precision
CYBERTECHNOLOGIES & DIGITAL SOLUTIONS LTD

CYBER DIGITAL WORLD

NEWSLETTER

Volume: 46 MAY 2025

Dr. Ronald Walcott
Managing Director

INTRODUCTION

Over the past few years, remote work has evolved from a short-term necessity into a long-term strategic approach. But with this shift came a complex new challenge: securing a dispersed workforce across varied devices, networks, and environments. As organizations rapidly adapted, many discovered vulnerabilities—and hard-earned lessons along the way.

In this edition of our newsletter, we dive into what those lessons are. From real-world case studies to practical strategies, we explore how companies have strengthened their cybersecurity posture, reshaped policies, and built resilience into their remote operations. Whether you're managing a hybrid team or fully remote workforce, these insights can help you stay a step ahead of the next security challenge.

Let's explore what we've learned—and how to put that knowledge into action.

SECURITY BREACHES IN REMOTE WORK ENVIRONMENTS

1. **AT&T Data Breach via Third-Party Cloud Provider** In 2024, AT&T experienced a data breach affecting millions of customers. Hackers exploited vulnerabilities in the cloud storage services provided by Snowflake, a third-party vendor, to access sensitive data such as call logs, text records, and location details. The breach was enabled by inadequate cloud security configurations and the absence of multi-factor authentication (MFA). This incident highlighted the risks associated with third-party dependencies and the importance of securing cloud environments in remote work setups.

2. **Remote Hiring Exploited by North Korean Operatives** A cybersecurity company discovered that a remote software engineer applicant, identified as "Kyle," was actually a North Korean spy using a stolen identity. This infiltration was part of a broader espionage operation where North Korean agents exploited weaknesses in remote hiring processes to gain access to Western companies. The operatives used sophisticated techniques to assume false identities and establish a foothold in company systems, aiming to deploy malware and steal intellectual property. This scheme reportedly funded North Korea's missile program through cyberattacks and cryptocurrency theft.

3. **Twitter Hack (2020)** In July 2020, Twitter experienced a major security breach where hackers gained access to the accounts of high-profile individuals and companies. The attack was traced back to a spear-phishing attack on Twitter employees working remotely. The hackers used social engineering to trick employees into providing their login credentials, which were then used to access internal systems.

4. **Zoom Bombing (2020)** With the surge in remote work during the COVID-19 pandemic, the video conferencing platform Zoom saw a massive increase in users.

CONTINUED ON PAGE 2

IN THIS ISSUE:

However, this also led to a rise in "Zoom bombing" incidents, where uninvited individuals would join and disrupt meetings. These incidents highlighted the importance of securing virtual meetings with passwords and waiting rooms.

5. **Colonial Pipeline Ransomware Attack (2021)** The Colonial Pipeline attack was one of the most significant ransomware attacks in recent history. The breach was attributed to a compromised password for a VPN account that was no longer in use but still active. This incident underscored the vulnerabilities associated with remote access systems and the need for robust password management and multi-factor authentication.
6. **Cognizant Ransomware Attack (2020)** IT services giant Cognizant fell victim to a Maze ransomware attack in April 2020. The attack disrupted their operations and led to significant financial losses. The incident was linked to vulnerabilities in remote desktop protocols (RDP) that were exploited by the attackers.

STRENGTHENING CYBERSECURITY POSTURE

Here are several real-world case studies illustrating how companies have strengthened their cybersecurity posture in response to the challenges of securing remote workforces:

1. **IBM: Proactive Employee Training** IBM recognized that human error was a significant vulnerability in their cybersecurity defenses. In response, the company invested heavily in comprehensive security awareness training for its employees, including regular training sessions, phishing simulations, and assessments. As a result, IBM reported a 40% decrease in successful phishing attacks and a stronger overall security posture.
2. **Microsoft: Zero Trust Implementation** Microsoft adopted the Zero Trust security model across its global network, emphasizing strict access controls, continuous monitoring, and the use of Multi-Factor Authentication (MFA). This approach significantly reduced the risk of data breaches and enhanced security for remote workers, aligning with recommendations from cybersecurity experts.
3. **Coinbase: Robust Remote Work Framework** Coinbase developed a robust remote work framework that prioritizes both security and productivity in a decentralized work environment. The company implemented stringent security protocols, including the use of Virtual Private Networks (VPNs) to ensure encrypted data transmissions, safeguarding sensitive information in the highly regulated cryptocurrency industry.

RESHAPING COMPANY POLICIES

Companies have adapted their rules and regulations to operate efficiently in this new climate. They have reshaped and implemented their company policies to ensure that they operate efficiently but securely at all times. These policy adaptations encompass various aspects; here are some of those aspects:

1. **Strengthening Access Controls** To mitigate unauthorized access, organizations have implemented robust authentication measures. For instance, the adoption of Multi-Factor Authentication (MFA) has become a standard practice, requiring users to provide multiple forms of verification before accessing systems. This additional layer of security significantly reduces the risk of breaches stemming from compromised credentials.
2. **Implementing Device and Endpoint Security Policies** With the increase in Bring Your Own Device (BYOD) practices, organizations have established policies to ensure that personal devices meet security standards before accessing corporate networks. This includes the use of Mobile Device Management (MDM) solutions to enforce encryption, remote wipe capabilities, and compliance with security protocols.
3. **Adapting to Hybrid Work Models** The shift towards hybrid work models has prompted companies to develop policies that ensure equitable access to resources and opportunities for both remote and in-office employees. This includes implementing rotation schedules for in-office work, offering stipends for home office equipment, and providing mental health resources tailored to remote workers.

BUILDING RESILIENCE

Companies worldwide have embraced innovative strategies to build resilience into their remote operations, ensuring continuity and adaptability in the face of disruptions. Here are several impactful approaches:

1. **Leveraging Technology for Operational Continuity** Heineken implemented a mobile-based custom app developed by ServiceNow to streamline incident management and maintenance across its global operations. This tool provided engineers with real-time guidance and offline functionality, enhancing resilience by enabling swift responses to issues and predictive maintenance, even in areas with poor connectivity
2. **Investing in Employee Training and Crisis Preparedness**

Organizations have recognized the importance of equipping employees with the skills to handle unforeseen events. Implementing regular training sessions, role-playing exercises, and virtual simulations has been shown to reduce downtime during emergencies by 40%, fostering a proactive and confident workforce.

Frequently Asked Questions:

WHAT ARE SOME TOOLS FOR SECURING HYBRID AND REMOTE TEAMS?

Identity & Access Management (IAM)

- Examples: Okta, Microsoft Entra (Azure AD), Duo Security
- Purpose: Controls who can access what, and ensures secure logins using multi-factor authentication (MFA).

Virtual Private Networks (VPNs)

- Examples: NordLayer, Cisco AnyConnect, Palo Alto GlobalProtect
- Purpose: Encrypts internet traffic to protect sensitive data, especially over public or home Wi-Fi networks.

Endpoint Detection and Response (EDR)

- Examples: CrowdStrike Falcon, SentinelOne, Sophos Intercept X
- Purpose: Monitors and responds to threats on individual devices.

Secure Access Service Edge (SASE)

- Examples: Zscaler, Netskope, Palo Alto Prisma Access
- Purpose: Combines networking and security services into one cloud-based solution for secure remote access.

WHAT ARE SOME BEST PRACTICES FOR SECURING HYBRID AND REMOTE TEAMS?

Adopt a Zero Trust Security Model

Always verify access—assume no device or user is automatically trusted, even inside the network.

Use Multi-Factor Authentication (MFA) Everywhere

Require MFA for email, VPNs, cloud services, and internal applications.

Enforce Least Privilege Access

Give users only the permissions they need to do their jobs—no more, no less.

Regular Security Awareness Training

Train employees to spot phishing, use strong passwords, and follow good cyber hygiene.

HOW OFTEN SHOULD REMOTE EMPLOYEES RECEIVE CYBERSECURITY TRAINING?

Answer:

Best practice is to:

- Provide comprehensive onboarding training for new hires.
- Conduct quarterly refresher courses and simulated phishing exercises.
- Issue immediate updates when new threats or scams emerge.
- Customize training by department and role to improve relevance and retention.

WHY CLIENTS CHOOSE US

We offer companies a complete, top to bottom approach to assess posture, identify gaps, implement securities and mitigate risk.

Headline News

Account Takeover Scams Are Bypassing Fraud Defences

Scammers are increasingly turning to account takeover fraud, as financial institutions ramp up their defenses. Instead of luring victims into making authorized transactions, cybercriminals are bypassing them altogether, hijacking their digital identities and draining accounts from within.

Account takeover fraud, which involves gaining unauthorized access to a victim's account to execute unauthorized transactions, has been rising in recent years, as scammers have become more sophisticated, taking advantage of phishing, credential stuffing and malware to exploit digital banking channels. Traditional fraud detection tools and static behavior analysis technology are ineffective because scammers can mimic legitimate user behavior.

NICE Actimize's 2025 Fraud Insights U.S. Retail Payments report found that from 2023 to 2024, fraudster's focus shifted slightly toward account takeover, in terms of the overall value of attempts. However, research shows that scams are still the method of choice across 57% of attempted fraud transactions.

In 2024, financial institutions globally experienced a steep rise in ATO-related incidents. According to Veriff's Identity Fraud Report, ATO fraud climbed 13% year-over-year. FinCEN's data further highlights the trend, revealing that U.S. banks alone filed over 178,000 suspicious activity reports linked to ATO, a 36% jump from 2023. AARP and Javelin's research found that ATO fraud caused $15.6 billion in losses last year.

To counter this, financial institutions must take advantage of artificial intelligence-fueled behavioral biometrics that aims to go beyond static credentials, experts say.

By continuously profiling how users interact with devices, firms can shift from one-time authentication to real-time identity assurance. Rather than static checks at login, hybrid AI models adjust for device type, time of day, geolocation and other scenarios, aligning with NIST's zero trust principle of continuous multifactor authentication. This approach catches account takeovers and eases the user journey by validating identity behind the scenes.

"The most sophisticated measurement approaches now employ AI analytics to establish dynamic baselines for these metrics, enabling continuous ROI assessment as both threats and solutions evolve over time," Jeremy London said, director of engineering for AI and threat analytics at Keeper Security.

EMERGING FRAUD TRENDS

The rise in ATO fraud is part of a broader trend of increasingly sophisticated cyberthreats. Cross-border payments are increasingly under threat. In 2024, even as total international wire activity dropped by 6%, the value of fraud attempts surged by 40%, highlighting a shift toward more sophisticated attacks targeting high-value, low-volume transactions. One of the most vulnerable points in this process is payee onboarding. An alarming 67% of fraud cases were linked to just 7% of payments, specifically those sent to newly added payees. This underscores how fraudsters are actively exploiting the initial stages of new payee relationships as a weak link in the payment chain.

It is clear that future of behavioral biometrics lies in integrating multimodal signals with AI models trained to detect adversarial threats. This combination is essential to effectively identify and block both human fraudsters and synthetic identities.

Source: databreachtoday.com

UPCOMING EVENTS

HEALTHSEC USA
June 3, 2025

INFOSECURITY EUROPE 2025
June 3, 2025

CS4CA CANADA
June 11, 2025

CYBERSECURITY SUMMIT: LONDON FINANCIAL SERVICES
September 11, 2025

868-610-7237
info@precision-cyber.com
www.precision-cyber.com
1st Floor, Brair Place, 10-12 Sweet Road
St. Clair, Port of Spain, Trinidad