# A CULTURE OF SECURITY: TURNING YOUR GREATEST THREAT INTO AN ASSET

***Authored by:***
*Emily Carlson, Principal, Divurgent*

# INTRODUCTION

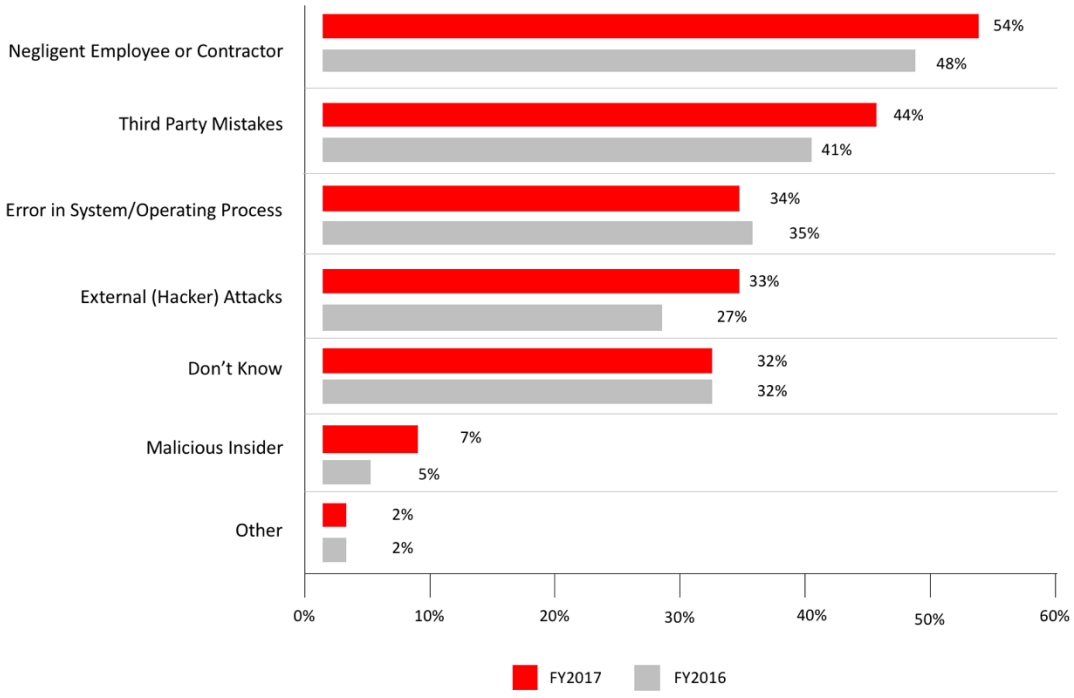
In the previous whitepaper in this series titled, "Navigating Healthcare Through Today's Cybersecurity Landscape," we made the point that the cybersecurity environment of today is no longer a matter of guarding against simple hacking, but about being at war. That being said, one of the biggest threats a healthcare organization faces is not from malicious, external bad actors, but from inside the organization.

When it comes to insiders, malicious acts are only a small fraction of the cybersecurity damage being done. The bulk of the damage internally is the result of two natural human tendencies: being too trusting and making careless mistakes.

In this whitepaper, we will explore some of these issues and provide a framework for educating your employees and creating a culture of security.

In September 2017, the Ponemon Institute published a survey of approximately 600 businesses with up to 1,000 employees in the United States and the United Kingdom, which stated that negligent employees were the leading cause of data breaches (See Figure 1.) Of those who reported a data breach in 2017, 54 percent said they were the result of negligent employees—an increase of 6 points from the 48 percent reported in the previous year's study.[1]

**Figure 1: Root Causes of Data Breaches**




*Source: Ponemon Institute. (2017). 2017 State of Cybersecurity in Small and Medium-sized Businesses. Chicago: Keeper Security.*

The problem is nearly the same throughout healthcare. Ponemon's Sixth Annual Benchmark Study on Privacy and Cybersecurity of Healthcare Data estimates half of all healthcare cyber breaches in 2016 were caused by human error.[2] The same 2016 study included a survey of nearly 100 healthcare entities, in which 69 percent of respondents said negligent or careless employees were their greatest security concern.[2]

Why does this happen? A primary reason is something cybersecurity experts call "Rational Response Theory," which is the psychology behind why people choose not to face the reality or audacity of a threat or risk. Simply put, it means most of us view the world as inherently good. This is particularly true with healthcare employees, given that most enter the field with an explicit passion for helping people. In fact, people in the healthcare arena are arguably the most compassionate and helpful compared to any industry, always available for people in their absolute worst moments.

So in terms of real–life cybersecurity application of Rational Response Theory, if a nurse is rushing to help a patient and can't remember the system password, a co-worker is likely to be quick to offer his or hers, or another employee is happy to bring a visitor or vendor in through the locked, employee-only door because it's closer to where the outsider needs to go.

## CYBERSECURITY SOLUTIONS STARTS AT THE TOP

Acts of careless kindness and other such mistakes come not only from innate personal traits of healthcare workers and people in general, but also from an inherent organizational-level lack of appreciation of the cybersecurity threat. And that comes from the top.

Do your board and C-suite understand and appreciate the gravity of the threats and risks to your institution from cyberattacks? If they don't, chances are very good the rest of the people in your organization don't either. Boards are being held accountable by law for cyber breaches, but many still do not consider cybersecurity as a primary component in their risk management strategies.[3]

In its "Top 10 Tips for Cybersecurity in Health Care," the Department of Health and Human Services (HHS) lists "Establish a Security Culture" as the #1 tip and emphasizes that "Security practices must be built in, not bolted on." HHS lists the following three items as foundational advice that every healthcare organization needs to take in this regard:[4]

1. Education and training must be frequent and ongoing
2. Those who manage and direct the work of others must set a good example and resist the temptation to indulge in exceptionalism
3. Accountability and taking responsibility for information security must be among the organization's core values

It all starts with awareness and education. Employees need not only awareness and education so they can avoid making mistakes themselves, but they also need to be able to help the organization's cybersecurity

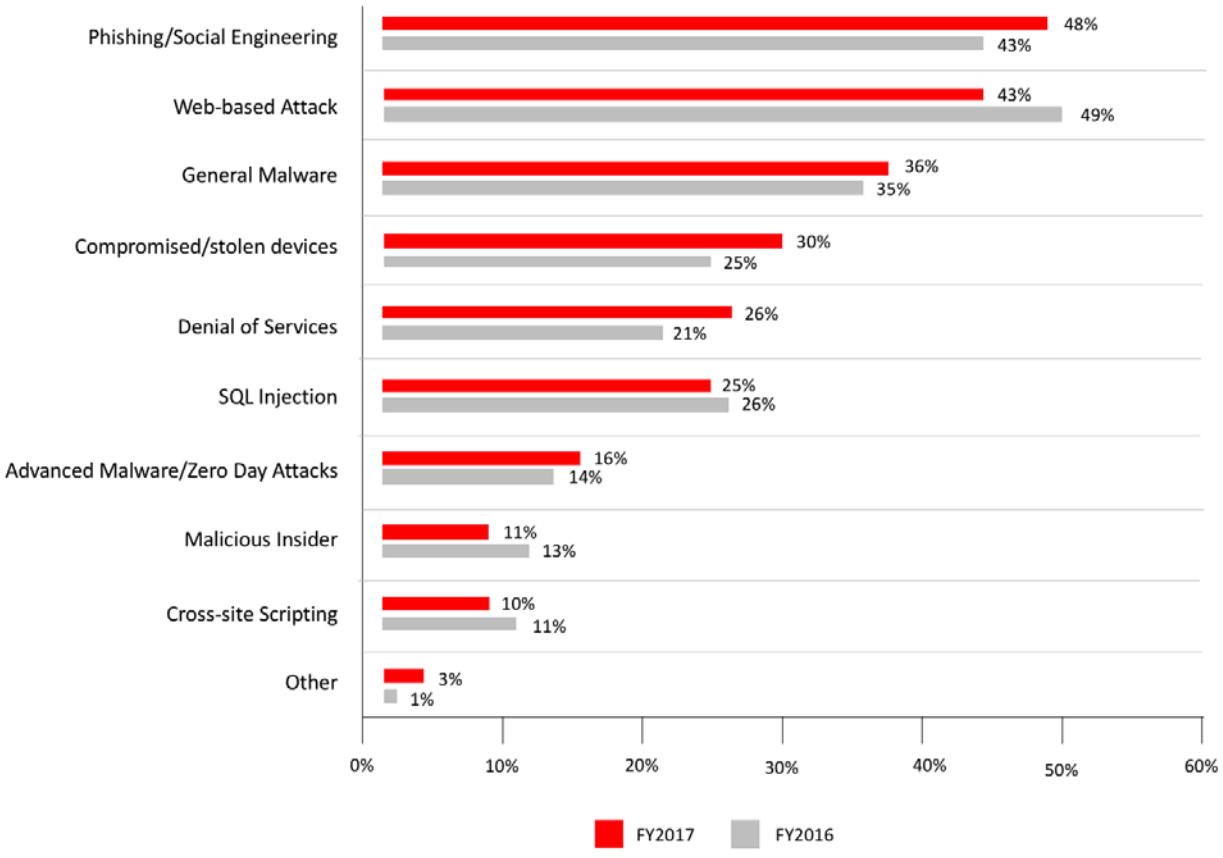
efforts by being enabled to recognize when a breach happens. From housekeeping to the C-suite, employees should serve as front-line intelligence when something has gone wrong.

## WHERE DO WE START IN EDUCATION?

Security awareness training is the best starting place in an education program as part of the goal of creating a culture of security. This training goes beyond basic cybersecurity education, which usually focuses on areas like spotting different types of scams. Awareness training includes understanding the tactics cybercriminals use, recognizing signs that a system may be under attack, and understanding how the consequences of an attack effect the organization.

Part of your continuously evolving awareness training is keeping your employees up to date on what kind of attacks they might be able to expect and their prevalence. Figure 2 shows results on this subject from the aforementioned 2017 Ponemon Institute survey.

**FIGURE 2: Types of Attack**




*Source: Ponemon Institute. (2017). 2017 State of Cybersecurity in Small and Medium-sized Businesses. Chicago: Keeper Security.*

Providing awareness training and regular cybersecurity education programs can turn your greatest threat into an asset. The more your employees know about the effects of their behavior on your company's security, the more they know how to avoid inadvertently exposing the system to threats. The more they know about the potential consequences of such breaches, the stronger your overall security becomes.

This is not an easy undertaking nor will the results be instantaneous. In fact, this is a continuous process. Just as cybersecurity threats are ever-evolving, so too must be your awareness and education efforts. There is no end to the education your employees need and to the culture changes you must make to continuously improve cybersecurity.

## GAINING BUY-IN FOR CYBERSECURITY

The first thing employees need to understand in an awareness and education campaign is that the leadership does not intend to single people out or punish them, but to keep them from being the problem and enlist them as assets in the fight against cyberattacks.

It is fine—in fact, vital—to let them know what a big problem unintentional acts by employees is in the industry, because this can introduce and communicate the true intention to ensure they do not become part of the problem.

Just as human behavior is often the cause behind many security incidents, human behavior can also be the catalyst for an improved security posture across the entire organization. It does, however, require a cultural change in which everyone on the payroll has a vested interest in better cybersecurity practices, and everyone is expected to follow the same rules.

Examples of where weak links lie can help set the stage for the cultural change in a relatable, understandable way. The introduction earlier of Rapid Response Theory provides some simple examples.

Within organizations and as an industry, healthcare needs to change this culture of impetuous helpfulness. We can still hold the door for others, but only if we check the person's badge and escort visitors to security to sign in. We can offer to look up information for that nurse in need without sharing our passwords.

The reality is that evil doesn't have rules, political correctness, or manners. And the fact is most of us don't recognize this is your organization's greatest vulnerability. You can't change the world, but you can start with your employees, and start the awareness effort with real-life examples like the following.

> In 2014, an employee at Rady Children's Hospital in San Diego intended to send a file containing a training exercise to four job applicants. Instead, the employee sent a spreadsheet with the protected health information for 14,000 patients. From there, one of the people forwarded the spreadsheet to two others, compounding the mistake.[5]

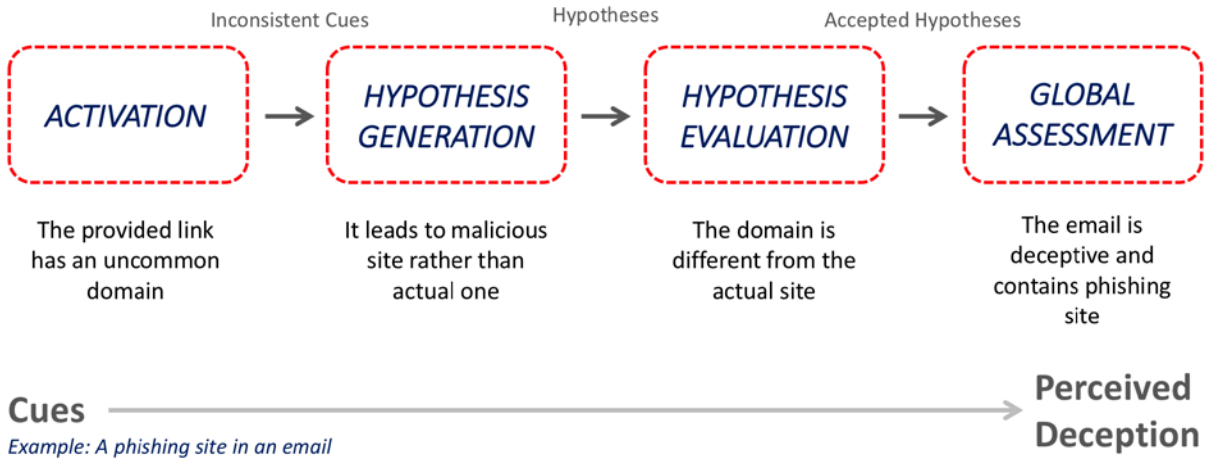
Oops. The same thing could easily happen in your organization, and that's a big oops. A Verizon report on 166 reported security events found that 32 percent were caused by lost or stolen devices, 23 percent by privileged user misuse, and 22 percent by simple mistakes like attaching the wrong file to an email.[6]

## FALLING PREY TO PHISHING & OTHER MISTAKES

By 2018, most of us think of ourselves as savvy email users. We see that a stranger from another country wants to make us instantly rich by giving us a cut of her grandfather's inheritance, and they are seeking our help getting it out of the country. All we have to do is provide a little account information so they can direct deposit the commission. Probably 99 percent of people nowadays would immediately delete that email. That is why cyber-deception on this level is becoming a thing of the past.

The modern cybersecurity environment is another matter. It is not so simple anymore. "Phishing" refers to the sending of emails designed to get the recipient to click through to a site that then installs malware onto the computer. The emails today are not coming from Nigeria, but are sophisticated messages often indistinguishable from legitimate ones (Figure 2). Studies find that people are terrible at differentiating between the two.[7]

**Figure 3: Model of Deception Detection**




*Source: Proctor RW, Chen J. (2015). The Role of Human Factors/Ergonomics in the Science of Security: Decision Making and Action Selection in Cyberspace. Human Factors. 57(5):721-727.*

Phishing emails are just one area in which human failings come into play. Actions such as choosing a password and determining if websites are legitimate both require decision making that rarely meets the security parameters IT professionals expect. That's why internal policies and protections are so important.

Another area of concern is when your employees are being used by malicious actors on the outside to gain access to your systems, and this goes back to that Rational Response Theory. We begin from a place of trust and only realize we've been dealing with evil when it's too late.

Don't believe us? Consider this true story from a man we will call John.

> *It's Sunday afternoon and the coffee shop is buzzing. Soccer moms during breaks. College students debating the world's problems. Entrepreneurs sketching out a new product. I try to engross myself in an e-book, but it isn't long before my attention is drawn to two men having a cybersecurity discussion.*
>
> *"We just installed a new threat intelligence system," says the one with the mustache.*
>
> *"Really? That rocks! We are redoing our perimeter defenses and trying to think through how we can develop better layers," responds the bald one.*
>
> *I listen for a while, collecting tidbits of intelligence, before chiming in and introducing myself, explaining what I do for a living. It isn't long before we exchange business cards (one is a CIO with a NJ-based insurance company and the other the CISO of a NYC-based finance firm) and talk more about intelligence systems. We explore the issues that prompted the rework on their perimeter and discuss the timeframe required to complete the project.*
>
> *At no point does it occur to them that I might be an evil cybercriminal with intent on bringing down their systems and stealing their data. Yet they gave me valuable information to do just that: their company, contact information, description of their system vulnerabilities, and overview of their efforts to protect themselves.*

As John reminds people when he tells this story: "This is a true story. It ends well because I eventually told the men what I do and warned them about talking to strangers in coffee shops. But then again, I'm a good person. What if I weren't?"

The truth is it takes just four steps to use your employees to gain access to your system:

- Step 1. Check your website and other open source intelligence for the names and backgrounds of your executive team and IT employees (LinkedIn is a great source for this information)
- Step 2. Find their home address, shopping patterns, clubs, and hobbies and become their new best friend, stalker, and adversary all rolled into one; easy enough to do using open source software, your team members' Wi-Fi authentication signals, and some Google maps
- Step 3. Compromise their home and personal networks, as well as all computing devices on those networks
- Step 4. Use their home network to burrow into your company's network
- Step 5. Bingo! Attack

Here are a few other ways criminals can break in:

- Book a room in the same hotel in which your CEO stays during an upcoming board meeting or conference and just "happen" to bump into her; after some conversation, the attacker knows what type of system and defenses are used, not to mention personal information about the executive and the company that can be used for additional spying

- Send your IT staff gifts that contain voice-activated recorders or software-defined radio systems
- Pose as a member of a school sports team to get to the CIO's Facebook page, and send a photo from the game that contains embedded malware

# REDUCING INSIDER THREATS TAKES AWARENESS AND VIGILANCE

Cybercriminals are always out there in the ether, on the look-out for your vulnerabilities, compromising your access credentials and finding avenues for breaching sensitive information. However insiders don't have to jump over these hurdles, because they often have as much access as they need.

Here we are talking about what we call, "The Enemy Within." Unlike cybercriminals or terrorists, these individuals are often operating from motives unrelated to financial gain. They are angry. They may have problems at work, divided loyalties between your company and another, or are trying to ingratiate themselves with their boss or someone else in the company by providing information above their pay grade. They typically have compulsive, destructive behavior and may also be having relationship, marital, or family difficulties. Keep in mind these aren't necessarily current employees; they may also be former employees who were fired, laid off, or left on their own accord but who still have an ax to grind.

They might also be after financial gain. We know of a nurse who was stealing information on patients who had been in accidents and feeding the information to an injury lawyer.

Wondering if you're the victim of an insider attack? The FBI identifies the following technological clues: [8]

- Misusing IT systems or noncompliance with corporate IT policies
- Accessing information systems or network areas without valid business reason
- Emailing sensitive information via internet without encryption
- Encrypting emails sent to private or personal accounts
- Conducting malicious activity (attacking systems, password cracking, accessing restricted information)
- Failing to turn in remote access capability such as a secure token upon termination or before an extended absence
- Attempting remote access to networks while on furlough or following termination

Then watch for more subtle behavioral clues. This would be the employee who:

- Without need or authorization, takes IP or other material home via documents, thumb drives, computer disks, or e-mail
- Inappropriately seeks or obtains IP or sensitive information on subjects not related to his or her work duties
- Demonstrates a strong interest in matters outside the scope of her duties
- Unnecessarily copies material, especially if it is proprietary or sensitive
- Remotely accesses the computer network while on vacation, sick leave, or at odd times
- Disregards company computer policies and installs personal software or hardware
- Works odd hours without need or authorization
- Makes short trips to foreign countries for unexplained or strange reasons
- Demonstrates unexplained affluence
- Engages in suspicious contacts, such as with competitors, business partners or other unauthorized individuals
- Is overwhelmed by life crises or career disappointments

Your organizational culture could also be contributing to this behavior. Missteps include providing access privileges to those who don't need them; missing or vague policies regarding working from home on projects of a sensitive or proprietary nature; a perception that security is lax and the consequences for theft are minimal or non-existent; and failing to train employees on protecting proprietary information.

You can mitigate insider threats in a variety of ways. Here's what we, and the FBI, recommend you do: [8]

- Institutionalize system change controls
- Use a log correlation engine or security information and event management (SIEM) system to log, monitor, and audit employee actions
- Monitor and control remote access from all end points, including mobile devices
- Develop a comprehensive employee termination procedure
- Develop a formalized insider threat program
- Establish a baseline of normal network device behavior
- Close the doors to unauthorized data exfiltration
- Educate and regularly train employees on security or other protocols
- Ensure that proprietary information is adequately, if not robustly, protected
- Use an appropriate screening process to select new employees
- Routinely monitor computer networks for suspicious activity
- Ensure security (to include computer network security) personnel have the tools they need

That takes care of the human insider threats. Now, what do we do about the electronic threats of their own that employees bring into the organization every day?

# GETTING A SECURITY HANDLE ON APPS & PERSONAL DEVICES

Bring your own device (BYOD) is ubiquitous across a wide range of industries, and healthcare is no exception. In the introduction to a Crowd Research Partners study published in September 2017, LinkedIn Information Security Group Founder Holger Schulze laid out a few statistics that are driving the allowance of mobile devices in the workplace: [9]

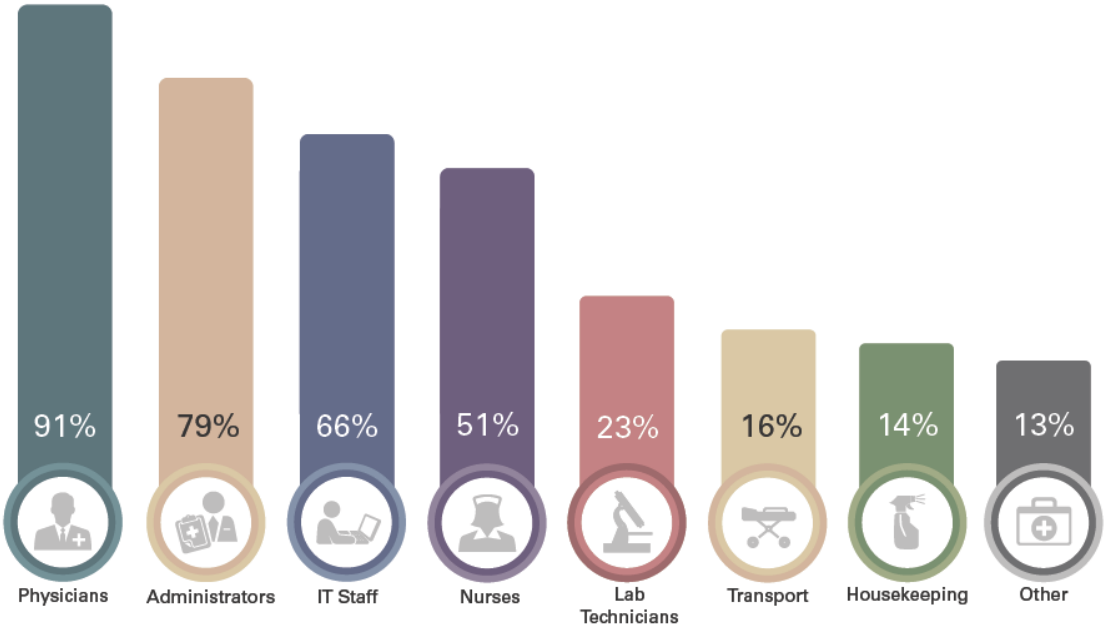
- 12.1 billion mobile devices will be in use by 2018
- Half of the world's employers required BYOD by 2017
- 67 percent of CIOs and IT professionals believe that mobility will impact their organizations just as much or more than the Internet did in the 1990s

This same study surveyed 800 cybersecurity professionals on what they felt were the main drivers of BYOD adoption. Increased employee mobility was cited by 63 percent of the respondents, followed by employee satisfaction at 56 percent and productivity at 55 percent. Sponsors of the study found it interesting that these were found to be even more important than reduced costs (47 percent).[9]

It's no wonder that not allowing BYOD at all in organizations is way down the list of options for people trying to counter the threats posed to cybersecurity. We need to come up with other solutions.

BYOD is growing in healthcare, which got a relatively early start in this arena. A 2015 survey of more than 450 healthcare organizations found that 73 percent allowed their employees to bring personal devices like smartphones and tablets to work, a slight drop over 2014. Overall, about half of all smartphones and tablets used in the health system surveyed were privately owned; and, as we know all too well, securing those devices is about as simple as moving the Grand Canyon five feet to the north.[10] Not surprisingly, physicians, administrators, and IT staff are the most common employees/staff allowed to participate in BYOD (Figure 6).

**Figure 6: Staff Members Allowed to Participate in BYOD Program**




*Source: SPOK Inc. BYOD Trends in Healthcare: An Industry Snapshot 2015. (2016). http://cloud.spok.com/IB-AMER-BYOD-2015-Survey.pdf.*

There are roadblocks within all organizations to advancing more universal BYOD adoption. According to the Crowd Partners survey, security (39 percent) and employee privacy (12 percent) are the biggest inhibitors of BYOD adoption, whereas management opposition (3 percent) and user experience concerns (4 percent) are small.[9]

The biggest concern, security, is due in great part to the vulnerabilities inherent in these devices themselves. A 2016 report from Arxan Technologies found that more than 80 percent of FDA-approved mobile health apps were vulnerable to hacking that could lead to privacy violations, personal health information theft, and tampering.[11] The same report found that 50 percent of organizations have no budget at all for mobile security.

Another report, this one from the Ponemon Institute and IBM, surveyed 640 people involved in the development and security of mobile devices and apps in their organizations (including healthcare organizations) and found that: [12]

- Sixty-five percent said the security of mobile apps is sometimes put at risk because of the rush to get to market
- Thirty-eight percent said their organizations do not scan for vulnerabilities in the app
- Fifty-five percent said they do not test apps or aren't sure if they do; even when they are tested, apps are most likely to be evaluated in development or post-development, not in production

- Sixty-one percent said their company needs to address the growing risk of malware-infected mobile apps; but, just a third said their organization has ample resources to prevent the use of vulnerable or malware-infected mobile apps
- Forty-one percent said their organization has sufficient mobile application security expertise
- Fifty-five percent said their organization does not have a policy that defines the acceptable use of mobile apps in the workplace

The survey also found that while an average of $34 million is spent annually on mobile app development, only 5.5 percent, or $2 million, is allocated to mobile app security.

Apps, of course, live on mobile devices, which pose another threat to healthcare entities. Employees and patients often connect their phones and tablets to a healthcare organization's network, creating another entry point for cyberattacks. We present the issue of employee-owned devices below.

Hospitals report that their greatest BYOD challenge is data security, which is the main reason those that forbid BYOD created the restriction. Below are other key findings from the report and our take on them:

- Just half (51 percent) of organizations have a BYOD policy
    - Question: Without a BYOD policy, how can you possibly prevent system attacks through the cell phone that belongs to the housekeeping manager? The good news is that of those that do have a policy, 89 percent cover device security and 74 percent have some type of punitive measures for not complying with the BYOD policy
- Few use any kind of mobile device management solutions to help manage security
- Just under half of hospitals surveyed (47 percent) use a secure texting solution

Having a BYOD policy is critical, and the process you go through to develop the policy will increase your cybersecurity on many levels. Answering the questions below first, before developing your policy, can show where the threats and concerns should lie, and guide you in addressing them.

## *Developing a BYOD Policy*

It starts with asking (and then answering) the right questions.

1. Why should employees be able to access your system on their own devices?
2. Who should have access to your system on their own devices? Why?
3. Will the level of access differ by type of job?
4. What devices will you support?
5. How will you educate users?
6. How will you protect patient data?
7. How will you protect your enterprise system?
8. What happens when a device is lost or stolen?
9. How will you secure apps that an employee downloads?
10. What are the repercussions for straying from the policy?
11. What kind of security system will be required?

*Note: The National Cybersecurity Center of Excellence (NCCoE), part of the National Institutes of Standards and Technology (NIST) "Mobile Device Security: Cloud and Hybrid Builds" provides information on commercially available products to help organizations manage their mobile devices. It is available at http://nccoe.nist.gov/.*

When it comes to BYOD security, health systems tend to worry about security as a privacy issue – i.e., protecting patient information from inadvertently being shared. What they should also be worrying about is the kind of security we've covered and will cover in this whitepaper series – the kind that can put every patient's physical well-being at risk.

The thing is, any time anyone brings a personal device into your facility, you can bet the device has already been compromised. You have no control over how it's been used; you can't scan it for malware; and you certainly aren't going to be able to browse through it before an employee goes home for the day. Consider the apps they download; apps provide the perfect opportunity for malware-related attacks. While all apps require that you accept their contracts before downloading—all of which contain information on security risks—just 17 percent of people even look at permissions text when downloading an app and only 3 percent read it carefully enough to answer questions about it.[7]

If you're going to allow staff (and patients, let's not forget patients!) to use their own devices to connect to your Wi-Fi, you better have policies and safeguards in place. A good place to start is with the same type of security you use to provide secure remote access to your system.

## *Mobile Device Management – Applied*

As part of our client's, a large Catholic healthcare system located across multiple locations in the Southeastern United States, Security Transformation Program, the Divurgent Team worked to implement Citrix's XenMobile Application to all mobile devices across the organization (3,500 devices for Calendar, Contacts, Email) to decrease the risk of malware, data leakage, and inappropriate use of enterprise resources and information that can occur through the use of mobile devices. All components are housed within a secure container on the mobile devices to ensure data cannot be penetrated. Here's a snap shot of the team's work:

| *CHALLENGE* | *DIVURGENT'S SOLUTION* |
|---|---|
| *Self-sufficient end user enrollment model caused additional time for device enrollments* | Allowing for a self-sufficient end user enrollment allowed resources time to focus on issues submitted; however, end users voiced some, initial, concerns with self-enrolling. As a resolution, we implemented 'cafeteria' rotations for side by side assistance during the process. This alleviated immediate angst and end users were successfully enrolling in the secure environment. |

| CHALLENGE | DIVURGENT'S SOLUTION |
|---|---|
| *Lack of understanding at the end user level of organizational security concerns being addressed within the project* | Technical 'jargon' made the overall security concerns indigestible with the standard workforce. We were able to place into consumable terms with corporate communications and this helped to arise awareness to mitigating chances of viral attacks to the client community. |
| *Outdated cell phone equipment required enterprise refresh of older model iPhones causing enrollment delays* | Attention to device refreshes for Mobile Devices was not in the forefront of leaderships attention; as such, several device models were out of date and could not support a containerized solution.<br><br>We were able to create a refresh schedule and also assist in the documentation of device lifecycle for the organization. |
| *Lack of organization security policy on iOS updates caused additional administrative overhead of ensuring iPhones were on most recent platform and could be enrolled within XenMobile* | Policies were not in place to ensure that mobile devices iOS updates were enforced and compliant with the platform releases from vendors.<br><br>We were able to work with the Security Operations Center to implement a policy to mandate updates were applied and further reduce the risk of organizations. |

## CONCLUSION

Hardware and software are vulnerable to intrusion, but they should not be the main focus of your cybersecurity efforts. These things can be patched and reengineered to harden them against threats. IT and organizational leaders need to recognize that the greatest risk to their data and information systems comes from current and former employees. This is just as important as our main point in the previous whitepaper, which is accepting today's reality regarding cybercriminals and cyberterrorists. Solving these problems requires a different kind of defense that goes beyond hardware and software. It requires considerable study and tireless teamwork, but the results will be worth the effort.

---

# ABOUT THE AUTHOR

***Emily Carlson – Principal, Divurgent***

Emily, as a Divurgent Principal, leads clients through a variety of projects and program initiatives, ranging from value-based care to mobile device management, and enterprise architecture security initiatives. She has been in the information technology field for over 20 years and has focused much of her career in the healthcare markets, including pharmaceutical, health care payer, and hospital system organizations.

Her professional sweet spot is in project management methodologies; she uses proven approaches to deliver best in class quality projects to aide strategic initiatives and grow revenue for her clients. Focused on transferring skills to her clients, Emily coaches and mentors organizations on Project Management disciplines and builds strong relationships across all levels of an organization.

Prior to joining Divurgent, Emily served as Program Director for Meaningful Use at Roswell Park Cancer Institute in Buffalo, New York. At Roswell, she had ownership of Project Managers, Requirements Analysts, and Testing resources to deliver MU2 for the organization. Emily also oversaw all aspects of Allscripts training initiatives to improve efficiencies within the physician practices.

Emily.Carlson@divurgent.com | LinkedIn

# REFERENCES

*1. Ponemon Institute. (2017). 2017 State of Cybersecurity in Small and Medium-sized Businesses. Chicago: Keeper Security.*
*2. Ponemon Institute. (2016). Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data.*
*3. Mangelsdorf, M. E. (2017). What Executives Get Wrong About Cybersecurity. MIT Sloan Management Review, 58(2), 22.*
*4. Department of Health and Human Services. (2014). Top 10 Tips for Cybersecurity in Health Care. Washington, DC. Retrieved from: https://www.healthit.gov/sites/default/files/Top_10_Tips_for_Cybersecurity.pdf*
*5.McCann E. (2014, June 19) Employee gaffe causes 2 data breaches. Healthcare IT News. June 19, 2014. Retrieved from http://www.healthcareitnews.com/news/employee-gaffes-cause-two-HIPAA-data-breaches.*
*6. Verizon. 2016 Data Breach Investigations Report. 2016. http://vz.to/DBIR16MEDIA.*
*7. Proctor RW, Chen J. (2015). The Role of Human Factors/Ergonomics in the Science of Security: Decision Making and Action Selection in Cyberspace. Human Factors. 5(5):721-727.*
*8. Nigro C. The Enemy Within: Dealing with Insider Threats. Paper presented at: Privacy and Security Forum; 2016; Boston.*
*9. Crowd Research Partners. (2016). BYOD and Mobile Security 2016 Spotlight Report.*
*10. SPOK Inc. BYOD Trends in Healthcare: An Industry Snapshot 2015. (2016). http://cloud.spok.com/IB-AMER-BYOD-2015-Survey.pdf.*
*11. Arxan Technologies. (2016). Fifth Annual State of Application Security Report.*
*12.Ponemon Institute. (2015). The state of Mobile Application Insecurity.*