CYFOR SECURE
CYBER SECURITY

MITIGATING EMERGING CYBER SECURITY RISKS

IN CYBER SECURITY

A Comprehensive Guide for Businesses

Presented by: William Poole,
Technical Director, CYFORSecure
Date: 25/10/2024

CYFOR SECURE
CYBER SECURITY

INTRODUCTION

Overview of the increasing cyber threats:
The cyber threat landscape is escalating with risks like third-party exploitation, AI-driven phishing, stealthy access brokers, and rising ransomware attacks, making robust security and vigilance essential for businesses.

Importance of Proactive Security

Proactive security measures are crucial to stay ahead of these evolving threats. Businesses must adopt layered defenses, regularly update systems, and train employees to recognize and respond to emerging risks.

Purpose of This Webinar

To educate businesses on identifying and mitigating the latest cyber threats, equipping them with strategies to protect their data, operations, and reputation in a dynamic threat environment.

CYFOR SECURE
CYBER SECURITY

CURRENT CYBER SECURITY THREAT LANDSCAPE

- **Rising Cyber-Attacks**: A global survey revealed that 83% of organisations experienced significant security breaches, with over half occurring in the past year. Cyber crime is escalating, driven by sophisticated attack methods and increased digital vulnerabilities.

- **Impact of AI and Skills Shortage**: AI is being leveraged by cyber criminals to automate and enhance attacks, such as phishing and deepfakes. Meanwhile, 54% of cyber security professionals report that the skills shortage has worsened, leaving organisations less equipped to respond to these evolving threats.

- **Importance of Employee Awareness and Training:** With the growing complexity of cyber-attacks, educating employees to recognise and respond to threats is critical. Regular training ensures staff can identify phishing scams, suspicious activities, and follow security protocols, reducing the risk of breaches.

CYFOR SECURE
CYBER SECURITY

KEY CYBER SECURITY RISKS COVERED

EXPLOITATION OF THIRD-PARTY RELATIONSHIPS:

Cyber criminals target vulnerabilities in third-party vendors to gain access to sensitive data and systems, leading to supply chain attacks and operational disruptions.

USE OF GENERATIVE AI IN SOCIAL ENGINEERING

AI is used to create more convincing phishing scams, deepfakes, and impersonations, making social engineering attacks harder to detect and increasing their effectiveness.

UNDER-THE-RADAR ATTACKS BY INITIAL ACCESS BROKERS (IABS)

IABs infiltrate networks and sell unauthorised access to other attackers, such as ransomware groups, often staying hidden for extended periods, making early detection challenging.

BIG-GAME HUNTING (BGH) RANSOMWARE

Targeting large organisations, BGH attacks involve double extortion, where attackers threaten to release stolen data if the ransom is not paid, leading to significant financial and reputational damage.

CYFOR SECURE
CYBER SECURITY

EXPLOITATION OF THIRD-PARTY RELATIONSHIPS

Overview:

Third-party vendors with access to sensitive data pose significant risks. If their security is compromised, it can lead to breaches, operational disruptions, and reputational damage.

Tactics:

01

DATA BREACHES:

Attackers exploit weak security measures at third-party vendors to steal sensitive information.

02

SUPPLY CHAIN ATTACKS:

Compromising vendor software or systems to gain unauthorised access to client networks.

03

REGULATORY COMPLIANCE RISKS

Non-compliant vendors can lead to legal and financial penalties for organisations.

CYFOR SECURE
CYBER SECURITY

Mitigation:

DUE DILIGENCE

Evaluate vendors' security posture before engagement.

REGULAR AUDITS

Continuously monitor and audit vendors to ensure compliance.

CLEAR CONTRACTS

Define security responsibilities and data handling protocols.

INCIDENT RESPONSE PLANNING

Develop robust plans that include vendor-specific scenarios to quickly address breaches.

CYFOR SECURE
CYBER SECURITY

USE OF GENERATIVE AI IN SOCIAL ENGINEERING

Overview:

AI has a dual role in cyber security, enhancing defenses but also enabling attackers to create more sophisticated and convincing attacks, making traditional security measures less effective.

Tactics:

01

PHISHING SCAMS

AI can automate and personalise phishing attacks, making them more convincing and difficult to detect.

02

IMPERSONATION ATTACKS:

Generative AI can create deepfakes and realistic impersonations, tricking individuals into revealing sensitive information or authorising fraudulent transactions.

CYFOR SECURE
CYBER SECURITY

EXAMPLES OF AI-BASED THREATS

Phishing Variants:

01

Spear Phishing

Targeted attacks using personalised information to trick specific individuals.

02

Vishing

Voice-based phishing, where attackers impersonate trusted entities over the phone.

03

Smishing

Phishing through SMS or text messages, often with malicious links.

04

Angler Phishing

Fake customer service accounts on social media used to deceive users and steal information.

Importance of Cryptographic Identities:

Implementing cryptographic identities ensures the authenticity of user identities, reducing the risk of impersonation attacks. It strengthens security by verifying identities and minimising unauthorised access.

CYFOR SECURE
CYBER SECURITY

Mitigation:

EMPLOYEE TRAINING

Regular training to help staff recognise AI-generated threats and stay vigilant.

AI DETECTION TOOLS

Deploy systems capable of identifying and filtering out AI-generated content.

REGULAR UPDATES

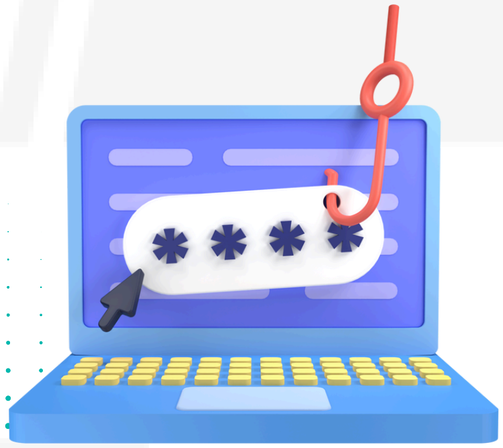
Stay informed on the latest AI developments and update security protocols to address emerging threats.

CYFOR SECURE
CYBER SECURITY

UNDER-THE-RADAR ATTACKS BY INITIAL ACCESS BROKERS (IABS)

Overview:

Initial Access Brokers (IABs) specialise in infiltrating networks and selling unauthorised access to other cyber criminals, such as ransomware operators, often staying undetected for extended periods.



Tactics:

01

COMPROMISED SERVERS

IABs gain access to servers using weak or exposed Remote Desktop Protocol (RDP) credentials.

02

VPN ACCESS

Exploit vulnerabilities in VPN configurations to gain entry into networks.

03

EMAIL ACCESS

Use stolen credentials to control email accounts and further compromise systems.

CYFOR SECURE
CYBER SECURITY

Mitigation:

PATCH MANAGEMENT

Regularly update and patch systems to address known vulnerabilities.

STRONG ENDPOINT SECURITY

Deploy robust endpoint protection solutions to detect and block unauthorised access.

ROBUST INCIDENT RESPONSE PLANS

Develop and maintain comprehensive plans to quickly address and contain breaches, minimising damage.

CYFOR SECURE
CYBER SECURITY

STRATEGIES TO COUNTER INITIAL ACCESS BROKERS (IABS)

01

Regular System Updates

Consistently patch and update software to address critical vulnerabilities that IABs might exploit. Keeping systems up to date reduces the risk of unauthorised access.

02

Access Controls & Log Monitoring

- Implement strict access controls following the principle of least privilege to limit exposure.
- Regularly monitor security logs to detect anomalies and unauthorised access, enabling a swift response to potential threats.

03

Enhanced Endpoint Protection

Deploy Endpoint Detection and Response (EDR) solutions to monitor and protect devices. EDR tools can quickly detect and block suspicious activities, preventing initial access attempts from escalating.

CYFOR SECURE
CYBER SECURITY

BIG GAME HUNTING (BGH) RANSOMWARE INCIDENTS

Overview:

Big Game Hunting (BGH) ransomware targets large organisations, seeking high payouts by exploiting their need to avoid operational disruptions and reputational damage.

Tactics:

01

RANSOMWARE-AS-A-SERVICE (RAAS):

Attackers lease ransomware tools to affiliates, enabling widespread attacks without needing advanced technical skills.

02

DOUBLE EXTORTION

Attackers not only encrypt data but also threaten to release sensitive information unless the ransom is paid, increasing pressure on victims.

CYFOR SECURE
CYBER SECURITY

Mitigation:

BACKUP AND RECOVERY PLANS

Regularly back up data across multiple locations, including offline copies, and test recovery processes to ensure quick restoration.

ZERO-TRUST ARCHITECTURE

Limit internal network access and continuously verify users and devices, reducing the ability of ransomware to spread.

THREAT INTELLIGENCE

Use real-time threat intelligence to detect potential threats early and strengthen defenses against known ransomware tactics.

CYFOR SECURE
CYBER SECURITY

STRENGTHENING CYBER RESILIENCE

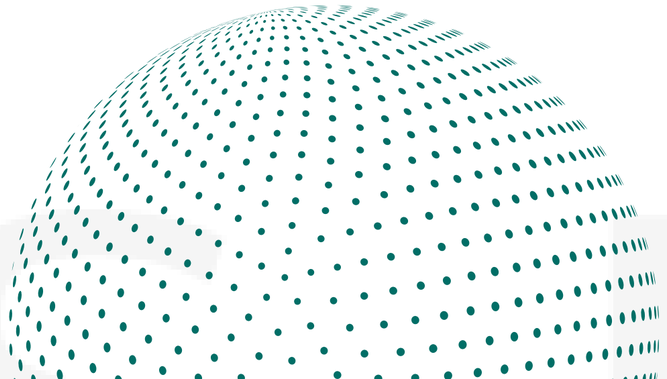
Cyber resilience ensures businesses can withstand attacks through early threat detection, secure recovery systems, and protected backups, minimising disruption and enabling swift recovery.

01 Early Warning Systems

Deploy technologies like Intrusion Detection Systems (IDS) and Endpoint Detection and Response (EDR) to identify threats at an early stage, including insider threats.

02 Secondary Clean Environments

Maintain isolated recovery systems (cleanrooms) to ensure business continuity and data integrity if the primary environment is compromised.



03 Immutable Data Storage

Use air-gapped systems to store unchangeable backups, protecting data from ransomware and unauthorised alterations

CYFOR SECURE
CYBER SECURITY

STRENGTHENING CYBER RESILIENCE

Benefits:

01

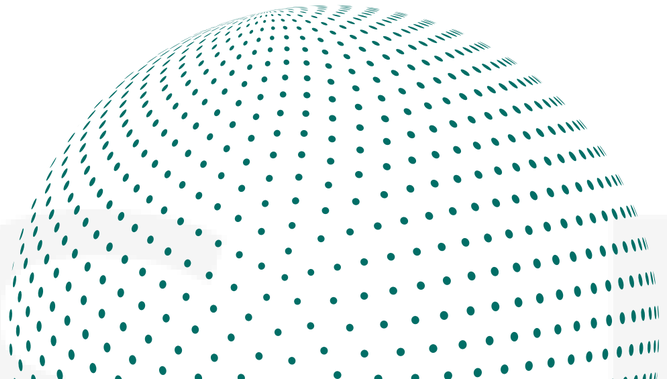
Minimise Operational Disruption

Ensure that essential business functions can continue even during a cyber-attack.

02

Quick Recovery from Attacks:

Robust recovery measures enable businesses to restore operations faster, reducing downtime and financial loss.



CYFOR SECURE
CYBER SECURITY

RECAP OF KEY POINTS

Mitigate Risks from Third-Party Relationships

Protect sensitive data by carefully managing vendor access, conducting regular audits, and establishing clear security responsibilities.

Address AI-Driven Social Engineering Threats

Stay vigilant against AI-enhanced phishing and impersonation by training employees and deploying detection tools

Strengthen Defenses Against IABs and Ransomware

Implement robust endpoint protection, regular system updates, and effective incident response plans to counter under-the-radar attacks and ransomware threats.

Build Robust Cyber Resilience for Ongoing Security

Prepare for potential breaches with early warning systems, secure recovery environments, and strong backup solutions to ensure quick recovery and minimal disruption.

CYFOR SECURE
CYBER SECURITY

NEXT STEPS FOR BETTER SECURITY

Adopt Best Practices

Implement a layered defense strategy with multiple security measures, conduct regular security training, and maintain vigilant monitoring to detect and address threats promptly.

Invest in Employee Education

Regularly train employees to recognise emerging threats like AI-enhanced phishing and ransomware. Continuous education is key to reducing human errors and strengthening your organisation's overall security

Follow the NIST Cyber Security Framework

Use the NIST framework as a guide to build a robust security posture, focusing on five core functions: Identify, Protect, Detect, Respond, and Recover. This approach helps in addressing risks systematically

CYFOR SECURE
CYBER SECURITY

ABOUT CYFORSECURE

Expertise in Cyber security Solutions:

CYFORSecure specialises in delivering comprehensive cyber security solutions tailored to meet the unique needs of businesses across various sectors. Our focus is on proactive threat management and robust security strategies.

Our Services Include:

- Threat Detection & Response: Identify and mitigate threats before they cause damage.
- Vulnerability Assessments: Regularly assess and address system vulnerabilities.
- Security Audits: Comprehensive evaluations of your security posture.
- And More: Custom solutions to enhance your organisation’s cyber resilience.

+44 (0)161 797 8123

enquiries@cyforsecure.co.uk

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

CYFOR SECURE
CYBER SECURITY

ANY QUESTIONS?

Thankyou for your attention.
Any Questions?