered Medium priority. Improper Disposal is considered Low priority. Of the 8 priorities assessed, 3 of these are significantly different from the average priorities assigned by other

health and life sciences organizations to these breach types. See Priorities and Readiness for further details on priorities assigned by Star Healthcare to various breach types and how these priorities compare to the health and life sciences industry.

In the Baseline maturity level, Star Healthcare was behind the average in 4 capabilities : Anti-Malware, Email Gateway, Web Gateway, and Backup and Restore. In the Enhanced maturity level, Star Healthcare was behind the average in 6 capabilities : Device Control, Penetration Testing, Vulnerability Scanning, Network Data Loss Prevention (Discovery Mode), Multi-Factor Authentication with Timeout, Secure Remote Administration, and Business Associate Agreements. In the Advanced maturity level, Star Healthcare was behind the average in 1 capability : Security Information and Event Management. See Maturity Details for how Star Healthcare was assessed across 42 security capabilities in the maturity model and how this compares with the health and life sciences industry.

During this assessment, 30 gaps in security capabilities were identified. These represent new opportunities for Star Healthcare to improve its security posture and further mitigate risk of breaches. Addressing these security capability gaps may also improve usability, reduce cost, and improve efficiency of IT operations. For details on specific gaps and opportunities for improvement, see Gaps and Opportunities for Improvement . It is recommended that Star Healthcare review these opportunities, and specific products, technologies, and services that can help, together with the account manager and assessor listed at the beginning of this report.

A 12-step, multi-year Action Plan is recommended for Star Healthcare to improve security posture and further reduce residual risk of breaches.

This report includes traceability to the following security and privacy standards, regulations, and data protection laws:

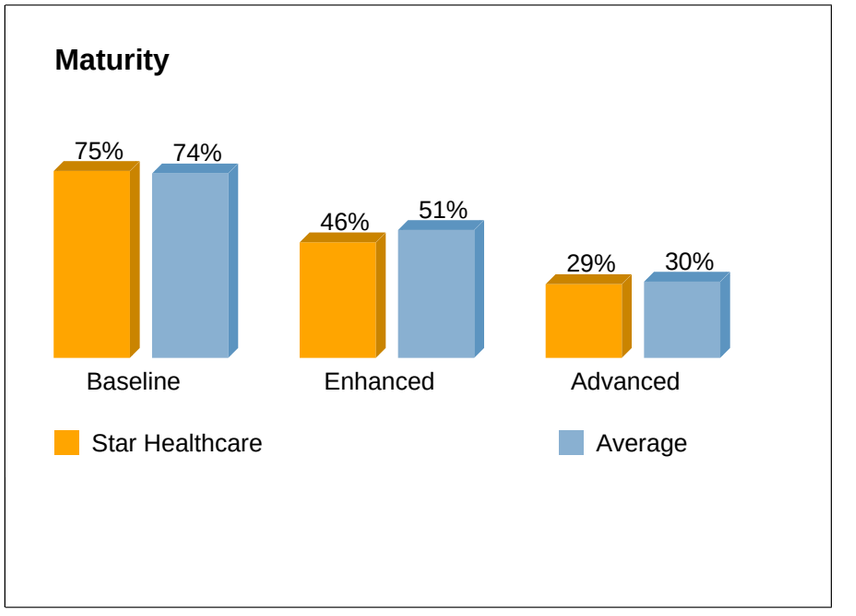
- HIPAA
- ISO/IEC 27000 - Series
- NIST
- PCI DSS
- CIS Controls
- GDPR
- ISO/IEC 80001 - Series
- EU Medical Device Regulation 2017/745

In addressing any security capability gaps identified in this report, such traceability helps you understand how addressing these gaps may also help with compliance with applicable standards, regulations, and data protection laws. Please see each of the 42 capabilities in the Capabilities section for details.

Thank you for participating in the Intel® Health and Life Sciences Security Readiness Program. We welcome any further updates you may have on your security priorities and capabilities to ensure the accuracy of your assessment and this report. Please coordinate any such updates with your account executive and assessor. We also 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

Your maturity is shown as the percentage of security capabilities you have implemented in the Baseline, Enhanced, and Advanced maturity levels. As your security posture improves, your assessment at each of these maturity levels will approach 100%. Important aspects to note in these results are the level at which your maturity peaks and how your Baseline, Enhanced, and Advanced maturity percentages compare with the rest of the industry. A higher-than-average percentage in a given maturity tier indicates that you are ahead of the industry average in that tier. These are high-level results for a broad overview of your maturity. See subsequent sections of this report for details on how your security priorities, readiness, and capabilities compare with the industry average. See Maturity Details for a detailed view of how you assessed across 42 capabilities, any gaps, and whether you may be lagging the industry in implementing any capabilities.



2. Priorities and Readiness

Your priority, or level of concern, and readiness have been analyzed across 8 breach types. Results enable you to compare your priority and readiness with the rest of the industry. If the Priority Assessed is significantly different than the industry average, an alert will be shown in Priority Alerts. Readiness Assessed for each breach type is the percentage of relevant security capabilities you currently have implemented. Readiness Percentile is the percentile Star Healthcare falls within, across all organizations assessed, based on their Readiness Assessed scores. The most important results here are the Readiness Percentiles for each of the breach types. Pay careful attention to any red Readiness Percentile results indicating lower percentile range (less than 33%). Click on the associated breach type link for more details.

Star Healthcare Breach Priorities and Readiness

#	Breach Type	Priority Assessed	Priority Alerts	Readiness Assessed	Readiness Percentile
2.1	Cybercrime Hacking	High		48%	28%
2.2	Loss or Theft of Mobile Device or Media	Medium		58%	69%
2.3	Insider Accidents or Workarounds	Medium		56%	60%
2.4	Business Associates	Medium		72%	70%
2.5	Malicious Insiders or Fraud	High	⚠ > Avg	54%	59%
2.6	Insider Snooping	Medium		56%	68%
2.7	Improper Disposal	Low	⚠ < Avg	67%	85%
2.8	Ransomware	High		57%	42%

⚠ Star Healthcare priority differs significantly from health and life sciences industry average

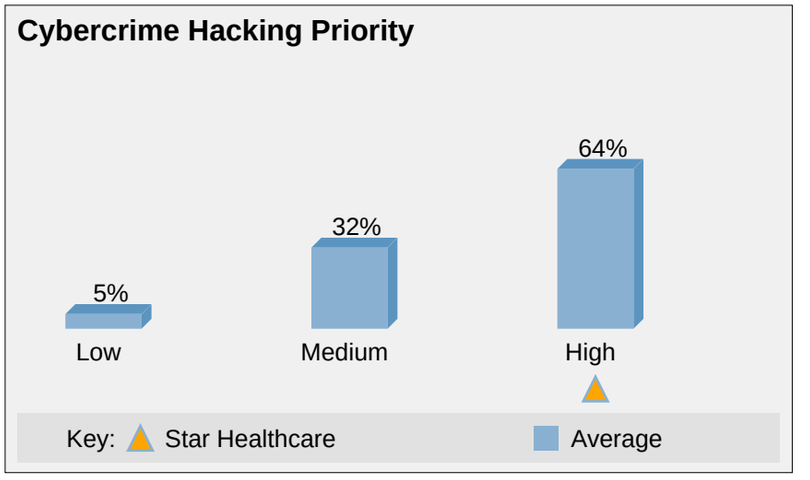
2.1 Cybercrime Hacking

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.

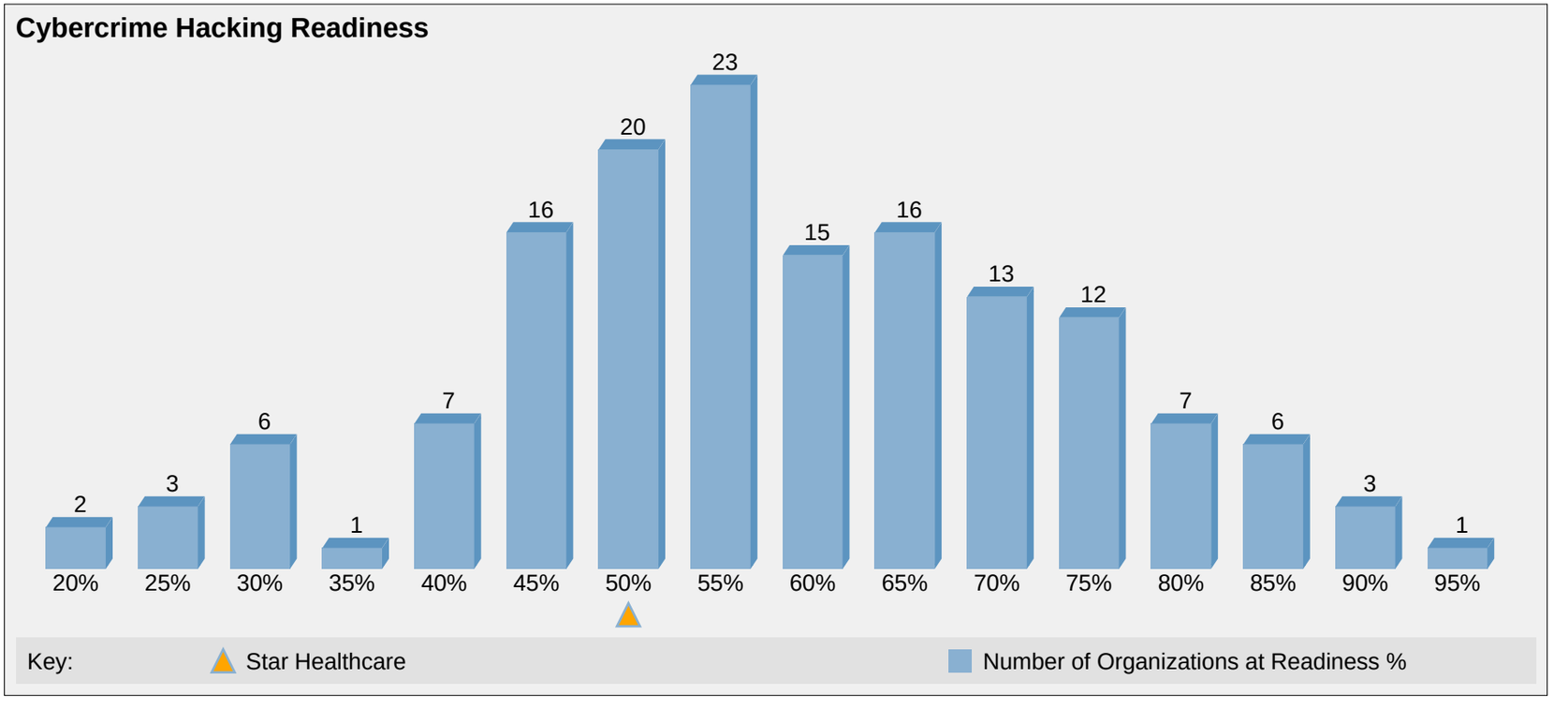
Workshop Overview More Info

Star Healthcare assigned a High priority to Cybercrime Hacking.

This is comparable to the average priority assigned by the rest of the health and life sciences industry to this type of breach.



Star Healthcare currently has approximately **48%** of the security capabilities relevant to Cybercrime Hacking. Based on this metric, when compared to other health and life sciences organizations, Star Healthcare is at the **28%** readiness percentile, putting it in the lower percentile range, lagging the health and life sciences industry. As Star Healthcare improves its Cybercrime Hacking readiness, the slider on the graph below would move to the right, corresponding to an increase in both its percentage of relevant security capabilities implemented and its readiness percentile.



The capabilities below are relevant to mitigating risk of Cybercrime Hacking breaches. This table shows the capabilities Star Healthcare has and where there are gaps. Alerts are shown where Star Healthcare lags the industry average - i.e., where Star Healthcare has gaps in capabilities that most other organizations already have implemented.

Star Healthcare Cybercrime Hacking Security Maturity

Baseline	Enhanced	Advanced
⊕ Policy	⊖ ⚠ ! Penetration Testing, Vulnerability Scanning	⊖ Network Data Loss Prevention (Prevention Mode)
⊕ Risk Assessment	⊖ ⚠ Network Data Loss Prevention (Discovery Mode)	~ Database Activity Monitoring
⊕ Audit and Compliance	⊖ ⚠ ! Multi-Factor Authentication with Timeout	~ Digital Forensics
~ ! User Awareness Training	⊖ ⚠ ! Secure Remote Administration	⊖ ⚠ ! Security Information and Event Management
~ ⚠ ! Anti-Malware	⊕ Network Segmentation	~ Threat Intelligence
⊕ Identity and Access Management, Single-Factor Access Control	~ Network Intrusion Prevention System	⊖ ! Multi-Factor Authentication with Walk-Away Lock
⊕ Firewall		~ Server Application Whitelisting
~ ⚠ ! Email Gateway		~ De-Identification / Anonymization
~ ⚠ ! Web Gateway		⊖ Tokenization
~ Vulnerability Management, Patching		~ Business Continuity and Disaster Recovery
⊕ Security Incident Response Plan		
~ ⚠ ! Backup and Restore		

(⊕ = present, ~ = partially present, ⊖ = not present, ⚠ = lagging industry in implementing, ! = action item in plan)

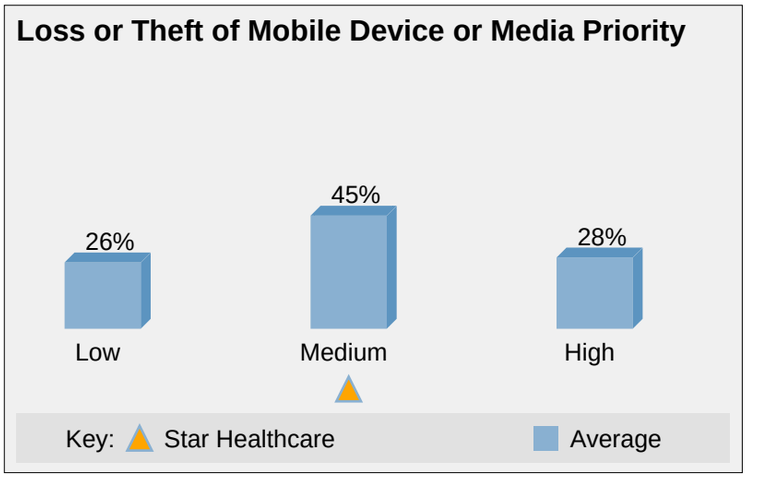
2.2 Loss or Theft of Mobile Device or Media

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.

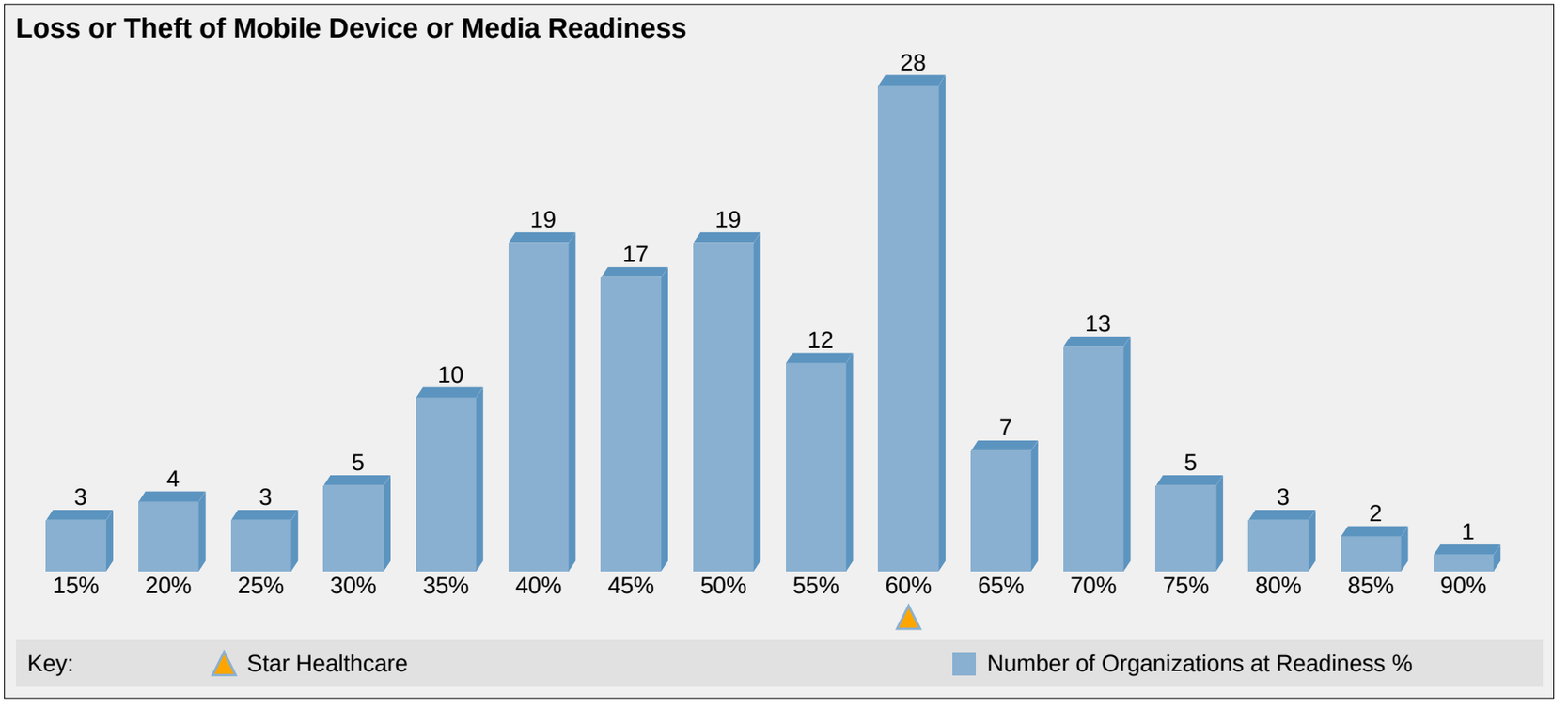
Workshop Overview More Info

Star Healthcare assigned a Medium priority to Loss or Theft of Mobile Device or Media.

This is comparable to the average priority assigned by the rest of the health and life sciences industry to this type of breach.



Star Healthcare currently has approximately **58%** of the security capabilities relevant to Loss or Theft of Mobile Device or Media. Based on this metric, when compared to other health and life sciences organizations, Star Healthcare is at the **69%** readiness percentile, putting it in the upper percentile range, leading the health and life sciences industry. As Star Healthcare improves its Loss or Theft of Mobile Device or Media readiness, the slider on the graph below would move to the right, corresponding to an increase in both its percentage of relevant security capabilities implemented and its readiness percentile.



The capabilities below are relevant to mitigating risk of Loss or Theft of Mobile Device or Media breaches. This table shows the capabilities Star Healthcare has and where there are gaps. Alerts are shown where Star Healthcare lags the industry average - i.e., where Star Healthcare has gaps in capabilities that most other organizations already have implemented.

Star Healthcare Loss or Theft of Mobile Device or Media Security Maturity

Baseline	Enhanced	Advanced
⊕ Policy	⊕ Client Solid State Drive (Encrypted)	⊖ Server Solid State Drive (Encrypted)
⊕ Risk Assessment	~ Anti-Theft: Remote Locate, Lock, Wipe	~ Digital Forensics
⊕ Audit and Compliance	⊖ ⚠ ! Multi-Factor Authentication with Timeout	⊖ ! Multi-Factor Authentication with Walk-Away Lock
~ ! User Awareness Training	⊖ ⚠ ! Secure Remote Administration	~ Client Application Whitelisting
~ ! Endpoint Device Encryption	~ Policy-Based Encryption for Files and Folders	~ De-Identification / Anonymization
~ ! Mobile Device Management	⊕ Server / Database / Backup Encryption	⊖ Tokenization
⊕ Endpoint Data Loss Prevention (Discovery Mode)	~ Virtualization	
⊕ Identity and Access Management, Single-Factor Access Control		
~ Vulnerability Management, Patching		
⊕ Security Incident Response Plan		
⊕ Secure Disposal		
~ ⚠ ! Backup and Restore		

(⊕ = present, ~ = partially present, ⊖ = not present, ⚠ = lagging industry in implementing, ! = action item in plan)

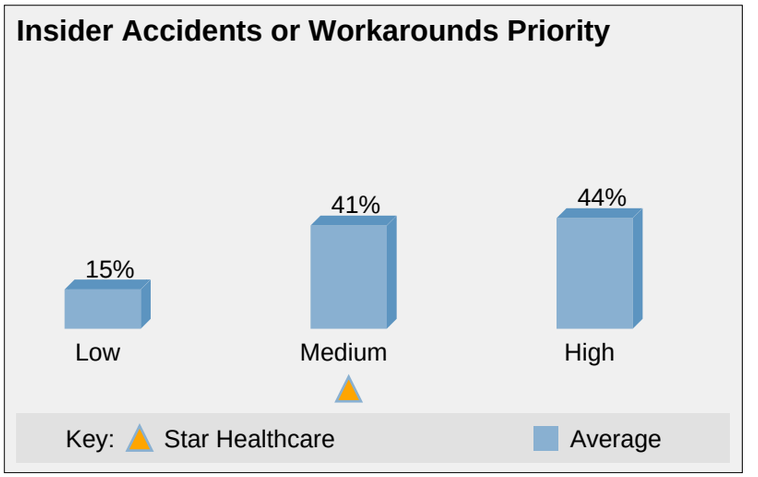
2.3 Insider Accidents or Workarounds

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.

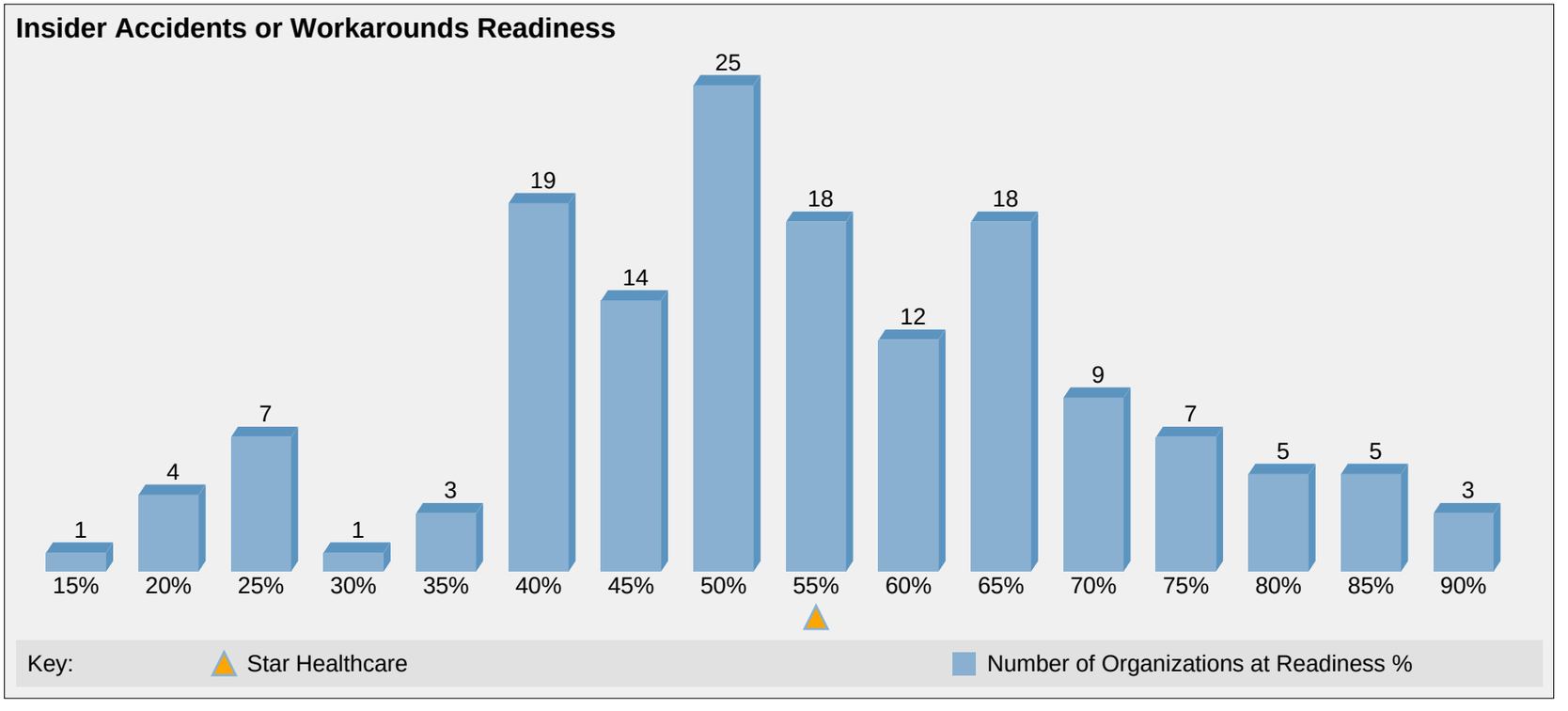
Workshop Overview More Info

Star Healthcare assigned a Medium priority to Insider Accidents or Workarounds.

This is comparable to the average priority assigned by the rest of the health and life sciences industry to this type of breach.



Star Healthcare currently has approximately **56%** of the security capabilities relevant to Insider Accidents or Workarounds. Based on this metric, when compared to other health and life sciences organizations, Star Healthcare is at the **60%** readiness percentile. As Star Healthcare improves its Insider Accidents or Workarounds readiness, the slider on the graph below would move to the right, corresponding to an increase in both its percentage of relevant security capabilities implemented and its readiness percentile.



The capabilities below are relevant to mitigating risk of Insider Accidents or Workarounds breaches. This table shows the capabilities Star Healthcare has and where there are gaps. Alerts are shown where Star Healthcare lags the industry average - i.e., where Star Healthcare has gaps in capabilities that most other organizations already have implemented.

Star Healthcare Insider Accidents or Workarounds Security Maturity

Baseline	Enhanced	Advanced
⊕ Policy	⊖ ⚠ Device Control	⊖ Network Data Loss Prevention (Prevention Mode)
⊕ Risk Assessment	⊕ Endpoint Data Loss Prevention (Prevention Mode)	~ Digital Forensics
⊕ Audit and Compliance	⊖ ⚠ Network Data Loss Prevention (Discovery Mode)	~ Threat Intelligence
~ ! User Awareness Training	⊖ ⚠ ! Secure Remote Administration	~ Client Application Whitelisting
~ ! Mobile Device Management	~ Policy-Based Encryption for Files and Folders	~ De-Identification / Anonymization
⊕ Endpoint Data Loss Prevention (Discovery Mode)	⊕ Network Segmentation	⊖ Tokenization
~ ⚠ ! Anti-Malware		
~ ⚠ ! Email Gateway		
~ ⚠ ! Web Gateway		
~ Vulnerability Management, Patching		
⊕ Security Incident Response Plan		
⊕ Secure Disposal		

(⊕ = present, ~ = partially present, ⊖ = not present, ⚠ = lagging industry in implementing, ! = action item in plan)

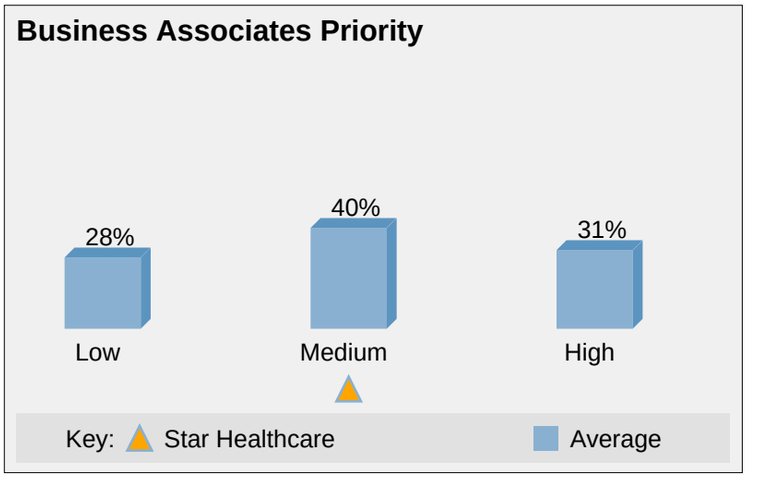
2.4 Business Associates

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.

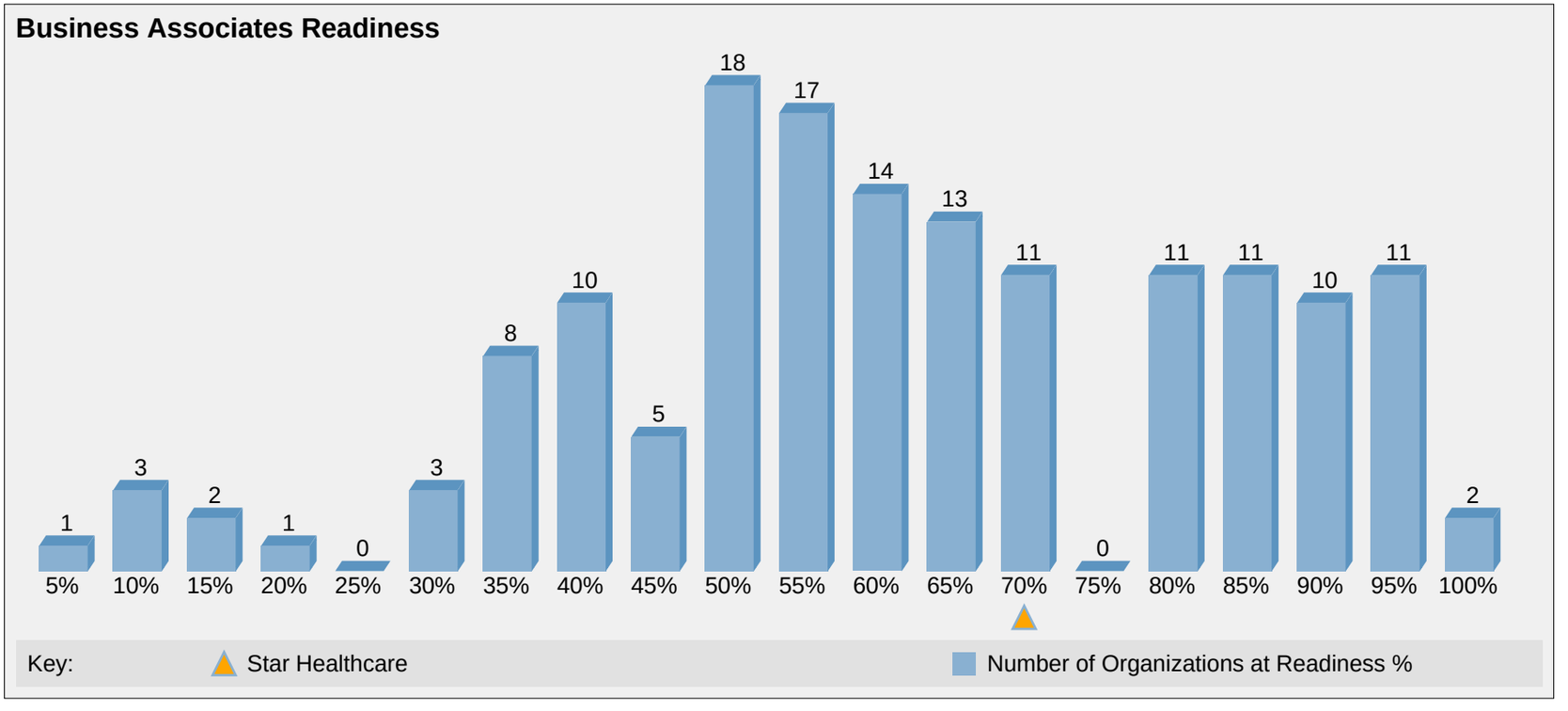
Workshop Overview More Info

Star Healthcare assigned a Medium priority to Business Associates.

This is comparable to the average priority assigned by the rest of the health and life sciences industry to this type of breach.



Star Healthcare currently has approximately **72%** of the security capabilities relevant to Business Associates. Based on this metric, when compared to other health and life sciences organizations, Star Healthcare is at the **70%** readiness percentile, putting it in the upper percentile range, leading the health and life sciences industry. As Star Healthcare improves its Business Associates readiness, the slider on the graph below would move to the right, corresponding to an increase in both its percentage of relevant security capabilities implemented and its readiness percentile.



The capabilities below are relevant to mitigating risk of Business Associates breaches. This table shows the capabilities Star Healthcare has and where there are gaps. Alerts are shown where Star Healthcare lags the industry average - i.e., where Star Healthcare has gaps in capabilities that most other organizations already have implemented.

Star Healthcare Business Associates Security Maturity

Baseline	Enhanced	Advanced
⊕ Policy	~ ⚠ Business Associate Agreements	~ Digital Forensics
⊕ Risk Assessment		~ Threat Intelligence
⊕ Audit and Compliance		~ De-Identification / Anonymization
~ ! User Awareness Training		
⊕ Security Incident Response Plan		

(⊕ = present, ~ = partially present, ⊖ = not present, ⚠ = lagging industry in implementing, ! = action item in plan)

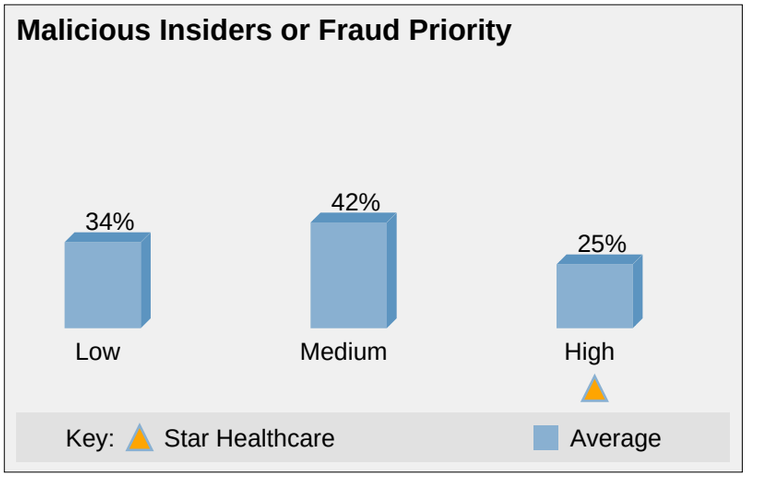
2.5 Malicious Insiders or Fraud

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.

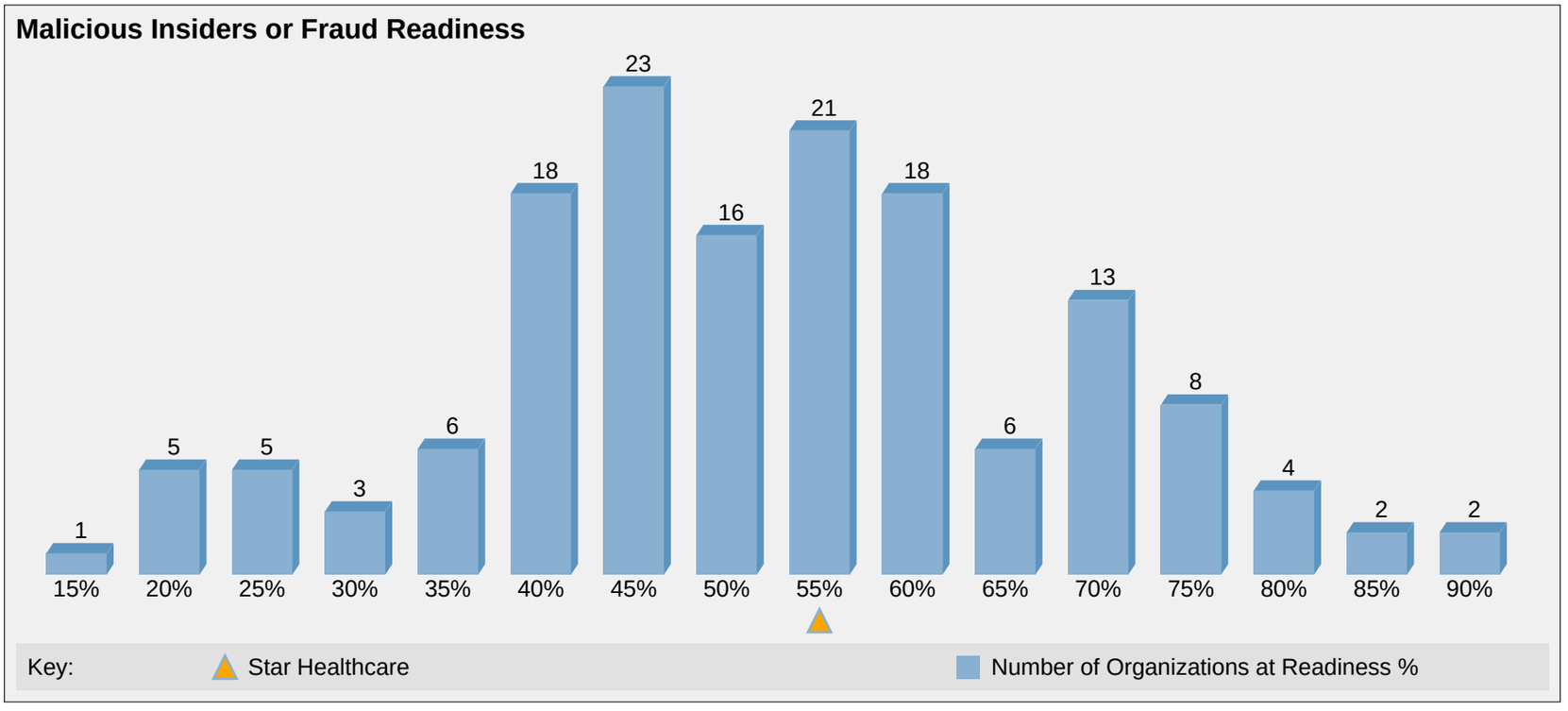
Workshop Overview More Info

Star Healthcare assigned a High priority to Malicious Insiders or Fraud.

⚠ This generated an alert because, on average, the health and life sciences industry prioritizes this type of breach lower.



Star Healthcare currently has approximately **54%** of the security capabilities relevant to Malicious Insiders or Fraud. Based on this metric, when compared to other health and life sciences organizations, Star Healthcare is at the **59%** readiness percentile. As Star Healthcare improves its Malicious Insiders or Fraud readiness, the slider on the graph below would move to the right, corresponding to an increase in both its percentage of relevant security capabilities implemented and its readiness percentile.



The capabilities below are relevant to mitigating risk of Malicious Insiders or Fraud breaches. This table shows the capabilities Star Healthcare has and where there are gaps. Alerts are shown where Star Healthcare lags the industry average - i.e., where Star Healthcare has gaps in capabilities that most other organizations already have implemented.

Star Healthcare Malicious Insiders or Fraud Security Maturity

Baseline	Enhanced	Advanced
⊕ Policy	⊖ ⚠ Device Control	⊖ Server Solid State Drive (Encrypted)
⊕ Risk Assessment	⊖ ⚠ ! Penetration Testing, Vulnerability Scanning	⊖ Network Data Loss Prevention (Prevention Mode)
⊕ Audit and Compliance	⊕ Client Solid State Drive (Encrypted)	~ Database Activity Monitoring
~ ! User Awareness Training	⊕ Endpoint Data Loss Prevention (Prevention Mode)	~ Digital Forensics
~ ! Endpoint Device Encryption	⊖ ⚠ Network Data Loss Prevention (Discovery Mode)	⊖ ⚠ ! Security Information and Event Management
~ ! Mobile Device Management	~ Anti-Theft: Remote Locate, Lock, Wipe	~ Threat Intelligence
⊕ Endpoint Data Loss Prevention (Discovery Mode)	⊖ ⚠ ! Multi-Factor Authentication with Timeout	⊖ ! Multi-Factor Authentication with Walk-Away Lock
⊕ Identity and Access Management, Single-Factor Access Control	⊖ ⚠ ! Secure Remote Administration	~ Client Application Whitelisting
⊕ Firewall	~ Policy-Based Encryption for Files and Folders	~ Server Application Whitelisting
~ ⚠ ! Email Gateway	⊕ Server / Database / Backup Encryption	~ De-Identification / Anonymization
~ ⚠ ! Web Gateway	⊕ Network Segmentation	~ Business Continuity and Disaster Recovery
~ Vulnerability Management, Patching		
⊕ Security Incident Response Plan		
⊕ Secure Disposal		
~ ⚠ ! Backup and Restore		

(⊕ = present, ~ = partially present, ⊖ = not present, ⚠ = lagging industry in implementing, ! = action item in plan)

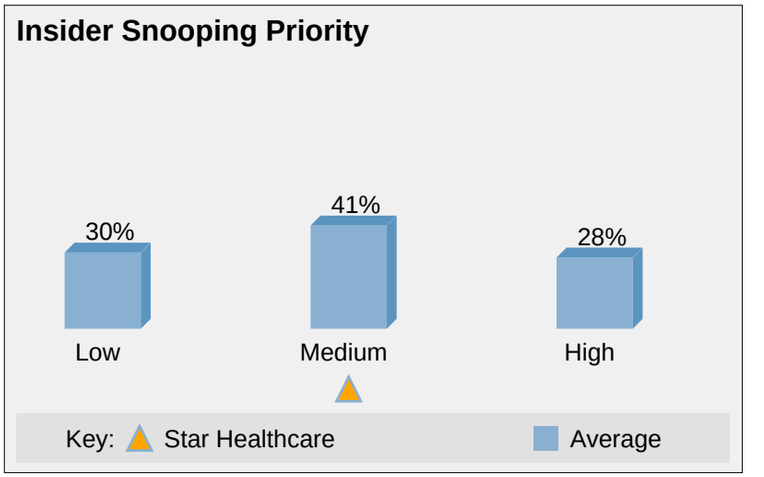
2.6 Insider Snooping

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

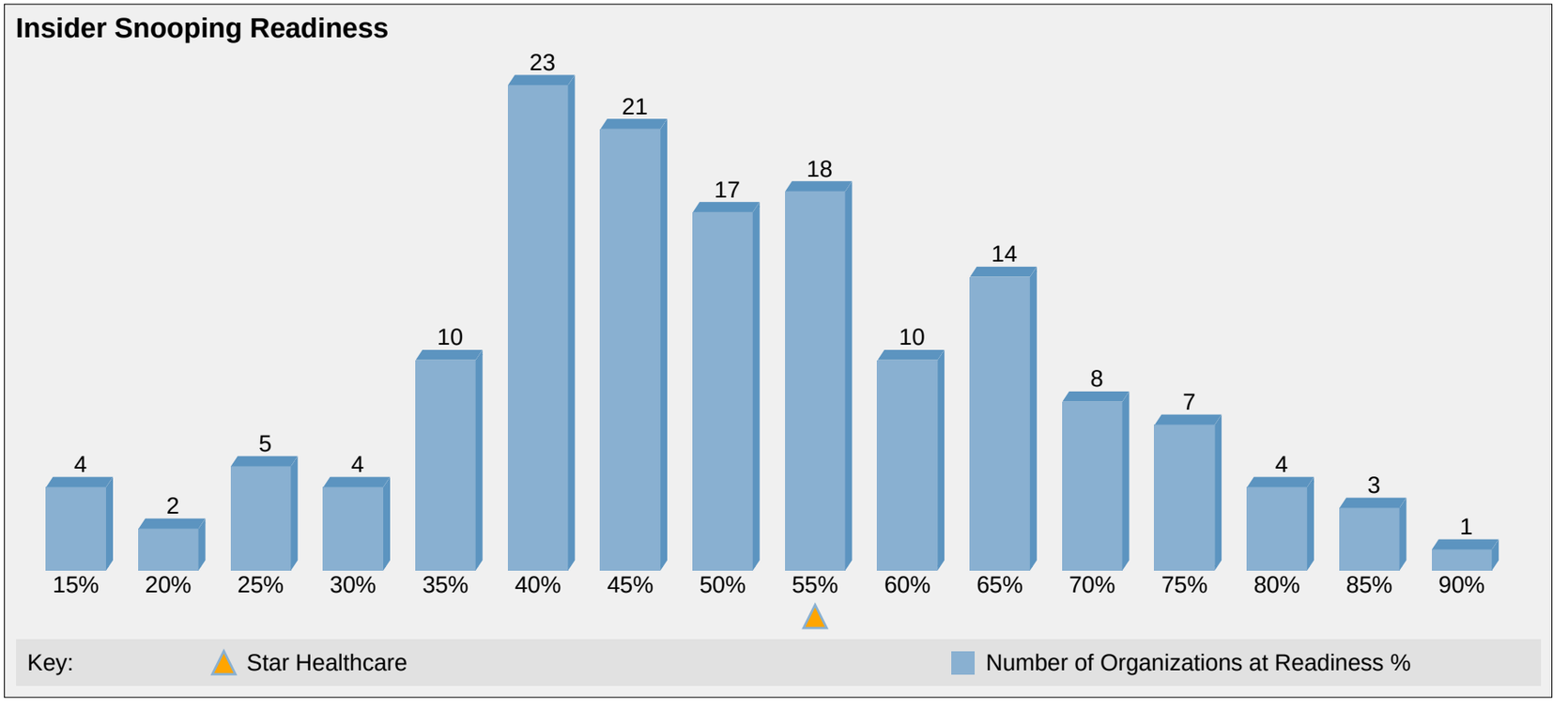
Workshop Overview More Info

Star Healthcare assigned a Medium priority to Insider Snooping.

This is comparable to the average priority assigned by the rest of the health and life sciences industry to this type of breach.



Star Healthcare currently has approximately **56%** of the security capabilities relevant to Insider Snooping. Based on this metric, when compared to other health and life sciences organizations, Star Healthcare is at the **68%** readiness percentile, putting it in the upper percentile range, leading the health and life sciences industry. As Star Healthcare improves its Insider Snooping readiness, the slider on the graph below would move to the right, corresponding to an increase in both its percentage of relevant security capabilities implemented and its readiness percentile.



The capabilities below are relevant to mitigating risk of Insider Snooping breaches. This table shows the capabilities Star Healthcare has and where there are gaps. Alerts are shown where Star Healthcare lags the industry average - i.e., where Star Healthcare has gaps in capabilities that most other organizations already have implemented.

Star Healthcare Insider Snooping Security Maturity

Baseline	Enhanced	Advanced
⊕ Policy	⊖ ⚠ Device Control	⊖ Network Data Loss Prevention (Prevention Mode)
⊕ Risk Assessment	⊖ ⚠ ! Penetration Testing, Vulnerability Scanning	~ Database Activity Monitoring
⊕ Audit and Compliance	⊕ Client Solid State Drive (Encrypted)	~ Digital Forensics
~ ! User Awareness Training	⊕ Endpoint Data Loss Prevention (Prevention Mode)	⊖ ⚠ ! Security Information and Event Management
~ ! Endpoint Device Encryption	⊖ ⚠ Network Data Loss Prevention (Discovery Mode)	~ Threat Intelligence
~ ! Mobile Device Management	⊖ ⚠ ! Multi-Factor Authentication with Timeout	⊖ ! Multi-Factor Authentication with Walk-Away Lock
⊕ Endpoint Data Loss Prevention (Discovery Mode)	⊖ ⚠ ! Secure Remote Administration	~ Client Application Whitelisting
⊕ Identity and Access Management, Single-Factor Access Control	~ Policy-Based Encryption for Files and Folders	~ Server Application Whitelisting
⊕ Firewall	⊕ Server / Database / Backup Encryption	~ De-Identification / Anonymization
~ ⚠ ! Web Gateway	⊕ Network Segmentation	
~ Vulnerability Management, Patching		
⊕ Security Incident Response Plan		
⊕ Secure Disposal		

(⊕ = present, ~ = partially present, ⊖ = not present, ⚠ = lagging industry in implementing, ! = action item in plan)

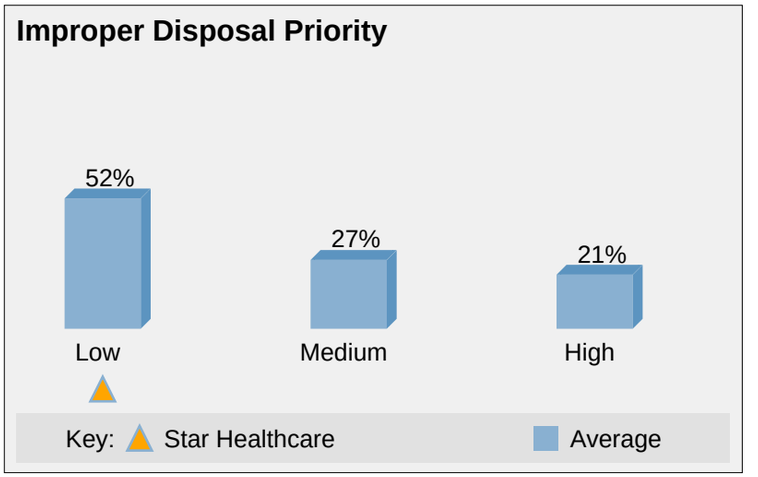
2.7 Improper Disposal

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.

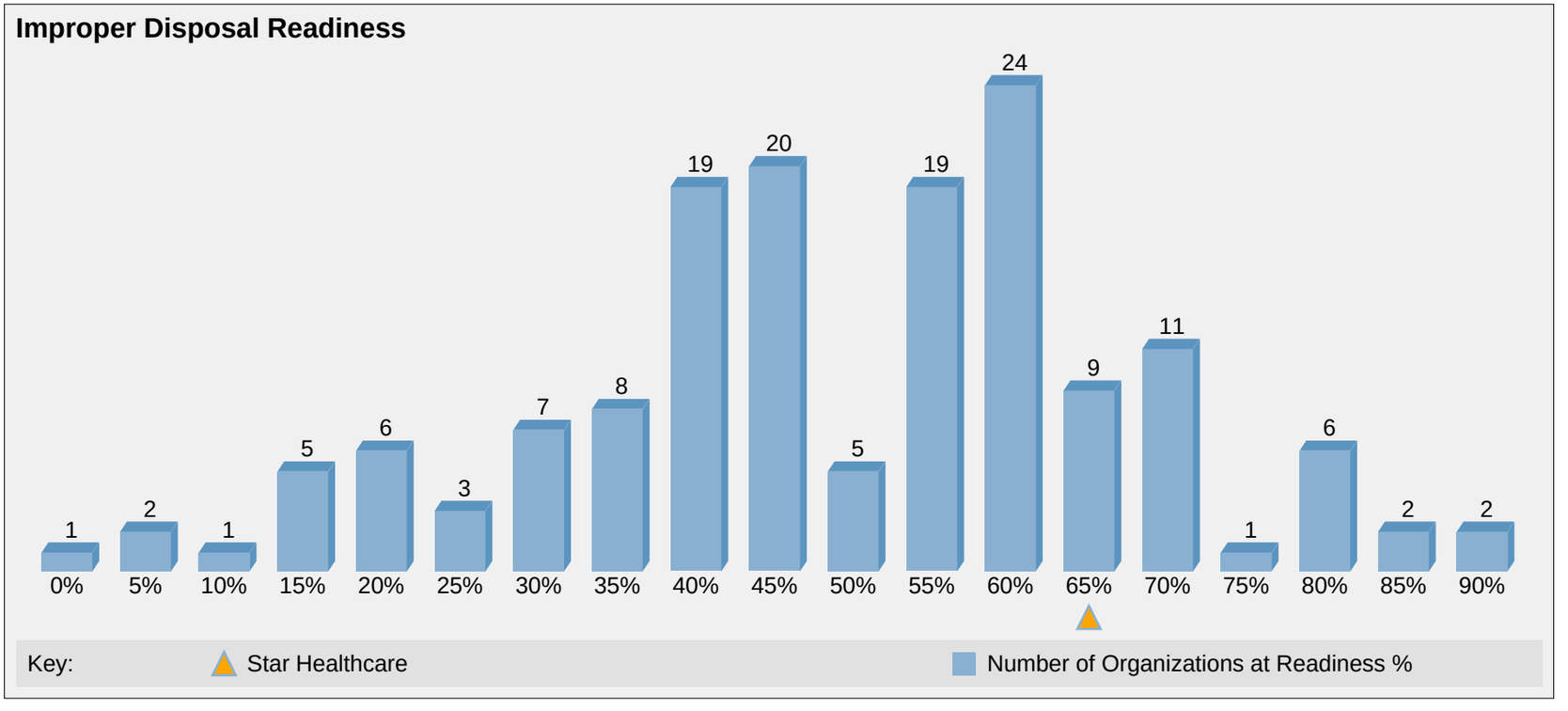
Workshop Overview More Info

Star Healthcare assigned a Low priority to Improper Disposal.

⚠ This generated an alert because, on average, the health and life sciences industry prioritizes this type of breach higher.



Star Healthcare currently has approximately **67%** of the security capabilities relevant to Improper Disposal. Based on this metric, when compared to other health and life sciences organizations, Star Healthcare is at the **85%** readiness percentile, putting it in the upper percentile range, leading the health and life sciences industry. As Star Healthcare improves its Improper Disposal readiness, the slider on the graph below would move to the right, corresponding to an increase in both its percentage of relevant security capabilities implemented and its readiness percentile.



The capabilities below are relevant to mitigating risk of Improper Disposal breaches. This table shows the capabilities Star Healthcare has and where there are gaps. Alerts are shown where Star Healthcare lags the industry average - i.e., where Star Healthcare has gaps in capabilities that most other organizations already have implemented.

Star Healthcare Improper Disposal Security Maturity

Baseline	Enhanced	Advanced
⊕ Policy	⊕ Client Solid State Drive (Encrypted)	⊖ Server Solid State Drive (Encrypted)
⊕ Risk Assessment	~ Anti-Theft: Remote Locate, Lock, Wipe	~ Digital Forensics
⊕ Audit and Compliance	~ Policy-Based Encryption for Files and Folders	~ De-Identification / Anonymization
~ ! User Awareness Training	⊕ Server / Database / Backup Encryption	⊖ Tokenization
~ ! Endpoint Device Encryption		
~ ! Mobile Device Management		
⊕ Endpoint Data Loss Prevention (Discovery Mode)		
~ Vulnerability Management, Patching		
⊕ Security Incident Response Plan		
⊕ Secure Disposal		

(⊕ = present, ~ = partially present, ⊖ = not present, ⚠ = lagging industry in implementing, ! = action item in plan)

2.8 Ransomware

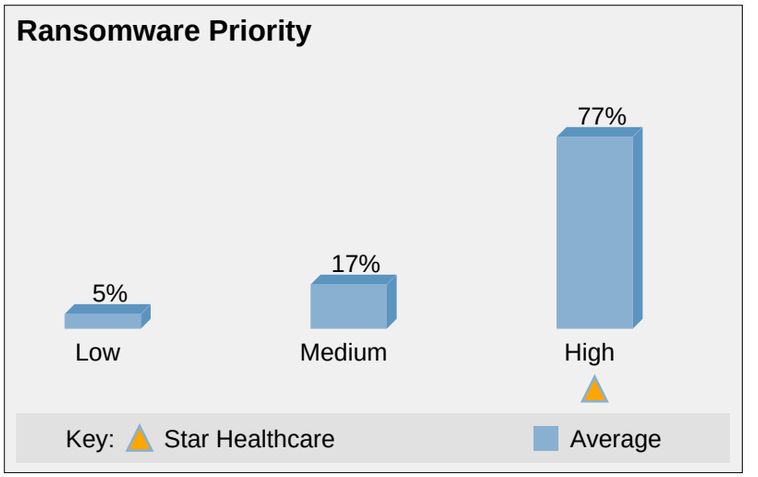
Ransomware breaches involve malware infections, often through phishing and drive-by download, where the malware encrypts sensitive information in electronic form and the hackers behind it withold the decryption keys, typically demanding a ransom. This type of breach compromises the availability of the 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.

Workshop Overview More Info

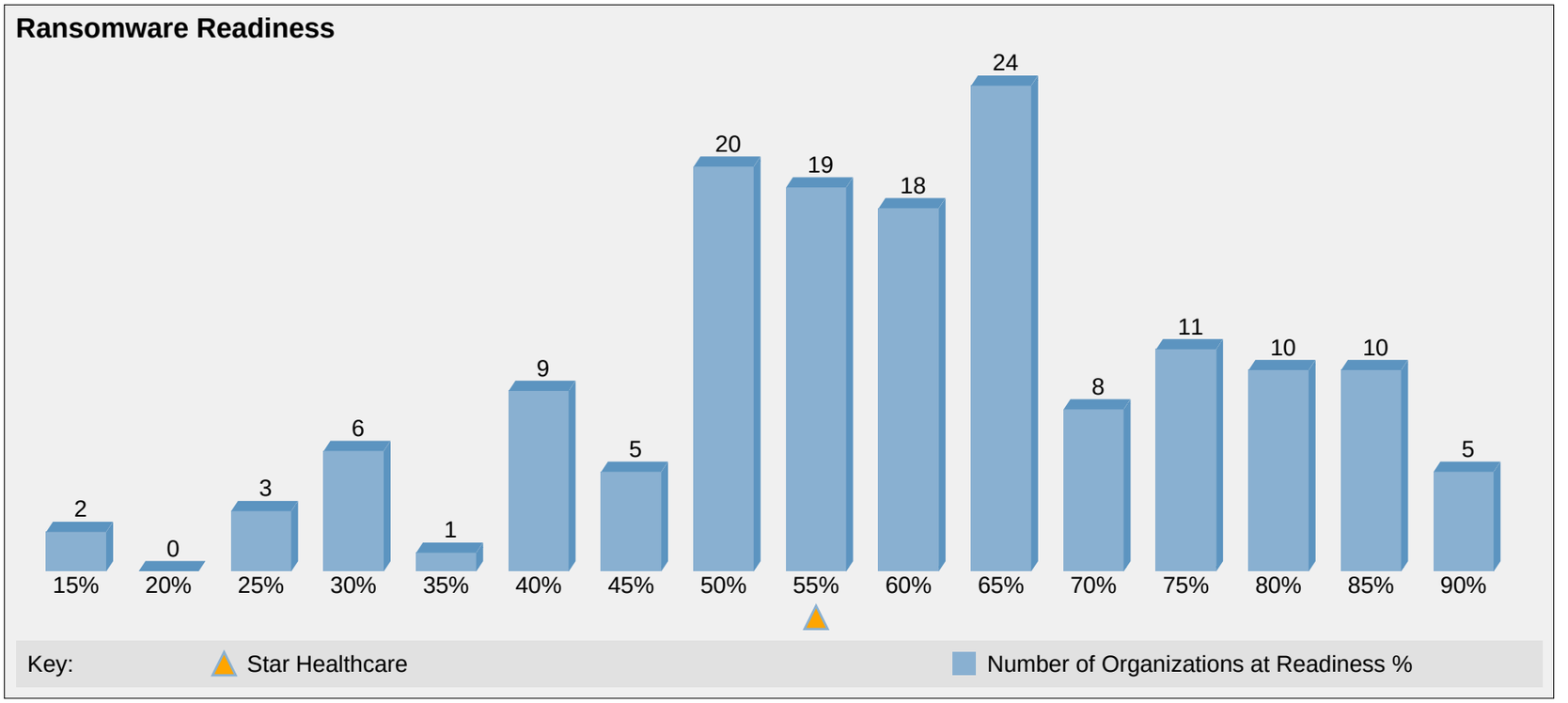
Star Healthcare assigned a High priority to Ransomware.

This is comparable to the average priority assigned by the rest of the health and life sciences industry to this type of breach.

Notes: We recently had a ransomware infection.



Star Healthcare currently has approximately **57%** of the security capabilities relevant to Ransomware. Based on this metric, when compared to other health and life sciences organizations, Star Healthcare is at the **42%** readiness percentile. As Star Healthcare improves its Ransomware readiness, the slider on the graph below would move to the right, corresponding to an increase in both its percentage of relevant security capabilities implemented and its readiness percentile.



The capabilities below are relevant to mitigating risk of Ransomware breaches. This table shows the capabilities Star Healthcare has and where there are gaps. Alerts are shown where Star Healthcare lags the industry average - i.e., where Star Healthcare has gaps in capabilities that most other organizations already have implemented.

Star Healthcare Ransomware Security Maturity

Baseline

- ⊕ Policy
- ⊕ Risk Assessment
- ⊕ Audit and Compliance
- ~ ! User Awareness Training
- ~ ⚠ ! Anti-Malware
- ⊕ Identity and Access Management, Single-Factor Access Control
- ~ ⚠ ! Email Gateway
- ~ ⚠ ! Web Gateway
- ~ Vulnerability Management, Patching
- ⊕ Security Incident Response Plan
- ~ ⚠ ! Backup and Restore

Enhanced

- ⊖ ⚠ Device Control
- ⊖ ⚠ ! Penetration Testing, Vulnerability Scanning
- ⊕ Endpoint Data Loss Prevention (Prevention Mode)
- ⊕ Network Segmentation
- ~ Network Intrusion Prevention System

Advanced

- ⊖ Network Data Loss Prevention (Prevention Mode)
- ~ Digital Forensics
- ⊖ ⚠ ! Security Information and Event Management
- ~ Threat Intelligence
- ~ Client Application Whitelisting
- ~ Server Application Whitelisting
- ~ Business Continuity and Disaster Recovery

(⊕ = present, ~ = partially present, ⊖ = not present, ⚠ = lagging industry in implementing, ! = action item in plan)

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 breach security maturity levels. To the left of each breach security capability is an icon indicating whether this capability is currently present (⊕), partially present (~), or absent (⊖) at Star Healthcare. (⚠) indicates a capability which Star Healthcare is significantly behind the health and life sciences industry average in implementing.

Star Healthcare Security Maturity

Baseline

- ⊕ Policy
- ⊕ Risk Assessment
- ⊕ Audit and Compliance
- ~ ! User Awareness Training
- ~ ! Endpoint Device Encryption
- ~ ! Mobile Device Management
- ⊕ Endpoint Data Loss Prevention (Discovery Mode)
- ~ ⚠ ! Anti-Malware
- ⊕ Identity and Access Management, Single-Factor Access Control
- ⊕ Firewall
- ~ ⚠ ! Email Gateway
- ~ ⚠ ! Web Gateway
- ~ Vulnerability Management, Patching
- ⊕ Security Incident Response Plan
- ⊕ Secure Disposal
- ~ ⚠ ! Backup and Restore

Enhanced

- ⊖ ⚠ Device Control
- ⊖ ⚠ ! Penetration Testing, Vulnerability Scanning
- ⊕ Client Solid State Drive (Encrypted)
- ⊕ Endpoint Data Loss Prevention (Prevention Mode)
- ⊖ ⚠ Network Data Loss Prevention (Discovery Mode)
- ~ Anti-Theft: Remote Locate, Lock, Wipe
- ⊖ ⚠ ! Multi-Factor Authentication with Timeout
- ⊖ ⚠ ! Secure Remote Administration
- ~ Policy-Based Encryption for Files and Folders
- ⊕ Server / Database / Backup Encryption
- ⊕ Network Segmentation
- ~ Network Intrusion Prevention System
- ~ ⚠ Business Associate Agreements
- ~ Virtualization

Advanced

- ⊖ Server Solid State Drive (Encrypted)
- ⊖ Network Data Loss Prevention (Prevention Mode)
- ~ Database Activity Monitoring
- ~ Digital Forensics
- ⊖ ⚠ ! Security Information and Event Management
- ~ Threat Intelligence
- ⊖ ! Multi-Factor Authentication with Walk-Away Lock
- ~ Client Application Whitelisting
- ~ Server Application Whitelisting
- ~ De-Identification / Anonymization
- ⊖ Tokenization
- ~ Business Continuity and Disaster Recovery

(⊕ = present, ~ = partially present, ⊖ = not present, ⚠ = lagging industry in implementing, ! = action item in plan)

4. Gaps and Opportunities for Improvement

Security capabilities for which your implementation was assessed as either "No" (⛔) or "Partial" (🗲) are listed below, together with whether your gap is significantly behind (⚠) the rest of the health and life sciences organizations assessed. Capability gaps below are listed in order from the first which if implemented has the most positive impact on your security readiness percentile scores across all breach types. Each subsequent capability in the list is the most beneficial capability to implemement at that step in terms of improving your security readiness percentile scores across all breach types. For each capability gap, the percentile improvement and final percentile score are listed under each associated breach type. These results are based on current security readiness assessment data across the current benchmark data set. Organizations security capabilities, and therefore security readiness assessment results change over time, and therefore so will these results. This list is not intended to be prescriptive. Please consult your account manager and assessor for further guidance in interpreting these results and recommendations on what actions to take.

Star Healthcare Security Gaps

#	Security Capability	Assess	Breach Types Mitigated and Star Healthcare Priorities								Behind Industry
			Cybercrime Hacking	Loss or Theft	Insider Accidents	Business Associates	Malicious Insiders or Fraud	Insider Snooping	Improper Disposal	Ransomware	
			High	Medium	Medium	Medium	High	Medium	Low	High	
	Current Security Readiness Percentiles		28%	69%	60%	70%	59%	68%	85%	42%	
1	Secure Remote Administration	⛔ !	+8% 36%	+10% 79%	+8% 68%		+5% 64%	+5% 73%			⚠
2	Digital Forensics	🗲	+6% 42%	+1% 80%	+6% 74%	+7% 77%	+6% 70%	+2% 75%	+4% 89%	+7% 49%	
3	Penetration Testing, Vulnerability Scanning	⛔ !	+9% 51%				+4% 74%	+6% 81%		+13% 62%	⚠
4	User Awareness Training	🗲 !	+5% 56%	+3% 83%	+4% 78%	+7% 84%	+2% 76%		+3% 92%	+3% 65%	
5	Security Information and Event Management	⛔ !	+8% 64%				+3% 79%	+6% 87%		+8% 73%	⚠
6	Tokenization	⛔	+8% 72%	+7% 90%	+5% 83%				+3% 95%		
7	De-Identification / Anonymization	🗲	+3% 75%	+2% 92%	+3% 86%	+7% 91%	+1% 80%		+2% 97%		
8	Device Control	⛔			+5% 91%		+5% 85%	+4% 91%		+6% 79%	⚠
9	Threat Intelligence	🗲	+4% 79%			+7% 98%	+1% 86%	+2% 93%		+4% 83%	
10	Network Data Loss Prevention (Discovery Mode)	⛔	+3% 82%		+3% 94%		+4% 90%	+1% 94%			⚠
11	Network Data Loss Prevention (Prevention Mode)	⛔	+6% 88%		+3% 97%		+3% 93%	+3% 97%		+6% 89%	

Star Healthcare Security Gaps

#	Security Capability	Assess	Breach Types Mitigated and Star Healthcare Priorities								Behind Industry
			Cybercrime Hacking	Loss or Theft	Insider Accidents	Business Associates	Malicious Insiders or Fraud	Insider Snooping	Improper Disposal	Ransomware	
			High	Medium	Medium	Medium	High	Medium	Low	High	
12	Vulnerability Management, Patching	~	+2% 90%	+2% 94%	+2% 99%		+1% 94%			+2% 91%	
13	Multi-Factor Authentication with Timeout	⛔ !	+3% 93%	+2% 96%			+1% 95%	+2% 99%			⚠
14	Backup and Restore	~ !	+2% 95%	+1% 97%			+1% 96%			+3% 94%	⚠
15	Multi-Factor Authentication with Walk-Away Lock	⛔ !	+3% 98%	+2% 99%			+1% 97%				
16	Web Gateway	~ !					+1% 98%			+2% 96%	⚠
17	Email Gateway	~ !	+1% 99%							+2% 98%	⚠
18	Server Solid State Drive (Encrypted)	⛔					+1% 99%		+2% 99%		
19	Anti-Malware	~ !								+1% 99%	⚠
20	Business Associate Agreements	~				+1% 99%					⚠
21	Client Application Whitelisting	~									
22	Server Application Whitelisting	~									
23	Policy-Based Encryption for Files and Folders	~									
24	Mobile Device Management	~ !									
25	Endpoint Device Encryption	~ !									
26	Business Continuity and Disaster Recovery	~									
27	Database Activity Monitoring	~									
28	Anti-Theft: Remote Locate, Lock, Wipe	~									
29	Network Intrusion Prevention System	~									
30	Virtualization	~									

Star Healthcare Security Gaps

#	Security Capability	Assess	Breach Types Mitigated and Star Healthcare Priorities							Behind Industry
			Cybercrime Hacking	Loss or Theft	Insider Accidents	Business Associates	Malicious Insiders or Fraud	Insider Snooping	Improper Disposal	Ransomware	
			High	Medium	Medium	Medium	High	Medium	Low	High	

(⊕ = present, ~ = partially present, ⊖ = not present, ⚠ = lagging industry in implementing, ! = action item in plan)

5. Action Plan

The following 12-step, multi-year action plan is recommended for Star Healthcare to improve their breach security posture and reduce residual risk of breaches:

2017

1. User Awareness Training : Enhance training to include spear phishing, and add new security training at the time of employee role changes.
2. Secure Remote Administration : Add ability to efficiently administer remote endpoints for maintenance, patching, updates, and support.
3. Backup and Restore : Add backup and restore (versioned) for all data for availability and protection against ransomware.
4. Endpoint Device Encryption : Add encryption to smartphones and tablets.

2018

5. Security Information and Event Management : Implement SIEM for improved detection of breaches to minimize business impact.
6. Penetration Testing, Vulnerability Scanning : Conduct penetration testing on external interfaces. Complete vulnerability scan to find unsecured machines, including unsecured development and test databases with PHI.
7. Multi-Factor Authentication with Timeout : Add tap-and-go MFA with proximity cards to improve usability and security.
8. Mobile Device Management : Add MDM for corporate-provisioned mobile endpoints.

2019

9. Multi-Factor Authentication with Walk-Away Lock : Upgrade tap-and-go MFA to also include walk-away lock to minimize risk of session hijacking when clinicians leave.
10. Email Gateway : Add monitoring of alerts, and management for Email Gateway.
11. Web Gateway : Add monitoring of alerts, and management for Web Gateway.
12. Anti-Malware : Add anti-malware to smartphones and tablets.

6. Capabilities

This assessment evaluated the presence of 42 security capabilities in Star Healthcare. This section defines each capability and shows how Star Healthcare compares with the health and life sciences industry in implementing each capability.

6.1 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

Notes: Need to update for BYOD.

HIPAA: 45 CFR 164.308(a)

ISO: 27001:2013 Section 5.2 Policy

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

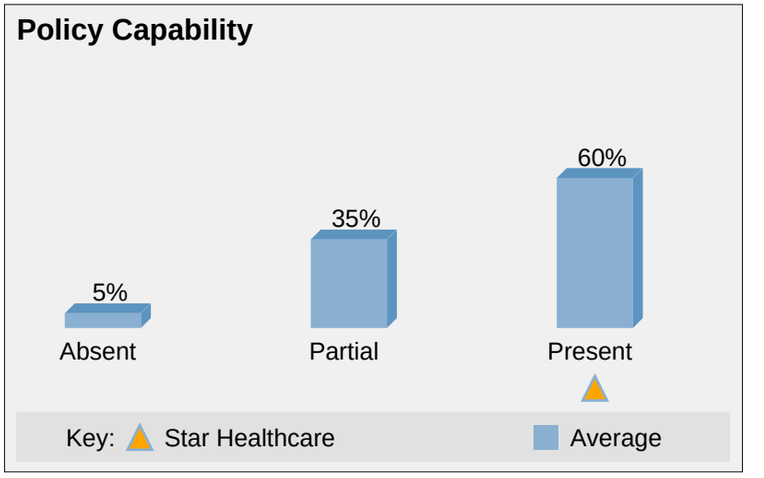
PCI DSS: v3.1 Section 12.1

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)



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

6.2 Risk Assessment

Documented risk assessments done annually.

Workshop Overview More Info

Notes: Last one completed about 2 years ago. Not currently done regularly.

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

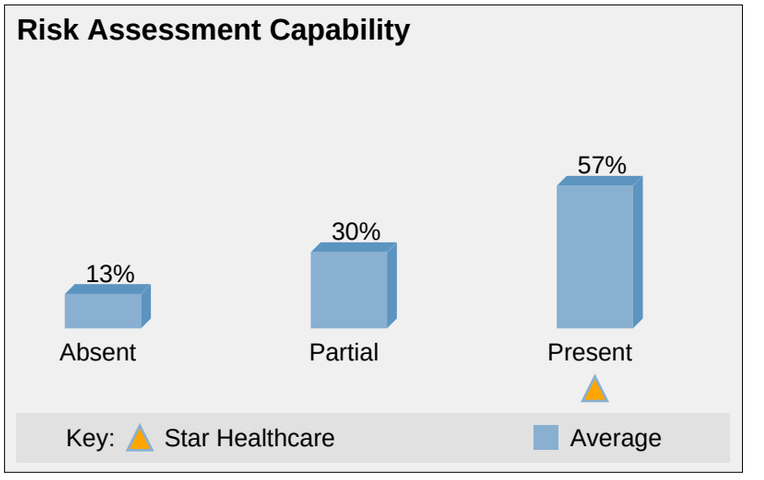
PCI DSS: v3.1 Section 12.2

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)



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

6.3 Audit and Compliance

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

Workshop Overview More Info

Notes: Logging and regular audits done to verify compliance with policy.

HIPAA: 45 CFR 164.312(b)

ISO: 27001:2013 Section 9.2 Internal Audit

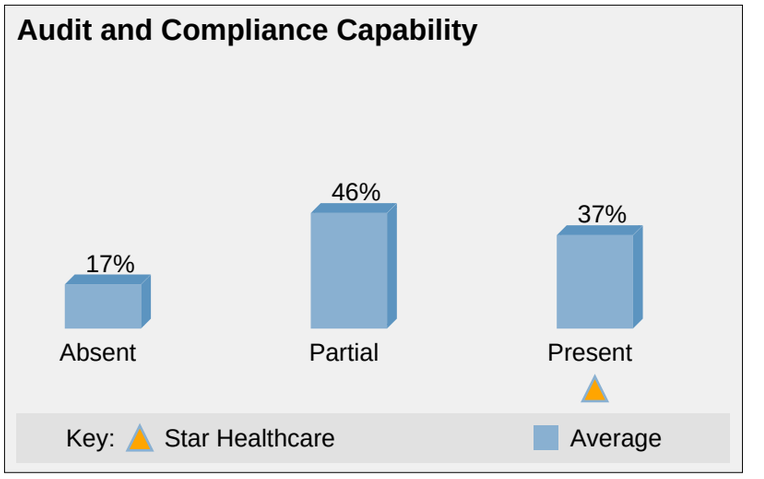
NIST: SP 800-53 Rev. 4 AU-1 to 16

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



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

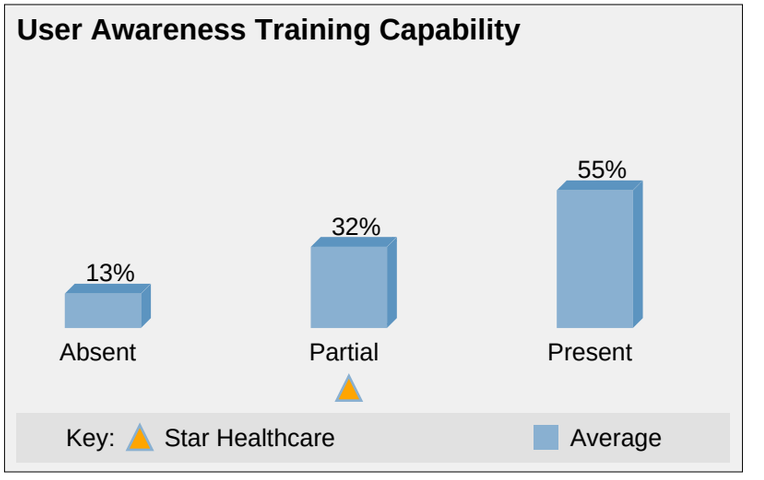
6.4 User Awareness Training

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

Notes: New employees trained. Need training on role change and spear phishing.

! Recommended Action: 2017 - Enhance training to include spear phishing, and add new security training at the time of employee role changes. See Action Plan.



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))

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

6.5 Endpoint Device Encryption

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

Workshop Overview More Info

Notes: Laptops encrypted. Need encryption for smartphones and tablets.

! Recommended Action: 2017 - Add encryption to smartphones and tablets. See Action Plan.

HIPAA: 45 CFR 164.312

ISO: 27002:2013 Section 10 Cryptography

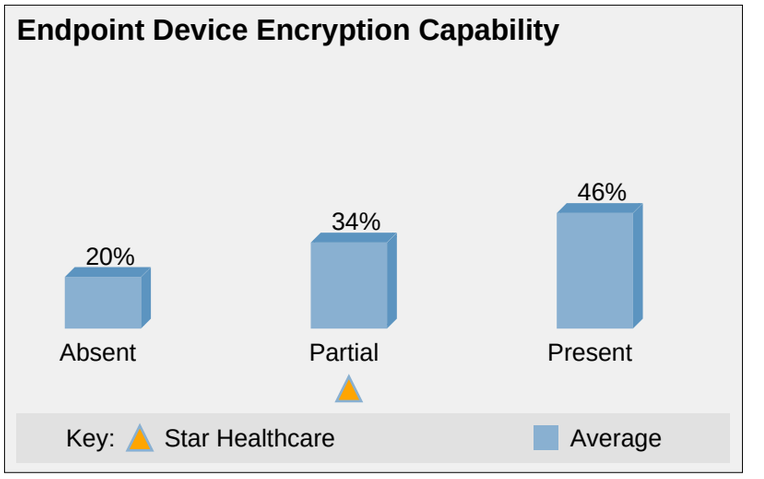
NIST: SP 800-53 Rev. 4 SC-28

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)



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

6.6 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

Notes: Currently in place for BYOD smartphones. Need for corporate smartphones and tablets.

! Recommended Action: 2018 - Add MDM for corporate-provisioned mobile endpoints. See Action Plan.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: 27002:2013 Section 6.2 Mobile Devices and Teleworking

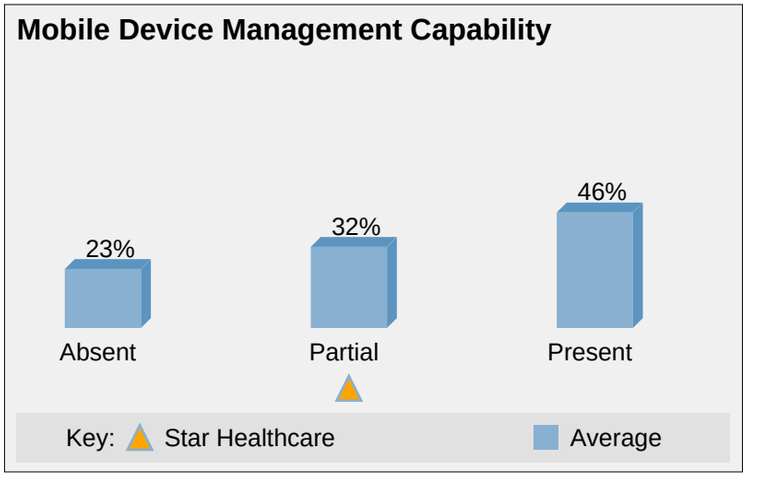
NIST: SP 800-53 Rev. 4 AC-19

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)



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

6.7 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

Notes: Currently used to discover patient data stored on laptops etc.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

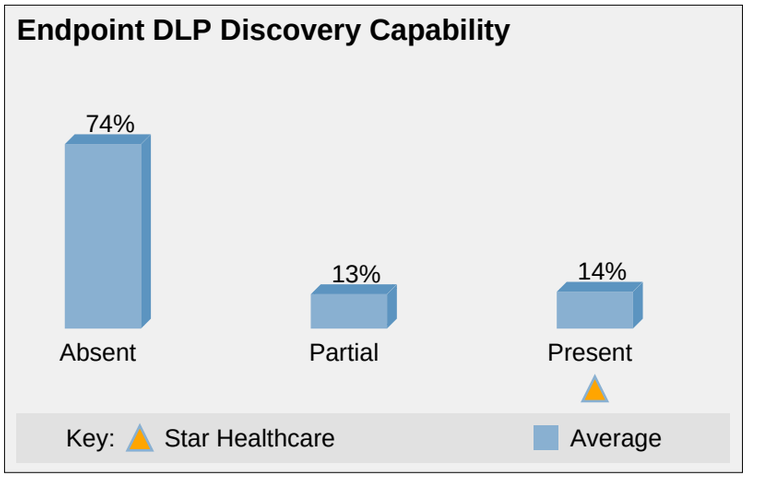
ISO: 27002:2013 Section 18.1.3 Protection of Records

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



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

6.8 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

Notes: Currently running on laptops. Need for smartphones and tablets as well.

! Recommended Action: 2019 - Add anti-malware to smartphones and tablets. See Action Plan.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: 27002:2013 Section 12.2 Protection from Malware

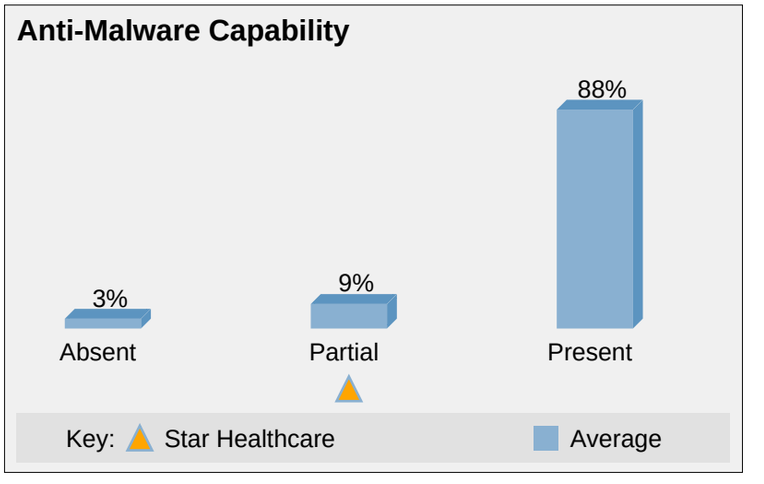
NIST: SP 800-53 Rev. 4 SI-3

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)

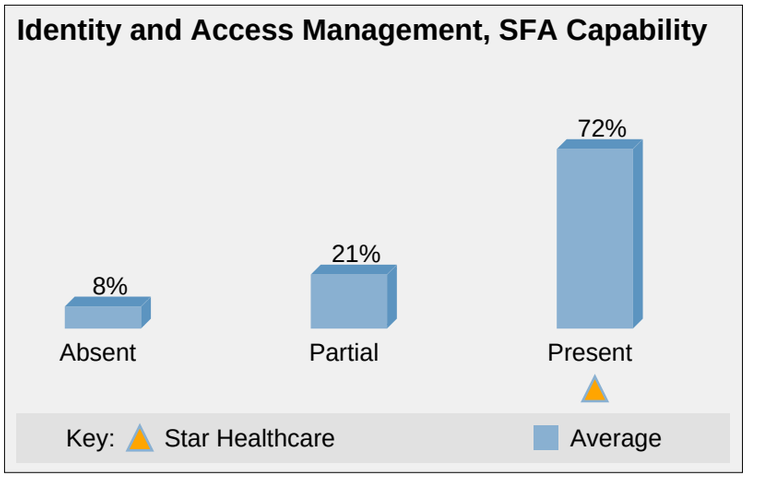


⚠ Star Healthcare is lagging the health and life sciences industry in implementing the Anti-Malware capability.

Anti-Malware is relevant to the following breach types:
- Cybercrime Hacking - Insider Accidents or Workarounds - Ransomware

6.9 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

Notes: Microsoft Windows login, as well as logins across various applications.

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

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

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

6.10 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

Notes: Currently have firewalls in place on perimeter of network, as well as endpoints.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: 27002:2013 Section 13.1.2 Security of Network Services

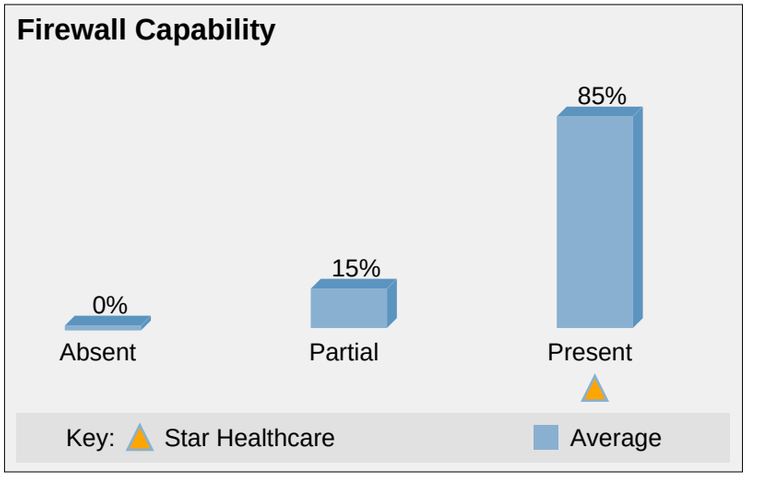
NIST: SP 800-53 Rev. 4 SC-7

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)



Firewall is relevant to the following breach types:

- Cybercrime Hacking
- Malicious Insiders or Fraud
- Insider Snooping

6.11 Email Gateway

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

Workshop Overview More Info

Notes: We have the appliance in place but need to establish process to configure and monitor it.

! Recommended Action: 2019 - Add monitoring of alerts, and management for Email Gateway. See Action Plan.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

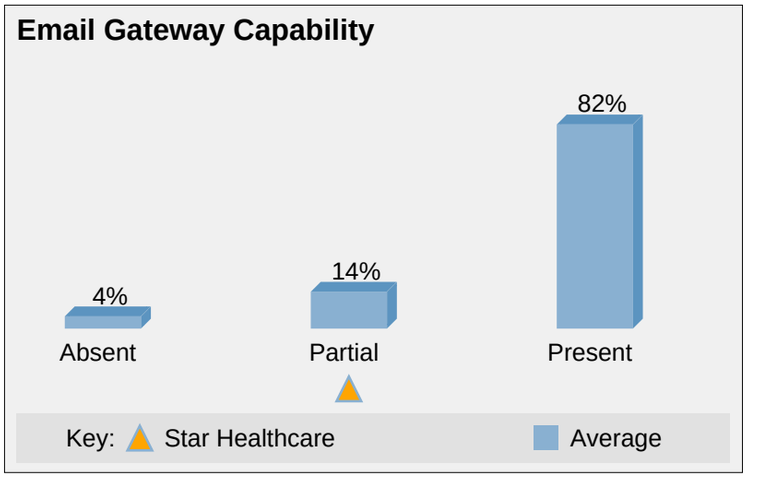
ISO: 27002:2013 Section 13.1 Network Security Management

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



⚠ Star Healthcare is lagging the health and life sciences industry in implementing the Email Gateway capability.

Email Gateway is relevant to the following breach types:

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

6.12 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

Notes: Appliance in place but need resources and process to monitor it to get full benefit.

! Recommended Action: 2019 - Add monitoring of alerts, and management for Web Gateway. See Action Plan.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

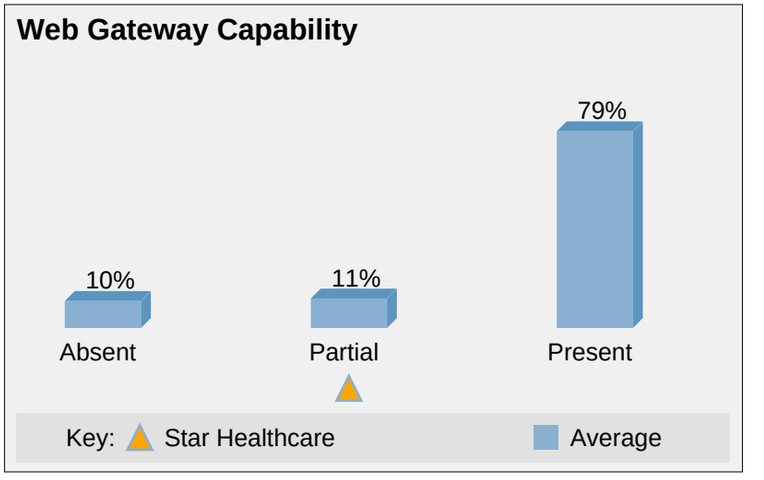
ISO: 27002:2013 Section 13.1 Network Security Management

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



⚠ Star Healthcare is lagging the health and life sciences industry in implementing the Web Gateway capability.

Web Gateway is relevant to the following breach types:

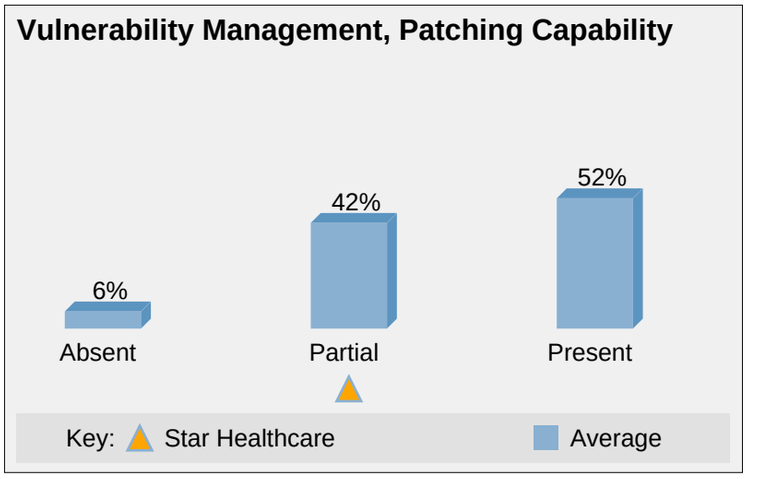
- Cybercrime Hacking
- Insider Accidents or Workarounds
- Malicious Insiders or Fraud
- Insider Snooping
- Ransomware

6.13 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

Notes: Currently PC's configured for automatic updates. Need to do more vulnerability management (e.g. with client configuration).



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)

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

6.14 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

Notes: Currently in place and tested. Good to go.

HIPAA: 45 CFR 164.308(a)(6)

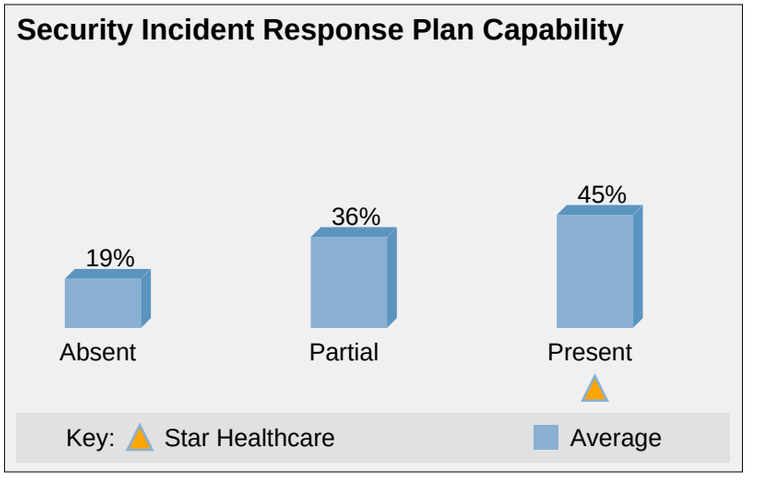
ISO: 27002:2013 Section 16 Information Security Incident Management

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



Security Incident Response Plan 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

6.15 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

Notes: Secure wipe for hard drives. Shredding for paper records.

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

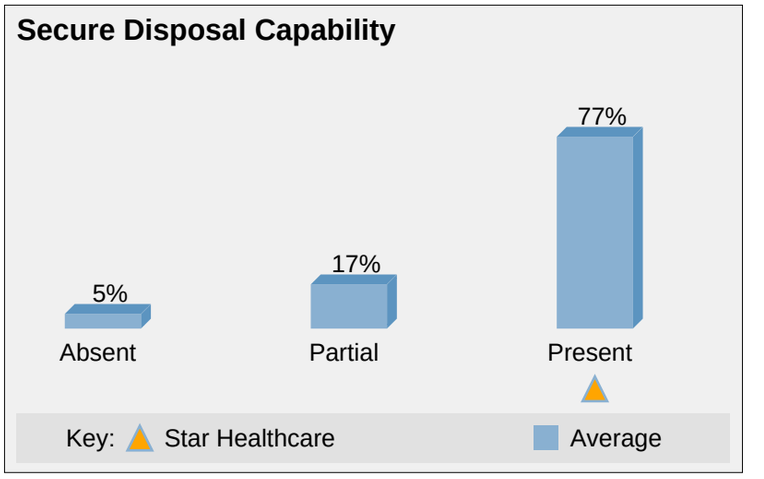
ISO: 27002:2013 Section 8.3.2 Disposal of Media, 11.2.7 Secure Disposal or Re-Use of Equipment

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



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

6.16 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

Notes: Some endpoints including smartphones and tablets not yet backed up.

! Recommended Action: 2017 - Add backup and restore (versioned) for all data for availability and protection against ransomware. See Action Plan.

HIPAA: Security Rule - Protect Availability - Technical Safeguard

ISO: 27002:2013 Section 12.3 Backup

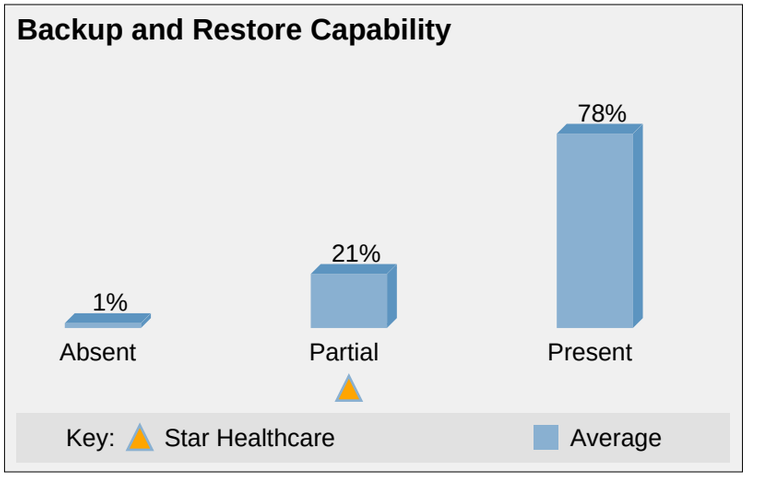
NIST: SP 800-53 Rev. 4 CP-9, 10

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)



⚠ Star Healthcare is lagging the health and life sciences industry in implementing the Backup and Restore capability.

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

6.17 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

Notes: Need to get this to prevent use of USB keys with laptops.

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

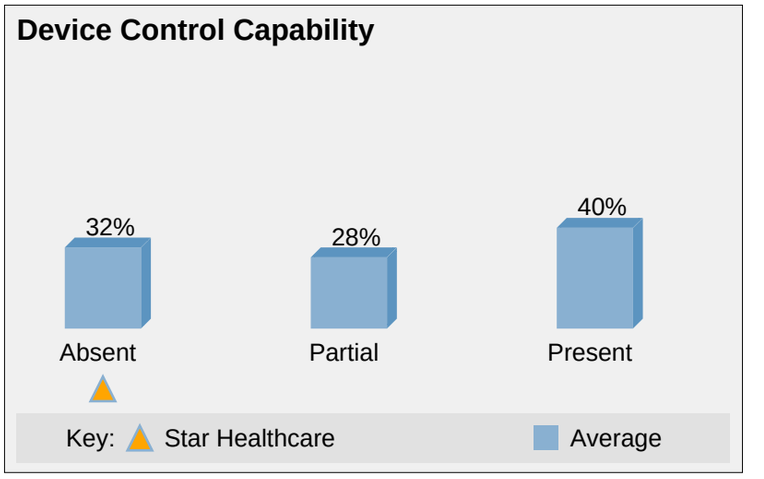
PCI DSS: v3.1 Requirement 5

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)



⚠ Star Healthcare is lagging the health and life sciences industry in implementing the Device Control capability.

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

6.18 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

Notes: Need to conduct this, especially on external network interfaces.

! Recommended Action: 2018 - Conduct penetration testing on external interfaces. Complete vulnerability scan to find unsecured machines, including unsecured development and test databases with PHI. See Action Plan.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

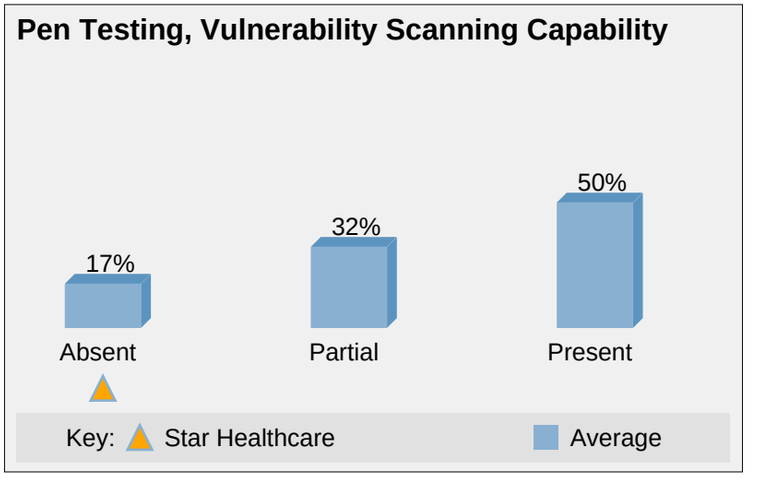
ISO: 27002:2013 Section 18.2.3 Technical Compliance Review

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



⚠ Star Healthcare is lagging the health and life sciences industry in implementing the Penetration Testing, Vulnerability Scanning capability.

Penetration Testing, Vulnerability Scanning is relevant to the following breach types:

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

6.19 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

Notes: Currently used in laptops.

HIPAA: 45 CFR 164.312

ISO: 27002:2013 Section 10 Cryptography

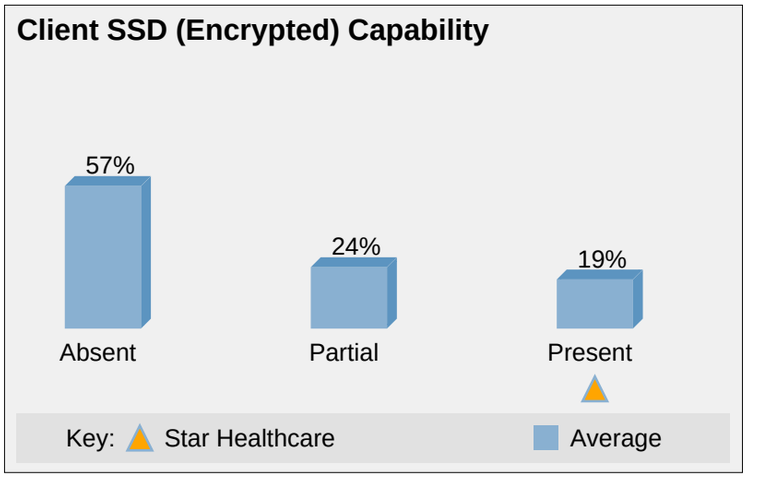
NIST: SP 800-53 Rev. 4 SC-28

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)



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

6.20 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

Notes: Working well as intended.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: 27002:2013 Section 18.1.3 Protection of Records

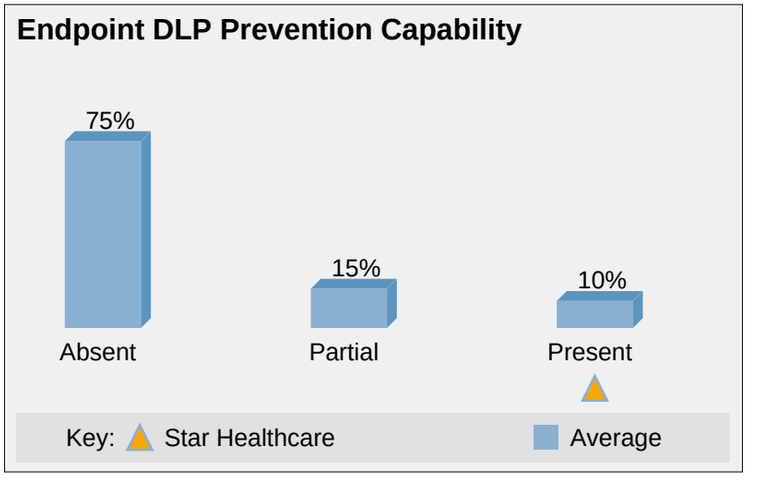
NIST: SP 800-53 Rev. 4 SC-7

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)



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

6.21 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

Notes: We don't currently have a network DLP appliance.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: 27002:2013 Section 13.1 Network Security Management

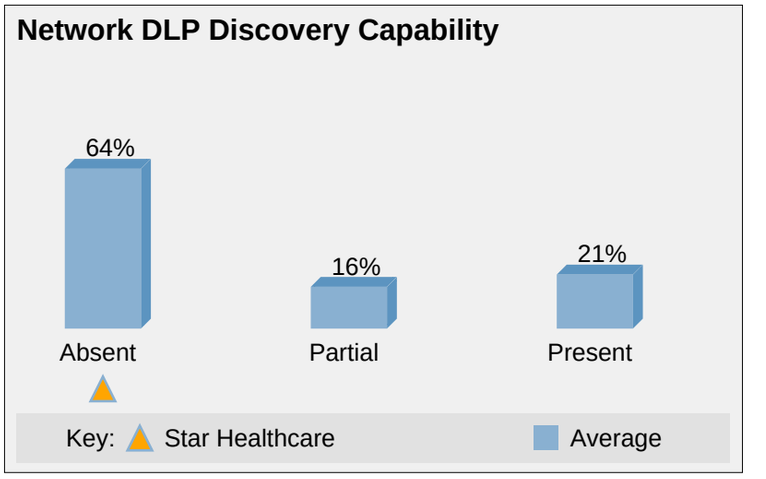
NIST: SP 800-53 Rev. 4 AU-13, 14

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)



⚠ Star Healthcare is lagging the health and life sciences industry in implementing the Network Data Loss Prevention (Discovery Mode) capability.

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

6.22 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

Notes: We have remote locate / lock / wipe only on smartphones and tablets, not on laptops currently.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: 27002:2013 Section 6.2 Mobile Devices and Teleworking

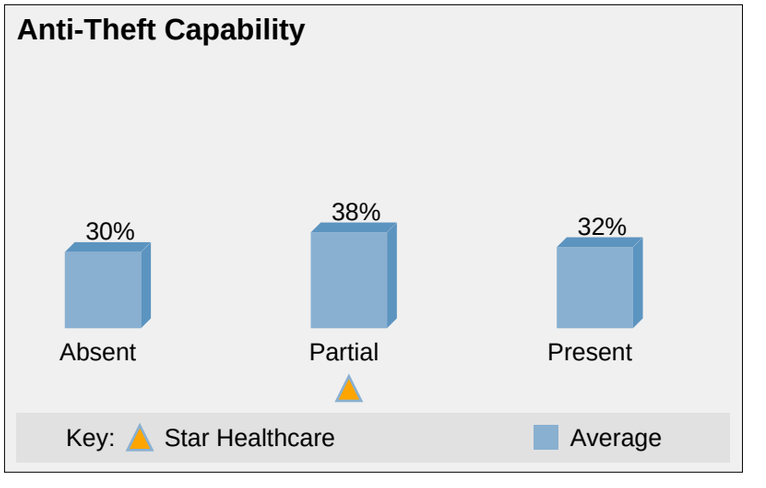
NIST: SP 800-53 Rev. 4 AC-7, AC-19

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)



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

6.23 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.

Workshop Overview More Info

Notes: We don't currently have MFA, but looking at Tap-and-Go proximity cards.

! Recommended Action: 2018 - Add tap-and-go MFA with proximity cards to improve usability and security. See Action Plan.

HIPAA: 45 CFR 164.312

ISO: 27002:2013 Section 9 Access Control

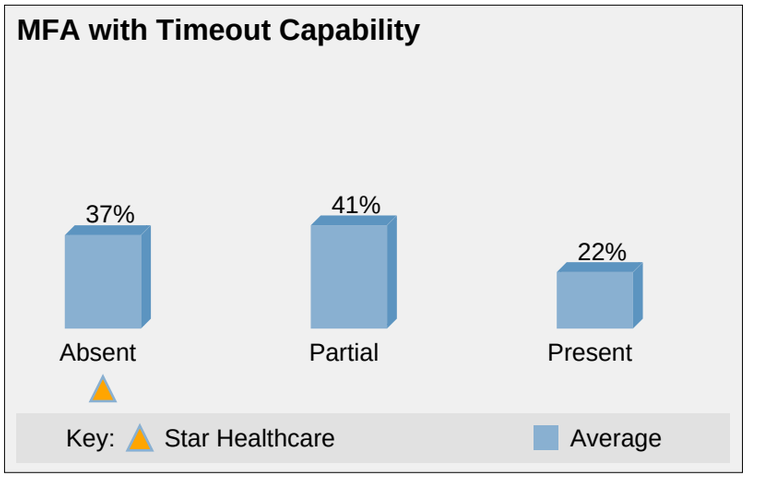
NIST: SP 800-53 Rev. 4 IA-2, AC-2, AC-11, AC-12

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)



⚠ Star Healthcare is lagging the health and life sciences industry in implementing the Multi-Factor Authentication with Timeout capability.

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

6.24 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

Notes: We don't currently have the ability to securely and remotely manage laptops.

! Recommended Action: 2017 - Add ability to efficiently administer remote endpoints for maintenance, patching, updates, and support. See Action Plan.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: 27002:2013 Section 12.6 Technical Vulnerability Management

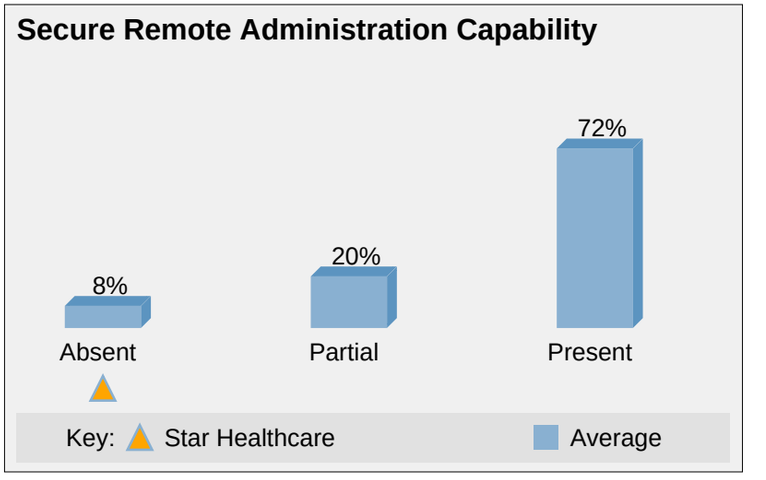
NIST: SP 800-53 Rev. 4 MA-4

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)



⚠ Star Healthcare is lagging the health and life sciences industry in implementing the Secure Remote Administration capability.

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

6.25 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

Notes: X-Ray images are automatically encrypted per policy. Need to get this in place for other types of files.

HIPAA: 45 CFR 164.312

ISO: 27002:2013 Section 10 Cryptography

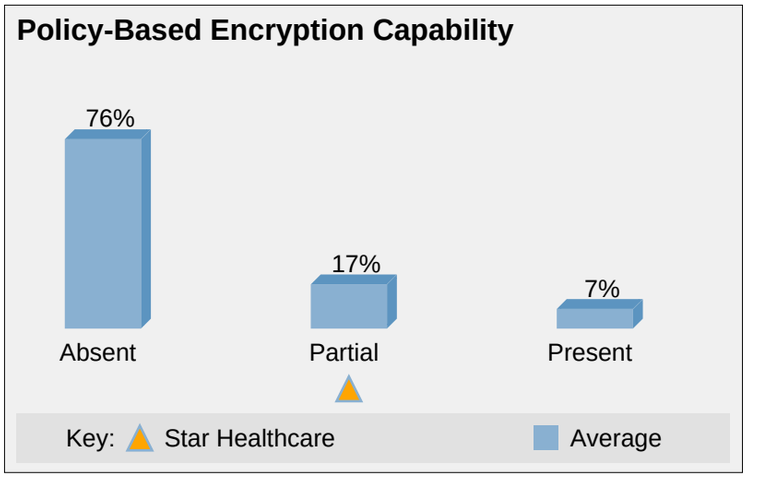
NIST: SP 800-53 Rev. 4 SC-28

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)



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

6.26 Server / Database / Backup Encryption

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

Workshop Overview More Info

Notes: Server filesystem encrypted. Database full-disk encryption in place. Backups encrypted before going onto tape.

HIPAA: 45 CFR 164.312

ISO: 27002:2013 Section 10 Cryptography

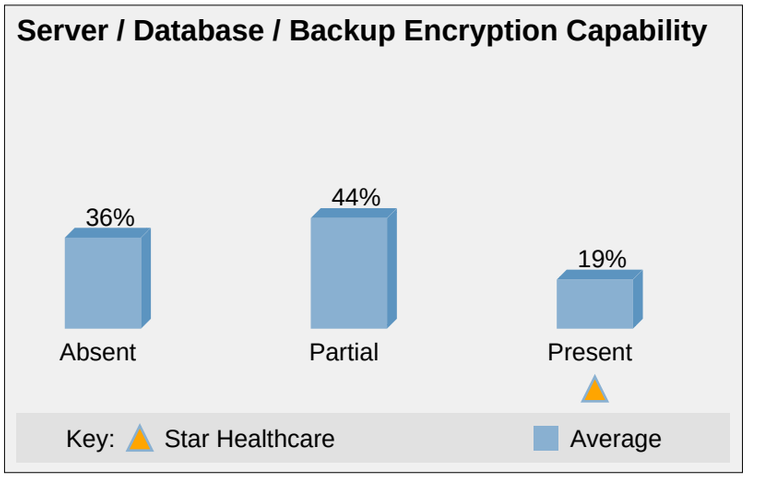
NIST: SP 800-53 Rev. 4 SC-28, CP-9

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)



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

6.27 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

Notes: Currently have network segmented for Intranet, DMZ, Guest, and Medical Devices.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: 27002:2013 Section 13.1.3 Segregation in Networks

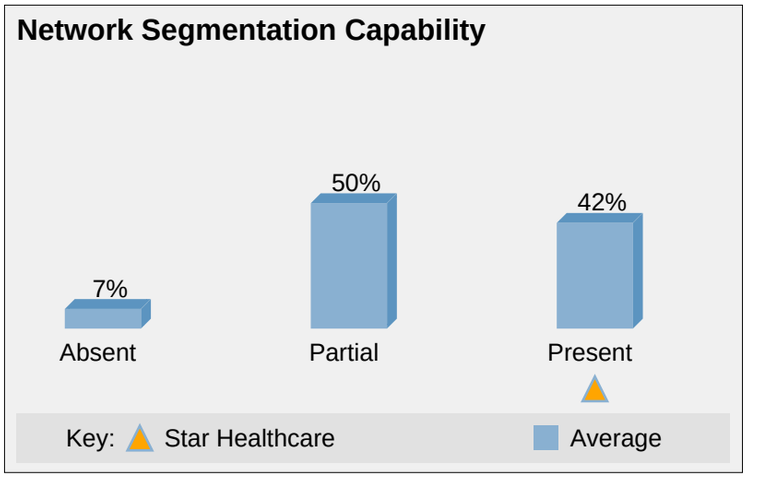
NIST: SP 800-53 Rev. 4 SC-7, SC-32

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)



Network Segmentation is relevant to the following breach types:

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

6.28 Network Intrusion Prevention System

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

Workshop Overview More Info

Notes: Needs better monitoring.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: 27002:2013 Section 13.1 Network Security Management

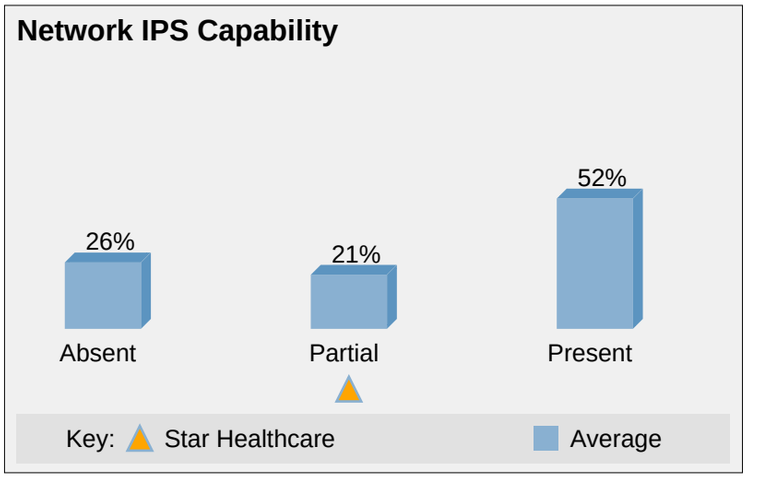
NIST: SP 800-53 Rev. 4 SI-4, SC-7

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)



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

- Cybercrime Hacking
- Ransomware

6.29 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

Notes: Most of our contractors have signed a BAA. Working on getting others.

HIPAA: 45 CFR 164.308(b)(1)

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

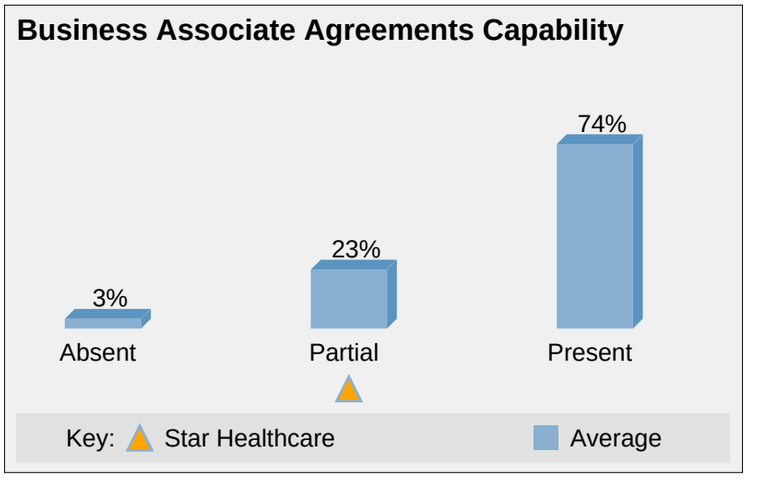
NIST: SP 800-53 Rev. 4 SA-9

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)



⚠ Star Healthcare is lagging the health and life sciences industry in implementing the Business Associate Agreements capability.

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

6.30 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

Notes: We have some VDI from zero client terminals, but we still have a significant portion of our endpoint PC's without VDI.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: 27002:2013 Section 11.2.1 Equipment Siting and Protection

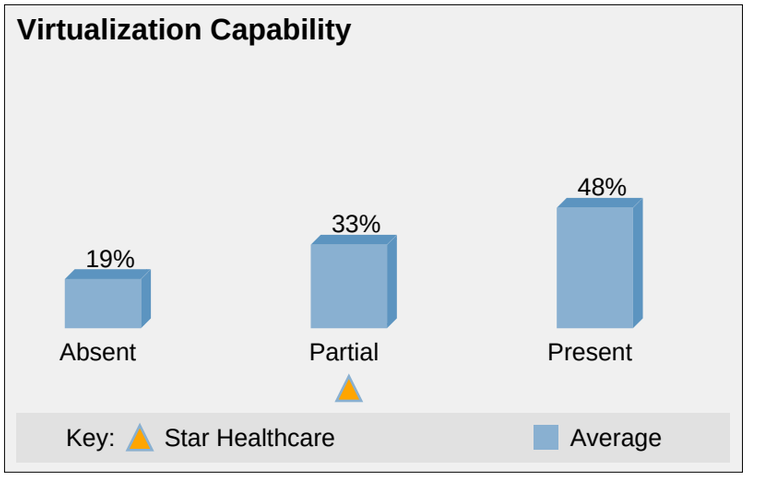
NIST: SP 800-53 Rev. 4 SC-2, SC-7, SI-14

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)



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

6.31 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

Notes: We don't use any SSD's on the server at present.

HIPAA: 45 CFR 164.312

ISO: 27002:2013 Section 10 Cryptography

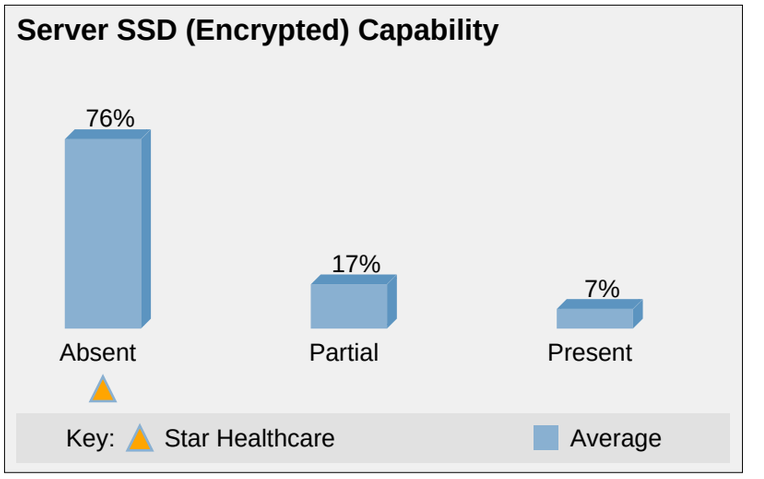
NIST: SP 800-53 Rev. 4 SC-28

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)



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

6.32 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

Notes: We don't currently have network DLP.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

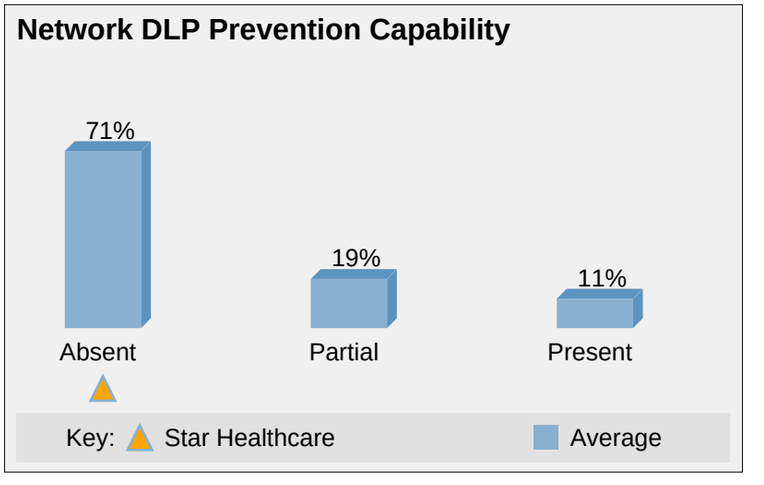
ISO: 27002:2013 Section 13.1 Network Security Management

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



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

6.33 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

Notes: We currently only have this on some of our databases containing patient information.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: 27002:2013 Section 12.4 Logging and Monitoring

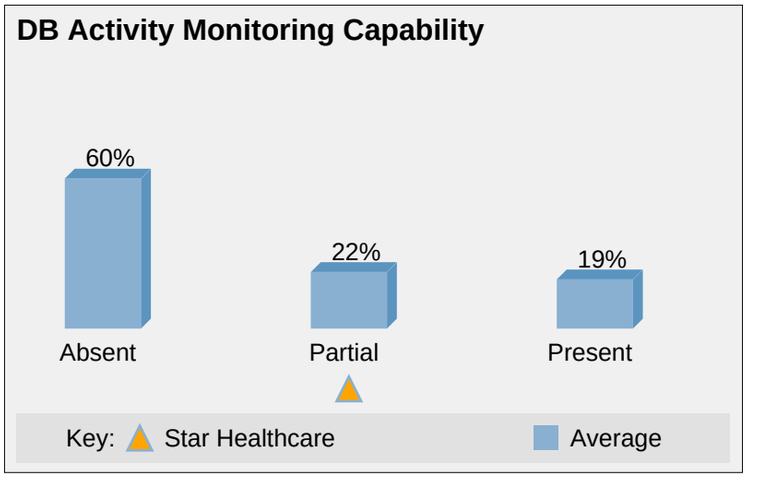
NIST: SP 800-53 Rev. 4 AC-23

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)



Database Activity Monitoring is relevant to the following breach types:

- Cybercrime Hacking
- Malicious Insiders or Fraud
- Insider Snooping

6.34 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

Notes: We contract an external organization for parts of this.

HIPAA: Incident Management - Forensics

ISO: 27002:2013 Section 16.1.7 Collection of Evidence

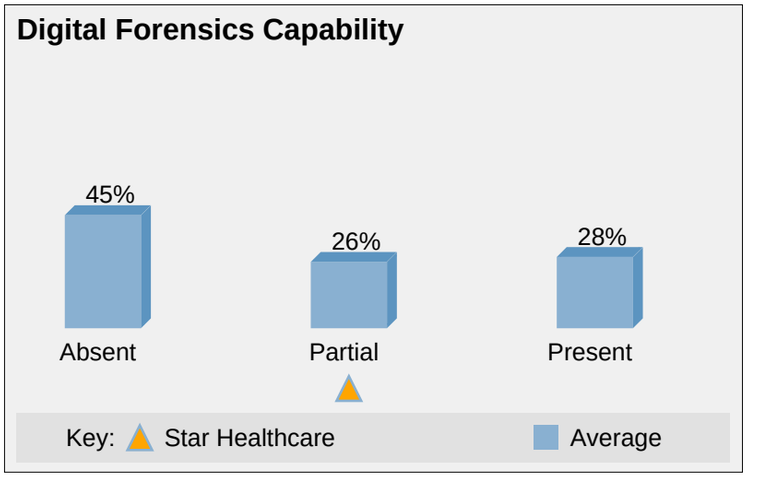
NIST: SP 800-53 Rev. 4 IR-7, 10

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)



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

6.35 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

Notes: We really need this to improve our detection capabilities.

! Recommended Action: 2018 - Implement SIEM for improved detection of breaches to minimize business impact. See Action Plan.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: 27002:2013 Section 12.4 Logging and Monitoring

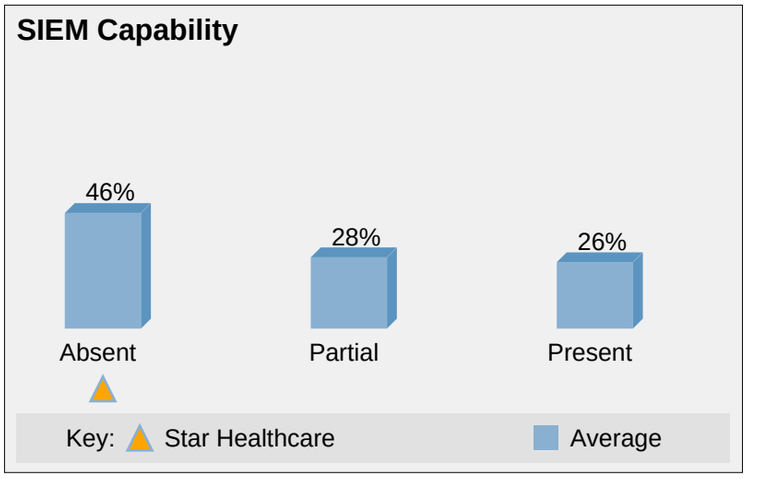
NIST: SP 800-53 Rev. 4 SI-4

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)

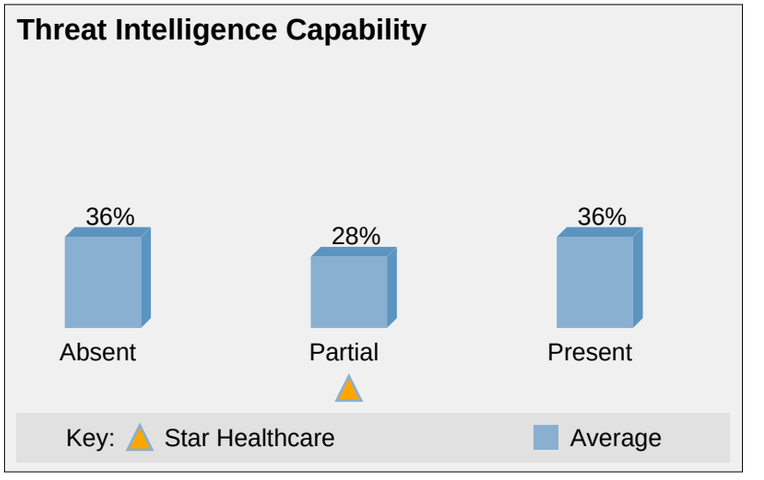


⚠ Star Healthcare is lagging the health and life sciences industry in implementing the Security Information and Event Management capability.

Security Information and Event Management is relevant to the following breach types:
- Cybercrime Hacking
- Malicious Insiders or Fraud
- Insider Snooping
- Ransomware

6.36 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

Notes: We get updates on new threats from our security provider. We really need the ability to automate update of security controls based on this feed, though.

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

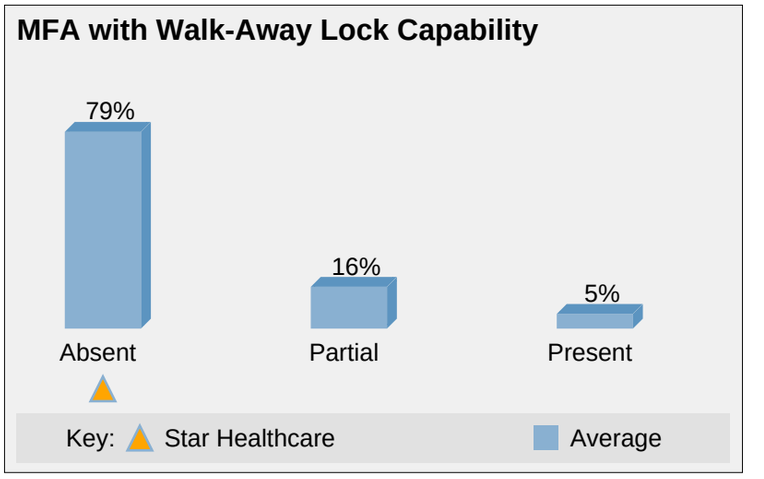
ISO: IEC 80001-1:2010:(4.6.1)

Threat Intelligence is relevant to the following breach types:

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

6.37 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.



Workshop Overview More Info

Notes: We don't currently have MFA. Once we have MFA we want to get this through Imprivata walk-away lock based on facial recognition.

! Recommended Action: 2019 - Upgrade tap-and-go MFA to also include walk-away lock to minimize risk of session hijacking when clinicians leave. See Action Plan.

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

6.38 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.

Workshop Overview More Info

Notes: We have this on some medical device machines. We need it on more.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: 27002:2013 Section 12.2.1 Controls Against Malware

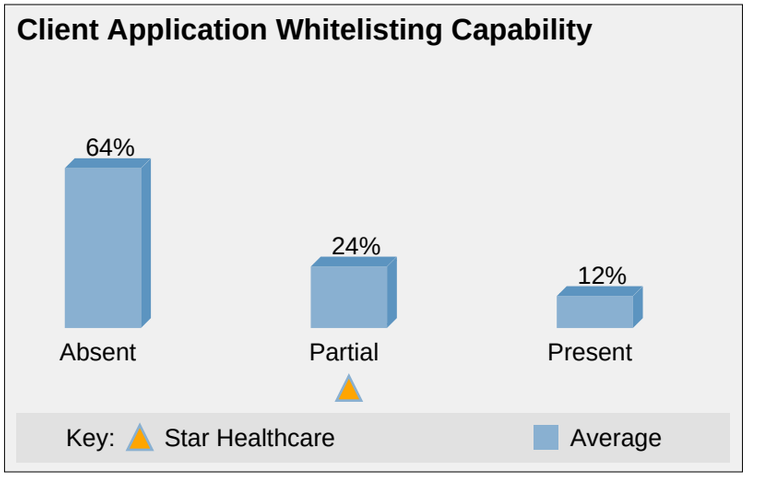
NIST: SP 800-53 Rev. 4 CM-7

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

6.39 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

Notes: Some servers associated with medical devices have this, but need it on all medical device servers.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: 27002:2013 Section 12.2.1 Controls Against Malware

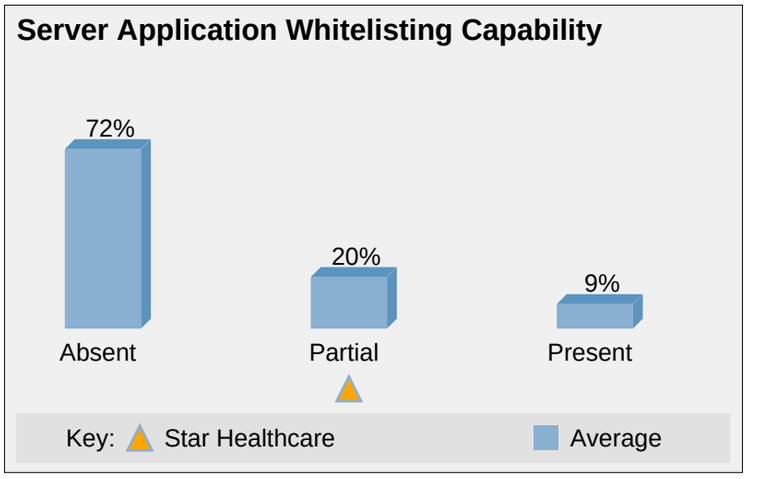
NIST: SP 800-53 Rev. 4 CM-7

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)



Server Application Whitelisting is relevant to the following breach types:
- Cybercrime Hacking
- Malicious Insiders or Fraud
- Insider Snooping
- Ransomware

6.40 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

Notes: We currently do this on data for research.

HIPAA: HHS Guidance

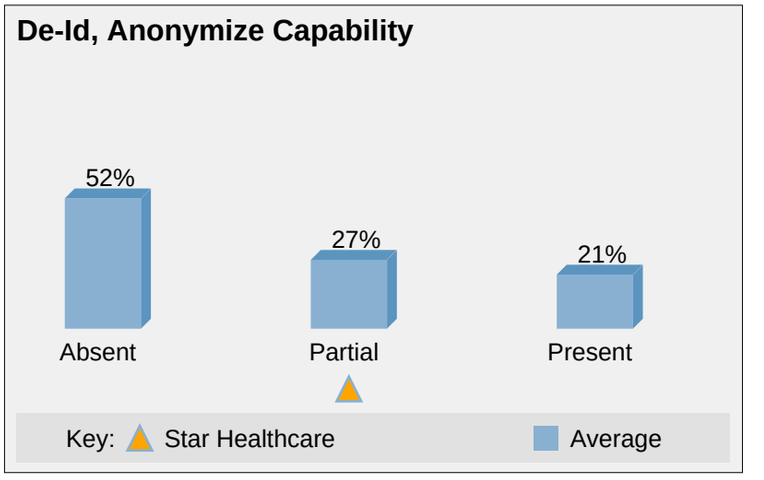
ISO: 27002:2013 Section 9.4.1 Information Access Restriction

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)



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

6.41 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

Notes: We don't do this but could use it for areas of our network that do payment processing and are subject to PCI DSS compliance.

HIPAA: HHS Guidance

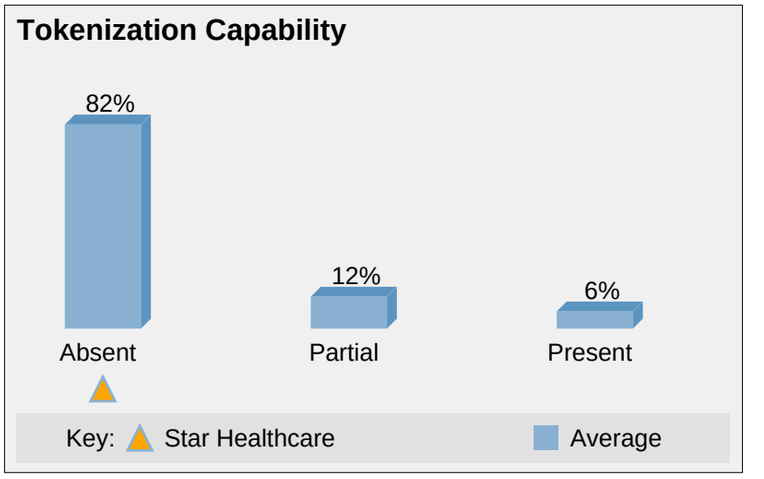
ISO: 27002:2013 Section 9.4.1 Information Access Restriction

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)



Tokenization is relevant to the following breach types:
- Cybercrime Hacking - Loss or Theft of Mobile Device or Media - Insider Accidents or Workarounds
- Improper Disposal

6.42 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

Notes: Some core / critical systems still need to be added.

HIPAA: Security Rule - Protect Availability

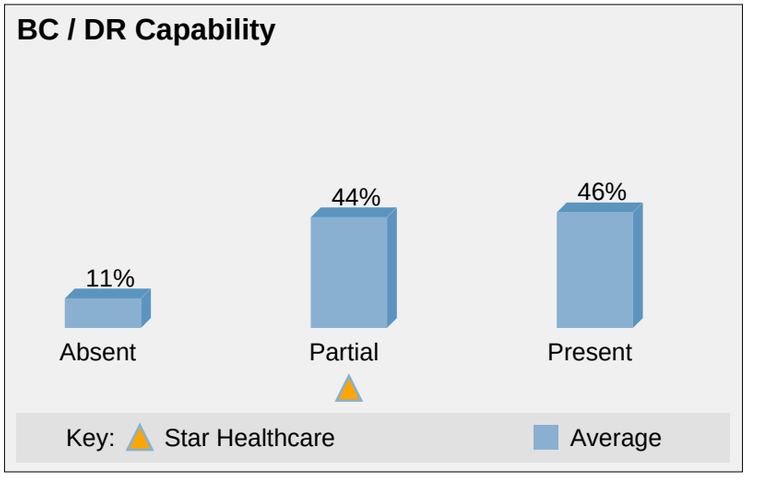
ISO: 27002:2013 Section 11.1.4 Protecting Against External and Environmental Threats

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



Business Continuity and Disaster Recovery is relevant to the following breach types:
- Cybercrime Hacking - Malicious Insiders or Fraud - Ransomware