FSJ Solutions
CONTENT - PROCESS - ANALYTICS - CLOUD SECURITY

eBook

Detect.Deflect. Protect.

3 Deceitful Ways Cybercriminals Target Your Business and How You Can Combat Them

BlueVoyant Core: MDR™ BlueVoyant Terrain: SCD™ BlueVoyant Sky: DRP™

BlueVoyant

New threats, smarter enemies, and increasing vulnerability.

The thought of a cyber attack causes sleepless nights for many, especially business owners. However, despite their best efforts, a sea of responsibilities, limited resources, and lacking skill sets combined with an ever-evolving threat landscape make effective cyber protection hard to achieve. But burying your head in the sand or thinking "It won't happen to us" is never the right call. The fact is the number of hackers out there is increasing, and their attack methods are more complex and evolving.

Rather than simply stumbling upon credentials or cracking simple passwords as was once commonplace, cybercriminals are more deceitful and technically adept than ever before. To compel people to click on malicious links (or open infected applications), they use sophisticated manipulation and social engineering techniques that leading ad agencies would be proud of. Cybercriminals happily pretend to be you or a senior leader within your business to convince your staff to give away information or make payments. They're patient, first gaining a small foothold, then gathering information snippets over time until they have enough to carry out a more powerful and potentially business-crippling attack. And, in an ever more connected, digital business world, they have even more routes from which to strike.

Today, hackers aren't necessarily knocking on your network's door but that of your extended network – partners, suppliers, and even your clients. In a calculated twist, your business may not even be the attack's initial target. Threat attackers may circumvent the security of a business you're connected to, and a lack of threat visibility and undetected security vulnerabilities could mean your data, as well as the very survival of your business, are at risk.

So what is it that drives these cybercriminals? Why do they want to attack your business, and how do they have access to such funding?

It's simple. Cybercrime is more profitable than the global illegal drug trade. Earning around $600 billion in 2018, hacker hauls eclipsed the total income of the world's contraband producers and traffickers by hundreds of billions.[2]

Aside from physically stealing funds from your business or holding systems to ransom for a fee, data is also valuable to digital criminals. A one-time influx of money is nothing when they can access your clients' credit card details or login credentials. They won't hesitate to steal from the hundreds, if not thousands of individuals or sell their information to the highest bidder.

Sometimes it's not even about the money. Cybercriminals may be motivated to steal intellectual property or personal information that may lead to broader attacks, or they simply just want to make a point. Whatever the hacker's motivation, a breach of any kind doesn't come cheap. No business wants to deal with the cleanup, fines, lost revenue, and reputational damage that goes with a cyber attack.

The hard truth is that a breach is inevitable, but you can be proactive.

In this eBook, we'll look at how cybercriminals are targeting your business, the areas they focus on, and the steps you can take to counter the threat.

44% of executives believe that their growing use of partners and suppliers exposes them to significant security risks, with 30% saying their budgets aren't sufficient to ensure proper cybersecurity. Several pointed out that the criminals are better funded than they are.[1]

An ever-changing enemy in an evolving business landscape

Your business is your castle. Once upon a time, you could keep it safe by constructing strong walls, posting a few guards at the door, raising the drawbridge, and digging a deep moat around it. That's now the stuff of fairy tales. Today's networks simply can't be locked down due to the nature of business itself. Consider the connections required for your company to operate. How many partners and suppliers do you interact, if not fully interface with, using linked systems and APIs? Your customers can't access your products and services without connecting to your network in some form, and your staff likely operates in multiple locations using devices you don't fully control. The perimeter that was once contained to a single building now spreads as far as your furthest third-party connection or remote employee. And while your business benefits from this greater flexibility and increased operational efficiency, so do cybercriminals.

Let's take a look at three "ways in" they commonly exploit that you should be aware of.

Internal breaches

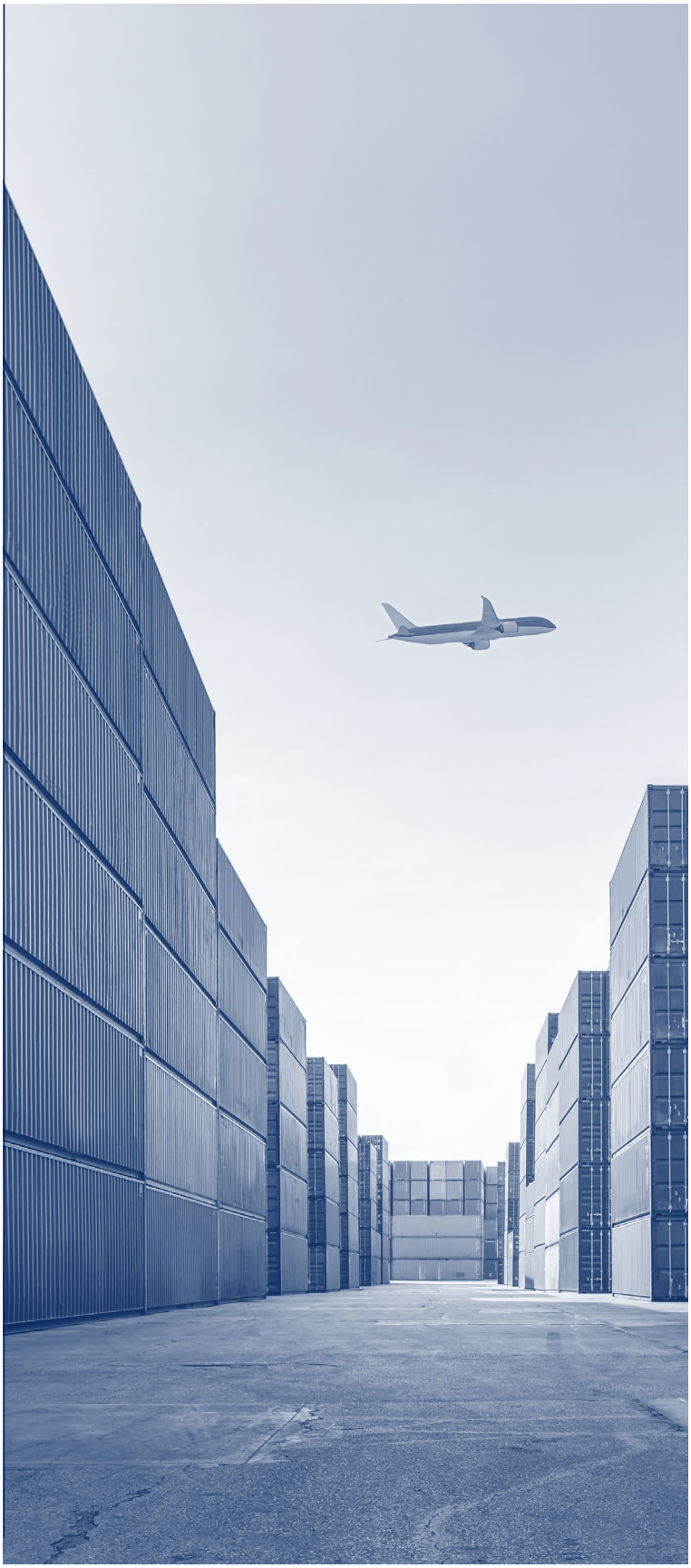
With cyber intruders able to spend longer inside company networks than ever, the risk of a more damaging attack is increased. The most common route into a network? Unpatched software and hardware presents a convenient vulnerability for hackers to exploit. They also target people to access information that will help them gain access or deploy malware. This normally comes in the form of a phishing attack via email or SMS, where a person is tricked into giving away sensitive information or clicking on a malicious link or file. Eighty-three percent of organizations experienced a phishing breach in 2021, and more than 6 billion phishing attacks are expected by the end of 2022. Even more worrying, 30% of phishing emails are opened.[3] Alternatively, hackers may take a "brute force" approach and attempt to compromise user accounts with weak passwords using manual methods, previously stolen data, or sophisticated software.

However, with "123456" as the most common password leaked on the dark web, closely followed by "Qwerty" and the wildly original "Password," hackers don't always have to work that hard.[4] It's also no surprise that 81% of the breaches carried out in 2020 were the result of stolen or weak passwords, according to the 2020 Verizon Data Breach Investigations Report.

Once they're in, hackers prefer to take their time. On average, cybercriminals spend more than two weeks digging around for useful or valuable information before they're either identified, leave of their own accord, or carry out a malicious act. And, if their entry point isn't secured afterward, the chances are they'll come back, too.

In addition to ensuring security patches are regularly administered, software is kept up to date, and employees are aware of phishing risks, organizations like yours must have visibility over the threat landscape and be able to quickly detect and act on suspicious network incidents. To do so, you should consider Managed Detection and Response (MDR).

Consider this scenario: Let's say you return from vacation and spot a broken window at the front of your house. As a chill washes over, several questions will immediately run through your mind. What caused that? Was it an accident or intentional? Has someone broken into my house? Have they taken anything? Are they still inside? MDR provides answers to questions like these for your internal network. With 24×7 monitoring of security logs, which helps to reduce your daily operational burden and focus on more strategic security activities, MDR helps to streamline threat alerts. It weeds out false positives to ensure that only serious threats are investigated. To continue the home security analogy, MDR acts like a super-smart surveillance system that knows the difference between a neighborhood cat crossing your front porch and a burglar checking to see if the patio door is unlocked. The best MDR solutions will draw from and enhance the value of the security tools you already have in place, including those from leading providers like Microsoft and Splunk, as well as offering ongoing expert support.



Supply chain breaches

According to a BlueVoyant report, Managing Cyber Risk Across the Extended Vendor Ecosystem, 93% of companies have suffered a cybersecurity breach because of weaknesses in their supply chain or third-party vendors, and 97% have been negatively impacted by a cybersecurity breach that occurred in their supply chain. Your goal should be to exist in the 3% of businesses that haven't.

Today, it's no longer enough to only focus on your own network. The threat now comes from your extended network too, and businesses are rapidly beginning to realize just how big those networks can be. A recent BlueVoyant survey revealed that the number of businesses reporting a supply chain of more than 1,000 companies more than doubled from 14% in 2020 to 31% in 2021. At the same time, the number of companies reporting 500 vendors or fewer dropped from 29% to 22%. Supply chains may well have expanded, especially in the wake of the pandemic, but it's more likely that companies have become more aware of the full extent of their vendor networks and the potential risks they pose.

A natural safeguard against supply chain breaches is to assess and audit vendors, ensuring they are taking the same steps you are to reduce risk. However, carrying out such checks on a monthly or even weekly basis won't enable your extended network to keep up with rapidly emerging new threats or stay ahead of agile, persistent attackers. It's also unlikely you'll know whether your vendors have taken the mitigation steps required. Thirty-eight percent of survey respondents said that they had no way of knowing when or if an issue arises with a third party, with 41% percent unable to easily verify if an issue they had informed suppliers about had been resolved.

For that reason, continuous monitoring and rapid remediation using Supply Chain Defense services are essential to avoid leaving your organization open to significant threats for an extended period of time.

Continuous monitoring and quick action against newly discovered critical vulnerabilities are no longer a "nice to have." You should consider a fully managed solution that can rapidly identify and resolve critical cybersecurity issues in your third-party ecosystem. Providers of such a service not only become your eyes on your wider network but can also work directly with vendors to solve issues for complete peace of mind.

Brand impersonation breaches

It's unlikely you operate a business without an online presence, whether it's a website, mobile app, or social media accounts. As a result, you face threats from cybercriminals in a number of different ways. Hackers can attack your business directly, compromising any one of your online entities, or they could go after your customers and employees, pretending to be your brand in order to receive payments or access sensitive information. Brand impersonation attacks of this nature increased by more than 360% in 2020.

Think about someone like John, a loyal customer who doesn't keep on top of things like phishing and other online scams. One day, he receives an email telling him that your company is updating its records and he needs to re-enter his bank details or risk having his account closed. John quickly types in his password and account details in the linked online form. Job done. Except your company wasn't updating its records and didn't send the email, and now John's checking account has been emptied. The same story can play out via SMS and on social media, with criminals preying on unsuspecting customers or employees disguised as your business, often using a sense of urgency to force people into taking action without thinking.

John and those like him are unlikely to think of your company as blameless in the matter. In fact, studies show that one in every three consumers exposed to a cyber attack or data breach see the brand as responsible for their damage and close their online account or end their business relationship with the organization. To be fair to them, they have a point. Without taking steps to detect and prevent such attacks, you're putting your customers and your business at risk.

A Digital Risk Protection service provides constant monitoring to detect external threats like these and takes steps to prevent them from damaging your brand. Combining advanced security technology and human expertise, they use intelligence to go beyond simply identifying brand references online but capturing data from across your organization's channels, as well as scouring the clear, deep, and dark web. With immediate alerts when suspicious activity is detected, or leaked data is found, steps can be quickly taken to mitigate them and prevent lost revenue and reputational damage. The ideal service will provide continuous monitoring to detect phishing attacks, social media impersonation, and application impersonation, as well as takedown services to neutralize the threat before it can harm your business or your customers.

The importance of being proactive

While it's true that it's no longer a case of if you'll suffer a breach but when, that doesn't mean there's nothing you can do. With breaches taking 277 days on average to be detected, improving visibility and response time enables you to be far more proactive. You can detect threats earlier and squash them or, should you suffer a breach, limit their impact on business and clients. With the average cost of a data breach sitting at around $4.24 million[5], taking every possible step to avoid one or at least reduce the potential damage will be well worth your while. This is especially true as regulations tighten and fines rise. The General Data Protection Regulation (GDPR), for example, can levy penalties of up to 10 million euros or up to 2% of a company's entire global turnover, whichever is higher. Likewise, the California Consumer Privacy Act (CCPA) can punish a breached business with a civil penalty of up to $7,500, plus fines between $100 to $700 per consumer.

Security and savings

If your security resources are stretched already, deploying a managed service will help to free your teams from alert fatigue and focus on priority tasks, including patching the vulnerabilities that pose a risk in the first place. Taking steps of this nature also supports your business when it comes to your cyber insurance policies. By showing you've made appropriate moves to defend your organization and your customers, insurers will look on your efforts favorably, which can potentially save you money through reduced premiums and copays.

Possibly more important than anything else, however, is the peace of mind that managed detection and response, supply chain defense, and digital brand protection has to offer. Adding eyes, ears and defensive faculties to your technology stack enhances not only your protection and reputation but helps to reduce complexity and risk while freeing up internal resources. More than just being seen to be doing the right thing, in a world of heightened cyber threats combining these three essential services with your existing security tooling is the right thing to do for your business, your customers, and your ability to sleep well at night.

The Real Cost of a Breach: Target
The 2013 cyber attack on retailer Target affected more than 41 million customer payment card accounts. Hackers compromised a third-party Target vendor using a phishing email to install malware and access login credentials. The company was required to pay an $18.5 million USD settlement.[6]

The Real Cost of a Breach: Equifax
In 2017, an unpatched Equifax credit agency database framework led to the personal and financial information of almost 150 million people being compromised. The company paid a settlement of $575 million with the potential for it to increase to $700 million.[7]

The Real Cost of a Breach: T-Mobile
In 2021, mobile communications firm T-Mobile failed to prevent unauthorized access to its systems, resulting in data linked to an estimated 77 million people being sold online. A class-action lawsuit demanded $350 million while the company also committed to investing $150 million in security technology.[8]

Protect your business with rock-solid cyber defense services

As you can see, cyber threats to organizations and their customers in today's interconnected business world are many. Companies like yours are aware of the growing risk and will likely have taken steps to combat them through security tooling. Despite these efforts, however, complexity and a lack of available resources, not to mention the frequent emergence of new and evolving threats, make protection an ongoing challenge. It's for that reason that we've partnered with BlueVoyant to provide you with rock-solid cyber defense solutions. With a robust platform and unparalleled expertise in today's leading security technologies, BlueVoyant enables you to elevate your security posture by leveraging the security tools you already have. With Core: MDR, Terrain: SCD, and Sky: DRP, BlueVoyant enhances threat visibility and provides proactive countermeasures while freeing internal teams to focus on more tactical projects. By partnering with BlueVoyant, we offer an end-to-end portfolio of security services from consulting and deployment support to 24×7 detection, response to, and eradication of threats in your environment. All of which means you don't need to be an expert to take your security and compliance posture to the next level.

Sources

1 Cybersecurity solutions for a riskier world. ThoughtLab. (2022, July 19). Retrieved August 26, 2022, from https://thoughtlabgroup.com/cyber-solutions-riskier-world/

2 40 worrisome hacking statistics that concern us all in 2022. WebTribunal. (n.d.). Retrieved August 26, 2022, from https://webtribunal.net/blog/hacking-statistics/#gref

3 Slandau. (2022, April 5). Phishing attack statistics 2022. CyberTalk. Retrieved August 26, 2022, from https://www.cybertalk.org/2022/03/30/top-15-phishing-attack-statistics-and-they-might-scare-you/

4 Jr., T. H. (2022, February 27). These are the 20 most common passwords leaked on the dark web - make sure none of them are yours. CNBC. Retrieved August 26, 2022, from https://www.cnbc.com/2022/02/27/most-common-passwords-hackers-leak-on-the-dark-web-lookout-report.html

5 Cost of a data breach report 2021. IBM. (2021, July). Retrieved May 23, 2022, from https://www.ibm.com/security/data-breach

6 McCoy, K. (2017, May 23). Target to pay $18.5M for 2013 data breach that affected 41 million consumers. USA Today. Retrieved August 26, 2022, from https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/

7 (2021, September 18). Equifax to pay $575 million as part of settlement with FTC, CFPB, and states related to 2017 data breach. Federal Trade Commission. Retrieved August 26, 2022, from https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach

8 T-mobile shares updated information regarding ongoing investigation ... (n.d.). Retrieved August 26, 2022, from https://www.t-mobile.com/news/network/additional-information-regarding-2021-cyberattack-investigation

Rock-solid cyber defense you can trust

FSJ Solutions
CONTENT - PROCESS - ANALYTICS - CLOUD SECURITY

BlueVoyant

Contact us today to learn how we can serve your security needs.

Frederik Søndergaard-Jensen
frederik@fsjsolutions.dk
(+45) 2684 3666