CW technology

CYBERSECURITY THREAT REPORT

OCTOBER 2021

TABLE OF CONTENTS

INTRODUCTION

In the last 19 months, the world has drastically changed. Between the technological advancements to the COVID-19 global pandemic, not a single business, organization, or individual has been left untouched. And with that, cybercriminals have leaped at this opportunity of a changing environment.

33 BILLION

Records estimated to be stolen by cybercriminals by 2023.

600%

Increase in cybercrime due to COVID-19.

1 TRILLION

Expected spending to cover cyber security by 2025.

Across the globe, cyberattacks are increasing in strength, size, and aggression, making them the largest and fastest growing crime in the world.

In effect, cybersecurity has become not just a necessity, but an unspoken requirement for businesses of all shapes, sizes, and industry sectors to embed into their organization. Battling these criminals are the IT and cyber security professionals, including managed services providers, and cyber security vendors.

In providing new, optimal technology services, products, and additional resources, such professionals give organizations the helping hand they need in establishing a secure working environment.

With over 35 years of experience and expertise in cyber security, CW Technology is one such professional. Standing by your side, we ensure you have the framework, visibility, and security IT infrastructure to protect your business against all cyber security threats.

> Going forward, security challenges will be the top priority for SMBs.
>
> At CW Technology, we have, and will continue to, significantly invest in the knowledge, tools, and planning necessary to ensure our clients' safety.
>
> - David Manion, *CEO*

As we move into the second half of 2021 and into 2022, everyone should be prepared when it comes to cyber security.

We have outlined the following report of current and upcoming cyber security threats, industry trends, and additional valuable information, allowing organizations to prepare, prevent, and protect their businesses from cyber security attacks.

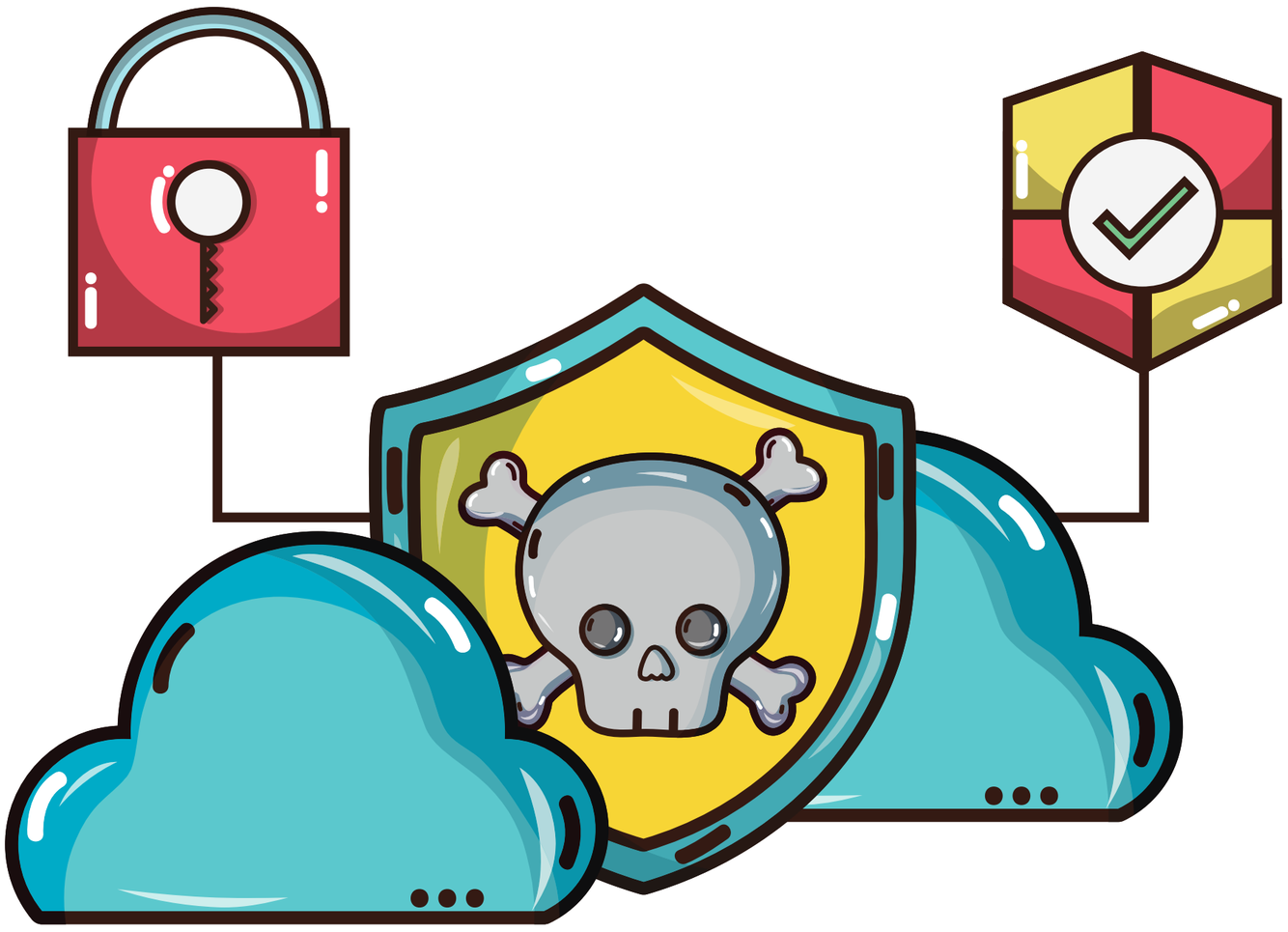
We hope you find this report both relevant and informative to your needs, as we do everything we can to help guide you in the right direction.

TYPES OF CYBER SECURITY ATTACKS

A WORLD FULL OF THREATS

Where to begin when it comes to cyber security? The first question you should ask yourself is simple: on a scale of 1 to 5, how protected do you feel you and your business is from cyberattacks? If your answer is anything but a 5, it's time to fully understand the depth and the magnitude of cybersecurity.

In our technologically-advanced world, it is especially crucial to be prepared and in-the-know of every evolving cyber threat to the world. In knowing these threats - where they come from, who is behind them, how they damage you and your business, different types - you instantly become that much more prepared to prevent them from happening to you.



At first, this may seem overwhelming to you, but rest assured, this cyber security threat report is exclusively designed to simplify the world of threats. For this reason, we have divided this section into three, primary threats, including the various types of threats that fall under each main one.

So, let's begin with the largest growing threat: malware.

MALWARE

OVERVIEW

Malware is any type of software designed to purposefully harm individuals, organizations, and corporations, all types of data (i.e. PII - personally identifiable information), networks, and devices (i.e. workstations). According to a recent Statista study (January 2021), over half of the world's population - **59.5%** - actively uses the Internet, **averaging 4.66 billion people.**

As this number rises and technology breakthroughs advance, malware steps up its level in sophistication, sneakiness, and increase in damage. In effect, it makes it that much easier for people to fall for the trap. Also known as malicious software, malware is used by cybercriminals to infect users' devices to gain access into their data, including:

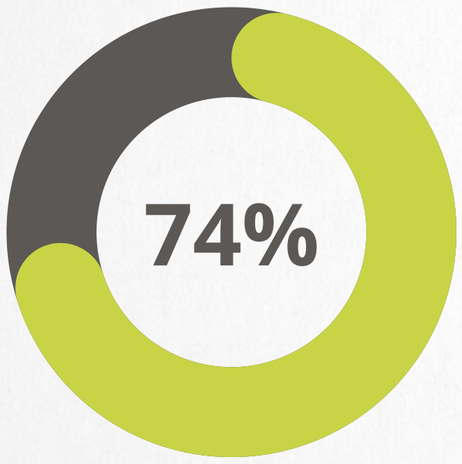
- Personal data (i.e. PII), often used for identity theft.
- Financial data (i.e. credit card information, bank accounts, etc.).

Cybercriminals also spread malware, like viruses, to infect users' devices to launch attacks on various networks, or to use them to mine cryptocurrencies. Now, you may be thinking that you know better than to click on the dated-looking pop-up "You've won $1,000,000! Click here to get it now!" This comes back to our previous point that as technology advances, so does malware...

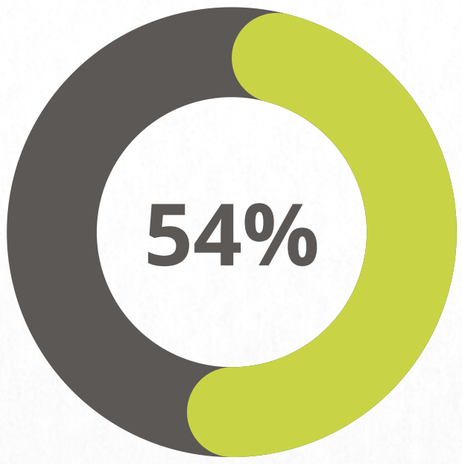
Today, malware often hides in plain sight and attacks in more cunning ways, hence why it's so easy to become infected. Most common ways malware spreads today is through email attachments, fake software installations, updates, and applications, text messages, and more.

EXAMINING THE FACTS

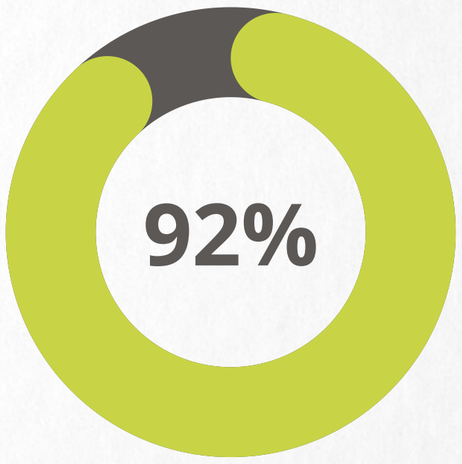
Now that you are better familiarized with malicious software, let's dive into exactly how dangerous it has become.



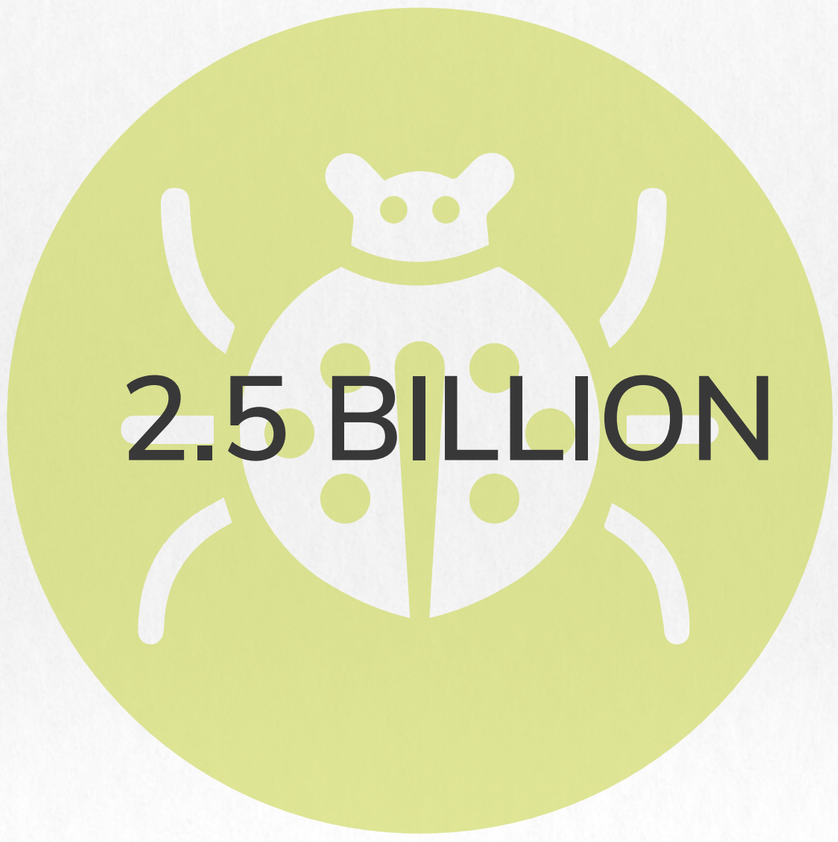
of organizations experienced malware in 2021.



increase in mobile malware.



of malware comes from email.



Malware attacks occurred in 2021 alone...

Malware attacks are gradually increasing, as shown above from 2019 to 2020.

MOVING FORWARD, OR BACKWARD...?

Fortunately, there is a bit of good news involving malware. Several types of malicious software are now on the decline, starting with the traditional vector forms. The number of websites infected by malware will continue to decrease in number, leaving the focus on emails, mobile, and the other popular methods previously mentioned.

Furthermore, cybercriminals are focusing less and less on attacking SMBs, and are rather directing their interest to larger corporations in hopes of a larger pay-off. What's more is malware detection has, and continues to, grow across businesses nationwide. With the COVID-19 pandemic, it shed a lot of light onto cybersecurity, putting many organizations in a place where they were left no choice, but to enhance the cybersecurity of their businesses.

Now, a piece of bittersweet news: malware, itself, may be on the slight decline, but many of its sister and brother types are on the excessive rise.

These malware types are trickier to detect, harder to keep track of, and are responsible for countless damaging attacks, resulting in data breaches, downtime, and worst of all, organizations going out of business...

So, what are these types of malware? Let's start with the worst one of all: ransomware.

RANSOMWARE

OVERVIEW

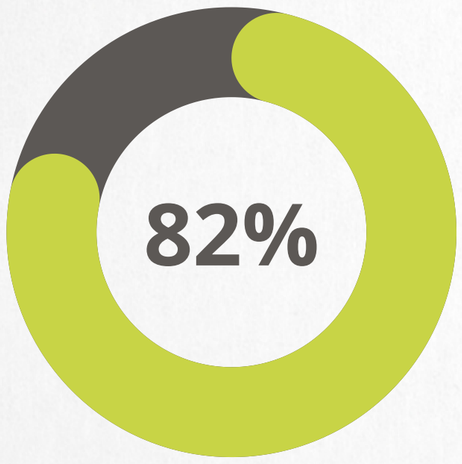
Ransomware is a type of malware that attacks a user's device by encrypting its information and holds it for ransom until an amount of money is paid. 2021 has been the worst year for ransomware... According to SonicWall's Cyber Threat Report (2021), there have been an estimated **304.7 million attempted ransomware attacks**. This is just the number that has been recorded, and it is up by **151%** from the previous year...

In addition to being most common, ransomware is one of the most costly forms of malware attacks, averaging **$6 trillion** in 2021. For this major reason, ransomware is on the rise. As more and more organization continue to pay the ransoms cybercriminals demand, they are giving room for more and more attacks. To make things worse, not all cybercriminals are technology masterminds. Yes, there are those who create ransomware, but there are now ransomware marketplaces all over online. From cheap purchasing to easy deployment, these Darknet forums have become the hotbed for cybercriminal activity. Literally, anyone and everyone has access to it...

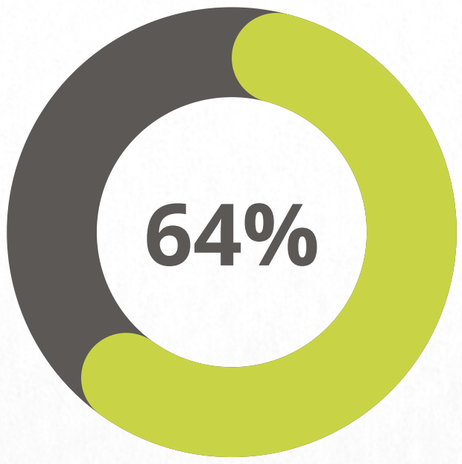
Referring back to how cybercriminals are focusing less on SMBs and more on large enterprises for malware attacks, this is far from the case when it comes to ransomware. Any organization - no matter size, shape, or sector - is a sitting duck to this attack. Making matters worse is the assumption that paying the ransom will prevent future attacks. How cybercriminals continue their attacks is by extorting their victims - asking for more money than initially - or by attacking again. In this case, SMBs are primary targets and are hurt the most. In addition to a damaged reputation and money loss, it comes to a point where many companies simply have nothing left to sustain itself...

EXAMINING THE FACTS

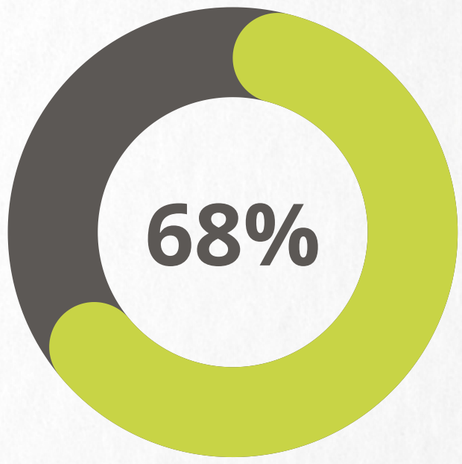
Now that you are better familiarized with ransomware, let's dive into exactly how dangerous it has become.



average increase in ransomware payments.



increase in attacks in first half of 2021.



of American businesses pay a ransom.

EVERY 11 SECONDS

A business falls victim to a ransomware attack.

$570,000

Minimum ransom amount paid in 2021.

$1,000,000

Maximum ransom amount paid in 2021.

NEVER PAY UP

Being in the fragile state they are in, companies are eager to move forward to quickly repair the damage the attack has made. In effect, not only are these organizations destroying their reputation and losing money and customers, they are placing a target on their back.

Simply put: who's to say that the criminals who attacked a business won't do it again once they've been paid? So, the golden rule with a ransomware attack is to never pay up for these top, three reasons:

YOU'LL BE FUNDING CRIMINAL ACTIVITY.

Think of it this way: if police don't negotiate with criminals and terrorists, neither should you for the safety of your business.

YOU'RE AN EVEN MORE ATTRACTIVE TARGET THAN YOU WERE BEFORE.

80% of organizations who pay a ransom experience a second ransomware attack shortly thereafter.

YOUR BUSINESS WON'T FULLY RECOVER, MAYBE EVER...

Even if you're lucky enough to receive a decryption key after you pay, that key might not be any good... Cybercriminals are just that, and not recovery specialists. So, there's a high chance your data and files could be lost, potentially forever.

TROJAN HORSES

OVERVIEW

Its name speaks for itself, relating to the historic significance it all started out as. The original Trojan Horse used by Greeks during the Trojan War has metaphorically become known as a trick played upon a victim (or enemy) to unknowingly let them in somewhere.

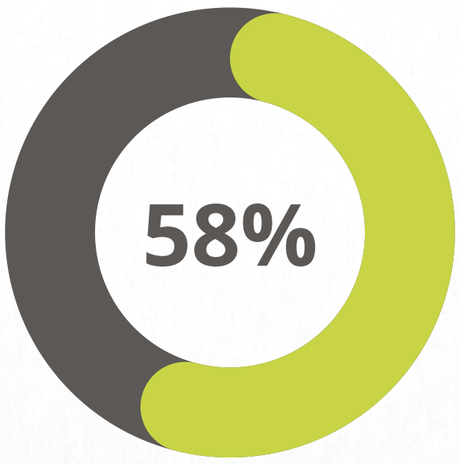
In the case of the Trojan Horse malware, it is practically an identical situation, with the one difference: it's not a place the victim is inviting the culprit into, but rather access into their devices. Disguised as legitimate online software, Trojan Horses are most commonly in the form of:

- **Email attachments**: fake emails with an attachment that once clicked, infects your entire device.
- **Software updates**: fake software that once clicked, infects your entire device.
- **File-sharing sites**: although helpful, cybercriminals easily can upload copies of illegitimate software to entrap users.
- **Hi-jacked websites**: hacked websites with malicious codes that once clicked, downloads a virus.
- **Infected Wi-Fi**: fake Wi-Fi designed to look real to gain access into a user's device.

Trojan Horses are the oldest form of malware, but that doesn't mean that they are not evolving and adapting to the cybersecurity practices being enforced. Although not as dangerous as ransomware, Trojan Horses have, and continue to, play a role in today's cyber threats.

EXAMINING THE FACTS

Now that you are better familiarized with Trojan Horses, let's dive into exactly how dangerous it has become.



of malware is made up
Trojan Horses.

Known as Zeus, this is of the most famous, recent Trojan Horses attacks (2010), where hackers stole this amount from numerous business accounts in Eastern Europe.

Trojan Horses are responsible anywhere between these percentages for global malware attacks.

PHISHING

OVERVIEW

Out of all cyber attacks, the most common and the one everyone must be extra prepared for is phishing. Unlike malware, this form of cyber attack is more personal and manipulative, uniquely designed for victims easily fall for.

Phishing is an online scam, usually in the form of an email (also in the form of text messages and advertisements), where cyber criminals present themselves as a legitimate operation/organization to access and steal your valuable data.

Most common phishing emails ask users to click on an embedded link or download an attachment, and input personal information. The moment a user interacts with such an email, they give the cybercriminal complete control and access to the user's valuable data and credentials.

To make matters worse, the COVID-19 pandemic has caused phishing to soar through the roof in both abundance, magnitude, and damage. A blessing in disguise for cyber criminals, this pandemic has given them an advantage to convince people to share their personally identifiable information, account credentials, and most valuable data (i.e. name, address, social security number, driver's license, credit card, etc.).

In effect, phishing has become the number one cyber attack on companies, the number one type responsible for global fraud, and the **root cause for data breaches - approximately 90%!**

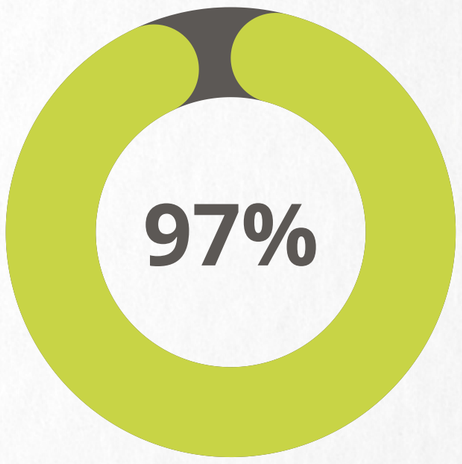
What's most important to understand is that phishing emails target companies of all shapes, sizes, and sectors. So, let's take a look at a few facts.

EXAMINING THE FACTS

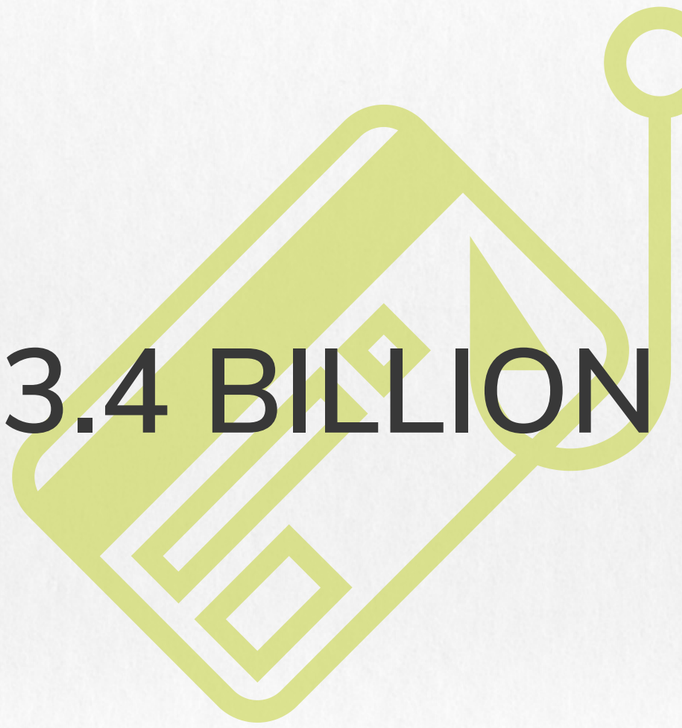
Now that you are better familiarized with phishing, let's dive into exactly how dangerous it has become.

of phishing emails are for gathering intelligence.

of cybersecurity attacks start with phishing.



of successful phishing attacks are caused by human error.



Phishing emails are sent everyday across the world.

Smaller businesses between this size are more at risk to phishing attacks.

Emails that individuals and businesses receive are a phishing email.

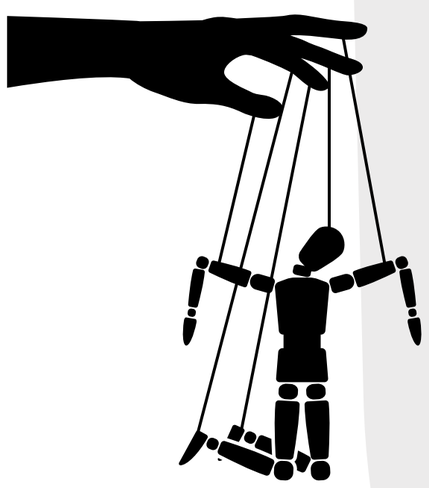
AVOIDING THE HOOK

If you have come across a phishing email in your inbox, it is important you know how to protect yourself. Simply put: do not interact with it in any way. According to the recent study by Security Affairs, it is stated that, "Human error remains the highest cause of successful phishing attacks worldwide, as **97% of users fail to identify phishing emails**." So, let's review how to recognize a phishing email.

A PHISHING EMAIL IS...

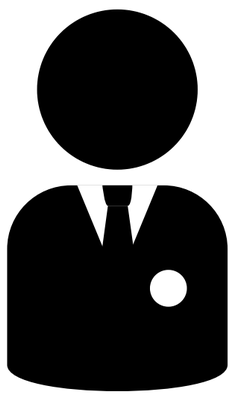
SUSPICIOUS

- Is sent from an unknown and unverified sender's email address - one you do not recognize.
- Is grammatically incorrect and has multiple spelling errors.
- Includes random and unverified links and/or attachments.



MANIPULATIVE

- Uses threatening language and/or instills panic.
- Requests and/or forces to click on a link or download an attachment.
- Is strategically written for reader to immediately carry out an action.



PERSONABLE

- Asks to confirm personal information.
- Asks to confirm financial information.
- Asks to change password or input credentials.

INSIDER THREATS

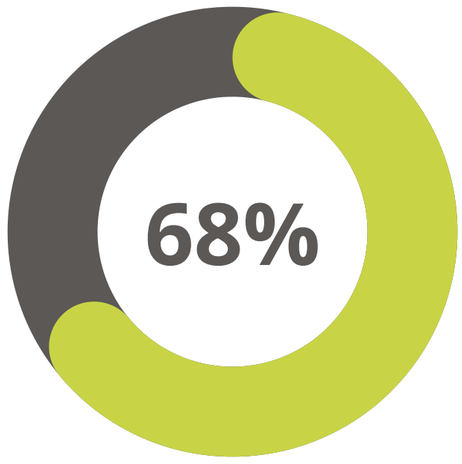
OVERVIEW

It's hard to imagine that the culprit responsible for a company's data breach is a fellow co-worker, an executive leader, or a third-party vendor, entrusted with to uphold the company's values and support its growth. But the unfortunate fact of the matter is that this is true...

To make matters worse, insider threats are one of the most difficult forms of cyber attacks to detect, not to mention report. **89% of security incidents go unreported every year** because most businesses sweep such news under the rug to avoid reputational damage. In 2020 alone, there were **approximately 4,716 reported insider incidents**, but that's not including the unreported numbers... The top, five reasons for an insider attack include:

- **Employee negligence.**
- **Personal gain and/or competitive advantage.**
- **Employee malice.**
- **Poor cybersecurity measures of a third-party or vendor.**
- **Social engineering vulnerability.**

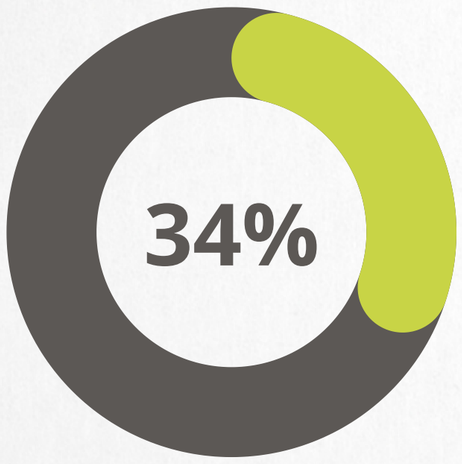
According to Gurucul's *Insider Threat Report* (2020), their findings regarding how serious insider threats are can be summarized with this key finiding:



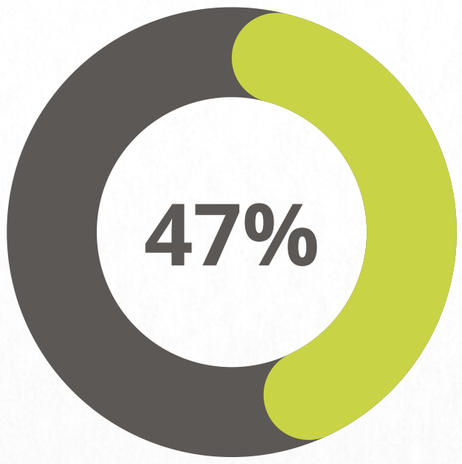
of organizations feel vulnerable and more susceptible to insider attacks.

EXAMINING THE FACTS

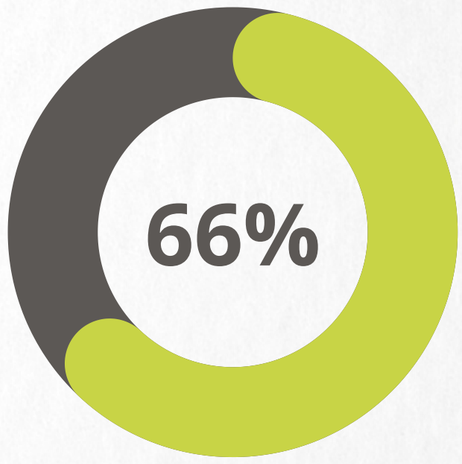
Now that you are better familiarized with insider threats, let's dive into exactly how dangerous it has become.



of businesses are affected by insider attacks globally.



increase in insider attacks over the last two years.



of organizations believe insider attacks are more likely than external.

Internal security breaches happen daily in the U.S.

Organizations cannot determine the complete damage of an insider attack.

Organizations consistently worry about insider attacks that they cannot prepare for.

EMPLOYEE THREATS

OVERVIEW

Let's begin with regular employees and the threat they bring. Back in December 2019, Microsoft found itself in an unfortunate position. Following the deployment of new security rules (*Azure*), Microsoft's employees incorrectly configured them, causing a data leak of over **250 million** entries of customer support information.

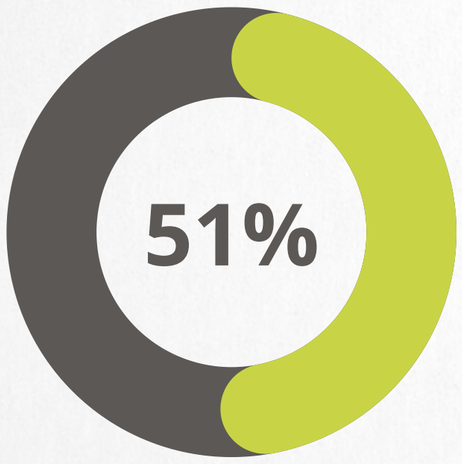
When it comes to your employees, you can never be too careful. In Microsoft's case, they were lucky that pure negligence was behind this attack. Because no PII (personally identifiable information) was leaked and Microsoft quickly took care of the matter, they avoided a fine of up to millions of dollars. However, in many other instances, the end result is not as fortuitous.

In September 2018, a (former) Cisco employee gained access to the company's cloud infrastructure and successfully **deleted 456 virtual machines.** Only last year was the situation resolved, ending with Cisco paying **$1 million** to their impacted users; Cisco also spent approximately **$1.4 million** in employee time for damage control and repair.

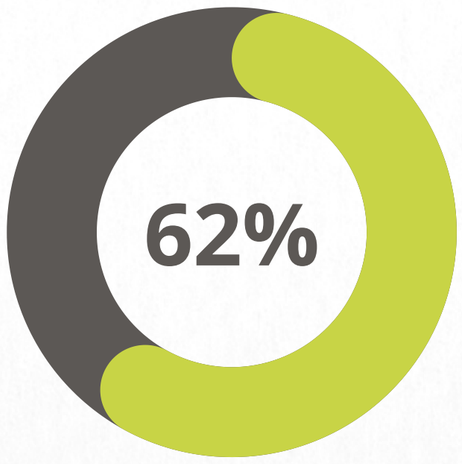
From employee negligence to personal gain, these are just a few of the countless examples of how big a security risk regular employees pose to companies. And it doesn't matter if it's a national corporation or a local SMB, any company can easily become a victim.

EXAMINING THE FACTS

So, exactly how big of a risk are employees when it comes to cyber security?



of insider attacks come from regular employees.



of employee-caused attacks are due to negligence.

of employee-caused attacks are due to malicious intent.

The average cost of insider attacks for organizations across the world.

Average cost per insider attack due to employee negligence.

Average cost per insider attack due to employee malice (criminal).

THIRD-PARTY THREATS

OVERVIEW

A trusted partner may not be so trustworthy after all. Similar to regular employees, third-parties or vendors cause insider attacks, primarily through poor cybersecurity measures (negligence). Fortunately, out of these three types of insider threats, third-parties are the least common. Unfortunately, they are on the rise... And the damage is just as severe...

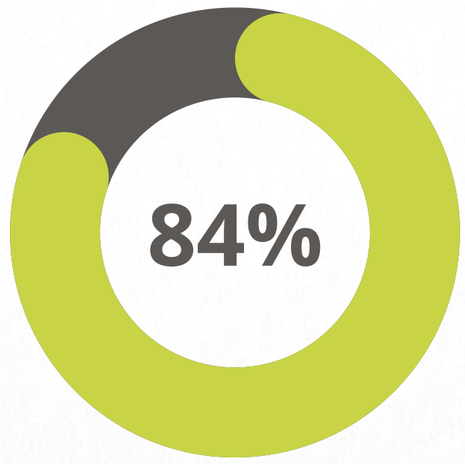
Last January (2020), cybercriminals compromised a third-party application regularly used by Marriot. The result? Over **5.2 million records of personally identifiable information**, including gender, birthdays, and account preferences. Because hackers were successfully able to gain access into Marriot's employees' credentials, this showed the cause as ineffective cybersecurity systems in place. Unlike the case of Microsoft, due to the PII leakage, Marriot faced **a fine of up to $124 million**.

A big factor as to why third-party insider attacks are on the rise is because cybercriminals are constantly looking to take advantage of a company's weakest link and soft spot(s). The COVID-19 pandemic became a hotbed for phishing attacks, and third-parties are becoming a hotbed for insider attacks.

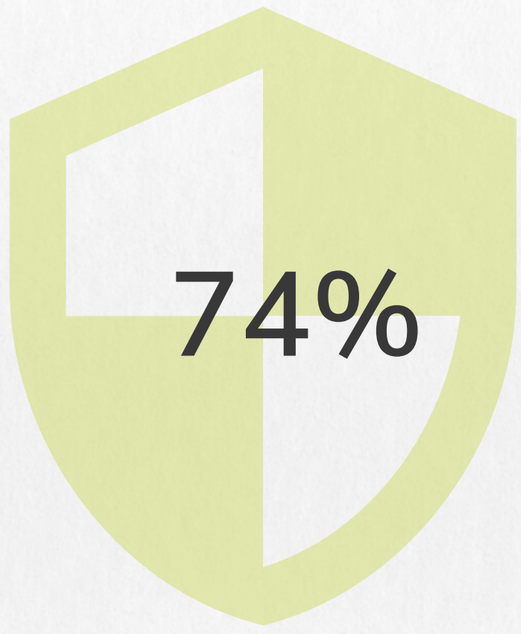
With a third-party as the source of an insider attack, the risks augment to not just cybersecurity, but operational, reputational, and compliance.

EXAMINING THE FACTS

So, exactly how big of a risk are third-parties when it comes to cyber security?



of organizations have had an insider attack perpetrated by a third-party, in the last three years.



Organizations are taking more extensive measures to protect themselves from third-party insider attacks.

Average range of insider attacks that are caused by third-parties and/or vendors.

PRIVILEGED IT USER THREATS

OVERVIEW

Last, but far from least, we arrive at the privileged IT users. This ranges from executives and high-level administrators, to managers and general business users. Because they hold the greatest access to all company information across the board, they pose the greatest cybersecurity risk with insider attacks. Approximately **63% of organizations state that privileged IT users are the greatest insider threat to their business**.

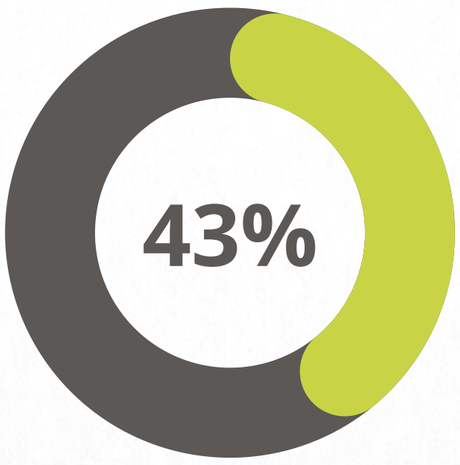
In March 2020, the (now former) VP of Stradis Healthcare in Georgia decided to disrupt countless numbers of the company's PPE (personal protective equipment) shipments. His actions resulted in **over 115,000 company records destroyed**, along with an additional **2,400 permanently lost**. As a result, Stradis Healthcare suffered a delay in fulfilling their vital PPE orders during the COVID-19 pandemic, in addition to the **$200,000 in damage** to company property and information.

According to a recent Fortinet survey, the top three reasons for an insider attack from a privileged user are as follows:

- **Fraud (55%).**
- **Monetary gains (49%).**
- **IP theft (44%).**

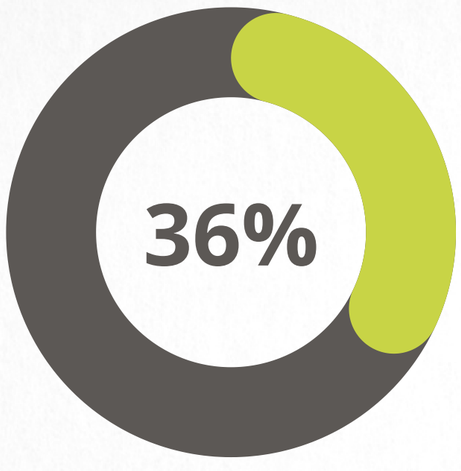
EXAMINING THE FACTS

So, exactly how big of a risk are privileged IT users when it comes to cyber security?



of insider attacks are due to malicious, privileged insiders.

Average cost of an insider attack caused by a malicious, privileged IT user.



of organizations actually monitor their user privileges.

of organizations state they don't have effective user management systems in place.

UPCOMING TRENDS

So, what are you to do with all this information? How do you best prepare, prevent, and protect yourself and your business from all these types of cybersecurity attacks?

For each of the threats we've discussed, there are numerous ways and best practices to implement to establish a strong and effective cybersecurity program in place. As move into 2022, here are our CW Technology predictions for the most important trends in cybersecurity.

1 REMOTE WORK: INCREASE IN USER AWARENESS

The impact of the COVID-19 pandemic will never be forgotten, and the workplace environment will certainly never go back to the way it was before. As more organizations move into a hybrid-model, greater cybersecurity swill be put in place.

If COVID-19 taught us anything, it's that companies depend on their employees for protection. A recent article by Finance Online estimated that 80% of cybersecurity attacks have been prevented, thanks to improved user awareness. Moving forward, we're expecting to see increased user awareness in the following ways:

- **Employee security awareness training.**
- **Stricter BYOD guidelines and greater use of VPN's.**
- **Installation of updated anti-malware and security patching.**

2 MFA: CENTER OF ALL

Be it at home, at work, or in your personal, social environment, increased security while using online services is a practice that simply cannot be ignored these days. Multi-factor authentication (MFA) - also known as two-factor authentication - is a solution for Internet safety and is slowly growing into a rule of thumb, implemented by all businesses and individuals.

So, in addition to adding this onto our personal accounts (such as social media platforms), we're expecting a surge in businesses making this a mandatory step for all employee account usage. With such a simple, but crucial step, it goes hand-in-hand in helping decrease the number of insider attacks, starting with those from regular employees.

3 RANSOMWARE: STILL #1 CYBER THREAT

Unfortunately, not much has changed in this area. As you remember, this type of malicious software is expected to grow in number of attacks and methodology. Starting with healthcare and education, more vulnerable industries must be fully equipped and prepared for this incriminating level of change coming their way.

To make matters worse, ransomware won't stop at just laptops and workstations. Cybercriminals have begun taking advantage of various mobile features to spread ransomware (i.e. emergency alerts).

A NOTE FROM CW TECHNOLOGY

Readily available for all, one of the primary reasons for this report was to provide highly valuable information on of one of the most important, relevant, ever-growing topics: cyber security.

Understanding this material is one step in the right direction. Another is sharing it. We highly recommend that you use, apply, and discuss this information with your employees, your coworkers, and even family and friends. The greater measures you implement, the greater protection your business will have.

At CW Technology, our purpose is an unwavering commitment to create success. One side to this includes having an ongoing discussion to determine how to best fit your security business needs. All of our clients have ongoing security and planning conversations with their team advisors, outlining the optimal business process and strategy.

That said, we'd like to share a few times of note that help you begin this process yourself!

1 CROWDSTRIKE EDR

Nowadays, anti-virus is simply not enough... EDR (enhanced detection and response) solutions provide a greater level of security by not only protecting your environment, but learning your usage and traffic patterns.

2 CYBERLIABILITY INSURANCE

All companies, regardless of size, scope, or industry, must explore cybersecurity policies. Be aware of the requirements of each policy, in order to ensure protection.

3 DISASTER RECOVERY PLANNING

An idea of what to do in the event of any disaster is not a solution. The key is having a solidified, written plan, outlining the optimal steps to take should a disruption occur.

4 ACCEPTABLE USE POLICY

Drawing a boundary is necessary. The development of a plan for acceptable use of company equipment (i.e. laptops, workstations, Internet access, etc.) ensures protection.

5 INTRUSION PREVENTION TESTING

What's the difference between hoping your environment is set up properly versus knowing your environment is set up properly? Regular testing!

6 EMPLOYEE SECURITY TRAINING

In any environment, the biggest security risk are the employees. Providing regular feedback and testing is essential to closing this loop.

SOURCES CITED

22, M., & Chavali, S. (2021, July 27). 5 examples of insider threat-caused breaches that illustrate the scope of the problem: Proofpoint us. Proofpoint. Retrieved October 18, 2021, from https://www.proofpoint.com/us/blog/insider-threat-management/5-examples-insider-threat-caused-breaches-illustrate-scope-problem.

Bisson, D. (n.d.). 7 data breaches caused by human error: Did encryption play a role? Venafi. Retrieved October 18, 2021, from https://www.venafi.com/blog/7-data-breaches-caused-human-error-did-encryption-play-role.

Brignall, M. (2018, November 21). Amazon hit with Major Data Breach days before Black Friday. The Guardian. Retrieved October 18, 2021, from https://www.theguardian.com/technology/2018/nov/21/amazon-hit-with-major-data-breach-days-before-black-friday.

Cook, S. (2021, May 29). Malware statistics in 2021: Frequency, impact, cost & more. Comparitech. Retrieved October 18, 2021, from https://www.comparitech.com/antivirus/malware-statistics-facts/.

Cyberwiser. (n.d.). The 5 types of insider threats and how to deal with them. WISER. Retrieved October 18, 2021, from https://www.cyberwiser.eu/content/5-types-insider-threats-and-how-deal-them.

Digital in the Round. (2021, July 19). 17 shocking phishing statistics you need to read in 2021. Digital in the Round. Retrieved October 18, 2021, from https://digitalintheround.com/phishing-statistics/.

Ekran. (2020, December 15). 5 real-life examples of breaches caused by insider threats. 5 Real-Life Examples of Insider Threat-Caused Breaches | Ekran System. Retrieved October 18, 2021, from https://www.ekransystem.com/en/blog/real-life-examples-insider-threat-caused-breaches.

Ekran. (2021, January 11). 7 third-Party Security Risk Management Best Practices. 7 Best Practices for Third-Party Security Risk Management | Ekran System. Retrieved October 18, 2021, from https://www.ekransystem.com/en/blog/third-party-providers.

Firch, J., Firch, J., Allen, R. by J., & Allen, J. (2021, July 13). 10 cyber security trends you can't ignore in 2021. PurpleSec. Retrieved October 18, 2021, from https://purplesec.us/cyber-security-trends-2021/#MFA.

Fortinet. (n.d.). What is a trojan horse? trojan virus and malware explained. Fortinet. Retrieved October 18, 2021, from https://www.fortinet.com/resources/cyberglossary/trojan-horse-virus.

Fortinet. (n.d.). What is a trojan horse? trojan virus and malware explained. Fortinet. Retrieved October 18, 2021, from https://www.fortinet.com/resources/cyberglossary/trojan-horse-virus.

Franks, K. (2020, April 3). Account for third party vendors in Your insider threat security program. Gurucul. Retrieved October 18, 2021, from https://gurucul.com/blog/account-for-third-party-vendors-in-insider-threat-security-program.

Gilbert, N. (2021, April 1). 31 crucial insider threat statistics: 2021 latest trends & challenges. Financesonline.com. Retrieved October 18, 2021, from https://financesonline.com/insider-threat-statistics/.

Howard, A. H. and K., Holub, A., & Howard, K. (2021, January 26). How trojan malware is evolving to survive and evade cybersecurity in 2021. Cisco Umbrella. Retrieved October 18, 2021, from https://umbrella.cisco.com/blog/how-trojan-malware-is-evolving-to-survive-and-evade-cybersecurity-in-2021.

SOURCES CITED

Johnson, J. (2021, September 10). Internet users in the world 2021. Statista. Retrieved October 18, 2021, from https://www.statista.com/statistics/617136/digital-population-worldwide/.

Johnson, J. (2021, September 9). Phishing: Most targeted industries 2021. Statista. Retrieved October 18, 2021, from https://www.statista.com/statistics/266161/websites-most-affected-by-phishing/.

Jones, C. (2021, September 6). 50 phishing stats you should know in 2021. Expert Insights. Retrieved October 18, 2021, from https://expertinsights.com/insights/50-phishing-stats-you-should-know/.

Jovanović, B., Vojinovic, I., Spajić, D. J., & Cvetićanin, N. (2021, March 22). A not-so-common cold: Malware statistics in 2021. DataProt. Retrieved October 18, 2021, from https://dataprot.net/statistics/malware-statistics/.

Kass , D. H. (2020, April 29). Insider threat costs: Key Cybersecurity Research Findings. MSSP Alert. Retrieved October 18, 2021, from https://www.msspalert.com/cybersecurity-research/insider-threats-key-findings/.

McAfee. (2019, November 26). What is malware and why do cybercriminals use malware? McAfee. Retrieved October 18, 2021, from https://www.mcafee.com/en-us/antivirus/malware.html.

McAfee. (n.d.). Business home. McAfee. Retrieved October 18, 2021, from https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware.html#how-it-works.

Moes, T. (2021, June 22). What is a trojan horse virus? 5 examples you need to know. SoftwareLab. Retrieved October 18, 2021, from https://softwarelab.org/what-is-a-trojan-horse/.

Proofpoint. (2021, September 21). 2021 report on phishing attacks - state of the phish. Proofpoint. Retrieved October 18, 2021, from https://www.proofpoint.com/us/resources/threat-reports/state-of-phish.

PurpleSec. (2021, August 12). 2021 ransomware statistics, data, & trends. PurpleSec. Retrieved October 18, 2021, from https://purplesec.us/resources/cyber-security-statistics/ransomware/.

Rosenthal, M. (2021, October 5). Insider threat statistics you should know: Updated 2021. Tessian. Retrieved October 18, 2021, from https://www.tessian.com/blog/insider-threat-statistics/.

Rosenthal, M. (2021, October 5). Phishing statistics (updated 2021) - 50+ important phishing stats. Tessian. Retrieved October 18, 2021, from https://www.tessian.com/blog/phishing-statistics-2020/.

Sobers, R. (2021, July 7). 81 ransomware statistics, data, trends and facts for 2021: Varonis. Inside Out Security. Retrieved October 18, 2021, from https://www.varonis.com/blog/ransomware-statistics-2021/.

SonicWall. (2021). Mid-Year Update SonicWall Cyber Threat Report. Retrieved October 18, 2021, from https://assets2.brandfolder.io/bf-boulder-prod/4tt88vkkfs6vnxjcwf5h4hf/v/1003039825/original/FY21-Jul-EN-Full%20Report%20-%20Mid-Year-Update-2021-SonicWall-Cyber-Threat-Report.pdf.

Stealthlabs. (2021, May 27). Infographic: 20 insider threats alarming facts and figures. Stealthlabs. Retrieved October 18, 2021, from https://www.stealthlabs.com/blog/infographic-20-alarming-insider-threats-statistics/.

SOURCES CITED

https://www.stealthlabs.com/blog/infographic-20-alarming-insider-threats-statistics/.
Swiss Cyber Forum. (2021, September 23). 41 insider threat statistics you should care about. Swiss Cyber Forum. Retrieved October 18, 2021, from https://www.swisscyberforum.com/blog/41-insider-threat-statistics-you-should-care-about/.

Talamantes, J. (n.d.). 7 times employees caused damaging data breaches. RedTeam Security - Union Depot Building, 214 4th Street E., Suite 140, Saint Paul, Minnesota 55101. Retrieved October 18, 2021, from https://www.redteamsecure.com/blog/danger-ranks-7-times-employees-caused-data-breaches.

The United States Department of Justice. (2020, October 20). Former employee of medical packaging company sentenced to federal prison for disrupting PPE shipments. The United States Department of Justice. Retrieved October 18, 2021, from https://www.justice.gov/usao-ndga/pr/former-employee-medical-packaging-company-sentenced-federal-prison-disrupting-ppe.

Vigderman, A. (2021, April 7). What is a trojan horse virus & how do you get rid of it? Security.org. Retrieved October 18, 2021, from https://www.security.org/antivirus/trojan/.

Vuleta, B. (2021, September 20). 44 must-know malware statistics to take seriously in 2021. 44 Must-Know Malware Statistics to Take Seriously in 2021. Retrieved October 18, 2021, from https://legaljobs.io/blog/malware-statistics/.

Waldman, A. (2021, June 16). Repeat ransomware attacks hit 80% of victims who paid ransoms. SearchSecurity. Retrieved October 18, 2021, from https://searchsecurity.techtarget.com/news/252502519/Repeat-ransomware-attacks-hit-80-of-victims-who-paid-ransoms.

Winder, D. (2020, April 28). Revealed: The supermarkets that will sell you malware for $50. Forbes. Retrieved October 18, 2021, from https://www.forbes.com/sites/daveywinder/2020/04/28/revealed-the-supermarkets-that-will-sell-you-malware-for-50/?sh=481c4a5c30ae.