The 14 Most Impactful Cyber Security Articles of the Last 12 Months

SUNGARD® AVAILABILITY SERVICES™

articles

Cyber Security Professionals Predict Their Biggest Concerns For 2015

How To Talk To Spooked Customers About Your Company's Cyber Security

Information Security: Is Your Company's Data Running Around Naked?

The Top 5 Information Security Breaches No One Is Talking About

The 6 Scariest Pieces Of Malware

Five Steps To Better Apps: A Cookbook For Mobile Application Security

Three Effective Approaches To Corporate Security

The Internet Of Things Poses New Security Challenges

What The Russian Cyber Gang Password Theft Means For All Businesses

Why Your LinkedIn Profile Might Be A Hacker's Best Friend

A Road Map For Beating Hackers At Their Own Game

How To Conduct An Information Security Gap

What Do Information Security Consultants REALLY Do?

The Year In Cyber Security: Sony's Hack Scandal And Various Retail Data Breaches

1 Cyber Security Professionals Predict Their Biggest Concerns For 2015

By Sue Poremba

With 2014 in the rear view mirror, it is fun to look forward to the year ahead and see if we can predict what may happen over the next twelve months. At the same time, predictions can prove to be very useful for businesses that are planning budgets and spending. So every December, cyber security experts begin to make their predictions on the future of information and network security.

“While no one can totally reliably predict the future, there are often good indications in what we see that provide likely directions for the coming year,” said Geoff Webb, senior director, security strategy with NetIQ. “For example, it was pretty clear at the end of last year, after the details of the Target breach become public, that it wasn’t going to be a one-off incident. Rather, it was the opening salvo in what has proven to be a year-long attack on the retail industry.”

Webb added that by being able to look across multiple sources of information, evaluating the patterns of attack and defense, and providing commentary to a broader market can help set the security conversation for the coming year. “After all, the more we can share information, the better we all are at responding quickly and preventing successful attacks. And that has huge value for everyone.”

With that in mind, here are five things that security professionals believe we need to think about in 2015.

Attacks against virtual payment systems

In light of the recent retail breaches involving credit and debit cards, there are many who think that the move to mobile payment solutions will help solve the security problem. Patrick Nielsen, Senior Security Research, with Kaspersky Lab, however, believes that it won’t take long for cybercriminals to take advantage of a potential vulnerability in the system.

“We expect to see cybercriminals focus more on new payment systems as they are adopted and the potential for criminal financial gain thus increases. This will be in the shape of attacks against banks/virtual currency operators, the end users and their devices, and everything in-between. In fact, we already have some examples of malware stealing virtual wallets from users’ devices, and very high-profile incidents of banks themselves being infiltrated,” he said.

More old security holes surface in open source software

One of the most talked about security problems of 2014 was the Heartbleed bug. However, Heartbleed and other vulnerabilities found in open source code have been lurking there for years before they were discovered. Nielsen said we should expect to see more of these old security holes causing problems in 2015.

continued on next page

Cyber security professionals have enormous concerns for 2015 including Data Loss Prevention (DLP) and an increase in “raw” security incidents.

articles

- Cyber Security Professionals Predict Their Biggest Concerns For 2015
- How To Talk To Spooked Customers About Your Company’s Cyber Security
- Information Security: Is Your Company’s Data Running Around Naked?
- The Top 5 Information Security Breaches No One Is Talking About
- The 6 Scariest Pieces Of Malware
- Five Steps To Better Apps: A Cookbook For Mobile Application Security
- Three Effective Approaches To Corporate Security
- The Internet Of Things Poses New Security Challenges
- What The Russian Cyber Gang Password Theft Means For All Businesses
- Why Your LinkedIn Profile Might Be A Hacker’s Best Friend
- A Road Map For Beating Hackers At Their Own Game
- How To Conduct An Information Security Gap
- What Do Information Security Consultants REALLY Do?
- The Year In Cyber Security: Sony’s Hack Scandal And Various Retail Data Breaches

continued from previous page

1

The reason why these old vulnerabilities are just now coming to light is because, for the first time, people are taking more time to look at the potential security problems. But just as this is good for those who want to make the Internet safer, it is also an opportunity for bad guys.

"As serious holes are found in critical pieces of software that we've assumed to be secure for years, other curious people are likely to try to find their own holes, for good and (unfortunately often) nefarious purposes," Nielsen said. "There's a shift happening in how quickly we assume something to be secure, and we will continue to see the effects of this: more holes in critical software we assumed to be secure, and more efforts taken by companies and organizations to make sure that their products have been properly audited and scrutinized."

Data Loss Prevention (DLP) will become a hot issue for business leaders

Businesses need to know where their business critical information is at all times. Flagging content and communication before it leaves the office is a good start but it is not enough. "Machine learning, pattern recognition and 'post-send' message controls are the next wave of DLP functionality that will protect employees, clients and increasingly the brand," said Cameron Burke, SVP of Business Development for Cirius.

Malware will be harder to detect and shutdown

It's time we stopped thinking about malware as a nuisance that has to be kept off computers and started recognizing what it actually is – big business. And just like any business wants to grow stronger and increase its earnings in the coming year, malware developers will continue to put out products that will be sneakier and harder to detect, all in the name of higher financial gains.

"In 2014 we saw a number of significant wins against malware with the dismantling of several major botnets. This type of takedown will be much harder in 2015 with malware becoming stealthier," said Andy Avanessian, VP of Professional Services at Avecto. "In the coming months, we will see increased use of p2p, darknet and tor communications, forums selling malware and stolen data will also retreat further into hidden corners of the internet in an attempt to avoid infiltration."

Raw security incidents will continue to rise

The recent Sony attack is a warning of just how devastating a cybersecurity incident can be, and that we need to be prepared for just about anything. As Sungard Availability Services' (AS) Matthew Goche stated, "There are more bad actors who are more organized with better tools and have more upside than ever before. This trend does not show signs of subsiding. Our internal data gathering shows a significant increase in cyber events."

Thinking beyond individual threats

Organizations today face unprecedented security challenges, Stephen Pao, GM Security at Barracuda, pointed out. Attacks often are targeted and increasingly sophisticated, and security professionals are being asked to address these risks across an ever more complicated environment.

"Focusing on the individual threat is a common approach to IT security; however, this doesn't work in today's threat environment," he added. "With the move to virtualization, the cloud and the mobile internet, the attack surface is expanding. Organizations must make that shift as well to cover all areas of exposure – email, web applications, remote access, web browsing, mobile Internet, and network perimeters."

The chances that all of these security predictions come true, at least in part, are pretty good. The question is whether or not businesses will be up to the challenge of tackling these security issues before they cause damage. And that, only time will tell.

articles

- Cyber Security Professionals Predict Their Biggest Concerns For 2015
- How To Talk To Spooked Customers About Your Company's Cyber Security
- Information Security: Is Your Company's Data Running Around Naked?
- The Top 5 Information Security Breaches No One Is Talking About
- The 6 Scariest Pieces Of Malware
- Five Steps To Better Apps: A Cookbook For Mobile Application Security
- Three Effective Approaches To Corporate Security
- The Internet Of Things Poses New Security Challenges
- What The Russian Cyber Gang Password Theft Means For All Businesses
- Why Your LinkedIn Profile Might Be A Hacker's Best Friend
- A Road Map For Beating Hackers At Their Own Game
- How To Conduct An Information Security Gap
- What Do Information Security Consultants REALLY Do?
- The Year In Cyber Security: Sony's Hack Scandal And Various Retail Data Breaches

2 How To Talk To Spooked Customers About Your Company's Cyber Security

By Natalie Burg

Since the dawn of doing business in a cyber way, organizations have worked hard to keep their customers' private data safe, with customers for the most part unaware of the efforts behind the scenes. They may even have been unaware that there was a need to secure data in the first place. They just did business with certain companies based on whatever goods or services they needed.

Oh, how times have changed. The high-profile security breaches of the last two years have made consumers much more aware of the risk to their financial and personal safety when a company they do business with is hacked.

"2013 was clearly one of the worst years on record in terms of the explosion of various criminal organizations targeting these large, batch thefts of credit cards," says Matthew Goche, director of security services for Sungard AS. "It entered the popular media in a much bigger way."

What do consumers with a heightened awareness of security issues mean for businesses? Some companies offer credit monitoring or consumer identity risk scores, but if you're just a regular business wanting to retain customers who are hyper-aware of their data security risk, what can you do?

According to Goche, it's all about communicating to consumers just how safe their data is with your company – after you ensure that the data truly is secure.

Get your security and vendors in line

You can't assure your customers that your company is safe to do business with unless you're sure that's actually the case. It's important to have a plan for cyber resilience in place – that is, knowing what you'll do if and when you're breached.

"Since the big brands got hit, and they spend a lot of money on security, you can make an assumption that if you're a midsize company, there is some probability that you will have a breach," says Goche.

This means determining what data your business could recover from losing, and what is essential to protect. Also, what will your response plan be if breached? Often, says Goche, a business's communication plan makes all the difference in damage control.

No company is an island

Your customers' security isn't always determined by your own protections, however. The vendors you work with can expose your customers' data to risk, as well. Goche recommends evaluating each vendor to determine which could negatively affect your customers if breached, a process that should include investigating their certifications and security advisers to assess their level of risk.

continued on next page

Do cyber security concerns have your customers spooked? Communicating your plan with them is key.

articles

Cyber Security Professionals Predict Their Biggest Concerns For 2015

How To Talk To Spooked Customers About Your Company's Cyber Security

Information Security: Is Your Company's Data Running Around Naked?

The Top 5 Information Security Breaches No One Is Talking About

The 6 Scariest Pieces Of Malware

Five Steps To Better Apps: A Cookbook For Mobile Application Security

Three Effective Approaches To Corporate Security

The Internet Of Things Poses New Security Challenges

What The Russian Cyber Gang Password Theft Means For All Businesses

Why Your LinkedIn Profile Might Be A Hacker's Best Friend

A Road Map For Beating Hackers At Their Own Game

How To Conduct An Information Security Gap

What Do Information Security Consultants REALLY Do?

The Year In Cyber Security: Sony's Hack Scandal And Various Retail Data Breaches

continued from previous page

2

Any vendor that balks at this kind of security review and testing should give you pause: “If they are unwilling to allow it, then you need to ask yourself, ‘Is this a good business partnership for my company?’” says Goche.

Receive and post security certifications

All of your due diligence will help protect your customers’ data. However, if your security efforts are not transparent to your customers—and potential customers— they won’t have any more reason to trust your business than any other business.

Prove you deserve their business by following official standards laid out by oversight organizations and receiving certifications. This should include PCI certification, as well as adherence to ISO 27000, an international security standard, and NIST 1,800-53, a U.S. standard.

Once you get these certifications, post them clearly for consumers to see, with clear explanations of what they mean to their security when doing business with you.

Craft and share a security commitment statement

Certifications provide proof of what you’ve done to keep customers secure, but your intention to continue to make security a priority are best described through a security commitment statement. While these statements can come in various forms, the goal should be to provide clear, honest communication about the company’s perspectives on security.

“What it’s really getting to is providing a customer with awareness that, one, the entity takes security really seriously,” Goche says. “And then, two, it gives a consumer a little more understanding of the rigor with which [a company is] going about it.”

Walmart is one company that has made an effort to clarify its commitment to customer security in a thorough and public way. Walmart’s website includes clear statements on privacy, identify theft, fraud alerts, information sharing, mobile security and even specific technical details on phishing attacks and other security-related items.

“It should be obvious to customers that information security is at the forefront of concerns and that your data is protected in a responsible fashion,” Goche says. “Making sure consumers see that statement can go a long way to assuaging their fears about your company’s security risk and [making them] feel comfortable doing business with you.”

It can be a scary world out there for consumers. With all the high-profile security breaches in the news lately, it’s no wonder consumers are hyper-aware of their own risk and looking for reassurance. It’s important for businesses to understand just how deep these consumer concerns are, and to go the extra mile to assure security-savvy customers just how seriously their protection is being taken.

articles

Cyber Security Professionals Predict Their Biggest Concerns For 2015

How To Talk To Spooked Customers About Your Company’s Cyber Security

Information Security: Is Your Company’s Data Running Around Naked?

The Top 5 Information Security Breaches No One Is Talking About

The 6 Scariest Pieces Of Malware

Five Steps To Better Apps: A Cookbook For Mobile Application Security

Three Effective Approaches To Corporate Security

The Internet Of Things Poses New Security Challenges

What The Russian Cyber Gang Password Theft Means For All Businesses

Why Your LinkedIn Profile Might Be A Hacker’s Best Friend

A Road Map For Beating Hackers At Their Own Game

How To Conduct An Information Security Gap

What Do Information Security Consultants REALLY Do?

The Year In Cyber Security: Sony’s Hack Scandal And Various Retail Data Breaches

3

Information Security: Is Your Company's Data Running Around Naked?

by Matthew Goche and John Beattie

You've probably had this dream: you're in a public setting and as you look down, you realize that you are (gasp!) stark naked!

Not good. Fortunately, it is just a dream. But here's a real-life question for you: is your company's information running around naked? In other (more technical) words, what is your information security exposure? Are you "covered"? Or can people see things you would rather that they not see?

One of the key problem zones for information security exposure is where companies intersect with their vendors. Do we need to remind you of Target? Probably not! And what about the breaking news about Home Depot's breach that has "unclothed" 56 million payment cards?

So what do you do to make sure your data is properly clothed? How do you ensure that you have adequately addressed your 3rd party risks? Here are three tips:

1

Rack and Stack Your Vendors

Before you dig into specifics about all your vendors (because we're sure you have quite a few), spend a little time assessing *how your vendors interact with you*. This will give insight into what your potential information security exposure is for each one. For example, there's obviously a big difference between the security risk associated with the vendor who is restocking your coffee room compared to the vendor who is remotely managing your firewall or directly interfacing with *your* customers or data about them.

To prioritize your information security exposure risks, answer the following for each of your vendors:

- Am I sharing my customer or confidential data with this vendor?
- If I am, is any of that data subject to federal or industry regulations?
- Is the vendor's network a conduit into yours?

These questions will show you where you need to concentrate your vendor risk assessment time and efforts.

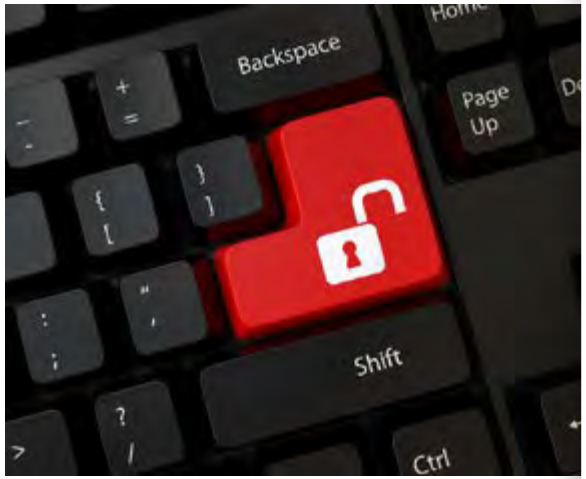
2

Look for Vendor Due Diligence

You very well might use the industry's preeminent tool, **Shared Assessments' Standard Information Gathering (SIG) questionnaire**, to assess your vendors. This will reveal key aspects of their security posture, including:

- Whether they have attained key certifications proving that they manage their facilities, payment card information (PCI), and other data in a compliant fashion.

continued on next page



Is your company's data exposed? Is your data secure or running around "naked?" Learn how you can protect your data!

articles

Cyber Security Professionals Predict Their Biggest Concerns For 2015

How To Talk To Spooked Customers About Your Company's Cyber Security

Information Security: Is Your Company's Data Running Around Naked?

The Top 5 Information Security Breaches No One Is Talking About

The 6 Scariest Pieces Of Malware

Five Steps To Better Apps: A Cookbook For Mobile Application Security

Three Effective Approaches To Corporate Security

The Internet Of Things Poses New Security Challenges

What The Russian Cyber Gang Password Theft Means For All Businesses

Why Your LinkedIn Profile Might Be A Hacker's Best Friend

A Road Map For Beating Hackers At Their Own Game

How To Conduct An Information Security Gap

What Do Information Security Consultants REALLY Do?

The Year In Cyber Security: Sony's Hack Scandal And Various Retail Data Breaches

continued from previous page

3

- How they have built out their overall security program, from access control to boundary protection, etc.
- How diligent they are in performing regular reviews and validations.

If you find, as a result of your vendor assessment, that there are information security gaps, you will need to take action. For example, you could require the vendor to pursue necessary certifications, or you could devise in-house procedures to compensate for the vendor's lack of controls. There are multiple options you can consider for any red flags that are raised during a vendor risk assessment.

3

Perform Your Own Due Diligence

Never forget: *you* have primary responsibility for your information security exposure. Be sure to perform your own due diligence, even as you are requiring it from your vendors. For example, take a vendor who doesn't share data with you, but they connect to you in a certain way. Perhaps they develop your Web applications. Examine the controls you have in place: do you need to perform additional security reviews on their deliverables or add a sign-off level before they access your systems to ensure information security?

Or again, let's say that you are giving third parties access to your environment – maybe not even to a critical area. Perhaps you have a vendor who monitors your inventory levels so they can automatically send you more supplies when you need it. It's a great symbiotic relationship: you benefit and the vendor benefits from this access to your systems.

If that is the case, you should treat any area of the IT environment where a vendor has access as an untrusted network. Assume that you can't be sure that the activity and data traffic is clean and safe through that conduit. Fence the area in with firewalls and layers of intrusion protection. Target showed what could happen when hackers got through a seemingly innocent ingress point. Beef up your contractual language to set expectations on what you expect from them and to assure that you can "verify" terms of the agreement and their in place controls at will. A level of trust is an important element of a vendor agreement, but the ability to "verify" is a vital part of that agreement.

Finding out that your data is naked in the corporate world isn't just a bad dream – it's a nightmare. But by following these three tips, you can be sure that you have information security fully "covered"!

Matthew Goche is a Director in Sungard Availability Services Consulting responsible for security services. He leads the development of SunGard AS' security solutions and expansion into new client markets. Mr. Goche firmly believes that his role includes educating organizations on the risks to their business, brand, data, employees, and customers posed by security vulnerabilities. He can be contacted at Matthew.Goche@sungardas.com.

John Beattie works closely with enterprise clients in the financial services and other industries where he has an extensive and proven track record of establishing and transforming enterprise-wide business continuity programs focused on the key business issues of regulatory compliance, revenue protection, risk management and mitigation, and critical resource recovery. John has pioneered several key Sungard AS service offerings focused on risk based exercise management, vendor risk assessment and mitigation, and Availability Effectiveness. He can be contacted at John.Beattie@sungardas.com.

articles

Cyber Security Professionals Predict Their Biggest Concerns For 2015

How To Talk To Spooked Customers About Your Company's Cyber Security

Information Security: Is Your Company's Data Running Around Naked?

The Top 5 Information Security Breaches No One Is Talking About

The 6 Scariest Pieces Of Malware

Five Steps To Better Apps: A Cookbook For Mobile Application Security

Three Effective Approaches To Corporate Security

The Internet Of Things Poses New Security Challenges

What The Russian Cyber Gang Password Theft Means For All Businesses

Why Your LinkedIn Profile Might Be A Hacker's Best Friend

A Road Map For Beating Hackers At Their Own Game

How To Conduct An Information Security Gap

What Do Information Security Consultants REALLY Do?

The Year In Cyber Security: Sony's Hack Scandal And Various Retail Data Breaches

4

The Top 5 Information Security Breaches No One Is Talking About

by Sue Poremba

In late August, there was a report that Dairy Queen was the latest victim of a security breach affecting credit and debit cards. Except nobody from Dairy Queen has actually confirmed the breach, saying because the stores are franchised and the franchises aren't required to report security problems, there is no way of knowing for sure. The speculation comes, according to **Krebs on Security**, from financial institutions that are reporting signs of credit card fraud.

This particular story goes to show that even when we think we know about a data breach, we don't know the whole story. And there is a good chance that before it is ever confirmed, it will join a very long list of breaches that don't get the publication they deserve. And these aren't necessarily breaches happening to small mom-and-pop businesses. For example, when the Target breach happened last year, it not only headlined the news, it also remained a news story for months. Even today, nearly a year later, the Target breach is regularly referenced in data breach stories. But around the same time of the Target breach, word came of a similar breach at Niemen Marcus. It was a story for a moment, and then disappeared.

Why is it that some breach stories catch fire in the media while others fly under the radar?

"It is all about timing and impact," Matt Goche, head of the Information Security Consulting practice at SunGard AS, says, "but there is also a large media aspect that determines which ones gain attention or notoriety and which do not. The more a breach fits into a narrative the more likely it will gain wider attention through wider dissemination."

The Target breach is an excellent example of this, he says, because it embodied the narrative that 2013 was a bad year for retailers in terms of breaches. The Heartbleed vulnerability is another security issue that took social media by storm, even though many websites had taken care of the problem before Heartbleed went viral.

On the other hand, breaches that go unreported or under-reported still cause a lot of damage. Here are a few security breaches that have happened in the past year that you may not have heard about:

Moon Malware Attacks

In February, a self-replicating piece of malware that bypassed authentication and exploited execution weaknesses in Linksys/Cisco home routers was discovered by security researchers. According to Jason Polancich, founder and chief architect at SurfWatch Labs, the malware, known as The Moon, affected millions around the world.

As Polancich explains, "The worm exploits flaws in the routers that allow for easy use of cybercrime techniques such as 'man-in-the-middle' attacks for

continued on next page

Think you've heard about all the major data breaches? Think again. Here are five information security breaches you've never heard about…but should have!

articles

Cyber Security Professionals Predict Their Biggest Concerns For 2015

How To Talk To Spooked Customers About Your Company's Cyber Security

Information Security: Is Your Company's Data Running Around Naked?

The Top 5 Information Security Breaches No One Is Talking About

The 6 Scariest Pieces Of Malware

Five Steps To Better Apps: A Cookbook For Mobile Application Security

Three Effective Approaches To Corporate Security

The Internet Of Things Poses New Security Challenges

What The Russian Cyber Gang Password Theft Means For All Businesses

Why Your LinkedIn Profile Might Be A Hacker's Best Friend

A Road Map For Beating Hackers At Their Own Game

How To Conduct An Information Security Gap

What Do Information Security Consultants REALLY Do?

The Year In Cyber Security: Sony's Hack Scandal And Various Retail Data Breaches

continued from previous page

4

use in stealing online banking log-ins, injecting malicious code, stealing sensitive info in transmission and gaining access to other data storage." Since it was identified, other similar home and small business router back doors have been discovered in Netgear, Netis/Netcore and other Cisco models. "And while many consumers and businesses have these routers, how many have gone through the steps to upgrade the firmware, or even know how to do it? How many of them realize they should?" Polancich asks.

Attacks Against Critical Infrastructure

"Despite all the news coverage this summer about data theft through hacking, some of it state sponsored, in my opinion the worst security breaches that seem somehow to fall under the radar are taking place in the critical infrastructure and health care sectors," says Alex Tarter, Technical Director for Ultra Electronics, 3eTI.

As recently as August 18, the Nuclear Regulatory Authority (NRA) was reported to have been the victim of email-based hacks, with foreign interests suspected of sponsoring the intrusions, Tarter adds, and the attacks are expected to increase.

"The fact is that many of the critical infrastructure breaches are not publicly reported. As a result, there is little public pressure to address them. Behind closed doors, there probably are numerous intrusions inside firewalls that are kept under wraps and downplayed, ostensibly in the interest of national security. As a result, vulnerabilities seem to persist behind a wall of silence," Tarter says.

University Security Breaches

Just like the critical infrastructure, security breaches that happen at colleges and universities tend to get very little coverage. In the past year, the Universities of Maryland and Wisconsin and Iowa State University were all victims of a security breach. "From Social Security and credit card numbers to health records and intellectual property produced by research departments, colleges and universities house a vast amount of sensitive data," Stephen Boyer, co-founder and CTO of Bitsight, which recently conducted a survey investigating cybersecurity on college campuses, was quoted by FierceCIO.

Data Breach at PF Chang's

Here is another nationally known brand to have recently suffered a breach affecting credit card information, but few realize it.

"The breach was reported by Brian Krebs in June and the situation was confirmed by PF Chang's later that month," says Joe Snell, CEO of Viableware. "Although ABC News mentioned the breach several days following the Krebs report and USA Today wrote a short article about it in August, the story was never aggressively followed up on and it eventually fell off the radar."

Credit and debit card information was skimmed over an extended period of time directly from a point-of-sale system that is commonly used by a significant segment of the full-service restaurant market.

"Unfortunately, I really don't know why this story has not been more widely covered," Snell continues. "Perhaps the story could not compete with other national and international events that have been taking place since the breach was first reported."

Will we eventually know more about the Dairy Queen breach (will headquarters ever know for sure?) or will this be yet another data breach that is swept under the rug? As is the case with most breaches, what we learn about Dairy Queen or any other cybersecurity news will depend on how the interests of social media and the mainstream press. What's important to remember is just because a breach flies under the radar doesn't mean it didn't happen.

articles

Cyber Security Professionals Predict Their Biggest Concerns For 2015

How To Talk To Spooked Customers About Your Company's Cyber Security

Information Security: Is Your Company's Data Running Around Naked?

The Top 5 Information Security Breaches No One Is Talking About

The 6 Scariest Pieces Of Malware

Five Steps To Better Apps: A Cookbook For Mobile Application Security

Three Effective Approaches To Corporate Security

The Internet Of Things Poses New Security Challenges

What The Russian Cyber Gang Password Theft Means For All Businesses

Why Your LinkedIn Profile Might Be A Hacker's Best Friend

A Road Map For Beating Hackers At Their Own Game

How To Conduct An Information Security Gap

What Do Information Security Consultants REALLY Do?

The Year In Cyber Security: Sony's Hack Scandal And Various Retail Data Breaches

5

The 6 Scariest Pieces Of Malware

by Sue Poremba

All malware is scary, all the time. It can take over your computer and turn it into a zombie. It can record your keystrokes and reveal all kinds of personal or sensitive information to a cybercriminal. It can infiltrate your operating system and force you to pay a ransom to recover data (or pay a ransom to a computer repair specialist to fix whatever the malware destroyed).

Some malware, however, is scarier than others, because just when we've been lulled into believing the malware is dead or dormant, it comes back to life – and when resurrected, is often more destructive than its original incarnation. Here are six popular pieces of malware that refuse to die.

1
Zeus

Zeus was first identified in July of 2007. This Trojan was developed to steal sensitive information from a computer. Its reputation was made in its attacks against the banking and financial industries. In time, Zeus was heard from less frequently, but variations of the Trojan periodically pop up, such as Kneber and Zbot. Zeus has also been recently seen partaking in installations of the ransomware GameOver, and has been used in a spearphishing campaign involving Dropbox. "Zeus is a cheap, easy-to-use toolkit for attackers to use for years to come," says Tom Gorup, security operations manager at Rook Security.

2
Conficker

Conficker was first identified in November of 2008, attacking vulnerabilities in the Microsoft MSFT +1.54% Windows operating system. According to Gorup, the malware has since taken on many different configurations, all of which had an enterprise level auto-update feature. "In recent (2014) reports Conficker has accounted for nearly 1/3 of the top 10 Internet threats detected," Gorup explains. "The largest issue with this malware now is that it disables auto-updates and anti-virus (AV). To the user, all seems to be fine until the dozens of other infectious software take hold of the host. By then, it's too late for the user, as all control of his/her machine is lost to attackers around the world."

3
Qakbot

At the end of last year, João Gouveia, CTO with Anubisnetworks, reported seeing hundreds of domains that matched the behavior of the Qakbot malware. "He wondered if this was merely a case of the domains being rotated, which could happen automatically, even if the botnet has been abandoned by its owners, or whether this indicated new activity. Further research into the command and control (C&C) communication has shown that there is indeed new activity and that Qakbot's C&C protocol has undergone a few changes since it made the news in 2011," the Anubisnetworks blog reported. This malware is infamous for stealing passwords. It attaches itself to file shares and spreading to any other unlucky user to access these folders. As recently as September 2014, warnings have been released about a resurgence of the malware.

continued on next page

No longer terrified of malware this Halloween? Here are 6 examples why you should be.

articles

Cyber Security Professionals Predict Their Biggest Concerns For 2015

How To Talk To Spooked Customers About Your Company's Cyber Security

Information Security: Is Your Company's Data Running Around Naked?

The Top 5 Information Security Breaches No One Is Talking About

The 6 Scariest Pieces Of Malware

Five Steps To Better Apps: A Cookbook For Mobile Application Security

Three Effective Approaches To Corporate Security

The Internet Of Things Poses New Security Challenges

What The Russian Cyber Gang Password Theft Means For All Businesses

Why Your LinkedIn Profile Might Be A Hacker's Best Friend

A Road Map For Beating Hackers At Their Own Game

How To Conduct An Information Security Gap

What Do Information Security Consultants REALLY Do?

The Year In Cyber Security: Sony's Hack Scandal And Various Retail Data Breaches

continued from previous page

5

4

Sykipot

Sykipot made its first appearance in 2007 as a backdoor Trojan that the attacker uses to execute commands on a computer. The malware's primary target has been the defense industry. Perhaps the scariest attribute of Sykipot is its ability to bypass two-factor authentication, which is being turned to more and more now due to the rising number of password-related breaches. Jaime Blasco, labs director of AlienVault, continues to see Sykipot show up in new targets, such as civil aviation and smart cards. The malware shifts in its attack methodology, as well, sometimes using typo-squatting while other times using socially engineered phishing attacks with attachments.

5

Document-based Malware/Sandworm

Microsoft Office-based macro malware had fallen out of vogue, but has returned as a powerful vector for targeted attacks where Office is used as a vector for delivering a more complex attack, according to Paul Morville, founder of Confer. Morville points to the recently revealed Sandworm as a prime example. As described by Wired, Sandworm "is believed to have been running since 2009, and used a wide-reaching zero-day exploit uncovered by the researchers that affects nearly every version of the Windows operating system released since Windows Vista." "The specific vulnerabilities exploited have evolved along with controls in Office, but the vector has been revived because it is effective (users are socially engineered to open a document), and the attack surface exposed by complex Office suites on top of complex operating systems is a great way to find a method for malicious code execution," Morville says.

6

CryptoLocker

CryptoLocker is one of the newer pieces of malware, but not only is it one of the scariest of all, it already shows signs that it refuses to die. First seen in September 2013, CryptoLocker encrypts the files on an infected computer, and then holds those files for ransom. The ransomware itself can easily be removed; however, the files are harder to recover, especially since the malware developers wanted to be paid in Bitcoin. Some declared the malware as dead this past summer and sites popped up that allowed users to decrypt their lost files, but others are warning that you shouldn't let your guard down. Expect to see variations of CryptoLocker in the not-to-distant future.

Being frightened at Halloween is all part of the holiday's fun, but all of the aforementioned malware are truly scary. However, rather than be scared, you can take a few steps to prevent these specters from showing up on computers at your company. These steps include:

- Making sure software and operating systems are regularly updated and patched
- Installing (and regularly updating) anti-virus and anti-malware software
- Warning users not to click on links or open attachments in any email without verifying the authenticity first
- Training users to tell the difference between a legitimate email and a phishing scam.

Malware developers depend on users being uninformed and lazy about security, and regularly take advantage of that by repurposing old malware. By practicing these basic security tips, you can keep these cyber-spooks safe in their graves.

articles

Cyber Security Professionals Predict Their Biggest Concerns For 2015

How To Talk To Spooked Customers About Your Company's Cyber Security

Information Security: Is Your Company's Data Running Around Naked?

The Top 5 Information Security Breaches No One Is Talking About

The 6 Scariest Pieces Of Malware

Five Steps To Better Apps: A Cookbook For Mobile Application Security

Three Effective Approaches To Corporate Security

The Internet Of Things Poses New Security Challenges

What The Russian Cyber Gang Password Theft Means For All Businesses

Why Your LinkedIn Profile Might Be A Hacker's Best Friend

A Road Map For Beating Hackers At Their Own Game

How To Conduct An Information Security Gap

What Do Information Security Consultants REALLY Do?

The Year In Cyber Security: Sony's Hack Scandal And Various Retail Data Breaches

6

Five Steps To Better Apps: A Cookbook For Mobile Application Security

By Matthew Goche and Trevor Christiansen

I love my smartphone. I use it all the time and it is my first reference point for almost any question. I have also come to depend on many of the apps to support my daily tasks. As more and more people become dependent on these apps, how do we know they are secure and protecting us from cyber risks?

Celebrities have had their phones hacked and pictures stolen. Starbucks recently allowed that its phone app passed user passwords in clear text. Millions of Android users just found out that they are vulnerable to the Heartbleed security flaw. In fact, **one study** collected 8,260,509 unique malware installation packs targeted at mobile devices, the majority of which were aimed at stealing money or personal data.

Everyday users have a responsibility to keep their phones secure by using strong (and unique!) passwords for your phone, your voicemail, and your phone accounts; installing security, encryption, and anti-malware software; and not going to untrustworthy sites. Companies that produce mobile apps, however, must do their part as well. As a consumer, I should be able to trust that mobile applications, especially ones that have sensitive data, have undergone sufficient security testing and evaluation. Oftentimes, speed to release trumps security evaluation and this pushes unacceptable risk onto unknowing consumers.

Companies have a responsibility to their customers to secure their mobile applications.

Here's a cookbook for companies on how to build a realistic application security model. (Most of these steps are good guidelines for web applications as well.)

1

Has the code been reviewed?

Code should be regularly scanned for security vulnerabilities during the development cycle. Companies that have to go back and add security after development often find that it can be more expensive. As Chris Wysopal, chief technology officer for Veracode, recently **wrote in an article for SC Magazine**, "it is cheapest to detect and correct defects as early in the process as practical." He goes on to explain that a design flaw not detected until final testing will likely require hundreds of other lines of code to be changed and retested, as well. Whereas, if the flaw were detected during a threat-modeling exercise before any code is actually written, one could save both time and money. Further, I believe, this review should include all mobile application components, including the app that is installed on the smartphones itself (i.e. Android, Apple, Windows), authentication process, web services, and middleware components.

continued on next page

Smartphone users should be able to rely on software development companies to create secure mobile apps.

articles

Cyber Security Professionals Predict Their Biggest Concerns For 2015

How To Talk To Spooked Customers About Your Company's Cyber Security

Information Security: Is Your Company's Data Running Around Naked?

The Top 5 Information Security Breaches No One Is Talking About

The 6 Scariest Pieces Of Malware

Five Steps To Better Apps: A Cookbook For Mobile Application Security

Three Effective Approaches To Corporate Security

The Internet Of Things Poses New Security Challenges

What The Russian Cyber Gang Password Theft Means For All Businesses

Why Your LinkedIn Profile Might Be A Hacker's Best Friend

A Road Map For Beating Hackers At Their Own Game

How To Conduct An Information Security Gap

What Do Information Security Consultants REALLY Do?

The Year In Cyber Security: Sony's Hack Scandal And Various Retail Data Breaches

continued from previous page

6

2

Has the app undergone security testing?

Applications produced should be automatically tested as part of a build automation process. This testing process then becomes as common as compiling and version controlling to validate the hardening of the bits and bytes while still under development. Using an automated build cycle and functional testing for common vulnerabilities, such as SQL Injection, Cross-site scripting, and user-role permissions, provides peace of mind that the new feature has not introduced a new vulnerability along with it.

3

Who actually wrote this?

All development staff should have received some secure application development security training. It is not realistic for all developers to be security experts, but they must understand the fundamentals of web application security as they have a very real part in the security process that is too often overlooked. Again, correcting mistakes at the end of the development cycle typically results in additional time and expenses. There is minimal cost involved in general best practice instruction for developers. These can also be tailored for web developers and mobile developers. In the end, this makes #1 much less painful.

4

Are there security gaps?

Once developed, applications bring together multiple different components. Each component may add additional vulnerabilities along with it. It is important to stay up-to-date with the latest releases and security patches for every third-party component that is a part of the app. For instance, the Heartbleed vulnerability will affect applications for months because many companies do not realize that OpenSSL is a component of their application and are not aware of the vulnerability. Web services and middleware are other components that must be included in application security testing, but are often left out. Lastly, once fully integrated, there can still be business logic flaws in the application that allow an attacker to gain access to information for which they do not privileges. Therefore, business logic testing of the application in its final state should be incorporated into all development lifecycles.

5

What else should be done?

Hackers will always prefer to attack the weakest link, and for many companies that may be their applications. However, by following items 1-4, the weakest link shifts to other aspects of the technology architecture, such as the infrastructure, the people, and the processes. By utilizing other testing techniques such as penetration testing, infrastructure tests, and risk reviews, a company can gain a holistic view into its weakest links and prioritize accordingly.

In the end, we want information as close and as ready as possible. In today's world, that's usually with our phones, and we want apps to push more information to us through this medium. Organizations that follow this cookbook above and build a cyber resilience approach will gain my confidence and win market share.

Matthew Goche is a Director in Sungard AS' consulting business responsible for security services. He leads the development of SunGard AS' security solutions and expansion into new client markets. Mr. Goche firmly believes that his role includes educating organizations on the risks to their business, brand, data, employees, and customers posed by security vulnerabilities. He can be contacted at **Matthew.Goche@sungard.com**.

Trevor Christiansen is a Senior Consultant with Sungard AS' consulting business. He is an expert in information security and threat analysis, but given today's cyber challenges, focuses most of his attention on web security. Mr. Christiansen has worked in the information security industry for over 15 years. Prior to being hired on at SunGard AS he was responsible for securing classified networks for the Department of Defense. He can be contacted at **trevor.christiansen@sungardas.com**.

articles

Cyber Security Professionals Predict Their Biggest Concerns For 2015

How To Talk To Spooked Customers About Your Company's Cyber Security

Information Security: Is Your Company's Data Running Around Naked?

The Top 5 Information Security Breaches No One Is Talking About

The 6 Scariest Pieces Of Malware

Five Steps To Better Apps: A Cookbook For Mobile Application Security

Three Effective Approaches To Corporate Security

The Internet Of Things Poses New Security Challenges

What The Russian Cyber Gang Password Theft Means For All Businesses

Why Your LinkedIn Profile Might Be A Hacker's Best Friend

A Road Map For Beating Hackers At Their Own Game

How To Conduct An Information Security Gap

What Do Information Security Consultants REALLY Do?

The Year In Cyber Security: Sony's Hack Scandal And Various Retail Data Breaches

7

Three Effective Approaches To Corporate Security

by Suhas Sreedhar

The IT security threats lurking out in the world are **greater, more varied, and far more insidious than ever before** – and high-profile incidents of hacking **have become routine news**.

"The greatest challenge in securing complex systems is that they are just that – complex," said Oren Hamami, Director of Security Strategy for Sungard Availability Services. "CIOs are charged with protecting a diverse ecosystem of inter-connected hardware, software, and data. Each of these elements comes with its own set of risks, which are further amplified once they are brought together."

As a result, there's a paradigm shift happening in the approach to corporate security. Companies are now understanding that effective IT security can't be cookie-cutter. In fact, it can take on many forms, but its central idea is simple – it needs to be tailored to fit the unique circumstances of each business.

Here are three different approaches worth considering as your company crafts a security system.

Establish Security as a Service Model

One of the most significant developments in recent years has been the rise of managed security solutions, offering businesses Security as a Service (SecAAS). In this model, businesses contract out their IT security, and the managing company handles the deployment and implementation of the security infrastructure. The greatest benefit is that the specific hardware, software, and policies used to secure a business are flexible and dynamic, and can change based on new threats or business needs.

"The best place to see this in action is not with any individual technology, but rather with how a type of protection is deployed and managed across multiple diverse platforms," said Hamami.

With criminal enterprises, ideological hackers, furtive malware, and other threats on the rise, it is essential that companies are equipped to face the latest security challenges.

Trick Hackers

In addition to SecAAS, some companies may want to employ creative, out-of-the-box security tactics. Solutions of this sort rely on **ingenious trickery** to confound hackers who manage to successfully break into a system. Examples of this include getting rid of admin accounts, installing software to non-standard locations, and creating honeypots – deliberate targets designed to lure hackers into fake systems and data.

How much and what kinds of these unconventional solutions to deploy is very business-specific, and once again highlights the need for security solutions to be tailor-made, not one-size-fits-all. External threats typically **bet on cookie-cutter approaches to security**, and the fewer there are the better.

continued on next page

Securing today's complex systems means tailor-fitting security solutions to your network.

articles

Cyber Security Professionals Predict Their Biggest Concerns For 2015

How To Talk To Spooked Customers About Your Company's Cyber Security

Information Security: Is Your Company's Data Running Around Naked?

The Top 5 Information Security Breaches No One Is Talking About

The 6 Scariest Pieces Of Malware

Five Steps To Better Apps: A Cookbook For Mobile Application Security

Three Effective Approaches To Corporate Security

The Internet Of Things Poses New Security Challenges

What The Russian Cyber Gang Password Theft Means For All Businesses

Why Your LinkedIn Profile Might Be A Hacker's Best Friend

A Road Map For Beating Hackers At Their Own Game

How To Conduct An Information Security Gap

What Do Information Security Consultants REALLY Do?

The Year In Cyber Security: Sony's Hack Scandal And Various Retail Data Breaches

continued from previous page

7

Create Internal Protection
What if the threat comes not from outside, but from within?

Insider threats are a huge problem facing IT security. Cases like Edward Snowden's highlight a startling fact – insiders are involved in two-thirds of all cybercrime involving the theft of intellectual property. Dealing with insider threats requires security policies that are able to identify, profile, track, and catch employees who violate security policies. Deploying effective security in this regard once again requires tactics that are **business-aware, and often business-specific**.

Cybercrime has evolved to a point where static, universally applied security methods leave an organization weak and vulnerable. Tailored solutions like SecAAS, out-of-the-box policies, and internal security offer robust technical flexibility to deal with a range of threats. They also make good business sense by shedding internal overhead – and free your IT employees to focus on the challenges ahead.

Suhas Sreedhar has been covering trends in science and technology for six years, writing on topics from cloud computing to audio engineering to neuroscience. He has previously written for IEEE Spectrum magazine.

articles

Cyber Security Professionals Predict Their Biggest Concerns For 2015

How To Talk To Spooked Customers About Your Company's Cyber Security

Information Security: Is Your Company's Data Running Around Naked?

The Top 5 Information Security Breaches No One Is Talking About

The 6 Scariest Pieces Of Malware

Five Steps To Better Apps: A Cookbook For Mobile Application Security

Three Effective Approaches To Corporate Security

The Internet Of Things Poses New Security Challenges

What The Russian Cyber Gang Password Theft Means For All Businesses

Why Your LinkedIn Profile Might Be A Hacker's Best Friend

A Road Map For Beating Hackers At Their Own Game

How To Conduct An Information Security Gap

What Do Information Security Consultants REALLY Do?

The Year In Cyber Security: Sony's Hack Scandal And Various Retail Data Breaches

8

The Internet Of Things Poses New Security Challenges

by Debra Donston-Miller

If you thought bugs, viruses and phishing schemes were tough on security, you ain't seen nothin' yet. Your business will soon be faced with a new, even more formidable foe: The Internet of Things.

When it comes to security, businesses have had to make some significant shifts with the advent of new technologies and computing paradigms. Twenty years ago, security was like an M&M or Tootsie Pop – it was all about securing enterprise networks and endpoints (the soft center) behind the network perimeter (the hard shell). In the last 10 years, laptops and mobile phones have slowly chipped away at that protection. Most recently, personally owned devices used for business have posed problems that were once unthinkable. Enterprise IT managers have risen to each and every one of these challenges, developing policy and applying technology to help mitigate risks as they arise.

It's 10pm. Do you know what your refrigerator is doing? Securing the Internet of Things poses new challenges.

But the newest hurdle may be the toughest one of all to clear. Forget about networked printers and iPhones. What do you do when the coffee maker and refrigerator in the break room come equipped with hidden spambots and wifi access? Researchers have already **hacked a building control system** at Google's Australia office. Does that make you think twice about installing a Nest thermostat on your premises? What happens when workers' watches and glasses – even their suit coats and dress shoes – are connected to the Net? That's the **Internet of Things** – the "network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment," according to Gartner – and it is expected to be the greatest challenge facing organizations during the next decade.

"Now, it is still early when it comes to the Internet of Things, but it is clear that change is afoot," said Edith Ramirez, chairwoman of the Federal Trade Commission, at the FTC's November **Internet of Things workshop**. "Five years ago, for the first time, more things than people connected to the Internet."

Ramirez said it is estimated that 25 billion things will be hooked up to the Internet by 2015. In 2020, that number will double.

The risks of IoT at work

There are many potential benefits to the Internet of Things. **Automated inventory** and **climate control** are two of the oft-mentioned advantages.

But there are also many potential risks, for individuals and consumers alike. According to the **InfoSec Institute**, privacy implications include unlawful surveillance, active intrusion in private life and data profiling.

For businesses, one of the biggest concerns is data compromise.

"In particular, expect [the Internet of Things] to challenge your conception of cyber security and your ability to deliver it in IoT-enabled digital networks, your commercial operations, and your partner ecosystems," states a Harvard Business Review **blog post** written by Christopher J. Rezendes, president of INEX Advisors, a consultancy focused on the Internet of Things, and David

continued on next page

articles

Cyber Security Professionals Predict Their Biggest Concerns For 2015

How To Talk To Spooked Customers About Your Company's Cyber Security

Information Security: Is Your Company's Data Running Around Naked?

The Top 5 Information Security Breaches No One Is Talking About

The 6 Scariest Pieces Of Malware

Five Steps To Better Apps: A Cookbook For Mobile Application Security

Three Effective Approaches To Corporate Security

The Internet Of Things Poses New Security Challenges

What The Russian Cyber Gang Password Theft Means For All Businesses

Why Your LinkedIn Profile Might Be A Hacker's Best Friend

A Road Map For Beating Hackers At Their Own Game

How To Conduct An Information Security Gap

What Do Information Security Consultants REALLY Do?

The Year In Cyber Security: Sony's Hack Scandal And Various Retail Data Breaches

continued from previous page

8

Stephenson, author of SmartStuff: An Introduction to the Internet of Things. "Paradoxically, the very principle that makes the IoT so powerful – the potential to share data instantly with everyone and everything (every authorized entity, that is) – creates a huge cyber security threat."

The challenges are big, but surmountable – only if IT and business managers start working together now to develop a plan. In another Harvard Business Review blog post, Chris Clearfield, a principal at consulting firm SystemLogic, noted that it will all have to start with the manufacturers of devices: They will have to place a new priority on security, said Clearfield, including:

1. **Applying existing systems engineering tools to security threats.**

2. **Training engineers to incorporate security into products by using modular hardware and software designs.**

3. **Using existing, open security standards where possible.**

4. **Encouraging a skeptical culture.**

"Companies should encourage a skeptical culture in which intellectually diverse groups from different product teams review one another's designs and give feedback about flaws, including those that affect security," he said. "One particularly useful approach is to designate internal specialists or external experts as devil's advocates and make it their job to independently review, test, and try to break existing systems."

Healthy skepticism will conquer IoT

That level of skepticism – or suspicion – should be applied at organizations from all industries, not just the makers of the "things" in the Internet of Things.

Indeed, Clearfield said companies must start paying closer attention to the different ways devices could be leveraged as a mode of attack.

While manufacturers must work to incorporate security into their devices from the ground up, organizations should not blindly assume that **Internet-enabled devices are safe**. It will be important for companies not only to be aware of any Internet-connected devices in the organization – from Google Glass to the new thermostat – but also to examine how these devices work and interact with each other, especially in terms of data transport.

Companies will also need to think about their own investments in IoT, including ownership and control of data.

"As a business investing in the IoT you'll need to establish new standards of construct (that is, the technologies to secure the IoT) and new standards of conduct (the policies to secure the IoT)," said Rezendes and Stephenson in their Harvard Business Review blog.

The Internet of Things is a work on progress – one that companies must be out in front of in order to both benefit and stay protected from the technology.

Debra Donston-Miller has been covering the intersection of business and IT for more than 20 years. Formerly editor of eWEEK, Donston-Miller now develops content for a variety of leading media outlets.

articles

Cyber Security Professionals Predict Their Biggest Concerns For 2015

How To Talk To Spooked Customers About Your Company's Cyber Security

Information Security: Is Your Company's Data Running Around Naked?

The Top 5 Information Security Breaches No One Is Talking About

The 6 Scariest Pieces Of Malware

Five Steps To Better Apps: A Cookbook For Mobile Application Security

Three Effective Approaches To Corporate Security

The Internet Of Things Poses New Security Challenges

What The Russian Cyber Gang Password Theft Means For All Businesses

Why Your LinkedIn Profile Might Be A Hacker's Best Friend

A Road Map For Beating Hackers At Their Own Game

How To Conduct An Information Security Gap

What Do Information Security Consultants REALLY Do?

The Year In Cyber Security: Sony's Hack Scandal And Various Retail Data Breaches

9

What The Russian Cyber Gang Password Theft Means For All Businesses

by Matthew Goche

Russian hackers steal 1.2 billion passwords! Or, depending on the headline, the hackers nabbed, pilfered, or reaped all of those passwords and user credentials from over 400,000 websites.

The headlines got attention, but they left a lot of unanswered questions. Here's what has been reported: a group of Russian hackers have accumulated more than 4 billion records that include passwords and user names, but because so many of those records were duplicates, the number was of unique records was lowered to 1.2 billion. The details are sketchy. We haven't been told which websites were affected or how long it took to steal all of that information. Still, there are a lot of companies and individuals out there who are worried that their personal information is in the hands of criminals and that they'll have to change all of their passwords. Again.

However, this latest breach news reveals something even more telling about the way organizations approach security. *They aren't doing enough to protect their customer personal and account information.*

Organizations are constantly reminded that they need to do a better job implementing defense mechanisms that are commensurate with the attacks that are coming in their direction. A good security approach doesn't have to be complicated. It begins with simple steps like reviewing websites for vulnerabilities, performing regular penetration testing, patching servers, using trusted providers, and forcing users to create stronger passwords.

If the Russian hackers have taught us anything, it is that we've all got to work together to improve security. The big hacks – Target, Sony, Adobe – are the breaches that make news. But this news shows that cyber criminals are not just targeting big brands and big banks. They are also going after SMBs (Small and Medium Businesses) since they are seen as easy targets. Home users too, need to step up their own security levels and take more responsibility for the information they are sharing with companies.

So let's break this down a bit more, starting with large organizations that may already have a CSO or CISO and security department in place. It's not just the security staff's job to execute security procedures. Every C-level executive needs to understand that security is paramount. It is not an IT only issue anymore; it can be a severe threat to a business at its core. Management buy-in for security and continued involvement is the single greatest measure in determining whether a security program will succeed.

continued on next page

1.2 billion passwords. 400,000 websites. The Russian Cyber Gang data breach should scare you… here's why.

articles

Cyber Security Professionals Predict Their Biggest Concerns For 2015

How To Talk To Spooked Customers About Your Company's Cyber Security

Information Security: Is Your Company's Data Running Around Naked?

The Top 5 Information Security Breaches No One Is Talking About

The 6 Scariest Pieces Of Malware

Five Steps To Better Apps: A Cookbook For Mobile Application Security

Three Effective Approaches To Corporate Security

The Internet Of Things Poses New Security Challenges

What The Russian Cyber Gang Password Theft Means For All Businesses

Why Your LinkedIn Profile Might Be A Hacker's Best Friend

A Road Map For Beating Hackers At Their Own Game

How To Conduct An Information Security Gap

What Do Information Security Consultants REALLY Do?

The Year In Cyber Security: Sony's Hack Scandal And Various Retail Data Breaches

continued from previous page

9

Steps that IT Leaders should be instituting:

- Conduct compliance “gap analysis” to identify security needs
- Develop an overarching information security program
- Focus on prescriptive standards like PCI DSS
- Perform periodic best practice validation
- Utilize Managed Security Service Providers (MSSP) or Software as a Service (SaaS) solutions supported by 24×7 security experts to augment current resources
- Leverage a trusted managed services provider for production and recovery environments to handle the difficult security operations tasks, i.e. patching, antivirus, SOC, DDOS prevention, etc.

As I said, SMBs are not exempt from cyberattacks just because they are small. If the data small businesses hold is worth something on the black market, cyber criminals will go after it. While SMBs may not have an in-house team focused on security, there is no excuse for not having a security budget to hire the right experts to map out a security roadmap. Small businesses should consider hiring an MSSP to manage their security operations. Think in terms of cyber resilience and what business functions and data need protected the most and use that as a security starting point. If you don’t think you can afford to add a security plan, consider this: approximately 60 percent of small businesses close their doors for good within six months of a cyberattack.

Finally, organizations of all sizes should encourage customers to do a better job protecting their personal information. Passwords are going to be here for a while. As customers, we all should take responsibility to make them stronger, change them regularly, and not use the same one everywhere. That said, it’s time to stop relying on passwords alone. Multi-factor authentication should be standard no matter what the size of business or product being sold.

The news of the Russian hackers should be seen as a wake-up call. Too many organizations are slumbering through their security practices, and the bad guys will only continue to take advantage of it.

articles

Cyber Security Professionals Predict Their Biggest Concerns For 2015

How To Talk To Spooked Customers About Your Company’s Cyber Security

Information Security: Is Your Company’s Data Running Around Naked?

The Top 5 Information Security Breaches No One Is Talking About

The 6 Scariest Pieces Of Malware

Five Steps To Better Apps: A Cookbook For Mobile Application Security

Three Effective Approaches To Corporate Security

The Internet Of Things Poses New Security Challenges

What The Russian Cyber Gang Password Theft Means For All Businesses

Why Your LinkedIn Profile Might Be A Hacker’s Best Friend

A Road Map For Beating Hackers At Their Own Game

How To Conduct An Information Security Gap

What Do Information Security Consultants REALLY Do?

The Year In Cyber Security: Sony’s Hack Scandal And Various Retail Data Breaches

10

Why Your LinkedIn Profile Might Be A Hacker's Best Friend

by Trevor Christiansen

I'm a penetration tester. My job is to try to breach my clients' systems in order to help them identify vulnerabilities in their IT security. In a nutshell, I try to find security gaps before the criminals do, so that my clients can shore up their defenses against hacker attacks.

Someone recently asked me, "If you were a criminal hacker looking to exploit a company – inflicting the irreparable harm of a data breach – what's the first thing you would do?" My short and easy answer: scour LinkedIn. LinkedIn is a treasure trove of easily accessible personal information and company IT data. Unbeknownst to most of the employees who post their information on LinkedIn, any hacker looking to wreak havoc on a company's highly sensitive, business-critical data could find his or her point of entry using this ubiquitous business networking forum.

Why is LinkedIn So Attractive to Hackers?

Here's a look at LinkedIn through a hacker's eyes. Conducting a search for a specific organization on LinkedIn will turn up any number of professionals' profiles, some of which will include the person's business e-mail address. Once a hacker has seen a few e-mail addresses for the same company, he's learned the company's e-mail address structure (e.g. firstname.lastname@companyname.com) and can build an e-mail list of employees to target. In fact, hackers can successfully guess 50 to 60 percent of all employee email addresses using this method.

Next, the hacker will formulate a phishing or social engineering plan. Using his knowledge of your firm's IT platforms, his scheme could take the form of an e-mail that directs his unsuspecting victims to a webpage requiring them to enter their username and password credentials, for example.

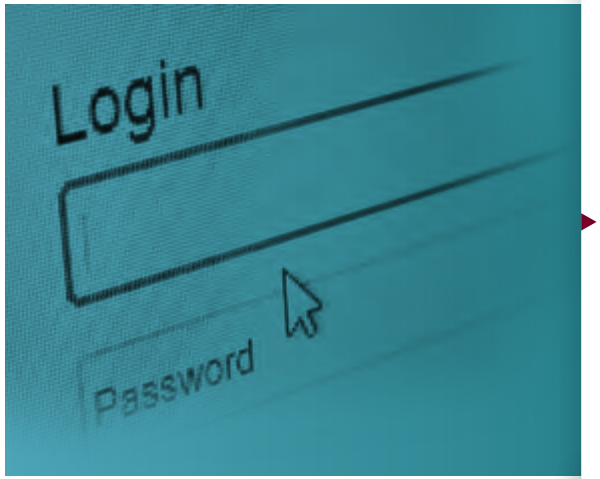
The hacker will avoid including IT staffers on his distribution list, as that's too likely to raise red flags. But customer service, accounting, marketing, and human resources personnel make much more attractive targets. The hacker will create urgency and emotion with his request. And, finally, he'll send out his bait, hook his targets and voilá: he's gained a foothold, the first step to getting the access he needs to breach the network and steal valuable credit-card, social-security or other data stores. A company's worst nightmare has just begun.

As a penetration tester, my best efforts result in me finding a vulnerability like this, and helping companies close this security gap before real hackers find their way through. The scariest part of this scenario is that any company with more than 100 employees is at risk for this kind of stealth attack from an ill-intentioned hacker who has made LinkedIn his or her best friend.

What's a Business to Do?

So, now that you know why LinkedIn has unwittingly become a hacker's BFF, what's a business to do? Companies have competing priorities when it comes to social media and LinkedIn in particular. They want their employees out there promoting the company, recruiting new customers and talent and driving up online visibility. But they

continued on next page



Your professional network may not be the only ones your LinkedIn profile is benefitting…

articles

Cyber Security Professionals Predict Their Biggest Concerns For 2015

How To Talk To Spooked Customers About Your Company's Cyber Security

Information Security: Is Your Company's Data Running Around Naked?

The Top 5 Information Security Breaches No One Is Talking About

The 6 Scariest Pieces Of Malware

Five Steps To Better Apps: A Cookbook For Mobile Application Security

Three Effective Approaches To Corporate Security

The Internet Of Things Poses New Security Challenges

What The Russian Cyber Gang Password Theft Means For All Businesses

Why Your LinkedIn Profile Might Be A Hacker's Best Friend

A Road Map For Beating Hackers At Their Own Game

How To Conduct An Information Security Gap

What Do Information Security Consultants REALLY Do?

The Year In Cyber Security: Sony's Hack Scandal And Various Retail Data Breaches

10

continued from previous page

also have a driving need to protect their data – especially in regulated industries where a data breach could cost them not only reputation points and customer loyalty, but also countless dollars in fines.

As far as anyone can tell, however. LinkedIn is here to stay. Smart companies will accept this fact, and quickly and effectively find the balance between freedom and security. Employees will continue to post personal data on LinkedIn, but their companies in turn will need to prevent that superficial information from becoming a hacker's key to their business-critical data stores.

Here are three things your firm can do to protect your business-critical data:

1

Invest in good, frequent social engineering training.
Just because hackers can guess your employees' e-mail addresses doesn't mean your people should fall for their schemes and provide their login or other information. A strong social engineering training program can help your employees learn to recognize and resist a phishing scam. And one-and-done is not the way to go here; frequent reminders and follow-up training can help keep employees vigilant.

2

Develop a statement that clearly tells employees how your company will handle network security information.
For example, "We will never ask for your username and password," or "All network-related communications will come only from this specific e-mail address." This statement should be well known to all of your people and can prevent employees from sharing usernames and passwords with parties who have malicious intent.

3

Have a clear reporting process for suspicious activity.
Make sure employees know how to report social engineering schemes and suspicious e-mails. Keep it simple, maybe with a catch phrase, for example, like "See something? Say something." Wallet cards or another physical reference might be a good idea here—anything that makes it easy to recognize a potential hacker and report suspicious activity before it becomes a full-blown network attack.

In today's social media environment, it's unrealistic to think that a business can avoid all exposure to hackers who are putting LinkedIn to work for their own purposes. However, educating and equipping your people can go a long way toward keeping your business-critical data safe and sound.

articles

Cyber Security Professionals Predict Their Biggest Concerns For 2015

How To Talk To Spooked Customers About Your Company's Cyber Security

Information Security: Is Your Company's Data Running Around Naked?

The Top 5 Information Security Breaches No One Is Talking About

The 6 Scariest Pieces Of Malware

Five Steps To Better Apps: A Cookbook For Mobile Application Security

Three Effective Approaches To Corporate Security

The Internet Of Things Poses New Security Challenges

What The Russian Cyber Gang Password Theft Means For All Businesses

Why Your LinkedIn Profile Might Be A Hacker's Best Friend

A Road Map For Beating Hackers At Their Own Game

How To Conduct An Information Security Gap

What Do Information Security Consultants REALLY Do?

The Year In Cyber Security: Sony's Hack Scandal And Various Retail Data Breaches

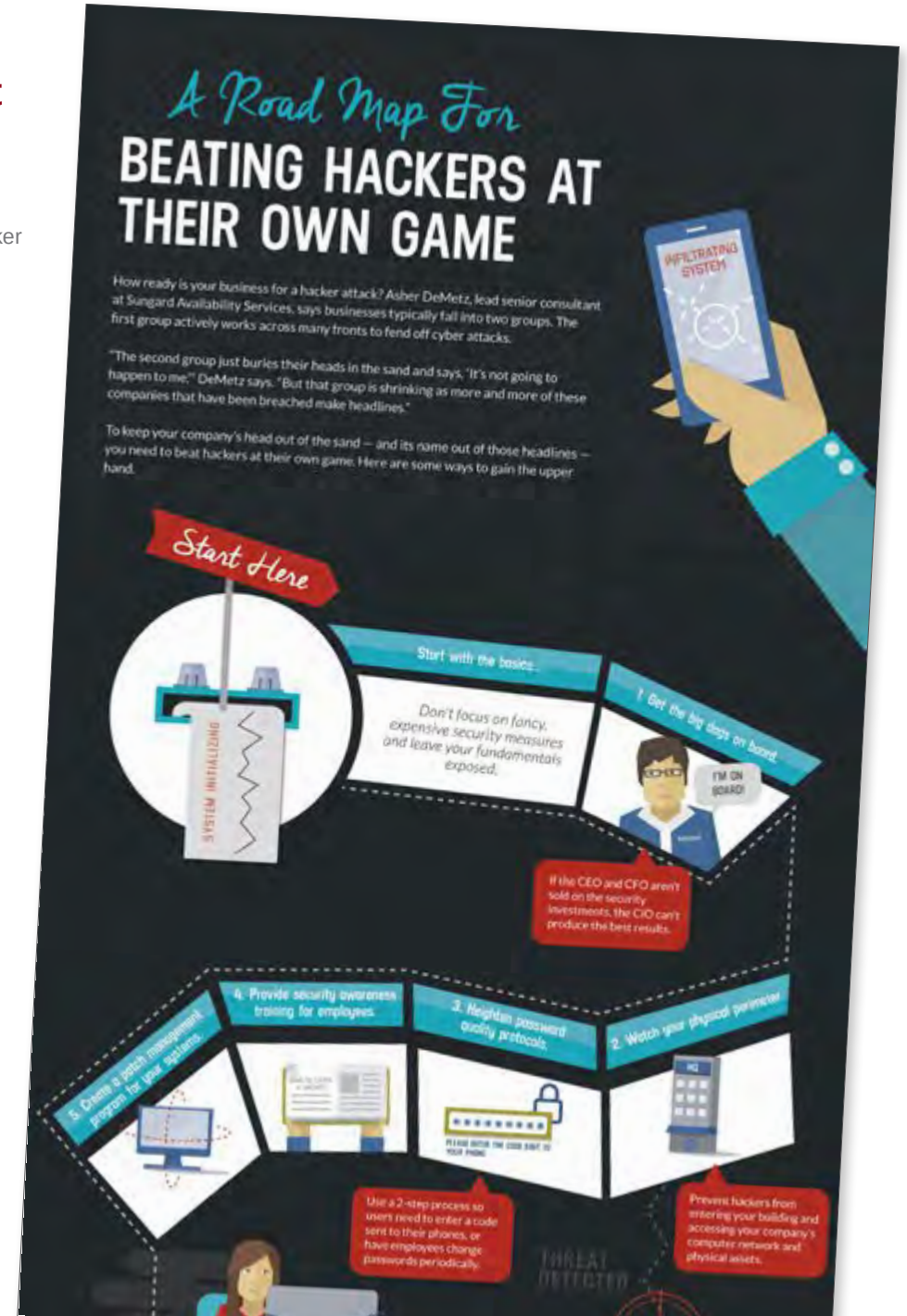
11

A Road Map For Beating Hackers At Their Own Game

by Natalie Burg and Michele Calderon

How ready is your business for a hacker attack? To keep your company safe, you need to beat hackers at their own game. Here are some ways to gain the upper hand.

View the entire infographic **here**.



sungardas.com

articles

Cyber Security Professionals Predict Their Biggest Concerns For 2015

How To Talk To Spooked Customers About Your Company's Cyber Security

Information Security: Is Your Company's Data Running Around Naked?

The Top 5 Information Security Breaches No One Is Talking About

The 6 Scariest Pieces Of Malware

Five Steps To Better Apps: A Cookbook For Mobile Application Security

Three Effective Approaches To Corporate Security

The Internet Of Things Poses New Security Challenges

What The Russian Cyber Gang Password Theft Means For All Businesses

Why Your LinkedIn Profile Might Be A Hacker's Best Friend

A Road Map For Beating Hackers At Their Own Game

How To Conduct An Information Security Gap

What Do Information Security Consultants REALLY Do?

The Year In Cyber Security: Sony's Hack Scandal And Various Retail Data Breaches

12

How To Conduct An Information Security Gap Analysis

by Chris Sell

As an information security consultant, one of the most important jobs I do is to conduct an information security gap analysis. This analysis provides a comparison of your security program versus overall best security practices. By comparing these best practices to actual practices, we can shed light on areas where vulnerabilities and risks are lurking.

However, it's not only important that a gap analysis be conducted; it's also important that it be done correctly. Here are 4 steps that are critical for every information security gap analysis.

Performing an information security gap analysis requires 4 critical steps.

Step 1:

Select an industry standard security framework

One of the most common frameworks is the ISO/EIC – 27002 standard. ISO/IEC 27002:2013 provides best practice recommendations on information security management. This standard covers best practices for such key security areas as risk assessment, access control, change management, physical security, and others.

The ISO standard provides a good benchmark that you can compare your security policies and network controls against. If you've got a good security team, you may be able to conduct the gap analysis yourself. However, even if you do have a good security team, having an independent person – someone without any connection to the network architecture – evaluate your security plan is recommended. In fact, some industry compliance standards (i.e., HIPAA or PCI) may require an outside consultant to provide an extra set of eyes to ensure that security measures are in compliance with state and federal regulations. The reason is simple: an outside consultant, such as Sungard Availability Services, can often catch gaps not found by people who work with the network day in and day out.

Step 2:

Evaluate People and Processes

This is the data-gathering phase: data on your IT environment, application inventory, organizational charts, policies and processes, and other relevant details. This could mean sitting down with your IT staff and your leadership to learn more about the organization's key objectives.

It definitely means learning which security policies are already in place and where your organization's leaders are taking your firm in the next three to five years and what security risks will be associated with it.

It's also important for the security analysts to conduct in-depth interviews with your company's key stakeholders and specific departments like HR and legal. Usually this includes IT staff, security administrators (if you have a dedicated security team in house), and anyone who works with the network, servers or workstations. Good security practices involve everyone in the company.

Many of the risks that company networks face are caused by human intervention – an employee innocently clicking on a link in a phishing email, insufficient training, or an angry employee who purposely sabotages the network.

continued on next page

articles

Cyber Security Professionals Predict Their Biggest Concerns For 2015

How To Talk To Spooked Customers About Your Company's Cyber Security

Information Security: Is Your Company's Data Running Around Naked?

The Top 5 Information Security Breaches No One Is Talking About

The 6 Scariest Pieces Of Malware

Five Steps To Better Apps: A Cookbook For Mobile Application Security

Three Effective Approaches To Corporate Security

The Internet Of Things Poses New Security Challenges

What The Russian Cyber Gang Password Theft Means For All Businesses

Why Your LinkedIn Profile Might Be A Hacker's Best Friend

A Road Map For Beating Hackers At Their Own Game

How To Conduct An Information Security Gap

What Do Information Security Consultants REALLY Do?

The Year In Cyber Security: Sony's Hack Scandal And Various Retail Data Breaches

12

continued from previous page

We need to address human behavior if we want to do as much as possible to decrease threats to data.

Key staff members can provide details on how the various controls are implemented. For example:

- How is access for new hires and terminations handled?
- Is there a standard role-based policy in place that helps ensure that the correct access is provided to each job position?
- How are changes implemented in your environment?
- Are there standard procedures and approvals that are required before a change is made?
- Is there a back-out procedure in case there is a problem?
- Is staff training provided to keep your company abreast of evolving security risks?

The more we know about the people accessing your network and the controls that are already in place, the easier it is for us to help you create the right security analysis.

Step 3:

Data Gathering/Technology

Through data gathering, our goal is to understand how well the current security program operates within the technical architecture. As part of this step, we compare best practice controls (i.e. ISO 27002 or NIST 800-53) or relevant requirements against your organizational controls; take a sample of network devices, servers, and applications to validate gaps and weaknesses; review automated security controls; and review incident response processes, communications protocols and log files. With data gathering, we gain a clear picture of your technical environment, the protections in place, and your overall security effectiveness.

As we go through the data gathering process in the security gap analysis, "we benchmark your organization's security program to our best practices. These standards were developed after years of observations and evaluations "to gain insight as to which controls are the most effective and where security shortcomings typically arise. This in-depth security knowledge allows us to see how your security process matches up to other processes and controls that have proven successful, especially when compared to other companies and security controls within your specific industry.

Step 4:

Analysis

After we get through the above phases, we perform an in-depth analysis of your security program. To do this, we correlate the findings and results across all factors to create a clear and concise picture of your IT security profile that includes areas of strength and areas where improvement is most needed. With that information in hand, we can make recommendations for moving forward with a security plan that is right for your company. That security roadmap considers risks, staffing, and budget requirements, as well as timeframes to complete the various security improvements.

As you've probably concluded by now, conducting a full information security gap analysis is a detailed, in-depth process that requires not only a thorough knowledge of security best practices but also an extensive knowledge of security risks, controls, and operational issues. We may uncover risks that can be remediated quickly with the installation of a security patch, or we may recommend that an outdated communications protocol be replaced with a more robust solution.

Performing a security gap analysis can't guarantee 100% security, but it goes a long way to ensure that your network, staff, and security controls are robust, effective, and cost efficient. When we conduct a thorough information security gap analysis, you can let your customers know that you are providing the best security possible. In turn, the better you can secure the information they entrusted to you, the better your business will thrive.

articles

Cyber Security Professionals Predict Their Biggest Concerns For 2015

How To Talk To Spooked Customers About Your Company's Cyber Security

Information Security: Is Your Company's Data Running Around Naked?

The Top 5 Information Security Breaches No One Is Talking About

The 6 Scariest Pieces Of Malware

Five Steps To Better Apps: A Cookbook For Mobile Application Security

Three Effective Approaches To Corporate Security

The Internet Of Things Poses New Security Challenges

What The Russian Cyber Gang Password Theft Means For All Businesses

Why Your LinkedIn Profile Might Be A Hacker's Best Friend

A Road Map For Beating Hackers At Their Own Game

How To Conduct An Information Security Gap

What Do Information Security Consultants REALLY Do?

The Year In Cyber Security: Sony's Hack Scandal And Various Retail Data Breaches

13

What Do Information Security Consultants REALLY Do?

by Matthew Goche

With all of the data breaches in the news lately, you might be thinking of calling in an information security consultant to help improve your network's protection. That's a good idea, and a good step to protect your company data. But consultants are not created equal. They have different areas of expertise and levels of expertise as well as different levels of commitment to your business.

Before you spend a lot of money on an information security consultant, you want to make sure you know your security goals and priorities. The following questions can help you determine your needs and ultimately choose the right consultant.

Do you have the staff and the skills to successfully manage your security in-house?
This expertise often is not found on staff in small and medium-sized businesses. The right consultant will have the expertise necessary to implement successful security plans.

Are you hiring a consultant to run and manage your security program or leveraging a third-party consultant to provide a different perspective from your in-house experts?
Some companies do not consider the latter option, but an outside party can provide direction or validation that the security program is on the right track.

Once the consultant is engaged, what are your security goals and priorities to drive their work?
There is a wide-range of security work consultants perform — regulatory analysis, technical evaluations, offensive penetration testing, Web security and everything in between. A security consultant can help with broader security strategy or objectives or they can service in a key tactical or niche role to round out the program that is already in place.

Do you need the consultant to perform a security gap analysis of the as-is security program and architecture versus best practices?
These gaps will illuminate where risks are. Again, this is to get the opinion of an impartial third party, but it also provides a broader evaluation. The consultant is able to catch obvious security problems that may have been missed. They also see a lot of implementation successes and failures and can provide valuable feedback on what works and does not work.

Once you make the decision to hire a security consultant, you want to make sure that you hire the right consultant for your organization's needs. That means asking key questions and doing your own homework before signing any contracts:

- Seek proof of how well the consultant's security reviews work.
- Ask what comes after the report of findings. Many consultants are good at identifying weaknesses but are poor at actually recommending and/or delivering concrete activities to correct challenges.
- Find out if they have expertise in your industry.

continued on next page

Thinking of getting an information security consultant to protect your company? Great idea! Just make sure to choose the right one for you.

articles

Cyber Security Professionals Predict Their Biggest Concerns For 2015

How To Talk To Spooked Customers About Your Company's Cyber Security

Information Security: Is Your Company's Data Running Around Naked?

The Top 5 Information Security Breaches No One Is Talking About

The 6 Scariest Pieces Of Malware

Five Steps To Better Apps: A Cookbook For Mobile Application Security

Three Effective Approaches To Corporate Security

The Internet Of Things Poses New Security Challenges

What The Russian Cyber Gang Password Theft Means For All Businesses

Why Your LinkedIn Profile Might Be A Hacker's Best Friend

A Road Map For Beating Hackers At Their Own Game

How To Conduct An Information Security Gap

What Do Information Security Consultants REALLY Do?

The Year In Cyber Security: Sony's Hack Scandal And Various Retail Data Breaches

13

continued from previous page

- Most insight actually comes from in-depth relationship development with the consultant and their team. There is no better way to gain a clear and accurate picture of their capabilities than to build a partnership prior to commencement of work.

Now that you have selected and signed your security consultant, what should you expect? A good information security consultant should:

- **Gather as much information about the company as possible and from every source you can imagine.** This allows the consultant to understand what the company is all about, what type of information is being secured, and where potential vulnerabilities may be. The consultant should be able to anticipate where common problems are based on the company's industry.
- **Come on-site knowing what types of regulations and security policies the company must comply with.** For a full gap analysis, the consultant will learn the technical architecture through a series of automated and manual evaluations, including scans, configuration analysis, and business analysis. This allows the consultant to understand how well the architecture is patched and protected.
- **Partner effectively with IT, leadership and other lines of business teams to understand how departments interact with each other.** Human error is a primary cause of security breakdowns. The better the communication between security experts and company leaders, the easier it is to close some of those error gaps.
- **Develop a comprehensive plan that outlines the risks the organization faces and an action plan for implementation.** Once that is developed, it is up to the company to decide whether or not the consultant is needed to actualize those changes. Many companies simply do not have the internal staff and capabilities to act on those recommendations and operationalize change.

Selecting the right security consultant is about people and performance. The security consultants you work with should demonstrate that they are a trusted adviser and partner, but they should also have excellent technical expertise on the latest threats and how they operate. Finally, they should be able to relate all of this information into business terms and demonstrate why having good security is good business. Hiring a good security consultant is not a luxury; it is an investment.

articles

Cyber Security Professionals Predict Their Biggest Concerns For 2015

How To Talk To Spooked Customers About Your Company's Cyber Security

Information Security: Is Your Company's Data Running Around Naked?

The Top 5 Information Security Breaches No One Is Talking About

The 6 Scariest Pieces Of Malware

Five Steps To Better Apps: A Cookbook For Mobile Application Security

Three Effective Approaches To Corporate Security

The Internet Of Things Poses New Security Challenges

What The Russian Cyber Gang Password Theft Means For All Businesses

Why Your LinkedIn Profile Might Be A Hacker's Best Friend

A Road Map For Beating Hackers At Their Own Game

How To Conduct An Information Security Gap

What Do Information Security Consultants REALLY Do?

The Year In Cyber Security: Sony's Hack Scandal And Various Retail Data Breaches

14

The Year In Cyber Security: Sony's Hack Scandal And Various Retail Data Breaches

by Sue Poremba

When looking back on the cyber security stories of 2014, there is one type of event that clearly stands out above all others: data breaches against major corporations, particularly retail operations. "While 2013 was a bad year for IT security, there's no disputing that 2014 was the worst," said Kevin Jones, senior IT security architect for Thycotic. "Whether it was insider threats, anonymous, or nation-state hackers, 2014 was a bad year for anyone whose job is to protect sensitive data from unsanctioned access."

But, while data breaches against retailers may be the top story of 2014, there's a lot that a "year in review" can tell us about the **state of information security today** … and what it may be like tomorrow.

Year of the Data Breach

Point of sale devices have come under a lot of fire in 2014 as they were the source for the breaches that hit companies like Home Depot, Dairy Queen, Goodwill, and countless other companies (Target marked the beginning of this trend, but that breach was revealed in 2013). According to SentinelOne Labs' **Advanced Threat Intelligence Report**, point of sale devices don't have security built into the systems, and most rely on Windows XP as an operating system. It was a security failure waiting to happen.

"The consumer-related data breaches in 2014 really underscore a larger point of concern," Jones explained. "Companies that have enormous resources dedicated to infrastructure security at point of sale terminals are failing. This has bad implications to the safety of shoppers. This year highlights a worrying trend that credit cards and traditional point of sale terminals are not something we can depend on in the future. "

Jeff Foresman of Rook Security doesn't expect this trend to come to an end any time soon, even as companies look forward to virtual payment options and credit card regulations change. "Hackers have established an eco-system that I believe is quite profitable. Hackers are either outsourcing the malware development or purchasing customized malware so they can focus on their hacking activities. Once hackers steal the card data, they use other people called 'Carders' to sell the stolen card data. Based on the number of breaches in 2014, I would expect this is a successful model for many hackers, and I expect them to be highly motivated to continue."

The Insider Threat

The FBI and Department of Homeland Security **released a warning** about the rising threat of malicious insiders – the employees who either purposely or unknowingly cause security threats to an organization. The 2014 **Verizon Data Breach Investigations Report** also reported on thousands of situations where someone connected to the company was responsible for corporate data leaks. At the same time, companies aren't providing enough data security education and training to staff.

continued on next page

Many of 2014's most prominent news stories were cyber security focused.

articles

Cyber Security Professionals Predict Their Biggest Concerns For 2015

How To Talk To Spooked Customers About Your Company's Cyber Security

Information Security: Is Your Company's Data Running Around Naked?

The Top 5 Information Security Breaches No One Is Talking About

The 6 Scariest Pieces Of Malware

Five Steps To Better Apps: A Cookbook For Mobile Application Security

Three Effective Approaches To Corporate Security

The Internet Of Things Poses New Security Challenges

What The Russian Cyber Gang Password Theft Means For All Businesses

Why Your LinkedIn Profile Might Be A Hacker's Best Friend

A Road Map For Beating Hackers At Their Own Game

How To Conduct An Information Security Gap

What Do Information Security Consultants REALLY Do?

The Year In Cyber Security: Sony's Hack Scandal And Various Retail Data Breaches

14

continued from previous page

"Employees continue to be the source of most security issues in organizations. They may be the victims of social engineering, or don't have the education about what kind of file attachments are safe and not safe to open," said Jones.

As cybercriminals become smarter and phishing emails become more sophisticated, employees will continue to put corporate data at risk.

Cyberespionage

As 2014 drew to a close, the hack against Sony dominated all cyber security conversations.

As this article goes to press, the attacker remains a bit of a mystery. While the FBI and others initially pointed fingers at North Korea, there is a **growing amount of skepticism** regarding North Korea's participation.

No matter who is responsible, the Sony hack spotlights a concern that is just beginning to bubble to the surface: cyberespionage. As Mike Elgan wrote in **eWeek**, "we seem to be entering a new era of bona fide cyber-war, where two nations engage in frequent attacks that are claimed to be retaliation for previous attacks."

Lateral Movement

One of the big trends in 2014 has been around attackers and the concept of lateral movement within an organization post-compromise, said Marc Maiffret, CTO for **BeyondTrust**. A wide variety of high profile breaches have shown that attackers consistently seek to gain a foothold into a corporate environment by leveraging vulnerabilities, and from there look to gain access to further privileged accounts which can be used to break into other systems within the target corporation.

"By the time hackers have gained access to corporate servers, there is not so much hacking taking place as simple abuse of existing stolen user account credentials," he added. "The leveraging of privileged accounts is something that has gained a lot of attention in 2014 and will continue to in 2015 as organizations struggle on bridging the gap between traditional security barriers and IT operational tasks."

DDoS Atttacks

Distributed Denial of Service (DDoS) attacks increased dramatically in 2014, in both scale and sophistication. For example, a "big" attack in early 2013 was on the scale of a few Gbps, according to Mark Kraynak, Chief Product Officer for Imperva. To be considered "big" now, an attack has to be a few hundred Gbps. Also, more than 80 percent of DDoS attacks are multi-vector attacks.

"We're seeing the attackers change vectors as targets start to mitigate," said Kraynak. "In other words, DDoS is beginning to resemble APT." He added that bots are getting smarter, many with the ability to defeat cookie-based challenges.

Unauthorized Disclosure of Electronic Protected Health Information

The security of medical records has been in the news in 2014, in part because of the **concerns surrounding Healthcare.gov**. Arlie Harman, a Consultant at **Rook Security**, adds that 2014 has seen a dramatic change in the sources of unauthorized disclosure (breach) of electronic protected health information (ePHI).

"In the past, most breaches were due to either mis-configurations of information systems or the loss/theft of unencrypted devices containing ePHI," Harman said. "In April, the FBI released a private industry notification (PIN) warning the healthcare industry that 'Cyber actors will likely increase cyber intrusions against health care systems – to include medical devices – due to mandatory transition from paper to electronic health records (EHR), lax cybersecurity standards, and a higher financial payout for medical records in the black market.'" This summer, Community Health Systems was breached by an external group of hackers attacked, with the records of 4.5 million patients stolen and/or compromised.

Expect these trends to continue into 2015. One thing that is certain about cybercriminals – once they find a type of attack that works, they'll stay the course until it is no longer financially feasible.

articles

Cyber Security Professionals Predict Their Biggest Concerns For 2015

How To Talk To Spooked Customers About Your Company's Cyber Security

Information Security: Is Your Company's Data Running Around Naked?

The Top 5 Information Security Breaches No One Is Talking About

The 6 Scariest Pieces Of Malware

Five Steps To Better Apps: A Cookbook For Mobile Application Security

Three Effective Approaches To Corporate Security

The Internet Of Things Poses New Security Challenges

What The Russian Cyber Gang Password Theft Means For All Businesses

Why Your LinkedIn Profile Might Be A Hacker's Best Friend

A Road Map For Beating Hackers At Their Own Game

How To Conduct An Information Security Gap

What Do Information Security Consultants REALLY Do?

The Year In Cyber Security: Sony's Hack Scandal And Various Retail Data Breaches

Why choose Sungard AS?

More than 30 years of experience supporting complex IT operations and providing availability management.

Highly flexible tailored solutions to support customers' unique business and IT requirements.

Managed services ranging from hosting to virtualization to cloud, in a resilient, secure, enterprise-grade IT environment.

Breadth of services and expertise to transform and operate business-critical hybrid IT environments.

For more information please visit our website at:
www.sungardas.com/solutions

Sungard Availability Services around the world

North America
Corporate Headquarters
680 E. Swedesford Road
Wayne, PA 19087
800-468-7483

Belgium
Pegasus Park
De Kleetlaan 12b
1831 Diegem
Belgium
+ 32 (0)2 513 36 18

France
93, Cours des Petites Ecuries
77185 Logne
France
+ 33 (0)1 64 80 61 61

Ireland
Unit 5 Beckett Way
Park West Business Park
Nangor Road
Dublin 12
Ireland
1 800 36 59 65
+ 353 (0)1 46 73 650

Luxembourg
6, Parc Syrdall
L-5365 Münsbach
Luxembourg
+ 352 35 73 05 30

Sweden
Sandhamnsgatan 63
Box 27 157
102 52 Stockholm
Sweden
+ 46 (0)8 666 32 00
info@sungardas.se

Sungard IT Availability (India) Private Limited
2nd Floor, Wing 4, Cluster D
MIDC Kharadi Knowledge Park
Pune – 411014
India
+ 91 20 673 10 400
info.asindia@sungardas.com

Sungard Availability Services UK Limited
United Kingdom
& European Head Office
Unit B Heathrow
Corporate Park
Green Lane
Hounslow
Middlesex
TW4 6ER
+ 44 20 8080 8002
0800 143 413
infoavail@sungardas.com

About Sungard Availability Services
Sungard Availability Services provides managed IT services, information availability consulting services, business continuity management software, and disaster recovery services.

To learn more, visit **www.sungardas.com**
or call 1-888-270-3657

Connect with Us