Healthcare Breach Security Assessment

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

How does your breach security compare with the rest of the healthcare industry? Join us for a quick assessment to analyze your current breach security posture and level of maturity. Identify gaps, and opportunities for improvements. Receive a post assessment report summarizing recommendations on how to improve your breach security with a multi-year plan. Receive quarterly reports for one year after assessment that enable you to compare your breach 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 breach security in your healthcare organization and mitigate breach risk.

Breaches in Healthcare

According to research conducted by Intel in 2015, avoiding breaches and associated business impacts is the top privacy and security concern across healthcare organizations, globally. Business impacts average USD 6.53 million per breach event, or USD 398 per patient record breached, according to the 2015 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.

Breach 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 breach security maturity model enables a healthcare organization to rapidly assess their breach security maturity, identify gaps, and a multi-year plan for improvement that fits within limited annual budget and resource constraints.

Highlights

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

Deliverables

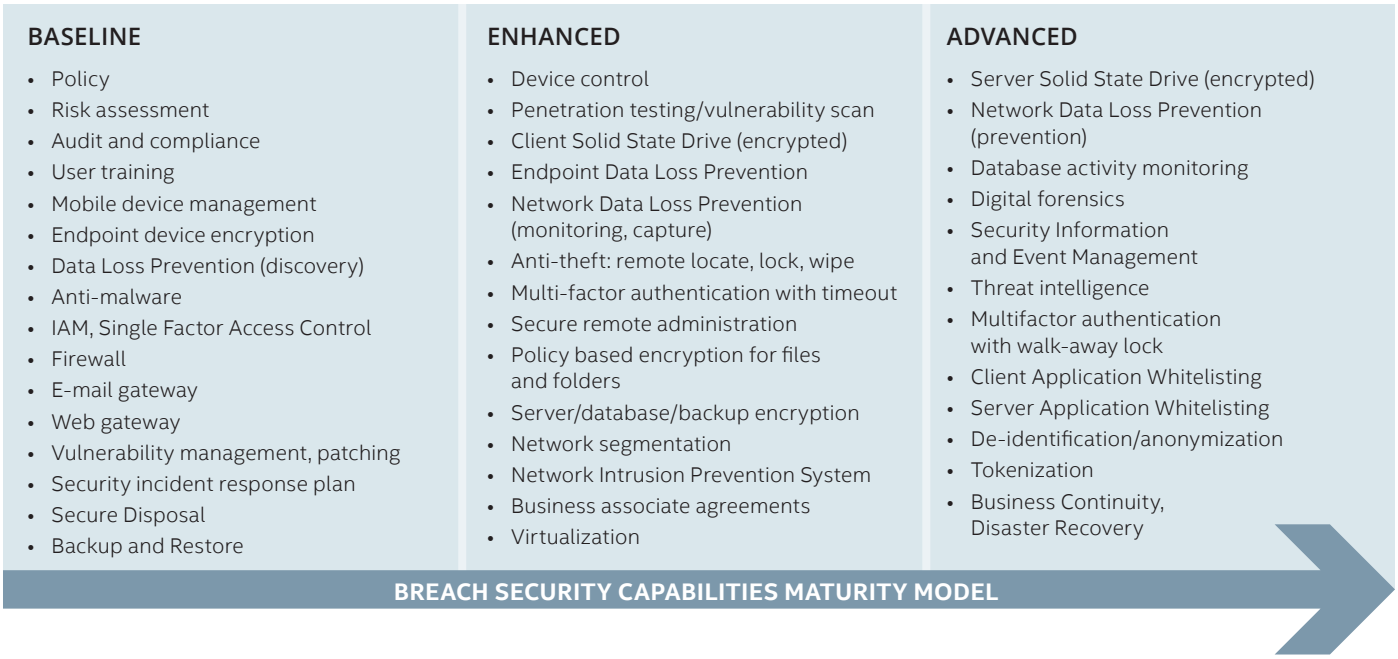
- Initial and quarterly reports
- Maturity level relative to the healthcare industry
- Gaps and improvements
- Multi-year plan fits budget, resource constraints
- Track progress against plan

Logistics

- 1-2 hours engagement
- Experts not required
- Review breach security
- Conducted by phone or face-to-face
- May qualify for Intel subsidy

Assess Your Breach Security

The Healthcare Breach Security Assessment is a 1-2 hour engagement with a security assessor to measure breach security safeguards in your healthcare organization against the healthcare breach 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 assessment 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 breach security. Participating healthcare organizations will also receive quarterly update reports for up to one year after assessment showing where they stand relative to the healthcare industry. Results of the assessment and reports are confidential. Only de-identified and anonymized information is aggregated with broader healthcare industry breach security posture 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 breach security maturity model may be used to rapidly assess the breach 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 breach security assessment is a high level survey of potential breach 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 assessment to determine where a healthcare organization stands in terms of their breach 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 breach security posture. A healthcare breach security assessment 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 breach security safeguards.

Improve Compliance

Improvements to breach security based on this assessment may also help with compliance with privacy and security regulations, data protection laws, and standards. This initiative will show traceability from safeguards in the breach security maturity model to various applicable and commonly used privacy and security regulations, data protection laws, and standards. This enables visibility into how improving breach security based on this assessment can help in compliance with applicable regulations, laws, and standards.

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.

Pilot Program

Intel and partners are conducting pilot healthcare breach security assessments for providers, payers, pharmaceutical, and life sciences organizations globally, running through 2016.

How to Engage

We welcome your participation in our pilot program. To find out more or sign up to participate please contact:

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

Copyright © 2016. All rights reserved. Intel and the Intel logo are trademarks of Intel Corporation in the U.S. and/or other countries.
*Other names and brands may be claimed as the property of others. 0516/DW/HBD/PDF ♻ Please Recycle