Myths and Fallacies of Computer Security in Healthcare Environments

BY SEAN PEISERT, PH.D., LAWRENCE BERKELEY NATIONAL LABORATORY

The U.K. National Health Service (NHS), U.S. Office of Personnel Management (OPM), Experian, Sony, the Democratic National Committee, the Republican National Committee, the U.S. Department of Health and Human Services, Yahoo, Anthem, Premera Blue Cross, 21st Century Oncology, Banner Health.

Anyone reading this probably recognizes each of these organizations as a few of the dozens that have reported a cyber attack in recent years, such as ransomware or a database breach, and a few of the hundreds or thousands that have been the victim of damaging attacks but did not report it, and/or had one but failed to find one.

But why should I worry about security? Why would attackers target my organization? There are at least two answers: first, not all attacks are targeted. Malware can spread across the Internet and via devices such as USB sticks indiscriminately, and collateral damage can be high. Second, much like the proverbial story about the way to survive an encounter with a bear or shark being merely the ability to swim or run faster than the other people you're with, attackers may target your organization simply because you've made it easy for them.

If the more well-resourced cyber attackers in the world, such as nation states, wanted to attack your organization, they could likely find a way to do so successfully. In the same fashion, should tanks roll up to the front door of your organization, they could probably find a way to get inside. On the other hand, most cyber attacks are not the equivalent of tanks rolling up to your front doorstep, but are much more often the equivalent of street muggings. In any case, there is no reason organizations should make it easy for such attackers.

Thus, there are three vital tenets for healthcare board members to keep in mind about computer security:

1. Security *is* your organization's responsibility. You have a responsibility to your employees, your customers, and patients, and much as is the case with public health, to your "neighbors"—the other organizations you interact with.
2. The security situation is *not* hopeless.
3. There is no such thing as "perfect" security. Your organization will *not* prevent all attacks. Some will succeed. What your organization needs to do is figure out how to architect its security program so that, when attacks are successful, the damage is limited.

In this special section, we discuss common misconceptions about security, ways in which organizations can try to succeed, and what boards need to know about security.

Mitigation

Conventional Wisdom and Compliance

"To be secure, here's what you need to do: install a firewall; have your employees make strong passwords of at least 12 characters, composed of upper and lowercase letters, numbers, and symbols, and change their passwords every six months; pay for a security monitoring system; install anti-virus scanners on all your computers; and put your employees through annual security training."

This is the kind of advice one might expect to hear from a computer security consultant. Some of these things *might* help, but there is also good evidence that some of these things produce no value or may even be counter-productive. Consider recent advice from the Federal Trade Commission:

> "...there is a lot of evidence to suggest that users who are required to change their passwords frequently select weaker passwords to begin with, and then change them in predictable ways that attackers can guess easily. Unless there is reason to believe a password has been compromised or shared, requiring regular password changes may actually do more harm than good in some cases. (And even if a password

Key Board Takeaways

There is no such thing as "perfect" security—it is impossible to prevent all attacks. Healthcare organizations need to architect their security programs so that, when attacks are successful, the damage is limited and recovery is swift. Moreover, security is an ongoing, continuous effort. The following are some key issues and questions for board members to consider:

1. Merely following the herd by using so-called "best practices" is no longer defensible. "Compliance" with regulations (e.g., HIPAA and HITECH) is *not* the same thing as true "security."
2. Security staff should regularly analyze potential points of vulnerability. Often those most vulnerable points are employees' desktop computers. Could some workers complete their tasks using more secure devices such as those that run on Apple's iOS or Google's Chrome OS? In addition, scenario planning must be robust so that, in the event of a breach, steps can be taken immediately to identify and remedy the problem.
3. Questions for board members to ask the CIO and CISO include:
   - » Are we storing the right amount of data in order to make meaningful decisions and actions related to patient care, or are we storing data we are not using?
   - » Once we have looked at the data, how long do we need to keep historical data?
   - » Are we properly destroying old data that is no longer required?
4. Emphasize bi-directional communication between the people who make decisions about security (e.g., the CISO's team) and the rest of the organization. Security is everyone's responsibility.
5. If you are running your own servers and backups, ensure there are multiple tiers/locations of data storage, and consider expanding to cloud provider solutions.
6. Don't go it alone, but don't blindly rely on vendors or consultants and consider the job done. Seek out other organizations in your region that have strong security infrastructure, or are seeking solutions as well, and share strategies, best practices, and lessons learned. Consider the possibility of creating an alliance of organizations that can build a unified security infrastructure with shared resources.

has been compromised, changing the password may be ineffective, especially if other steps aren't taken to correct security problems.)"[1]

Others cite similar issues:

- "...None of the common recommendations that user passwords should be long, strong, contain certain characters, kept unique to each account, never written down, and changed regularly appears to be supported.... While numerous organizations give password guidance, none that we can find supports them with evidence of improved outcomes..."[2]
- "This week, Google security researcher Tavis Ormandy announced that he'd found numerous critical vulnerabilities in Symantec's entire suite of anti-virus products. That's 17 Symantec enterprise products in all, and eight Norton consumer and small-business products. The worst thing about Symantec's woes? They're just the latest in a long string of serious vulnerabilities uncovered in security software."[3]
- "Department of Defense data (cleared for release) shows on average one-third of vulnerabilities in government systems is in the security software."[4]

So, rotating passwords and installing security software may actually make your organization *more* vulnerable? It is important to note that proper authentication is *vital*, as is the use of certain types of security software. But what if the solution to malware isn't installing virus scanners, but in broadening the use of devices that are more "locked down" and less "open" than traditional desktop PCs? As an analogy, the solution to surviving a tornado may not be the world's fastest car that can outrun tornados, along with sensors that can provide

real-time wind speed, but rather may well be a traditional U.S. Midwestern basement.

Organizations looking to deploy more secure systems expect that attacks can and will occur. They develop systems that regularly identify the most valuable assets in the organization and potentially weak entry points, and assume that any system can and will be breached. In addition, organizations must regularly have scenario planning and exercises to identify what could happen in the event of a breach, and what actions can be taken to minimize damage and restore the system.

To that end, it should come as little surprise that security experts are finding that endpoints such as those based on Apple's iOS or Google's Chrome OS are often more secure[5] than endpoints running traditional desktop operating systems, such as Microsoft's Windows. Tim Cook, the CEO of Apple, has indicated that an iPad, not a Mac, is his primary work machine.[6] How many people who live in Microsoft Word, Excel, PowerPoint, and Outlook could instead do just fine with Chrome OS?[7] How many people who are doing primarily Internet research could similarly use a Chrome OS device or iPad? A question from the board to your organization's Chief Information Officer might be: could some of our workers complete their tasks using more secure devices such as those that run on Apple's iOS or Google's Chrome OS?

The answer to security training is similarly nuanced. Security training of employees *can* improve results.[8] However, "beyond a certain threshold, increasing demands [on users] are simply met with attempts to circumvent onerous procedures. The thresholds appear to have been long exceeded for most users."[9]

This critique is not to say that conventional wisdom should be stopped

1 Lorrie Cranor, "Time to Rethink Mandatory Password Changes," Federal Trade Commission, March 2, 2016 (www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes).

2 Cormac Herley, "Unfalsifiability of Security Claims," *Proceedings of the National Academy of Sciences,* Vol. 113, No. 23 (2016), pp. 6415–6420, available at www.pnas.org/content/113/23/6415.

3 Kim Zetter, "Symantec's Woes Expose the Antivirus Industry's Security Gaps," *Wired,* June 30, 2016, available at www.wired.com/2016/06/symantecs-woes-expose-antivirus-software-security-gaps/.

4 Mudge (Peter Zatko), "DoD data (cleared for release) shows on average 1/3 of vulns in government systems is in the security software," September 12, 2015 (twitter.com/dotmudge/status/642758829697056768?lang=en).

5 Rich Mogull, "Tidal Forces: The Trends Tearing Apart Security As We Know It," January 3, 2017 (https://securosis.com/blog/tidal-forces-the-trends-tearing-apart-security-as-we-know-it); and Rich Mogull, "Tidal Forces: Endpoints Are Different—More Secure, and Less Open," January 18, 2017 (https://securosis.com/blog/tidal-forces-endpoints-are-different-more-secure-and-less-open).

6 Jake Smith, "Tim Cook: 80 percent to 90 percent of my time is spent on an iPad, working and consuming," *9to5Mac,* February 14, 2012; Adrian Weckler, "Tim Cook: Apple won't create 'converged' MacBook and iPad," *Independent.ie*, November 15, 2015 (www.independent.ie/business/technology/tim-cook-apple-wont-create-converged-macbook-and-ipad-34201986.html).

7 Google Chromebooks (www.google.com/chromebook/).

8 Iacovos Kirlappos and M. Angela Sasse, "Security education against phishing: A modest proposal for a major rethink," *IEEE Security & Privacy*, Vol. 10, No. 2 (2012), pp. 24–32.

9 Adam Beautement, M. Angela Sasse, and Mike Wonham, "The Compliance Budget: Managing Security Behavior in Organizations," *Proceedings of the 2008 New Security Paradigms Workshop (NSPW),* September 2008, pp. 47–58; and Cormac Herley, "More is Not the Answer," *IEEE Security & Privacy,* Vol. 12, No. 1, 2014.

immediately. But at the same time, it is important to note that merely following the herd by using so-called "best practices" is no longer defensible. In addition, it is vital for board members to understand that "compliance" with regulations (e.g., HIPAA and HITECH) is *not* the same thing as true "security." Computer security is about defending against active and well-financed adversaries. Running a computer in a public environment today means the weather is *always* snow with a chance of tornados, and the roads are *always* covered in black ice.

The HIPAA Security Rule[10] underlies most of the techniques that are used in healthcare to protect patient health information (PHI). However, the HIPAA Security Rule itself is rather high-level and non-prescriptive. This is probably intentional, because the rule must apply equally to organizations of any size and capability and therefore must target the lowest common denominator. The guidance from the National Institute of Standards and Trust (NIST) on HIPAA[11] is significantly more detailed, but still out of reach of many organizations. On the flipside, DHHS's "Security Standards: Implementation for the Small Provider"[12] provides so little detail as to enable "small providers" to do little more than "check the box" about being in compliance with the HIPAA Security Rule, which, as we've discussed, is *not* the same thing as true security. Take note that being in compliance with the HIPAA Security Rule may help a medical organization in a federal audit, but it does nothing to help with the confidence of the public and patients in the event of a breach. In the event of such a breach, for every minute of downtime, the worried public will be wondering if their own heath might be impacted by the failure. Boards should ask their Chief Information Security Officer if there has been scenario planning analysis to examine the potential impact to their systems in the event of a breach due to an unknown vulnerability, and what the steps might be to minimize the damage and restore operation.

Finally, thus far, we've spoken primarily about PHI and the HIPAA Security Rule, and not at all about medical sensors and devices. It is important to note that the same denial-of-service attacks that were unleashed in late 2016 by malware installed on so called "Internet of Things" devices such as remote cameras and network-connected baby monitors could easily have been installed on network-connected patient ventilators, MRI systems, radiation machines, computer-controlled drug dispensing machines, and more. Indeed, it is worth noting that one of the earliest catastrophes causing loss of life due to a computer controlled system was due to a radiation therapy machine, the Therac-25, which gave massive overdoses of radiation to at least six people[13]—and that error was due only to a bug in the software that was accidentally triggered, and not due to an intentional attack.

Challenging Conventional Wisdom

In contrast, therefore, to advice from a security consultant, this is the kind of general insight that executives and boards actually need to hear:

- "Software is the most complex thing made by humans…. [Developing software] is like having to assemble a bridge starting from subatomic particles, and you're not allowed to use the current laws of physics as a reference.[14]
- "Data is a toxic asset."[15]
- "Behavioral data: Don't collect it. If you have to collect it, don't store it. If you have to store it, don't store it long."[16]
- "It is a *fantasy* to think that our current security methods have any chance of protecting [critical] systems…. This fantasy is protected and promoted by an elaborate and pernicious mythology based solely on existing practice."[17]

However, if this set of advice is really what healthcare executives and boards need to hear, what should they do, as a result? After all, if data is a "toxic asset," what should a medical institution do, since patient data is an essential aspect of providing medical care? Unlike other organizations that collect data more or less indiscriminately—consider the department store that installs beacons around the store to monitor the Bluetooth signals emanating from customers smartphones to track their movement through the store, or the Web site that tracks every purchase a customer makes in order to send targeted ads to them—a hospital collects patient data for the express

10 U.S. Department of Health and Human Services (HHS), HIPAA Security Rule (www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/).
11 U.S. Department of Health and Human Services (HHS), HIPAA Security Rule Guidance, July 14, 2010 (www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf).
12 U.S. Department of Health and Human Services (HHS), HHS Security Standards: Implementation for the Small Provider, December 10, 2007 (www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/smallprovider.pdf).
13 Nancy G. Leveson and Clark S. Turner, "An Investigation of the Therac-25 Accidents," *Computer,* Vol. 26, No. 7 (1993), pp. 18–41.
14 John Siracusa, "Accidental Tech Podcast," Episode 56, March 14, 2014 (atp.fm/episodes/56-the-woodpecker).
15 Bruce Schneier, "Data Is a Toxic Asset" (blog), March 4, 2016 (www.schneier.com/blog/archives/2016/03/data_is_a_toxic.html).
16 Pinboard, Twitter post, November 11, 2016 (twitter.com/Pinboard/status/797169153194889218).
17 Sean Peisert, Ed Talbot, and Matt Bishop, "Turtles All the Way Down: A Clean-Slate, Ground-Up, First-Principles Approach to Secure Systems," in *Proceedings of the 2012 New Security Paradigms Workshop (NSPW),* pp. 15–26, Bertinoro, Italy, September 19–21, 2012.

We interviewed Neil Gomes, Chief Digital Officer and Senior Vice President for Technology Innovation and Consumer Experience at Thomas Jefferson University and Jefferson Health to get his perspective on how Jefferson is building cybersecurity infrastructure and ongoing strategies for maintaining security in a rapidly growing academic health system. He also serves on advisory boards for IBM and Adobe and is in the Google Next Leaders Circle.

The Governance Institute (TGI): *Where and how are you focusing efforts right now related to cybersecurity?*

Neil Gomes (NG): The primary challenge facing Jefferson is joining disparate health systems with different processes, networks, protocols, and training. Once infrastructure is addressed, security is first a human problem. So our first efforts have been focused around training and simulations; getting people to better understand what they should or shouldn't send via email, what phishing scams look like, when in doubt don't click, and so forth.

Another education focus is of our own IT employees. For example, with the WannaCry issue, if everyone had installed the patch, it would have been fine. But when a patch is released it needs to be vetted because we run a lot of complex systems like FAA code and EMR, or business process applications and financial applications. Some of them don't work if you apply these patches. They could break the interfaces or the functioning of certain software, so you have to test. Some of it is manual. Some of it is automated. Some of it is your relationship with the vendors providing you with other applications that could be affected. We are hiring security analysts so we can accelerate the process of vetting these types of solutions that come onto our network or patches that need to be applied, and do that in a much faster way.

Then in the innovation space, there's a lot happening in machine running where we can establish baseline activity and then start looking at hotspots of sudden activity on the network—the ability to identify sudden increases in activity, either around an application or a type of process that's happening, that could be an indicator of some kind of inappropriate activity on the network. Once the system senses a potential issue, we can orchestrate multiple sets of automated processes that run to either contain the threat or alert people that something is going on.

These threats come up so often that you cannot rely on manual security analysts to find these things on your network, or react in an analog kind of manner. You need to orchestrate and automatize.

TGI: *Are HIPAA compliance and using the HITRUST framework secure enough, or do you feel it's important to go further?*

NG: I think it's important to go further because those regulations many times are set in place to deal with the bare minimum but to real risk to the organization. These are lessons we learned when we went through this process. We have a huge responsibility to our own patients. They trust us with our data. Some of the vendors walk away from us because they can't meet our requirements. It also ensures that the vendor has some skin in the game.

TGI: *What advice do you have for other organizations that might not have the same degree of capability as Jefferson or need to outsource security?*

NG: If you do everything in-house, you first have to purchase all the software and hardware, even before you start using it. That's a high cost burden. Then you also have to hire very talented security professionals. And your ability to hire someone who is better than someone at Google is probably lower because Google has the attractive brand and can afford to pay at a higher level. Slowly over time, Google and Amazon and other large cloud providers have commoditized the solution.

And most importantly, that's their business; it's not mine. My business is taking care of other people, saving lives. So I think it's a matter of being able to level with these types of companies. The commoditization is making the cost low. It's delivering it to you at the point of use. Google has over 750 security analysts and engineers, and they have skin in the game. So they're not going to risk their own reputation—they'll go way beyond what HIPAA or HITECH requires.

TGI: *From your perspective, what do you feel the board needs to know to feel ensured that the organization is doing what it needs to for cybersecurity?*

NG: The board needs reports on the current state and what the big problems are. They need us to ensure that at least we address the foundational issues. But beyond that I think there needs to be some structural question marks. For example, it is important to separate the functions of networking and security. They cannot be managed by the same people because if there's a security issue, often the problem lies with the networking team overlooking something. So if both teams are managed by the same people or group, the board is never going to realize the real problem. Another thing to look for is redundancy. An ideal redundancy is multi-tiered. If I'm storing my data with Google and my backup is also with Google, then that could be a problem. So you may want to have your redundancy services with a different cloud provider, and/or stored locally.

Secondly, IT staff should be running scenarios of what happens when a system goes down, and provide the board with some level of detail about plans in place to handle those scenarios. Suppose we get hit by a system lockout issue. How are we going to run through that whole scenario? If people start pointing to the same systems that could be affected, ask if those systems reside on the same server. I don't know if boards do really get involved in that. Boards generally ask for due diligence, but sometimes the problem is as simple as investing millions of dollars in something and then realizing you're relying on the same thing to get the whole network back up and running. There are vendors that will run simulations on your backup system to help determine possible scenarios and solutions.

Third, there is huge advantage in the cloud. If any proposal is presented to the board that doesn't involve some level of cloud in it, if it's all investment in local infrastructure, those systems are usually very proprietary and you'll run into problems and limitations.

Finally, especially with healthcare institutions, I think we should not be afraid of things we don't know. We owe that responsibility to our patients.

purpose of treating patients. And if our current security methods can't protect critical systems, what is the alternative?

For institutions—particularly academic medical centers that may already be familiar with everything in this piece—such organizations may have additional challenges of their own. These include not only patient records, but potentially also data and computing pertaining to medical research environments, such as the massive amounts of data being created by next-generation gene sequencers, and the analysis of that data. The solutions for securing such applications is not yet obvious, since as has been empirically demonstrated, traditional protection techniques, such as traditional firewalls are often not appropriate in such environments. To be sure, techniques are on the horizon—the "Science DMZ" network design pattern, which enabled "big data" network transfers for "open science" has led to the Medical Science DMZ.[18] And special-purpose computing chips can encrypt at higher rates than ever before. Cryptographic and statistical techniques to limit data exposure, such as fully homomorphic encryption, secure-multiparty encryption, and differential privacy are becoming realistic—the latter is now commonplace enough to be deployed by Apple and Google, for example. But "big data" in medicine, and the need for pooling and sharing that data to enable the kinds of research discoveries envisioned by the medical science community, is clearly a challenge of its own.

"No Silver Bullet"[19]

The reality is that there is no simple answer. But at the same time, as suggested earlier, the situation is not hopeless. Organizations must invest in security and take security seriously, even with the knowledge that no protection will be perfect. A set of questions from the board to the Chief Information Officer and Chief Information Security Officer might include:

1. Are we storing the right amount of data in order to make meaningful decisions and actions related to patient care, or are we storing data we are not using?
2. Once we have looked at the data, how long do we need to keep historical data?
3. Are we properly destroying old data that is no longer required?

Alternative Approaches

Don't Go It Alone

There is at least one truism for many organizations struggling to find a path forward: for most organizations, unless you are Google, Facebook, Microsoft, or Apple, or unless you are a major medical center with a very large IT budget and are located in a city rich with computer security talent, you probably should not try to solve the problem on your own. Organizations such as these are familiar with the HITRUST CSF[20] inside and out, and have large security programs with elements such as strong, multi-factor authentication, system hardening, backups, meaningful and appropriate training, and real-time network and system visibility. Incident response and recovery are well understood and integrated into the environment. These organizations probably already identified whether they need to run their own storage and email systems, and if each of their personnel needs a full system running Windows, or whether Google Apps and Chromebooks will do.[21] If this describes your organization, you have a massive head start on doing "all the right things."

Outsourcing and Consultants May Not Be the Answer

However, most healthcare organizations may have only pieces of this, and a budget to enable hiring the right team to put all of this in place in a way that is truly effective, rather than merely lip service to security, may be out of reach. On the other hand, outsourcing is not necessarily an effective solution, either. Consider the example of the Marin Healthcare District and Prima Medical Foundation whose patients were victims of a ransomware attack,[22] many of whose medical records were subsequently lost entirely due to an allegedly unrelated failure of the backup system.[23] These organizations *did* outsource, but did so to a small company that was not only incapable of blocking ransomware, which may well have been inevitable even for a more capable organization, but could not even maintain effective computer backups.

Healthcare executives and boards need to also keep in mind that not all computer security "experts" are created equal. While certifications from organizations such as

18 Sean Peisert et al., "The Medical Science DMZ: A Network Design Pattern for Data-Intensive Medical Science," *Journal of the American Medical Informatics Association (JAMIA),* 2017 (DOI: 10.1093/jamia/ocx104; https://academic.oup.com/jamia/article/doi/10.1093/jamia/ocx104/4367749/The-medical-science-DMZ-a-network-design-pattern).

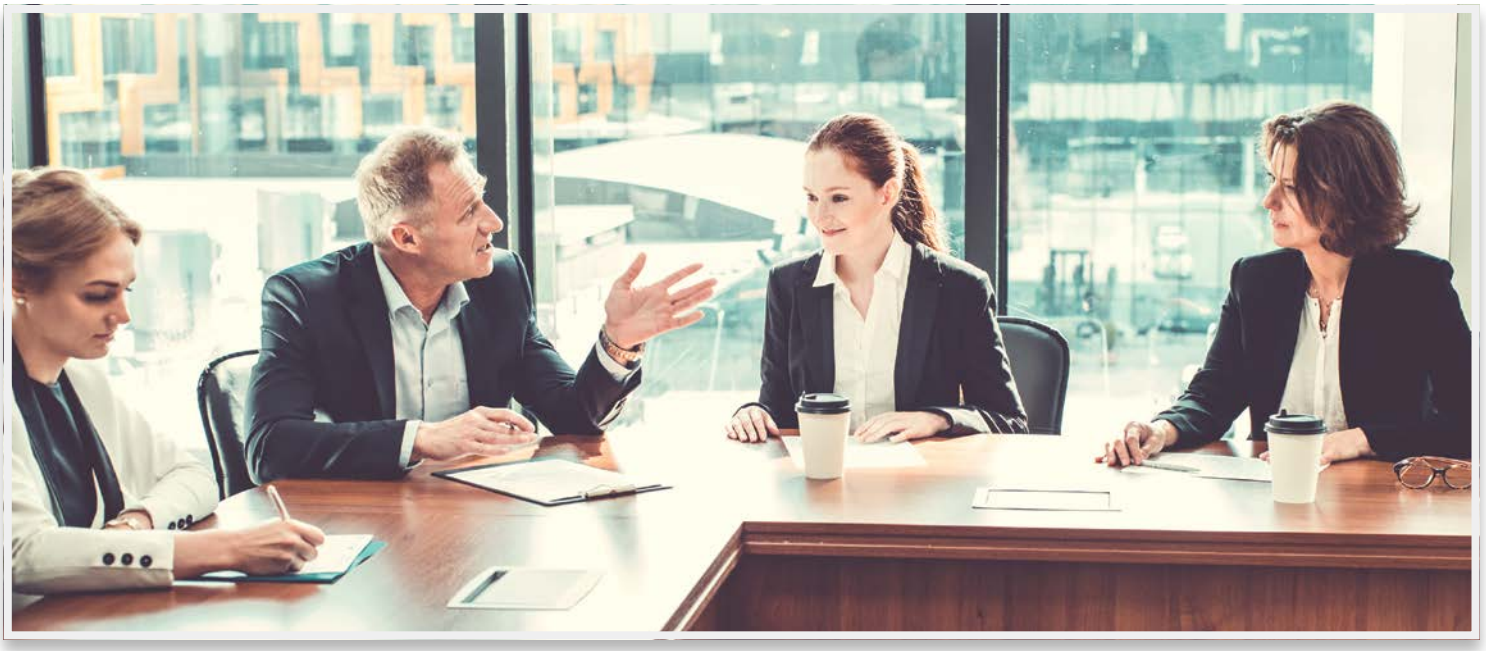
19 Fred P. Brooks, "No Silver Bullet—Essence and Accidents of Software Engineering," *IEEE Computer,* Vol. 20, April 1987, pp. 10–19.

20 HITRUST CSF v8, June 2016 (https://hitrustalliance.net/hitrust-csf/).

21 "Omada Health chooses Chromebooks to grow its business," March 11, 2014 (https://cloud.googleblog.com/2014/03/omada-health-chooses-chromebooks-to.html); and "The Roche Group goes Google," (https://gsuite.google.com/customers/the-roche-group/).

22 Richard Halstead, "Marin electronic medical record system hacked, ransom paid," *Marin Independent Journal*, August 4, 2016.

23 Richard Halstead, "Marin patients' medical data lost after cyber attack," *Marin Independent Journal*, September 29, 2016.



the SANS Institute's "Global Information Assurance Certification (GIAC)" and the International Information System Security Certification Consortium's "Certified Information Systems Security Professional (CISSP)" exist to provide a base level of competence in certain activities pertaining to computer security, and serve useful purposes, true excellence in leadership pertaining to computer security, including both in-house, top-flight chief information security officers and security engineering talent, are extremely rare. But that is what is needed, rather than consultants who parachute in to stand up a token security program and then depart until there is an incident to recover from. The consequence, of course, is that trusting a large part of a modern medical institution's lifeblood—patient data and, increasingly, network-connected medical instruments—to anyone less than top-flight talent is a Las Vegas gamble.

In the very short term, hiring a security consultant to come in to assess risk and implement mitigations is one option. Organizations such as the HITRUST Alliance may be able to help find such a person. This should not be considered the end of the problem, but rather a starting place. Finding the "right" consultant is not an easy task. There is no reliable set of criteria that would distinguish a consultant who is not only generally qualified, but has sufficient abilities to understand the distinctive aspects of your organization, in order to understand and implement the risk mitigation mechanisms. And further, consultants, by definition, are typically adjunct to the organization, and come in to do something and then leave. In contrast, security must be continuous, ongoing, and deeply ingrained. In my opinion, the most effective approach for the long term is for organizations to partner together to work on common, secure infrastructure, practices, and procedures that are both broadly effective *and* broadly implementable. A "lowest common denominator" implementation that only reaches the "compliance" bar is no longer a viable option.

"In my opinion, the most effective approach for the long term is for organizations to partner together to work on common, secure infrastructure, practices, and procedures that are both broadly effective *and* broadly implementable. A 'lowest common denominator' implementation that only reaches the 'compliance' bar is no longer a viable option."

—Sean Peisert, Ph.D.

Consider the actions after the 4.5-million patient breach at the UCLA Health System[24] and the two breaches at UC Berkeley resulting in the theft of 80,000 employee records[25]—the University of California instituted a system-wide "threat detection and identification approach" covering all 10 campuses and five academic medical centers to obtain consistency of practice, economies of scale, and leverage the limited pool of top security talent across the entire

24 Chad Terhune, "UCLA Health System data breach affects 4.5 million patients," *The Los Angeles Times*, July 17, 2015.
25 Dave Lewis, "University of California Berkeley breached again," *CSO*, February 27, 2016.

system.[26] All of a sudden, the entire University of California is more or less able to be one of the types of organizations referred to earlier with "a very large IT budget and are located in a city rich with computer security talent."

Not every organization can implement something as extensive as the University of California has, with a combined, system-wide annual budget of nearly $30 billion and a president who was formerly Secretary of the U.S. Department of Homeland Security. However, it may be possible to form some kind of coalition with sufficient financial and personnel resources to bring solid capabilities.

How many organizations run their own email server? In contrast, how many organizations that *do* have cybersecurity talent choose to run their own mail server rather than leveraging Google's cloud services? Consider the many organizations, again, including the University of California, the U.S. Department of Defense, the U.S. Naval Academy, and the U.S. National Oceanic and Atmospheric Administration, who do the latter? The same thought process should apply to medical systems. Would the NHS ransomware attack[27] have been effective if the data had been stored in databases (compliant with U.K. health security and privacy laws) run by a major cloud provider? I think it is unlikely. The conclusion that one might draw from the decisions these organizations have made is that running one's own computing systems is often *not* the right idea if other organizations with extremely strong reputations may be able to do so more reliably, more securely, and at lower cost. (This is an example of outsourcing done right.)

> "My guess is that before long most processing of HIPAA data will be in cloud providers... imagine a world where there was a vetted architecture implemented by each of Google, Amazon, and Microsoft, with a safe harbor provision for use of technologies in approved ways."
>
> *—Eli Dart, Network Engineer, ESnet Science Engagement Group, Lawrence Berkeley National Laboratory*

Security Is the Responsibility of the Entire Organization

One extremely important point is that security needs to be the responsibility of the entire organization, not just the people who have "security" in their job title. This distinction is not unlike the responsibility of all personnel with regard to patient safety—it is not just the role of the physician and nurse, but includes everyone from purchasing representatives to custodial staff.

Given that computer network-connected devices, from computers running EHRs to network-connected sensor and imaging equipment to HVAC systems, are critical to the function of a hospital for providing high-quality patient care, it is similarly the responsibility of the entire organization to ensure cybersecurity as well.

To build such a culture, the board should emphasize open, strong, and continuous bi-directional communication between the people who make decisions about security (e.g., the CISO's team) and the rest of the organization. In addition to the "core" security team composed of the CISO and security engineers and analysts, create a "virtual" security team of personnel from other parts of the organization, perhaps on a rotating basis, to join in weekly or bi-weekly security meetings as well.

Creating such a virtual security team enables personnel outside the core security team to learn more about the security challenges the entire organization faces, and to disseminate that knowledge to their peers. It also provides an opportunity for personnel outside the core security team to bring in fresh ideas and perspectives that the core security team may not have considered. This not only conveys information in both directions but helps align the motivations and goals of both sides—personnel outside the core security team better understand the needs of the security team, and the core security team better understands how other people in the organization need to be able to do their jobs.

A similar discussion between security staff and management is also vital. Many organizations have their CISO reporting to the CIO, or perhaps to someone even lower down in the organization. This can be a mistake, because frequent and bi-directional lines of communication between security and management, and indeed between security and the board of directors, are vital. Organizations with top security functions also tend to be organizations in which boards and management hear as regularly from security leads as they do from other business leads such as the CMO.

26 University of California Office of the President, "Purposes of a Systemwide TDI Approach," https://security.ucop.edu/services/threat-detection-and-identification/purposes.html.

27 Brian Krebs, "U.K. Hospitals Hit in Widespread Ransomware Attack," May 17, 2017 (https://krebsonsecurity.com/2017/05/u-k-hospitals-hit-in-widespread-ransomware-attack/).

Conclusions

What should healthcare institutions do? First and foremost, it is vital that executives and boards learn to embrace security rather than resist it. Effective security need not be burdensome,[28] and can even be an *enabling* technology, not unlike how cleaning the oil filter in a car can do double duty for reducing emissions *and* making the car perform more responsively.

Second, find partners so you are not going it alone.

It's worth noting that there is some reason for optimism against all the bad news. For example, a community effort to create a "building code" for medical devices[29] has led to guidance issued by the U.S. Food and Drug Administration to produce more secure medical devices.[30] While the guidance is optional at this point, there is reason to be optimistic that the tide is turning. In addition, the rise of large "cloud" infrastructures also creates reason for optimism as well.

Hospitals need no longer necessarily install and maintain all of their own, internal computer systems—something that has long been both costly and error prone. Google has email, calendars, and collaborative document editing in the cloud. While there are not yet robust, reliable cloud solutions for everything, the list is growing, and most organizations should be asking themselves, for each piece of software, if they should be running that software in-house, and assuming internal responsibility for securing the infrastructure and the data processed by and/or stored on it, or if it might be better run by a major cloud provider such as Amazon, Google, or Microsoft.

And, in many cases hospitals need no longer maintain as many traditional "computer systems" at all. There is almost a complete lack of malware that effects Apple's iOS operating system, for example, and unlike past arguments about the lack of malware affecting MacOS due to low market penetration, the same argument cannot be made about iOS. And the reason is not because of better "security software"—there is effectively none, or at least no anti-virus or traditional monitoring software[31]—but due to the ways in which iOS is more locked down and the iOS App Store has basic curation elements. To be sure, no one would claim that iOS is *secure*—no-non-trivial piece of software is. But it does appear to have key advantages. Given all this, what might a world look like in which data is largely stored on large, centrally monitored systems by professionals with experience comparable to those from the best companies and institutions in the U.S., and access to that data were mostly via highly-locked down iOS and other mobile devices?

The Governance Institute thanks Sean Peisert, Ph.D., Staff Scientist at Lawrence Berkeley National Laboratory, for contributing this special section. He is also an Adjunct Associate Professor of Computer Science at the University of California, Davis, where he does research and development in a broad cross-section of computer security, and teaches a course on security in health informatics at the UC Davis Medical School. He is also Chief Cybersecurity Strategist for CENIC, a non-profit organization that operates the network that provides Internet connectivity for over 20 million users in California, including the world's largest education system—the California K-12 system, California Community Colleges, the California State University system, California's Public Libraries, the University of California system, Stanford, Caltech, and USC, including the UC, Stanford, and USC medical centers and health systems. He received his Ph.D., Master's, and Bachelor's degrees in Computer Science from UC San Diego. He can be reached at sppeisert@lbl.gov.

28 Edward B. Talbot, Deborah Frincke, and Matt Bishop, "Demythifying Cybersecurity," *IEEE Security & Privacy*, Vol. 8, No. 3, pp. 56–59, May/June 2010.
29 Tom Haigh and Carl Landwehr, "Building Code for Medical Device Software Security," 2015 (cybersecurity.ieee.org/images/files/images/pdf/building-code-for-medica-device-software-security.pdf).
30 U.S. Food and Drug Administration, "Information for Healthcare Organizations about FDA's 'Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-The-Shelf (OTS) Software,'" June 14, 2017 (www.fda.gov/RegulatoryInformation/Guidances/ucm070634.htm) and "Postmarket Management of Cybersecurity in Medical Devices—Guidance for Industry and Food and Drug Administration Staff," December 28, 2016 (www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf).
31 Rich Mogull, "Tidal Forces: Endpoints Are Different—More Secure, and Less Open," January 18, 2017 (https://securosis.com/blog/tidal-forces-endpoints-are-different-more-secure-and-less-open).