
What Every CEO should know about IT SECURITY

Foreword

What could be more important to any business than data? Whether it's customer information or stores of intellectual property, it's the lifeblood of any organization. Unfortunately though, most CEOs aren't aware they need to make it a priority.

In fact, according to our 2011 State of the Endpoint Survey conducted by the Ponemon Institute, nearly half of responding technology decision-makers said they couldn't solve their security problems because it just didn't interest their CEO enough.

Now, as a CEO, I understand how security could take a backseat to your other business priorities. I know you've got to lead an organization to profitability and success without getting mired in technical details. But as a long-time security industry veteran, I have also seen the heavy toll that ignoring risks can take on a business. While you can't solve every data security issue, you should break it down to your top few. As is with everything, protecting your vital data is a balancing act with cost and organizational productivity.

TRUST ME, WHEN IT COMES TO A DATA BREACH, IT'S NOT IF BUT WHEN. AND IT MAY EVEN BE NOW.

You are vulnerable to attack because everyone is vulnerable to attack. And I want to help. Given the dual nature of my experience--bottom-line-oriented CEO on one hand, security expert on the other-- I'm in a unique position to talk to my executive peers plainly about data security. I've filtered out the techno babble and the marketing mumbo jumbo to serve it up to you straight.

SHARE THIS VIDEO

What I offer you now is a CEO-to-CEO explanation about why you need to care about IT security and how to use your leadership role to build a culture of security within your organization. Doing so could very well make or break your company's ability to deliver its product to customers.

Pat Clawson | Chairman & CEO, Lumension

SHARE THIS EBOOK

Table of Contents

SHARE THIS EBOOK

1. IT Security is a Boardroom Issue

Take a minute to think about the data that drives your business: the R&D breakthrough that will soon give you a leg up on the competition, the schematics for your newest product, the data you use to negotiate contracts, the marketing plans that will launch your sales into the stratosphere, the comprehensive customer list and their personal information that keeps you in contact with your buyers.

All of those information stores are critical to your organization's health. How is your staff protecting this data? Do you know? Shouldn't you know?

CONTRARY TO WHAT SOME CEOS MAY THINK, INFORMATION SECURITY IS ABSOLUTELY A BOARDROOM ISSUE.

When you hear your CIO or CISO throw around foreign terms like web application firewalls, antivirus signatures or whitelisting, it's easy to dismiss the majority of it as technical minutiae not worth your leadership time.

Ignore IT security and you're going to learn the hard way, like many before you, if you don't address it in the boardroom, you'll be addressing a breach in your financials--or worse yet, in the newspapers. If a business fails to set security policies, or sets them so loosely that it suffers a highly publicized attack, it could find itself ostracized by its largest customers, partners, even government. Just ask Citigroup. Or Bank of America. Or better yet, ask Sony — estimates report its recent blunders have cost the company millions of dollars and countless more in customer goodwill. These aren't technology issues; these are core business issues. And no longer is data security only a concern for banking, healthcare and government agencies.

SHARE THIS VIDEO

So how do you narrow it down to a boardroom issue? You have a duty to ask your frontline technologists how the organization is keeping its data safe, what forms of measurements are in place to track protection measures and attacks, and how policies are being enforced. You have fiduciary responsibility to understand what data you own, where the greatest risk is and what you're doing to protect it.

> "If I could have a CEO boot camp, I'd say, 'Make sure you put security top of mind to all of your direct reports: your CFO, your CIO, your HR people, your sales people and so on.' For most businesses today the product is information and security is key. So you have to make sure that your top reports understand security is part of their evaluation. It's not just the CIO's responsibility. It is part of life for every one of your direct reports."
>
> John Pescatore | Gartner

2. Ignoring Security Will Cost You

Data breaches cost companies millions of dollars every year in forensic investigations, regulatory fines and remediation costs but the largest cost of ignoring security might be much more difficult to measure. Brand is the bedrock upon which most major enterprises build. The loss of brand equity caused by lax security practices is perhaps the largest risk of all.

SHARE THIS VIDEO

EXECUTIVES WHO IGNORE SECURITY NOT ONLY GAMBLE WITH THEIR COMPANY'S BRAND AND GOOD NAME, THEY ALSO LOSE AN OPPORTUNITY TO SET THEMSELVES APART FROM THE REST OF THE CROWD.

Of course, plenty of damages from breaches can be measured. Industry figures show that in 2010, the average data breach cost organizations about $7.2 million[1] per incident or $214 per compromised data. Included within these figures are estimates for:

- loss of customer business due to abnormal churn
- forensics investigations
- compliance remediation costs and regulatory fines
- notification of breach victims and government officials

The shame of it all is once this money has been laid out, the new scrutiny you'll face after a breach will force your company to spend on the security program you should have implemented in the first place. Why not spend that money up front and avoid all of those millions in breach costs? While there is no silver bullet, you can narrow the aperture by understanding your top risks.

Among the Hardest Hit

Sony's Security Megabreach

Sony's data breach should be an eye-opening account for all of us on what could go wrong when it comes to data loss. Reportedly, more than 100 million Sony user accounts were compromised at a cost to the company estimated in excess of $170 million. From the beginning, Sony did not respond to the crisis with best practices – in security or communications.

Misstep Number 1.

Risk management was overlooked by Sony leadership. Many of the issues reported could have been easily mitigated thereby preventing this mega breach from happening in the first place. While any company can have a security issue, a company that has not followed basic risk management best practices will fall prey easier and will suffer a deeper and more lasting impact than a company who has not.

Misstep Number 2.

To make matters worse, Sony did not follow effective crisis communication best practices in the beginning. What angered Sony customers perhaps the most was the delay of a week or more after the company originally discovered the breach before notifying customers.

Because data breaches can happen to anyone, you should ask yourself, what are you doing to make sure your company doesn't make similar mistakes?

Read more about the Sony breach and what should have been done on our blog, Optimal Security.

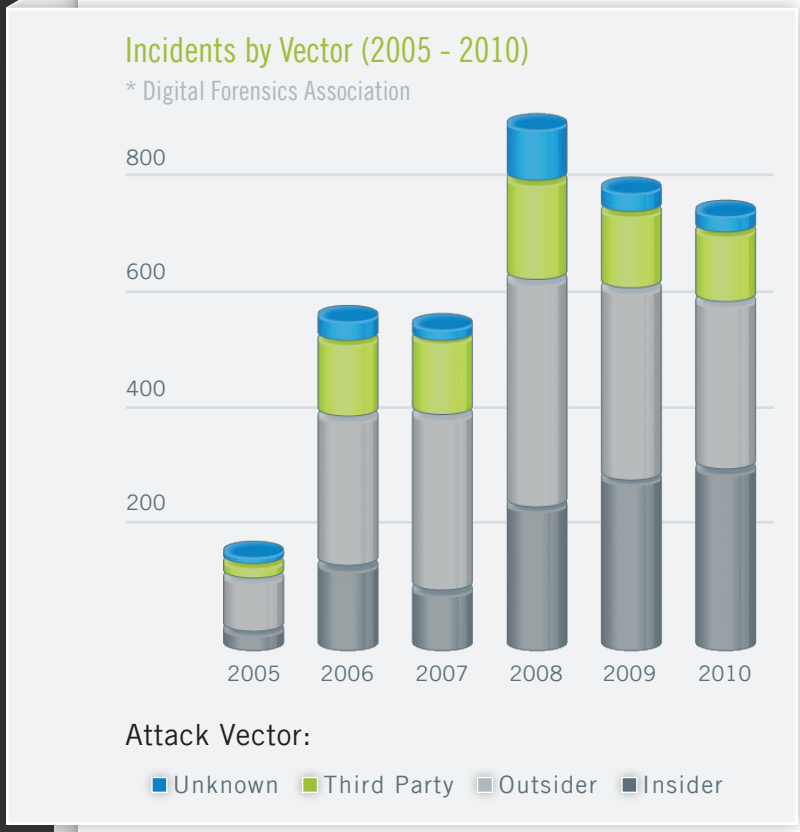
1. 2010 U.S. Cost of a Data Breach Ponemon Institute

3. Hackers Come in Different Forms with Varying Motivations

Too many CEOs believe that the 'stealthy hackers' their IT teams warn them of are simply boogeymen they're using to beat leadership into budgetary submission. The truth is these attackers are very real and they're picking off organizations whose executives fail to make security a priority.

In 2011, the Digital Forensics Association studied 3,765 publicly disclosed data breach incidents from 33 countries between 2005 and 2010, accounting for over 806 million known records exposed.

As you can see, outside hackers represent the largest category of attacks, followed by insiders.



Who's behind this massive loss of data? There are very savvy criminals out there looking to profit from the sale of your customer data and your proprietary information.

SHARE THIS VIDEO

To satisfy their need for financial gratification, the attackers are able to convert just about any type of data into cash through a black market economy that rewards bad guys for their digital plunder. Sophisticated criminal networks are now supplying the black market with more than $5.6 billion in stolen corporate and personal information obtained by exploiting known security flaws.

Data theft isn't always a direct cash-stolen endeavor. Other hackers are less interested in profiting from your organization's financial transactions and more interested in taking your intellectual property. Corporate espionage remains alive and well in the digital age as hackers zero in on new product designs, manufacturing schedules and even anticipated sales prices because that information is, of course, very valuable to many of your competitors. Hackers are quick to grab it and offer it up to the highest bidder.

SHARE THIS EBOOK

We've also seen the rise of a new kind of hacker recently– the hacktivist. Rather than trying to make a profit, this hacker is looking to make a point and he's using your company to do so. Hacker groups like Lulzsec and Anonymous have attacked numerous corporations in protest of their actions.

Such was the case with Sony after the company prosecuted an individual who tried to manipulate Sony hardware. Hacktivists have also hit every level of government, like the Arizona Department of Public Safety in protest over the state's immigration policies and the City of Orlando's website to object to the arrest of citizens as they fed the homeless in a city park without a permit.

Hackers Aren't the Only Ones to Worry About:

Insider Threats

It isn't just those well-funded bad guys outside the business that you should worry about, either. There are also numerous threats much closer to home —literally inside your business.

The risks posed by employees and trusted partners can run from out-and-out fraud to simple user error. Typically, both are caused by lack of controls and poor oversight of employee computer activities, and exacerbated by the consumer-grade mobility and collaboration tools that have permeated your workforce.

Too many companies don't monitor employee interaction with intellectual property and sensitive data and they end up paying a steep price for their lack of verification.

Does your organization have a way of tracking how information is being copied and transported? Does it have a way of protecting the data at rest, in motion and in use? As a CEO, you should at least know the answer to those questions.

4. Attack Vectors Continue to Evolve

The scary thing about cyber risks today is the companies that completely ignore security may have already been breached and don't even know it. The modern hacker's MO is not to make a splash attacking your infrastructure. No, they're more concerned with attacking you quietly and stealing as much data as possible, without your knowledge.

They start by continually running automated scans of the internet looking for common vulnerabilities to stealthily exploit, no matter how big or small the company with those problems.

Then they come at you with malicious malware created to disrupt, deny, steal... you name it. The amount of malware has skyrocketed in volume and jumped in sophistication to meet these criminal's own bottom-line financials as they've quickly built up their illegal empires.

There are many different kinds of malware out there today. Some of it is designed to cast a wide net, scouring the Internet for vulnerabilities. Others are very targeted. Regardless of the type, criminals can be in and out of your network without ever being noticed.

They're not just attacking your Microsoft operating system. To a larger extent, they're going after just about any web-based applications you use in the name of productivity. According to a recent report, among the top 50 applications installed on the typical endpoint, vulnerabilities increased 71 percent in 2010[2]. And this is only getting worse in this day and age of virtualization, cloud and mobile applications.

Chances are virtualization, cloud, and mobile deployments have revolutionized the way your IT department delivers services to your business units. They certainly all offer businesses a ton of opportunity to cut down on capital expenses and operational costs.

While virtualization makes it possible for businesses to affordably deploy more computing firepower for less outlay in cash, with great opportunity comes great risk. Virtualization and cloud introduce a spate of operational headaches and security problems that many company CEOs, and even CIOs, fail to properly consider before they rush headlong into it.

Virtual Desktops

Take your in-house desktop virtualization deployments, for example. This is the first time in computing history that we can give people a virtual desktop and let them work without maintaining computing hardware. The problem is those virtual desktops are subject to whatever infections may

2. Secunia Yearly Report 2010 Secunia Yearly Report 2010

be sitting on the host operating system and vice versa. Without specialized technology to protect those virtual images and prevent nasty viruses from swimming back and forth between the virtual host, you could have either one infecting the other. It gets messy very quickly. The problem is that the charm of cost-savings has drawn most organizations to deploy virtualization before the security technology has had a chance to catch up with the rest of the innovation.

While you can't just toss out virtualization because of these issues, CEOs and other executives need to figure the security risks into their cost-savings equations.

Cloud Computing Risks

The issues around cloud computing are even more complicated because not only are these environments vulnerable to all of the risks presented by virtualization, but cloud-bound data is also outside your sphere of influence.

Today's cloud providers offer far too few protections or assurances about your data because they haven't been pressured to do so. Many CEOs and CIOs have been seduced by the savings of the cloud that they've ignored the risks and signed on with little knowledge of how their providers are protecting critically important data.

Anytime your data leaves the corporate bubble, you and your employees need to ask yourselves whether you have a contracted chain of trust with what is essentially the weakest link in the chain, your business partner. If you don't, you can bet you'll see that risk come back to haunt you – just like it did for the dozens of big brands impacted by the breach at email service provider Epsilon.

In the spring of 2011, this company was the weak link in the security chain for big corporations like JPMorgan Chase, Hilton, Disney and more. The hackers don't make their money by being stupid. In the case of Epsilon, they knew the best way to go after seven of the Fortune 10 was not to attack those enterprises' well-fortified data structures. All they needed to do was go after the weakly defended marketing firm.

5. Compliance Does NOT Equal Security

Unfortunately, most executives don't think about security beyond complying with security regulations such as HIPAA, Sarbanes-Oxley, PCI Data Security Standards (PCI DSS) and for anyone hoping to do business in Massachusetts, the Massachusetts Data Privacy Law.

I can't reinforce this enough – compliance does not equal security. Take the sensational story of credit card processor Heartland Payment Systems to heart. In 2009, Heartland suffered what is still the biggest breach on record. Attackers stole more than 130,000,000 credit and debit card numbers at a cost to the company that exceeded $12 million. At the time of the breach, the company was deemed compliant with PCI DSS.

Of course, you can't ignore compliance. Organizations that don't create solid compliance programs risk fines and exhaustive external audits. According to a recent survey[3], many firms can't even meet the bare minimum security standards laid out by regulators.

More than half of organizations say they've recently failed regulatory compliance audits and another nine percent have already failed an audit that has resulted in a fine—from either the government or an industry.

SHARE THIS VIDEO

It's obvious your peers are standing up and listening because their feet are being held to the fire by regulators. Just about half of organizations say they plan to spend extra cash in 2011 to meet compliance demands, with spending expected to rise 21 percent. In some ways, this can be a good thing.

But compliance as a security driver is a double-edged sword. It has definitely helped bump up the visibility of security topics amongst the C-suite. At the same time, though, it has made too many executives equate compliance rules with real, comprehensive security. Instead, separate the issues of compliance and security in your own mind and for your staff. Make sure you're meeting the compliance guidelines - that's one issue. Separately, ensure strong security.

3. 2011 Risk and Compliance Outlook report, McAfee

6. Balancing the Need for Security with the Need for Productivity

The reign of desk-bound office workers has come and gone. The escalation of mobile devices and applications within our enterprises over the last few years is absolutely unprecedented and it has forever changed the way we work.

SHARE THIS VIDEO

But mobility has thrown such a serious curve-ball into the security mix that businesses are simply striking out at trying to keep up. Just look at all of your employees with their iPads, Androids, Blackberries and USB devices. Many of these devices aren't even owned by your business, and yet your employees are downloading and touching tons of valuable corporate data while using them. This alone should be enough to tell you that your valuable data is leaving the safety of the corporate network completely unprotected. It's in the wild, it's unmanaged and it is on current and former employees' devices without control.

Seven Things Your Employees Won't Tell You

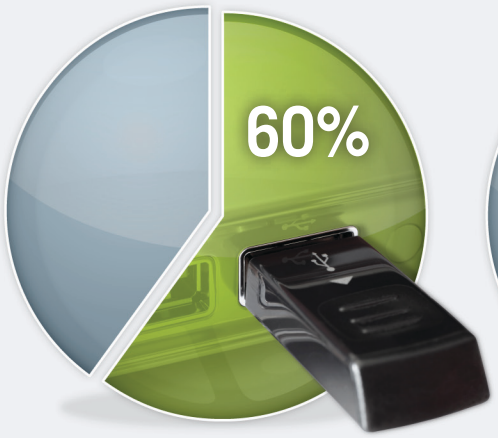
» By Rob Pegoraro | CLICK TO READ

As you guide your technology staff, think about specific times when employee flexibility overrides security concerns and vice versa. This takes solid data and device classification, role-based access policies and the right tools to enforce those policies.

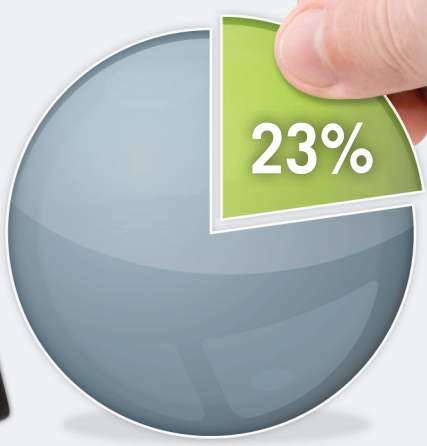
Ideally, your organization needs to gain better visibility into who is connecting into the network, with what mobile devices, how and when they're accessing data and how much of that data is being taken out from under the corporate umbrella of data protection. As a CEO you may not need to know the particulars of how that visibility is achieved, but it does have to be there for you. Without it, you'll never be able to make intelligent decisions about the policies you and your executives make about appropriate mobile use within the organization.

User Habits and Influence

76% of security and IT leaders believe user influence on decisions to acquire devices and applications is increasing.



The majority of IT leaders say their companies have policies regarding connection of personal devices on the network, but almost 60% reported unauthorized connections still occur.



23% of organizations have experienced a serious security incident or breach due to the connection of a personal device on the network.

Security for Business Innovation Council, 2010

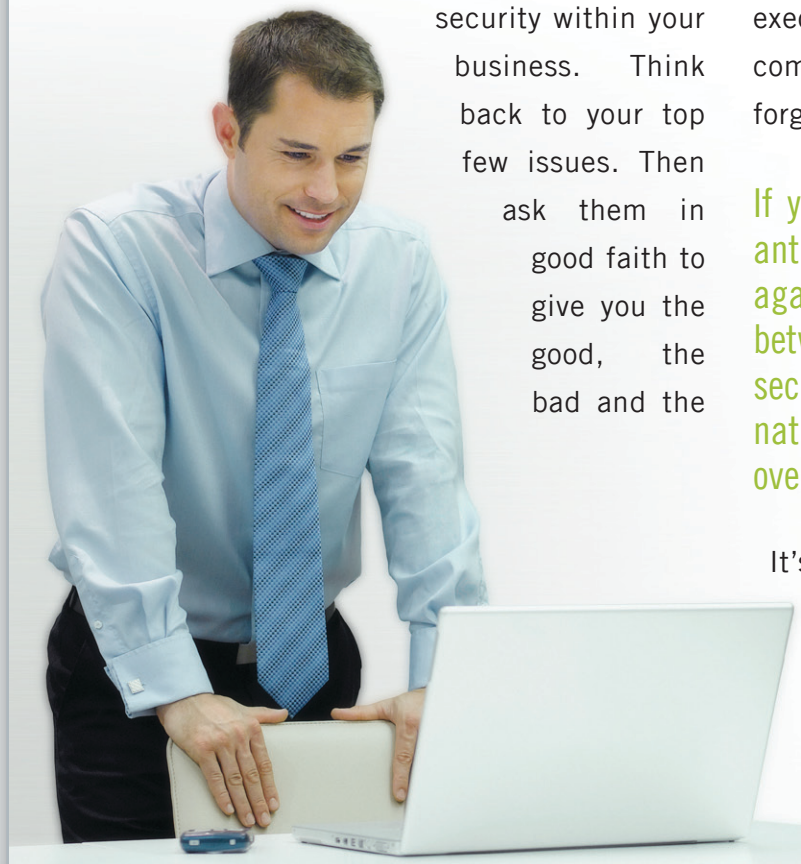
7. Security is NOT Just a Technology Problem

SHARE THIS VIDEO

All CEOs worth their salt figure out very early on that in order to be successful they've got to let their employees do the specialization. You can't be the master of everything you're doing inside your business--that's why you have a stable of competent employees.

However, you do need to closely monitor their progress and guide their decisions in order to ensure they're sticking to your vision of business priorities. That is just as true for IT security decisions as it is for financial choices.

If your organization is to stay on top of risks and develop a culture of security, you and your senior management team need to ask your technology staff to give you the real picture of the state of security within your business. Think back to your top few issues. Then ask them in good faith to give you the good, the bad and the ugly about how well (or poorly) you're protecting important data, including regular reports on where the data resides, what kinds of risks it faces, how it is currently protected and a measurement of that protection.



One of the real dangers of working with technical executives is that some of them tend to fall so completely in love with certain technologies they forget their overarching goals.

If you think that your corporate installation of antivirus (AV) software is a foolproof talisman against today's security threats, think again - between 2007 and now, the number of threats security researchers found needing new AV signatures rose from around 250,000 per month to over 2 million per month.

It's a sickness suffered by many in security, who unfortunately focus on buying and implementing tools they view as a panacea.

SHARE THIS EBOOK

As a CEO you probably already know there's no single product in the world that can completely solve a complex business problem. It is no less true for information security than anything else in the business.

As in many other aspects of the business, technology tools support a solid foundation laid by effective policies and processes. It is your job as the head honcho to guide your CIO and CISO to make sure they aren't using technology as an ineffective crutch.

These "other things" need to include risk assessment, standardized procedures, boundary setting around what employees should and shouldn't be doing with systems and with data, and also setting baselines on how systems are configured. From there, the technology can monitor and enforce all of those policies and procedures, providing reporting to prove to the auditors that everything is working.

In order to make improvements, consider having regular conversations about what your technologists would do if they had a 'magic wand' and how they would fix problems if budget wasn't a problem. From there you can have meaningful discussions about how to come to a cost-effective compromise that meets your organization's risk appetite and heads off costly incidents.

> "So if every time there's a problem and the only thing your CISO is suggesting is technology, you should poke 'em with a stick. You should say, 'Wait a minute, where's the process change or the other things that always have to go with technology to make it work.'"
>
> John Pescatore | Gartner

If your CISO is doing a good job setting policies, the SANS Institute suggests that they will be:

- identifying all of the assets that we are trying to protect
- identifying all of the vulnerabilities and threats and the likeliness of the threats happening
- deciding which measures will protect the assets in a cost-effective manner
- communicating findings and results to the appropriate parties (i.e. you and the board)
- monitoring and reviewing the process for improvement along the way

SHARE THIS RESOURCE

Be Aware of What You Share

Because the biggest risk to an organization is often the behavior of the people inside, Lumension has launched a video series for technology users.

Share these basic strategies for protecting both personal information and organizational data with your company employees. Other videos in the Lumension resource center include topics like phishing scams, secure websites, secure passwords and what is a computer virus.

lumension.com/be-aware

Conclusion: The Security Role of the CEO

SHARE THIS VIDEO

Because security can have such a dramatic effect on an organization's bottom line, you have an obligation to provide strong leadership on the matter.

According to many of the CISOs we speak with here at Lumension, the only way to get user buy-in for major infosec initiatives is by relying on support from the top of the food chain. As a CEO you're the first person who must nourish a culture of security. Without that, you will have zero chance of good security trickling down across departments and remote offices.

As one of our customers puts it, "When it comes from the CEO, it's a bigger deal than when it comes from the security officer. You're going to get more penetration through your enterprise. The folks in accounting are going to go, 'Oh! It's the CEO!' They don't care about me, but they'll listen to the CEO. There are a lot of companies with silos that are so deep these days that the security departments don't have a lot of visibility. If you can work to get some kind of company message, it's helpful."

START IMPROVING YOUR SECURITY TODAY

So where do you begin? Remember, the bad guys are no dummies—they know how to exploit holes in the network and how to take advantage of offline systems and endpoints in order to gain future access to your data stores.

By implementing some basic security best practices, you will be able to adjust and defend against cybercriminals' new tactics:

1. Change your thinking

Security is no longer the domain of the IT geeks down in the data center. You and your board will be held accountable when you're breached so get involved in the decision making now.

2. Have a plan

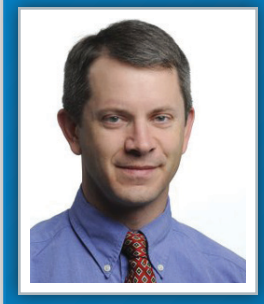
Businesses aren't made secure by accident. And the regulations are simply not comprehensive enough to ensure success on their own. Simplify your view by recognizing you can't solve every problem. Then, appoint business executives to work with technologists (yourself included) to map things out meticulously.

3. Defense in depth

Throwing up a firewall and some antivirus isn't going to cut it in today's threat environment. That plan needs to include multiple layers of technological defense that makes sure attacks don't fall through the cracks.

APPENDIX

Seven Things Your Employees Won't Tell You



By Rob Pegoraro

Your employees certainly don't tell your IT department what they do on their own computers for fun. But they're probably not sharing relevant details about how they work from home either. And if my experience and the stories I heard from co-workers and readers at the Post add up to any guide, your IT department won't be happy to hear the truth.

1) They reuse passwords at multiple sites--from 31 to 43 percent of them in a recent University of Cambridge researcher's study, 10 to 20 percent in older research. This should not be a surprise: When so many sites demand passwords for such low-value uses as the ability to read stories, users will save their creativity for other outlets. It's your IT department's job to remind that whatever else they do, they shouldn't use the same password for your network and any other site.

2) They write down passwords. Nobody should be shocked about this either. Password-expiration policies--especially those with paragraph-long "minimum complexity requirements"--all but invite users to write down each new password after creating it, lest they forget it by the time they get home. Thing is, writing down a password can keep it secure--if you think to stuff it in your wallet.

3) They probably don't understand password strength. If they were to look at a table that showed that adding one more character to a seven-letter password changed the cracking time from days to months (or, at worst, minutes to hours), they might understand where those obnoxious complexity requirements come from. And they might be motivated to choose stronger passwords on their own.

4) They conduct company business on personal e-mail accounts. Consider the ease of remote access provided by, say, an older Lotus Notes installation versus that of Gmail. Busy employees will often use the easiest communications channel available--even if that exposes them to spear phishing attacks. It's not as if they get a bonus for the degree of difficulty involved in working remotely.

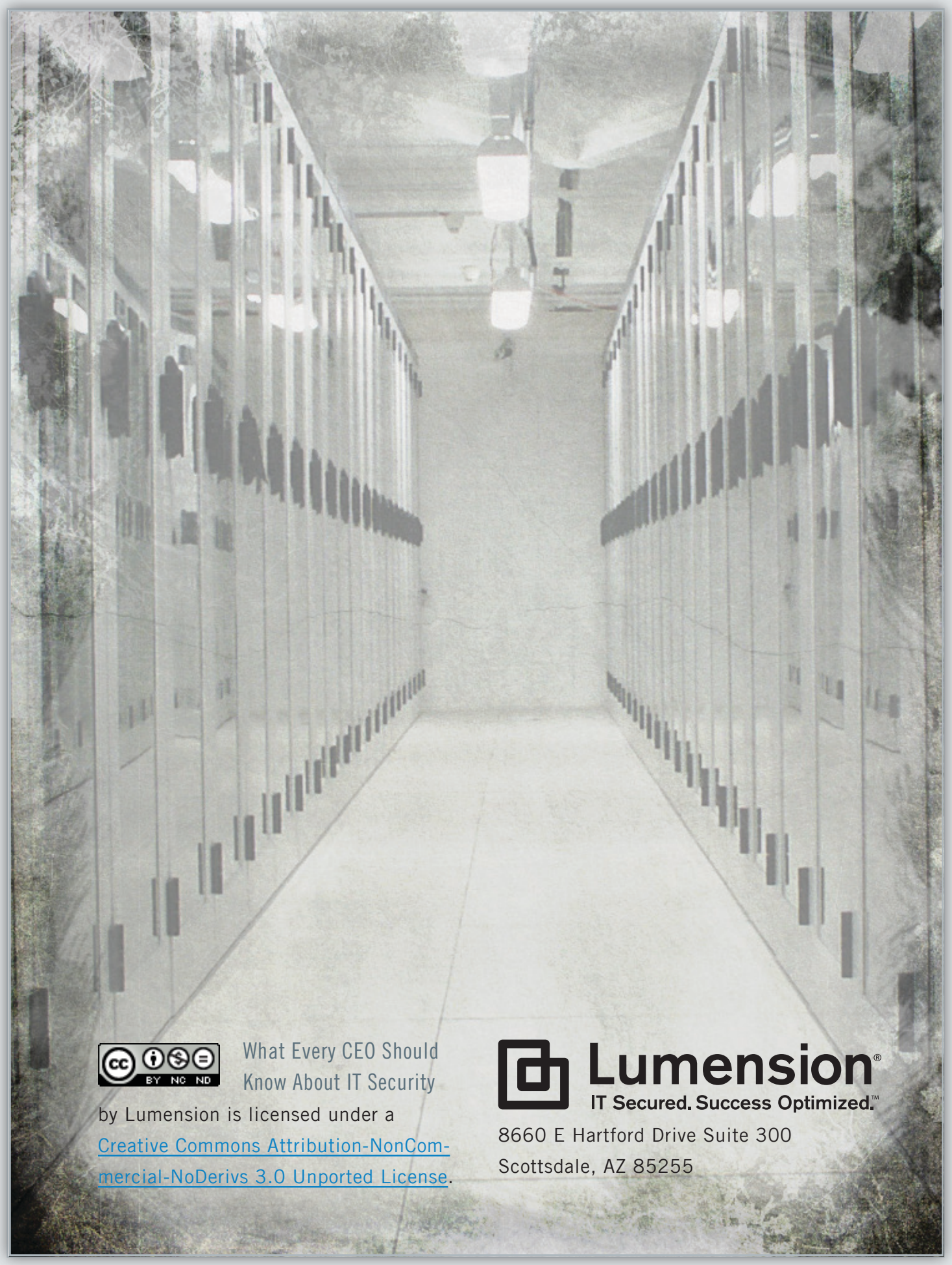
5) They lose flash drives with work documents. See the last sentence of the previous paragraph. To a certain degree, this is an unavoidable downside of the compact dimensions of flash drives. If you're lucky, these drives aren't lost so much as buried at the bottom of a laptop bag or jacket pocket.

6) They don't update the software on their own computers often enough. Sure, they keep Windows and IE or Firefox up to date. But what about the plug-ins in those browsers, which increasingly get attacked directly by malware? The numbers are discouraging: In 2008, Secunia estimated that 25.1 percent of Windows PCs were missing critical updates for six to 10 vulnerable applications.

7) If they get hacked, they won't know how. The hardest conversations I had with readers happened when they asked about malware attacks. Not one of them could tell me how their computer or their account got compromised--which made it difficult to tell them what they should have done differently.

If you're tempted to scold employees about all these failings--don't. Consider the example of the recording industry's battle against file-sharing sites: Nagging listeners didn't help; but giving them honest, easy options like Apple's iTunes and Amazon's MP3 store did. Good security doesn't have to be difficult; it doesn't have to impede productivity. Rather, work together to come up with a solution that works for everyone.

Rob Pegoraro writes about computers, the Internet, software, smartphones, gadgets and other things that beep--from 1999 to 2011 as the Washington Post's consumer-tech columnist, now for a variety of freelance clients--and regularly discusses these topics on radio and TV.



Lumension®
IT Secured. Success Optimized.™

8660 E Hartford Drive Suite 300
Scottsdale, AZ 85255