Foliage
Developing products with a difference

A Foliage Article

As seen in

MD+DI MEDICAL DEVICE AND DIAGNOSTIC INDUSTRY

Securing Today's Healthcare Enterprise Systems

Time to Rethink Your Cybersecurity Strategy

Adam Hesse – Foliage, Inc.
Published June 26, 2015

Anyone following today's headlines is aware that cyberattacks represent a very serious threat to virtually every business sector. Even the largest enterprises are susceptible to cyberattacks that result in not only data breaches, but also data corruption and the introduction of destructive viruses. Still, the numbers may surprise you. According to IBM, companies are attacked an average of 16,856 times per year, with many resulting in a quantifiable data breach.1 The cost of an average breach? Around $3.5 million in US dollars in 2014, which is 15% more than the previous year.2

The most recent casualties of cyberattacks—Target, Home Depot, Anthem, and Premera Blue Cross—highlight not only the vulnerability of business entities, but also the reality that security is only as effective as the weakest point in an organization's perimeter. In fact, security concerns are so integral to software systems today that they shouldn't be considered as 'afterthoughts' or separate components.

The healthcare sector has particularly acute pains relative to security due to the sensitive nature of protected health information (PHI). And, ensuring tight security for a sector as sensitive to information, quality and controls as healthcare is extremely challenging. Facing this head on, the manufacturers of medical devices and systems must consider:

- How do they ensure that security is a consideration of the system architecture from the very beginning?
- What constitutes a cybersecurity evaluation and can they do it on their own?
- What is the right level of investment for cybersecurity?
- How can they identify the specific threats relative to their system?

Today's Healthcare Ecosystem

Generally, the challenge of security is directly related to the level of complexity and volume of interactions that devices or systems must handle. A completely closed system (e.g.,Fort Knox) is comparatively easy to protect. An open, accessible venue (e.g., New

A Foliage Article

York's Central Park) can be very difficult to protect. Healthcare IT systems are more akin to Central Park than Fort Knox.

Today's healthcare ecosystem is a large-scale complex distributed system made up of devices, software systems, users and suppliers. This ecosystem is becoming increasingly integrated with a larger dependence on extremely sophisticated software systems that in turn expand the network perimeter and make security much more challenging. And at the same time, many new security vulnerabilities and points of entry are increasing due to:

- More fully integrated technologies and processes of accountable care organizations (ACOs), health information exchanges (HIEs), providers and payers
- Increased demand for patient empowerment portals and system accessibility
- Widespread adoption of "bring your own device" (BYOD) among caregivers
- Proliferation of wearable devices connected to networks and software systems

Simply put, the healthcare ecosystem has all the hallmarks of a very difficult environment to protect.

Prevention is No Walk in the Park

Security for today's distributed systems is extremely difficult given the current state of technology. And coupled with the frequency and sophistication of attacks, it's clear that strategies that may have worked in the past are insufficient to safeguard today's highly complex health IT systems. It's not just security. You have to split it apart. There are aspects of security that have to do with access. There are also aspects of security that have to do with resilience—how protected is the environment itself from some kind of corruption event? The HIPAA and PHI regulations in and of themselves are very complex.

The HIPAA security rule covering electronic Protected Health Information (ePHI)—although familiar to systems developers—provides little specific guidance. It is possible to satisfy the Security Rule without addressing primary cybersecurity threats. HIPAA identifies 18 protected health information fields and general security controls, but not all fields are created equal and the controls must be applied based on the information that is being protected. After a cybersecurity attack, declaring compliance to the Security Rule will provide very little comfort to customers.

Yes, it is possible to develop solutions that significantly reduce the risk and the impact of a cyberattack. However, a fragmented approach to the application of security will not work. The overall architecture of the system must have security as a core design challenge. Healthcare enterprise systems, medical devices and mobile applications, for example, must all be viewed as part of an integrated system. Segmentation of data, controls, and levels of access control is important to having a highly resilient architecture so in the event of a penetration, the depth of the violation can be controlled. This is why a system level perspective is most effective.

A Foliage Article

Where to Start

Conducting a cybersecurity evaluation is a reasonable first step. However, this should be followed by an assessment by an independent third party. This relatively minor investment in an external audit is a small price to pay for a partner with the system level perspective and industry best practices this work requires.

A thorough review of the security strategy by a qualified partner with deep domain experience can reveal where the system under development is most vulnerable:

- Where do security threats reside?
- Which systems provide a level of access to sensitive data (and other systems)?
- Who has access to these systems including employees, patients, payers and vendors – are they properly trained?
- Where is the entire system – including their solution – most vulnerable to direct threats from inside and outside?
- How is off-the-shelf (OTS) software implemented, used and updated within firewalls?

After completion of the assessment, it is important to understand the three elements essential to establishing the appropriate investment in a security strategy—cost, risk and usability.

The Cost, Risk and Usability Framework

A proper risk analysis is necessary to "right size" the solution along the cost and usability spectrums. For example, adding too many security controls may decrease the usability of a system. But investments in security must be guided by risk, and without a risk assessment, it is difficult to identify the proper security controls. It is critical to the security strategy that cost, risk and usability are balanced.

Cost

The consumer fear and lasting damage that resulted from the attacks on Target, Home Depot, Anthem and Premera might suggest that cost is not an issue, but clearly that is never the case. The truth is any incremental investment in security is worth it to avoid millions of dollars in fines and the publicized loss of customer confidence. Nevertheless it is important to identify the point of diminishing returns in security investments, and to ensure that investments are focused to secure the weakest or highest risk points in the system. Incremental investments that do not reduce risk profile are not a smart investment.

Risk

It is critical to evaluate the total risk that customers may face and how the new solution can minimize this risk level. There is no such thing as no risk. The acceptable risk level is defined by the customer. It is important to assess whether or not the new solution is

meeting or exceeding that level. Variables that can influence an organization's risk level are the type of data and how much is to be stored.

For example, if one develops a system that holds a list of pharmacy prescriptions that include a prescription number and pharmacy ID, but not patient name or demographics, a breach is still a loss of data. The prescription numbers are only useful if they can be connected to a patient record in the individual pharmacy systems. The same information that includes patient names is a much higher risk.

Usability

It is also important to identify operations and technical safeguards that do not prohibit end users' ability to operate, but still reduce risk to acceptable levels. Security cannot limit the ability of clinicians to provide care. For example, does the technology ensure that clinicians can always access the data they need to provide care, even if they forget their password? Connected devices inside and outside the hospital represent points where cybersecurity overlaps with patient risk. Any tampering or corruption of this information could result in patient injury or death.

Risk Versus Reward in Security Investment

In 2014, healthcare organizations reported 278 data breaches compared to 197 in 2010.3 The number of cyberattacks is growing at an alarming rate, and it's time to recognize that attacks are not limited to large consumer-facing organizations and household brand names. Today's rapidly evolving healthcare ecosystem with its complex network of interconnected systems and devices—collecting and sharing massive amounts of data across vast networks, devices and stakeholders—is highly susceptible to cyberattacks.

As a primary stakeholder in this ecosystem, healthcare enterprise solution providers are faced with developing solutions that fit into their customer's larger technology infrastructure in a way that does not disrupt its security efforts, but provides tighter security against the threat of cyberattacks. Developing solutions that significantly reduce the risk and the impact of a cyberattack must be informed by a holistic assessment that identifies and prioritizes individual threats.

A comprehensive assessment of one's current security strategy can identify where security is in the overall architecture of the system. Working with a partner with both medical domain experience and a system level perspective will quickly identify gaps and risks in the strategy. From this vantage point, the next steps are easier. The decisions on where and how much to invest in cybersecurity will be more straightforward using a framework that balances cost, risk and usability. An iron-clad front door is not useful if the backdoor is left unlocked.

[1] IBM Security Services, "The 2014 IBM Cyber Security Intelligence Index," April 2014.

[2] Ponemon Institute, "2014 Cost of Data Breach: Global Analysis," May 2014.

A Foliage Article

[3] Telegraph-Forum, “Health Data Breaches Rise, but Fines Rare,” Jessie Balmert, Gannett Ohio, March 16, 2015.

As Technical Director, Adam engages with clients on strategic initiatives–from next generation architectures to process improvements. He has over 12 years of experience in software development, technical leadership, and product marketing. Adam’s focus during his career has been medical devices, imaging systems and semiconductor capital equipment. He holds a Bachelor of Science in Computer Science from the University of Minnesota. Contact Adam at ahesse@foliage.com