THE ITSUMMIT

Technology Executive Magazine

April, 2010

Defenders of the Realm

Steven Porter, CIO
Touchstone Behavioral Health

There are only two types of connected organizations: those who are currently remediating a security breach, and those who are actively under attack. The "script-kiddies" have grown up, and skills honed penetrating networks 10 years ago are now being used to harvest confidential data streams for financial gain. Buffer-overflows, remote code execution, phishing, pharming, worms and Trojan Horses are just a few of the exploits used to gain unauthorized entry into our networks, looking for information that can be sold to the highest bidder. When you consider that all of these tools can be automated to run from thousands of previously-compromised consumer computers 24/7, it is no wonder that the truly determined will eventually find their way in.

As "*Defenders of the Realm*", we counter these threats by locking down all but the most-essential services on our firewalls; installing intrusion prevention and detection devices; religiously patching our application, operating system, and anti-virus solutions – and fervently hoping that we've sufficiently hardened our perimeter that the marauders will move on to easier prey. Still, they come – wave after wave – probing our defenses, picking at the edges, trying to wriggle their way between the cracks of our overlapping layers of protection. As the attacks evolve, so do our responses. They intercept our wireless traffic, so we encrypt it. They add malicious code to websites we visit; we add malware inspection and behavior-based threat mitigation. As our users become mobile, we extended multi-layered protection out to the endpoint.

At the end of the day, we play to a draw and call ourselves HIPAA compliant.

Our "moat-and-castle" mentality has locked down data systems to a level of least-privilege, yet has ignored the human interface. As behavioral health providers, our caring, believing, skilled, and sometimes forgetful staff – the greatest single resource in our daily mission – also represents the single greatest threat to data security within our organizations. We install and maintain systems to minimize the inappropriate material that reaches their mailbox, encrypt confidential email, automate processes and procedures to update and secure software, and enforce policies that limit access to sensitive data. We teach users to question email claims that slip through our filters, not to open attachments they aren't expecting, and that not every statement on the Internet is factual. We devise and deliver awareness programs focusing on the dangers of social engineering. We show videos, post flyers, beg, plead, badger and cajole – all to protect them from themselves – but we still haven't addressed how to protect our data once it is out of our control.

For Information Technology, the devil is in the duality of our mission. We are tasked with providing both productivity tools and access to highly sensitive data in order to enhance the quality of care our clients receive. Laptops, wireless broadband Internet cards, and a secure, web-enabled EMR system add up to care-givers having access to charts regardless of their physical location. Tangible benefits include timely, accurate documentation, and a level of coordinated care previously unavailable in a geographically dispersed service environment. With each requisite form at their fingertips, administrative time is reduced, freeing staff to encounter more. From an IT perspective, what could possibly be more satisfying than knowing your technical solution allows each provider to see at least one additional client per week?

And therein resides the dilemma. Our *other* primary task is to protect the integrity of all electronic personally identifiable information, regardless of where it resides within our systems. How do we reconcile the simple fact that our intricately planned and exquisitely executed network defense offers no protection for data on a $3.00 thumb drive lost in the parking lot? Notes stored contrary to existing policy on a hard drive stolen from a parked car have more street value than the laptop itself. The same tools we so eagerly deploy, empowering our providers to work anywhere and anytime, are counterintuitive to the sanctity of our institutional grail. Office-bound workers with desktop computers are no more secure than their mobile counterparts. Records copied to portable media for use at other locations are just as vulnerable, and the machines themselves are prized targets during office burglaries. Our challenge is to walk the tightrope between usability and security, seeking a balance that will satisfy our regulatory obligations without creating an undue burden on our practitioners.

Closing the security loop requires that we protect data at rest, regardless of where it is stored. Encryption is an essential weapon in our arsenal – a last line of defense for data integrity, even in the most adverse conditions. Our business side needs to encourage and enable users to capture and store information under a wide variety of circumstances, even as our compliance side cringes at the thought of data in the wild. Users will exercise their creativity, particularly when it comes to transferring data between sites, so protection needs to extend beyond the physical disk to include any USB device as well as the CD/DVD drive. Eventually these devices will be misplaced or stolen. Once gone, we need assurance that the information they hold is still protected.

How We're Doing It

Security is a journey, not a destination. Each business decision made, every process implemented, guides an organization down the specific path that best serves their individual requirements. For Touchstone Behavioral Health, the die was cast when we opted for a hosted Electronic Medical Records system. The mobile solution we've adopted enhances our business model of providing service wherever our client is most comfortable, but carries its' own inherent risks. We leveraged our EMR launch to quietly evolve the agency's security culture toward an untethered workforce.

TBH is in the business of modifying behavior in others, but we don't necessarily embrace change ourselves. To the casual observer it may appear that we followed the path of *most* resistance – over a period of 30 days we deployed laptops to our care-givers, and mandated that all documentation and billing be performed in the new system. Underlying this wholesale transformation, however, is an iterative design for data integrity, enthusiastically supported by Management and coordinated across all departments. Without careful and thorough planning, the weeks following July 1st could have been an unmitigated disaster.

Pre-launch tasks revolved around getting back to basics – analyzing our current security stance and reaching consensus on where we needed to be. Human Resources, Quality Assurance and Information Technology reviewed and collaborated on updating policies regarding everything from acceptable use to passwords, keeping in mind that users would spend much of their time outside of our facilities. Impromptu groups were formed across the agency to find the proper balance between security and usability in the "real-world". Priorities established, available tools and existing processes were reworked to provide both reporting and enforcement, keeping with current and anticipated standards. Finally, the remaining requirements provided the basis for working with a number of vendors to find the perfect fit for the missing pieces of our Phase 1 deployment.

Early conversations included consideration for the implications of misplaced, lost, or stolen hardware. In accordance with HIPAA guidelines we performed a risk assessment, and concluded that mitigation would be cost-prohibitive for immediate implementation, but agreed to revisit the issue quarterly while investigating possible solutions. The administrative overhead of touching approximately 200 machines, spread from Flagstaff to Tucson, eliminated the machine-level offerings of our hardware and OS vendors. Device recovery systems provide some satisfaction in knowing that the hardware will disclose its' location and notify the authorities, but only once it has connected to the Internet… attractive, but there remains a level of vulnerability if the hard drive is slaved specifically to harvest data. We ultimately selected a partner who not only met our technical specifications (device-agnostic encryption with minimal machine overhead, no user intervention, and global administration capabilities), but also appreciates and supports our mission within the communities we serve.

None of this works without the underpinning of an ongoing and pervasive security awareness program. Our users didn't grow up wanting to be computer users, and they don't intuitively understand the security ramifications of surfing the web, responding to email, or even the risks associated with leaving a computer screen unattended. It is our duty to educate, ingrain, and reinforce our policies at every opportunity, yet in a manner that doesn't seem overbearing (on our laptops, Ctrl + Alt + ↓ will rotate the display 180 degrees – not enough to harm anything, but a great reminder to lock your machine before walking away). The road goes on forever… Phase 3 will be followed by Phase 4. Security is not a technology, nor is it an IT project – it is the foundation of our continued success.

Considerations

Like every other technology, encryption comes in flavors – full disk and file. Each has pros and cons, and there are multiple vendors to choose from on either side of the aisle. Still, there are a few universal factors, regardless of the direction that works best for you. In my experience, the most important consideration revolves around the end-user. Ideally, the solution has no apparent impact on their daily operations. There are no additional passwords to remember, no special locations to save to, and most importantly, no performance degradation. Nothing will kill a technology quicker than unhappy users.

Unless you have time to spare, the system also requires a central administration console to provide granular control over the enterprise. You need the ability to manage and modify accessibility at the user level, and a means to recover data at the admin level. "Phone home" capabilities provide an additional level of oversight, allowing you to modify policies regardless of whether the machine is attached to the local network.

Vendor selection is another key ingredient. You need a supplier who will take the time to understand your unique requirements, and work within your comfort zone. Make your selection carefully – you want a partner who will be there to support their product for years to come.

The third prong of the equation is fiscal responsibility. HIPAA says that we need to assess risk potential against the cost of mitigation, so I offer a couple of questions for your consideration. How likely are you to lose control of a device used to access or store sensitive data? How many clients are in your database, and how much will it cost to contact each of them? Finally, can your organization survive the adverse publicity, lack of consumer confidence, and potential litigation expenses? Ultimately, encryption is insurance against the inevitable.

Steve's credentials include: business major; boilermaker; TV producer; IT exec… He still hasn't decided what he wants to be when he grows up, but odds are he'll have a slightly different perspective on it. When playtime comes, look for him on the open road with the top down and the music up, or maybe pretending to play golf – cigar (and tongue) firmly in cheek.

Touchstone Behavioral Health, based in Phoenix, Arizona, is a national leader in providing positive outcome, evidence-based behavioral health services to youth and their families through prevention and outpatient therapy. Founded in 1968, Touchstone has four offices throughout Arizona. The agency was recognized in 2008 as a Computerworld Honors Program Laureate for the project "Secure EMR for Remote Providers".