Mastering mobility: Keeping data secure in a fast-moving, fluid environment

Sponsored Content
Jan 27, 2017, 11:27am CST

The ability for employees, business partners and customers to access company data while on the go presents new challenges for the professionals responsible for keeping that information secure. In order to better understand the challenges inherent in an increasingly mobile economy, the Milwaukee Business Journal recently assembled a panel of experts to explore cybermobility and its potential risks for businesses.

GARY LATO (MODERATOR): WHAT ARE SOME OF THE KEY CYBERSECURITY RISKS ASSOCIATED WITH MOBILE WORKFORCES? DO THEY VARY DEPENDING ON THE SIZE OR COMPLEXITY OF THE ORGANIZATION?

NATHAN LASNOSKI: The market is going through a digital transformation in which every business is becoming a technology business. This increases the extent to which mobile security risks impact businesses and their reputations. Five or six years ago, companies spent a lot of time building firewalls around their network. Now, the expectation is ubiquitous connectivity, where employees and consumers are continuously connected to the information sources they need. This has changed the focus from securing the network to securing the content itself.

SCOTT VANDERSANDEN: A large company may have greater exposure and be a bigger target, but a breach may not be as damaging as it would be for a smaller company. If a small firm's intellectual protocol is compromised, its business could be in jeopardy. Larger companies may be better positioned to take a hit, but they also have much greater exposure. If you have 250,000 employees and each employee has one, two, three or four devices that can access the network, then you have more than a million access points. You have to make sure that all of the devices are layered for security.

THOMAS BURNETT: The risk of a breach in some ways is greater for a larger company because there are so many employees, so many access points, and because large companies are always going to be a big target of intentional efforts to compromise data. Smaller companies, however, possess a lot of sensitive information as well, and a breach may be more of a problem because they don't have the resources that large corporations do.

MODERATOR: THERE IS NOW A LOT OF DATA IN THE CLOUD AS WELL AS CLOUD APPLICATIONS AND SOFTWARE SERVICES. WHAT ARE THE BENEFITS AND RISKS OF USING CLOUD STORAGE AND/OR CLOUD-BASED APPLICATIONS?

BURNETT: The benefits of cloud storage are fairly obvious. It allows the mobile workforce to exist. I can be 500 miles from my office and access the information I need as if I were sitting at my desk in Milwaukee. The risk is that when you rely on cloud-based applications or service providers, you are outsourcing some of your security protocol, so it's important that you conduct proper due diligence to make sure you know how your data is going to be protected. That can be beneficial, though, because it allows you to shift some risk through careful contracting, You also need to know that, if something goes wrong, you know how it is going to be fixed and who—between you and the service provider—will be responsible for the cost.

MODERATOR: HOW DOES CYBERMOBILITY AND CLOUD STORAGE IMPACT THE WAY BUSINESSES LOOK AT DATA SECURITY?

LASNOSKI: There is an interesting paradigm shift in the way we protect information. The traditional focus has been on securing the container in which the data is stored, whether it is a file in a locked file cabinet or data stored on a secure, internal network.

The problem with this traditional approach has been securing that data when it is outside of its container; for instance, when it is shared with one person, but is not supposed to be shared with others. The modern security approach focuses on protecting the data itself, not the container in which it is stored. Access to the data is based on the person's identity.

VANDERSANDEN: That's a very interesting point. Smartphones are amazing because of their capabilities, but they are difficult to secure. We are constantly working with device manufacturers to improve the way security is included in the way devices are built or developed. That said, smartphone users prefer that their devices simply allow them to access their cloud-stored data rather than contain any data themselves. That way, no one could access their valuable data if the devices were stolen or left in a coffee shop.

MODERATOR: ARE SECURITY PROTOCOLS CHANGING AS WELL?

LASNOSKI: People are moving away from the idea that a password alone is sufficient. A lot of companies are implementing multi-factor authentication where the user must provide a password and a generated pin that is texted or emailed to them when they seek to access data. People are always going to have terrible passwords, but if you put in additional layers of authentication, biometrics and touch ID, you are going to have more protection.

VANDERSANDEN: Biometrics is the next frontier. I don't know if you can go much beyond that.

MODERATOR: TOM, YOU TOUCHED ON THIS BEFORE, BUT WHAT DUE DILIGENCE SHOULD COMPANIES DO IF THEY RELY ON EXTERNAL, THIRD-PARTY DATA STORAGE OR CLOUD-BASED, BUSINESS-CRITICAL APPLICATIONS?

BURNETT: At the most basic level, you need to ensure the appropriate security features are there and that you know what is going to happen if something goes wrong. Who will be the point person for coordinating and paying for the response, including a forensic investigator if necessary? Whose general counsel will be responsible for ensuring compliance with all of the varying state data breach notification requirements? Every state has different notification laws, which are triggered if the breach exposes personally identifiable information of customers, employees, or others. One of the things we advise our clients when they are entering into an agreement with a service provider is to make sure their contract clearly defines who owns the data, which is important for a lot of reasons, including for purposes of determining, from a legal perspective, who is responsible for notifying affected individuals in the event of a breach, and the cost that comes with it.

MODERATOR: OVER THE LAST DECADE, WE HAVE SEEN A MOVEMENT FROM CORPORATE-ISSUED PHONES AND LAPTOPS TO MORE AND MORE PERSONAL DEVICES BEING USED FOR BUSINESS PURPOSES. I HAVE THREE DEVICES THAT HAVE BOTH PERSONAL AND BUSINESS INFORMATION ON THEM. HOW CAN COMPANIES PROTECT THEIR DATA AND NETWORKS FROM POTENTIAL SECURITY BREACHES CAUSED BY EMPLOYEE PHONES AND OTHER PERSONAL DEVICES?

VANDERSANDEN: Personal devices add another layer of exposure that is very difficult to protect against, even if someone assures you that they can partition the device and isolate personal and business data. At AT&T we look at it very cautiously. We require our employees to have separate personal and business devices. There are some exceptions, but they are very, very few.

MODERATOR: WHAT CAN COMPANIES DO TO OVERCOME EMPLOYEES' AMBIVALENCE TO MOBILE SECURITY ISSUES?

VANDERSANDEN: It's a challenge because most people are more concerned about conveniently accessing data than they are security. If someone uses their phone to pay for something, that opens a channel that can be very difficult to firewall. It's important to ensure that company devices are equipped with mobile device management services to help secure applications that store proprietary company data. That way your organization can update security policies in real time across all company devices. Using virtual private networks for company email and applications can also add another layer of security for mobile networking.

BURNETT: It is important to get employees to fully appreciate why multiple layers of security are necessary. There will always be a hole in the security you put in place and if they don't buy in, they are going to look for a work-around and you are going to be vulnerable. At first employees may be annoyed when they have to run to get their phone to sign in with a text code to verify their identity when trying to log in, but if they understand and appreciate why that's important, eventually it will become second nature.

LASNOSKI: Because the percentage of people who have a security mindset is relatively low, companies need to proactively protect their digitally-accessed documents. The onus is on the employer to provide governance over the use of personal devices and for providing different layers of protection depending on the content. Modern management technologies do allow companies to wipe out business data without impacting any personal data on the device; however, everything that a company can do to a personal device needs to be spelled out in their human resource policies.

MODERATOR: WHAT IS BEING DONE TO IMPROVE CYBERSECURITY AT THE NETWORK LEVEL?

VANDERSANDEN: AT&T began re-engineering our network five or six years ago into something we call the software-designed network. We took much of the intelligence out of the hardware and put it in the software, which makes it much easier for us to make wholesale changes. We are doing the same thing with security. We are making various levels of security a component on the network, almost like an app. Virtualized defenses let us deploy and scale security in near real-time across our network. We can also provide customers with security policy deployed and updated when and where the customer needs it. The customer can select and adjust the level of security they want based on their company needs, and security solutions are then activated through software updates, like downloading a new application or application update.

LASNOSKI: One of the biggest transitions we have seen is the emergence of technologies like machine learning that can be used to see if someone is taking advantage of your network. There is simply too much data for an individual to make heads or tails out of it. Machine learning uses artificial intelligence to determine what is normal, then looks for changes from the norm and applies defense techniques against the threat.

MODERATOR: MACHINE LEARNING BRINGS TO MIND THE INTERNET OF THINGS. WHAT ARE SOME OF THE "WHAT'S COMING NEXT" ISSUES THAT COMPANIES NEED TO BE THINKING ABOUT WHEN IT COMES TO THE INTERNET OF THINGS AND OTHER CHANGES?

VANDERSANDEN: The internet of things is going to generate unforeseen amounts of data given the number of devices that will be talking to each other. That is going to create a lot of new challenges, making it essential that security is layered in through devices, networks, and applications.

BURNETT: We could probably have a weeklong session on the internet of things and the complexities that are introduced by the increasing connectivity it brings. As we become more connected, data security will become both more important and more difficult. And it is already hard for companies to know just how much is enough in terms of security efforts. There hasn't been a lot of guidance from courts on the threshold measures a company needs to implement to protect itself from liability, but regulators, including the FTC, are ramping up enforcement activities because they know the risk is there.

LASNOSKI: The digital transformation that is driving the internet of things greatly increases the risks for companies that aren't focusing on security. Even the perception that the technology they are using has opened up individuals to greater risk will impact their product. The onus is on the business to invest in the operating system, the application, the communication channel and the content protection to make consumers confident in their business. We advise our clients to leverage the NIST cybersecurity framework, which was developed by the government to protect power plants and covers identification, protection, detection, response and recovery. If a company does that, they will be able to prioritize activities to mitigate risks and protect customers, partners, and employees from themselves.

MODERATOR: DO YOU HAVE ANY FINAL THOUGHTS ON WHAT COMPANIES CAN DO TO MITIGATE THE RISKS ASSOCIATED WITH CYBERMOBILITY?

LASNOSKI: As a consumer, you have a responsibility to be an intelligent, security-aware consumer. As a business, you also have the responsibility to be an intelligent, security-aware company. If you are intentionally approaching your security challenges with modern approaches and technologies, you are a step ahead of others and going in the right direction.

VANDERSANDEN: Get a professional assessment of your risks and develop an end-to-end solution that addresses your risks on all of your platforms. You don't have to be smart enough to do it yourself, but you have to be smart enough to get it done. And you can't just buy something, implement it, and then put it on the shelf. It needs to be kept current. Make sure the operating systems on all of your devices are as current as possible. Every new operating system closes the loopholes that were found in the old system. With each new operating system, you are closing the doors to hackers.

BURNETT: It can be intimidating. It is a pretty weighty endeavor.

VANDERSANDEN: And costly.

BURNETT: I think that is why businesses aren't always as proactive as they should be about data security. They don't want to incur the time, burden or costs of identifying their shortcomings on a continuous basis, but they need to do it.

VANDERSANDEN: As we think about these things, we have to remember that there are practical limits to what you can do to make your data completely bulletproof. No matter what we are doing, or what any network provider is doing to secure and insulate their network, there are a group of people out there who are trying to break it. It is a cat-and-mouse game that will never end. □

TABLE of EXPERTS

SCOTT T. VANDERSANDEN

AT&T

A 28-year veteran of AT&T, Scott T. VanderSanden was appointed to the Wisconsin president's position in November 2006. He worked closely with the Wisconsin State Legislature on Act 42, the Video Competition bill. VanderSanden led AT&T's efforts to support the Telecommunications Modernization Act of 2011. With this legislation, the Wisconsin Legislature further modernized the industry in an effort to adapt to the realities of today's commerce.

NATHAN LASNOSKI

Concurrency

Nathan is the Chief Technology Officer at Concurrency, a national technology solutions company headquartered in Brookfield, WI. He is responsible for helping customers realize the value of Digital Transformation through an inventive set of integrated technology consulting services. Nathan is responsible for what Concurrency delivers, how it is delivered, and the operational delivery of technology services.

THOMAS BURNETT

Reinhart Boerner Van Deuren

Thomas Burnett is a shareholder in Reinhart's Litigation Practice where he specializes in complex commercial litigation, particularly in the areas of product liability, product distribution, and privacy and security. Tom helps clients in a wide range of industries evaluate and manage risk, including risks presented by new and emerging technologies, to assist them in making business decisions with the goal of avoiding litigation.

MODERATOR, GARY LATO

Hudson Business Lounge

Gary Lato, Co-Managing Partner of Hudson Business Lounge, also advises numerous national nonprofits and small business startups. His career in metro Milwaukee includes stints with manufacturer Generac Power Systems and accounting firm Price Waterhouse. Gary and his team at Hudson strive to build a vibrant place where the confluence of creativity, relationships, and projects leads to member success.

Table-of-Experts.jpg

TABLE of EXPERTS

SCOTT T. VANDERSANDEN

AT&T

A 28-year veteran of AT&T, Scott T. VanderSanden was appointed to the Wisconsin president's position in November 2006. He worked closely with the Wisconsin State Legislature on Act 42, the Video Competition bill. VanderSanden led AT&T's efforts to support the Telecommunications Modernization Act of 2011. With this legislation, the Wisconsin Legislature further modernized the industry in an effort to adapt to the realities of today's commerce.

NATHAN LASNOSKI

Concurrency

Nathan is the Chief Technology Officer at Concurrency, a national technology solutions company headquartered in Brookfield, WI. He is responsible for helping customers realize the value of Digital Transformation through an inventive set of integrated technology consulting services. Nathan is responsible for what Concurrency delivers, how it is delivered, and the operational delivery of technology services.

THOMAS BURNETT

Reinhart Boerner Van Deuren

Thomas Burnett is a shareholder in Reinhart's Litigation Practice where he specializes in complex commercial litigation, particularly in the areas of product liability, product distribution, and privacy and security. Tom helps clients in a wide range of industries evaluate and manage risk, including risks presented by new and emerging technologies, to assist them in making business decisions with the goal of avoiding litigation.

MODERATOR, GARY LATO

Hudson Business Lounge

Gary Lato, Co-Managing Partner of Hudson Business Lounge, also advises numerous national nonprofits and small business startups. His career in metro Milwaukee includes stints with manufacturer Generac Power Systems and accounting firm Price Waterhouse. Gary and his team at Hudson strive to build a vibrant place where the confluence of creativity, relationships, and projects leads to member success.