Microsoft

Secure Software Trends in Healthcare

How the Microsoft Security Development Lifecycle is helping to protect confidential healthcare information

Secure Software Trends in Healthcare

Microsoft

Table of contents

Microsoft

Introduction

In 2008, Dartmouth College professor Eric Johnson and a team of researchers at the school's Center for Digital Strategies discovered the kind of technical sophistication it takes to expose 20,000 electronic healthcare records.

None.

"It would get emailed or put onto a shared drive. It wasn't even password-protected, let alone encrypted," said Johnson, then the Center's director. "These records were just sitting out there. They didn't require any hacking at all."

The Center - which studies enterprise technology across a range of industries - was exploring weaknesses in electronic healthcare record (EHR) protection methods. Although they documented many leaks, in one particularly egregious incident they found a simple, non-access-protected Microsoft Excel spreadsheet with the names of 20,000 patients and 81 rows of information about each one, including Social Security numbers and diagnoses, all readily available to anyone who was logged on to the company's network.

Patient healthcare records are moving online fast, and they include all manner of sensitive personal data that must be kept safe. But in too many cases, these records aren't protected at all.

It's not that the industry is complacent, Johnson said. It's that its priorities in many ways conflict with data security. Healthcare records must be accessible to a vast number of people and organizations, even for routine patient encounters. And any potential solution cannot slow the delivery of actual healthcare.

"I think there is a culture of privacy in healthcare, but there is not so much concern for security," he said. "And, quite frankly, what do patients really value? When you go to a hospital you are not very concerned about protecting your data. When you're on a stretcher, the last thing on your mind is identity theft."

Even as day-to-day routines have moved online, the nation's massive healthcare sector - which employs one of every eight Americans, according to the Georgetown University Center for Education and the Workforce - has lagged. Healthcare providers are just beginning to use the Internet to computerize, store, and share vast troves of healthcare-related data.

But industry stakeholders that include the government, healthcare providers, and vendors see promise that electronic healthcare records and other cloud-based platforms can improve healthcare in the U.S. Indeed, EHRs were a centerpiece of the White House's 2009 economic stimulus bill—the American Recovery and Reinvestment Act—with hefty incentives for healthcare providers to make the transition.

Healthcare providers and vendors agree that they face a fundamental problem: how to provide the right level of security for EHRs. Not only do records themselves need to be secured, but so do the applications and platforms that access them.

As the healthcare industry struggles to figure out how to implement appropriate security measures, the principles of secure application development are slowly getting the attention of those who are tasked with solving this vast problem. A mix of industry analysts and watchdogs as well as organizations that face strict new legal requirements to secure patient data are advocating for an emphasis on standards in an effort to build a security culture within the industry.

"Healthcare security is at least 10 years behind most other industries," Johnson said.

Bringing secure application development to the healthcare industry

As the world continues to transition to the digital age, the complex and sprawling healthcare industry has serious security problems. In a $2.7 trillion industry, Johnson said that by most estimates roughly three to five percent of U.S. healthcare dollars spent are lost to fraud.

Experts believe that cloud-based healthcare portals and applications may actually reduce the risk of data breaches by moving patient information away from notoriously unsecure platforms such as email. Well-established Fortune 1000 healthcare vendors such as San Francisco-based McKesson Corporation and Dublin, Ohio-based Cardinal Health are beginning to take steps to give providers the ability do things such as collect and share vital medical records to manage billing.

Speaking at the CloudBeat 2012 conference on cloud computing in Redwood City, California., Mike Kelly, chief information officer for McKesson Specialty Care Solutions, said his organization is cognizant of the risk it faces rolling out cloud-based applications for patient data. This statement makes him one of the few healthcare technology executives to comment publicly on the subject.

“One of the things that's tricky for us in this industry about the cloud is the confidentiality associated with this data,” he said in a panel discussion. “And the limitations of liability that go along with that, especially as you start talking about patient records.”

Redmond, Washington-based software developer Microsoft faces similar challenges in its own EHR electronic health data platform, branded as HealthVault. For roughly the last decade, the company has been developing data-management products for healthcare. Company executives say they have been aggressive about employing secure development principles in their healthcare offerings from the very beginning, including the tenets of the Microsoft Security Development Lifecycle[1]. Microsoft uses this step-by-step process internally and freely shares it with organizations that want to incorporate security into applications from conception to release and beyond.

Sean Nolan, who holds the title of Distinguished Engineer at Microsoft and chief software architect for Microsoft HealthVault, describes the health data service as a cloud-based information hub, controlled and managed by individuals. The platform allows people to collect their personal health records on the Internet and control access to healthcare applications, providers, and data sources they choose.

Microsoft’s efforts deploying the SDL in its HealthVault offering may offer one model for the future of security in digital healthcare. According to Nolan, the core principles of threat modeling, risk analysis, secure testing, and deployment were used from the earliest days of building HealthVault. At first glance, the security problems it faced were similar to security issues faced on any network**:** developers were charged with anticipating problems, limiting the damage if there was a breach, and continuing to test as conditions evolve. But to apply those precepts in the policy-rich environment of healthcare, Nolan said that Microsoft had to focus on managing how the network connected to outside apps.

[1] www.microsoft.com/sdl

"We're trying to be truly transparent by showing the privacy policy," Nolan said. "It's simple for a database guy, but complicated for laypeople."

The level of complexity specific to healthcare applications is not the only challenge to securing EHRs, outside security consultants say. Greg Porter is a Pittsburgh-based information security consultant who created a curriculum on healthcare security as an adjunct faculty member at Carnegie Mellon University. He said that in addition to sophisticated application security that protects the integrity of software, the principles of basic network security—hardware access control, stout firewalls, and file and directory administration—are also scarce in the industry.

"We've tested EHRs," Porter said, "Where we've gained root access to the system through something as simple as a misconfigured password." Essentially, this vulnerability boiled down to default password settings from the manufacturer that were left unchanged.

"Once we got in, we could have changed anything," he said.

Porter describes cases in which mandatory healthcare information security officers — required by the Health Insurance Portability and Accountability Act (HIPAA) and the Healthcare Information Technology for Economic and Clinical Health Act (HITECH) — have been drafted from the ranks of administrative or nursing staffs and may have little to no formal security training.

Implementing some kind of standard—as Microsoft does with the SDL in its HealthVault offering—in many cases will be critical in the effort to secure the healthcare information ecosystem, Porter said.

But in many cases, those responsible for protecting healthcare information aren't aware that such security frameworks exist, he said.

In addition to the Microsoft SDL, the National Institute of Standards and Technology (NIST) offers a lightweight risk guidance frameworks known as NIST 800-30 and the HIPAA Security Rule Toolkit. The Frisco, Texas-based Health Information Trust Alliance offers a Common Security Framework dubbed HITRUST in the industry, to unify the many security approaches on the market and focus them on medical environments.

But even these standards are limited if not actively deployed, said Porter.

The case for secure application development in healthcare

Industry participants say increased awareness of application security is a direct result of high-profile problems the healthcare sector has had securing its data, combined with the onset of strict new regulations. As of 2013, under new rules from the US Department of Health and Human Services, the responsibility for securing patient data falls not just on healthcare providers, but on business associates who touch patient data. This includes contractors and service providers that provision e-prescribing gateways and EHRs. All now face stiff federal penalties for security breaches.

These new rules are the most sweeping changes to occur since HIPAA became law in 1996. They require more breaches of unsecured health information to be reported to the government and they increase the maximum penalty for negligence to $1.5 million per violation.

Denver-based IT security firm Accuvant is one company that has successfully employed secure application development in the healthcare industry. As a vendor to established healthcare organizations, Accuvant has used the Microsoft SDL extensively in its security practice, which includes assessing the security of software development lifecycles.

Without adopting proper security standards, "You have a real possibility of being found not in compliance with HIPAA and HITECH," said Phil Brass, a software security practice manager at Accuvant, "and paying lots of money until you get right again."

In making its evaluations, Accuvant uses the principles outlined in the Microsoft SDL. The process-based approach addresses not only software security, but also broader infrastructure design. A draft memo, created by Accuvant and submitted to several companies within the healthcare industry, outlines how the SDL will be deployed in a massive, integrated operation.

The process includes threat modeling, setting benchmarks for security and privacy, identifying common risks, selecting software assessment tools, and training employees in the principles of application security.

Accuvant feels that the Microsoft SDL provides large organizations with a coherent way to adapt their culture to one that is focused on security. McKesson, for example, is 14th on the iconic Fortune 500 list of the nation's biggest companies, with a sprawling infrastructure encompassing numerous business divisions and services. Cardinal Health is not far behind, ranked 21st on Fortune's list.

"A good comparison is the federal government, or maybe the state of California," said Robi Papp, a former global account manager at Accuvant, currently employed at Cupertino, California-based endpoint security firm Bromium. "It's not disjointed, but there are a lot of different initiatives happening across business units."

Wherever a business fits into a large federated organization, the fundamental principles are the same. They're also easy to understand and similar in application across a wide range of products. And, in the end, secure application development is a worthy investment for organizations in the healthcare industry of any size.

"We work with 30 or 40 different organizations," said Jon Bock, application security practice director at Accuvant. "We use it so we can have central standard. That's what the SDL is really good at. It creates a psychology of best practices"

Microsoft

Making the healthcare ecosystem secure

Secure application development is critical to organizations who seek to open up the potential of EHR data. Healthcare providers obviously stand to benefit from cost-savings and efficiency gained, but third-party application developers stand to benefit as well. The healthcare market is seeing a boom in consumer healthcare applications, including smartphone apps for monitoring health and fitness plans as well as connected healthcare devices such as scales and blood pressure monitors than can feed data collected at home to healthcare providers.

Microsoft's Nolan said that developers should not take the risk of allowing outside entities access to healthcare data without creating a secure ecosystem first. The SDL has proven useful for this, Nolan said, because it forces developers to think deeply about the ways in which they hand off responsibility for healthcare data.

"Giving any freedom of data to the app developers has proven to be a bad bet," Nolan said. "They tend to use laughable back-end security practices, like building behind firewalls. If you look at 90 percent of apps operating behind firewalls, if you can break the network, you're home free."

In the case of HealthVault, putting out an SDL-compliant product meant making the software development kit as secure as possible before making it available to third parties. For HealthVault, the bulk of the work went toward developing the handoff screen, where a doctor or entity accepts responsibility for the data transmitted.

But in general, Nolan said, the benefit of the SDL is in knowing that your bases are covered if you are following the steps, because the process is secure—even in a complex industry such as healthcare.

"From a software creation viewpoint, it basically supersedes most requirements I've had to face," Nolan said. "The SDL is more about your process, less about operations."

Security consultant Porter said that, no matter what security tools are deployed, software developers should seek to anticipate risks before they happen. A simple risk analysis followed by mitigating actions can save enormous sums of money compared with the cost of fixing problems after there is a breach.

"If you have a good process in place, you can identify what the risks are beforehand and then take steps to mitigate those risks," Porter said. "Everyone needs to be proactive."

Looking ahead

As healthcare continues to change, the need for security is only going to increase along with the need for a systematic way to approach it. It's likely that providers, consumers, and regulators will increasingly demand that organizations guarantee that EHRs will be protected.

Implementing secure application development is one way to meet the need for security, and it is how Accuvant has pitched it to companies in the healthcare space, Papp said.

"Application security will become a competitive differentiator in the marketplace. They're putting programs in place," he said. "In the near future you will need to have certain things to play ball."

In a video briefing to Forbes magazine in June 2012, Randy Spratt, McKesson's joint CIO and CTO, predicted that as healthcare evolves, the information available will become more sophisticated in the ways it is used to prevent fraud and abuse, reduce administrative costs, and manage healthcare for individuals and communities.

"It will require access to information at a very different level than we have it today," he said. "How do we bring this information together from all of the different places it lives, be able to exchange it effectively, and put it to new use that today simply can't be had?"

One thing seems certain: Secure application development will be part of the answer.

Microsoft

Data breaches, HIPAA, and hacking

A look at the US Department of Health and Human Services Breach Reporting Database

Robert Y Oikawa MD MPH CISSP CPPS CPHQ

The Final HIPAA Omnibus Security Rule announced in January 2013 provides stronger privacy protection for patients and strengthens the ability of the Office of Civil Rights (OCR) to enforce the HIPAA security and privacy regulations. It broadens the definition of a business associate and makes business associates that receive or process protected health information (PHI) and their subcontractors directly accountable to the OCR, including civil penalties up to $1.5 million per year per violation. The rule went into effect on March 26, 2013, and everyone must comply with its provisions after September 23, 2013.

> "This final omnibus rule marks the most sweeping changes to the HIPAA Privacy and Security Rules since they were first implemented," said HHS Office for Civil Rights Director Leon Rodriguez. "These changes not only greatly enhance a patient's privacy rights and protections, but also strengthen the ability of my office to vigorously enforce the HIPAA privacy and security protections, regardless of whether the information is being held by a health plan, a health care provider, or one of their business associates." (HHS Press release 1/17/13)2

The Final Omnibus Rule, along with the launch of the OCR's audit program, clearly signals an important change in the landscape for healthcare organizations, and should be a wake-up call to the industry as it moves forward with automation. To better understand where to focus our efforts in securing healthcare information systems, let's begin with looking at what we know already about healthcare data breaches from the OCR's records.

HIPAA-HITECH requires covered organizations to report all breaches involving PHI. HHS publishes a list of confirmed breaches affecting 500 or more individuals, including the name of the organization involved, size the breach and date, location of breached data, and the way that the breach occurred. The website containing this list is aptly called the "CMS Wall of Shame."

Since the start of the breach reporting program in September 2009 through December 2012, the OCR website lists 543 breaches affecting 500 or more individuals for a total of 21.5 million affected individuals. The median number of individuals affected per "large" breach was 2113 and the largest single breach affected 4.9 million individuals. The OCR also investigates breaches affecting fewer than 500 individuals, but does not make the details publically available on these "small" breaches. Likewise, information from the OCR Audit Program also remains confidential. Between September 2009 through April 15, 2013, OCR has received reports on 78,000 "small" incidents. Breach report numbers are expected to increase significantly as the updated Omnibus HIPAA Security Rule provisions enter into effect, and as the OCR Audit Program ramps up.

The HHS-OCR "large" breach reporting database can help us visualize the size of the health data breach problem. HHS classifies each breach by the location and the type of threat. Figure 1 shows how breaches size up by the location of the breached data. Paper records were involved in 24% of the breaches, but affected only 3% of individuals. Laptops were the most common location for an electronic data breach (29%), but affected only 11% of individuals. Other portable electronic devices (OPEDs), including cell phones, tablets, and

[2] US Department of Health and Human Services, HHS Press Office, Press Release, January 17, 2013. New rule protects patient privacy, secures health information. www.hhs.gov/news/press/2013pres/01/20130117b.html

external storage such as USB drives were less frequently involved (15%), along with generic computers (not otherwise classified as laptops, desktops, or servers) (15%), and network servers (11%).

EHRs were involved in only 13 events (2% of breaches) but affected a disproportionately large number of individuals (2.6 million 12% of total). Backup storage or tapes were rarely involved (1%), but these breaches affected extremely large numbers of individuals (29%).

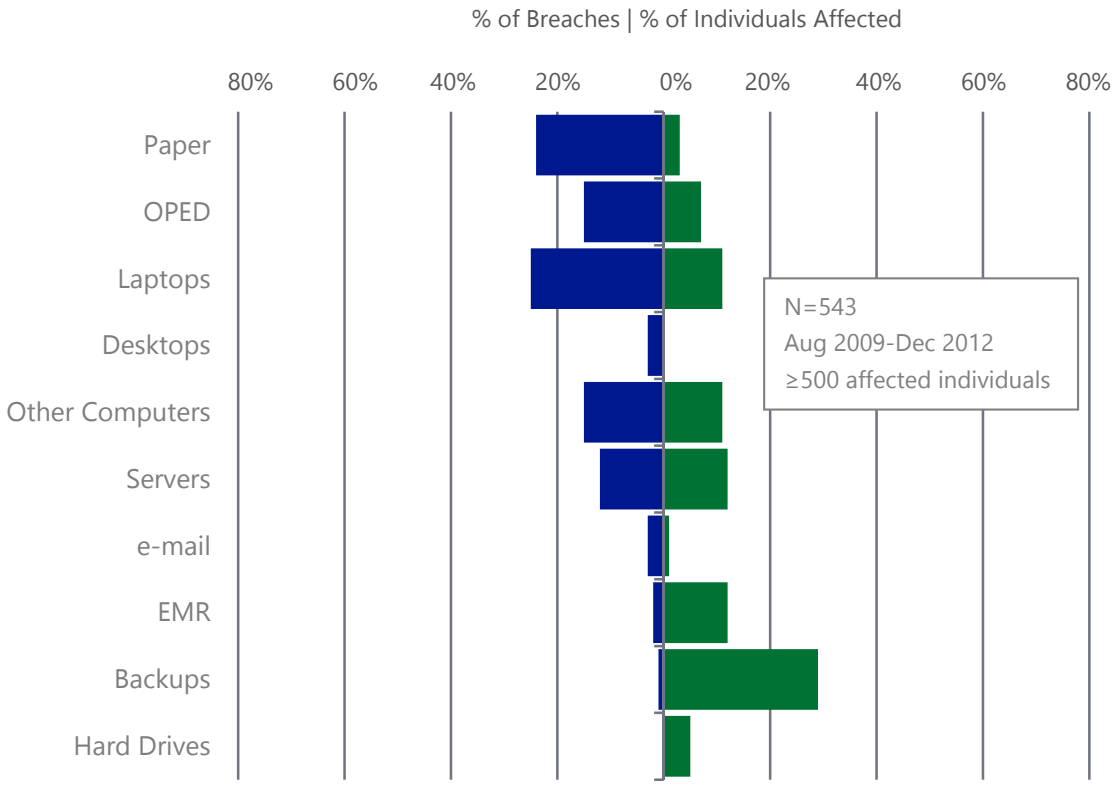
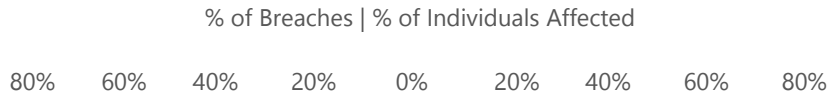


Figure 1. DHHS "Large" Breaches by Location of Data

Figure 2 shows how breaches sized up by the type of threat. Theft was the most common cause (56%), affecting 40% of individuals, followed by Unauthorized Access and Disclosure (UAD), and Loss. Hacking or IT incidents (HITI) were relatively uncommon (8%), followed by Improper Disposal (ID) (5%). Breaches in which a specific threat could not be identified were classified as Unknown. While uncommon (2%), events with an Unknown cause involved a disproportionately large number of individuals (2.2 million or 10% of individuals affected).



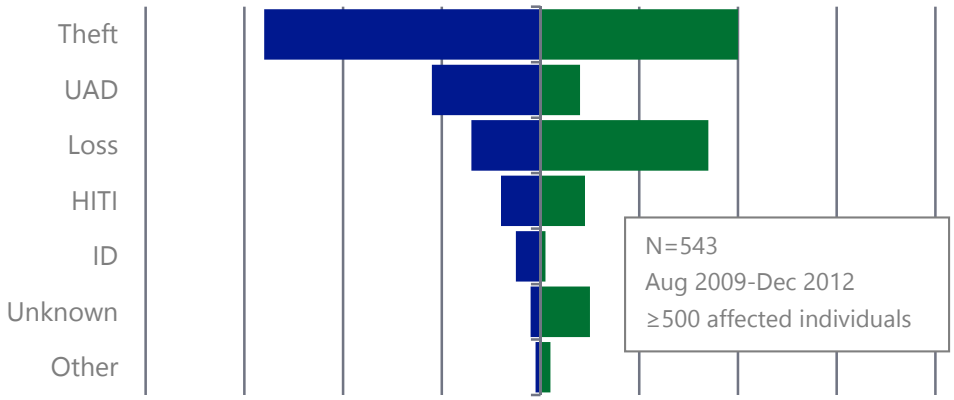


Figure 2. DHHS "Large" Breaches by Threat Classification

HHS does not give a precise definition for "Hacking and IT Incidents." Reporting organizations must choose a class based on the nature of the incident. Intuitively, HITI events include deliberate internal or external technology based attacks as well as inadvertent errors in the operation of computers, describing a breach in terms of a mechanism of attack. UAD, on the other hand, describes a breach in terms of its functional outcome (disclosure). The choice may result from the depth of analysis and perspective of the individual filling out the report. Investigations focused on establishing individual accountability may stop at functional outcome (UAD), but deeper, root cause investigation may lead to HITI, and even deeper investigation may point to systemic, organizational and policy weaknesses.

Although the overall frequency of reported breaches gradually fell over the past 3 years, the incidence of HITI-related breaches has remained constant, hovering around 1 event per month (Figure 3).

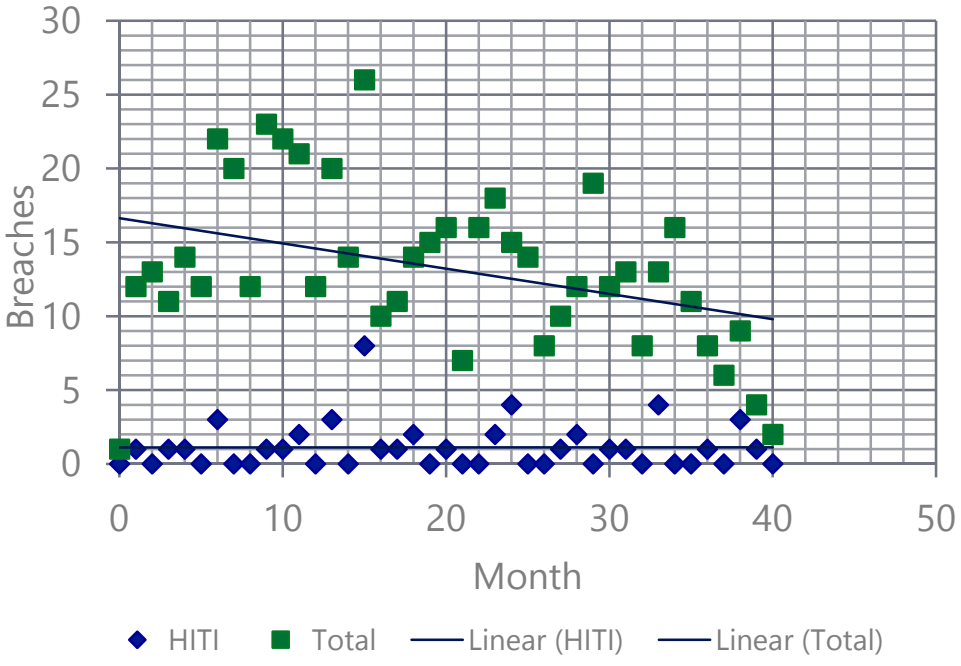


Figure 3. Time Trend HITI and All Breaches

The HHS-OCR data shows that HITI incidents (lower line) are not following the same downward trend seen for breaches in general (upper line), an observation which should increase our level of attention, and prompt us to ask the question "Why *not*?"

It's also important to keep perspective on the absolute size of the problem, and not focus only on percentages. Even though they represented only 8% of all breaches, HITI affected over 1.8 million individuals from August 2009 through December 2012. This is equivalent to every resident of the cities of Seattle, Boston and Washington D.C. combined (Figure 4).

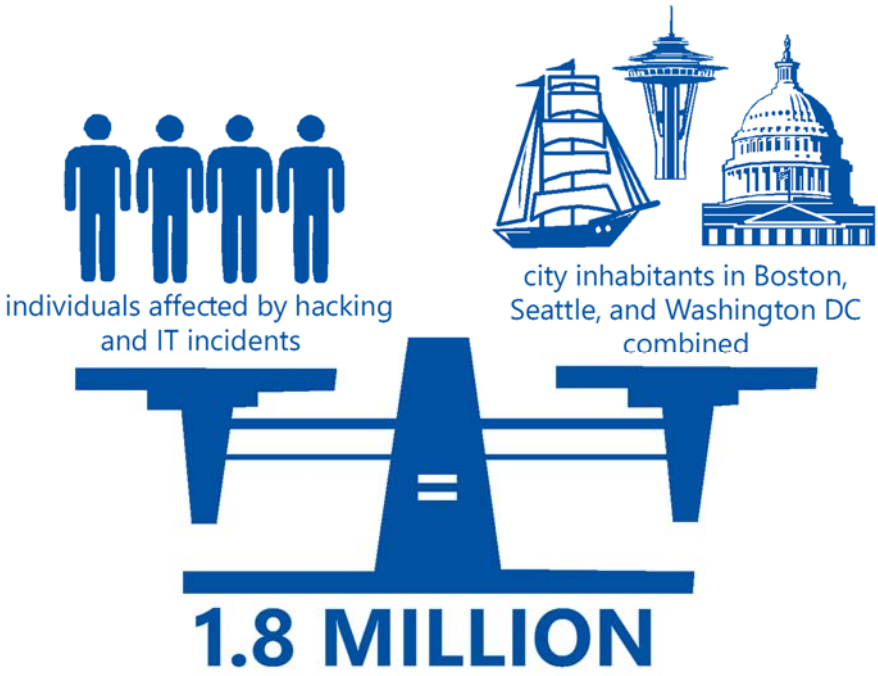


Figure 4. Impact of Hacking & IT Incidents – August 2009 through December 2012

It's even possible that the 46 reported HITI breaches are an underestimate; a recent 2012 report by the Ponemon Institute showed that over half (54%) of 80 surveyed healthcare organizations had little or no confidence that they could detect all patient data loss or theft.[3] If the breaches of Unknown cause were actually due to HITI, then the total could be as high as 4.8 million affected individuals, more than the population of the entire Boston-Cambridge-Newton area (4.6 million), the San Francisco-Oakland-Hayward area (4.5 million), or the combined population of the cities of Philadelphia and Chicago (4.2 million.

HITI is clearly a big problem and the historical trend suggests that attempting to address it is challenging. One explanation offered for this is that the HITI incidents represent the basic "background noise" of human errors accumulating through the full lifecycle of IT design, development, integration, and operation. Another reason that HITI rates may have apparently remained constant while the rates for other classes of threats were evidently falling is that malicious individuals are motivated to exploit vulnerabilities in the face of tougher policies, safeguards, and controls at a level of activity that provides sufficient reward to offset the risk of being caught. Certainly the continuing evolution of attacks from simple scripts to coordinated multi-prong threats shows that attackers adapt their methods to deal with the increasing security controls and safeguards in the financial services and manufacturing sectors.

[3] Ponemon Institute. Third Annual Benchmark Study on Patient Privacy & Data Security, Sponsored by ID Experts and Independently Conducted by Ponemon Institute LLC, December 2012.

Microsoft

What we can do

So what can we do about these problems? How can software developers address the theft and loss problems, which seem to lie in the far-off realms of physical security and human behavior? And what, specifically, can they do to address the HITI threat in their own domain?

Notably, the revised Omnibus HIPAA Security Rule introduced a "safe harbor" provision for lost or stolen devices. If an organization encrypts PHI, rendering into a form that is "unusable, unreadable or indecipherable to Unauthorized Individuals," then there is no breach reporting requirement.[4] By building applications with encryption and other security safeguards, software developers can help enable organizations to reduce the risks that stolen devices or HITI incidents will result in breaches of unencrypted data, and thereby help such organizations earn the protection of the safe harbor provision..

How SDL can help

While it's easy to say "encrypt everything and you'll be fine," the real challenge is actually delivering software with effective encryption and security safeguards. To be successful with encryption, or with any other techniques intended to improve the security of software products, it's necessary to use a systematic and end-to-end process.

SDL is an example of a process innovation that can have a huge impact on healthcare security. By providing a firm foundation and proven approach for designing security into software from its inception, products and solutions can be delivered to the market that can better resist HITI threats and help organizations encrypt their data to guard against theft or loss of computers, mobile devices, and storage media. SDL is a collection of proven practices integrated into a comprehensive process that extends across the full system lifecycle. Table 1 shows how using SDL practices[5] can help address the top threats identified in the HHS-OCR database.

[4] HIPAA Final Security Rule, Feb 2013, p 316.

[5] Microsoft Corporation, Simplified Implementation of the Microsoft SDL, March 2, 2011 [Internet] Available via www.microsoft.com/en-us/download/details.aspx?id=12379 [Accessed April 19, 2013]

	HHS-OCR Threat Classification		
	Theft, Loss and Improper Disposal (ID)	Unauthorized Access or Disclosure (UAD)	Hacking and IT Incidents
Desired safeguards	Encryption	Access controls Logging and Auditing	-Reduce code vulnerabilities -Prompt patching -Reduce configuration and operation errors
SDL Practices[6]	Benefits of SDL		
1-Training	Ensures development team understands secure coding practices including encryption, key management, hazards of weak cryptography, risk management	Ensures development team understands secure coding practices, current threat environment, principle of least privilege, risk management	Ensures development team understands secure coding practices, current threat environment, lifecycle risk management, principle of least privilege
2-Security Requirements	Ensures the development team identifies, articulates, documents the specific security requirements, including encryption, least privilege, and use of secure defaults, as early as possible in the development process		
4-Security and Privacy Risk Assessment	Ensures development team has identified where threat models , security design reviews, penetration testing, fuzz testing will be needed to address security and privacy risk, including those needed for customer organizations to achieve and maintain compliance with the HIPAA regulations.		
5-Design Requirements	Ensures that the development team creates security and privacy design specifications, cryptographic design requirements, user authentication requirements, and validates them against both the functional specification and security requirements, including how to deploy and operate features and functions must be operated in a secure fashion that will enable customers to remain compliant with HIPAA.		
6-Attack surface reduction	Ensures that the development team shuts off or reduces access to services, applying the principle of least privilege.		
7-Threat modeling	Ensures that the development team has considered how well the design addresses the threats in the intended operating environment, including internal and external threats, inadvertent human errors, and physical loss or theft of devices and media.		
13-Threat model and Attack Surface review	Ensures that the actual implementation is still consistent with the requirements, and that new threats are being addressed as well.		
14-Incident Response Plan	Ensures that the team has a tested response plan for fixing vulnerabilities discovered after release.		

Table 1. Addressing Threats using a subset of Security Design Lifecycle (SDL) practices

So let's do the back-of-the-envelope math again: if adopting SDL practices could render *only 20%* of the electronic PHI being lost each year "unreadable or undecipherable to unauthorized individuals" and could reduce losses related to HITI, UAD, and ID by *only 20%* by reducing software vulnerabilities and effectively implementing the principle of least privilege, then there would be about *1.4 -1.5 million fewer individuals affected each year by a HIPAA privacy violation* involving e-PHI. That's very close to the number of people that live in the cities of Phoenix or Philadelphia. And with breach notification and remediation costs estimated to be as much as $200 per record, that could amount to $280 million annually that could be used to treat patients.

[6]Table is based on Simplified Implementation of the Microsoft SDL.

Microsoft

Summary

The HHS-OCR breach records show us that physical threats like theft and loss of devices and media are the main causes for data breaches. However, HITI have remained persistent and important causes for data breaches despite our best efforts to control them. The proper use of encryption is an attractive way to address theft, device or media loss, and improper disposal, and the use of secure development practices can help address HITI-related breaches and those UAD incidents which are facilitated by the lack of proper authentication, access controls, logging and audit, or failure to apply the principle of least privilege.

Microsoft's SDL is an example of an integrated framework of proven best practices for secure software development that can help developers build more secure software, and reduce the burden of healthcare data breaches significantly.