Everything You Need to Know About Cyber Threats But Were Too Afraid To Ask

Ben Bourne
Director of Customer Success, EMEA

Magdalena Borcal
Director of Customer Success, EMEA

Nathan Birtle
VP Sales and Business Development, EMEA

Boards of directors are too often kept in the dark about the security risks to their organisations.

That's what the Ponemon Institute discovered last June when they surveyed members of the board of directors and IT security experts from the same companies. The Ponemon researchers found that 30 per cent of directors[1] acknowledge that they don't understand the risks that their organisation faces in security matters. Yet more than half of the IT security experts believe that the directors who sit on the boards of their companies don't understand the security environment that they are working in, or the risks it represents.

This is a big deal, considering how many data breaches companies have seen. Some 90 per cent of large companies suffered a cyberattack, according to Kaspersky Lab's 2015 report.[2] The finger of blame for breaches is often pointed at malicious outsiders, cybercriminals who are intent on gathering information through malware and theft.

When people in an organisation fail to recognise basic security threats and how they can affect the organisation, things can get costly pretty quickly. Cybercrime is expected to reach $2 trillion[3] in corporate losses by 2019. Those losses may be the result of simple mistakes that lead to data breaches — an assistant who clicks on a link in a phishing email, a salesperson who leaves his smartphone in a coffee shop, or a board member who opens a malicious attachment sent via a spoofed email account. Without solid security education and training, everyone within an organisation puts their company in jeopardy of a data breach and its fallout, which includes costly fines and often a reputation hit. However, to improve an organisation's security IQ, everyone needs to have a better understanding of where the risks are and what can be done to eliminate potential threats.

Diligent

1. "Dell SecureWorks and Ponemon Institute Present the 2015 Global IT Security Spending & Investments Report" https://www.secureworks.com/about/press/ponemon-2015-global-security-spending-report
2. "90 per cent of companies have suffered at least one cyber attack" Ian Barker, October 7, 2015. BetaNews http://betanews.com/2015/10/07/90-percent-of-companies-have-suffered-at-least-one-cyber-attack/
3. "Cybercrime will cost businesses over $2 trillion by 2019" Juniper Research, May 12, 2015 https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion

THE RISKS

Insiders

The biggest security threat to any company is the people who have direct access to the network and sensitive data, according to a number of studies such as the Verizon Data Breach Report 2016[4] and security monitoring firm Spiceworks' "Battling the Big Network Security Hack"[5] report.

Insider threats come in a variety of ways, but often, these actions are not purposely malicious. Yet, whether malicious or not, these actions still lead to serious security events. Sometimes, it's as simple as losing unlocked devices or using devices that lack data-wipe software, or plugging unverified storage devices into a computer. Even in a large corporation, all it takes is one bad action, one single click, to cause millions in damage, and cost millions to recover from.

A Thomson Reuters survey[6] found that board members create a variety of security risks. For example, more than half of board members continue to print and carry board documents, which could get lost or misplaced. This puts sensitive corporate data at risk of being found and compromised by those outside of the organisation.

Social Media

Social networking is a double-edged sword. On the one hand, it allows corporations to reach their audiences in real time and with targeted messaging. It also allows quick and easy communication between company and client.

But social media can also be the source of cybersecurity nightmares. According to a report by IFSEC Global,[7] an online community for the security industry, the majority of IT and IT security professionals found that social media in the workplace creates a serious risk, but very few organisations are addressing the threat. Your company's social media account could be hijacked and used to launch social engineered attacks meant to scam customers and anyone affiliated with the corporation. This could lead to malware downloads, theft of personally identifiable information, leaks of corporate data or loss of reputation.

Multiple Devices

A Citrix report[8] stated that the average employee uses at least three devices to connect to the corporate network. This matches a GlobalWebIndex study[9] that found that the typical person uses three devices and that number goes up with income levels. Based on this, it is safe to say that most board members own at least four devices. More than 60 per cent will be connecting to the network outside of the office. The Bring Your Own Device (BYOD) movement allows companies to spend less on these devices, but it also means that IT has less control over the software, security practices and overall access.

Expect the security concerns around these devices to get worse. According to research firm Gartner,[10] more than 6 billion devices will be connected to the Internet in 2016. Employees could potentially connect a wide range of devices to a company's Wi-Fi network, and due to vulnerabilities in the operating systems of many of these devices, businesses could fall victim to security risks and backdoor hacks.

Emerging Technologies

Every new technology advancement will eventually become a target for hackers and other malicious actors, and that means the technology board members use could put them, and potentially the organisation, at increased risk. Security experts agree that smart cars, smart buildings and the latest in wearable devices can be — and will be — attacked sooner or later, according to ZDNet.[11] Even if emerging technology isn't directly connected to your business's data centres, the new tech can allow access to the company in other ways. A hacked building security system can open the doors for thieves, which researchers at the University of Michigan[12] proved when they were able to hack into a smart home security system.

User Authentication

User authentication systems, such as using a password, are supposed to safeguard data and accounts, but stolen passwords are also a gold mine for data thieves. It isn't just the passwords themselves that are valuable, a Trend Micro report[13] found, but how access to these accounts can have a deeper security impact, as a board member for Shipley Energy[14] discovered when a hacker mined her email and computer after gaining access to her password. Having a single password/username combination makes that mining work simple for cybercriminals. By not enforcing the company-wide — and that includes boards of directors — use of multi-factor authentication systems, entry into the network by unauthorised users is easy.

Third-Party Vendors

Third-party vendors were to blame for some of the highest profile breaches of the past few years. Target may be the most infamous example, as its breach was caused through security mistakes made by an HVAC contractor. As MacDonnell Ulsch

4. "Leaky end users star in DBIR 2016" Susan Richardson, May 23, 2016. Data on the Edge, http://blog.code42.com/leaky-end-users-star-in-dbir-2016/
5. "Battling the Big Hack: Inside the ring and out… IT pros plan to land some blows in 2016" Spice Works, December 2015: https://www.spiceworks.com/marketing/resources/reports/it-security/?utm_function=dg&utm_channel=swemail&utm_source=securitypromo&utm_medium=e-mail&utm_campaign=2016itsecurity&utm_content=151216-button&mkt_tok=3RkMMJWWfF9wsRoksqrMd%2B%2FhmjTEU5z16egrXaS2gIkz2EFye%2BLIHETpodcMTsFgNrvYDBceEJhqyQJxPr3MJNkN1NxvRhnjCQ%3D%3D
6. "Are your board members a security risk?" Thomson Reuters, http://www.biia.com/is-your-board-member-a-security-risk
7. "Global Survey: Malware attacks up because of social media" IFSEC Global, October 12, 2011. http://www.ifsecglobal.com/global-survey-malware-attacks-up-because-of-social-media/
8. "7 Enterprise Mobility Statistics You Should Know" Citrix, June 12 2015 https://www.citrix.com/articles-and-insights/workforce-mobility/jun-2015/7-enterprise-mobility-statistics-you-should-know.html
9. "Digital consumers own 3.64 connected devices" Global Web Index, February 18, 2016 http://www.globalwebindex.net/blog/digital-consumers-own-3.64-connected-devices
10. "6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Per cent From 2015" Gartner Report, November 2015, http://www.gartner.com/newsroom/id/3165317
11. "A huge security breach traced back to an unsecured IoT device will happen within the next two years, warn security experts" Danny Palmer, July 1, 2016. ZD Net, http://www.zdnet.com/article/the-first-big-internet-of-things-security-breach-is-just-around-the-corner/
12. "Hacking into homes: 'Smart home' security flaws found in popular system" Nicole Casal Moore, May 2, 2016. Michiga News, University of Michigan. http://ns.umich.edu/new/multimedia/videos/23748-hacking-into-homes-smart-home-security-flaws-found-in-popular-system
13. "How much your passwords are worth to cybercriminals" Market Watch, December 31, 2015 http://www.marketwatch.com/story/how-much-your-passwords-are-worth-to-cybercriminals-2015-12-11
14 "Kill the password: a string of characters won't protect you", Mat Honan, November 15, 2012. Wired, https://www.wired.com/2012/11/ff-mat-honan-password-hacker/

pointed out in TechTarget[15], third-party vendors are often trusted "quasi-insiders," which gives them a large amount of insider access without the same level of security controls as regular insiders.

"This is why third-party management and service-level agreements (SLAs) are so critical in the management of risk," Ulsch wrote.

Of course, many third-party vendors do take these risks seriously, keeping clients' security needs in mind at all times. Quality third-party vendors tend to be open and willing to discuss a client's security needs, and to work together with the client to ensure networks are safe and all concerns are addressed.

TYPES OF ATTACKS

Malware

Malware is the comprehensive term for the most common and most familiar cyber threats, such as viruses, Trojans, worms or ransomware.

Malware often comes in families, based on its coding, with more than 1,500 malware families identified as recently as fall 2015, according to the trade publication *Help Net Security.* [16]

Some of the most popular malware families are Conficker, Sality and Cutwail. Once in the system, every strain of malware has a particular role to play. Some target financial records or other types of data, others are designed to make your system inoperable, and still more may turn your machine into a bot, sending out spam.

No one is immune to malware attacks, and board members may be at even greater risk because they may be connected to multiple organisations. Malicious actors use a wide variety of attacks to infect your system with malware. These attacks include:

- **Phishing attacks** mimic legitimate communications in order to fool the email recipient into clicking on a bad link or opening a malware-loaded attachment. They come in a variety of formats, according to security company Tripwire.[17] The average phishing email is sent randomly in hopes that someone will take the bait. Spear phishing attacks are more directly targeted to specific people and often appear to come from trusted sources sharing legitimate work-related documents. Whaling takes spear phishing to a higher level, targeting executives, top-level personnel, and high-profile individuals like celebrities and politicians. Whaling emails are highly personalised anddifficult to detect.

- **Distributed denial of service attacks** do exactly as the name implies; they are meant to deny service to the network. DDoS attacks, as defined by the Department of Homeland Security, are a favourite attack method of hacktivist organisations like Anonymous, which shut down websites in order to make a political statement or protest.

- **Advanced persistent threat** is a corporation's worst nightmare. The goal of the APT is to steal as much information as possible, according to an article published in the journal *Network Security.*[18] A hacker, usually part of a cybercriminal ring, infiltrates the network and remains undetected for long periods of time. This gives the hacker virtually unlimited access to information flowing through the infrastructure. You can detect an APT takeover in different ways, such as unusual login activity or large unplanned data transfers.

- **Zero-day attacks** come through vulnerabilities in a software programme. Hackers rush to use these vulnerabilities before the hole is discovered and patched. To avoid a zero-day attack, experts urge users to deploy software patches as soon as they are offered, according to the firm Malwarebytes.

- **Man in the Middle Attacks (MitM)** are the kind that eavesdrop on communications so that the hacker can insert himself into the middle of these online conversations in order to gain information. For example, a MitM attack, as the experts at Veracode[19] discuss, could hijack the transaction between a bank and a person making a financial transaction, and would then have access to account numbers, names and passwords.

- **Malvertising and drive-by downloads** are different types of attacks, but are similar in how the malicious actor takes over someone else's website. Malware code is injected into the site, almost always without the owner's realisation. In a malvertising attack, the malware is downloaded when an infected ad is clicked on. Drive-by downloads, Fox Business[20] notes, infect a system when someone just visits the site.

Ransomware

Ransomware is technically malware, but the attacks are becoming so sophisticated that it needs to be discussed as an individual attack vector. Ransomware takes data hostage by encrypting it and forcing the owner to pay a ransom within a certain number of days in order to receive the encryption key. A study by PhishMe found that in the first quarter of 2016,

15. "Third-party risk management: Horror stories? You are not alone", MacDonnell Ulsch, Tech Target, http://searchsecurity.techtarget.com/feature/Third-party-risk-management-Horror-stories-You-are-not-alone
16. "Top malware families targeting business networks", Help Net Security November 30, 2015 https://www.helpnetsecurity.com/2015/11/30/top-malware-families-targeting-business-networks/
17. "6 Common Phishing Attacks and How to Protect Against Them" David Bisson, June 5, 2016 http://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/
18. "Advanced Persistent threats and how to monitor and deter them" Colin Tankard, August 2011. Elsevier, http://www.sciencedirect.com/science/article/pii/S1353485811700861
19. "Man-in-the-Middle Tutorial: Learn About Man-in-the-Middle Attacks, Vulnerabilities and How to Prevent MITM Attacks" Veracode, http://www.veracode.com/security/man-middle-attack
20. "What You Need to Know About 'Drive-By' Cyber Attacks", Jason Glassberg, February 04, 2015. Fox Business, http://www.foxbusiness.com/features/2015/02/04/what-need-to-know-about-drive-by-cyber-attacks.html

93 per cent of phishing emails contained ransomware.[21] If a board member accidentally clicks on a link or an attachment that is loaded with ransomware, it could infect the organisation's network and cost the organisation hundreds to thousands of dollars to recover the data.

Although it has been around for a long time, ransomware's popularity is attributed to several different reasons: payments are made anonymously, usually through Bitcoin or other online currencies; the exploit kits are readily available and hackers don't need to constantly develop new malware to be effective; and it is a quick attack-and-reward system.

PREVENTION AND PROTECTION

Prevention and protection means committing to security best practices like conducting regular penetration testing, instituting security policies, immediately updating and patching software, and regulating the devices connecting to the network. In addition, security experts suggest the following:

Education

Providing all employees with mandatory security training is essential. Everyone who accesses the network must understand the cybersecurity risks and prevention tactics. Education should include:

- Regular communication, such as weekly or monthly security tips, regarding the latest threats, and what expectations are regarding security.
- Regular hands-on training. There are online cybersecurity modules available for monthly or quarterly training that include detecting phishing scams and other potential attacks.
- Social networking best practices that include what not to share in social media and how to recognise social engineering.
- Instituting security policies for BYOD and enforce them.
- An open line of communication. Everyone with network access should be able to bring their concerns to IT or those in charge of security. All questions and comments should be taken seriously.

Focus on Data, Not Networks

More security experts are recommending that organisations restructure the approach of protecting the network to protecting the data. Because there are now so many endpoints with access to sensitive data and much of that information is stored outside of an onsite server, traditional perimeter security methods are no longer as effective. This means thoroughly vetting third-party vendors, especially cloud providers, on how they protect data. Best practices for cybersecurity include:

- Encrypting data when at rest
- Using secure email options
- Deploying security tools for every endpoint, including smartphones and tablets

Use Technology Advancements

Technology can also improve security. By using a board portal, for example, communications and documents are encrypted and more difficult for potential hackers to steal. Board portals also give board members a single location from which to access information, so there are no worries that email or documents are stored on insecure or outdated systems, which are more vulnerable and lend themselves to great risk of exploitation.

National Security Agency Director Mike Rogers told the *Wall Street Journal*[22] that it isn't a matter of if your networks will be penetrated but when, and every organisation, no matter its size, has to take cybersecurity more seriously.

21. "93% of phishing emails are now ransomware", Maria Korolov, Jun 1, 2016. CSO, http://www.csoonline.com/article/3077434/security/93-of-phishing-emails-are-now-ransomware.html
22. "NSA Chief Expects More Cyberattacks Like OPM Hack", Robert Wall and Alexis Flynn, July 15 2015. The Wall Street Journal, http://www.wsj.com/articles/nsa-chief-expects-more-cyberattacks-like-opm-hack-1436985600

Using a board portal makes communications and documents more difficult for hackers to steal.

Call: 1 800 646 207 / 0800 434 5443
Email: info@diligent.com
Visit: diligent.com/au