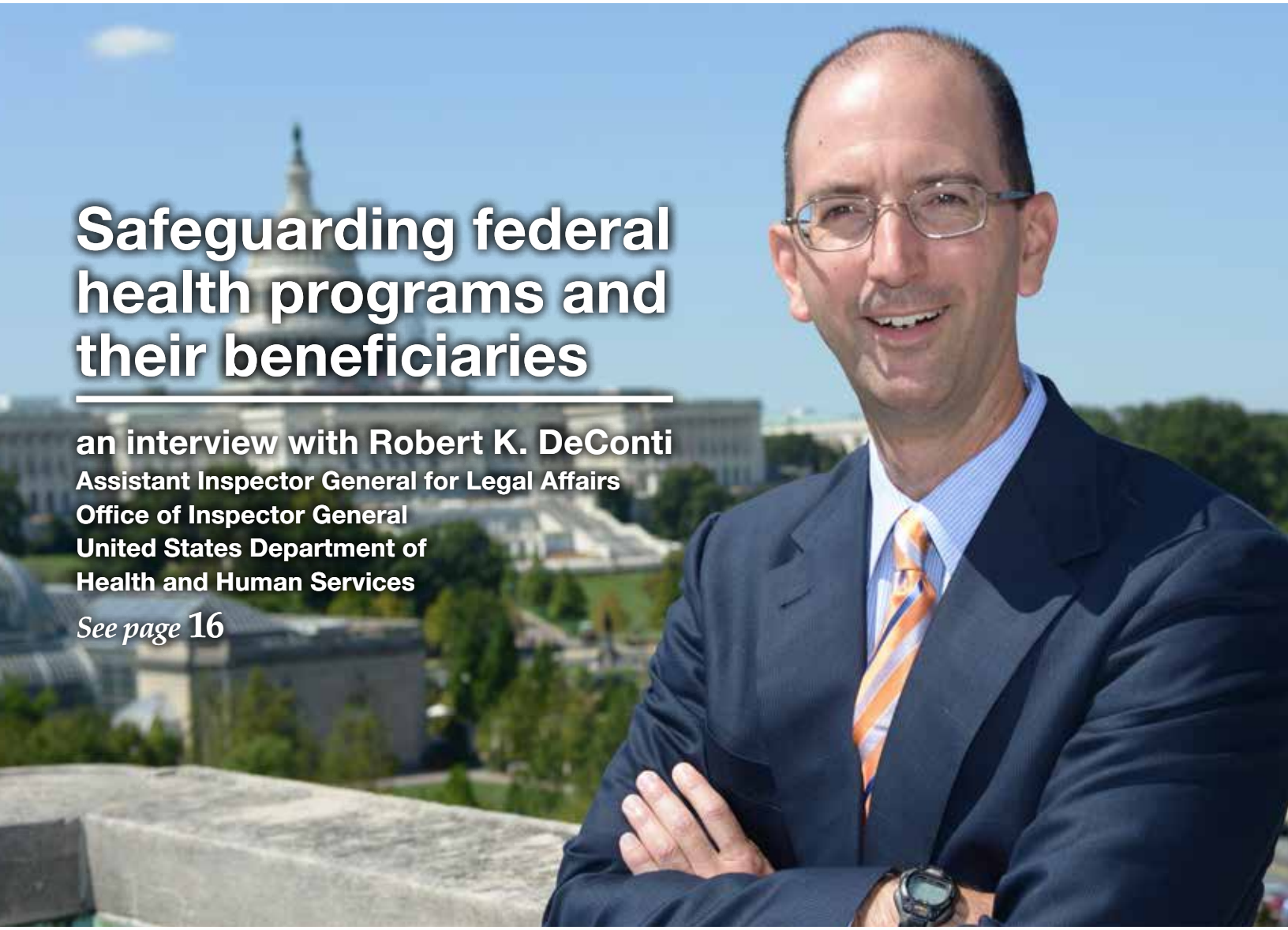
HCCA HEALTH CARE COMPLIANCE ASSOCIATION

Compliance TODAY

December 2016

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

WWW.HCCA-INFO.ORG



Safeguarding federal health programs and their beneficiaries

an interview with Robert K. DeConti
Assistant Inspector General for Legal Affairs
Office of Inspector General
United States Department of Health and Human Services

See page 16

by Bob Chaput, MA, CISSP, HCISPP, CRISC, CIPP/US

Building a business case for cybersecurity investments

» CISOs need to stay on top of the evolving threats to cyber information with effective security controls and practical remediation activities.

» Few organizations are conducting bona fide comprehensive risk analyses, and that is where the journey must begin.

» Conducting a bona fide risk assessment can be an effective first step in building credibility with the executive team and board.

» Identify an executive sponsor to use as a sounding board on risk appetite and recommendations on mitigating risks.

» Any function that has access to PHI or is involved in procedures for providing or terminating access to PHI should be part of a cross-functional team that helps identify and respond to threats and vulnerabilities.

Bob Chaput *(Bob.Chaput@ClearwaterCompliance.com) is the CEO and Founder of Clearwater Compliance LLC in Nashville, TN.*

With the increase in the number of people who now have insured access to healthcare and the increase in organizations with access to health information, combined with the increase in the number of devices containing that information, chief information security officers (CISOs) need to have an increase in their security budgets. But studies show that IT budgets are virtually flat in 2016, and expenditures do not include much for information security. Despite pressure from boards and regulatory agencies, many CEOs don't believe they are responsible for cybersecurity; they point to their CISOs as the culpable parties. But how can CISOs protect the data when money continues to be invested in other business priorities? Only by submitting a compelling business case can CISOs increase their chances for greater investments in information security.

Chaput

More healthcare data

Just two years ago, *USA Today* headlines read "Health care spending growth hits 10-year high."[1] The article noted, "The Centers for Medicare & Medicaid Services expects health spending to rise 6.1% this year, up from about 4% in 2013, as an estimated 11 million Americans gain health insurance," and join the legions of patients in the US healthcare ecosystem.

More organizations with healthcare data

According to a report by Kalorama Information, the electronic medical records (EMR) market is projected to grow by 7% to 8% each year for the next five years, driven by physicians finally adopting EMR rather than facing a Medicare fee reduction of 1% for each of the next three years and EHR vendor replacement contracts (aka "EMR rip and replace") that require consulting, training, and system upgrades.

In January 2016, the Centers for Medicare & Medicaid Services (CMS) welcomed 100 new accountable care organizations (ACOs) to the Medicare Shared Savings Program, bringing the total to 434. With the move to

preventive care, the number of firms providing population health analytics has also expanded as a result of the Department of Health and Human Services' (HHS's) recent decision to tie 90% of Medicare payments to value based models by 2018.[2]

Although fairly new and unproven, the number of telemedicine or telehealth organizations and their software providers continues to increase and will likely accelerate with Congress working to loosen some of Medicare's rules regarding reimbursement.[3]

There are new players in the retail clinic space, bringing the total to over 1,800 country-wide.[4] The healthcare ecosystem continues to expand.

More medical devices, apps, and wearables

More than 6,500 medical device companies[5] do business in the U.S., consisting of electromedical equipment, irradiation apparatuses, surgical and medical instruments, surgical appliances and supplies, and dental equipment and supplies. New companies breaking into this field are finding new solutions to old healthcare problems, including allergies, walking disabilities, degenerative disc disease, and Ebola, to name a few.[6] Many smartphone apps and wearable devices track and maintain healthcare data.

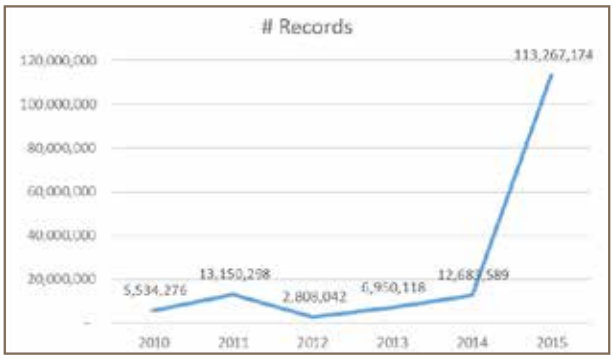
New healthcare applications were announced almost weekly throughout 2015 to address expanding needs for telehealth, prescription management, physician reference, patient portals, and house calls. The growth of the use of mobile applications by healthcare professionals is expected to increase to 46%over the next five years from 16% as of November 2015, according to a survey by Research Now.[7]

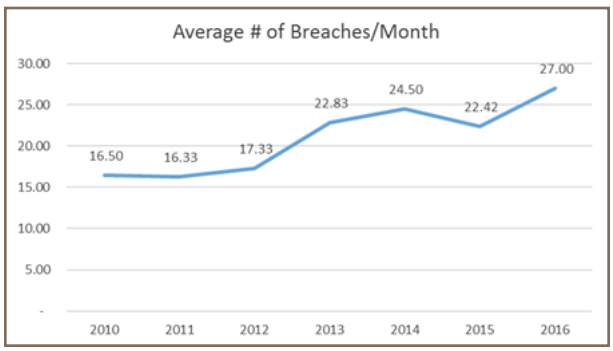
The number of wearable medical devices and their applications, addressing either diagnostic or therapeutic needs, has also mushroomed and is projected to expand over the next eight years at an annual compound growth rate of 16.4%.[8] Reasons for the growth include increasing interest and emphasis on fitness and disease prevention, in addition to the increasing geriatric population requiring home-based monitoring.[9]

Breaches and ransomware attacks accelerate

No surprise, with the increases in the amount of health information, the number of organizations involved in healthcare, and the increase in medical devices, the number of breaches has also accelerated. The number of breached records reported on the HHS website in 2015 (113,267,174) was eight times higher than 2014 (12,683,589) and more than two times greater than all the breached records reported in 2009 through 2014 (41,261,096) (see Figure 1). The average number of reported breaches per month in the first seven months of 2016 was 20% higher than in 2015.

Figure 1:
Analysis of HHS Breach Report as of July 31, 2016[10]





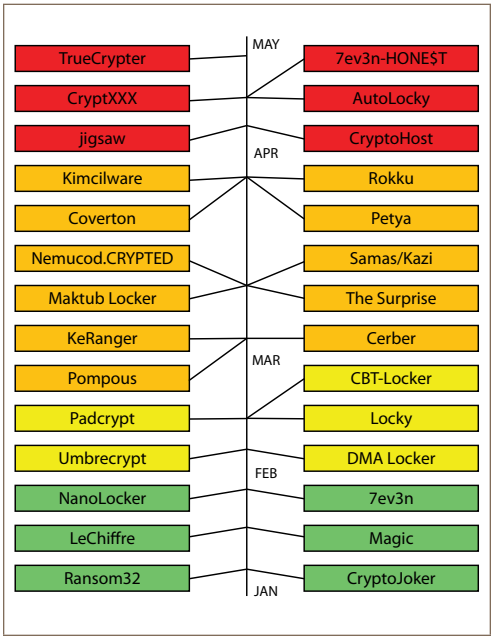
As of August 4, 2016, the Office for Civil Rights (OCR) had negotiated settlement agreements with or issued Civil Money Penalties to 40 covered entities or business associates following breach investigations for a total of $52,589,700 and a 2-year (at least) corrective action plan requirement.

Although not reportable as breaches due to the low probability of compromise, ransomware attacks have been on a steady increase in 2016 with at least 28 new strains having been identified through May (see Figure 2). According to a report released by PhishMe on June 1, 93% of all phishing emails in the first quarter of 2016 contained encryption ransomware, compared to 56% in the 4th quarter 2015. The raw number of phishing emails in Q1 hit 6.3 million.

Although historically ransomware relied on unsuspecting users to click on phishing emails or infected websites, SamSam now exploits unpatched server vulnerabilities.

A recently discovered ransomware strain called Crysis doesn't just encrypt files, it pulls them from their network and sends them to a remotely controlled server. When files leave the building, the organization is now in reportable data breach territory.

Figure 2: Identified ransomware attack strains



Although no organization is immune to ransomware, criminals are targeting hospitals due to the critical nature of the information, its availability, and the ease of acquiring it. Hospitals that have been victims of ransomware in the last five months include, but are not limited to:

- Feb 2016 – Hollywood Presbyterian Hospital
- Mar 2016 – Methodist Hospital
- Mar 2016 – Baltimore's Union Memorial Hospital
- Apr 2016 – Alvarado Hospital Medical Center
- Apr 2016 – King's Daughter's Health
- May 2016 – Christopher Rural Health
- May 2016 – Kansas Heart Hospital

The largest ransom payment that has been made public was $17,000 by Hollywood Presbyterian Hospital. With the capability of taking down full networks and/or moving the data offsite, criminals will start to ask for more. And in some cases, even after payment, the hackers did not return full access to the files.

IT security spending stagnates

Given the current escalating environment, CISOs need to stay on top of the evolving threats to cyber information, effective security controls, and practical remediation activities—all of which suggests an organization might allocate a bigger percent of the slight increase in the organization's planned technology investments. Gartner's 2016 IT Spending Forecast reported that information technology (IT) spending in 2015 only increased 1.6% and that the same was

expected in 2016. And the focus of expected 2016 technology expenditures is on innovation, not cybersecurity.

Competing priorities

Headlines following Gartner's CEO survey in 2014 emphatically proclaimed "Technology investment returns to the CEO agenda." Following growth, cost, and profit, technology came in #4 in the CEOs' investment priorities. By the time of the survey in April 2015, the "second-most-important category" of business priority for 2015 and 2016 was "technology related" – the highest since 1999![11] Yet more than half of the responses highlighted technology investments related to revenue and growth (e.g., multichannel, e-commerce, m-commerce). The top three technology investment priorities over the next five years? Customer engagement management, digital marketing, and business analytics.

In 2016, the PwC CEO Survey indicates that CEOs plan to set their organization apart through strengthening their technology foundation. According to the survey, "As … technologies cross the threshold from immature to mainstream, CEOs are mindful of the need to build a cohesive digital infrastructure that positions them to really innovate."

According to the 2015 Gartner CIO Agenda Report, "Though digital opportunity is everywhere, the overwhelming majority of this year's CIO respondents (89%) agree that the digital world engenders new, vastly different and higher levels of risk, and that the discipline of risk management is not keeping up (69%)." In terms of IT priorities, investments in security came in at #7 (11%), significantly behind those in analytics (50%), infrastructure (37%), cloud computing (32%), and mobile devices (36%).

Although board members are becoming more engaged in risk management discussions, like the CEOs, the prioritization of IT investment is still focused on the top and bottom lines, according to a study commissioned by the New York Stock Exchange. In fact, security risks were listed as only the #4 board concern when introducing new technology-based products and services, behind concerns for revenue potential, competitive differentiation, and development costs.

The impact lands on CISOs and CIOs

In February 2016, Donna Seymour, OPM's Chief Information Officer, resigned two days before she was to appear before a Congressional Committee to discuss the OPM data breach. House Oversight Committee Chairman Jason Chaffetz (who called for Seymour's resignation) said, "While I am disappointed Ms. Seymour will no longer appear before our committee this week to answer to the American people, her retirement is necessary and long overdue. On her watch, whether through negligence or incompetence, millions of Americans lost their privacy and personal data."

Earlier, at a House Oversight and Government Reform Committee meeting, Rep. Ted Lieu (D-CA), who has a background in computer science, scoffed at the agency for not conducting a risk assessment, calling it a "failure of leadership," something that goes beyond the OPM. "Leadership at the DEA, the VA and SSA have all been fired," he said, adding, "The status quo is not acceptable," and that he's "looking for leadership to resign for the good of the nation."

Few organizations in the government and the public and private sectors are conducting bona fide comprehensive risk analyses, and that is where the journey must begin. Not with "controls checklists," not with "audit opinions," and certainly not with meaningless certifications.

In April 2016, *CSO* featured a story about the firing of chief information security

officers (CISOs). The job title emerged in the late 1990s and initially was "focused largely on fixing firewalls and patching vulnerabilities." Today they are "charged with juggling the day-to-day operations of their security team with meeting board expectations while also staying abreast of an ever-evolving threat landscape and regular regulatory changes." The average tenure for a CISO is 18 months or less.

Most CISO or CIO firings are not made public, and the vacating of an office is not always the result of a firing. Confidential interviews with CISOs who were fired revealed these primary causes:

- Disagreeing with senior management on risk management processes and priorities,
- Inability to address risk satisfactorily and economically,
- Not following business strategies,
- Failing to discover or report a vulnerability, and
- Not meeting budget targets.

Building a business case

In order to get the funds needed to shore up an information security program, CISOs need to develop a comprehensive and compelling business case for doing so. This process needs to include details and facts and will take time to complete but will improve your odds for gaining the investment dollars you need to secure the information entrusted to your care.

Comprehensive risk analysis

Conduct a comprehensive, bona fide risk analysis of all assets that create, receive, maintain, or transmit ePHI.

Examine all the threats to information security and vulnerabilities to those assets; assess the ability of the controls in place to minimize exploitation. Identify the media where the PHI "lives" (e.g., laptops, desktops, servers, back-up tapes, flash drives). Detail the threats to that media (e.g., environmental threats such as hurricanes, structural threats such as power outages, accidental threats such as errant or misdirected emails, and intentional threats such as ransomware attacks). Bona fide, comprehensive risk analysis considers numerous "asset-threat-vulnerability" combinations. Consider the following steps.

1. Assess and rank the risks

Rate each risk in terms of the likelihood of a compromise of the confidentiality, integrity, or availability of the information and the impact if such a compromise happens. By using a scale from 1 to 5 (5 being the highest likelihood), you can begin the risk-ranking process. There are a number of data sources that you might use to assess the likelihood of a compromise:

- **Threats and threat sources**
  - Data from the HHS website listing all reported breaches of 500 or more records. Examine what threats have exploited what vulnerabilities that may exist in your own environment. As of 6/23/16, 20% of the breaches of 500 records or more reported on the HHS website this year are attributed to hospitals, clinics, and health systems—37% of those breaches were due to hacking or IT incidents: email (6), network server (1), and desktop computers (3).
  - Information from other best practice websites and sources regarding emerging threats and vulnerabilities. For example, ransomware exploiting unpatched vulnerabilities of JBoss. Sign up for alerts from the US Computer Emergency Readiness Team (US-CERT) and FBI Crime Complaint Center. Other resources include, for example, the KnowBe4 blogs and the NH-ISAC,

among others. Include emerging threats and vulnerabilities in ongoing risk analyses.
    - Security or privacy incidents that have been reported in your own organization may identify threats that have not yet been addressed.
- **Vulnerabilities**
    - Insufficiently documented and enforced policies and procedures
    - Lack of practices regarding system back-up, workforce access, updating patches
    - Undocumented or untested disaster recovery and business interruption plans
    - Limited and ineffective workforce training and security awareness programs
- **Controls**
    - Typically categorized as administrative, physical, and technical, control sets can be found in sources such as:
        - NIST 800-53
        - ISO 27001
        - CCS CSC

2. Rate the impacts

Rate each risk in terms of the impact of a compromise of the confidentiality, integrity, or availability of the information and the impact if such a compromise actually happens. There are basically two ways you can calculate the impact of a breach:

- **Using the annually-updated average cost of a data breach** conducted by the Ponemon Institute and sponsored by various companies. In 2016, the study was sponsored by IBM and the average cost of a data breach was determined to be $221 per record. So the impact for a breach would be calculated on the number of records that would be involved in the compromise of each asset. Just to put it in perspective, on the HHS website for the first seven months of 2016, the number of breached records per hospital or health system due to hacking or IT incidents totaled 12,612, making the average cost due to hacking or IT incident for each breached organizations $2.8 million. The only problem with this approach is that the calculation does not include all costs that would be incurred because of the difficulty in doing so, such as reputational repercussions, business disruption, or the loss and replacement of an executive leader or other key workforce members.
- **Calculating the cost of a breach specifically for your organization.** The elements of that exercise are outlined in a free report from the American National Standards Institute (ANSI) entitled "The Financial Impact of Breached Protected Health Information – A Business Case for Enhanced PHI Security."[12] This thoughtful calculation will be more persuasive as it will be specific to your organization.

Because no studies have been done on the cost of recovering from ransomware, the bottoms-up calculation could be prepared by considering these factors (details of which may be found in the ANSI report mentioned above):

- **Payment of the ransom:** This may be the smallest expense to be dealt with, although ransom demands are expected to increase significantly.
- **Forensics and investigation activities:** This cost can vary depending on the number and types of systems involved and the complexity of the recovery of evidence. According to the 2016 Ponemon Cost of a Data Breach study of 64 organizations, average detection and escalation costs increased 20% from $610,000 in 2015 to $730,000 in

2016, making it one of the three highest costs following lost business and legal defense services.[13]

- **Mitigation:** 72% of organizations infected with ransomware required a minimum of two days to restore access to their data and a third required five days or more, according to a study by Intermedia.[14] The time and cost associated with recovery (i.e., containing the infected systems, wiping them completely, and then restoring them) must be included in the impact calculation. Recovery is measured in terms of how much data an organization can afford to lose (i.e., 1 hour or 24 hours) and how long it can operate without an asset or group of assets being available before it impacts the bottom line (i.e., 1 hour or 24 hours.)
- **Remediation:** Updated and tested disaster recovery and business interruption plans, back-up procedures, workforce training, business disruption, replacement of leaders held accountable, public relations costs, and lost business due to reputational damage.
- **Fines and penalties:** OCR fines and identity theft services, and possibly lawsuits, following ransomware attacks that include the transfer of information out of the organization's environment to a command server elsewhere.

3. Compare risk-ranking to your organization's risk appetite

Translate your impact calculations for each risk into the scale from 1 to 5 (with 5 being the highest impact). Multiply the likelihood ranking and the impact ranking to produce a risk-ranking of your risks from 1 to 25. Test the waters on your organization's risk appetite by developing remediation plans for any risks with a score higher than 14, which would include calculation results from a 3*5 or a 4*4 and higher.

4. Develop and recommend thoughtful remediation plans

Information risk management and thoughtful remediation planning involves risk-rank ordering all the organization's identified risks, prioritizing this list from the most significant to least significant risks, and using the organization's risk appetite to draw an initial "line in the sand" to identify which risks will be accepted. Then the organization must make decisions about avoiding, mitigating, and/or transferring those risks that exceed an organization's risk appetite.

Summary

There are an ever-increasing number of threats to healthcare information. Healthcare information is more valuable and visible than ever and, at the same time, more vulnerable than ever. You feel responsible and, as the CISO, you are responsible for its security. Conducting a bona fide risk assessment can be an effective first step in building credibility with the executive team and board and, therefore, in building a business case for cybersecurity investments in your organization. In addition to conducting the risk assessment, you should:

- Find a sponsor on the executive team to use as a sounding board on risk appetite, sufficiency, and the understandability of supporting information and recommendations on mitigating risks.
- Build a cross-functional team to help identify and respond to threats and vulnerabilities, including representatives from any function that has access to PHI or is involved in procedures for providing or terminating access to PHI.
- Change the technology language you and your team use from "compliance and information security" to "patient satisfaction

and quality of care." These words will resonate more with CEOs and other functional leaders you'll want on your side.

Your own reputation, and next job, depends on it.

1. Paul Davidson: "Health care spending growth hits 10-year high" *USA Today*, April 1, 2014. Available at http://usat.ly/2eGa80d
2. Jennifer Bresnick: "90% of Medicare Will Be Value-Based Reimbursement by 2018" *HealthIT Analytics*, January 27, 2015. Available at http://bit.ly/2ebi5Hm
3. Bob Herman: "Virtual reality: More insurers are embracing telehealth" *Modern Healthcare*, February 20, 2016. Available at http://bit.ly/2eRPjwI
4. Timothy Magaw: "Retail health clinic business gets more competitive" *Crain's Cleveland Business*, August 11, 2015. Available at http://bit.ly/2evOdse
5. SelectUSA: "Medical Technology Spotlight" *The Medical Technology Industry in the United States*, Available at http://bit.ly/2dXbdjb
6. MedReps.com: "5 Medical Device Startups to Watch" *Job Market*, September 23, 2015. Available at http://bit.ly/2dKRiAG
7. Joseph Conn: "Easy on those apps: Mobile medical apps gain support, but many lack clinical evidence" *Modern Healthcare*, November 28, 2015. Available at http://bit.ly/2dIVntZ
8. PR Newswire: "Wearable Medical Devices Market to Touch US $10,697.0 Million in 2023" *News Releases*, April 20, 2016. Available at http://prn.to/2dXa5fo
9. Grand View Research: "Wearable Medical Device Market Analysis by Product, By application and Segment Forecasts to 2022" *Industry Analysis*, February 2016. Available at http://bit.ly/2eGMbmL
10. DHHS: Office for Civil Rights: Breach Portal: "Breaches Affecting 500 or More Individuals" July 31, 2016. Available at http://1.usa.gov/1yY3CaK
11. Gartner Newsroom, press release: "Gartner CEO and Senior Business Executive Survey Shows Technology Related Change Is a Higher Priority Than Ever Before" April 21, 2015. Available at http://gtnr.it/2eGaIew
12. American National Standards Institute: "Protected Health Information (PHI) Project Overview" *ANSI Standards Activities*, 2012. Available at http://bit.ly/2evPaAy14.
13. Ponemon Institute: "2016 Cost of Data Breach Study - United States" Available at http://ibm.co/2eOTzvT
14. John P. Mello Jr.: "Ransomware's Aftermath Can Be More Costly Than Ransom" *TechNewsWorld*, March 24, 2016. Available at http://bit.ly/2eROBht