It's Not If or How, But When You Will Be Subject to a Cyber Attack

Jacqui Magnes
CEO and Owner | COMSO, Inc. dba CISPOINT

Understanding the Inevitable

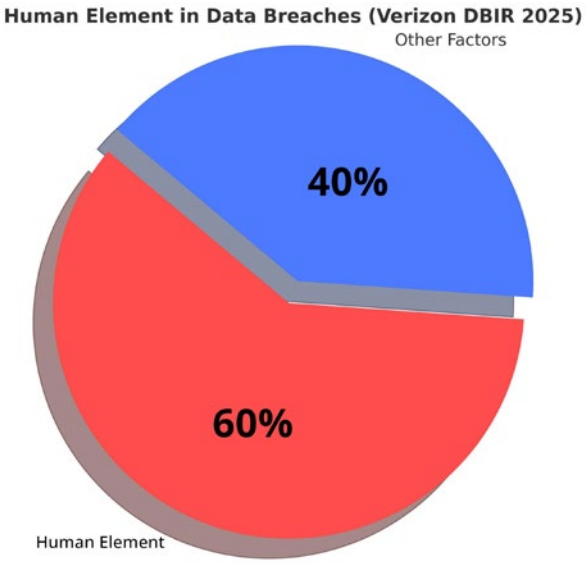
The rapid evolution of cyber threats means that every organization, from multinational corporations to small nonprofits, is in the crosshairs. Cybercrime costs are projected to reach $10.5 trillion annually by 2025, according to Cybersecurity Ventures. Attackers are armed with automated tools that scan for vulnerabilities 24/7, leaving no room for complacency. These scans do not differentiate between a large enterprise and a small local business—if a vulnerability exists, it will eventually be found. The outdated concept of an 'IT guy' handling all technology problems is no longer sustainable—modern cybersecurity requires a multi-layered, organization-wide approach where every department plays a role in maintaining security.

The Root Causes – Why Attacks Are Unavoidable

The expanding attack surface—driven by remote work, cloud proliferation, and the increasing presence of IoT (Internet of Things) devices—creates more opportunities for compromise. Remote work exposes organizations to risks from home networks and unmanaged devices. Cloud adoption distributes sensitive data across multiple SaaS platforms, each of which can become a target. IoT devices, often left unpatched and insecure, provide additional attack

vectors, especially in industries such as healthcare and manufacturing where operational technology is directly connected to the internet.

> **Spear phishing in particular has evolved to mimic genuine correspondence from trusted contacts, making it difficult for even vigilant employees to identify threats.**



Source: Verizon DBIR (2025) data

The human factor remains the most significant vulnerability, with the Verizon Data Breach Investigations Report (2024) attributing 74% of breaches to human error. Employees may click on phishing links, use weak or reused passwords, or fall for sophisticated social engineering campaigns. Spear phishing in particular has evolved to mimic genuine correspondence from trusted contacts, making it difficult for even vigilant employees to identify threats.

Common attack vectors include:

- Session Hijacking: Attackers intercept authentication cookies to gain unauthorized access.
- Phishing & Spear Phishing: Deceptive messages to deliver malware or steal credentials.
- Ransomware: Malicious encryption of data, demanding payment.
- Insider Threats: Malicious or negligent actions from individuals with privileged access.

Mobile Device Risks in Business

Conducting business on a mobile phone introduces unique cybersecurity risks. Mobile devices are inherently more personal, used for both work and leisure, creating opportunities for data leakage between personal and corporate environments. Many employees access corporate email, cloud storage, and collaboration platforms on their phones without the same security controls enforced on laptops. This can expose sensitive data if the device is lost, stolen, or compromised.

Statistics underscore the scale of the problem: A Lookout study found that 27.6% of personal mobile users and 11.8% of enterprise users clicked on six or more phishing links annually. Smishing—phishing via SMS—has surged, with about 40% of victims clicking on malicious links. A separate experiment revealed that 16.9% of mobile users clicked on harmful SMS links, with many falling for repeated attempts.

Identifying a cyber attack on a mobile device is often more difficult than on a laptop. Smaller screens can obscure the full URL of a link, making it harder to detect phishing attempts. Mobile operating systems often hide technical indicators—such as file extensions or email headers—that could reveal a threat. Additionally, security tools for mobile devices typically provide less granular visibility and control compared to those available for desktops and laptops.

Source: www.embroker.com

The Solution – Defense in Depth

Defense in Depth (DiD) is a strategy built on multiple overlapping layers of security controls to ensure that a single failure does not compromise the entire system.

These layers include:

- Perimeter Security: Firewalls and intrusion detection/prevention systems (IDS/IPS).

- Endpoint Protection: Endpoint Detection and Response (EDR) solutions.
- Access Control: Multi-factor authentication (MFA), least privilege, and zero trust policies.
- Network Segmentation: Limiting lateral movement within the network.
- Continuous Monitoring: Security Information and Event Management (SIEM) systems for real-time threat detection.

Session hijacking can be mitigated by:

- Enforcing HTTPS for all data transmission.
- Using secure cookie flags (`HttpOnly`, `Secure`, `SameSite`).
- Implementing strict session timeouts.
- Regularly rotating session tokens.

Technical Implementation – Feasibility

Zero Trust Architecture applies the principle of 'Never Trust, Always Verify', enforcing continuous authentication and micro-segmentation to limit access strictly to necessary resources. Advanced email security should incorporate DMARC, SPF, and DKIM standards to authenticate sending domains, alongside AI-driven phishing detection systems that adapt to new attack methods. Incident response automation, through Security Orchestration, Automation, and Response (SOAR) platforms, ensures rapid containment by automatically locking accounts and triggering investigation workflows when suspicious activity is detected.

Integration into General Use

Integration begins with clearly defined policies, regular training, and enforced technical controls. Vendor security must be addressed through strict supply chain management. Routine penetration testing and vulnerability scanning should be scheduled, and remediation progress should be monitored as a key security performance metric.

> **Regular updates and patches for mobile operating systems and apps should be part of the organization's patch management cycle, and security awareness training should address mobile-specific threats such as smishing, malicious apps, and insecure Wi-Fi connections.**

Mobile device security must also be incorporated into integration strategies. This includes enforcing Mobile Device Management (MDM) policies, requiring device encryption, and ensuring that corporate data on smartphones is containerized and remotely wipeable in case of loss or theft. Regular updates and patches for mobile operating systems and apps should be part of the organization's patch management cycle, and security awareness training should address mobile-specific threats such as smishing, malicious apps, and insecure Wi-Fi connections.

Conclusion

Cybersecurity is no longer a luxury—it's a fundamental requirement in today's connected world. Relying on a lone 'IT guy' to manage all security risks is unrealistic and dangerous. Modern threats demand layered defenses, constant monitoring, and shared responsibility across the entire organization.

Mobile security must be part of this plan. Apply strict controls to any device accessing corporate resources—including personal smartphones under BYOD policies—enforce encryption, keep software updated, avoid unsecured networks, and ensure the ability to remotely wipe lost or stolen devices. In a mobile-first workforce, securing phones is just as critical as protecting laptops and servers.

Within the next month, every business should take decisive action: perform a risk assessment, enable multi-factor authentication, review user access, deploy endpoint protection, and establish ongoing security awareness training. Don't wait for a cyber-attack to occur to act!

ABOUT THE AUTHOR

Jacqui Magnes *is the owner and CEO of COMSO, Inc., an IT services firm supporting the Intelligence Community with cutting-edge solutions in system integration, software development, and training. Since acquiring the company in 2017, she has built a top workplace culture and launched initiatives like the Empowering Women in Technology Scholarship.*

In 2023, COMSO acquired CISPOINT, Inc., a Managed Security Service Provider (MSSP) that is a CyberAB Registered Practitioner Organization (RPO) specializing in managed services and CMMC 2.0 compliance for small to mid-sized businesses. Prior to COMSO, Ms. Magnes spent over two decades at Bristol-Myers Squibb in leadership roles across sales, training, federal policy, and market access.

She holds a B.S. in Medical and Research Technology, an M.S. in Marketing Management, and an MBA. Ms. Magnes serves on the Cybersecurity Association Board and the Early College Cyber Advisory Board for Howard County Public School System.

CISPOINT
MSSP Focused on Rightsizing Your IT

References:

Cybersecurity Ventures (2023). Cybercrime Damage Costs to Reach $10.5 Trillion Annually by 2025.

Verizon (2024). Data Breach Investigations Report (DBIR).

Lookout (2022). Global State of Mobile Phishing Report.

OWASP (2024). Session Management Cheat Sheet.

NIST Special Publication 800-207. Zero Trust Architecture.