Healthcare Security Readiness Program

Reduce breach risk. Enable adoption of new technology to improve patient care.

How does your security compare with the rest of the healthcare industry? Join us for a quick readiness workshop to analyze your current security posture and level of maturity. Identify gaps, and opportunities for improvements. Receive a report summarizing recommendations on how to improve your security with a multi-year plan. Receive quarterly reports for one year after your workshop that enable you to compare your security, and track your progress against the rest of the healthcare industry. Use this information to motivate change and inform your decisions on the best next steps to improve security in your healthcare organization and mitigate breach risk.

Breaches in Healthcare

According to research conducted by Intel in 2016, avoiding breaches and associated business impacts is the top privacy and security concern across healthcare organizations, globally. Business impacts average USD 7.01 million per breach event, or USD 355 per patient record breached, according to the 2016 Ponemon Cost of a Data Breach research. With the pace of change and innovation in healthcare driving increased risk, 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 you are vulnerable relative to peers and the rest of the healthcare industry. No healthcare organization wants to be "low hanging fruit" for breaches, for example at the hands of 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.

Security Maturity

Maturity models have a proven track record of success in healthcare. For example the HIMSS Analytics EMRAM, or EMR Adoption Model has over 5,300 hospitals using it globally. It is based on a maturity model that enables healthcare providers to rapidly assess their level of maturity, any gaps, and improvements to get to the next level. It enables healthcare providers to track their maturity level and progress against the healthcare industry norms. The proven merits of a maturity model approach may also be used to help simplify breaches and associated risk mitigation for healthcare. A security maturity model enables a healthcare organization to rapidly assess their security maturity, identify gaps, and a multi-year plan for improvement that fits within limited annual budget and resource constraints.

Highlights

- Quickly assess security
- Analyze security relative to healthcare industry
- Create action plan to improve security, reduce risk, and enable adoption of beneficial new technology to improve care

Deliverables

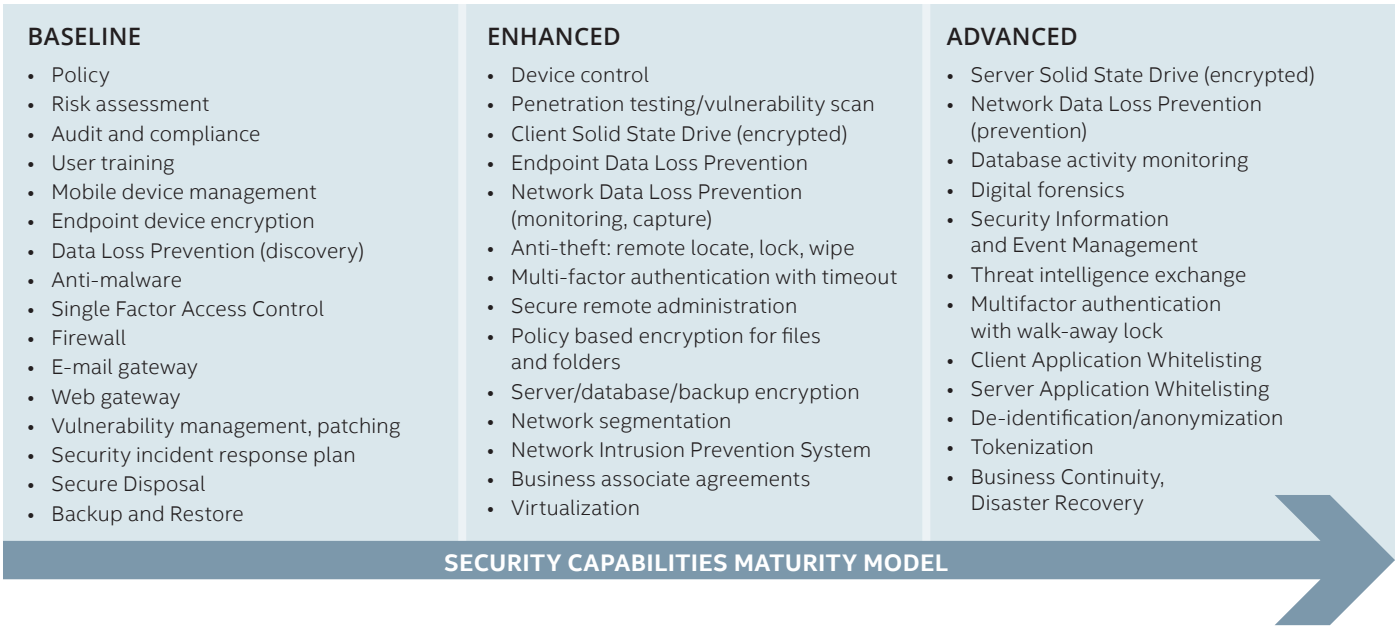
- Initial and quarterly reports
- Maturity level relative to the healthcare industry
- Gaps and improvements
- Multi-year plan fits budget, resource constraints
- Track progress against plan

Logistics

- 1-2 hours engagement
- Experts not required
- Review security
- Conducted by phone or face-to-face

Assess Your Security

The Healthcare Security Readiness Workshop is a 1-2 hour engagement with a security assessor to measure security safeguards in your healthcare organization against the healthcare security maturity model. It does not require a security expert from your healthcare organization, just someone that is knowledgeable, at a high level, about what security safeguards are in place. It may be conducted by phone or face-to-face. After the workshop the healthcare organization will receive



a report summarizing the findings, including their maturity level, how they compare with the rest of the healthcare industry, any gaps, and a multi-year plan to incrementally build their security. Participating healthcare organizations will also receive quarterly update reports for up to one year after the workshop showing where they stand relative to the healthcare industry. Results of the workshop and reports are confidential. Only de-identified and anonymized information is aggregated with broader healthcare industry security readiness data.

Focus on Top Breach Concerns

There are many types of breaches including cybercrime hacks, loss or theft of mobile devices or media, accidents or workarounds, business associates, malicious insiders or fraud, snooping, improper disposal, ransomware, and so forth. For each type of breach, the set of safeguards required to mitigate it vary. Given a particular type of breach, the healthcare security maturity model may be used to rapidly assess the security posture for a healthcare organization, for that type of breach. This enables focus on top breach concerns, while also enabling healthcare organizations to measure their security posture across a variety of breach types.

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 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 healthcare security workshop may in fact 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

Improvements to security based on this workshop may also help with compliance with privacy and security regulations, data protection laws, and standards. This initiative will show traceability from safeguards in the security maturity model to various applicable and commonly used privacy and security regulations, data protection laws, and standards. This enables visibility into how improving security based on this workshop may also help in compliance with applicable regulations, laws, and standards. These include HIPAA, NIST, PCI DSS, CIS, ISO2700x, and GDPR.

Industry Collaboration

This program is an open initiative led by Intel Health and Life Sciences, and is a global collaborative effort between multiple healthcare organizations, assessors, security and hardware vendors, resellers, system integrators, and distributors.

Program

Intel and partners are conducting healthcare security workshops for providers, payers, pharmaceutical, and life sciences organizations globally, running through 2017. Any organization worldwide that works with sensitive patient information in some form is eligible to participate.

How to Engage

We welcome your participation in our program. To find out more and see a sample report, please visit **intel.com/securityreadiness**, or contact:

Intel Health & Life Sciences
Privacy & Security
securityreadiness@intel.com