

ESO - Security Trends Report

10/11

Legal risks abound for firms without a mobile device security policy

Eric B. Parizo, Sept 20, 2011

ORLANDO -- Enterprises that issue, support or simply grant access to mobile devices without first putting a stringent [mobile device security policy](#) in place are setting themselves up for not only potential data loss, but also a myriad of nightmare legal entanglements.

That was the message from A. Spencer Wilcox, supervisor of compliance services for Constellation Energy, during a presentation Monday at the (ISC)² Security Congress.

Before ever permitting an employee to [access corporate networks and data with a mobile device](#), Wilcox said, enterprises should mandate that employees sign a written agreement to abide by the organization's [mobile device security policy](#) and all other applicable policy statements. That document should state that the company retains the right to any corporate data on the device, including usage and location data, and that it may share that data with third parties if necessary.

That level of submission may seem unusual or unnecessary, but Wilcox explained how a variety of legal precedents sets the stage for companies to pay a heavy price if the wrong set of circumstances occurs involving employee use of mobile devices.

For instance, in the 2009 case of [LVRC Holdings LLC v. Brekka](#) (.pdf), a rogue employee stole data from his company-issued device in order to advance his career. The company sued the employee, citing a violation of the Computer Fraud and Abuse Act, but the U.S. Ninth Circuit Court of Appeals ruled in favor of the employee, Wilcox said, largely because the organization hadn't properly defined what actions constituted violation of its policy and, in turn, revocation of the employee's access rights.

"The court said, 'You gave the employee permission to act as he saw fit,'" Wilcox said. "Therefore he's allowed to use the computer without restraint. He had a blanket authorization. He can do anything he wants with your data because you didn't set limitations on it."

Wilcox also encouraged companies to have a policy that forbids engaging in phone conversations with employees who are driving. An Indiana court last year ruled that a mother who knowingly spoke with her daughter while the daughter was driving was equally negligent for the accident her daughter caused while on the phone.

The implication for enterprises, Wilcox said, is companies that issue phones to employees and then expect them to be available anytime, anywhere for a phone conversation, including on the roadways, could be exposing themselves to legal liability should an accident occur.

Another potentially worrisome scenario without a specific legal precedent tied to it involved pictures taken with corporate-owned or managed devices. Wilcox said many people don't realize digital photos have embedded metadata that includes information about the photo; that data can include latitude and longitude data of where the device was when the photo was taken if the device that took the picture has [GPS capabilities](#).

The takeaway, Wilcox indicated, is that attackers can easily harvest that data to reveal the location of something they want to get their hands on.

Wilcox admitted that the pervasive nature of mobile technology today and the emergence of popular new devices like iPhones and iPads make it difficult to deny access to mobile devices outright, meaning some legal liability and risk of data loss will always be present, but he encouraged organizations to use technology, policy and controls to limit data exposure.

Attendee Krister Samuelsson with Volvo Sweden said his organization has a mobile device security policy in place, but the process of managing that policy is challenging because it extends across numerous countries. Because the legal landscape is different in each nation, geographic policy exceptions are commonplace, increasing the difficulty of ensuring employees adhere to policy.

Social engineering attacks costly for business

New research from Check Point Software finds social engineering is now a common attack strategy and organizations are getting hit frequently by hackers

[Joan Goodchild](#), Senior Editor

September 21, 2011 — [CSO](#) —

[Social engineering](#) attacks are widespread, frequent and cost organizations thousands of dollars annually according to new research from security firm Check Point Software Technologies.

A survey of 850 IT and security professionals located in the U.S., Canada, U.K., Germany, Australia and New Zealand found almost half, 48 percent, had been victims of social engineering and had experienced 25 or more attacks in the past two years. Social engineering attacks cost victims an average of \$25,000 - \$100,000 per security incident, the report states.

"Socially-engineered attacks traditionally target people with an implied knowledge or access to sensitive information," according to a statement from Check Point on the survey. "Hackers today leverage a variety of techniques and social networking applications to gather personal and professional information about an individual in order to find the weakest link in the organization."

Among those surveyed, 86 percent recognize social engineering as a growing concern, with the majority of respondents, 51 percent, citing financial gain as the primary motivation of attacks, followed by competitive advantage and revenge.

The most common attack vectors for social engineering attacks were [phishing emails](#), which accounted for 47 percent of incidents, followed by [social networking sites](#) at 39 percent.

New employees are the most susceptible to social engineering, according to the report, followed by contractors (44 percent), executive assistants (38 percent), human resources (33 percent), [business leaders](#) (32 percent) and IT personnel (23 percent). However, almost a third of organizations said they do not have a social engineering prevention and awareness program in place. Among those polled, 34 percent do not have any employee training or security policies in place to prevent social engineering techniques, although 19 percent have plans to implement one, according to Check Point.

IT managers start supporting employee-owned smartphones

Still, about a third of companies frown on using personal smartphones for work tasks, Forrester finds

By **Matt Hamblen**

September 20, 2011

Computerworld - Despite the increasing use of [smartphones](#) at work, more than a third of companies still provide no support for personal phones or outright prohibit their use at the office.

This was a finding by Forrester Research in a recent survey of 1,051 IT managers in North America and Europe. The data found that while 26% of the companies don't provide support for personal mobile phones and smartphones, another 10% prohibit the use of personal devices, for a total of 36%.

At the same time, about 16% of the IT managers surveyed said their companies support all kinds of personal

devices, while 14% support only certain types and models.

Some companies have developed long sets of policies for when and how to support personal devices used by workers. The most progressive companies are investing in mobile device management (MDM) software, available from many vendors, to track employee devices and the applications used on them. This software also has the ability to wipe sensitive data off of a lost device.

Forrester said in a new research note that increasing numbers of employee-owned devices and questions of supporting them are "crippling" existing mobile strategies. The effect has led companies to rethink their strategies and to begin supporting both company-owned and employee-owned devices.

Forrester said that nearly 600 of its clients asked for advice in the past six months, including ways to support employee-owned devices. The research firm gleaned some lessons from early adopters of mobile device management in a set of extensive interviews.

Among the tips they received was that IT managers should create a single mobile policy for both corporate and employee-owned devices. Many firms either have no policy or have practices that apply only to corporate-owned devices.

Because [Apple's iPhones](#) and [iPads](#) and devices running the [Android](#) operating system are most preferred by employees, Forrester said progressive IT managers are starting to support both platforms and work around some of their security limitations.

Forrester found that IT managers will deliver only basic services, such as email, contacts and calendar functionality, to Android and Apple's iOS devices because of security concerns. However, the companies plan to allow more functionality as the operating systems and the mobile device management software matures. More functionality could include access to corporate apps used for inventory control, for example.

Regarding support for personally owned devices, Forrester said MDM software can help protect a company should it need to wipe data from an employee's phone. But users first need to be aware of the possibility that their data could be wiped from their device. Forrester found that some companies compromise by providing some support of employee-owned devices but then don't allow employees to use the devices to connect to company networks.

Allowing Personal Devices At Work: A Faustian Bargain?

Progressive CIOs and their organizations can realize big benefits, but tread carefully.

By [Michael J. Belak](#) [InformationWeek](#)
September 21, 2011

The rapid growth in mobile device usage is creating a tsunami of change for CIOs and corporate IT departments.

A growing number of CIOs are embracing mobile device management programs that let employees "bring your own device" (BYOD) to work. But are they unknowingly making a Faustian bargain, compromising corporate security and by extension brand loyalty and customer good will?

Resistance to BYOD may not be futile, but it will get more difficult as employees insist on using the tools they need to succeed. The worldwide mobile phone market grew about 65% in the second quarter compared with a year ago, according to IDC, which forecasts that the smartphone segment, led by Apple, will grow 55% this year compared with 2010.

That rapid growth hasn't gone unnoticed by corporate IT departments. In a survey of delegates at a recent *SC Magazine* conference on mobile device management, 60% said they supported a BYOD policy, while 32% were planning to support one in the future. So BYOD is happening, for at least a couple of good reasons:

- Reduced IT hardware and support costs. A BYOD policy lets companies shift some portion of the cost of mobile devices to their employees and contractors. Companies may get additional cost savings by reducing training and IT support.
- Increased employee productivity. The theory, at least, is that employees who use the devices they're most comfortable with are happier, more productive employees. And rather than have to rely upon the traditional IT organization's command-and-control procurement policies, employees in a BYOD world move to the latest device at their own, faster pace.

While a BYOD policy offers companies seductive promises, you can't ignore the ever-present risks, including:

- Exposing sensitive data. As employees use more and different mobile devices in various settings, they're more likely to lose those devices or have them stolen.
- Introducing malware to the corporate network. If CIOs thought it was difficult to maintain network security with standardized devices via controlled access, just wait until their departments have to work with a multitude of non-standardized devices connecting to the corporate network, perhaps without all the proper security updates applied. .
- Greater need to control network access and ensure data privacy. When employees leave an organization, or they lose a mobile device, corporate IT will need to quickly terminate network access and restrict access to corporate data residing on the device. Additionally, corporate data must be protected and segmented at all times from the employee's personal data stored on the device. .

Despite all the risks, a BYOD policy is a valuable opportunity for CIOs to position their organizations as value adders and revenue drivers instead of fat cost centers that can't keep pace with business needs.

Data security--ensure that corporate data is kept separate from personal data. Most mobile device management software provides a protected sandbox for corporate data.

- Device diversity--state which devices will be allowed and which not. BYOD doesn't necessarily mean any and all.
- Cost--state clearly which items the company will pay for and set limits on reimbursements.
- Access controls--identify how devices will be provided to employees. Employees should understand their eligibility.

The second step is to implement supporting technology to manage and secure both corporate data and the mobile devices that data resides on. Two software vendors, MobileIron and Good Technology, provide a good starting point when evaluating mobile device management solutions. Other MDM software vendors include Zenprise, AirWatch, and Mobile Active Defense.

Progressive CIOs need to evaluate BYOD carefully. Big benefits await those who manage it right.

The Social Business And The Social Brand

Michael Brito | *September 21, 2011*

They're different--and the same. For starters, there needs to be consistent alignment between the two to generate true business results.

There's some confusion in the marketplace about the difference between a social brand and a social business. First, a couple of quick definitions:

A social brand is any company, product, or individual that uses social technologies to communicate with social customers, their partners and constituencies, or the general public. A social business is any company that has integrated and operationalized social media within every job function internally.

Social business planning is internal; a social brand is external. But more important, there needs to be consistent alignment between both internal and external programs and initiatives to generate true business results. I have always been a firm believer that an organization cannot and will not have meaningful conversations with the social customer unless it can have meaningful conversations internally first.

Here's my logic and one example that illustrate my point:

John is irritated because he dialed in to a customer support department and was put on hold for 30 minutes. No one ever answered his call. He goes to the brand's Facebook page and leaves a comment expressing his anger. No response. He then tweets at the brand's Twitter profile. No response. So he writes a blog post criticizing the heck out of the brand and shares it all over the social Web. Still no response.

In most organizations, a corporate Twitter handle is owned and managed by someone in PR. And because of organizational silos that still plague businesses, the PR folks probably aren't talking with their colleagues in customer support.

So here's a situation where a social brand is unresponsive and is pissing off the social customer because its internal communication is lacking. Now, let's take a different angle. Assume the PR person did send an email to customer support, which took care of John's issue so he's happy now. And then the same thing happens with Mary, Chris, Steve, and several other customers, and the support team realizes it needs to shift internally to address all of these online inquiries. Progress, for sure. Happy customers are a good thing.

But a true social business will go above and beyond addressing isolated customer support issues. It will take that feedback (because its people are communicating and working together internally) and fix the root cause of the problem.

Another quick example is when companies create products with their customers, giving birth to innovation. Take Starbucks' Splashstick. In creating a product with its community, [Starbucks](#) changed the coffee-drinking experience for millions of customers and solved a vexing business problem: hot coffee spillage.

Of course, I'm oversimplifying the issue because situations like these take time, a commitment to change and new processes, and the establishment of governance models. But Starbucks provides a good example of an organization reaping the benefits of social brand and social business alignment.

But here is why a social brand and social business are completely different:

-- A social brand focuses on external communications. A social business focuses on internal communications.

-- A social brand is all about engagement with the social customer. A social business is all about engagement with employees.

-- A social brand is owned by marketing. A social business should be owned by the entire organization.

-- A social brand is measured by clicks, impressions, reach, Likes, comments, RTs, etc. A social business is measured by organizational change.

-- With a social brand, budgets are usually allocated toward agencies, community management, Facebook applications, blog development, etc. Most investments in social business initiatives revolve around internal communities, social technologies, and training.

And here's the one reason they're exactly the same:

-- They serve the same purpose and underlying goal: creating value for the social customer.

The social customer, in turn, is creating value by offering insights and opinions (both good and bad) about his or her brand experience. The social brand creates value with the customer by listening, engaging, and solving problems, and it shares those insights, feedback, and best practices internally. And finally, the social business is creating value for the social customer by listening to the collective feedback of the community and innovating its products, services, policies, and processes--creating a cycle of value creation.

1 in 3 in Massachusetts had Personal Data Compromised

By Tim Greene

September 21, 2011 — [Network World](#) — [Personal information](#) on about a third of Massachusetts residents has been compromised, according to the state's attorney general, citing statistics gleaned from the tough data breach reporting law there.

About 2.1 million of the state's roughly 6.6 million residents had some form of personal data put at risk in 1,166 reported theft incidents, says Attorney General Martha Coakley, according to a report in the Boston Globe. She was citing numbers gathered from the start of 2010 through this August.

She says she is reviewing the stats to see whether the law, which imposes heavy fines for non-compliance by entities entrusted with this data, is cutting back on breaches that lead to compromises.

The AG says a combination of hacking, errors by employees and a growing body of personal data that is stored electronically by businesses will put that data at more risk over time. "This is going to be an increasing target," she says.

The largest breach in the time period Coakley is reviewing involved information on about 800,000 people that was lost by a vendor hired to destroy it. Even information on 210,000 residents entrusted to a state agency was put at risk.

The types of data covered by the law include credit card and bank account numbers, Social Security numbers and medical records. Massachusetts' reporting law is considered one of the toughest in the nation. The state is also the home of TJX whose loss of millions of credit card numbers was notable for its scale and is still one of the largest ever.

Coakley says the compromised records were not necessarily exploited. So a person's credit card number might have been removed from a secure and trusted environment but not necessarily used without authorization.

Of the 1,166 breaches since 2010, 41% have occurred in the past eight months. A quarter of the compromises stem from hacking, but the data was also put in jeopardy by loss of laptops and paper documents, sending information to the wrong recipient and unauthorized viewing of files by employees.

Many of the reported incidents were small, with just one person being affected in 30% of the cases.

Facial Recognition Security, Privacy Issues Grab FTC Attention

By Michael Cooney

September 21, 2011 — [Network World](#) — The Federal Trade Commission the week said it will hold a workshop that examines how burgeoning use of facial recognition technology impacts [privacy and security](#).

From the FTC: "Facial recognition technology has been adopted in a variety of new [contexts](#), ranging from online social networks to digital signs and mobile apps. Its increased use has raised a variety of privacy concerns. The FTC workshop will gather consumer protection organizations, academics, business and industry representatives, privacy professionals, and others to examine the use of facial recognition technology and related privacy and security concerns."

The agency said the workshop will look at many topics including:

What are the current and future uses of facial recognition technology?

How can consumers benefit from the technology?

What are the privacy and security concerns surrounding the adoption of the technology; for example, have consumers consented to the collection and use of their images?

Are there special considerations for the use of this technology on or by children and teens?

What legal protections currently exist for consumers regarding the use of the technology, both in the United States and internationally?

What consumer protections should be provided?

The workshop will take place in Washington, DC on Dec. 8, 2011 is free and open to the public.

Use of facial recognition technology is growing fast. One of its biggest pushes could come in the form of [Microsoft's Windows 8](#). Network World recently wrote that the software giant is building facial recognition technology into Windows 8, offering a more secure way to access your computer.

This month the U.K.'s largest airport, [Heathrow](#), will install facial recognition scanners for international and domestic passengers to prevent illegal immigration in the country, the IDG News Service reported. The facial recognition technology comes from Aurora Computer Services, a U.K.-based company. It's called the Aurora Image Recognition (AIR) system and uses a camera with an infrared flash, which the company says can function in either bright or low light. It can identify a person from about 3 feet away. The camera verifies a person's identity using biometric details, identifying a person in 4.7 seconds, a time that includes properly positioning a passenger, according to Aurora.

And facial recognition technology has raised privacy concerns. Recently Connecticut Attorney General George Jepsen expressed concern that Facebook's "Tag Suggestions" face recognition feature compromises consumer privacy, and asked for a meeting with company officials.

According to an IDG News Service story: In Facebook's desire to [promote photo sharing](#) and tagging among its users, it appears to have overlooked a critical component of consumer privacy protection, which is an opt-in requiring users to affirmatively consent before Facebook can use those images, Jepsen wrote in a letter this week to Facebook's director of public policy and its product and regulatory counsel. Jepsen joins European Union (EU) regulators and consumer advocacy groups that are questioning the feature on Facebook.

The Electronic Privacy Information Center and three other advocacy groups filed a complaint asking the U.S. Federal Trade Commission to require Facebook to get affirmative opt-in consent from users before collecting and using their biometric data.

Corporate Espionage's New Friend: Embedded Web Servers

Many types of Web-connected photocopiers, scanners, and VoIP servers have no default passwords or other security enabled to stop remote eavesdropping.

By [Mathew J. Schwartz](#) [InformationWeek](#)
September 26, 2011

Numerous models of printers, photocopiers, and voice over IP (VoIP) systems are Internet-connected. But their embedded Web servers often use well-known default passwords or firmware that has known vulnerabilities, either of which could be used by remote eavesdroppers to intercept internal communications.

That warning was issued by Michael Sutton, VP of security research for Web security firm Zscaler Labs, last month at the [Black Hat](#) security conference, in a session titled "Corporate Espionage for Dummies: The Hidden Threat of Embedded Web Servers." Sutton presented the results of his research, based on using multiple search engines to fingerprint more than one million Web servers, as well as identifying--as much as possible--which of those servers are embedded. Interestingly, Google search appears to suppress results for embedded Web servers. But other search engines, such as [Shodan](#), do not.

Of the one million Web servers fingerprinted, 34.2% ran Microsoft IIS, and 33.6% ran Apache. Beyond that, there were 2,737 unique server headers on the remaining machines, and "a lot of that is embedded Web servers," said Sutton. Many of those servers also lack any security, such as requiring a password to access stored documents or VoIP calls. As a result, Sutton was able to freely download numerous types of documents, including voting advice from a pro-Tea Party organization, copies of signed checks, and scanned technical reports. "My absolute favorite," he said, "is documentation letting us know that Jim is actually a certified mold inspector."

While that recovered information isn't necessarily earth-shattering, Sutton said that Web-accessible photocopiers and the like are essentially repositories of any recent documents or communications of interest, and thus could serve as a competitive intelligence treasure trove. Some devices even offer would-be attackers time-saving shortcuts. Certain models of Sharp photocopiers, for example, can be set to upload all scanned or copied documents to an external site via FTP, or email them to an outside email address. Meanwhile, some HP all-in-one printers have a feature called Webscan, which allows anyone with a browser to [scan and download](#) whatever is on the scanner bed.

Interestingly, the most-prevalent Web-connected devices Sutton found were security cameras, including babycams. "I found a lot of McDonald's Web cams; I don't know why," he said. Most cameras, however, appeared to have been set up to monitor employees.

Of all the devices fingerprinted, however, "the ones that are most concerning are the Ricoh copiers," said Sutton. In particular, 2% of all of the embedded Web servers he found were Ricoh copiers that use a default password of "admin." While the devices offer SSH encryption, many also ran services such as telnet, which an attacker could easily enable and then use to directly access the machines at a later date. Some of the machines also make recently scanned documents available for immediate download in TIFF or PDF format.

Going forward, Sutton said he's hoping to amass better information--which he'll share freely--for fingerprinting every type of embedded Web server (EWS) he finds, in part to help businesses understand which internal devices may have embedded Web servers with known vulnerabilities. To that end, he's released [BREWS](#) (for basic request embedded Web server), which he described as a "crowd-sourcing initiative to build a global database of EWS fingerprinting data."

But what can be done to EWS vulnerabilities now? First, embedded Web servers need to be included in corporate patch management plans, and vendors must push patches. "The hardware industry is at least a decade behind the software industry in terms of security," said Sutton. "We definitely need to move to a system that's more common, like Apple TV, where new patches just get pushed to you." For example, one of the most widely used embedded Web servers is Allegro RomPager, which its manufacturer says runs in 75 million devices. During his research, Sutton found at least 3,000 devices running a [version of RomPager](#) that contains a known vulnerability that could be used to crash the server.

Next, devices need to ship with security-compromising features, such as the ability to automatically upload scanned documents to an FTP site, disabled. "I really place the blame on the vendors," said Sutton. "This functionality often serves no useful purpose, and it really doesn't need to be there." When it is useful, however, such functionality should be enabled by default, using a unique password such as the serial number of the device's MAC address.

Until those changes occur, corporate IT managers should regard anything with an embedded Web server as a potential security threat, and secure it appropriately. "In the enterprise ... you need to treat a photocopier or any network-enabled device the same way as a computer," said Sutton.