Healthcare Data Breaches:
Continual Security Improvement as a Path to Lower Risk

Jarad Carleton, Principal Consultant,
Digital Transformation Consulting Practice
Data Breaches on the Rise While Preparedness is Stuck in Neutral ................................. 3
The Wild World of Data Breaches .......................................................................................... 5
  Insider Workarounds and Accidents ................................................................................. 5
  Mobile Device Loss or Theft ............................................................................................. 5
  Compromised Business Partners ...................................................................................... 6
  Malicious Insiders ............................................................................................................ 6
  Cybercrime ....................................................................................................................... 6
Security is Complex .............................................................................................................. 7
The Healthcare Security Maturity Model ............................................................................. 8
Assessing Your Security Breach Posture ............................................................................ 8
Intel Security Products and the Security Maturity Model .................................................... 9
Why Intel Security Group? .................................................................................................. 9
A Wait-and-see Approach to Security is Not an Option for Healthcare ............................ 10
Appendix ............................................................................................................................... 10
  A Partial list of Data Protection Authorities (DPAs) ....................................................... 10
  Mapping Intel Security Products to the Security Maturity Model .................................. 11
DATA BREACHES ON THE RISE WHILE PREPAREDNESS IS STUCK IN NEUTRAL

One doesn’t have to be from an advanced e-society like Estonia1 to comprehend that the world is in a race to digitize records and to network every database, computer, tablet, and device of all types. The path every society is taking toward the Internet of Everything2 (IoE) will increase the speed of our transition to digital records and the accessibility of that data in the future.

However, as society deepens its commitment to a highly networked digital life, even non-technical individuals that benefit from fast and easy access to data are aware that the frequency of data breaches year over year has continued at the same pace with only slight fluctuations. In addition, the negative impact of data breaches has become a fiscal metric that many organizations are tracking.

As data breaches continue unabated, the healthcare industry must confront significant challenges. On the one hand, the industry is striving to implement electronic health record (EHR) initiatives that have been mandated by governments around the world. On the other hand, healthcare organizations are less confident of their security processes and practices. In fact, only 43% of the industry is considered to have highly sophisticated security, and it is the least likely industry to have an executive accountable for data security in the organization.3

There is no question about the sensitive nature of data the healthcare industry has and its ability to be used for identity theft and variety of other unethical and criminal acts. That is one of the leading reasons why the per capita cost for healthcare data breaches is $363, which is the highest of every other industry4 and has been for years.5 Due in part to the fact that all organizations are taking longer to find and remediate data breaches,6 the total cost for healthcare data breaches will continue to rise.
Just as troubling is that despite persistent stories in the global press, seminars on cybersecurity, and regulatory requirements for industries such as healthcare to protect personally identifiable information (PII), more than half of all organizations in every industry have not improved their security posture vis-à-vis their security adversaries.

Source: Frost & Sullivan 2015 (ISC)² Global Information Security Workforce Study, N = 14,000
THE WILD WORLD OF DATA BREACHES

The world of data breaches is a broad area, but most breaches fall into five general categories that healthcare organizations are not always on guard to protect themselves against:

Insider Workarounds and Accidents

The vast majority of employees in healthcare organizations are honest, hard-working individuals that chafe against inefficient administrative processes. As innovative workers do in every other industry, healthcare employees at all levels of the organization will find workarounds to processes that impede their ability to deliver better patient care, and do their jobs faster and better. A technology workaround nearly everyone is familiar with today is using a personal mobile device to access email, work documents, and other work data on the go.

Unfortunately when bring your own device (BYOD) is not managed by an IT department, it is the same as bringing an unsecured network and public cloud into a work environment where 44% of healthcare providers don’t have a security strategy for cloud computing. That’s a significant concern as mobile devices connect to not only mobile telecom networks, but also public Wi-Fi, and use insecure cloud-based applications that retain data in perpetuity.

Data breach accidents can happen through man-in-the-middle (MitM) attacks on Wi-Fi networks, breaches at cloud-based services providing mobile apps, unintentional download of mobile malware, phishing, spear phishing, and more. In addition, the physical locations of data center servers that support mobile apps on personal devices can create complicated challenges. This is because of regulatory requirements that restrict the movement of healthcare data across geopolitical boundaries and prohibit data storage outside of defined legal jurisdictions. Unfortunately, healthcare workers are not information security professionals, so they aren’t always on guard against the variety of ways PII breaches occur.

Mobile Device Loss or Theft

Given the prevalence of personal mobile device use in the global healthcare industry, one would assume that almost every organization has security strategies in place to manage BYOD. The reality is that 38% of healthcare organizations do not have a security strategy for employee use of personal devices in the workplace. This is problematic for several reasons, the first of which is that mobile devices are frequently left in airports and train stations, as well as on airplanes, taxis, busses, trains, store checkout counters, and a number of other places.

The bad news for the healthcare industry, its partners, and patients is that in the US alone, 43% of healthcare data breaches are attributed to lost or stolen devices. This strikingly high number can be attributed to users that fail to password lock their devices and users that lock their devices with easily guessed pass codes. What’s more, when someone has a lax attitude toward locking a mobile device, that behavior carries over to mobile apps where the user will have weak passwords and will let the app leave him or her logged in for the sake of convenience. The resulting combination of lax security is disastrous when a device is lost or stolen.
Compromised Business Partners

As stories of data breaches continue to make a splash in the news media, it’s a safe bet to say that everyone in the healthcare industry is aware that there are individuals and organized groups whose primary goal is to break into networked systems and steal data. The data breach stories in the mainstream media tend to report on types of data stolen such as credit card numbers, tax-payer ID numbers, names, addresses and telephone numbers. It’s with far less frequency that the media tells the story of how a data breach occurred. In the case of Target, a HVAC vendor that worked with the retail chain was the victim of a malware phishing attack that compromised its computer systems. That opened a door into Target’s external billing system that eventually led to additional systems compromises at Target and one of the largest data breaches in history. With the number of companies healthcare organizations work with daily, a business partner that is compromised could be the root cause of future healthcare PII data breaches.

Malicious Insiders

While most employees are ethical and trustworthy, the risk of a data breach caused by a malicious insider is real. All it takes is a single employee to use their access to health records because of curiosity, anger, or the lure of potential profit to cause a PII data breach that can lead to lawsuits and fines.

In the United States alone, the root cause of 12% of data breaches in healthcare organizations was due to a malicious insider. However, the access that a malicious insider has to computer systems with full medical records and payment information means that the severity of this type of data breach could be catastrophic. That’s one reason why 26% of healthcare organizations worry about security threats originating from malicious insiders.

Cybercrime

It isn’t difficult to draw direct links between cybercrime and data breaches in the healthcare industry. The loss of partial or full medical records resulting from insider accidents, mobile device loss, compromised business partners, and malicious insiders provide PII that’s used to steal identities.

Whereas the news media focuses a lot on the theft of credit card data, the fact is that data from healthcare organizations is up to 20 times more valuable to cybercriminals. The reason is that healthcare data is a digital version of durable goods; it can’t be canceled like a credit card number and lasts for the life of an individual. The danger is that security professionals believe that with this type of information it will be possible to destroy a person’s cyber footprints to the extent that legacy IT systems can’t tell the difference between a real person and the stolen identity. When this occurs a stolen identity will be unrecoverable, a situation referred to in the security circles as individual obliteration.
Regrettably, the healthcare industry has detected, on average, almost 60% more security incidents than in 2013 and the efforts of cybercriminals are paying dividends; 20% of the healthcare industry has reported incidents where PII was compromised. At the same time, the industry has observed a 32% increase in identity theft.

**SECURITY IS COMPLEX**

Security is a complex ecosystem that can seem overwhelming at times, but it’s important for healthcare organizations, large and small, to avoid getting hung up on the complexity of the challenge and use it as an excuse to postpone what needs to be done. A wait-and-see approach isn’t a viable strategy for an industry that has to protect PII and ensure that those efforts are aligned with corporate governance and compliance requirements.

Instead of getting overwhelmed to a point of inaction, healthcare IT professionals should approach the data breach prevention challenge as a process of continual year-over-year improvement, similar to the seven-level HIMSS Continuity of Care Maturity Model. As with any multi-year improvement initiative, an assessment of baseline conditions has to be developed. Thus, to proactively address the healthcare data breach challenge, one must begin with a thorough annual risk assessment, which is also necessary to satisfy governance and compliance requirements for ISO27001, HIPAA, and Meaningful Use Stage 3.

A risk assessment can be conducted by an internal or external security team and should assess:

- **Types of Data Collected**
- **Sensitivity of the Data**
- **Where the Data is At Rest**
- **How it Moves Across the Network**
- **Prioritize According to the Probability and Impact**
- **Triage Risks Based on the Baseline of Acceptable Risk**

It should also include a vulnerability assessment and penetration testing to find forgotten data in test databases, and to find application and service interfaces that could leak sensitive data when under attack.

A comprehensive assessment will illuminate the potential risks an organization faces, but it also requires taking a holistic approach that examines administrative, physical, as well as technical safeguards. Each risk identified should be classified by probability of occurrence (high, medium, and low) and business impact (high, medium, and low). Examples of risks that must be considered include distributed denial of service (DDoS) attack, ransomware, and any others that can:

1. Suspend the availability of mission-critical healthcare data.
2. Call into question the integrity of mission-critical healthcare data.
The availability and integrity of healthcare data can be the difference between life and death, which is the best reason for critical consideration of all potential risks during the assessment process. Once a thorough risk assessment is complete, all high-impact/high-probability risks should be easily identified. Only at that point can educated decisions be made about the risks to be addressed in the first year of a multi-year security improvement initiative.

**THE HEALTHCARE SECURITY MATURITY MODEL**

Following the risk assessment, mapping out the security an organization has in place is the next step. However, understanding where your security solutions fall on the spectrum of baseline, enhanced, and advanced security is critical to understanding where future improvements will provide the highest return on investment (ROI).

**Data Breaches Security Maturity Model - Architecture**

![Data Breaches Security Maturity Model - Architecture](image)

<table>
<thead>
<tr>
<th>CLIENT</th>
<th>NETWORK</th>
<th>SERVER</th>
</tr>
</thead>
<tbody>
<tr>
<td>MFA with Walk AwayLock</td>
<td>Network DLP Protection</td>
<td>SIEM</td>
</tr>
<tr>
<td>MFA with Timeout</td>
<td>Network DLP Monitor/Capture</td>
<td>DB Activity Monitoring</td>
</tr>
<tr>
<td>SSD with Encryption</td>
<td>Email Gateway</td>
<td>Digital Forensics</td>
</tr>
<tr>
<td>Endpoint DLP</td>
<td>Web Gateway</td>
<td>SSD with Encryption</td>
</tr>
<tr>
<td>Endpoint Encryption</td>
<td>Firewall</td>
<td>Server/DB/Backup Encryption</td>
</tr>
<tr>
<td>Device Control</td>
<td>Access Control (single factor)</td>
<td></td>
</tr>
<tr>
<td>Anti-Malware</td>
<td>DLP Discovery</td>
<td></td>
</tr>
<tr>
<td>Secure Remote Administration</td>
<td>Policy Based File Encryption</td>
<td></td>
</tr>
<tr>
<td>Mobile Device Management</td>
<td>Anti-theft (locate, lock, wipe)</td>
<td></td>
</tr>
<tr>
<td>DLP Discovery</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device Control</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NETWORK SERVER</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SRC LEVELS</td>
<td>Baseline</td>
<td>Enhanced</td>
</tr>
</tbody>
</table>

*Source: Intel Security*

**ASSESSING YOUR SECURITY BREACH POSTURE**

The keystone of every security risk assessment comes when a healthcare organization maps the security solutions it has in place to the Healthcare Security Maturity Model. What many organizations may find is that they have a mix of baseline, enhanced, and advanced security technologies in place. The goal of the exercise, however, is to determine if your organization is more heavily weighted toward baseline, enhanced, or advanced on the security maturity model spectrum. Once that is known, it is far easier to identify the missing pieces in your defenses and leverage your risk assessment to close security gaps and move your organization to the next level of security maturity.

Again, this exercise should be viewed in the context of a multi-year approach to layering your security. When it is done in that manner, it enables an organization to focus on the largest security issues identified in each annual assessment, and to implement missing technologies that best address those issues. In that way, your organization...
Healthcare Data Breaches: Continual Security Improvement as a Path to Lower Risk

will be able to measure year-over-year progress that clearly shows incremental improvements against an evolving threat landscape. It will also ensure new security investments provide the biggest boost to governance and compliance efforts.

INTEL SECURITY PRODUCTS AND THE SECURITY MATURITY MODEL

Intel Security has a broad portfolio of software and hardware solutions that healthcare organizations can use to address every level of the security maturity model (Appendix section) and minimize end-user opportunities for workarounds. However, the strength of Intel Security solutions is that the sum equals more than the individual parts because of synergy between the technologies. This is crucial for the healthcare industry because it needs well-integrated, seamless, and easy-to-use security with a single dashboard to monitor the entire ecosystem. Tightly integrated security also eases the administrative burden on IT professionals combating multiple simultaneous attacks, which is a common strategy of experienced cybercriminals that steal PII and sell it to the highest bidder.

A prime example of the need for tightly integrated security can be seen in the renewed interest in data encryption after several high-profile healthcare data breaches. Although encryption is an excellent security measure to have at your disposal, end users at every level of the organization will avoid it if given a choice. This is because encryption in many implementations requires the user to remember to encrypt, requires additional passwords, and causes noticeable performance degradation on the endpoint.

The synergy of McAfee Complete Data Protection with Intel AES-NI changes the playing field for encryption in the healthcare industry. The power of the combined solution is that IT departments can centralize data policy management and enforce data protection policies across the organization with FIPS 140-2 and Common Criteria EAL2+ certified encryption, even on personally owned storage devices. In addition, it leverages hardware acceleration on the CPU to mitigate perceptible performance degradation while encrypting and decrypting data. Sidelining the performance penalty historically associated with encryption means that healthcare organizations now have a feasible way to encrypt sensitive data and mitigate breach risk.

WHY INTEL SECURITY GROUP?

When considering the large ecosystem of security solutions available to the healthcare industry today, CIOs and CFOs alike need a strong business case for investing in a complementary set of technologies from a single vendor. The fact is that justifying an investment in Intel Security technology isn’t a difficult exercise.

Intel is not only a trusted technology provider with chipsets at the heart of computing devices throughout the healthcare industry, it brings security down to the silicon that McAfee products actively leverage to further accelerate and harden your security defenses. Intel Security Group is a one-stop security shop with well-integrated security technology to improve your security posture against sophisticated malware used by cybercriminals targeting healthcare organizations. With bundled security solutions, including encryption acceleration, multifactor authentication (MFA) support, and a presence across the network and to the server, IT departments can achieve important cost reductions annually in terms of man hours needed to support a modern security infrastructure.
A WAIT-AND-SEE APPROACH TO SECURITY IS NOT AN OPTION FOR HEALTHCARE

As sensitive healthcare data continues to be successfully compromised across the healthcare industry spectrum, a wait-and-see approach to security is no longer an option. Governance initiatives that focus on risk reduction and regulations in nations around the world are focused on protecting sensitive EHR data, which makes security improvements an operational necessity. To begin on the path towards enhancing your security posture, take the Intel Healthcare Security Survey25 to get an overview of how secure your organization is. Knowing your security score and where your organization stands along the spectrum of baseline, enhanced, and advanced security is a positive first step prior to a formal risk assessment.

Intel Security Group is committed to healthcare-friendly security and is ready to help you understand your unique security score. It can also help with your risk assessment and answer questions about solutions that can improve your security posture and score. To learn more about governance and compliance, visit the HIPAA Help Center,26 your national Data Protection Authority (DPA – see the Appendix), and contact the Intel Security Group to learn about innovative solutions that can improve security in your organization.

APPENDIX

A Partial list of Data Protection Authorities (DPAs)

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Canada</td>
<td><a href="https://www.priv.gc.ca/">https://www.priv.gc.ca/</a></td>
</tr>
<tr>
<td>Israel</td>
<td><a href="http://www.justice.gov.il/MOJeng/default.htm">http://www.justice.gov.il/MOJeng/default.htm</a></td>
</tr>
<tr>
<td>Dubai</td>
<td><a href="http://www.difc.ae/data-protection">http://www.difc.ae/data-protection</a></td>
</tr>
<tr>
<td>Asia Pacific Privacy Authorities (including some Pacific Rim Latin American Nations)</td>
<td><a href="http://www.appaforum.org/members/">http://www.appaforum.org/members/</a></td>
</tr>
<tr>
<td>Argentina</td>
<td><a href="http://www.jus.gob.ar/datos-porsonales.aspx">http://www.jus.gob.ar/datos-porsonales.aspx</a></td>
</tr>
<tr>
<td>Uruguay</td>
<td><a href="http://www.datospersonales.gub.uy/">http://www.datospersonales.gub.uy/</a></td>
</tr>
</tbody>
</table>
### Mapping Intel Security Products to the Security Maturity Model

<table>
<thead>
<tr>
<th><strong>Maturity Level</strong></th>
<th><strong>Solution</strong></th>
<th><strong>McAfee &amp; Intel</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Advanced</strong></td>
<td>MFA with walk-away lock</td>
<td>Intel® Identity Protection Technology</td>
</tr>
<tr>
<td></td>
<td>Threat intelligence exchange</td>
<td>McAfee Threat Intelligence Exchange</td>
</tr>
<tr>
<td></td>
<td>SIEM</td>
<td>McAfee Security Information and Event Management (SIEM)</td>
</tr>
<tr>
<td></td>
<td>Digital forensics</td>
<td>McAfee Incident Response &amp; Forensics</td>
</tr>
<tr>
<td></td>
<td>DB activity monitoring</td>
<td>McAfee Database Activity Monitoring</td>
</tr>
<tr>
<td></td>
<td>SSD with Encryption</td>
<td>McAfee Complete Data Protection and Intel® Data Protection Technology with AES-NI and Secure Key</td>
</tr>
<tr>
<td></td>
<td>Network DLP prevention</td>
<td>McAfee DLP Prevent and Intel® Data Protection Technology with AES-NI and Secure Key</td>
</tr>
<tr>
<td></td>
<td>Policy based file encryption</td>
<td>McAfee Encryption for Files and Folders and Intel® Data Protection Technology with AES-NI and Secure Key</td>
</tr>
<tr>
<td></td>
<td>Secure remote administration</td>
<td>McAfee ePO Deep Command and Intel® Active Management Technology</td>
</tr>
<tr>
<td></td>
<td>MFA with timeout</td>
<td>McAfee One Time Password and Intel® Identity Protection Technology</td>
</tr>
<tr>
<td></td>
<td>Anti-theft; remote locate, lock, wipe</td>
<td>Intel® Data Protection Technology with AES-NI and Secure Key</td>
</tr>
<tr>
<td></td>
<td>Network DLP monitoring &amp; capture</td>
<td>McAfee DLP Monitor</td>
</tr>
<tr>
<td></td>
<td>Endpoint DLP</td>
<td>McAfee DLP Endpoint</td>
</tr>
<tr>
<td></td>
<td>SSD with encryption</td>
<td>McAfee Drive Encryption and Intel® Solid State Drives</td>
</tr>
<tr>
<td><strong>Baseline</strong></td>
<td>Web Gateway</td>
<td>McAfee Web Gateway</td>
</tr>
<tr>
<td></td>
<td>Email Gateway</td>
<td>McAfee Email Gateway</td>
</tr>
<tr>
<td></td>
<td>Firewall</td>
<td>McAfee Firewall Enterprise</td>
</tr>
<tr>
<td></td>
<td>User awareness training</td>
<td>McAfee Education Services</td>
</tr>
<tr>
<td></td>
<td>Single factor access control</td>
<td>---</td>
</tr>
<tr>
<td></td>
<td>Anti-malware</td>
<td>McAfee VirusScan Enterprise</td>
</tr>
<tr>
<td></td>
<td>Device control</td>
<td>McAfee Device Control</td>
</tr>
<tr>
<td></td>
<td>DLP discovery</td>
<td>McAfee DLP Discover</td>
</tr>
<tr>
<td></td>
<td>Pen Testing/ vulnerability scanning</td>
<td>McAfee Foundstone Professional Services</td>
</tr>
<tr>
<td></td>
<td>Mobile device management</td>
<td>McAfee Enterprise Mobility Management</td>
</tr>
<tr>
<td></td>
<td>Endpoint encryption</td>
<td>McAfee Complete Data Protection and Intel® Data Protection Technology with AES-NI and Secure Key</td>
</tr>
</tbody>
</table>
ENDNOTES

4. Ponemon Institute. “Per capita cost by industry classification.”
6. Frost & Sullivan. “Remediation Time Following a System or Data Compromise.”
8. Ibid.
10. Heating, Ventilation, and Air Conditioning
   http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/
   http://www.healthcareinfosecurity.com/ucla-health-system-fined-865000-a-3826
13. Ponemon Institute. “What was the root cause of the healthcare organizations’ data breach?”
    February 2012, pages 55-57.
22. One classic example of multiple simultaneous attacks is a front-end DDoS attack paired with a back-end spear phishing attack.
Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today’s market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?

For information regarding permission, write:
Frost & Sullivan
331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041