WHITE PAPER

Health & Life Sciences
Security & Privacy

Healthcare Security Readiness – Global Industry Highlights

The Intel® Security Readiness Program assesses security maturity, priorities, readiness, gaps, and opportunities for improvement

Author

David Houlding
Director, Healthcare Privacy & Security
Intel Health & Life Sciences

Table of Contents

Executive Summary

Breaches and ransomware continue to have alarming impact and disruption across the Health & Life Sciences (HLS) industry worldwide. The global average total cost of data breaches is now USD 3.62 million, with healthcare having the highest per-capita cost across all industries at USD 380 per patient record[1]. Ransomware infections such as the WannaCry attack in May 2017 severely disrupted HLS critical infrastructure as encrypted patient information became unavailable, compromising patient care and forcing many HLS organizations to direct patients elsewhere[2]. In 2016, ransomware payments were expected to exceed USD 1 billion, according to the FBI[3]. Global ransomware damage costs are predicted to exceed USD 5 billion in 2017, up over 1,400 percent from USD 325 million in 2015[4], making cybercrime and ransomware increasingly lucrative and likely to continue to grow. Many breaches and ransomware attacks are untargeted, opportunistic, and affect HLS organizations that are lagging in cybersecurity and relatively vulnerable. However, HLS organizations typically do not know how their security capabilities compare with the industry and peers.

The Intel® Security Readiness Program (SRP) is a global open industry initiative with over 40 partners collaborating worldwide to enable HLS organizations to benchmark their cybersecurity compared to the HLS industry and peer organizations of a similar focus, locale, and size. Currently, this program has over 143 HLS organizations participating across nine countries, and is projected to more than double through 2018. In this whitepaper we share highlights from industry level, aggregate, and anonymous results of the SRP.

Ransomware (85 percent) is by far the highest priority, followed by Cybercrime Hacking (78 percent), and Insider Accidents or Workarounds (65 percent). A wide distribution in security readiness is evident across all eight breach types; for example, ransomware readiness scores range from 17 percent to 91 percent with an average of 60 percent, indicating there are many HLS organizations that are significantly lagging in security and relatively vulnerable, and on average the HLS industry has a lot of room for improvement in anti-ransomware security capabilities. Readiness for a given breach type reflects the percentage of capabilities the HLS organization has implemented that are relevant to mitigating risk of that breach type. Average readiness scores across eight breach types (see Table 1) range from 49 percent to 61 percent indicating the HLS industry has much room for improvement in security capabilities to mitigate risk of breaches and ransomware. Several foundational security capabilities in the baseline tier of maturity had relatively weak levels of implementation including Endpoint Data Loss Prevention (Discovery Mode) (20 percent), Audit and Compliance (59 percent), Endpoint Device Encryption (62 percent), and Security Incident Response Plans (61 percent). These security capabilities represent areas in urgent need of improvement for the HLS industry. On the other hand, several foundational security capabilities in the baseline tier had relatively strong levels of implementation including Firewall (92 percent), Anti-malware (92 percent), and Backup and Restore (89 percent). These represent areas where the HLS industry is relatively strong in security and in less need of attention.

Future breaches and ransomware attacks are likely to increasingly use broadcast phishing emails, computer worms, and other highly scalable propagation techniques to infect and penetrate the broadest possible target base, thereby increasing their total available market for monetization. It is therefore increasingly important for HLS organizations to understand how their security posture compares with peers and the industry and be prepared to proactively remediate security capability gaps as needed to mitigate risks and enable improved patient care.

Introduction to the Intel® Security Readiness Program

Organizations that work with sensitive patient information are eligible to participate in the Intel® Security Readiness Program (SRP). This program provides information to motivate change and inform Health & Life Sciences (HLS) organizations on how to improve security and mitigate risk of breaches and ransomware.

Scope

The healthcare SRP is an open industry initiative where Intel and over 40 industry partners worldwide provide one-hour workshops for HLS organizations to benchmark their security readiness across eight types of breaches and 42 key security capabilities. This workshop includes a high-level survey of security priorities and capabilities, which is intended to help participants learn about where they stand on selected security practices in relation to other similar participants in this study. It is complementary to and synergistic with participants' other compliance or security due diligence activities, but it is not intended to replace them. It is also different from and complementary to risk assessments that are required by several regulations and security standards. The SRP workshop reviews an organization's risk assessment capability as one of 42 key security capabilities, and if an HLS organization has a gap in this capability then the security readiness results may include a recommendation to complete a subsequent risk assessment. Participating in the healthcare SRP enables HLS organizations to review their security maturity, priorities, readiness, and security capability gaps compared with peers and the HLS industry, and consider a course of action to improve security.

Compliance

These workshops also enable HLS organizations to map their capabilities and gaps to eight different regulations, data protection laws, and security standards including HIPAA, NIST, PCI DSS, ISO2700x, GDPR, CIS, ISO80001 and EU MDR 2017/745. This enables participating HLS organizations to see how addressing a gap may also help with their regulatory, data protection law, or security standards compliance. Please consult publicly available information on your applicable regulations, data protection laws, and security standards for further information.

Table 1. Priority levels and readiness averages for benchmark set for eight breach types.[5]

			READINESS			
#	BREACH TYPE	AVERAGE PRIORITY	MIN	MEAN	MAX	STD DEV
2.1	Cybercrime Hacking	Medium/High (78%)	23%	60%	92%	16%
2.2	Loss or Theft of Mobile Device or Media	Medium (51%)	14%	51%	90%	15%
2.3	Insider Accidents or Workarounds	Medium/High (65%)	15%	54%	90%	16%
2.4	Business Associates	Medium (52%)	6%	61%	100%	21%
2.5	Malicious Insiders or Fraud	Medium (44%)	15%	52%	89%	15%
2.6	Insider Snooping	Medium (48%)	13%	50%	89%	16%
2.7	Improper Disposal	Low/Medium (36%)	0%	49%	92%	18%
2.8	Ransomware	High (85%)	17%	60%	91%	16%

Eligibility

Any HLS organization that works with sensitive patient information is eligible to participate in the SRP, including providers, payers, pharmaceuticals, life sciences, and business associates or data processors. HLS organizations worldwide, whether small, medium, or large, are eligible to participate in the SRP. To date, more than 143 HLS organizations from 9 countries are participating in this program, including the United States, the United Kingdom, Germany, France, Sweden, Brazil, Canada, Denmark, and Ireland, and this program is available to HLS organizations worldwide.

Format

The one-hour SRP workshop can be conducted by Intel or an industry partner, remotely via conference call, or in person. Workshops may be done with either a single HLS organization or in a group format with multiple HLS organizations. This workshop involves a trained security assessor from Intel or an industry partner helping the HLS organization's security team to complete a security readiness worksheet or questionnaire. To date, over 143 SRP workshops have been completed.

Complimentary

SRP workshops and participation in the healthcare SRP are complimentary and free of obligation for HLS organizations, including both the one-hour SRP workshop and reports issued based on it. If the SRP identifies security capability gaps and an HLS organization requests help from Intel or an industry partner to address such gaps, Intel and industry partners are ready to assist as needed and where applicable solutions and services are available.

High-Quality Data

The quality of the data acquired through the SRP is considerably higher than typical security surveys. This is achieved through the use of trained security assessors, verified HLS organization security teams participating in the SRP, and by enabling participating HLS organizations to update their assessed data any time. This leads to high-quality security readiness benchmarking data, which is paramount as HLS organizations that participate look to make decisions based on security readiness benchmark reports.

Confidentiality

The SRP workshop only involves completion of an SRP worksheet. It does not include any scanning or running anything on the HLS organizations networks. Information collected is minimal but sufficient for the purpose of benchmarking security readiness and does not include collection of any Personally Identifiable Information (PII) or Protected Healthcare Information (PHI) from the HLS organization. Information is treated as strictly confidential, with encryption at rest and in transit, including the security readiness reports delivered as encrypted PDF documents. SRP information is accessed only on a need-to-know basis for the purpose of completing SRP analytics and reporting, and delivering confidential, encrypted reports to HLS organizations. Non-Disclosure Agreements (NDAs) can be set up as needed with Intel or industry partners to support participation in the SRP.

Results and Analysis

These SRP results represent highlights from industry level, aggregate, and anonymous data from 143 HLS organizations participating in the program. More detailed and updated HLS industry level results may be found at Intel.com/SecurityReadiness.

Maturity

Maturity is shown as the percentage of security capabilities that the benchmark set has implemented in the Baseline, Enhanced, and Advanced maturity levels. As the security posture for the benchmark set improves, the assessment at each of these maturity levels will approach 100 percent. These are high-level results for a broad overview of the maturity of the benchmark set.

In Figure 1, the results show that while healthcare has most (73 percent) of the Baseline security capabilities, it only has half (50 percent) of the Enhanced capabilities, and few (30 percent) of the Advanced capabilities. Gaps represent increasing opportunities for healthcare to bolster security going from Baseline, to Enhanced, and Advanced maturity tiers and associated security capabilities. See the Capabilities section for a detailed view of the level of implementation of each of the 42 security capabilities across the three tiers of maturity.

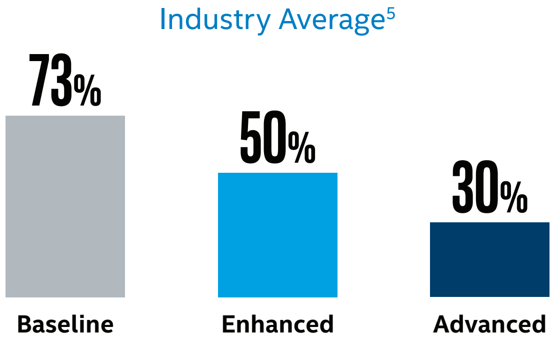

Figure 1. The percentage of security capabilities that the benchmark set has implemented in the Baseline, Enhanced, and Advanced maturity levels.

Priorities and Readiness

The results in Table 1 show the priority (level of concern) and readiness for the benchmark set across eight breach types. Readiness for each breach type is the percentage of relevant security capabilities the benchmark set currently has implemented. Statistics for readiness show the minimum, average, maximum, and standard deviation scores for the benchmark set.

These results show that Ransomware (85 percent) is the highest priority, followed by Cybercrime Hacking (78 percent), and Insider Accidents or Workarounds (65 percent). Across all eight breach types, readiness scores show a wide variation between the Min and Max readiness. For example, in Ransomware, the lowest scoring HLS organization had only 17 percent of the anti-ransomware security capabilities, while the highest scoring HLS organization had 91 percent. Average readiness across breach types ranged from 49 percent to 61 percent indicating much room for improvement in security capabilities in the HLS industry as a whole across all breach types.

Capabilities

The capabilities in the security maturity model (Table 2) are directly relevant to mitigating risk of various types of breaches. These capabilities span administrative, physical, and technical safeguards. Each capability is assessed from the standpoint of whether it is effective or not, and this includes any required people, process, and technology aspects. This info presents a comprehensive overview of all 42 assessed security capabilities. Each capability is classified in the Baseline, Enhanced or Advanced security maturity levels, and the percentage next to each capability indicates the current level of implementation of that capability in the HLS industry.

These results show more green (most have the capability) in the Baseline tier, and then progressively more yellow (some have the capability) and red (few have the capability) moving into the Enhanced and Advanced tiers. Endpoint Data Loss Prevention (Discovery Mode) (20 percent), Audit and Compliance (59 percent), Endpoint Device Encryption (62 percent), and Security Incident Response Plans (61 percent) represent the weakest security capabilities in the Baseline tier. These represent areas urgently in need of improvement across the HLS industry to mitigate risk of breaches and ransomware. On the other hand, Firewall (92 percent), Anti-malware (92 percent), and Backup and Restore (89 percent) represent areas where the HLS industry security is relatively strong and in less need of attention.

Table 2. A comprehensive overview of the level of implementation of all 42 assessed security capabilities.[5]

KEY + Most have it ~ Some have it – Few have it

BASELINE		
+	77%	Policy
+	71%	Risk Assessment
~	59%	Audit and Compliance
+	70%	User Awareness Training
~	62%	Endpoint Device Encryption
~	61%	Mobile Device Management
–	20%	Endpoint Data Loss Prevention (Discovery Mode)
+	92%	Anti-Malware
+	81%	Identity and Access Management, Single-Factor Access Control
+	92%	Firewall
+	89%	Email Gateway
+	85%	Web Gateway
+	72%	Vulnerability Management, Patching
~	61%	Security Incident Response Plan
+	85%	Secure Disposal
+	89%	Backup and Restore
ENHANCED		
~	53%	Device Control
+	66%	Penetration Testing, Vulnerability Scanning
–	29%	Client Solid State Drive (Encrypted)
–	17%	Endpoint Data Loss Prevention (Prevention Mode)
–	29%	Network Data Loss Prevention (Discovery Mode)
~	51%	Anti-Theft: Remote Location, Lock, Wipe
~	42%	Multi-Factor Authentication with Timeout
+	83%	Secure Remote Administration
–	15%	Policy-Based Encryption for Files and Folders
~	40%	Server/Database/Backup Encryption
+	67%	Network Segmentation
~	61%	Network Intrusion Prevention System
+	85%	Business Associate Agreements
~	64%	Virtualization
ADVANCED		
–	15%	Server Solid State Drive (Encrypted)
–	20%	Network Data Loss Prevention (Prevention Mode)
–	28%	Database Activity Monitoring
~	41%	Digital Forensics
~	40%	Security Information and Event Management
~	49%	Threat Intelligence
–	13%	Multi-Factor Authentication with Walk-Away Lock
–	23%	Client Application Whitelisting
–	19%	Server Application Whitelisting
~	34%	De-Identification/Anonymization
–	12%	Tokenization
+	67%	Business Continuity and Disaster Recovery

Conclusion

Ransomware and breaches are disruptive and degrading patient trust and quality of care, and in some cases compromising patient safety. Many types of attacks are untargeted, opportunistic, and tend to affect HLS organizations that are lagging in security, have weak security posture, and are relatively vulnerable. Through the Intel Healthcare Security Readiness Program (SRP), HLS organizations can benchmark their security capabilities against the HLS industry and peers of similar locale, type, and size to understand if they are lagging, and if so, which capabilities specifically. They can then use this information to prioritize security initiatives to proactively remediate gaps to mitigate risk of breaches and ransomware. Security teams in HLS organizations can also use this information to help rally support from stakeholders to allocate resources necessary to address gaps. This report shares highlights from HLS industry level, aggregate, and anonymous results from over 143 HLS organizations across nine countries participating in this program. These results show top priorities, readiness distributions, and levels of implementation of 42 key security capabilities across the HLS industry worldwide. Guided by this high-quality data, we can move the discussion from "healthcare security is lagging" to specific high-priority breach types and specific security capabilities in urgent need of improvement across the HLS industry. This enables proactive mitigation of risk of breaches and ransomware across the HLS industry, and helps pave the way for improved patient care.

If you are an HLS organization interested in participation in the Healthcare Security Readiness Program, or an industry partner interested in collaboration opportunities in this program, contact **SecurityReadiness@Intel.com** for more information.

Learn More

Visit **intel.com/SecurityReadiness** for additional information on the Intel Healthcare Security Readiness Program including an overview, sample security readiness report, and detailed updated HLS industry-level security readiness results.

- Healthcare Security Readiness Program: concise overview brief
- Sample Security Readiness Report: representative of the benchmark report received by Health & Life Sciences organizations participating in the Security Readiness Program
- HLS Security Readiness Program – Global Industry Report: details industry level, aggregate, and anonymous results of the Security Readiness Program
- Contact SecurityReadiness@Intel.com for further information and how to participate in the Security Readiness Program.

[1] Ponemon 2017 Cost of Data Breach Study – Global Overview www.ibm.com/security/data-breach/

[2] WannaCry Ransomware Attack en.wikipedia.org/wiki/WannaCry_ransomware_attack

[3] Ransomware: Now a Billion Dollar a Year Crime and Growing www.nbcnews.com/tech/security/ransomware-now-billion-dollar-year-crime-growing-n704646

[4] Ransomware Damage Report by Cybersecurity Ventures cybersecurityventures.com/ransomware-damage-report-2017-5-billion/

[5] Source: Intel.com/SecurityReadiness

This health & 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.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software, or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer, or learn more at Intel.com.

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

THE INFORMATION PROVIDED IN THIS PAPER IS INTENDED TO BE GENERAL IN NATURE AND IS NOT SPECIFIC GUIDANCE. RECOMMENDATIONS (INCLUDING POTENTIAL COST SAVINGS) ARE BASED UPON INTEL'S EXPERIENCE AND ARE ESTIMATES ONLY. INTEL DOES NOT GUARANTEE OR WARRANT OTHERS WILL OBTAIN SIMILAR RESULTS.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS AND SERVICES. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS AND SERVICES INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

0917/JBLA/KC/PDF ♻ Please Recycle 335894-001US