Healthcare Security Readiness Program

Reduce risk of ransomware and breaches. Enable adoption of new technology to improve patient care.

Breaches and ransomware are having major impact and disruption to healthcare organizations worldwide. Many attacks are untargeted, opportunistic, and use broadcast propagation techniques such as phishing and computer worms. These attacks and breaches tend to affect organizations lagging in security. Is your organization's security lagging, on par, or leading peers and the industry? How do your security capabilities and gaps compare? Join us for a quick security readiness workshop to analyze your current security maturity, priorities and readiness across 8 of the most common types of breaches including ransomware, and security capabilities across 42 key security safeguards. Identify gaps, and opportunities for improvements. Receive a detailed, confidential, and encrypted report that benchmarks your security against peers and the industry, and summarizes recommendations on how to improve your security with a multi-year action plan. Receive quarterly updated reports for one year after your workshop to track your security against peers and the industry. Use this detailed, data rich report to prioritize remediation, rally support to address gaps, motivate change, and inform your decisions on the best next steps to improve your organization's security, mitigate risk of ransomware and breaches, and pave the way for improved patient care.

Breaches in Healthcare

Avoiding breaches and associated business impacts is the top privacy and security concern across healthcare organizations, globally. Business impacts average USD 3.62 million per breach event, or USD 380 per patient record breached, according to the 2017 Ponemon Cost of a Data Breach research. Ransomware outbreaks such as WannaCry and Petya are having major disruption on healthcare organizations worldwide. In 2016 ransomware payments were expected to exceed USD 1 billion, according to the FBI. The need to rapidly address breaches has never been greater.

Healthcare security is becoming about survival. Even with good security, residual breach risk is never zero. While no organization is immune from breaches, it is increasingly important to understand whether your security is lagging peers and the rest of the industry, and relatively vulnerable. No organization wants to be "low hanging fruit" for breaches, for example at the hands of ransomware or cybercrime hackers.

However, security is complex, with many risks, safeguards, and a rapidly changing threat landscape. Compounding this is a dire shortage of security experts in healthcare. Increasingly, healthcare organizations view basic regulatory compliance as necessary but insufficient to adequately mitigate risk of breaches.

Benchmark Your Security

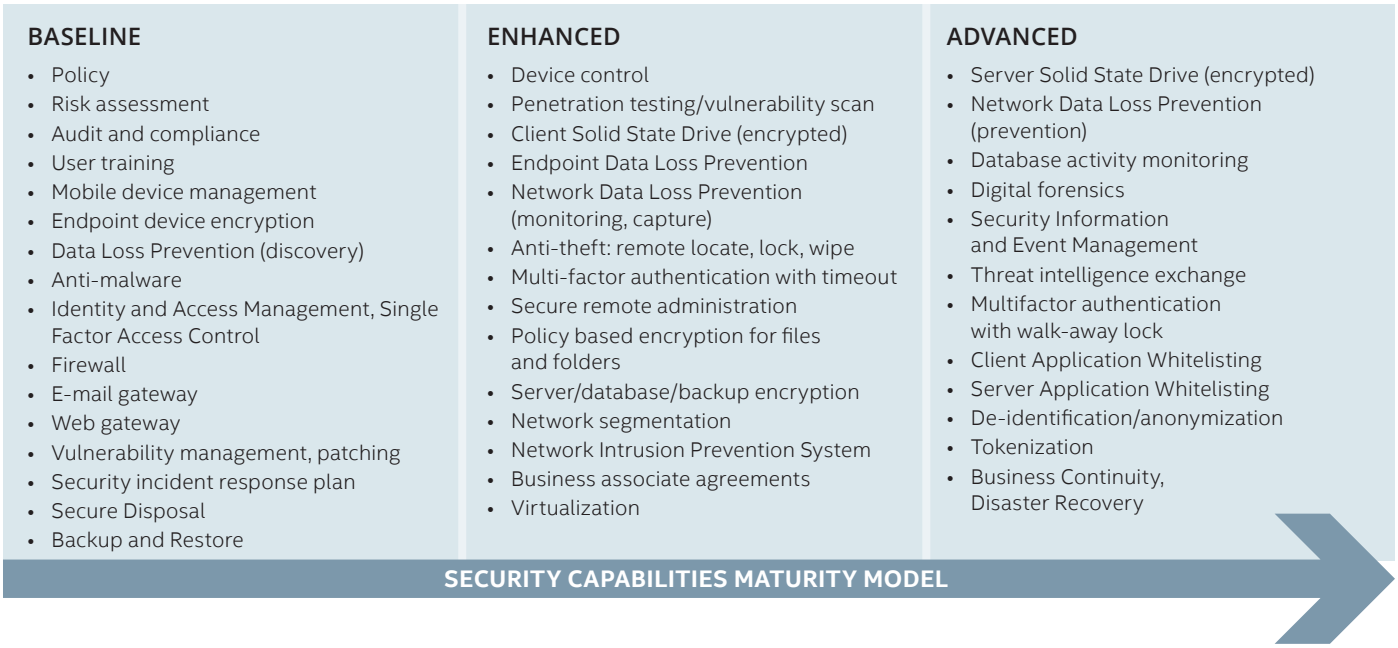
The Security Readiness Workshop is a 1 hour, complimentary, confidential engagement with a security assessor to measure security priorities and safeguards in your organization using a security maturity model. It does not require a security expert from your organization, just someone that is knowledgeable, at a high level, about your organization's security priorities and capabilities. It may be conducted remotely or in person, either as a direct engagement with your organization, or in a group workshop. Participating organizations receive a detailed, data rich, confidential, and encrypted report benchmarking their security against the industry and peer organizations of a similar locale, focus, and size. Analysis results include security maturity,

Highlights

- Benchmark your security against peers and the industry
- Identify if you are lagging in security, and if so where
- See if you may be over or under prioritizing across 8 of the most common types of breaches
- Analyze how your security capabilities and gaps relate to regulations, data protection laws, and security standards
- Receive a multi-year action plan with recommendations to improve security
- Initial and quarterly reports for one year provide updates and enable tracking against plan

Logistics

- All health & life sciences organizations worldwide that work with sensitive patient information are eligible including providers, payers, pharmaceuticals, life sciences, and business associates or data processors
- 1 hour workshop
- Complimentary, confidential
- Conducted by phone or face-to-face, by Intel or a partner



priorities and readiness across 8 of the most common types of breaches, and how security capabilities compare across 42 key security safeguards. Any security gaps are highlighted, and a multi-year plan provided to incrementally improve security and reduce risk. Participating healthcare organizations are eligible to receive quarterly updated reports for 1 year after the workshop. Participation and reports are confidential. Only anonymized information is aggregated with broader industry security readiness data, for benchmarking purposes.

Focus on Top Breach Concerns

There are many types of breaches including ransomware, cybercrime hacking, insider accidents or workarounds, loss or theft of mobile devices or media, business associates, malicious insiders or fraud, snooping, improper disposal, and so forth. For each type of breach, the set of safeguards required to mitigate it vary. Given a particular type of breach, the security maturity model may be used to rapidly assess the security posture for an organization, and readiness for that type of breach. This is also compared with the industry and peer organizations of a similar locale, focus, and size. This enables focus on top breach concerns, while also enabling healthcare organizations to measure their security across 8 of the most common breach types relative to peers and the industry.

Prioritize Security Initiatives

The healthcare security readiness workshop is a high level survey of potential security issues and is intended to inform participants where they stand on selected security practices in relation to other similar participants in this study, and 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 is a quick checkpoint workshop to determine where a healthcare organization stands in terms of their security posture, relative to peers and the rest of the healthcare industry. It provides an opportunity to look at gaps and next steps that can be taken to improve security posture. A security readiness workshop may identify needs and lead to deeper subsequent engagements including policy creation or update, risk assessment, penetration testing, vulnerability scanning, audit, user training, or implementation of various security safeguards.

Improve Compliance

Security readiness reports map 42 key security capabilities and any gaps to regulations, data protection laws, and standards including HIPAA, NIST, PCI-DSS, CIS, GDPR, ISO2700x, ISO80001, and EU MDR 2017/745. This enables organizations to see how addressing gaps may also help with compliance.

Industry Collaboration

This program is an open industry initiative led by Intel Health and Life Sciences, with over 40 industry partners collaborating to make security readiness workshops available to healthcare organizations worldwide. Over 170 health and life sciences organizations are currently participating in the security readiness program, from across 9 countries, and participation is projected to more than double worldwide through end of year 2018.

Program

Intel and partners are conducting healthcare security readiness workshops for providers, payers, pharmaceuticals, life sciences, and business associates or data processors globally. Any organization worldwide that works with sensitive patient information is eligible to participate.

How to Engage

We welcome your participation in this program. To find out more please visit:

SageDataSecurity.com/Security-Readiness

or contact:
SecurityReadiness@SageDataSecurity.com

sage DATA SECURITY

intel