CYFOR SECURE
CYBER SECURITY

Safe Guard your business. Learn the latest threats and tips for protection and resilience.

Mitigating Emerging Cyber Security Risks: A Comprehensive Guide for Businesses

Mitigating Emerging Cyber Security Risks: A Comprehensive Guide for Businesses

Table of Contents:

Introduction

Overview of the Current Cyber Security Threat Landscape

A recent report by the Enterprise Strategy Group (ESG) and TechTarget found that 54% of cyber security professionals believe the impact of the skills shortage on their organisations has worsened over the past two years. With the advent of AI, cyber criminals have found it easier to enhance their operations and launch more sophisticated attacks. This makes it essential for cyber security experts and SMEs to ensure that all employees are equipped to recognise and respond to these threats effectively.

A global survey conducted by CommVault, which included 1,000 cyber security and IT leaders, revealed that 83% of respondents had experienced a significant security breach. More than half of these breaches occurred within the past year, and over 75% were reported within the last 18 months. [1] Cyber-crime is gaining momentum, making it crucial for everyone to be aware of potential threats and understand how to protect their data. Identifying vulnerabilities, reducing risks, and increasing cyber resilience have never been more important.

Purpose of This Guide

This guide aims to provide a clear understanding of how to identify and protect against online threats. It includes practical tips and software recommendations to help counteract cyber-attacks.

Key Topics Covered in This Guide

- Exploitation of Third-Party Relationships (Or data process attacks if you're familiar with the GDPR): Understanding these risks and steps to protect your data.
- Generative AI in Social Engineering and Information Warfare: How cyber criminals use AI to enhance their attacks, and how it can also be leveraged to strengthen defences.
- Under-the-Radar Attacks by Initial Access Brokers (IABs): What these attacks involve and how to defend against them.
- Big-Game Hunting: Understanding this type of attack and strategies to improve your cyber resilience if targeted.

This guide will focus on identifying threats related to the four key areas mentioned above and providing steps to protect your data. Additionally, it will offer tips on how to recover and strengthen your cyber resilience in the event of an attack.

[1] [1] Commvault - English - United States. (2024). 2024 Cyber Recovery Readiness Report. [online] Available at: https://www.commvault.com/resources/analyst-report/2024-cyber-recovery-readiness-report.

Exploitation of Third-Party Relationships

Overview

Working with third-party vendors can expose organisations to various risks, primarily because these vendors often have access to sensitive data, systems, or infrastructure. It's essential to understand what these vendors can access, take steps to select secure data processors, and clearly define the security responsibilities of both parties. Threat attacks are specifically targeting organisations like the NSP or Data storage providers. These attacks offer threat actors more leverage, as its imperative the providers recover quickly, due to things like contractual agreements.

Risks posed through third parties come in many forms, from IT Supplier's having cyber incidents, such as the CTS incident from 2023, to vulnerable software libraries. Threat actors know that they can cause damage to a large number of businesses through one incident or vulnerability, and increase their odds of a successful ransom demand, through such incidents. The lack of shared responsibility between third parties and visibility over software supply chains introduces a variety of vulnerabilities. Further, the complexity of software dependencies and shared libraries makes it difficult for businesses to track which software their suppliers use. Companies often lack the resources to thoroughly audit every software package and dependency within their systems, leading to heavy reliance on third-party vendors for timely updates and patches. This dependency creates additional risk, as businesses must trust vendors to address vulnerabilities before they can be exploited.

Being aware of these risks allows organisations to implement robust security strategies.

Risks

- Data Breaches: Third-party vendors often handle sensitive data like customer information and financial records. If their security is inadequate, they can be an entry point for attackers, leading to data theft or compromise.
- Supply Chain Attacks: Attackers may target a vendor's systems to access client data or systems, as seen in cases like SolarWinds and Log4j, where vulnerabilities in vendor software exposed organisations globally.
- Operational Disruption: Cyber-attacks or downtime affecting vendors can halt essential services, disrupting business operations, such as when ransomware impacts production or access to critical services.
- Regulatory Compliance Risks: Organisations must ensure vendors comply with standards like GDPR or HIPAA. Non-compliance by a vendor can lead to legal and financial repercussions for both parties, and many regulations require audits or testing to secure the supply chain.
- Financial Risks: Incidents involving vendors can incur costs for response, recovery, and legal actions, along with reputational damage that may result in lost business opportunities.
- Intellectual Property Theft: Compromised vendors may expose proprietary information, allowing attackers to steal intellectual property.

- Insider Threats: Vendor employees or contractors may misuse or accidentally expose sensitive information, creating potential insider threats.
- Vendor Management Risks: Managing multiple vendors can be challenging, with potential security gaps and risks from ineffective monitoring or assessment.

Mitigation and Avoidance

In a recent interview with Help Net Security, Ismael Valenzuela, Vice President of Threat Research & Intelligence at BlackBerry, shared strategies for securing supply chains against cyber-attacks: [2]

- Layered Defense Approach: Utilise multiple defensive mechanisms to protect against cyber-attacks.
- Secure Code Review: Regularly review code to identify and address vulnerabilities.
- Digital Certificate Signing and Review: Ensure the authenticity and security of software components.
- Product Security Incident Response Team (PSIRT): Establish a dedicated team to handle security incidents.
- Threat Intelligence Integration: Enhance defensive measures by integrating up-to-date threat intelligence.
- Access to Up-to-Date Threat Intelligence: Gain insights into cyber-criminal activities, including tactics, techniques, and procedures (TTPs).
- Early Warning System: Implement systems to identify and prepare for potential threats to the supply chain.
- Deep-Web Monitoring: Gather intelligence on vulnerabilities and initial access brokers (IABs) related to the supply chain.
- Vulnerability Flagging: Identify risks within third-party and open-source software often used in supply chain networks.
- Mitigation of Supply Chain Vulnerabilities: Proactively identify and address weaknesses using threat intelligence to strengthen defenses and reduce attack risks.

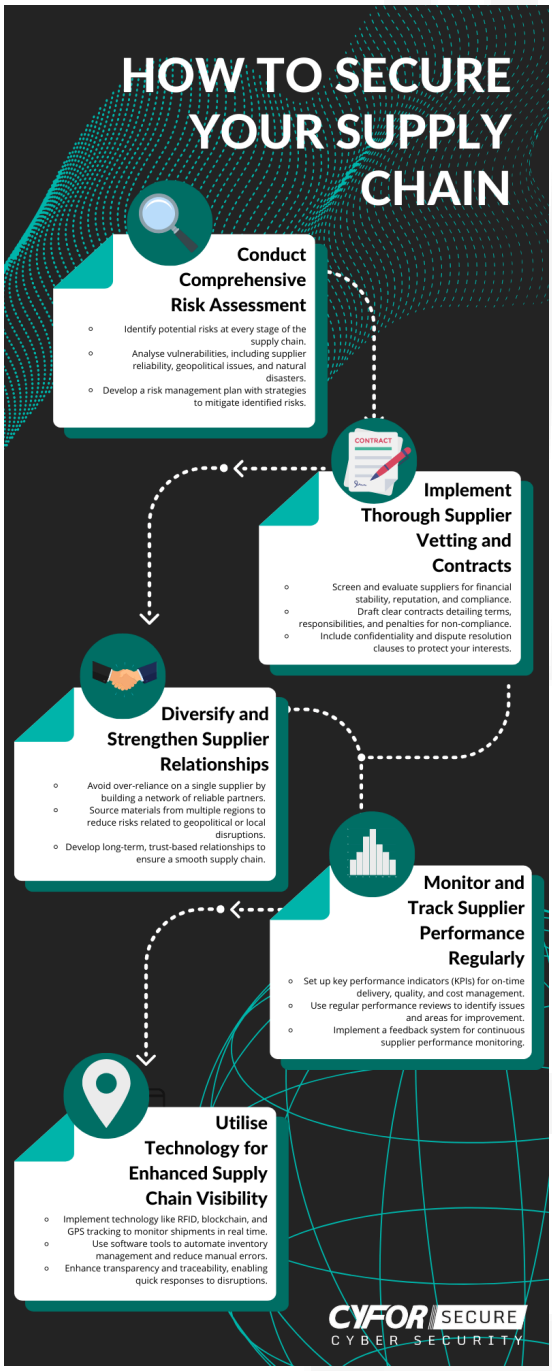
CYFORSecure's Recommended Mitigation Strategies:

- Conduct Due Diligence: Thoroughly evaluate the security posture of third-party vendors before engagement.
- Regular Audits: Continuously audit and monitor vendors' security practices to ensure ongoing compliance.
- Clear Contracts: Define security responsibilities, data handling requirements, and compliance obligations in vendor contracts. Shared responsibility models- amazon web services, makes it clear what each vendor is responsible for.

[2] Mirko Zorz (2024). How nation-states exploit political instability to launch cyber operations - Help Net Security. [online] Help Net Security. Available at: https://www.helpnetsecurity.com/2024/10/15/ismael-valenzuela-blackberry-political-instability-cyber-operations/ [Accessed 24 Oct. 2024].

- Incident Response Planning: Develop a comprehensive incident response plan that includes protocols for handling third-party vendor incidents, ensuring swift action in case of breaches or attacks. For example, last December's CTS incident—a major IT provider hit by ransomware—left many clients without access to their systems, virtual desktops, and data. CTS were unprepared to manage the fallout, underscoring the importance of diversifying IT vendors and having a clear, actionable plan for when a third-party vendor faces an incident. This approach helps mitigate risk and ensure continuity if one vendor is compromised.
- Access Control: Limit vendor access to sensitive systems and data, ensuring permissions align with the "principle of least privilege."

By being vigilant and implementing these strategies, organisations can minimise the risks associated with third-party vendors and safeguard their sensitive information and operations.



Use of Generative AI in Social Engineering and Information Warfare

Overview

AI plays a significant role in cyber security by detecting threats, analysing incidents, and identifying vulnerabilities through pattern recognition and automation. However, it also introduces risks, as cyber-criminals can exploit AI to develop sophisticated malware and phishing scams. Additionally, data entered into AI systems like ChatGPT may be vulnerable to leaks if not managed properly.

According to Will Poole, Technical Director at CYFORSecure, one of the most common attacks the team encounters is phishing scams, which are easily created and amplified using generative AI. A study by Teleport, which surveyed 250 senior decision-makers in the US and UK, found that social engineering remains a top tactic for cyber-criminals to install malware and steal sensitive data. Further, among respondents, 52% identified AI impersonation as the most challenging attack vector to defend against. Ev Kontsevoy, CEO of Teleport, noted that "AI-generated impersonation is challenging to defend against... AI and deepfake tools have made phishing campaigns more efficient, reducing the time and cost to launch them, enabling even less skilled individuals to conduct numerous attacks easily." [3] Commvault's survey also highlighted that the use of AI by cyber-criminals is one of the biggest challenges organisations and experts are currently facing.

[4]

Risks

There are several types of AI generated attacks to be aware of:

- Email Phishing: Sending deceptive emails to trick recipients into sharing sensitive information.
- Spear Phishing: Targeting specific individuals with personalised, convincing messages. Currently, generative AI is being used predominantly in this area.
- Whaling: Aimed at high-profile targets like executives, using tailored tactics.

[3] Help Net Security (2024). AI and deepfakes fuel phishing scams, making detection harder - Help Net Security. [online] Help Net Security. Available at: https://www.helpnetsecurity.com/2024/10/24/ai-impersonation-cyberattack-vector/ [Accessed 24 Oct. 2024].
4] Commvault - English - United States. (2024). 2024 Cyber Recovery Readiness Report. [online] Available at: https://www.commvault.com/resources/analyst-report/2024-cyber-recovery-readiness-report.

- Smishing: Phishing through SMS or text messages- Less prevalent nowadays, but we still see these – primarily to target individuals rather than organisations.
- Vishing: Voice-based phishing where attackers impersonate trusted entities over the phone.
- Clone Phishing: Replicating legitimate messages but altering links to direct recipients to malicious sites.
- Angler Phishing: Using fake customer service accounts on social media to steal information. [5]

SEO Poisoning- SEO poisoning is a cyber-attack where hackers manipulate search results to rank malicious sites highly. These sites appear legitimate, but contain malware, phishing schemes, or fake pages that steal data. These often come in the form of commonly searched for documents (e.g., “CV Templates” or “Contract Template”) but, rather than leading to the download of a legitimate PDF, download malicious software which compromises a user’s devices. Users unknowingly click on these links, leading to potential infections or data theft.

Attackers are increasingly shifting to identity-based attacks, using sophisticated phishing techniques and compromised credentials. Will Poole (Technical Director, CYFORSecure) notes a rise in multi-stage phishing attacks, replacing the simpler, single-stage scams of the past. The team often encounters a phenomenon they call “Friday Fraud,” where phishing attacks are timed for Fridays to allow threat actors to intercept upcoming payments – especially in the conveyancing industry.

Unlike traditional scattershot phishing, attackers now use a targeted approach: they initiate contact by requesting service information or a quote and only introduce a malicious link when documentation is exchanged. By this stage, the victim’s guard is down, making them more likely to click the link. AI is increasingly used to automate these sophisticated email interactions, with the trend gradually expanding to voice phishing (vishing) and generative AI attacks to mimic trusted contacts.

Effective defenses involve reducing human error, monitoring or blocking suspicious logins (e.g., from unusual locations or VPN services) enhancing knowledge on AI safety within organisations[6], implementing least privileged access, and establishing robust identity governance and policy management.

To mitigate these risks, users should avoid sharing sensitive information, ensure secure connections, and implement strong cyber security measures such as firewalls and multi-factor authentication (MFA). However, CYFOR Secure’s Technical Director, Will Poole, highlighted a caveat to MFA: tools like "EvilGinx," encountered frequently in incident responses, are undermining MFA's effectiveness in protecting Microsoft 365 and email environments by compromising MFA codes and session tokens. Microsoft has introduced guidance called "Token Protection in Conditional Access," which provides policies and steps to guard against session token hijacking—a technique now prevalent in sophisticated phishing attacks.

[5] www.metacompliance.com. (2023). The Dark Side: How AI Enables Sophisticated Phishing Attacks. [online] Available at: https://www.metacompliance.com/blog/phishing-and-ransomware/how-ai-enables-sophisticated-phishing-attacks.
6] Malwarebytes. (n.d.). What is ChatGPT? ChatGPT Security Risks | AI Chatbots. [online] Available at: https://www.malwarebytes.com/cybersecurity/basics/chatgpt-ai-security

Mitigation Strategies

- Employee Training: Conduct regular training sessions to equip staff to recognise AI-generated threats. While many companies already offer phishing training, it's crucial to update these programs to address evolving tactics. Modern threats require employees to verify they're on legitimate pages, like Microsoft 365, and go beyond traditional signs of phishing. With generative AI making emails look highly convincing, old indicators are no longer so reliable. Training should focus on validating email sources and understanding new tactics, ensuring employees stay prepared for increasingly sophisticated attacks.
- AI Detection Tools: Implement tools capable of identifying and filtering AI-generated content. These tools analyse content to detect AI generation, and we can anticipate their integration into email filtering systems in the future. While their accuracy is still being evaluated, cyber security professionals and data protection officers (DPO's) should monitor these developments closely.
- Regular Updates: Stay informed on the latest advancements in generative AI and its potential misuse by consulting with cyber-security experts to identify any security gaps. Ensure employee training is updated consistently, to keep pace with emerging threats.
- Staying Alert: While new threats may arise, fundamental safety practices remain essential. Always verify the sender addresses of emails, validate URLs, and confirm details directly before proceeding with financial transactions, even in the face of newly emerging threats.

By understanding and preparing for the potential risks associated with generative AI, organisations can strengthen their defences against increasingly sophisticated social engineering tactics.

Under-the-radar attacks, conducted by Initial Access Brokers

Overview

Cyber-crime is becoming increasingly organised, with large-scale, multi-layered operations that resemble legitimate businesses. These operations often rely on Initial Access Brokers (IABs), specialised threat actors who infiltrate networks, systems, or organisations and sell unauthorised access to other cyber-criminals, such as ransomware groups. These IABs and 'affiliate models' are becoming more prominent currently. They can remain undetected for months or even years, waiting for the right opportunity to sell access, thus streamlining the process for ransomware operators, such as Akira, by handling the initial breach.

The CYFORSecure team recently handled an incident where initial access occurred at the end of May, but no malicious activity surfaced until three months later. The team believes this delay was due to a different criminal group gaining initial access than the one that eventually deployed the ransomware. The first group accessed the system by installing AnyDesk on a server, leaving it in place for eventual sale on the dark web. The second group purchased the access keys, logged into AnyDesk's remote control, and proceeded with their typical attack strategy.

According to Cyberint's research over the past 18 months, IABs frequently target the business services sector, aligning with broader ransomware trends. The retail industry remained a consistent target throughout 2023 and 2024, while the manufacturing sector saw a notable increase in attacks, rising from 14% in 2023 to 23% in 2024. [7]

[8]

[7] Adi Bleih (2024). A Deep-Dive Into Initial Access Brokers: Trends, Statistics, Tactics and more. [online] Cyberint. Available at: https://cyberint.com/blog/research/a-deep-dive-into-initial-access-brokers-trends-statistics-tactics-and-more/.
8] Adi Bleih (2024). A Deep-Dive Into Initial Access Brokers: Trends, Statistics, Tactics and more. [online] Cyberint. Available at: https://cyberint.com/blog/research/a-deep-dive-into-initial-access-brokers-trends-statistics-tactics-and-more/

In 2023, the majority of ransomware attacks facilitated by IABs involved compromised servers via exposed Remote Desktop Protocol (RDP), accounting for over 60% of cases. By 2024, VPN access surged, challenging RDP as the primary method (45% VPN vs. 41% RDP).

IAB's:

The three main types of Initial Access Brokers are:

1. Backdoored Systems Brokers: Sell access to computers infected with malware, often within corporate networks.
2. Credential Access Brokers: Provide access to servers compromised through brute-force attacks on weak credentials.
3. Network Device Brokers: Exploit vulnerabilities in devices like VPN servers and firewalls to offer internal network access.

IAB activities are highly lucrative, with access listings typically ranging from $500 to $2,000, though high-value listings can exceed $10,000. However, these actors are not commonly looking for inventive ways to access your system. They're looking for quick access, hitting as many organisations as possible to increase their chance of a payday, rather than crafting bespoke or technically complex attacks.

Risks

Phishing Campaigns:

- Malicious emails designed to deliver malware, which, once clicked, grant attackers' access to the company's network and servers.

Vulnerable external internet facing services:

- RDP Access: Allows remote control of a compromised computer or server.
- VPN Access: Allows Threat Actors to connect to a network by imitating legitimate remote access. This often involves using leaked or outdated credentials to perform credential-stuffing or brute-force attacks through the VPN, potentially gaining direct access to databases via credential theft or exploiting vulnerabilities.
- Outdated Firewall: IAB's could use remote vulnerabilities on outdated firewalls to launch attacks: Fortinet have mentioned quite a few in the past weeks.
- Web Shell Access: Scripts that permit remote administration of web servers.
- Shell/Command-Line Access: Provides command-line interface control over systems. Often achieved via "remote code execution" vulnerabilities on outdated firewalls or other internet facing systems.
- File Share Access: Access to shared drives and file servers, typically via compromised credentials. [9]

Research from Cyberint found that IABs often advertise the level of antivirus (AV) software on compromised machines. Alarmingly, it was discovered that 40% of these machines had no AV software mentioned, and over 60% relied solely on Windows Defender – which is often, and easily, disabled by threat actors during incidents. This indicates a lack of stronger security measures, making these systems easier targets for attackers. [10]

- [9] Adi Bleih (2024). A Deep-Dive Into Initial Access Brokers: Trends, Statistics, Tactics and more. [online] Cyberint. Available at: https://cyberint.com/blog/research/a-deep-dive-into-initial-access-brokers-trends-statistics-tactics-and-more/
- [10] Adi Bleih (2024). A Deep-Dive Into Initial Access Brokers: Trends, Statistics, Tactics and more. [online] Cyberint. Available at: https://cyberint.com/blog/research/a-deep-dive-into-initial-access-brokers-trends-statistics-tactics-and-more/

One advantage of an initial access attack is that threat actors often remain undetected for extended periods, giving organisations time to identify the breach before significant damage occurs. However, this requires effective detection software, monitoring systems, and regular review of system logs to catch any suspicious activity early.

Mitigation and Avoidance Strategies

- Patch Management: Regularly update all systems to address critical vulnerabilities—from endpoints and servers to firewalls. An outdated firewall, especially one with remote command execution vulnerabilities, poses a significant risk if left unpatched. Defence in depth and internal monitoring are key to detect and prevent incidents, but your external perimeter can prevent incidents before they begin. Threat actors need to breach this perimeter first, and if they succeed, they gain a foothold in your network for potential attacks. Begin by securing your perimeter and work inward, ensuring a robust patching strategy throughout.
- Endpoint Security: Protect all endpoints with strong security solutions, such as SentinelOne. Don't relay on last generation Anti-Virus systems. Ensure all alerts generated by your endpoint systems are monitored and actioned – just because a threat was quarantined, doesn't mean you don't need to know how it got there!
- Incident Response Plan: Develop a comprehensive response plan to quickly address attacks and prevent escalation into serious threats like ransomware. It's crucial to log and handle incidents thoroughly; the CYFORSecure team has encountered cases where malware incidents were initially detected and quarantined by antivirus software but later revealed broader vulnerabilities. Investigating how the malware entered, how attackers moved laterally through the system, and the malware's intended actions helps determine if there's a larger threat at play.
- Log Reviews: Actively monitor and review logs generated by security systems. Logs often alert to potential attacks, but they must be monitored to respond effectively before damage occurs.

The majority of ransomware attacks stem from social engineering (like phishing emails) or exploiting vulnerabilities in internet-facing services (such as VPNs and firewalls). Reduce exposure by securing remote access with multi-factor authentication, strong passwords, and email protection. Understanding the role of Initial Access Brokers (IABs) and implementing these measures can protect networks from covert attacks, deterring IABs from targeting your organisation and preventing over 90% of incidents.

Big Game Hunting (BGH) Ransomware Incidents

Overview

Big Game Hunting (BGH) ransomware attacks are on the rise, with increasing sophistication that poses serious concerns for companies and governments. BGH attacks specifically target large organisations that are more likely to pay ransoms to avoid reputational damage or financial loss. Many victims hesitate to report such incidents, fearing exposure or regulatory action, especially in the UK, where personal data breaches must be reported to the Information Commissioner's Office (ICO) within 72 hours. Support for victims is often limited, primarily coming from private firms or insurance.[11]

The UK has seen a significant increase in ransomware incidents, doubling from 326 in 2020 to 654 in 2021. Sectors like healthcare and utilities are particularly vulnerable due to the potential for operational disruption. The COVID-19 pandemic further increased remote work vulnerabilities, leading to a surge in attacks.[12] Will Poole (Technical Director at CYFORSecure) commented that the main two reasons for this surge are:

1. The financial rewards for ransomware groups can be extremely lucrative, especially when targeting third party suppliers/vendors.
2. The capabilities of these threat groups- These originations will work with affiliates, to launch far more sophisticated attacks.

How Do BGH Attacks Work?

Once attackers gain access to a network, they move laterally to take control of critical systems and steal sensitive data. They may use this data as leverage, threatening to release it if the ransom isn't paid—a tactic known as double extortion. When ready, they deploy ransomware across the network, encrypting files simultaneously to maximise disruption while avoiding detection until the attack is fully executed.
An example of this kind of attack occurred in 2020, when Garmin was hit by WastedLocker ransomware. The attack shut down the company's services globally, affecting aviation and fitness tracking. Reports suggest that Garmin paid a multimillion-dollar ransom to regain control of its systems.

Given the complexity and adaptability of these attacks, no single security solution is foolproof. Effective defence requires multiple layers of security, ensuring that if one barrier is breached, others can provide backup and prevent a total compromise.

[11] Chance LLP and FTI Consulting LLP (2021). Ransomware Threats: Analysis, UK Victim Experience, and Resilience. [online] Parliament.uk. Available at: https://committees.parliament.uk/writtenevidence/114499/html/ [Accessed 24 Oct. 2024]
[12] Crowdstrike.com. (2024). What is Cyber Big Game Hunting? | CrowdStrike. [online] Available at: https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/big-game-hunting/

Risks

According to a study by CrowdStrike, cyber-criminals increasingly use Ransomware-as-a-Service (RaaS), a model that allows attackers to lease ransomware, similar to how software-as-a-service (SaaS) operates. This has broadened the distribution of ransomware, with notable RaaS platforms linked to major cyber-crime groups. Attackers also exploit cloud vulnerabilities and zero-day flaws, using known software weaknesses to gain initial access. These tactics enable broader attacks, making detection more challenging and posing significant security risks. The table below details the RaaS, techniques and the associate BGH.

RaaS	Technique	Big Game Hunter
DarkSide	DarkSide operators traditionally focus on Windows machines and have recently expanded to Linux, targeting enterprise environments running unpatched VMware ESXi hypervisors or stealing vCenter credentials. DarkSide RaaS is also believed to be the attack vehicle leveraged in the high-profile Colonial Pipeline attack.	CARBON SPIDER
REvil (also known as Sodinokibi	REvil is a RaaS most commonly used by PINCHY SPIDER. In such attacks, victims usually receive a warning of an impending data leak if a ransom is not paid. REvil is credited with being the ransomware behind one of the largest ransom demands on record: $10 million USD.	**PINCHY SPIDER**
Dharma	Dharma ransomware attacks are mainly associated with remote desktop protocol (RDP) attacks. Dharma variants come from many sources and are nearly identical in nature, making it difficult to ascertain who is behind an attack.	Linked to a financially motivated Iranian threat group Not centrally controlled
LockBit	In development since 2019, LockBit attacks demand a ransom to avoid the publication of a stolen data set. The RaaS is confirmed to have been involved in at least nine attacks.	Affiliated with Russian-speaking users or English speakers with a Russian-speaking guarantor

[13]

Mitigation & Avoidance

- Backup and Recovery Plans: Regularly back up data across multiple locations, ensuring at least one copy is offline. Frequently test recovery processes to confirm that backups are secure from potential deletion by malicious actors. Ensure backups remain disconnected from the live network, with one offline copy for added protection
- Zero-Trust Architecture: Limit internal movement by implementing a zero-trust model that continuously verifies user and device activity.
- Threat Intelligence: Use real-time threat intelligence to detect and mitigate risks early.
- Employee Training: Educate staff on cyber security best practices, including strong password management, secure Wi-Fi usage, and avoiding suspicious links.
- Regular Updates: Consistently patch and update software to minimise vulnerabilities.
- Email Security: Implement URL filtering, attachment sandboxing, and automated responses to detect and prevent email threats.
- Continuous Monitoring: Deploy endpoint detection and response (EDR) tools to maintain visibility and catch anomalies.
- Identity Protection: Utilise identity management systems to monitor account behaviour and enforce strict access controls.

By implementing these strategies, organisations can strengthen their defences against BGH ransomware, reducing the risk of attacks and mitigating their impact when they do occur.

[13] Crowdstrike.com. (2024). What is Cyber Big Game Hunting? | CrowdStrike. [online] Available at: https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/big-game-hunting/

Cyber Resilience

Overview

Cyber resilience ensures that your company can continue business operations even during a cyber-attack. However, many organisations are slow to implement these protocols due to several factors. According to a CommVault survey, cost and complexity are key reasons why companies hesitate to invest in and develop robust cyber resilience strategies.
The financial and reputational impact of a cyber breach can be significant. Therefore, implementing strong cyber resilience measures is essential to ensure your operations can continue smoothly, even in the face of an attack.

[14]

Resilience Strategies

- Early Warning Tools: Deploy technologies like Intrusion Detection Systems, Deception Technology, and Endpoint Detection and Response to identify risks, including insider threats, at an early stage. SentinalOne is a key system to install.
- Secondary Clean Environment: Maintain an isolated recovery system (e.g., a cleanroom) to preserve business continuity and data integrity if the primary site is compromised.
- Immutable Data Storage: Use air-gapped systems to store unchangeable data copies, safeguarding against ransomware and insider threats.
- Incident Response Preparedness: Establish clear runbooks, roles, and processes to ensure efficient incident handling and faster recovery.
- Cyber Recovery Readiness: Regularly test and measure recovery capabilities to identify and address potential vulnerabilities.[15]

[14] Commvault - English - United States. (2024). 2024 Cyber Recovery Readiness Report. [online] Available at: https://www.commvault.com/resources/analyst-report/2024-cyber-recovery-readiness-report.
[15] Commvault - English - United States. (2024). 2024 Cyber Recovery Readiness Report. [online] Available at: https://www.commvault.com/resources/analyst-report/2024-cyber-recovery-readiness-report.

Conclusion

Recap of Key Points

The evolving cyber security landscape presents increasing challenges, particularly with the rise of AI-enhanced attacks and the growing sophistication of cyber-criminal operations. A report from the Enterprise Strategy Group (ESG) and TechTarget highlighted that 54% of cyber security professionals have seen the impact of the skills shortage worsen over the past two years. This, coupled with the accessibility of AI for malicious purposes, emphasises the need for SMEs and cyber security experts to ensure employees are well-prepared to identify and respond to potential threats.

Global surveys, such as the one conducted by CommVault with 1,000 cyber security and IT leaders, reveal the growing prevalence of security breaches, with 83% of respondents reporting incidents, over half of which occurred within the past year. The threat landscape continues to expand, making it more important than ever to understand potential risks, identify vulnerabilities, and strengthen cyber resilience.

This guide has covered these key areas:

- Exploitation of Third-Party Relationships: Understanding the risks involved and strategies to protect sensitive data. Implement Shared Responsibility Models: AWS have great examples of Shared Responsibility Models.
- Use of Generative AI in Social Engineering and Information Warfare: How AI can be exploited by attackers and how it can also be used defensively: Update your awareness of phishing attacks.
- Under-the-Radar Attacks by Initial Access Brokers (IABs): Recognising these threats and implementing measures to mitigate them.
- Big-Game Hunting (BGH) Ransomware: Understanding BGH tactics and enhancing cyber resilience to defend against these complex attacks.

Encouragement to Implement Strategies for Better Security

As cyber threats are become more sophisticated and widespread, taking preventive measures is not just advisable—it's essential. By proactively identifying vulnerabilities and implementing robust security strategies, organisations can protect their assets, reputation, and operations. Following best practices like layered security defences, regular training, and vigilant monitoring can significantly reduce the risk of a successful attack.

NIST Cyber security Framework is a very American framework, focusing on the five core functions: Identify, Protect, Detect, Respond, and Recover. However, it’s something more and more organisations are adopting. NIST has very strict guidance, and a great resource to tap into.

We encourage all organisations, regardless of size, to invest in cyber security measures, educate their teams on recognising threats, and adopt a mindset of continuous improvement. Implementing the strategies discussed in this guide can help build a resilient defence against the growing range of cyber threats, ensuring business continuity and long-term security.

About CyforSecure

Brief overview of CyforSecure’s expertise in cyber security solutions.

CYFORSecure specialises in providing comprehensive cyber security solutions tailored to meet the needs of businesses across various sectors. With a focus on proactive threat management, the company offers services including threat detection and response, vulnerability assessments, and security audits. Their team of experts is dedicated to helping organisations safeguard their digital assets, mitigate risks, and enhance their overall cyber resilience. CYFORSecure employs cutting-edge technologies and industry best practices to deliver effective security strategies that protect against evolving cyber threats.

Contact Information for Further Assistance

For more information about CyforSecure's services or to get assistance, please visit CYFORSecure.com, or reach out via the following contact options:

Phone: +44 (0)161 797 8123

Email: enquiries@cyforsecure.co.uk

Address: CYFORSecure, Unit 5, Parkside Business Park, Clayton Street, Manchester, M11 4RQ, United Kingdom

CYFORSecure is committed to helping businesses enhance their cyber security posture and address their unique security needs.

Useful Resources and Software

Potential Exploitation of Third-Party Relationships

- Vendor Risk Management: OneTrust, RiskRecon, Prevalent
- SIEM: Splunk, IBM QRadar, LogRhythm
- Cloud Security Tools: AWS Security Hub, Microsoft Defender for Cloud
- Supply Chain Security: Sonatype Nexus, Veracode
- Network Security: Fortinet FortiGate, Palo Alto Networks

Use of Generative AI in Social Engineering and Information Warfare

- Email Security Solutions: Proofpoint, Mimecast
- AI Detection Tools: Darktrace, OpenAI Moderation
- Security Awareness and Training: KnowBe4, Cofense

Under-the-Radar Attacks Conducted by Initial Access Brokers

- Endpoint Protection: CrowdStrike Falcon, SentinelOne
- Vulnerability Scanning: Nessus, Qualys
- Intrusion Detection: Snort, Suricata
- MFA Solutions: Duo Security, Okta

Big-Game Hunting

- Backup and Recovery: Veeam, Acronis Cyber Protect, Carbonite
- Zero-Trust Architecture: Microsoft Azure AD, Zscaler Zero Trust Exchange
- Threat Intelligence Services: Recorded Future, Anomali
- Continuous Monitoring: SentinelOne, CrowdStrike Falcon
- Identity Protection: Microsoft Entra ID, Ping Identity

A Final Note...

Will Poole,
Technical Director
CYFORSecure:

“The most useful piece of advice we can always give is that almost all incidents start via either phishing or an exploitation of internet facing systems - so if businesses can protect against these two areas they are ahead of the game”

A bit about Will Poole:

Will brings over five years of experience in cyber incident response from the Information Commissioner’s Office. He specialises in identifying root causes, stopping malicious activity, and preventing future incidents for businesses of all sizes. With expertise in UKGDPR, NIS, ISO27001, and Cyber Essentials, Will ensures clients maintain top security and compliance standards throughout and beyond the incident lifecycle.

Authored by William Poole, Technical Director &
Anna Mason, Marketing Executive

Appendix:

Glossary of Key Terms:

- AI (Artificial Intelligence): The simulation of human intelligence processes by machines, especially computer systems. In cyber security, AI is used for detecting threats, analysing data, and automating responses.
- Big-Game Hunting (BGH) Ransomware: A type of ransomware attack that targets large organisations, often demanding significant ransoms by threatening to release sensitive data (double extortion).
- Cryptographically Authenticated Identities: Security technique using cryptographic methods to verify the authenticity of user identities, reducing the risk of impersonation attacks.
- Cyber Resilience: The ability of an organisation to continue operating during and after a cyber-attack by maintaining essential functions and recovering quickly.
- Data Breach: The unauthorised access, exposure, or theft of sensitive information, such as personal data or financial records.
- Deep-Web Monitoring: The practice of scanning the deep web, including dark web forums, to gather intelligence on vulnerabilities, threats, and malicious activities.
- Endpoint Detection and Response (EDR): Security solutions that monitor end-user devices (endpoints) to detect and respond to cyber threats.
- Exploitation: The act of using a vulnerability or weakness in a system to gain unauthorised access.
- Firewall: A security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
- Generative AI: A type of artificial intelligence that can generate new content, such as text, images, or sounds. It can be used maliciously for creating phishing scams and deepfakes.
- Initial Access Brokers (IABs): Cyber criminals who specialise in gaining unauthorised access to networks and then selling that access to other attackers, such as ransomware groups.
- Insider Threat: A security risk that originates from within the targeted organisation, often from employees or contractors who have access to sensitive data.
- Intrusion Detection System (IDS): A security solution that monitors network or system activities for malicious behaviour and policy violations.
- Layered Defence: A security strategy that uses multiple security measures to protect against threats, ensuring that if one layer fails, others are in place to provide defence.

Glossary of Key Terms:

- Least Privileged Access: A security principle that gives users only the access rights they need to perform their tasks, minimising the risk of unauthorised actions.
- Malware: Malicious software designed to damage, disrupt, or gain unauthorised access to computer systems. Types include viruses, worms, ransomware, and spyware.
- NIST Cyber Security Framework: A set of guidelines created by the National Institute of Standards and Technology to help organisations improve their cyber security practices. It includes five core functions: Identify, Protect, Detect, Respond, and Recover.
- Phishing: A method of social engineering where attackers deceive individuals into providing sensitive information, such as login credentials, by pretending to be a trustworthy entity.
- Ransomware: A type of malware that encrypts a victim's data, holding it hostage until a ransom is paid to the attacker.
- Ransomware-as-a-Service (RaaS): A business model where ransomware developers provide their software to affiliates, who then use it to carry out attacks. The profits are shared between the developers and affiliates.
- Remote Desktop Protocol (RDP): A protocol that allows users to connect to a computer remotely. Attackers often exploit weak RDP configurations to gain unauthorised access.
- Social Engineering: A tactic used by attackers to manipulate individuals into revealing confidential information or taking actions that compromise security.
- Supply Chain Attack: An attack where cyber criminals compromise a third-party vendor or supplier to gain access to the systems of that vendor's clients.
- Threat Intelligence: Information that helps organisations understand potential threats, including the tactics, techniques, and procedures (TTPs) used by attackers.
- Vulnerability: A weakness in a system, software, or network that can be exploited by attackers to gain unauthorised access or cause harm.
- Zero-Trust Architecture: A security model that assumes no user or device should be trusted by default, regardless of whether they are inside or outside the network. Access is only granted after verifying the user's identity and device.
- VPN (Virtual Private Network): A service that encrypts a user's internet traffic and hides their online identity by routing their connection through a secure server. It is often used to protect data when accessing public networks.
- Web Shell: A script that attackers install on a web server to gain remote access and control over the server.

Links to Additional Reading

- -https://www.commvault.com/resources/analyst-report/2024-cyber-recovery-readiness-report.
- -https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/big-game-hunting/
- -https://committees.parliament.uk/writtenevidence/114499/html/
- -https://cyberint.com/blog/research/a-deep-dive-into-initial-access-brokers-trends-statistics-tactics-and-more/
- -https://www.malwarebytes.com/cybersecurity/basics/chatgpt-ai-security
- -https://www.metacompliance.com/blog/phishing-and-ransomware/how-ai-enables-sophisticated-phishing-attacks.
- -https://www.metacompliance.com/blog/phishing-and-ransomware/how-ai-enables-sophisticated-phishing-attacks.
- -https://www.commvault.com/resources/analyst-report/2024-cyber-recovery-readiness-report.
- -https://www.helpnetsecurity.com/2024/10/24/ai-impersonation-cyberattack-vector/
- -https://www.helpnetsecurity.com/2024/10/15/ismael-valenzuela-blackberry-political-instability-cyber-operations/
- -https://www.commvault.com/resources/analyst-report/2024-cyber-recovery-readiness-report.