eGuide

IDG Enterprise is CIO COMPUTERWORLD CSO InfoWorld ITWORLD NETWORKWORLD

CITRIX®

presents

The State of Mobile Security

Mobile payments, mobile apps, mobile health—new pieces to the increasingly complex and always changing security environment. Enterprises are struggling to keep up with mobile security demands, and one-fifth of IT pros say their companies had a mobile data breach. Yet mobile is here to stay, so organizations must shore up their security strategies.

In this eGuide, *Computerworld, CSO* and *InfoWorld* take a look at the state of mobile security and current vulnerabilities, and speak with an expert on securing the mobile minimum viable app. The eGuide also includes articles on how to reduce mobile app security risks, and the unique challenges of securing mobile health records.

One-fifth of IT pros say their companies had mobile data breach

Survey shows wide uncertainty about whether smartphones and tablets were involved.

BY MATT HAMBLEN, COMPUTERWORLD | IT pros have long been concerned about the potential for security breaches with increased employee use of mobile devices, including smartphones and tablets owned by workers who bring in their own devices from home.

A new survey of 882 IT professionals has quantified those concerns, revealing that one in five organizations (21%) suffered a security breach involving a mobile device sometime in the past, primarily due to connections to malicious Wi-Fi hotspots and malware.

The online survey was conducted by Crowd Research Partners and was sponsored by six top data security vendors: Bitglass; Blancco Technology Group; Check Point Technologies; Skycure; SnoopWall; and Tenable Network Security. All six vendors offer various approaches to protecting corporate data used by mobile workers.

The full survey is available online with registration.

Nearly one-fourth (24%) of respondents said mobile devices used in their organizations had connected to a malicious Wi-Fi hotspot in the past, while 39% said those devices downloaded malware. The responses included both worker-owned or corporate-owned devices.

Perhaps more troubling was a finding that 37% of organizations were not even sure whether mobile devices had been involved in security breaches in the past.

The survey involved 882 IT professionals who are part of the 300,000-member Information Security Community on LinkedIn. About 30% of the respondents were from the U.S., although nine other countries were represented.

Holger Schulze, the founder of the LinkedIn community, said the survey indicates that mobile security data breaches and risks are on the rise. Many companies see productivity improvements with BYOD, but those gains can be undercut by security threats and burdens placed on IT support staff to remedy breaches and monitor security.

In fact, security worries were cited by 39% of the IT pros as the biggest inhibitor of BYOD adoption, with the main worry being the loss of sensitive corporate data.

Despite such concerns, the survey found just 30% of respondents plan to increase security budgets for BYOD programs in the coming year; 37% have no plans to change their budgets.

"BYOD can be a tough nut for organizations to crack," Blancco

Many companies see productivity improvements with BYOD, but those gains can be undercut by security threats and burdens placed on IT support staff to remedy breaches and monitor security.

CEO Pat Clawson said in a statement. Some organizations worry whether to adopt BYOD without complete security controls in place, he added.

Part of the purpose of the survey is to better educate businesses about mobile security risks and remedies, he added.

Gartner and other analyst firms have long urged companies to carefully manage corporate data on workers' smartphones and tablets, whether they are corporated-owned or employee-owned. End-to-encryption of data is encouraged, along with partitioning corporate data from personal data, a feature available now on many smartphones.

The survey found that just 34% of respondents wipe sensitive data from employee devices when they leave the company. Whether the device is employee- or corporate-owned, unwiped data can be stolen by unauthorized parties, risking a worker's privacy as well as corporate and customer data.

The vendors who underwrote the survey recommended the use of enterprise-class, certified mobile data erasure software to wipe data permanently, although they didn't name any particular product. Dozens of companies offer such software.

Mobile security: The coming battle of hardware vs. software

According to security experts, there are several paths forward for mobile payments, each with its own security implications.

BY MARIA KOROLOV, CSO | I'm starting to see signs for Apple Pay and Google Wallet everywhere I go. Google just announced its Android Pay platform and deals with AT&T, Verizon and T-Mobile to preinstall it on Android phones. Samsung is gearing up for its own payment system, Samsung Pay; Walmart is planning its retailer-focused CurrentC system; and PayPal, about to spin off from eBay, has been buying up payment technology vendors and can't be counted out yet.

For consumers, the decision will likely boil down to whether they own an iPhone or an Android phone, and which apps are easier to use and accepted by most merchants.

Merchants are upgrading this year anyway, as part of a mandated transition to chip-and-pin or "smartcards" and might as well bite the bullet and go all the way to mobile payments while they're at it. Fortunately, they won't have to decide between supporting Apple's platform or Google's—adding support for one automatically means that they'll be able to accept the other.

But what about the back-end technology at work? How do they stack up in terms of security?

According to security experts, there are several paths forward, each with its own security implications.

Hardware versus software

The main distinguishing characteristic between Apple Pay and most other mobile payment platforms is that Apple Pay uses hardware-based security, a "secure element" inside the phone, protected against tampering.

On the iPhone, this is combined with a fingerprint scanner for additional security.

According to Adam Kujawa, head of malware intelligence at Malwarebytes, no unencrypted personal information is transmitted.

The only security problems reported so far are with initial onboarding, where scammers were able to talk call center operators into adding stolen credit cards to their iPhones.

In addition, thieves might, theoretically, be able to fool the fingerprint scanners and make unauthorized purchases, said Kujawa.

But the biggest downsides of Apple Pay aren't so much technical, he said, as practical. The phones are expensive, and there's no way to make a payment, for example, if the iPhone's battery is dead.

The chief alternative to the secure element is HCE, or host card emulation. It's the software alternative to hardware-based security, and uses a cloud-based tokenization process.

"From a security standpoint, HCE provides the best protection because the encryption and communication of your financial information is in the hands of a bank and there is no connection between payment info and the device itself, in case it gets stolen."

Adam Kujawa
Head of malware intelligence, Malwarebytes

"From a security standpoint, HCE provides the best protection because the encryption and communication of your financial information is in the hands of a bank and there is no connection between payment info and the device itself, in case it gets stolen," said Kujawa.

However, it could be that malicious apps will be designed to hijack the HCE process and steal money from users.

The ideal combination, said Kujawa, would be a secure element on the device, combined with HCE, combined with biometric authentication.

Mobile versus web

With all the discussion about Apple Pay and what Google and Samsung might or might not do, what actually happens is that most mobile payments have nothing to do with any of these technologies.

Instead, they are simply web-based payments made via browsers on mobile devices, or dedicated apps. For example, Amazon has a shopping app for smartphones and tablets, and PayPal has a mobile app that lets you send money to friends.

According to San Francisco-based payments company Adyen, these kinds of mobile payments account for 27% of all online payments in the first quarter of this year, a growth of 39% compared to the same period last year.

A small subset of these mobile payments are for local purchases—you can pay for your Starbucks coffee for example, or your Uber ride, by using their respective apps. These are in-person mobile payments, and totaled $3.74 billion in the U.S., according to Forrester Research. But Forrester expects them to grow faster than other kinds of mobile payments, to reach $34.2 billion by 2019.

Security-wise, the big downside to that approach is that of any web-based payment system, said Andrew Blaich, lead security analyst at Bluebox Security. If there was a data breach, hackers could potentially steal all the saved financial information about users.

"And if someone steals your username or password they can impersonate you and make payments under your name," he said.

In addition, the mobile apps themselves could be compromised, said Andrew McLennan, president of the mobile division of Inside Secure, which is based in France. This has already happened with both the Starbucks and Uber apps.

Hackers can download the apps, root their devices, switch off wireless connectivity if necessary, and then spend all the time they need to take apart and analyze the apps.

"Once they have done this they can weaponize what they learn for later, mass attacks—from simple theft to more insidious harvesting of personal data for future use, far removed from the original app," said McLennan.

It's not either-or

Because of the way that NFC technology works, if a terminal accepts one payment system, such as Apple Pay, then it will automatically accept others, such as Google Wallet. And web-based payments, such as those of Starbucks and Uber, don't depend on specialized payment terminals at all.

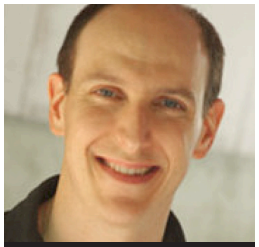
That means that neither customers nor retailers will have to choose.

"I think everything will co-exist," said Jerry Irvine, CIO at Prescient Solutions. "It's not whether NFC or HCE are better than one another, but do they fulfill the requirements of secure payments as defined by PCI and banking institutions—and both of them do."

"And you're not going to get away from companies taking payment over the Internet," he said. "If you look at Startbucks, their application over the years has not been the easiest, has not been the best, but it's the biggest thing out there right now. If people want to use something, they will use it."

Mobile security Q&A: Securing the mobile minimum viable app

As enterprises struggle to keep up with their internal demand for mobile apps, more are turning to rapid development workflows. What does this mean for security?


Potoczny-Jones

BY GEORGE V. HULME, CSO | As enterprises struggle to keep up with their internal demand for mobile apps, more are turning to more speedy development workflows, such as the Minimum Viable Product (MVP), which essentially calls for mobile development teams to focus on the highest return on effort when compared to risk when choosing apps to develop, and features to build within them. That is: Focus on apps and capabilities that users are actually going to use and skip those apps and features they won't.

Sounds simple, but what does that mean when it comes to security? We know application security is one of the most important aspects of data security, but if software teams are moving more quickly than ever to push apps out, security and quality assurance needs to be along for the process.

The flip side is minimum apps and features could mean less attack surface. To get some answers on the state of mobile app security and securing the MVP, we reached out to Isaac Potoczny-Jones, research lead, computer security, with computer security research and development firm Galois.

Potoczny-Jones has been a project lead with Galois since 2004, and is an active open source developer in cryptography and programming languages. He has led many successful security and identity management projects for government organizations including Navy, DOD, DHS; federated identity for the Open Science Grid (DOE); and mobile password-free authentication (DARPA), and authentication for anti-forgery in hardware devices (DARPA).

Q. Please tell us a little about Galois and your role there in security.
Galois is a computer security research and development firm out here in Portland, Ore. We do a lot of work with the U.S. federal government, been around since 1999, and I've been here for 11 years now. I think a lot about this topic. I really appreciate and employ myself the lean methodologies for product development, and I love the lean startup approach. I also do security analysis for companies, so I've gone into a number of startups too and looked at their security profile for their products or their infrastructure,

You have to squint to figure out how to apply nonfunctional requirements like security to a lot of these processes like scrum.

and help them to develop a security program. I've definitely seen both sides of the issue as far as where MVP thinking leads you.

Q. What are you seeing out within organizations today when it comes to mobile security?

There's definitely a lot more development in mobile happening. The best practices in mobile aren't as well developed as best practices for the web. That's getting a little bit better. Consider HTTPS. What we saw for quite some time was something that on the web is relatively straightforward, which HTTPS is. People were doing it wrong on mobile for years before anyone really noticed. There's a lot you can get wrong with HTTPS, and they were getting it all wrong. As people move over to mobile they are definitely having to relearn some of the lessons we learned over the years.

Password security is another one of those. People began to make passwords on websites a lot more robust. You can't just have a four- or five-letter password anymore on most websites. But because mobile devices are so difficult to type a password into, a lot of sites have relaxed those password rules. In reality, the threat is just the same as it always has been.

Q. What impact do you see the minimum viable product, or minimum viable app, trend having?

On the MVP front, there's a very fascinating challenge with security because security is a nonfunctional requirement. I tend to like the lean scrum methodology. I don't know if you're familiar with that one, but I can use that one as an example. They're all kind of similar in some ways. They emphasize features, they emphasize things the users can see. They emphasize testing out ideas, and getting them into the market. Testing them, gathering metrics about how effective they are, and using that as feedback into the product. That's a really good idea about how to develop a product. Even just the terminology, minimum viable product, it is really emphasizing minimizing.

It emphasizes getting rid of what you don't need. Those things together, minimizing things and really having an emphasis on what the user can do and see, that makes it so that nonfunctional requirements are kind of an afterthought. You have to squint to figure out how to apply nonfunctional requirements like security to a lot of these processes like scrum.

Q. I would imagine with an MVP teams want to move the app out as quickly as possible, so they don't spend a lot of time threat modeling and going through a lot of additional process, because that's all adding to development time. So there seems to be a natural friction between the goals of MVP and good security.

It's absolutely a friction. It's challenging because securing is mostly invisible. That means good security and bad security look exactly the same, until something goes wrong. Security is really visible when something is broken or somebody gets hacked and then you make the news. Then it kind of blows up in your face. We've seen this a few times, I don't know how many startups it's killed—it's probably killed a few—but it's definitely cost a lot of startups when their first major news coverage is that they were hacked.

Q. What are some ways organizations can ease that tension when it exists? Is there a way to bring security in so it's not too obtrusive? Is there a way to separate out apps by data type? And possibly greenlight MVP apps that don't touch more sensitive data, and give a closer look at those apps that do?

I think that's a good approach. As you point out, one way is to say, let's see if we can do an MVP with data that's not as sensitive so you won't have to focus as strongly on security.

Nowadays, it's a little more challenging. Even the minimum things you do you will need security. It kind of doesn't matter what your data is; you will get targeted, you will get attacked, and even if it's just with these automated bots that run around the Internet attacking everything. They'll use your infrastructure for sending spam at the very least, if that's all they can do. To me, the approach is you have to implement some of the industry best practices as far as the OWASP Top 10. You have to believe that security is an important part of a minimum viable product to start to even begin to get these user stories in there.

What I like to tell people is think about user stories, even negative user stories or things like that are, as a user, I don't want to see my personal information leaked on the internet because I've shared something sensitive in your app or your website, I've stored something sensitive in your website. I don't want to see that in the hands of people who will use my private information against me.

Q. Seems like a security team could put a guide together, or put in place an app checkpoint. For instance, if an app meets one or more conditions, it must go through a security review; if not, it's OK to take a 'security-light' approach, as long as it fits within the guidelines.

That'd be perfect. Typically these lean approaches have at least some kind of testing methodology built in, or acceptance testing. Or, as some of them say, "What's your definition of 'done'?" The first step is just saying, "We're going to include security in these definitions of done," and once you've at least penetrated that level, which I don't think a lot of people have, but once they get that, then they're going to at least do the right things. You're either going to start to build it either into the user stories or the acceptance testing.

But you can't leave it to just be at the end of the process. If you leave security acceptance testing toward the end, and naturally your schedule is going to slip. Then you'll get to the security testing and find there's a lot more work to do. Then you'll be in this unfortunate decision of either having to fix things and let your schedule slip, or choose to let something go out the door that's not secure.

The real tragedy is when a system is kind of inherently insecure; it was built in a really insecure way that requires major rework, because you didn't think about security at the beginning. A lot of things are easy to add at the end with security, but sometimes you run into systems that are just kind of broken from the foundation. As with any of these things, the later you catch it, the costlier it's going to be.

Q. What are some indications organizations could look for that would indicate that they're doing this right?

If you're looking at your to-do list, whatever that to-do list is, whether it's a list of stories or a big list of tasks and action items, you should be recognizing some security issues in there, as you go. You'll get to a point, you're developing something and one of your developers hopefully will say, "Well, look, our system is vulnerable to whatever cross-site request forgery, cross-site scripting attack. Which any system that's not designed to protect against it, is going to be.

If you look at your bug list, you should see that pop up there at some point. Some of these security issues will come up during development, because nothing will be perfect. That'll be an early indicator.

If you don't have anything, if you look at your bug list and you don't see anything, if your developers aren't actively talking about security or saying, "We're going to have to add some tasks for security," you're going to say, "Well, I want to add that feature for you but that's going to have an impact on security." If you're not hearing it as part of the conversation, then there's going to be a problem.

Mobile app security grabs feds' attention

A report from NIST outlines key areas where businesses can reduce security risks in their use of mobile apps.

BY PAUL KRILL, INFOWORLD | Recognizing the increased use of mobile apps at businesses, the National Institute of Standards and Technology (NIST), a U.S. government agency, has come forward with recommendations on vetting security of these applications with steps ranging from risk management to testing.

In the January report, NIST notes how mobile apps can provide "unprecedented" connectivity between employees, customers and vendors. The apps also offer unrestricted mobility, as well as improved functionality and real-time information sharing.

At the same time, NIST points out concerns. "Despite the benefits of mobile apps, however, the use of apps can potentially lead to serious security issues. This is so because, like traditional enterprise applications, apps may contain software vulnerabilities that are susceptible to attack," the report says. "Such vulnerabilities may be exploited by an attacker to gain unauthorized access to an organization's information technology resources or the user's personal data."

NIST advises development of security requirements on issues such as securing of data and acceptable levels of risk. Specific recommendations are offered for the planning, app testing and app approval/rejection processes. For planning, key recommendations include:

- Performing a risk analysis to understand the potential security impact of mobile apps on computing, networking and data resources
- Documenting mobile device hardware and operating system security controls and identifying which security and privacy requirements can be addressed by the device itself
- Documenting mobile enterprise security technologies, such as mobile device management, and identifying security and privacy requirements that can be addressed by these technologies
- Reviewing the organization's mobile security architecture
- Developing application security requirements by noting general and context-sensitive requirements
- Procuring an adequate budget for vetting of applications

In the testing realm, NIST advises:

- Identifying general app security requirements
- Selection of testing tools and methodologies for determining the satisfaction or violation of general app security requirements
- Reviewing licensing agreements associated with analyzers and understanding security implications and licensing issues

"Despite the benefits of mobile apps, however, the use of apps can potentially lead to serious security issues. This is so because, like traditional enterprise applications, apps may contain software vulnerabilities that are susceptible to attack."

NIST Special Publication 800-163

- Ensuring that apps transmitted over the network use an encrypted channel and that apps are stored on a secure machine at the analyzer's location. Only give authorized users access to that machine.

For app approval/rejection, recommendations include:

- Identifying criteria for vetting context-sensitive app security requirements
- Monitoring public databases, mailing lists and other publicly available security vulnerability reporting repositories
- Training auditors on security requirements and interpretation of analyzer reports and risk assessments

The report also covers Android and iOS vulnerability types, as well as testing approaches and understanding the limitations of vetting. NIST touches on traditional vs. mobile security issues too. "Mobile devices provide access to potentially millions of apps for a user to choose from. This trend challenges the traditional mechanisms of enterprise IT security software where software exists within a tightly controlled environment and is uniform throughout the organization."

Securing mobile health records remains a significant challenge

Healthcare organizations are investing big into mobile medical records, but are they keeping them secure?

BY GEORGE V. HULME, CSO | Fewer enterprise technologies are growing more rapidly than mobile health (mHealth) software and devices. Healthcare organizations are investing heavily in their mobile devices and applications, a market that will grow from its current size of $10 billion to $31 billion by the year 2020, according to market research firm Research 2 Guidance. Healthcare organizations hope that mHealth will enable their front-line providers to have the access to the information they need wherever they may need it.

Criminals have also taken notice. A quick search of the Privacy Rights Clearinghouse data breach database finds that since 2005 there have been 1,889 healthcare data breaches that have been made public consisting of 421,885,347 medical records exposed. Ponemon Institute's Annual Benchmark Study on Privacy & Security of Healthcare Data estimates that criminal attacks aimed at healthcare data have risen 125% since 2010.

When it comes to security, mHealth poses some unique challenges. Many medical devices and apps can't be patched as swiftly as traditional enterprise systems because device certifications forbid it, clinical environments are chaotic, and many clinical environments are understaffed when it comes to security and IT.

"This is a big problem because the healthcare industry today isn't even good at securing traditional environments. There's the potential for security and privacy lapses when the healthcare records move between different providers," said Amrit Williams, CTO at CloudPassage. "That breaks the chain of trust. You could have service providers with access using different forms of transporting and encrypting the data. The data may be stored locally, which increases the potential for compromise if the device is lost or stolen."

"People don't think of hospital equipment as being a source of security issues, but with many of these devices having mobile capabilities and storing data (part of the healthcare Internet of Things), the potential for hacking is great," said Ciaran Bradley, chief product officer at mobile network security firm AdaptiveMobile. "Many of these devices have only the basics in security—such as password protection or firmware that may or may not have regular updates, leaving diagnostic and other data at risk."

The U.S. Food and Drug Administration has taken notice of the weak security in clinical devices, and published draft cybersecurity guidance that is directed at medical device manufacturers and how they can better assess and respond to security-related device flaws.

Many medical devices and apps can't be patched as swiftly as traditional enterprise systems because device certifications forbid it, clinical environments are chaotic, and many clinical environments are understaffed when it comes to security and IT.

Beau Adkins, co-founder and CTO at Light Point Security, said healthcare environments are also facing many of the security hurdles other types of enterprises face when trying to secure mainstream mobile devices, including relatively immature mobile operating systems when it comes to enterprise device management and security capabilities. "Security was not at the top of the list of priorities. Stock Android devices are notorious for coming bundled with what basically amounts to spyware," Adkins says.

There are mitigations, of course, Adkins pointed out, many of which are detailed in depth in this NIST Special Publication 1800-1b Securing Electronic Health Records on Mobile Devices, which stresses detailed risk assessment and appropriate security controls to mitigate risk in these environments.

It's not as if healthcare organizations haven't tried to keep their networks and mobile apps secure. They have. It's just that many didn't go about it well—at least not initially.

Gary Sheehan, chief security officer at technology and security services provider ASMGi, explained most healthcare organizations tried to keep data safe by instituting restrictive use policies. But that's changing, Sheehan said, as advanced hospitals and healthcare providers are now embracing innovation, and are relying more on secured and encrypted environments on cloud and mobile platforms to do so. "There's a lot to think about to keep everything secure and a healthcare environment compliant, but we've seen more and more organizations find it is worth the effort," Sheehan said.

"The key to creating a successful, secure environment is to build a system that allows doctors and nurses to continue doing exactly what they want to do—just to put the right tools in place to help them do it the right way," Sheehan said. "Hospitals and organizations can install layers of security into mobile devices, securely use cloud services, and track data access usage. The real challenge is making sure the apps used on the phone and within the cloud are both secure and easy to use. Ease of use is critical. If it's not convenient, people will naturally look to find an easier way or they simply won't use the technology."

Tom Davis, CTO at LANDESK, advises healthcare IT teams on things they need to do, such as ensuring mobile devices are hardened, that software is patched and up to date, that an accurate enterprise inventory of assets is in place. Davis said that it's especially important that healthcare organizations centrally manage data and not allow data to be downloaded onto endpoints. In addition, healthcare providers need to remember to continuously educate their employees when it comes to secure mobility and encourage swift data breach notification.

"With data on them, when a loss happens or if someone had unauthorized access, it's best to be informed quickly by the users without penalty to them or fear of action against them. Create the right privacy responsibilities with your mobile employees to lessen the time to notify," he said.

"The model to move to is to store the data in the cloud where it is encrypted and secure until the mobile app accesses it and not stored locally at all," said Williams.

Sounds simple, but that doesn't mean it's easy. And if recent history of healthcare breaches are any indication, it's going to take some time to mitigate the risk of there continuing to be a great many healthcare breaches.

Is mobile the new squirrel?

Mobile is just the newest piece to the always changing puzzle of security.

BY KACY ZURKUS, CSO | Perhaps you've seen the Disney film, *Up*, and you remember Dug the talking dog. Despite his ability to speak, Dug often became distracted at the sight of a squirrel. In the same way, security professionals are often distracted by the challenges mobile devices present.

While the power and capabilities of mobile devices continue to grow, you cannot afford to let it distract you from securing the laptops, gateways and many other parts of the extended network.

Because there are daily new threats to Android and Apple, said Dave Barton, CISO, Forcepoint, "Security practitioners are always working through that mobile risk model in their heads. How do we protect end points? Those end points are all different and personally owned and might not be compatible with software we want them to use."

What to protect and how much to classify is most relevant for mobile or end point or any part of the extended network. "You need tools in place that will block it from moving across the network or being moved off the network," said Barton. There is no one silver bullet. Strong security requires various data theft protection tools.

Different protection tools can be set to manage and limit access to data, said Barton. "There are tools that you can say, 'for this type of data don't allow it to be used for a USB device. Don't allow it to be printed.' Other tools let you segment mobile so that the data is protected," Barton explained.

Whether your information is on a laptop, iPad or any other mobile or network device, you want to know what you are protecting. "If you have credit card information, that database of credit cards is the first priority," said Barton.

For healthcare organizations, records are the first priority, especially any information around HIPAA. For other organizations the top priority might be intellectual property. "Whatever the business is, you need something that will interpret the handheld device and evaluate that against your data," said Barton.

Good security means knowing the business and the data that you are protecting and understanding the tools you need to secure the crown jewels. "In the data theft prevention category, they build their tools so that if they are tampered with things are taken away," Barton said. Spending money on tools without knowing the abilities they have and how those technologies will work for your business does not create strong security.

"I encourage everybody who practices security to focus on what's the most important thing. What are you most concerned about protecting? Security practitioners need to focus on what is important to their company," Barton said. Every security professional should know what a loss of data is going to cost the enterprise. Will they lose market share or will it cause a public uproar?

"Focus on what's important. If key data is in a single server, that is where you start protecting," said Barton. "For new folks, it's tough. They probably haven't learned a good risk management program," he continued.

Part of the challenge for security practitioners is getting out to

There is no one silver bullet. Strong security requires various data theft protection tools.

the business and building a relationship with the business. “The bottom line is, if the business isn’t there, they don’t need me,” said Barton. “Go find out what makes the company tick. What makes the money.”

Particularly for those who are new, the best first step you can take is to go out into the business and ask a lot of questions that focus on the big picture. Barton said, “As you are able to narrow down, then you can go figure out where they are at and how you can protect them.”

Barton said reading security website resources is another way to learn the industry. “They need to know what kind of cyber security framework should be in place and which tools will help them mature their own personal skill sets quicker, which will help them answer that question more effectively.”

Mobile is distracting because it causes security practitioners to rethink how they protect and give end users what they want in a secure fashion. Barton said, “I’m a security practitioner, but I have a passion for what we do as a company. We focus on protecting that data at end point and in transit.”

The mission of every security professional is to protect the data no matter where it sits. As technology continues to evolve in ways we’ve yet to even imagine, keep the focus on securing the data.