WHITEPAPER

Cyberattacks pose one of the greatest risks to company security

Executive Summary

Stopping cyber-attacks is now one of the greatest priorities for companies across the world.

As work increasingly moves online, hackers have fine-tuned their skills to steal sensitive private and personal data from organizations and generate a handsome profit for themselves.

The problem grew in 2020 after the start of the COVID-19 pandemic. Most companies were forced to move their operations online, a trend expected to continue even after the pandemic subsides. Employees moved away from their secure company networks onto their less secure residential networks, creating an attractive — and lucrative — opportunity for hackers. At current projections, cyberattacks are expected to cost companies across the world a total of $6 trillion in 2021.[1]

> *Cyberattacks are expected to cost companies across the world a total of $6 trillion in 2021*

Companies have consequently become more aware of the need for robust cybersecurity strategies, but much work remains to be done. Many organizations report that their cybersecurity teams are understaffed, and many of their positions are filled by inexperienced individuals.

> *Companies need to ensure their data is confined to only those that need access to it, and they need to ensure their employees are educated on best practices to enable better security.*

So how can executive teams better protect their operations? Dealing with a complex problem like cyberattacks requires a comprehensive solution. Companies need to ensure their data is confined to only those that need access to it, and they need to ensure their employees are educated on best practices to enable better security. Software needs to be constantly updated to ensure protection from the latest threats. In the event of a breach, designing an appropriate business continuity plan will help enable companies to overcome and thrive even if disaster strikes.

Growing cybersecurity risk

The enormous growth of online communications and data storage in recent years has created a treasure trove for hackers, and they have used the opportunity to fine-tune their hacking capabilities and become more adept at stealing organizations' data.

The problem exploded in 2020 during the pandemic, when virtually all work, social and private activity moved online. This concentrated all company activity into online channels, exposing many organizations to attack. The problem was made significantly worse by the fact that most employees had moved away from offices containing more secure networks to their homes, where residential networks were less equipped to withstand sophisticated cyberattacks.

The result was predictable. One study found that large-scale data breaches jumped 273% in the first quarter of 2020 alone.[2]

> *Most employees had moved away from offices containing more secure networks to their homes, where residential networks were less equipped to withstand sophisticated cyberattacks.*

Challenges facing companies

Despite the growing prevalence of cybersecurity attacks, many companies are still severely under-equipped to deal with them, lacking many of the basic requirements needed to defend themselves. One study found that 62% of companies reported that their cybersecurity teams were either "somewhat" or "significantly" understaffed.[3]

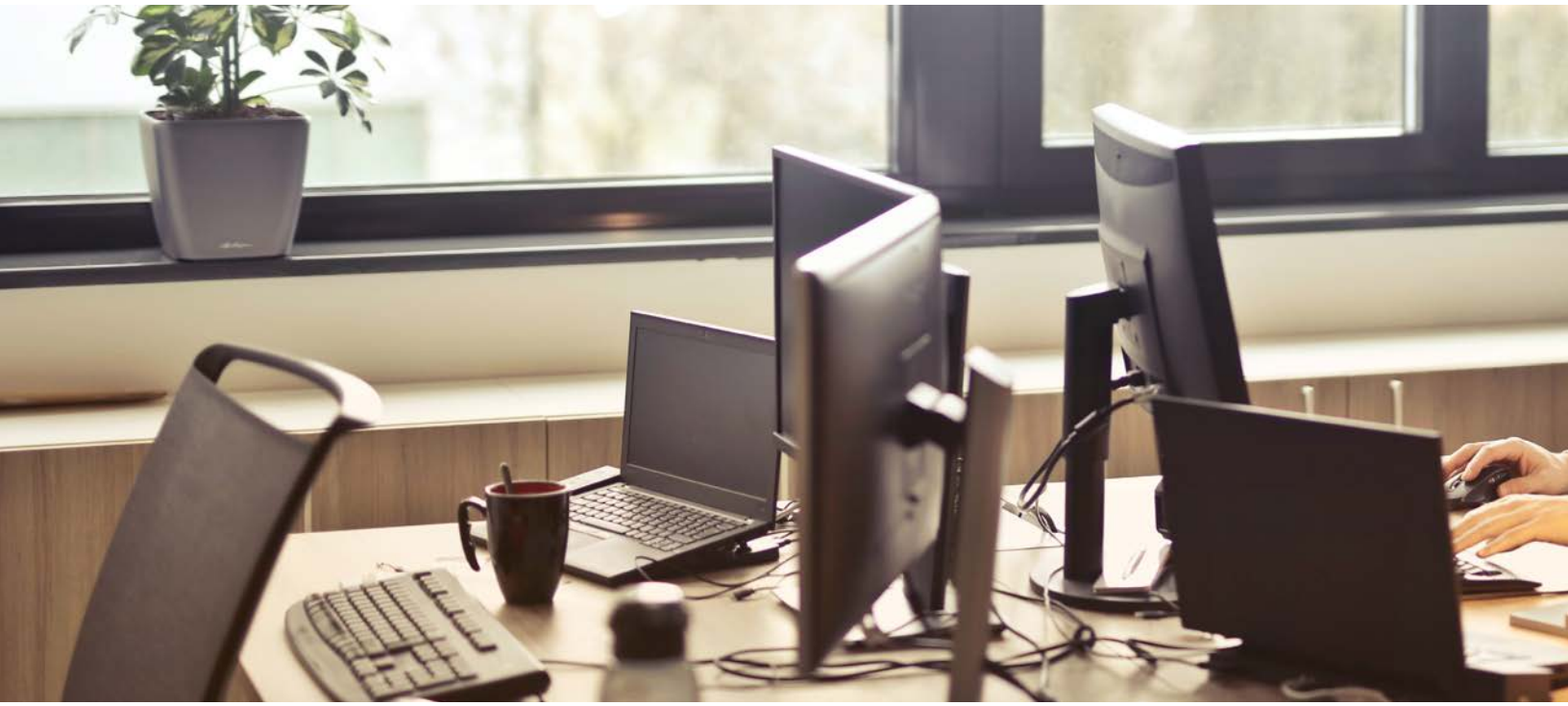
Shockingly, the same study found that 70% of organizations reported that less than half of their cybersecurity staff were well-qualified, a problem made even worse by what respondents reported to be a long and cumbersome hiring process.

62%

of companies reported that their cybersecurity teams were either "somewhat" or "significantly" understaffed

70%

of organizations reported that less than half of their cybersecurity staff were well-qualified



Organizations need to act fast to overcome these challenges. The technology companies use is quickly evolving, and hackers are quickly adapting to exploit vulnerabilities. This is especially the case in the cloud computing space. Cloud computing is becoming one of the primary forms of data storage and computing power used by organizations, making this one of the fastest growing targets for hackers.

There were more than 7.5 million external attacks on cloud accounts in the second quarter of 2020 alone.[4] The total number of attacks in the first part of the year surged by 250% compared to 2019.[5] As companies continue to develop and rely on more advanced technologies, they must equip their cybersecurity teams with the personnel and resources they need to ensure equally skilled hackers cannot gain access to them.

> *"There were more than 7.5 million external attacks on cloud accounts in the second quarter of 2020 alone. The total number of attacks in the first part of the year surged by 250% compared to 2019."*

Ransomware

One of the most common types of cybersecurity attacks is ransomware, and the threat is growing.

According to VMware, ransomware attacks increased 150% in 2020.[6] This spike was undoubtedly exacerbated by the COVID-19 pandemic, but ransomware attacks have been steadily increasing for several years, so this trend is likely to continue. Early figures suggest that the frequency of ransomware attacks has continued to climb in 2021.[7]

Ransomware attacks occur when hackers gain access to a company's software and encrypt sensitive data information and other files. They then demand a ransom from the company and network administrators, which some executives, unsurprisingly, feel obliged to pay. The average cost of a ransomware attack was more than $84,000 in 2019. Similar to the total number attacks, total dollar figures paid out to ransomware hackers have skyrocketed since the start of 2020.

Companies do not just lose the amount paid in ransom when an attack occurs. Losses also include the amount of lost revenue while data files are encrypted, costs associated with fixing and replacing damaged software or hardware, and any costs required to repair the brand image in the eyes of customers. There are additional costs associated with notification provisions — the process by which companies must notify all individuals of a security breach. Some companies may even be expected to pay fines if their security infrastructure was non-compliant.

The problem is getting worse. More hackers are beginning to store copies of the data they steal and threaten to release it publicly. For company executives, this is a practically unthinkable prospect, and hackers know it. This enables them to demand still higher ransom sums.

Fortunately, most ransomware attacks happen due to phishing, accounting for around 67% of the total in 2020.[8] That means companies can narrow their focus when building their security plans against ransomware attacks, potentially making them more successful at stopping ransomware in the long term.

67%

Fortunately, most ransomware attacks happen due to phishing, accounting for around 67% of the total in 2020.

Phishing

Phishing occurs when hackers gain access to private data information by digitally disguising themselves as clients, senior executives, or other trusted individuals or entities and sending emails to unsuspecting employees requesting sensitive information. Information commonly stolen through phishing attacks include passwords, social security numbers and other personal information, all of which attackers can use to access email, bank and other private accounts.

Phishing is a serious threat to companies, and it remains one of the most common forms of data breaches. In 2019 alone, 88% of organizations reported experiencing a phishing attack at least once.[9] As mentioned, it can also lead to other forms of attack, making it an especially urgent and important challenge to overcome.

Like ransomware, the number of phishing attacks saw an enormous spike in 2020. According to data from the FBI, the total number of attacks jumped from 114,702 in 2019 to 241,324 the following year, making it the most common type of cyberattack in 2020.[10]

88%

of organizations reported experiencing a phishing attack at least once.

What can companies do?

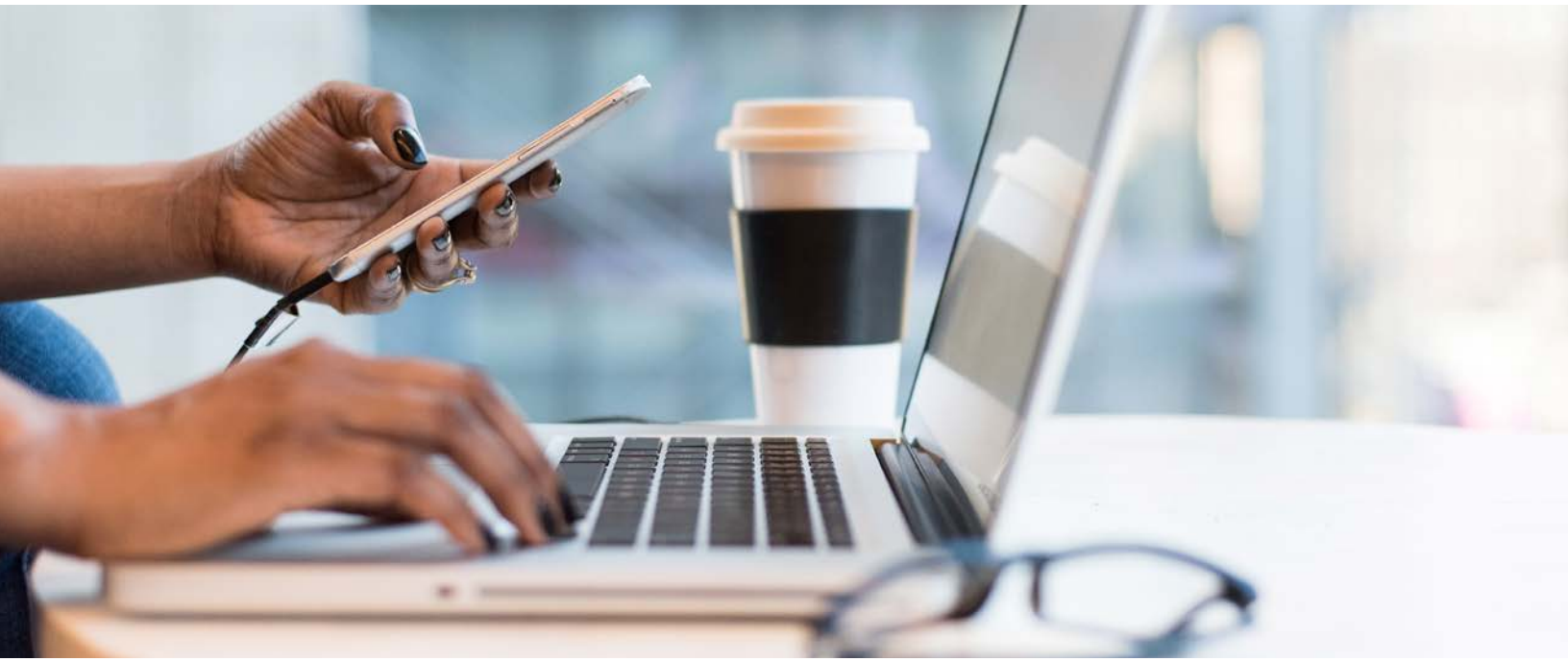
The best way to handle a threat is to prevent it from ever taking place.In addition to hiring and training a skilled, experienced and capable cybersecurity team, companies can also take the following proactive steps to keep their data safe:

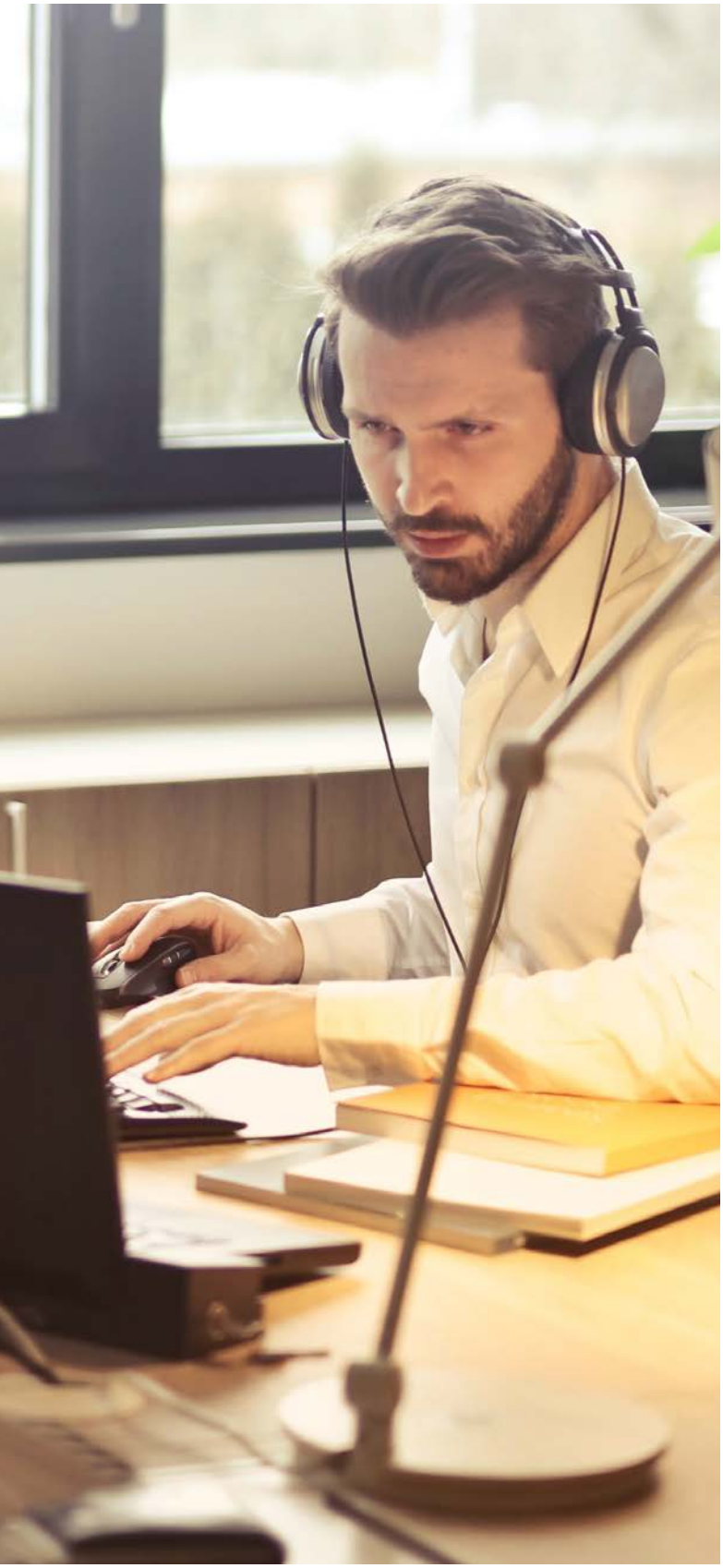
Prevent human error

Human error is one of the most common causes of cybersecurity breaches. Limit how many employees have access to company data so that, in the event an employee causes a data breach, the information hackers can steal will be restricted to that individual. It is also important to ensure outgoing employees lose all access to company data as soon as they leave the organization.

Invest in employee education

It is important that employees are properly trained on best practices to prevent common attacks from occurring. Using company computers on personal or residential networks can pose a risk, so employees should understand how to use their computers at home safely and securely. This also applies to mobile phones and personal devices. They may not be as well secured as company networks, so conducting business over these networks can increase the chances of a breach.





Create business continuity and response procedures

On the macro level, it is important to develop a comprehensive business continuity plan to help restore any lost data in the event of a breach. Ensure that every step is minutely detailed and that key individuals are identified and their roles clearly outlined. A solid business continuity plan should also ensure that all data is backed up regularly and copies are stored in a secure, dedicated offsite location.

Update and patch security software

Lastly, companies need to invest in high-quality cybersecurity software to guarantee they have strong protection against the latest threats. Part of this process is ensuring software updates are properly scheduled and applied as soon as possible to maximize the efficacy of their security infrastructure. If they identify a vulnerability in any part of their security infrastructure, they should ensure that it is patched as soon as possible.

Cybersecurity threats are on the rise, and this trend is likely to continue as more companies shift to a totally virtual or hybrid work environment. Those that are unable (or unwilling) to keep up with the threat will unnecessarily expose themselves to risk, theft and loss, severely threatening their bottom line. The more prudent organizations, however, will ensure that their sensitive information stays safe, helping them stay agile in the face of threats and paving the way for future growth.

900 Route 9 North, Suite 503
Woodbridge, NJ 07095-1003
800.446.7647
www.nipgroup.com

1. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
2. https://www.cnbc.com/2020/07/29/cybercrime-ramps-up-amid-coronavirus-chaos-costing-companies-billions.html
3. https://www.isaca.org/go/state-of-cybersecurity-2020
4. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-nov-2020.pdf
5. https://www.zdnet.com/article/vast-majority-of-cyber-attacks-on-cloud-servers-aim-to-mine-cryptocurrency/
6. https://www.cnbc.com/2020/07/29/cybercrime-ramps-up-amid-coronavirus-chaos-costing-companies-billions.html
7. https://hbr.org/2021/05/ransomware-attacks-are-spiking-is-your-company-prepared
8. https://www.safetydetectives.com/blog/ransomware-statistics/#:~:text=Ransomware%20isn%27t%20going%20away,will%20continue%20to%20be%20targeted.
9. https://www.proofpoint.com/sites/default/files/gtd-pfpt-uk-tr-state-of-the-phish-2020-a4_final.pdf
10. https://www.tessian.com/blog/phishing-statistics-2020/#:~:text=According%20to%20the%20FBI%2C%20phishing,in%202020%20compared%20to%202016