skillsoft technology & developer

Enterprise Technology and Compliance:

Understanding and Navigating Today's Challenges to Secure Your Business and Data.

It seems that every month there is news involving a company being hacked, personal information being inadvertently released, or a new device exploit that opens up a previously unknown vulnerability. These are not only concerns for professionals in enterprise technology, but also those in compliance. The best compliance and enterprise technology professionals are starting to merge in mission and purpose in security. Previously, General Counsels (GCs) were primarily concerned with tangible, "real" risks, e.g., tort liability or transactional exposure. But as products and services have moved into the digital space, so have the risks. However, the common thread these risks share remains the same: people.

Digital risks were formerly restricted to company hard drives, servers and network infrastructure, but in the age of bring your own device (BYOD) this is no longer the case. BYOD is shown to increase productivity by 34% and save businesses an average of $350 per employee per year;[2] it's no wonder why more and more organizations are considering the measure. But it means that now both enterprise technology executives and GCs have to worry about data breaches from personal devices—a non-issue in former years. It is well understood that data breaches continue to increase in frequency, sophistication and severity, but what are today's most common forms of attack? Where are they occurring? And how can your company reduce its risk of breach in the BYOD era?

> "The devices and the people affected are becoming harder to both control and protect as they become increasingly mobile and opt to use their own technology as opposed to that supplied by the IT function."[3]

SPEAR-PHISHING IS STILL THE MOST COMMON VECTOR

Spear-fishing remains the most common point of entry for all malware threats and variants, used by 71% of organized groups in 2017.[4] Almost all companies run into spear-fishing, and the attackers using this approach have become much more advanced than the obvious email-chain scams of the early 2000s.

Most attackers will employ social engineering techniques to personalize and target the email specifically to the user. Relying on various channels across social media and the web, an attacker can gain an understanding of who the user is and can craft a tailored message that may entice the user to take a certain action.

SECURITY THREATS FOR ORGANIZATIONS

1 out of 13 web requests lead to malware

92% increase in malware variants

54% increase in mobile malware variants.[1]

1 *"Internet Security Threat Report." Volume 23, Symantec, 2018.*
2 *"The Smartphone Productivity Effect: Quantifying the Productivity Gains of Smartphones in the Enterprise." Frost and Sullivan, 2016.*
3 *"Ready... Or Not? Balancing Opportunities with Future Risks." Kaspersky Lab, 2018.*
4 *"Internet Security Threat Report." Volume 23, Symantec, 2018.*

> "Spear-phishing emails are the number one means of attack we've seen used, meaning a well-crafted email, sent to an unsuspecting staff member is the most likely source of compromise and can be the trigger to a potentially serious security breach.[5]"

Attacks are becoming more focused and are more refined, and attackers are concentrating on specific industries for a greater opportunity for success. Healthcare has become particularly targeted in recent years; "healthcare organizations experience more than twice the number of attacks on average as compared to organizations in other vertical market categories."[6]

SOCIAL SCAMS ARE A REAL THREAT

Previously, social media scams took the form of a suspiciously worded post or message that was sent to a user's entire contact list. Relatively easy to detect by the recipients, this style of scam resulted a meager number of manual shares. Today's social media attacks are more sophisticated and believable.

Social networking is now considered the second biggest threat to enterprise technology security.[7]

Attackers have come to be known as social engineers and have seemingly "cracked the code" on how to induce users to share messages or open infecting content. While checking social media was a strictly off-limits activity at work in the past, it's becoming increasingly acceptable and creates vulnerabilities for company devices. Additionally, the BYOD trend only increases the possibility that an employee could unknowingly fall victim to a scam on an employer-networked device.

RANSOMWARE

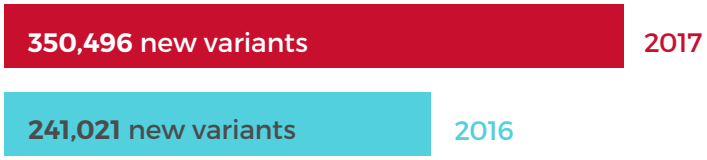
Imagine turning on your device one morning and seeing a message that you have to pay to access your files. This is the reality of ransomware. Relatively new as a serious threat in the world of security, ransomware gained much notoriety in May 2017 with the WannaCry cyberattack which targeted holes in the Windows 10 operating system. This type of attack is taxing for all but especially troublesome and costly for businesses when down time and lost revenue is considered.

Global costs associated with ransomware are projected to hit $11.5 billion by the end of 2019.[8]

"Ransomware does exactly what it sounds like—it presents users with an ultimatum: pay a fee to unlock and reclaim personal data, or don't pay the fee and lose the data indefinitely."[9] These attacks are so new, varied and prevalent, there is truly no operating system or virus protection software that can keep a company absolutely safe. Because these attacks can travel through and between network drives, they can lock down entire servers. Ransomware attacks are traditionally associated with computers, but increasingly, mobile devices are just as vulnerable. Many experts recommend never paying a ransom, but businesses and individuals are eager to get their files back and many pay, keeping the scam profitable and attractive to hackers.

Ransomware continues to grow—both in number of variants and frequency of attacks. According to Symantec:[10]

Ransomware variants **grew by 45%** in 2017.



Ransomware attacks detected **increased by 41%.**

WHAT ARE ATTACKERS AFTER?

When considering the problem of data breaches, it is useful to understand what attackers do with the information they steal. A vast network of underground marketplaces exist where data thieves can sell anything from Social Security Numbers to credit card accounts, or even full "packages" of sensitive, personally identifiable information. Purchases are often made in bulk and can include hundreds or thousands of data points.

Mobile phones have become a keep-all in this day and age. We access our bank accounts, store credit card information and addresses, and

5 *"Internet Security Threat Report." Volume 23, Symantec, 2018.*
6 *"Healthcare Experiences Twice the Number of Cyber Attacks As Other Industries." Ladi Adefala, CSO, March 6, 2018.*
7 *"Ready... Or Not? Balancing Opportunities with Future Risks." Kaspersky Lab, 2018.*
8 *"Global Ransomware Damage Costs Predicted to Hit $11.5 Billion BY 2019." Steve Morgan, Cybersecurity Ventures, November 14, 2018.*
9 *"What Is Ransomware?" Symantec, 2018.*
10 *"Internet Security Threat Report." Volume 23, Symantec, 2018.*

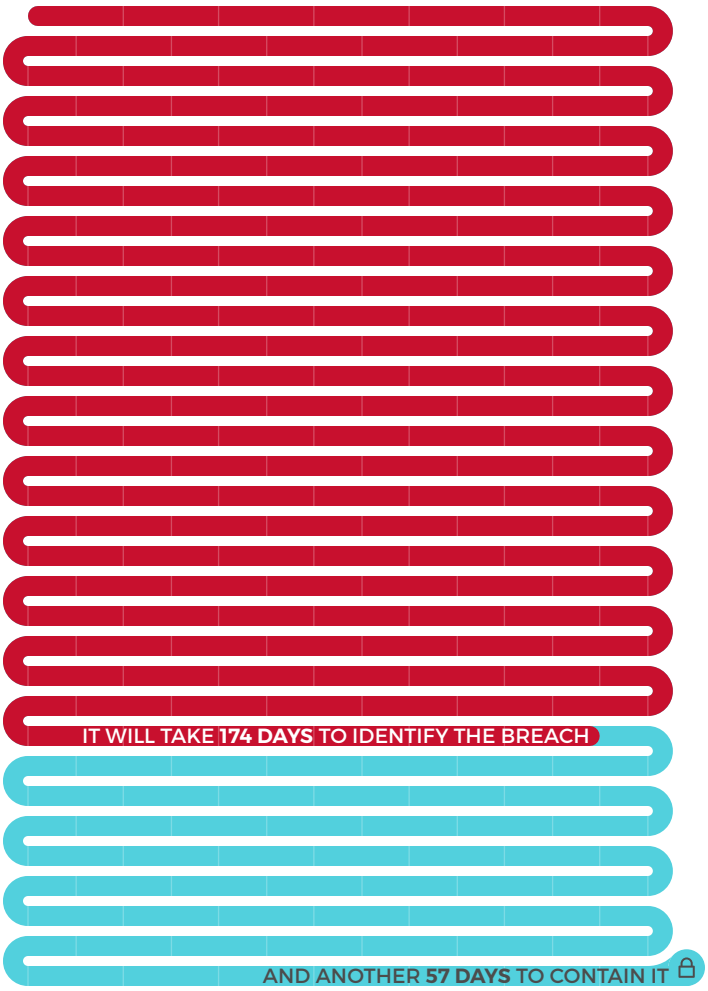
increasingly, access company email or other networked accounts. This makes mobile phones the holy grail for hackers.

HUMANS ARE YOUR WEAK LINK

While attackers have grown more sophisticated, and hardware and software exploits more numerous, one of a company's greatest weaknesses remains the same—human error. Where an attacker can target the end user, or an "everyday employee," it is most likely to succeed. Businesses have the Sisyphean task of playing constant defense while all a hacker needs is a single opportunity to get through. In the age of IoT where everything from thermostats to office printers are connected to the company network, those opportunities are everywhere. This makes education all the more important. With so many potential breaks in integrity of the network, employee training is one way to make your weakest link your greatest defense.

A strong understanding of threats and compromises by your employees will help protect against future threats, but also help contain the cost of existing ones; a recent IBM and Ponemon Institute found that the longer it takes to detect a threat, the more costly it is to an organization. Educating employees beyond security professionals is imperative to keeping your data safe and secure.

It takes an average of **231 days** to **identify** and **contain** a data breach caused by human error.[10]



WHY REGULATIONS AREN'T ENOUGH

In 2013 President Obama issued Executive Order 13636: Improving Critical Infrastructure Cybersecurity, and the National Institute of Standards and Technology (NIST) was tasked with creating a "set of existing standards, guidelines, and practices to help organizations manage cyber risks."[12]

This framework was intended as guidance and was therefore optional. Today, its design is still helpful in giving companies a starting point for creating and maintaining an effective security program, but attackers have still been successful in finding new ways of compromising systems and targeting employees. Humans remain the weak link.

Ultimately, the most effective strategy is to establish a culture of compliance. When a company is able to align across all areas of the business and devices and use the practices established in the NIST framework, employees at all levels will understand what the objectives of compliance are.

BYOD appears to be a money-saving measure that also boosts productivity—but without an organization-wide culture of compliance, the measure could cost you. Training is essential to educating your team, establishing stringent security protocols, and ensuring that every individual across the organization is "on the same page."

WHAT'S THE SOLUTION?

There is unfortunately no simple way to resolve the threats posed by the digital age and all the various devices that come with it. Having effective security technology in place will help, but a company's first and best line of defense is a digitally savvy workforce. Through training and proper support, you can significantly reduce the most pressing threats, and take advantage the cost-saving measures like BYOD. When employees understand what to look out for, and are alerted to emerging threats, they will become empowered to think before they act and seek help when in doubt.

Yet competing priorities and 24/7 connectedness leave many employees feeling that their time is already limited. Therefore, the training you provide must be engaging, relatable and current. Employees must feel the content is useful to them and understand its connection to the company's objectives of protecting its valuable resources.

Training is needed at all levels of the organization, including enterprise technology professionals and general employees, and for the global workforce in the native language. Offer learners multi-modal content, available 24/7 with assignment tracking and completions to encourage a culture of compliance.

11 "2018 Cost of a Data Breach Study: Global Overview." IBM and Ponemon Institute, 2018.

12 "Framework for Improving Critical Infrastructure Cybersecurity." National Institute of Standards and Technology, February 12, 2014.

Learn more about Technology and Developer and Compliance training solutions: www.skillsoft.com

skillsoft technology & developer

linkedin.com/company/skillsoft

facebook.com/skillsoft

twitter.com/skillsoft

skillsoft.com

844-509-9585

ABOUT SKILLSOFT

Skillsoft is the global leader in corporate learning, delivering beautiful technology and engaging content that drives business impact for modern enterprises. Skillsoft comprises three award-winning solutions that support learning, performance and success: Skillsoft learning content, the Percipio intelligent learning platform and the SumTotal suite for Human Capital Management.

Skillsoft provides the most comprehensive selection of cloud-based corporate learning content, including courses, videos, books and other resources on Business and Management Skills, Leadership Development, Digital Transformation, IT Skills and Certification Training, Productivity and Collaboration Tools and Compliance. Percipio's intuitive design engages modern learners and its consumer-led experience accelerates learning. The SumTotal suite features four key components built on a unified platform: Learning Management, Talent Management, Talent Acquisition and Workforce Management.

Skillsoft is trusted by thousands of the world's leading organizations, including 65 percent of the Fortune 500.

ABOUT SKILLSOFT COMPLIANCE SOLUTIONS

Skillsoft is a pioneer in the field of learning and talent management with a long history of innovation. Our compliance centric business unit, Skillsoft Compliance Solutions provides compliance-based risk mitigation and safety training, along with certification preparation for customers ranging from global enterprises, government and education institutions to mid-sized and small businesses. Today our compliance business solutions serve over 1,400 organizations worldwide, of which many are leading Fortune 500 companies.

Our compliance courseware and videos have been developed in partnership with industry-leading compliance experts to ensure customers receive up-to-date, relevant and reliable content. We provide one of the largest selections of compliance content to ensure organizations effectively meet regulatory requirements, mitigate risks—all while building awareness and developing a strong culture of compliance.

We help businesses protect themselves and their employees through a comprehensive suite of training services and compliance-based learning solutions.