RCM&D

Assurex™ GLOBAL

Defending Against an Invisible Threat

Pragmatic Cybersecurity for the Interconnected Business

assurexglobal.com

SUMMARY

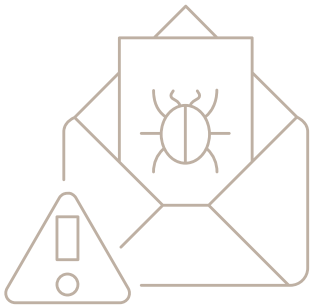
THINK YOUR BUSINESS IS REASONABLY SAFE FROM A CYBER-ATTACK? Think again. The threat is so widespread that there is an entire black market built to arm hackers with the tools they need to breach your systems. Even worse, 50 percent of online traffic is automated. It does not sleep. It is ever-present, and it can be searching for your data—or your client's data at any moment. Should a hacker gain access into your business' network, the results could be devastating in terms of lost assets, lost credibility, and a tarnished reputation.

The good news is that there are a number of steps your business can take to not only protect your employee and client data, but also to demonstrate the level of diligence that is critical to your customers and insurers.

The first step is understanding the extent of cyber-attacks and familiarizing yourself with the various methods hackers use to infiltrate your system. Armed with this basic knowledge, you will be better equipped to recognize the signs of an attack and prevent a breach from happening in the first place.

This white paper is based on a presentation from Mr. Chris Ensey, COO of Dunbar CyberSecurity. By reading it, you will learn what constitutes a cyber-attack and the associated tactics. You will also learn about preventative measures that you can take to strengthen your company's security.

Overview



WHAT IS A CYBER-ATTACK?

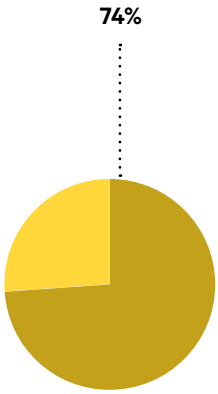
According to the Random House dictionary, the definition for cyber-attack is, "An attempt to damage, disrupt, or gain unauthorized access to a computer, computer system, or electronic communication network."[1] Over the last 15 to 20 years, cyber-attacks have evolved from simple ad pop-ups to an intricate black market economy that supports every stage of a cyber-attack.

Cyber-attack overview

Since 2013, over three billion online records have been lost, 74 percent of which were from the United States. This translates roughly into one record for every U.S. citizen stolen on three separate occasions. Within industry verticals, retail and technology have been hit the hardest, followed by the financial and government sectors.

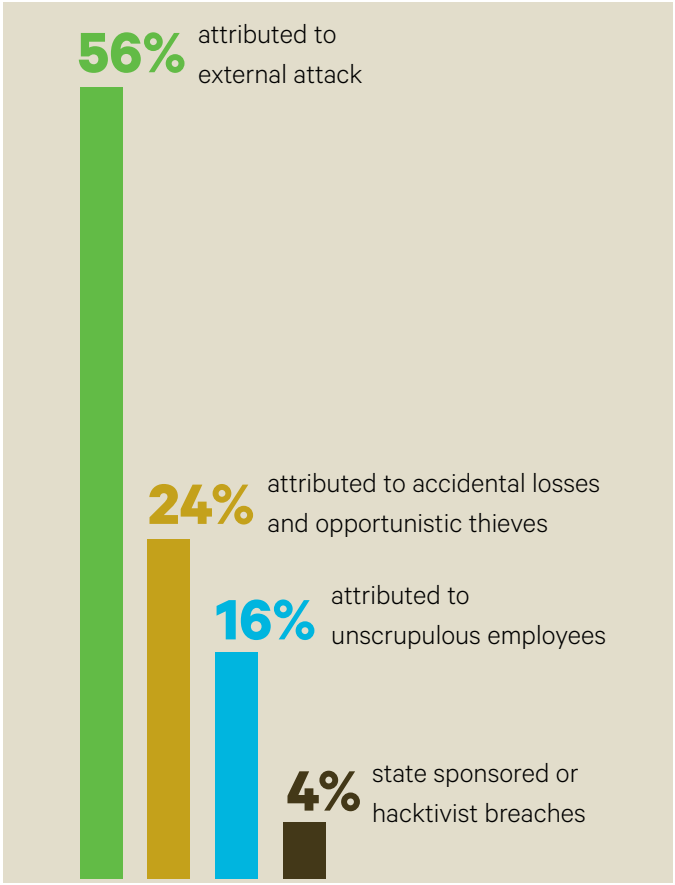
Only 56 percent of data breaches are the result of an external attack. A full 24 percent can be attributed to accidental losses and opportunistic thieves. An additional 16 percent can be attributed to unscrupulous employees. The remaining 4 percent are either state sponsored or hacktivist breaches.

Nearly every two seconds a new malicious URL is created online. As a whole, the online populace sees 30,000 malicious URLS each day, 80 percent of which are legitimate sites that have been compromised.



In 2013, over 3 billion online records were lost, 74% of which were from the U.S.
source: Ensey, Chris. 'Cyber Risk Management'. 2015. Presentation.

Data Breaches



HOW DO CYBER-ATTACKS WORK?

In this technological age, you can no longer consider cyber-attacks as unlikely, siloed, or unsophisticated events that happen to other people. Cyber-theft is so prevalent that there is an established and lucrative black market to support it, with products for sale that enable anyone with a basic understanding of HTML to launch an attack.

In general, cyber-attacks work in the following manner: A hacker employs any one of several methods of delivery to spread the attack. You click a link within the method of delivery, downloading a program. This program, known as a Trojan virus, is contained within the smallest amount of code possible, which enables it to avoid your security software's detection.

The Trojan is intended to perform one task—to open the backdoor of your system and download a payload. While the term "payload" is typically used to describe the things carried by an aircraft (like explosives), in the cybersecurity world, "payload" refers to what a Trojan, or other virus, downloads into your system.

Once the Trojan downloads the payload, often malware or ransomware, your system is officially compromised. Scarily enough, you may not even have to click a link to become compromised—it can happen automatically.

THE FIRST CYBER-ATTACK

According to NATO, the first recognized "cyber-attack" on the world stage was a worm created in 1988 by Robert Tapan Morris, called the Morris worm. Although the MIT professor's purpose for creating the worm was simply to determine the Internet's size, he was convicted for computer fraud and abuse.

source: http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm

About Dunbar Cybersecurity and Chris Ensey

After nearly a century of protecting its clients' physical assets through armored trucks and security services, Dunbar Armored established Dunbar Cybersecurity in 2012 to protect clients online. The cyber arm of the company offers its clients 24/7 protection from online threats, with services including network security operations, web attack defense, security information and event management, data protection and encryption, social threat analysis, and information security consulting.

Chris Ensey, COO of Dunbar Cybersecurity, is the founder of Dunbar's cybersecurity specialty service. Throughout his 15-year career in cybersecurity, he has worked in many aspects of the business, from writing, designing, and developing secure sharing platforms for intelligence agencies, to running a specialized team that assesses and protects the security of corporate clients. He has also worked for SafeNet, IBM, SAIC, and other major companies. He currently runs Dunbar Cybersecurity's team of security professionals, largely consisting of former military intelligence personnel and researchers.

*Note: All stats provided in graphics provided by Chris Ensey "Cyber Risk Management" presentation.

Methods of delivery

Methods of delivering cyber-attacks are vast, and include, but are not limited to:

- **Phishing emails**—Hackers cast a wide net for victims using these untargeted, unsolicited emails that often appear as though they are coming from a trusted organization. These very realistic-looking emails entice you to click a link, allowing the hacker access into your system.

- **Spear phishing**—As the name would suggest, spear phishing emails are targeted phishing emails sent to specific individuals or groups. Because of the nature of the targeting, the messages often look and feel like they come from a real person that you know and trust. As a result, spear phishing emails are much harder to detect than their conventional counterparts.

- **Illegitimate websites**—It is often difficult to tell the difference between an illegitimate site and a legitimate one. Although they look credible, illegitimate sites are fronts used to gain personal information. They are often accessed from a phishing email link.

- **Legitimate websites**—Hackers don't need to create their own site to exploit victims—they can compromise legitimate ones as well. For example, should a hacker attack your bank's website, he could record your user name and password keystrokes as you log in, or he could set up a redirect that would link you to an illegitimate website once you have logged in.

- **Advertisements**—Banner ads, pop-ups, pre-rolls, and any other type of online advertisement can become a vehicle for delivering an attack. With one click on the wrong ad, your system could be compromised.

- **Social attacks**—Hackers create false accounts on social networking sites like LinkedIn or Facebook. These fake accounts, which often contain hundreds of connections, a rich background history, and even published white papers, can be extremely deceiving. Hackers can also hack into existing accounts. By using the veneer of a trusted person, hackers send out direct messages with malicious links directly to you.

- **Plug-ins**—A download that extends or updates an existing software's capabilities, plug-ins can be used as a method of delivery for cyber-attacks. Hackers exploit the weaknesses of plug-ins and anyone with the download can become a target.

- **Drive-by downloads**—A drive-by download is a download that you didn't intend to initiate. In the event that you visit a compromised website, malware can take advantage of your out-of-date security system and download itself without your knowledge.

Each method of delivery is disguised to trick you into trusting its authenticity. When you encounter one of these delivery mechanisms, you are typically asked to click something. Once you click, the attack, usually malware or ransomware, is granted entry into your system.

Malware

Today's malware (short for malicious software) is an amalgamation of many things, including bots, Trojan horses, and viruses. It is its own holistic toolkit, needing only itself to wage war against your system. By changing algorithms to encrypt itself multiple times, malware can successfully hide from antivirus software, making it highly effective in an attack.

Once the malware unpacks itself and hides, it recognizes the system that it's in and exploits all of its vulnerabilities. If it's in a Windows system, it will use pre-canned, Windows-specific attacks. In this way, it has evolved from a classic worm or virus, making it very dangerous.

When malware reaches this point, your system is completely compromised. The malware will search for anything of interest, like files, user credentials, or social security numbers, and set up a conduit between your system and the hacker's dashboard. The hacker just has to wait.

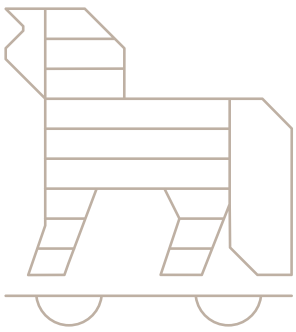
Malware and business applications

Hackers will often attack business enterprise applications like Workday, Salesforce, and UltiPro, which can house employee W2s, social security numbers, and tax-required data. In order to steal this personal information, hackers will target Human Resource professionals or senior leadership who have access to these applications. Targeting these people has been successful and, in recent years, there has been a huge uptick in tax fraud.

Ransomware

Ransomware (short for ransom software) is similar to malware in many ways. It can be built or bought on the black market and it is distributed through common delivery methods. Unlike malware, however, it is programmed to hold the victim's data hostage, to be released only after a ransom has been paid. If the ransom is not paid in a timely fashion, the data is encrypted or destroyed.

Because of the numerous random encryptions on a victim's data, and through continuous ransomware innovations from the black market community, it is practically impossible for a non-professional to get the stolen data back without paying the ransom. Since 2013, hackers have extorted over $3 million using ransomware.



CASE STUDIES

MINI CASE STUDY:
Ransomware in the financial services market

A privately held, mid-market financial services firm manages its clients' wealth, retirement plans, health benefits, investments and more. The firm has been in business for more than 80 years and, during the majority of that time, it was never the victim of a cyber-attack.

However, one of the employees encountered a drive by download, which installed CryptoWall. Once the malware was in the firm's system, it downloaded and encrypted two terabytes and ten years of data, then held it for ransom. Luckily, the firm had an excellent business continuity strategy in place and had all of its data backed up offsite. Because of this, they were able to avoid paying the ransom for their data.

Lessons learned

The good news is that the firm was able to get all of its data back without paying the ransom. The bad news is that they lost over four days of business productivity waiting for the data to be restored. The worse news is that their systems were so easily penetrated. ***After the attack, the firm reassessed the security of their systems.***

MINI CASE STUDY:
Spear phishing for human resource administrators

A healthcare provider employing more than 1,200 people was the target of a clever spear phishing campaign. A hacker sent an email that looked like an invoice for UltiPro, the company's human resources management system. Falling prey to this legitimate looking email, the administrator unsuspectingly opened up the company's records to the hackers, exposing the personal information of all their employees. Dozens of employees had their W2 information stolen and later had falsified tax returns filed.

Lessons learned

Human resources professionals and senior level managers are frequently the target of attacks. These individuals require extra training to ensure that they are able to identify and appropriately respond to threats. *If there is the slightest doubt or gut-feeling about an email, they should call the business in question, or visit their website through the URL bar, not through the email link.*

MINI CASE STUDY:
Malicious insider and outsiders attack database

A group of corrupt mortgage brokers bought access to the LendingTree database through a former employee. Access to the database provided the criminals with lucrative mortgage lead information, valued at $745,152.

Lessons learned

A business should provide minimal employee access to secure systems, and should monitor activity levels of all important company assets.

Regardless of size, industry, or location, no company is truly immune to a cyber attack. Criminals don't discriminate, and unsuspecting businesses pay the price—in time, money, and reputation. While the black market continually finds new ways to breach security, there are methods you can employ to protect your business from attacks.

HOW TO PREVENT A CYBER-ATTACK: A STARTING LIST OF MEASURES

While no one is completely immune to cyber-attacks, there are safeguards that, if enacted, will reduce your likelihood of becoming a victim. A few of the first steps: **(1)** reduce the "surface area" of your system, **(2)** inventory and evaluate asset activity, and **(3)** keep cybersecurity as a staple of boardroom conversation.

Reduce the Surface Area of Your System

The surface area of your system is the amount of ways a hacker can enter your system and potentially cause damage. The larger the surface area, the more opportunity there is for attack.[2] Generally, turning off unnecessary functionality and having less code available are best practices for reducing your system's surface area.[3] The following are specific methods for reducing the surface area of your system.

Implement safe surfing policies

There are some obvious policies to implement within your business, such as not allowing searches for adult, criminal, or offensive content or permitting online gambling. You could implement safe surfing technologies, like URL filtering across all company computers, or go so far as to block social sites and other sites where predators could be lurking. If your company does not have technology that filters or blocks offensive content or warns of potentially compromised websites, get it. This is a must for protecting against attacks.

Enforce strong passwords

It is human nature to create passwords that are easy to remember. Thus, it is likely that many of your passwords are similar across every site. Should a data breach occur, a hacker could use your password from one application and apply it to another and gain access. Your company must have a strong password policy in order to protect itself from this easy access point. Implement technologies that mandate long and complex passwords that change on a schedule.

Control application downloads

If you allow your employees free access to download anything from the Internet, you will end up with a host of garbage that may or may not have been properly tested living on your network. Not only can this make your employees' computers run slower, it can also compromise your security. Enforce policies or implement technologies that limit the amount of applications an employee can download. You can also work with IT to reduce the number of plugins, which are also a source of infiltrations.

Require patch management

How many times have you ignored your computer's request to update software? These often-ignored updates are essential when it comes to keeping security settings updated. By allowing employees to ignore their computer's requested updates, you leave your system vulnerable to more up-to-date malware that can take advantage of your system's weaknesses. Implement policies and technologies that do not allow a delay of the required system updates.

Inventory and Evaluate Asset Activity

In addition to implementing the technologies and policies above, you can work with your IT team to inventory and evaluate your current asset activity. A step-by-step approach and an overall explanation of how to inventory, evaluate, and create security policies for your business's assets is provided below.

As a note, when we discuss asset, we're speaking about any important component in your business's security, like your computers, cellphones, servers, data, applications, backup systems, and more.

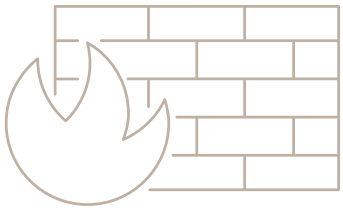
Quick step-by-step

1. Inventory your business's assets.
2. Collect security policies tied to the assets.
3. Select metrics to capture from the assets.
4. Map risk management processes to status and event feeds associated with each asset.
5. Define a process for escalation of events to asset owners.
6. Capture data and establish a baseline of activity.
7. Configure alerts based on past incident response action.
8. Reevaluate and repeat.

Overview of step-by-step

Create a detailed list and audit trail of where the assets are, who is responsible for them, what the business criticality is for each of them, and the security policies associated with them. You can then determine the ripple effect across assets should a single entity become compromised. Once you've documented this, it is important to identify the metrics that you can use to measure the health of the assets. Metrics can include, but are not limited to, system health, alarms, logs, state, and traffic.

Next, plot out the risk management protocols for each application and create processes for your employees to follow should an attack occur. Educate your asset holders on these policies so if something goes wrong, they know whom to contact.



Continue monitoring your assets to establish a baseline of activity. For example, once you begin monitoring activity on your company's website, you will be able to determine average traffic levels. If and when an anomaly occurs, either a spike or complete absence in traffic, you will know to investigate.

Based on your baseline activity and your risk management practices, configure alerts for your assets and continue the process. As technology continues to change, so too should your policies. This is an iterative process that will change as you progress.

Keep Cybersecurity as a Staple of Boardroom Conversation

Preventing cyber-attacks is an ongoing process, but cybersecurity can be attained and improved by keeping it as a staple topic of boardroom conversation. Do not ignore the threat—it is ever-present and growing stronger by the day.

In addition to keeping the topic of cyber-attacks and cybersecurity top of mind, consider the following as tips and discussion points in your next board meeting:

- **Get your organizational chart and employee vcards off of your website**—Although a heated topic among companies wanting to be easily accessible and transparent to their consumers, these practices feed hackers pivotal information and enable them to more easily steal your data.
- **Make passwords strong and random**—Implement a randomizing password generator as much as possible. Not having to write down or remember passwords lessens security risks. Your passwords will also become stronger due to the random nature of the passwords.
- **Retire old data from the archives**—Consider auditing your assets for data that is no longer useful to your business, but could be useful to a hacker gaining access to your systems.
- **Encrypt as much of your data as possible**—Is your employee information encrypted? Although it is possible to decrypt data, encryption is data's last-line of defense and should be used on anything of value.

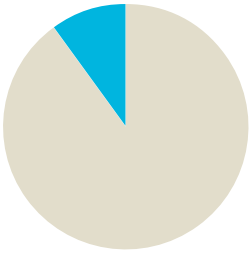
INSURING YOUR COMPANY'S SAFETY

Cybersecurity insurance addresses cyber-attacks from two angles—risk prevention and coverage should a loss occur. The insurance often promotes risk prevention by providing services and offering incentives to companies that strengthen their security. However, if an attack occurs, and for many companies, it's not "if" but "when," the insurance is designed to cover a multitude of losses.

What does cybersecurity insurance protect?

Cybersecurity insurance policies are designed to cover data breaches, business interruptions, security audits, post incident public relations, network damage, customer credit monitoring services, and even criminal reward funds. While around 10 percent of U.S. businesses have some form of cybersecurity insurance, many companies choose not to purchase policies due to confusion about the specifics of coverage (and lack of time/resources to sort it out), and the perceived risk/reward of paying for insurance that may never be needed.[4]

As cyber-attacks pose more than financial risks—they affect the reputation and customer trust as well—cyber insurance can only go so far in protecting a business. Insurance does not protect from long-term damages, including reputational damages, loss of customers, some lawsuits, and loss of intellectual property. However, it can protect a significant share of your business's financial assets and promote a more secure operation.



Around 10 percent of U.S. businesses have some form of cybersecurity insurance.

Benefits of cyber insurance

As indicated earlier, companies wanting cybersecurity insurance, reasonable premiums, and robust coverage will be required to implement risk prevention measures. In this way, the benefits of cybersecurity are twofold—the protection of loss if an attack occurs, and the encouragement of better preventative measures to mitigate the risk of an attack from occurring. Cyber insurance forces the conversation of security to executives, requiring them to invest in and pay closer attention to security programs and monitoring. In this way, insurance promotes protection for employees and clients alike.

CONCLUSION

One small cyber-attack can have an enormous ripple effect, for example, the 2013 cyber-attack on Target. Approximately 40 million of Target's customers had their credit or debit card information stolen, and it all began with an innocuous attack on a third-party HVAC vendor.[5]

According to the Huffington Post, hackers targeted the HVAC vendor with a spear phishing campaign. Once an employee downloaded the malware, the hacker gained entrance into the HVAC vendor's system, and because the vendor had access to Target's network, the hackers gained access into the retail store's system as well.[6] It only took one email downloaded by one employee to jeopardize more than 40 million people's security.

In addition to the huge impact one attack can make, consider how little effort it takes for a hacker to purchase the malware that can get to your data, the amount of times you've hit "postpone" on your computer's security update request, and the variety (or lack thereof) of passwords that you use across all of your accounts. While the threat of cyber-attacks is ever-present, there are relatively straight forward preventative methods you/your business can take to reduce your exposure and demonstrate diligence.

Top tools used by hackers:

- 25% Zbot
- 18% Ransomware
- 12% PWS
- 11% Sinowal
- 11% FakeAV
- 6% Backdoor
- 6% ZAccess
- 2% Downloader
- 9% Other

source: Ensey, Chris. 'Cyber Risk Management'. 2015. Presentation.

Must-have security features:

- Spam filtering
- Real-time URL reputation filtering
- Web malware scanning
- Automatic updates
- Client anti-virus with HIPS
- Locked down firewall

Glossary

- **Spam filtering:** detects unsolicited and unwanted emails from a user's inbox
- **Real time URL reputation filtering:** protects against URLS containing malware by confirming the reputation or stability of that URL before allowing a user to access
- **Web malware scanning:** checks for malicious and unwanted software on your computer
- **Automatic updates:** provides updates to your system as soon as they are available to enhance security performance
- **Client anti-virus with HIPS (Host Intrusion Prevention System):** alerts you in the event of malware or an unauthorized user gaining access to your system
- **Locked down firewall:** halts inbound and outbound connections from the internet to your computer

Sources

[1] cyberattack. Dictionary.com Unabridged. Random House, Inc. http://dictionary.reference.com/browse/cyberattack

[2] Manadhata, Pratyusa (2008). "An Attack Surface Metric." Carnegie Mellon University. http://reports-archive.adm.cs.cmu.edu/anon/2008/CMU-CS-08-152.pdf

[3] Microsoft (2006). SQL Server Surface Area Configuration. Technet. https://technet.microsoft.com/en-us/library/ms173748(v=sql.90).aspx

[4] Cybersecurity Insurance Industry Readout Reports. U.S. Department of Homeland Security. http://www.dhs.gov/publication/cybersecurity-insurance-reports

[5] Krebs, Brian. (2014). "Target Hackers Broke in Via HVAC Company." Krebs on Security. http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

[6] Smith, Gerry. (2014). "Massive Target Hack Traced Back To Phishing Email." Huffington Post. http://www.huffingtonpost.com/2014/02/12/target-hack_n_4775640.html

RCM&D

rcmd.com

RCM&D is ranked among the top independent insurance advisory firms in the United States. Our specialized teams provide strategic solutions and consulting for risk management, insurance and employee benefits. Leveraging 130 years of experience and strong local, national and global reach, we partner with you to meet all of your business objectives.

Assurex™ GLOBAL

assurexglobal.com

Founded in 1954, Assurex Global is an exclusive Partnership of the most prominent independent agents and brokers in the world. With $28 billion in annual premium volume and more than 600 Partner offices, Assurex Global is the world's largest privately held commercial insurance, risk management and employee benefits brokerage group. An international insurance powerhouse, the Partnership combines the local expertise and global reach of international brokers on six continents.