LastPass

From Cyber Risk to Resilience in 2025:

A Playbook for Emerging and Mid-Sized Companies

DR. CHASE CUNNINGHAM

About the Author

Dr. Chase Cunningham—known globally as "Dr. Zero Trust"—is one of the most recognized voices in cybersecurity strategy and digital transformation. A retired US Navy Chief Cryptologist with more than two decades of operational and strategic experience, Chase has built his career at the intersection of national security, enterprise defense, and cutting-edge technology.

He is the creator of the Zero Trust Extended (ZTX) framework, developed during his tenure as Principal Analyst at Forrester Research, which has become a foundational model for governments and enterprises worldwide. His work has directly influenced US federal cybersecurity mandates, defense initiatives, and commercial adoption of Zero Trust architectures.

Chase has served as Chief Strategy Officer at Demo-Force.com, advising leading security vendors and partnering with organizations across the public and private sectors to drive real-world Zero Trust adoption. He is a prolific author of multiple books on cybersecurity, including bestsellers on Zero Trust strategy, cyber warfare, and the business of security.

A dynamic speaker and storyteller, Dr. Cunningham brings a unique blend of hard-won operational insight, academic rigor, and straight-talking analysis. He has presented at major global events, including RSA and Black Hat, as well as government briefings, while also hosting The Dr. ZeroTrust Show, a widely followed podcast and media platform.

Audiences value Chase for his authentic approach: he cuts through industry hype to deliver actionable insights on cyber defense, AI, risk management, and the business impacts of security. Whether addressing policymakers, CISOs, or frontline practitioners, Dr. Cunningham's message is clear—trust nothing, validate everything, and build security strategies that actually work.

Table of Contents

From Cyber Risk to Resilience in 2025:
A Playbook for Emerging and Mid-Sized Companies

Emerging and mid-sized companies from all verticals today face cyber threats as dangerous as those targeting large enterprises. Recent breach investigation reports, including Verizon's 2025 Data Breach Investigations Report (DBIR), Mandiant's M-Trends, and CrowdStrike's Global Threat Report, reveal that no organization is "too small" to be a target. These reports debunk the misconception that cybercriminals primarily target large companies.

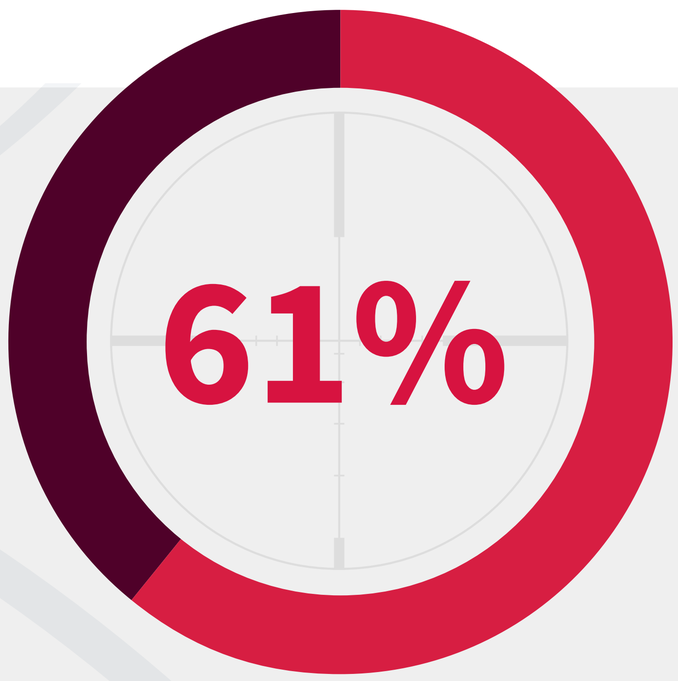
Ransomware gangs, for example, are "**quite happy to breach smaller organizations and adjust their ransom demands accordingly,**"

meaning small and scaling companies are very much in the crosshairs. A sobering anecdote from the DBIR recounts how a tiny data aggregation firm with just a handful of employees was breached, resulting in 2.9 billion sensitive records being stolen and sold on the dark web. This "mouse that roared" incident dramatically illustrates that even a minor business breach can have an outsized impact on millions of people.

Why are growing firms at such risk? Simply put, **those businesses now face the same threats as large enterprises, without the same defenses.** Adversaries have realized emerging and mid-sized companies often have weaker security postures, limited budgets, and minimal incident response capabilities, making them attractive targets. Meanwhile, the cyber threat landscape continues to evolve rapidly, as attackers leverage automation, artificial intelligence (AI), and stolen credentials at an unprecedented scale. The result is that 61% of emerging and mid-sized companies experienced a cyberattack in the last year (BlackFog, 2023).

The message is clear: emerging and mid-sized companies must shed any notion of "security by obscurity" and proactively harden their defenses. The following sections consolidate key findings from 2024 breach data and translate them into strategic recommendations to help companies not only catch up but get ahead of adversaries.

This paper takes a deep dive into the latest breach trends affecting smaller companies and distills them into concrete, forward-looking action plans. Also included is a cybersecurity maturity model tailored for emerging and mid-sized companies. It is a roadmap to elevate security systematically and highlights how simple **"blocking and tackling" methods can be leveraged to mitigate threats.** The goal is to go beyond generic advice, instead presenting detailed insights and new, practical measures that can stand up to academic and industry scrutiny.



of emerging and mid-sized companies **experienced a cyberattack in the last year**

A Snapshot of the 2025 Threat Landscape for Emerging and Mid-Sized Companies

Recent breach reports paint a stark picture of the challenges emerging and mid-sized companies face. Several dominant trends emerged in 2024 that are especially relevant to smaller organizations. Understanding these trends is critical, as they inform where companies should focus their security efforts.

RANSOMWARE REMAINS RAMPANT:

Ransomware remains the defining threat for emerging and mid-sized companies. Verizon's 2025 DBIR found that **ransomware was a factor in 44% of all breaches** (across organizations of all sizes), a sharp increase from 32% the year prior. Strikingly, when broken down by organization size, ransomware was present in *88% of breaches affecting emerging and mid-sized companies,* compared to 39% of breaches in large enterprises. In other words, virtually nine out of ten breaches of emerging and mid-sized companies involve ransomware – an astounding proportion.

This finding definitively debunks the myth that "ransomware groups only target big companies"; the data show precisely the opposite. Criminals simply calibrate their ransom demands to the victim's size and assume growing companies lack the robust backups or recovery capabilities of larger organizations. Indeed, attackers count on the fact that **these companies are less likely to have up-to-date, readily available backups to save them.** The outcome is prolonged downtime and greater pressure to pay.

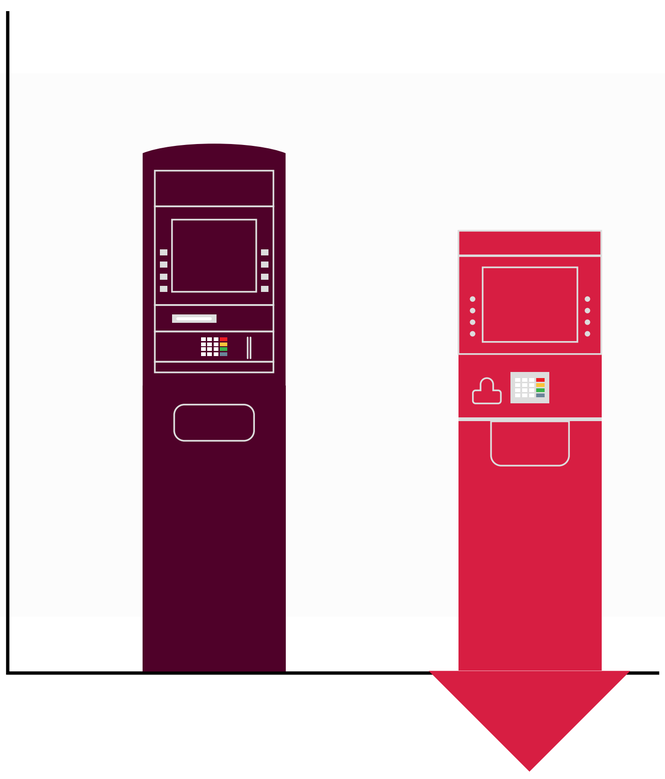
Verizon noted 88% of ransomware attacks on emerging and mid-sized companies led to extended business downtime.

nine out of ten breaches
of emerging and
mid-sized companies
involve ransomware

RANSOMWARE PAYMENTS DECLINE (RESILIENCE IS IMPROVING):

Despite ransomware's prevalence, there is a glimmer of positive news: more victims are refusing to pay ransoms, likely thanks to better preparedness. The 2025 DBIR reports that the median ransom payment dropped to $115,000 (down from $150,000) and 64% of victim organizations did not pay – a meaningful improvement from 50% two years prior. Law enforcement pressure and corporate policies against paying may be factors. Still, a significant reason is that **companies are increasingly able to restore systems without paying** due to stronger backups and incident response plans.

As Verizon's incident response lead observed, many organizations have "learned a lot" and invested in backup/disaster recovery, so they no longer feel forced to pay ransom under duress. This trend is encouraging as it suggests that even as ransomware attacks surge, proactive measures are yielding tangible results in undermining attackers' business models. Notably, by late 2024, only ~25% of ransomware victims ended up paying at all, according to Coveware data. For emerging and mid-sized companies, the key takeaway is that **resilience is achievable** – preparation directly reduces the likelihood of needing to pay criminals to recover.



median ransom payment

dropped to $115,000 (down from $150,000)

64% of victim organizations did not pay

EXPLOSION IN CREDENTIAL THEFT AND "MALWARE-FREE" ATTACKS:

Threat actors have doubled down on stealing or abusing credentials as a primary attack vector, often rendering traditional malware unnecessary. In 2024, 79% of intrusions that CrowdStrike detected were "malware-free," meaning attackers relied on legitimate credentials and living-off-the-land techniques (a method where the attacker uses the readily available users, passwords, and access to stay "hidden" in the network for a prolonged period of time) rather than file-based malware. Similarly, the DBIR notes that **stolen credentials were used in 22% of all breaches** analyzed. *88% of web application breaches* involved compromised credentials, often obtained through phishing or database leaks. For both smaller and larger companies, the **use of stolen passwords is the top hacking method** (appearing in about one-third of breaches for each).

79% of intrusions that CrowdStrike detected were "malware-free."

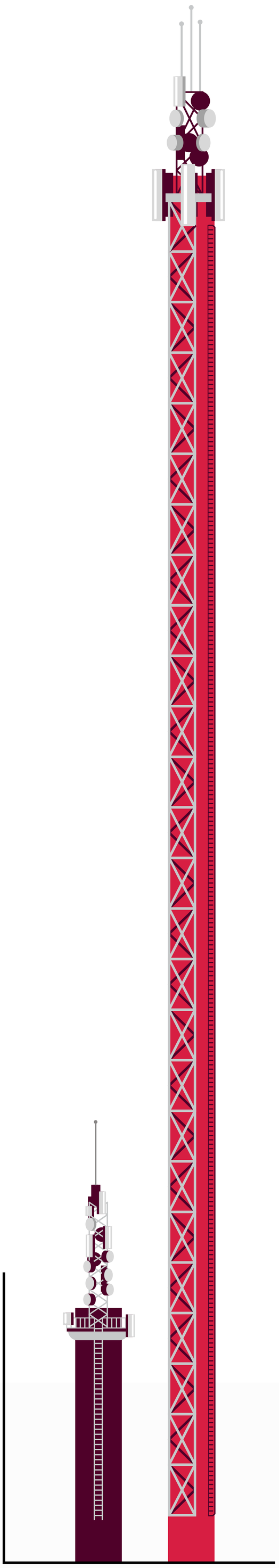
Verizon notes that these numbers are identical across organization size, despite smaller companies having a far less mature identity security program. The implication is clear: weak or reused passwords and a lack of multi-factor authentication (MFA) are open doors to attackers. Once they obtain an admin's credentials (via phishing, brute-force, or purchase on the dark web), intruders can often gain access without triggering any anti-malware alarms. The fastest breakout time observed in 2024 was a blistering 51 seconds from initial access to lateral movement, achieved by an attacker who had stolen credentials, according to CrowdStrike. This stresses how quickly an adversary can escalate an intrusion when no malware must be dropped – a likely scenario in environments lacking strong identity controls.

fastest breakout time
observed in 2024

SURGE IN SOCIAL ENGINEERING (PHISHING, VISHING, AND PRETEXTING): Humans remain a favored entry point. Social engineering, or when a threat actor uses overt social channels to target users, could be phishing or using a simple social interaction to prompt a user to interact with malicious software. It was tied to **60% of breaches** in the DBIR dataset (when errors and misuse are included).

Emerging and mid-sized companies' employees are just as likely to be phished as those in enterprises – social tactics accounted for ~18% of emerging and mid-sized companies' breaches, comparable to 13% in larger orgs (Verizon DBIR, 2025). However, specific social scams appear to hit **smaller** companies harder.

Business email compromise (BEC) and pretexting (attackers impersonating trusted parties) were found to be more common in incidents involving emerging and mid-sized companies than in significant enterprise cases. One emerging trend is **voice phishing (vishing)** and AI-driven fraud. In late 2024, there was a 442% increase in vishing attacks (phone calls impersonating IT support or executives) compared to earlier in the year, according to CrowdStrike. Attackers are leveraging AI to generate convincing deepfake voices and personalized phishing messages at scale. For resource-strapped emerging and mid-sized companies' security teams, this onslaught of highly believable scams is a serious concern – one that technology alone can't completely solve. It reinforces the need for continuous security awareness training (discussed later) and phishing-resistant MFA, since even savvy employees might eventually fall for a sophisticated con.



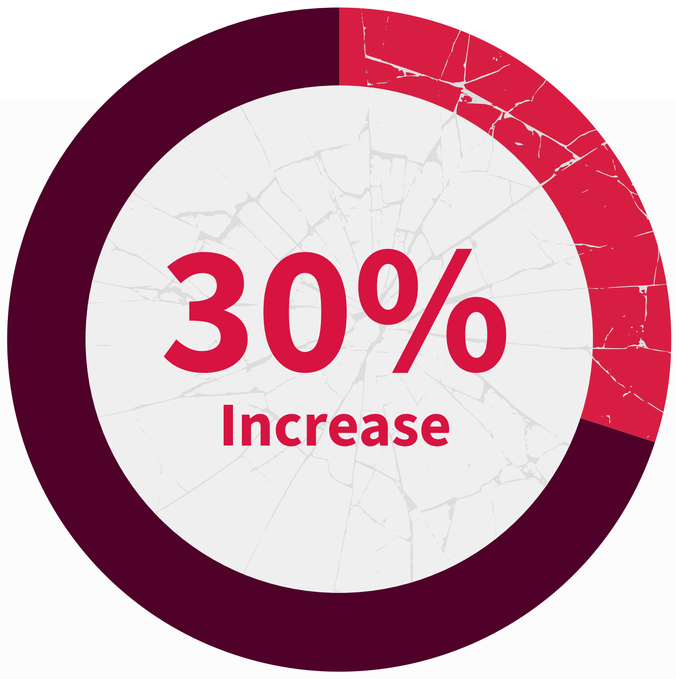
442% increase
in vishing attacks

MORE – AND FASTER – EXPLOITATION OF VULNERABILITIES AND SHADOW APP ISSUES: Another trend is the uptick in attacks exploiting software vulnerabilities, often to gain an initial foothold. According to Verizon, exploiting known (or unknown, "zero-day") vulnerabilities contributed to 20% of breaches, a 34% increase from the prior year. Attackers are quickly targeting unpatched internet-facing systems, such as VPN appliances and servers, as well as newly disclosed "0-days" (new, previously unknown malware types), before fixes are applied. The sheer volume of new vulnerabilities disclosed each year is daunting: over 22,000 vulnerabilities were reported in the first 8 months of 2024 alone (30% more than in 2023), according to Qualys.

Exploiting known (or unknown, "zero-day") vulnerabilities **contributed to 20% of breaches,** a 34% increase from the prior year.

Fortunately, only a tiny fraction (under 1%) of these vulnerabilities were actively used by attackers; however, the challenge for emerging and mid-sized companies is knowing which ones to patch first. The data shows attackers tend to exploit the easy, externally exposed weaknesses – the unpatched server or outdated software that's visible on the internet. Without a structured patch management process, these companies often fall behind on critical updates, leaving openings for breaches. The increase in vulnerability-driven breaches suggests that **"cyber hygiene" gaps (like missing patches) are catching up with organizations,** especially those without dedicated security staff. Additionally, shadow application access (apps that are no longer in use but still have valid credentials and access) is growing as a threat vector. More software and more development mean more opportunities for added areas of risk, thanks to the constantly changing nature of the current application lifecycle.

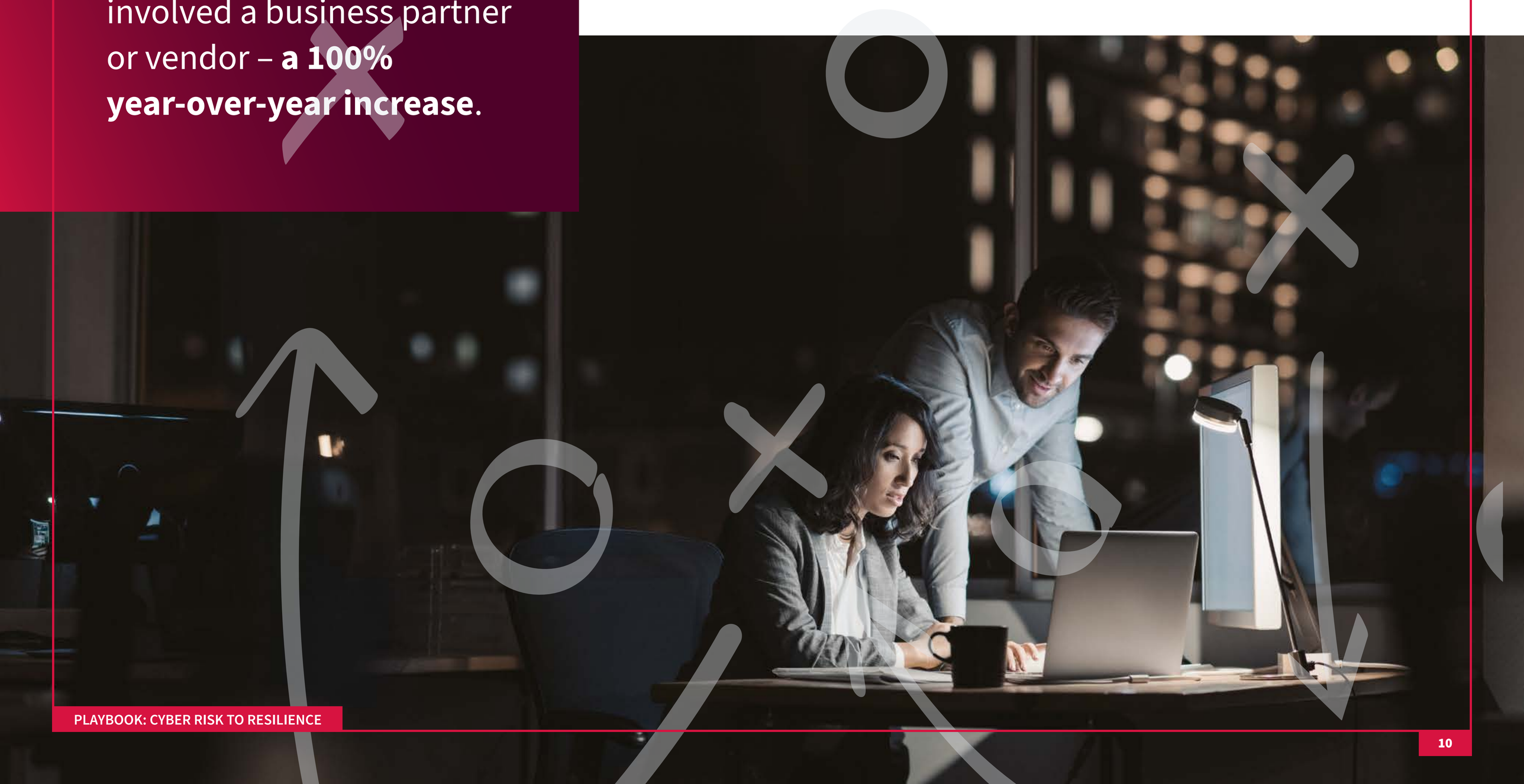
22,000 vulnerabilities
were reported in the first
8 months of 2024 alone
(30% more than in 2023)



THIRD-PARTY AND SUPPLY CHAIN RISKS SKYROCKET: Perhaps the most dramatic statistic in the 2025 DBIR is the doubling of breaches stemming from third parties. Thirty percent of all violations in the past year involved a business partner or vendor – a 100% year-over-year increase. In other words, one in three breaches now originates via a compromised supplier, service provider, or software supply chain – not within the victim's environment. This trend affects organizations of all sizes, but emerging and mid-sized companies can be especially vulnerable for two reasons. First, growing companies often rely on a multitude of external service providers (for IT support, payment processing, data storage), effectively extending their trust boundary. Second, **many of these companies fail to apply the same security rigor to their vendors as they do internally,** as Verizon's investigators note.

Attackers are exploiting this by breaching a weaker link (say, a small software vendor or a cloud-hosted database) to pivot into client networks subsequently. The implication: even if an emerging or mid-sized company does everything right internally, a partner's breach could lead to your data or systems being compromised. Or your firm might be the avenue of compromise for a larger partner business or enterprise; either way, nothing good comes from the risk that these connections introduce. It's a force multiplier for risk that must be managed proactively (discussed in the action plan later).

Thirty percent of all violations in the past year involved a business partner or vendor – **a 100% year-over-year increase**.



THREAT ACTORS: ORGANIZED CRIME VS. NATION-STATES: Most breaches in 2024, for emerging and mid-sized companies and enterprises alike, were perpetrated by financially motivated organized crime groups (cybercriminals). These include ransomware crews, fraudsters, and other e-crime actors looking for profit. **When you see "organized criminal"mentioned in a breach, you can usually assume ransomware was involved.** The DBIR's breakdown by organization size highlights that **external attackers were overwhelmingly responsible for emerging and mid-sized companies.** In contrast, large organizations saw a small slice of incidents caused by internal actors (employee errors or misuse). For smaller businesses, actual insider incidents are rare.

Few small companies have malicious insiders stealing data at scale, and even honest mistakes (misconfigurations, email errors) accounted for only 1% of emerging and mid-sized companies' breaches (versus 18% of breaches in large firms). This is one silver lining for small and scaling companies: fewer employees can mean fewer mistakes.

However, it's a mixed blessing because the slack is picked up by malware and hacking incidents. On the other end of the spectrum, nation-state espionage attacks remain relatively uncommon against emerging and mid-sized companies. State-affiliated hackers tend to go after large targets or critical supply chain hubs. Unless a smaller company owns very sensitive data or intellectual property (or is a government/defense contractor), **advanced nation-state Advanced Persistent Threats (APTs) are rarely targeting the emerging and mid-sized companies of the world.** That's a modest relief and a "positive note" to end a threat briefing on, as the DBIR wryly suggests. Still, exceptions exist – for example, a small tech company with valuable patents might be targeted by spies or APT actors – so these smaller sized companies should not entirely ignore sophisticated threats. To put it simply, every organization that is doing business digitally is a viable target for an APT.

Nation-state espionage attacks remain relatively uncommon against emerging and mid-sized companies.

TODAY'S MODERN THREAT LANDSCAPE DEMANDS THAT EMERGING AND MID-SIZED COMPANIES PROTECT AGAINST A RANGE OF HIGH-IMPACT THREATS:

- Ransomware and Double-Extortion
- Credential Theft and Phishing (Now Turbocharged by AI)
- Unpatched Software Exploits
- "Indirect" Attacks Through Third Parties

The data indicates that external attacks by organized cybercrime groups pose the principal danger, far outpacing insider threats or nation-state hacks in this sector. Emerging and mid-sized companies' leaders should internalize that no business is beneath notice: if you have money, data, or digital operations, you are a target.

The following section will examine how these threat realities translate into business impact for growing companies, and why traditional defenses and mindsets are no longer sufficient.

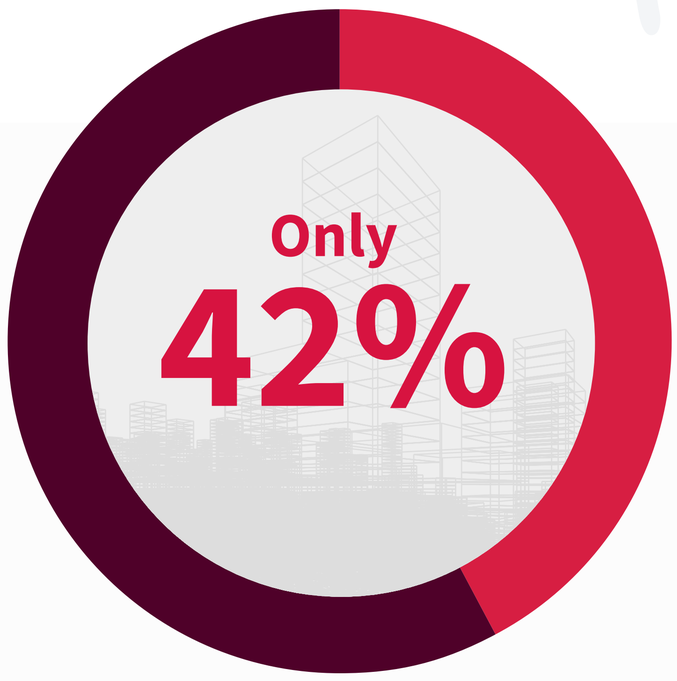
Risks and Roadblocks for Emerging and Mid-Sized Companies

Facing enterprise-grade threats with a fraction of the resources – that is the crux of the emerging and mid-sized companies' cybersecurity challenge.

The breach reports and surveys from 2024 expose a troubling gap between small and scaling companies' awareness of risks and their readiness to address them.

On the one hand, **emerging and mid-sized companies' leaders are not oblivious:** 94% of emerging and mid-sized companies' executives say they are somewhat or very knowledgeable about cyber threats (CrowdStrike, 2025). In conversations, they've heard of ransomware, phishing, and data breaches, and express concern about these dangers. **However, awareness does not necessarily equate protection.** Many small businesses still lack basic cybersecurity measures or consistent practices.

Only 42%
of emerging and mid-sized companies
provide regular security training to employees

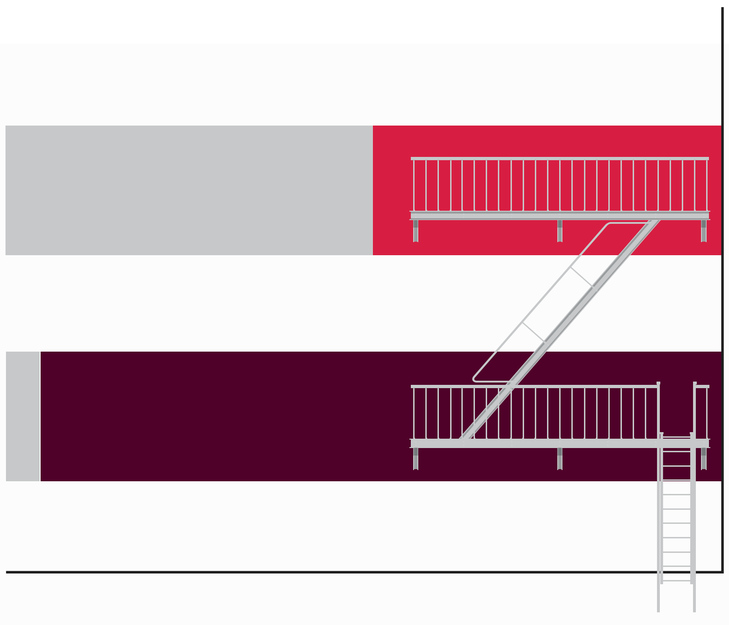


A 2025 CrowdStrike survey of emerging and mid-sized companies found that despite high awareness, most fall short on training, tools, and execution:

Only 42% of emerging and mid-sized companies provide regular security training to employees. This means most emerging and mid-sized companies' staff are not routinely educated on how to spot phishing or avoid common threats – a significant problem given the human element in breaches.

A mere 11% of emerging and mid-sized companies are leveraging AI-powered security tools (e.g., advanced threat detection or response solutions). The vast majority rely on traditional antivirus or manual processes that cannot keep up with modern "malware-free" attacks and AI-enhanced threats.

Even fundamental planning is lacking in the smallest businesses. Just 47% of micro-businesses (<25 employees) have a formal security plan, compared to nearly 90% of larger emerging and mid-sized companies (100-249 employees) who have one. This reveals a clear maturity divide by size: the tiniest firms often operate ad hoc, while the upper end of emerging and mid-sized companies may start to resemble mini enterprises with policies in place. **Many small businesses have never documented their response to an incident or protection of critical assets, leaving them dangerously unprepared.**



just 47% of businesses with less than 25 employees
have a formal security plan, compared to nearly 90% of larger emerging and mid-sized companies

Why do these gaps persist despite knowing the risks? **Resource constraints and competing priorities are key factors.** Emerging and mid-sized companies' budgets and IT teams are small. Two-thirds of smaller firms say cost is a significant barrier that prevents them from upgrading security tools and protections. Only 7% of emerging and mid-sized companies' respondents felt their security budget was entirely sufficient for their needs. The remaining 93% see a shortfall (CrowdStrike, 2025). Money isn't the only issue; expertise is also a concern. **Seventy percent of emerging and mid-sized companies rely on outside experts or consultants for cybersecurity guidance** because they lack in-house security staff, according to CrowdStrike.

Only 7% of emerging and mid-sized companies' respondents felt their security budget was entirely sufficient for their needs.

Most emerging and mid-sized companies lack 24/7 security monitoring or a dedicated incident response function.

Many smaller companies cannot afford a full-time cybersecurity professional, let alone a team, which means tasks like monitoring logs 24/7 or performing threat hunting just don't happen. As a result, most emerging and mid-sized companies lack 24/7 security monitoring or a dedicated incident response function. A breach might go on for days or weeks before being detected, simply because no one is watching in real time. Likewise, **incident response (IR) tends to be improvised** – without an IR plan or team, small and scaling companies struggle to contain breaches quickly, which leads to more damage and higher recovery costs.

Another challenge is **keeping up with compliance and regulatory requirements,** which are increasingly applying to smaller entities. From privacy laws like GDPR in Europe or CCPA in California to industry-specific regulations (HIPAA for healthcare, PCI DSS for those handling credit cards), emerging and mid-sized companies are finding themselves accountable for security controls that they are not ready for. Many are caught off guard by security questionnaires from business clients or cyber insurance underwriting requirements. This adds pressure and potential legal liability when breaches occur, yet many companies lack the internal expertise to navigate compliance effectively.

This leads to a vicious cycle: emerging and mid-sized companies remain in “cybersecurity survival mode,” addressing issues haphazardly and reactively. It’s often said that small businesses don’t believe it will happen to them, but that denial is fading as more emerging and mid-sized companies personally experience incidents. A 2025 ConnectWise report even dubs this **“the year of emerging and mid-sized companies’ cybersecurity adoption,”** noting that cyber incidents are finally prompting emerging and mid-sized companies to prioritize security and budget for it as a necessity, not a luxury (perhaps because boards and owners have witnessed peers suffer losses). Client expectations are also rising as small businesses now demand better security from their IT providers after seeing competitors suffer breaches. This is driving managed service providers (MSPs) and IT consultants to offer more cybersecurity services and emerging and mid-sized companies to allocate more of their IT spend to security tools.

Emerging and mid-sized companies remain in “cybersecurity survival mode,” addressing issues haphazardly and reactively.

Some business owners still view cybersecurity as something with unclear return on investment (ROI), right until they are hit with a crippling ransomware outage.

Yet, cultural and practical obstacles remain. Some business owners still view cybersecurity as something with unclear return on investment (ROI), right until they are hit with a crippling ransomware outage. Others implement specific tools (like endpoint security or backup software) but misconfigure them or fail to monitor them, leading to a false sense of security. For example, an emerging and mid-sized company might install an endpoint detection and response (EDR) agent on all PCs. Still, without anyone analyzing the alerts, attacks slip through – a scenario Coalition’s incident responders have often observed. Partial implementation without follow-through is a common pitfall.

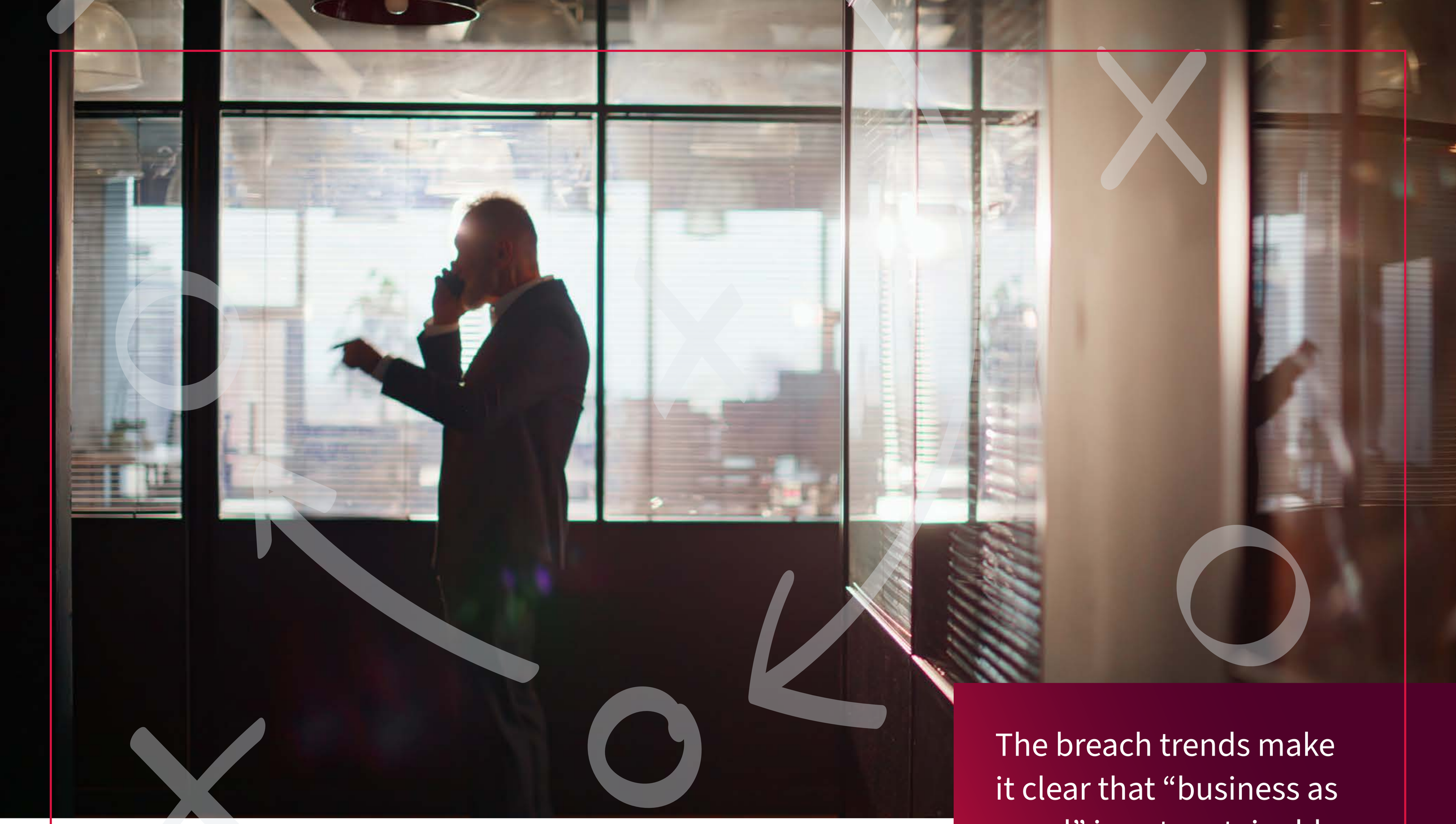
The consequence of these challenges is evident in breach impacts:

DOWNTIME AND BUSINESS DISRUPTION: As noted, emerging and mid-sized companies hit by ransomware often suffer significant downtime. Many lack the redundant infrastructure or cloud failovers that large companies use for continuity. If a smaller company's servers are encrypted, operations might halt completely. Verizon's DBIR emphasized that the impact of an emerging and mid-sized company's breach can be just as disastrous as a significant enterprise breach – it's a mistake to assume a minor breach means small damage. It can be fatal to the business.

FINANCIAL LOSSES AND RECOVERY COSTS: The immediate costs of incidents (ransom payments, recovery services, lost sales) can be devastating relative to a small company's revenue. Cyber insurance can help, but only ~20-30% of small businesses reportedly carry cyber insurance, and those that do are facing higher premiums and stricter prerequisites, such as multi-factor authentication (MFA) on email, to obtain coverage (CrowdSrike, 2025).

CUSTOMER TRUST AND LEGAL FALLOUT: Emerging and mid-sized companies are custodians of valuable data, whether it's customer personal information, payment data, or business partner information. A breach can erode client trust and lead to lost contracts. If regulated data is involved (personal data, health records), small firms may face fines or breach notification costs that they are ill-equipped to handle. The example of the National Public Data breach (2.9 billion records leaked from a tiny firm) shows how emerging and mid-sized companies can inadvertently cause harm on a national or international scale. Regulators and law enforcement will not overlook such incidents simply because the company is small.

Verizon's DBIR emphasized that the impact of an emerging and mid-sized company's breach can be **just as disastrous as a significant enterprise breach.**



The breach trends make it clear that “business as usual” is not sustainable – the cost of inaction can be the business’s survival.

Emerging and mid-sized companies today understand the threat but struggle to respond effectively due to limited resources, expertise, and formalization. The breach trends make it clear that “business as usual” is not sustainable – the cost of inaction can be the business’s survival. The encouraging news is that improvements are achievable: even incremental steps can lower risk (as evidenced by fewer ransom payouts when good backups exist). The following sections focus on exactly those steps, including a tailored maturity model to help companies assess and elevate their security posture over time, followed by detailed action plans in key control areas. With a strategic roadmap and prioritization, emerging and mid-sized companies can escape reactive survival mode and build genuine cyber resilience despite their constraints. The journey begins with understanding where you are on the security maturity curve.

Password Management:
A Strategic Pillar of Zero Trust

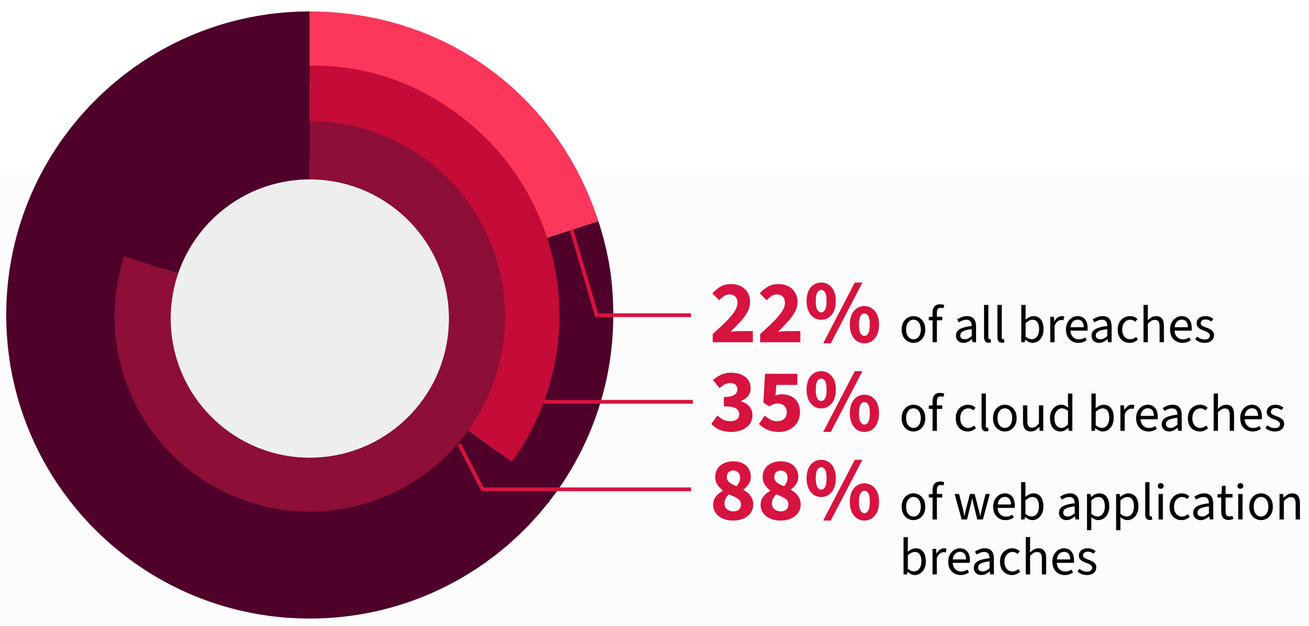
The foundational element of any cybersecurity strategy is ensuring that the “keys to the kingdom” — digital credentials — are created, stored, and managed securely. The 2025 Verizon DBIR found that stolen credentials were used in 22% of all breaches and in 88% of web application breaches. CrowdStrike’s 2025 Global Threat Report revealed that 35% of cloud breaches involved valid account abuse, while Mandiant’s M-Trends 2025 report identified credential theft as the second most common initial infection vector.

This is not an anecdotal risk; the data is overwhelming and consistent across sources.

Weak, reused, or unmanaged credentials are an existential organizational threat, not just a user-level issue. Emerging and mid-sized companies and large enterprises alike experience similar rates of credential-related breaches, meaning attackers do not discriminate by size when targeting identity systems. Once credentials are compromised, attackers often bypass traditional malware defenses entirely, blending into regular traffic and avoiding detection.

Enterprise-grade password management addresses these systemic weaknesses by enforcing unique, complex passwords, centralizing credential storage in secure vaults, integrating with MFA, and enabling rapid credential recall in the event of compromise. Password managers also allow organizations to monitor exposed credentials on the dark web or in infostealer dumps, closing the window of opportunity before an attacker can act.

stolen credentials were used in:



The ROI is compelling. IBM's 2024 Cost of a Data Breach Report showed that **breaches caused by stolen credentials cost nearly 10% more than the average breach, while organizations using password managers combined with MFA reduced their likelihood of credential-related violations by 60%.** For emerging and mid-sized companies, this can mean the difference between surviving a cyberattack and closing their doors.

In the cryptocurrency sector, the stakes are even higher. Chainalysis reported that over $1 billion in crypto thefts in 2023–2024 were directly tied to credential compromises. Because blockchain transactions are irreversible, the compromise of hot (digital) wallet keys or admin credentials often results in instant, unrecoverable losses. Secure password management, paired with hardware-based MFA, is not optional in this sector — it is critical.

From a Zero Trust (never trust, always verify) perspective, NIST SP 800-207 emphasizes the importance of high-assurance credentials as the foundation for continuous authentication. CISA's Zero Trust Maturity Model requires eliminating unmanaged or shared credentials as organizations advance in maturity.
By deploying password management solutions that ensure credential uniqueness, protection, and governance, organizations move decisively toward Zero Trust maturity.

A practical maturity metric for this domain is the percentage of enterprise credentials stored in a centrally managed, access-controlled password vault: less than 25% indicates low maturity, 25–75% shows developing maturity, and over 90% reflects a mature, Zero Trust-aligned state. **This metric enables organizations to quantify their progress and establish specific targets for improvement.**

Secure password management is not just good hygiene — it is a measurable, enforceable, and strategically essential control that directly impacts breach likelihood, detection speed, and business continuity. The easiest door to the world of compromise is via bad passwords and bad password management. The only thing any business has to do to close that door is use technology to solve the password management issue. In cybersecurity, the one apparent need that is well managed by a simple technical control is the password.

The Cybersecurity Maturity Model:
A Roadmap for Progress

One useful concept for an organization looking to improve its security is a maturity model – a framework that defines levels or stages of capability. By assessing their current level and identifying what's needed to reach the next level, emerging and mid-sized companies can methodically upgrade their cybersecurity posture. Below is a five-level cybersecurity maturity model tailored explicitly for the environments of emerging and mid-sized companies.

This new model is called the The Cyber Resilience Index (CRI). On the follow-on attachment, there is a code sample and fundamental tool for smaller companies to design their own CRI.

This new emerging and mid-sized companies focused model draws inspiration from established frameworks (like the NIST Cybersecurity Framework and the US Department of Defense's Cybersecurity Model Certification (CMMC)) but is simplified and oriented to the realities of small business operations.

Progression should be risk-driven and resource-aligned – not every small business will need Level 5 capabilities. Still, every company should strive not to be stuck at Level 1 or 2, given today's threat environment.

Level 1
Initial

Level 2
Basic

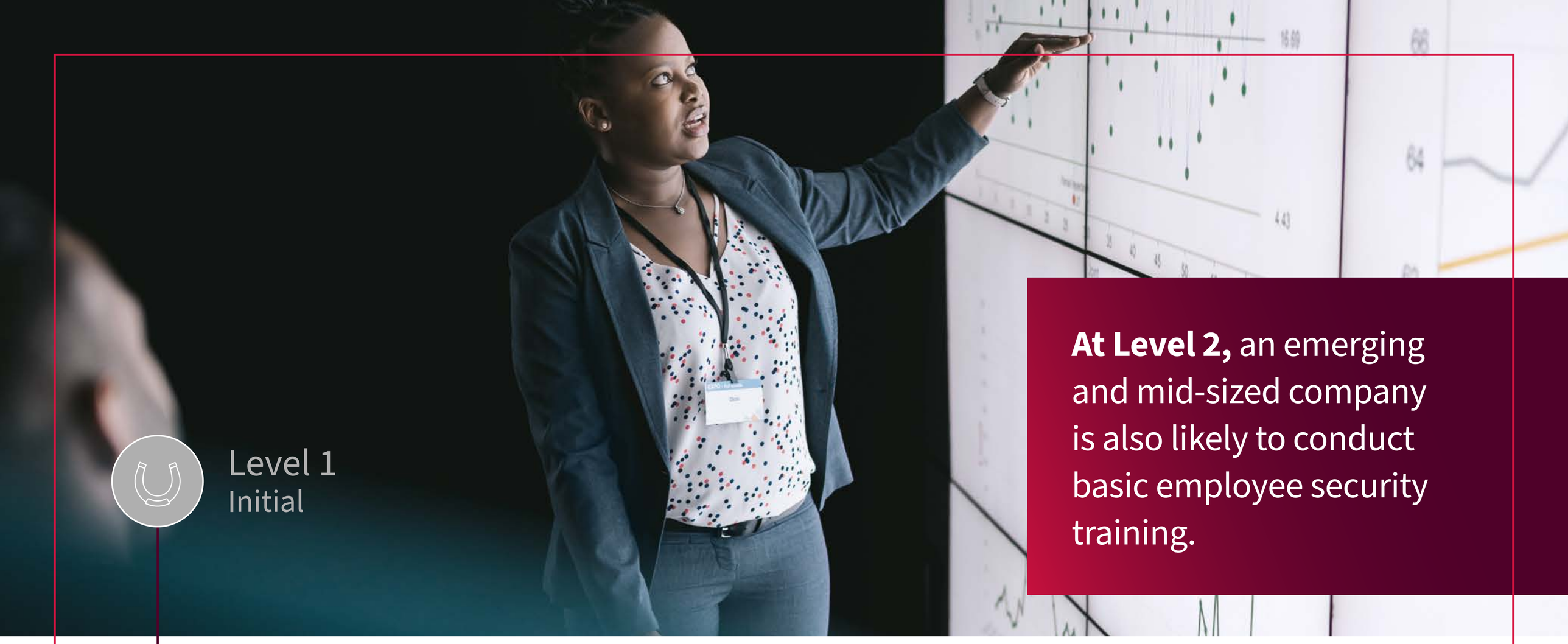
Level 3
Intermediate

Level 4
Advanced

Level 5
Optimal

INITIAL (AD HOC): Security is minimal or reactive. The company may not have any dedicated IT security personnel. **Controls are mainly limited to whatever comes out of the box:** perhaps a basic firewall on the office router, consumer-grade antivirus on PCs, and default security settings on SaaS apps. **There are no written security policies.** Patching and backups are sporadic, left to individual IT staff or vendors without central oversight. **Users might be reusing weak passwords,** and there is likely no multi-factor authentication. At this stage, the organization's approach could be described as "hope and luck" – hoping that nothing bad happens and reacting ad hoc if it does. Unfortunately, many micro-businesses and startups begin here, sometimes not moving until a painful incident occurs.

At Level 1, security is minimal or reactive, and the company may not have dedicated IT security personnel.



At Level 2, an emerging and mid-sized company is also likely to conduct basic employee security training.

Level 1
Initial

Level 2
Basic

Level 3
Intermediate

Level 4
Advanced

Level 5
Optimal

BASIC (DEFINED CONTROLS FOR KEY RISKS): The organization has recognized the need for cybersecurity basics and has implemented foundational protections, although execution may be uneven. There is now at least an informal **security plan or policy** covering the essentials (acceptable use policies, password rules) – a big step up from Level 1. The most critical controls are put in place: for example, **enabling multi-factor authentication for email and critical applications** (a response to the prevalence of credential attacks), deploying reputable anti-malware/endpoint protection on all systems, and setting up regular data backups.

At Level 2, an emerging and mid-sized company is also likely to conduct basic employee security training (perhaps an annual briefing or distributing security tips) to raise awareness of phishing and social engineering. Patching of systems happens occasionally or with external prompting (e.g., the IT provider updates servers monthly, or Microsoft updates are on auto-install). While still largely reactive, the company has at least defined who is responsible for IT security tasks and addressed the “low-hanging fruit” controls. Many small businesses in regulated industries or those that’ve passed a security audit reach this stage, covering requirements like antivirus, firewalls, and basic policies.

Level 1
Initial

Level 2
Basic

Level 3
Intermediate

Level 4
Advanced

Level 5
Optimal

Level 3
organizations have moved from purely defensive to detect and respond capabilities, albeit with limited scope.

INTERMEDIATE (PROACTIVE AND MANAGED): The organization moves into a proactive posture. Security processes are documented and managed. Notably, the emerging and mid-sized companies have implemented a broader set of controls and **begun monitoring their environment regularly.** At Level 3, one would expect to see: **centralized logging and alerting** (maybe using cloud Security and Information Event Management (SIEM) or an MSP's monitoring service) to catch suspicious activity; a vulnerability management process (with periodic scans and a schedule for applying critical patches – addressing the rise in exploits of known flaws); and stricter access controls, such as **role-based access and periodic user access reviews.**

Importantly, security awareness efforts are ongoing – for instance, the company might run phishing simulation tests for employees and track improvement. There may be an incident response plan on paper, and the company may have even practiced a basic incident drill or a ransomware tabletop exercise. Backups are verified and include offsite/cloud copies (aligned to the 3-2-1 rule: three copies of data, on two different types of media, with one copy stored offsite) so that ransomware can't easily destroy them. At this stage, smaller companies likely leverage external expertise heavily: e.g., a **managed security service** (MSS) or a virtual chief information security officer (CISO) consultant guiding their program. Overall, Level 3 organizations have moved from purely defensive to detect and respond capabilities, albeit with limited scope. Many medium-sized businesses (100-500 employees) aim to be at least at this maturity level.

Level 1
Initial

Level 2
Basic

Level 3
Intermediate

Level 4
Advanced

Level 5
Optimal

At Level 4, security monitoring is 24/7, either via an in-house Security Operations Center or a Managed Detection and Response (MDR) service, ensuring that alerts from EDR or network logs are promptly investigated.

ADVANCED (ROBUST AND ALIGNED WITH BEST PRACTICES):

Security is now a significant, continuous function in the business. The organization's practices align well with the industry's best practices and compliance standards. **All high-value data is protected with strong measures.** For example, sensitive customer data is encrypted at rest and in transit, and perhaps tokenized (replacing sensitive data with non-sensitive, unique tokens), so that a breach won't easily expose plain text records (embracing the "devalue data" principle). There is a formal incident response team or retained IR firm on standby, and the company conducts regular incident response exercises (at least annually) with executive participation, so that when an incident occurs, they can react quickly and effectively. Security monitoring is 24/7, either via an in-house Security Operations Center or a Managed Detection and Response (MDR) service, ensuring that alerts from EDR or network logs are promptly investigated.

Organizations at this level often invest in **endpoint detection and response tools on all devices** and ensure they are tuned correctly; any alerts that trigger after hours will be caught by the MDR team (significantly reducing mean time to respond by ~50% as studies show, according to IBM. At Level 4, **multi-factor authentication is widespread** for all users and apps (ideally using phishing-resistant methods like FIDO2 security keys). The company likely has network segmentation deployed, separating critical servers or production environments from the corporate network to contain breaches. They also actively manage vendor risk: performing due diligence on partners, requiring contracts with security clauses, and monitoring third-party access. Security metrics are reported to top management regularly, and a culture of security is integrated into decision-making processes. This is a mature stage that relatively few emerging and mid-sized companies reach – those that do often have strong regulatory drivers (e.g., handling credit cards, health data, or operating in the finance sector) or enlightened leadership that has invested heavily in security.

OPTIMAL (ADAPTIVE AND RESILIENT): This is the pinnacle where an emerging and mid-sized company's security is on par with leading practices of large enterprises, albeit scaled to its size. The company at Level 5 anticipates threats and continuously improves. Threat intelligence feeds inform adjustments to defense; the security team (internal or external) actively hunts for signs of attackers in the network, even without alerts. The organization has likely embraced **Zero Trust principles** – meaning identity is verified for every access, devices are validated as healthy, and lateral movement is tightly restricted by design. Advanced technologies like **behavioral analytics and AI-based defenses** might be in use, both to detect anomalies (e.g., unusual login patterns) and to automate response (like isolating a machine that's behaving suspiciously within seconds).

Level 2
Basic

Level 3
Intermediate

Level 4
Advanced

Level 5
Optimal

The company at Level 5 **anticipates threats and continuously improves.**

At this level, the company not only has encrypted and backed up its data but also has **resilience plans to operate through an attack,** for instance, having manual workarounds or secondary systems if primary IT is locked by ransomware. Business continuity and cybersecurity are fully integrated. Security considerations are embedded in all projects ("secure by design" mindset). Very few emerging and mid-sized companies will attain this level of maturity, and it's not always necessary to reach it. However, aiming for Level 5 in critical areas can be a strategic advantage, especially for emerging and mid-sized companies that are tech companies or data custodians, where trust is a differentiator.

This maturity model provides an outline for emerging and mid-sized companies to **identify their current state and target a higher state.** For example, a 50-person company might assess that they are at Level 2 (Basic) currently – they have antivirus, some MFA, and backups, but no monitoring or IR plan. Their goal for next year could be reaching Level 3: implementing log monitoring via a managed service, running quarterly phishing drills, and formalizing an incident response plan. For each level, the investments and effort roughly increase, but so do the risk mitigations. The following section breaks down concrete security controls and practices (many mentioned in the maturity model) into actionable recommendations. Emerging and mid-sized companies can use these as building blocks to move up the maturity curve, achieving a stronger security posture step by step.

Action Plan:
How to secure your business, from one employee to 1000.

Translating insights from breach reports into practical applications, this section outlines specific security actions for emerging and mid-sized companies.

The security domain organizes these recommendations. Taken together, they form a comprehensive defense strategy. Small and scaling businesses should prioritize implementing these measures based on their risk profile and maturity; however, all are essential components of the puzzle. Where possible, data or expert insight is cited underscoring why each control matters for smaller companies in 2025 and beyond.

1. Strengthen Identity and Access Management (IAM)

2. Enhance Security Awareness and Training

3. Secure Email and Communication Channels

4. Defend Endpoints and Networks

5. Implement Rigorous Patch and Vulnerability Management

6. Backup Data and Test Recovery

7. Develop an Incident Response Plan and Practice It

8. Protect and “Devalue” Sensitive Data with Cryptography

9. Leverage External Security Expertise and Services

1. Strengthen Identity and Access Management (IAM)

Manage who can get into your systems, because credential abuse is rampant.

Stolen or weak credentials were the most popular “unauthorized gateway” to private data last year, according to Verizon. To counter this:

- **ENFORCE MULTI-FACTOR AUTHENTICATION (MFA) ON ALL CRITICAL ACCOUNTS:** If there is one single improvement an emerging and mid-sized company should make immediately, it is to enable MFA for email, remote logins, banking platforms, and cloud services. With passwords alone so often compromised, adding a second factor (one-time code, mobile app prompt, or hardware key) stops most automated account hijacks. As Coalition’s security engineers note, requiring two or more forms of verification means attackers “can’t achieve their goals with compromised credentials alone.” Wherever possible, use an authenticator app or hardware-based MFA rather than SMS texts (which can be spoofed or SIM-swapped). Many emerging and mid-sized friendly software-as-a-service (SaaS) apps integrate easily with free authenticator apps.

- **UPGRADE TO PHISHING-RESISTANT MFA (FIDO2 AND MODERN SOLUTIONS):** Traditional MFA (e.g., SMS codes or app push prompts) can be phished – attackers can trick users into giving up the code or approving a fake login. To get ahead of this, consider **FIDO2 security keys or platform biometrics** (Windows Hello, Touch ID) for employee logins. FIDO2 (Fast Identity Online 2) is a standard where authentication is tied to the device and user via cryptographic keys, and it’s currently the “gold standard” in MFA. For instance, a YubiKey or built-in biometric that adheres to FIDO won’t send a reusable code that a phisher can steal; it automatically verifies the service, so lookalike sites can’t trick it.

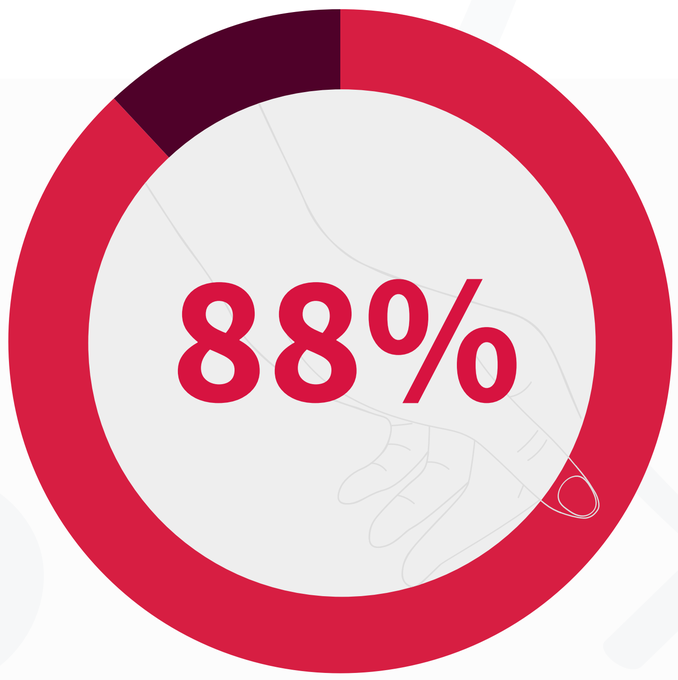
These technologies have become more affordable and user-friendly – many laptops and phones already have compatible hardware (fingerprint readers). Adopting phishing-resistant MFA significantly reduces the risk from sophisticated phishing and man-in-the-middle attacks, which are rising. While not every emerging and mid-sized company may roll out security keys overnight, planning for a gradual move to stronger MFA for high-risk users (admins, finance, executives) is wise.

- **ADOPT ROBUST PASSWORD POLICIES AND MANAGEMENT:** Even with MFA, passwords still matter (especially where MFA isn't yet in place). Enforce strong password requirements (length and complexity, or even better, passphrases) and discourage reuse of passwords across accounts. **Regularly prompt users to change default passwords** on any new devices or applications – many breaches still occur because growing companies never change the default admin password on a router or database. Use a password manager solution to help employees generate and securely store complex passwords, reducing the temptation to reuse the same password. Additionally, **monitor for exposed credentials** belonging to your domain (some services scan breach dumps for your company's emails/passwords). If an employee's work credentials show up in a leak, have them change it immediately. Given that 88% of web app breaches involve stolen credentials, catching leaked passwords before attackers use them is essential (Verizon, 2025).

Quick Tip: Enforce strong password requirements (length and complexity, or even better, passphrases) and discourage reuse of passwords across accounts.

- **IMPLEMENT PRINCIPLE OF LEAST PRIVILEGE:** Audit your user accounts and access rights. Each employee should have the minimum access necessary for their role – no one should casually have domain administrator or financial system access unless required. Remove or restrict shared accounts. If possible, use unique accounts for each user (avoid generic logins) and eliminate accounts that are no longer needed (former employees, old contractors). Many emerging and mid-sized companies' breaches involve attackers finding an orphaned admin account or using a standard user account that has unnecessary high privileges. By limiting privileges, even if an account is compromised, the damage can be contained. For example, a user with no access to the accounting system can't facilitate a fraudulent funds transfer if phished.

of web app breaches
involve stolen credentials
catching leaked passwords before attackers use them is essential

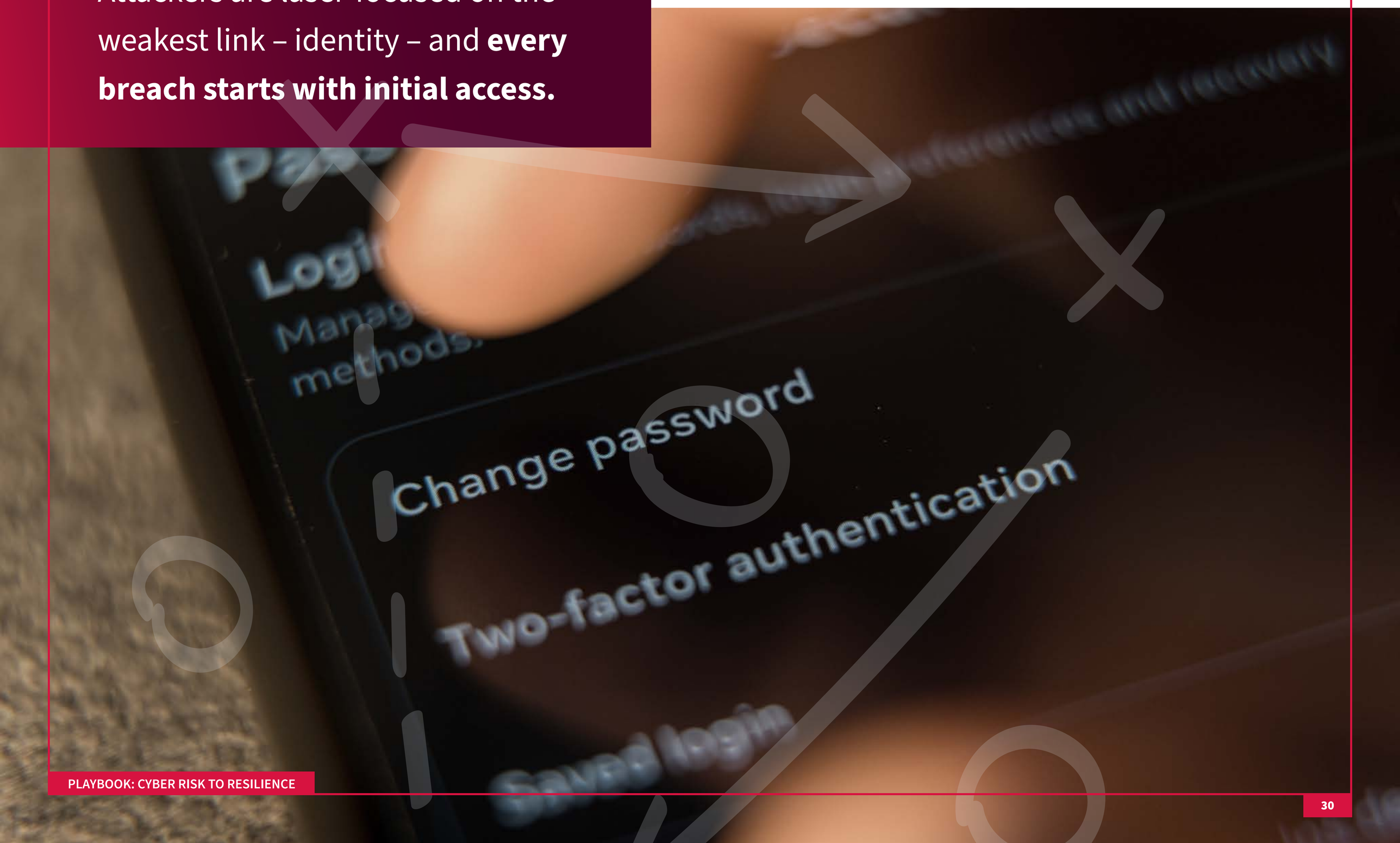


USE IDENTITY AND ACCESS MANAGEMENT (IAM) TOOLS AS YOU GROW:

For emerging and mid-sized companies with dozens of employees, manual account management becomes error prone. Consider using an IAM or directory service (like Azure AD, Okta) to manage authentication and single sign-on (SSO) centrally to all your apps. These platforms can enforce MFA, password policies, and let you immediately disable all access for a departing employee – critical for preventing accidental insider risks. They also often include anomaly detection (alerting if an account logs in from an unusual location or device). Some advanced solutions even monitor for **impossible travel (logins that suggest the credential was stolen)** or other identity threats. While these might sound enterprise-grade, many providers have emerging and mid-sized companies' packages, or there are open-source solutions for the basics.

Securing identity is priority #1. As CrowdStrike's report puts it, attackers are laser-focused on the weakest link – identity – and every breach starts with initial access. By hardening authentication and access controls, emerging and mid-sized companies can shut down the most common intrusion paths. It's worth noting that many cyber insurers now *require* MFA for email and remote access before issuing a policy, which underscores how fundamental this control has become in risk management.

Attackers are laser-focused on the weakest link – identity – and **every breach starts with initial access.**



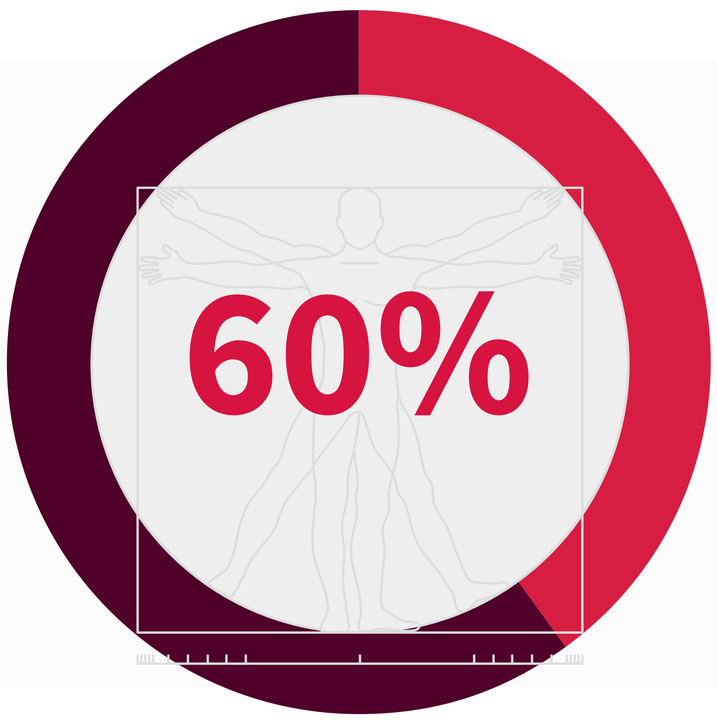
2. Enhance Security Awareness and Training

Technology defenses alone are not enough when social engineering is so prevalent. **Employees are the frontline of defense** against phishing, impersonation, and fraud attempts. Investing in their awareness and caution can bring considerable returns in risk reduction. Key steps include:

- **CONDUCT REGULAR SECURITY TRAINING:** Provide training for all staff at least annually (and ideally with ongoing smaller trainings throughout the year). Topics should include how to recognize phishing emails, suspicious links or attachments, and common scam tactics (like fake tech support calls or urgent requests for money). Importantly, cover procedures: teach employees what to do if they suspect a phishing attempt, e.g., how to report it to IT/security. Organizations with regular security awareness programs see tangible benefits; the DBIR noted companies with frequent training saw **phishing reporting rates improve fourfold** (employees became four times more likely to report phishing emails rather than clicking). Another study found that practical training can **reduce cyber incident risk by 60% within a year.** These are easy wins for emerging and mid-sized companies: even if you can't afford fancy tools, you can educate your people using free or low-cost training content from reputable sources (there are many cybersecurity awareness toolkits available from government agencies and vendors).

- **SIMULATE PHISHING ATTACKS:** It's one thing to tell employees about phishing, but quite another to have them experience realistic simulations. **Running phishing simulation exercises** involves sending fake but harmless phishing emails to staff to see who clicks. When someone does, it becomes a teachable moment (usually, they're redirected to a short training or notified of the mistake). This hands-on practice significantly boosts vigilance. As one incident responder noted, *"running phishing simulations builds your employees' confidence in spotting and escalating suspicious emails."* Over time, users get better at recognizing the telltale signs of phishing – mismatched sender addresses, generic greetings, unusual urgency. The goal isn't to shame employees but to normalize reporting. Employees should feel it's a positive thing to report a possible phishing email, even if it turns out **to be a false alarm.** Celebrating those who successfully identify phishing tests can reinforce the culture. For emerging and mid-sized companies, affordable phishing simulation services exist, or an IT partner can conduct them. The result is a more cyber-savvy workforce that acts as a human sensor network to catch attacks early.

- **INSTILL A SECURITY CULTURE:** Foster an environment where security is essential to everyone's role. This means top leadership needs to openly prioritize security (if the CEO is the first to complete training and talks about its importance, employees listen). Make it clear that people won't be punished for reporting incidents or mistakes – you want them to speak up. Simple practices, such as including security tips in company newsletters or hosting a "cybersecurity month" awareness campaign, can help keep knowledge fresh. Given that the human element (errors, social engineering, misuse) accounts for 60% of breaches, according to Verizon, cultivating a healthy security culture is arguably as critical as any hardware you can buy. One practical example: establish a process for verifying unusual requests. If an employee receives an urgent email from the CEO requesting gift card codes (a common scam), they should be empowered to verify the request through an alternative channel. Make "trust but verify" a mantra – verify requests for fund transfers or sensitive data via a quick phone call or face-to-face check. Attackers often exploit fear and urgency; a culture that encourages verification can lessen that.

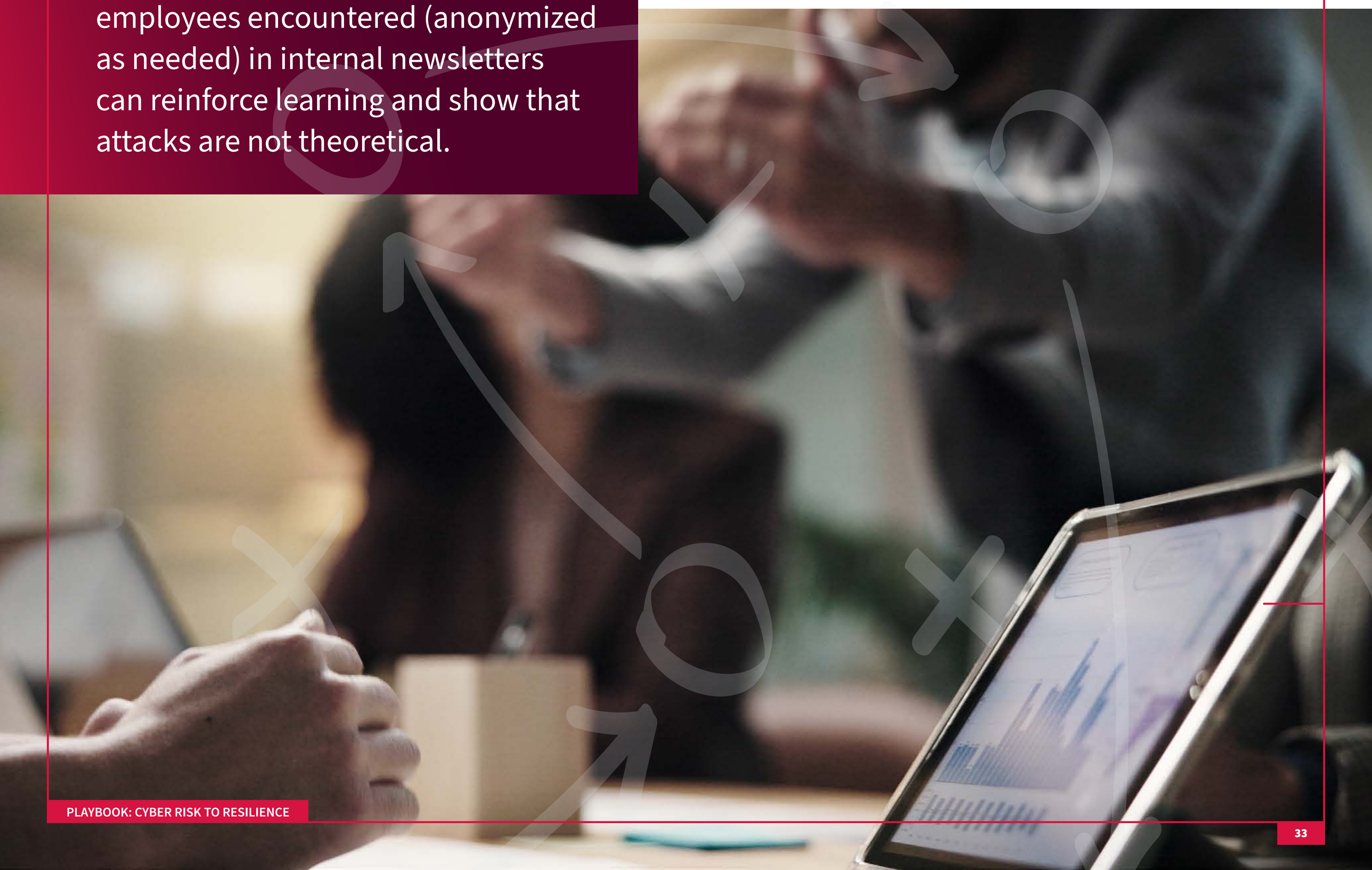


- **EXPAND AWARENESS TO NEW THREATS (VISHING, DEEPFAKES):** As attackers innovate, so too must training content. Ensure employees know that phishing isn't just email – it can be **phone calls (vishing)** or text messages (smishing). The surge in voice phishing means staff may receive calls from someone pretending to be IT support, asking for MFA codes or passwords. They should be trained never to share this information over the phone and to contact the supposed caller's organization if they are unsure independently. Additionally, make employees aware of the possibility of **deepfake audio/video scams.** For example, if they get an odd voicemail from a company executive making an unusual request, it could be an AI-generated fake. While this is cutting-edge, early awareness can foster healthy skepticism of "urgent" messages. The overarching point is to educate that **attacks may come in any communication form** – email, phone, messaging apps, even physical visits – and the same principles of caution apply.

- **LEVERAGE METRICS AND FEEDBACK:** Track the outcomes of training and simulations. What percentage of users clicked on phish simulations last quarter versus this quarter? Are specific topics confusing people? Use this data to refine your program. Also, gather feedback from employees: what suspicious emails or calls have they received? Sharing real examples that employees encountered (anonymized as needed) in internal newsletters can reinforce learning and show that attacks are not theoretical – “last week, one of our team members received a convincing scam email; here’s how they spotted it.” This peer sharing makes the threat more tangible and the desired response clearer.

An aware and vigilant workforce is one of the best defenses an emerging and mid-sized company can have. Technology can’t stop every social engineering ploy – at some point, a user’s decision stands between the attacker and success. By educating and empowering your people, you strengthen that human firewall. And as the Verizon DBIR observed, organizations that commit to security awareness that is combined with solid security controls and policy-level controls see measurable reductions in incidents.

Sharing real examples that employees encountered (anonymized as needed) in internal newsletters can reinforce learning and show that attacks are not theoretical.



3. Secure Email and Communication Channels

Email continues to be a primary vector for cyberattacks, from phishing and malware delivery to business email compromise (BEC) scams. **Most cyber attacks originate in the inbox.** For emerging and mid-sized companies, protecting email accounts and usage is critical because a compromise here can lead to many downstream harms (fraudulent money transfers, data theft, malware infiltration). Key practices include:

- **IMPLEMENT STRONG EMAIL SECURITY GATEWAYS/FILTERS:** Utilize a reputable email security service or gateway to filter out spam, malicious attachments, and phishing emails. Modern email security products employ multiple detection techniques techniques:
  - Blocking known dangerous senders
  - Looking for suspicious patterns or behaviors
  - Sandboxing for attachments (safely opening these attachments in a controlled environment)

  These techniques can drastically cut down the volume of threats reaching users' inboxes. Even the default filtering in platforms like Microsoft 365 or Google Workspace, when properly configured, is quite effective at blocking obvious phishing and junk. Tune the filters to be as aggressive as practical – blocking emails with executable attachments, macro-laden Office documents, or known phishing keywords (like "urgent payment") can stop "low-hanging fruit" attacks. Just remember to review quarantined messages periodically so legitimate mail isn't lost. This first line of defense is essential, but not foolproof, so it must be coupled with user awareness as discussed.

- **ENABLE EMAIL AUTHENTICATION (SPF, DKIM, DMARC):** Work with your IT provider to set up Sender Policy Framework (SPF), Domainkeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, Conformance (DMARC) records for your domain. These email authentication protocols help prevent attackers from spoofing your domain in emails. For example, DMARC can tell recipients to reject emails that aren't verified to come from your domain. While this doesn't stop inbound phishing, it does protect your brand and partners from fake emails that appear to come from you. It also provides reports so you can see if someone is attempting to abuse your domain. Additionally, using these standards can slightly improve how other mail systems treat your emails (less likely to be flagged as spam). Implementing them is a one-time effort that can result in long-term benefits in the war against email fraud.

- **PROTECT AGAINST BUSINESS EMAIL COMPROMISE (BEC):** BEC is a form of targeted phishing where the attacker often compromises an email account (sometimes a vendor or customer of yours) and then uses that trusted account to insert themselves in business communications (e.g., altering an invoice to redirect payment). To reduce BEC risks:

    - **Set up payment verification procedures:** For any financial transaction requests received over email, especially wire transfers, bank detail changes, and large invoice payments, require an out-of-band verification (authentication using a separate communication channel). That could mean a phone call to a known number for the person, or confirmation from two people. This process should be formalized so that even if an email looks legitimate, finance personnel know a secondary check is mandatory.

As one expert noted, the days of obviously fake “Nigerian prince” emails are over; today’s BEC actors will compromise a vendor’s actual email account, learn context like your colleagues’ names or ongoing projects, and then send a perfectly tailored fraudulent invoice. Only a vigilant process of verification will catch that something is off.

    - **Monitor email account activity:** Many email providers allow admin oversight of unusual login activity (e.g., alerts if an account logs in from a new country). Ensure those alerts are on and being watched. Also consider employing rules that **flag emails with certain red flags** – for instance, if an email’s reply-to differs from the sender (a common phishing tactic), or if an external email is impersonating an internal sender name. Some advanced email security solutions will detect “CEO impersonation” attempts or BEC patterns. For emerging and mid-sized companies using Microsoft 365, enabling features like Defender for Office 365 can catch these types of attacks.

    - **Educate employees about BEC by including a BEC scenario in training.** This scenario should illustrate that an attacker can still hijack an email thread with a known partner, and any urgent requests to change payment details or send money should be treated with skepticism. Encourage staff to slow down and consult a second person if they have any questions. Many costly scams could be stopped if the employee just took a breath and double-checked with a colleague or the supposed sender via phone. This scenario should illustrate that an attacker can still hijack an email thread with a known partner, and any urgent requests to change payment details or send money should be treated with skepticism.

- **SECURE YOUR EMAIL ACCOUNTS WITH MFA AND GOOD HYGIENE:** This overlaps with identity management but bears repeating here: ensure every email account (especially for high-privilege users like executives or the finance team) has MFA enabled. Cloud email accounts are prime targets; without MFA, a phished or leaked password means instant email breach. Also, periodically review mailbox forwarding rules (attackers who get into an email often set up hidden forwarding to Gmail accounts to monitor conversations). Disallow automatic forwarding to external domains at the admin level if possible, or at least review it. Keeping your email system access tight will prevent many incidents from **getting out of control.**

- **CONSIDER DATA ENCRYPTION FOR SENSITIVE EMAILS:** If your business regularly transmits highly sensitive information via email (e.g., personal data, confidential designs), investigate using encryption tools or secure messaging alternatives. Many email platforms have an option to send an “encrypted message” or use OME (Office Message Encryption), which ensures only the intended recipient can open it (they might need to log in to a portal). While this may be overkill for routine communications, for use cases it’s worth the extra step. At a minimum, never send passwords or similarly sensitive credentials over email in plain text – use a phone call or a secure file share if you must share these.

In essence, treat email as the high-risk asset it is. It’s not just correspondence – it’s an entry point to your organization and store of valuable data (executives’ communications, customer info). By hardening email security and establishing strict processes around email-based requests, emerging and mid-sized companies can eliminate a vast array of threats. Remember that many attackers won’t bother hacking your firewall if they can simply trick someone into opening the door or sending money via email. Cutting off that route is a top priority.

Treat email as the high-risk asset it is. It’s not just correspondence – it’s an entry point to your organization and store of valuable data (executives’ communications, customer info).

4. Defend Endpoints and Networks (Detection and Response)

Every device on your network – laptops, desktops, servers, even Internet of Things (IoT) devices – is a potential target. With so many attacks being “malware-free” and using legitimate tools once inside, having visibility into endpoint and network activity is crucial for detecting breaches. Key measures in this domain:

> Having visibility into endpoint and network activity is crucial for detecting breaches.

- **DEPLOY ADVANCED ENDPOINT PROTECTION (EDR/XDR):** Traditional antivirus, which relies on known virus signatures, is not enough for modern threats. Invest in an Endpoint Detection and Response (EDR) solution or its broader cousin, Extended Detection and Response (XDR), which can cover endpoints and cloud workloads. These tools use behavioral analysis to identify suspicious activities on devices. For example, if a process starts dumping passwords from memory or launching a sequence of unusual commands, the EDR can flag or stop it. In many cases, EDR has been effective at catching ransomware early in the encryption phase or detecting hacker tools that antivirus software misses. Products from vendors like CrowdStrike, SentinelOne, and Microsoft Defender for Endpoint are popular.

For **smaller companies,** the challenge is not just deploying EDR but **managing the alerts** – these tools can generate a high volume of signals that require analysis. That leads to the next crucial step: consider a **Managed Detection and Response (MDR)** service. MDR providers have security analysts who monitor your endpoint and network alerts 24/7, investigate them, and even directly contain threats. This is an excellent option for emerging and mid-sized companies that can’t staff a Security Operations Center (SOC) around the clock. Studies indicate that companies with MDR in place can cut their response time roughly in half on average, minimizing damage. Many MDR services are priced per device and scale down to small business sizes. The Vijilan ThreatRemediate service, for instance, bundles CrowdStrike EDR with 24/7 SOC support specifically for emerging and mid-sized companies’ clients. Whether via an MDR or an internal person, ensure someone is actively watching and responding to endpoint alerts – **unmonitored EDR is like an alarm system blaring in an empty building.**

- **KEEP ENDPOINTS PATCHED AND CONTROLLED:** Basic endpoint hygiene is still fundamental. Configure automatic updates for operating systems and standard software where feasible – this addresses many vulnerability exploits that attackers rely on being unpatched. Utilize a centralized patch management tool or service if you have a large number of devices. Ensure all devices have a host firewall enabled (modern operating systems have this by default – just don't turn it off). Limit administrative rights on endpoints: employees should not all be running as local admins on their PCs, as that makes malware's job easier. Instead, have a separate admin account for IT tasks.

Additionally, consider **device encryption** (BitLocker on Windows, FileVault on Mac) so that if a laptop is stolen, the data isn't exposed (since it has been transformed into an unreadable format). This ties into cryptographic controls and often satisfies compliance requirements. Most modern systems have encryption capabilities built in – it usually just needs to be enabled, and recovery keys stored safely.

Ensure all devices have a host firewall enabled. Modern operating systems have this by default – just don't turn it off.

- **NETWORK SECURITY AND SEGMENTATION:** While many emerging and mid-sized companies have migrated to cloud services, there's usually still an on-premises network (office Wi-Fi, some local servers or network attached storage (NAS)). Protect the network using a business-grade firewall or Unified Threat Management (UTM) appliance. These devices can filter malicious traffic, block known bad IPs, and enforce VPN access for remote connections. Ensure Wi-Fi networks are secured (WPA2 or WPA3 encryption, strong unique passphrases) and, if possible, segregate a guest Wi-Fi from the internal network. For slightly larger emerging and mid-sized company environments, implement basic **network segmentation:** for example, separate the accounting system or point-of-sale network from the general office network, so that an infection on an employee's PC doesn't immediately have access to critical servers.

At a minimum, isolate backups and management interfaces to a restricted subnet. This way, if malware spreads, it might hit a firewall barrier. Attackers often try to move laterally once inside; segmentation can trip them up or contain the blast radius.

- **LOGGING AND INTRUSION DETECTION:** Turn on logging features on your systems and network devices. Key events – such as Windows event logs, VPN login logs, and firewall connection logs – should be retained and preferably aggregated to a central log management system (even if it's just a syslog server or a cloud service). These logs are invaluable for detecting suspicious behavior (like repeated failed logins or connections to known malicious domains) and for forensic analysis if an incident occurs. For emerging and mid-sized companies that cannot dedicate people to watch logs, leveraging automated alerts or an MDR (as mentioned) is the solution. Additionally, consider deploying a simple **Network Intrusion Detection System (NIDS)** on your network – there are free or low-cost options (e.g., Zeek, Snort) that can sniff traffic and alert on known threat signatures or anomalies. Even a router that supports basic threat intelligence feeds (some Unified Threat Management (UTM) firewalls do) can add a layer of defense by blocking communications with known bad IPs or domains.

- **24/7 MONITORING THROUGH EXTERNAL PARTNERS:** Given the difficulty emerging and mid-sized companies have staffing nights and weekends, use external services for after-hours monitoring. Many MSPs offer some form of SOC as a service. If the budget is tight, at least set up automated critical alerts (for example, if your server or website goes down or if certain high-severity logs appear, have an alert sent to key personnel's phones). You don't want to find out Monday morning that your systems were breached Friday night. Early detection can be the difference between a contained event and a full-blown breach. To emphasize the importance, the average eCrime **"breakout" time (time from initial compromise to moving deeper into the network) is now just 48 minutes, according to CrowdStrike.** That means if you're not responding within an hour or two, the attackers could have already spread far. Rapid detection and response are a must, and if you can't do it internally, bring in help.

In short, **think beyond prevention and plan for detection and response.** Assume an attacker might slip past your preventative defenses (phishing click, unpatched software hole). What measures will you have in place to catch them and act? That's where endpoint monitoring, network security, and response planning come in. For emerging and mid-sized companies, the theme should be simplicity and outsourcing – use managed solutions to cover the complexity. The good news is that enterprise-grade endpoint and SOC services are increasingly available "as a service" to smaller businesses. By leveraging them, these companies can achieve a level of security monitoring that rivals far larger organizations, which is crucial given the speed and stealth of today's adversaries.

5. Implement Rigorous Patch and Vulnerability Management

Many attacks aren't sophisticated zero-days (unknown vulnerabilities); they often exploit known vulnerabilities in systems that victims simply failed to patch. With the vast increase in vulnerabilities being disclosed (over 22,000 in 2024 by August) (Qualys, 2024), it's understandable that emerging and mid-sized companies feel overwhelmed. However, many of those flaws will never be targeted by attackers – typically, bad actors zero in on a smaller subset of high-impact, easy-to-exploit holes, especially in externally facing systems. A sensible vulnerability management strategy can significantly reduce risk:

Many attacks aren't sophisticated zero-days (unknown vulnerabilities); they often exploit known vulnerabilities in systems that victims simply failed to patch.

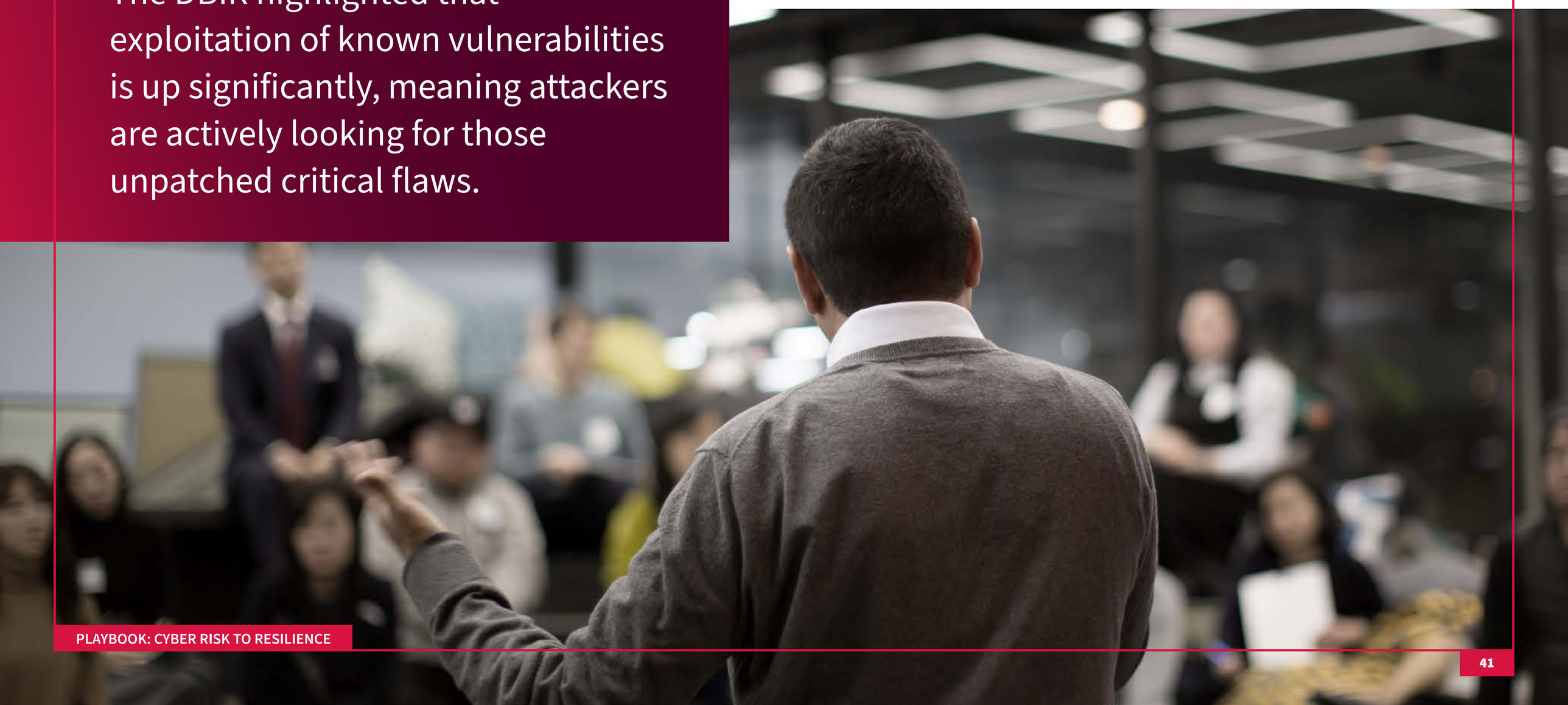
- **PRIORITIZE PATCHING OF EXTERNAL-FACING SYSTEMS:** Focus on anything in your network that's exposed to the internet – this includes your website, content management system (CMS), VPN gateway, email server, e-commerce platform, cloud servers. As one security engineer put it, **"anything that's exposed to the public internet should get your immediate attention"** when it comes to patching. These are the systems attackers will scan and hit first. Ensure you subscribe to security bulletins for those products and apply updates as soon as possible when critical vulnerabilities emerge. For example, if a crucial flaw in your firewall VPN is announced , treat it as an emergency – either apply the patch or if you cannot, temporarily shut off that service until mitigations are in place. Many 2024 breaches occurred via unpatched perimeter devices and VPN appliances.

- **KEEP SERVERS AND SOFTWARE UPDATED:** Maintain an inventory of all your software and periodically update it. This includes web server software, CMS like WordPress (which should be updated to the latest version, given the constant discovery of new common vulnerabilities and exposures), database software, and any frameworks your applications rely on. For desktops and laptops, enabling auto-updates for the OS and browsers is usually best. For specialized software that doesn't auto-update, set a monthly or quarterly schedule to check for updates. A patch management tool can automate a lot of this, installing updates during off-hours. The key is consistency: patching should be a regular, ongoing process, not just an annual fire drill.

- **USE VULNERABILITY SCANNING TOOLS:** Employ vulnerability scanning against your environment to identify and address security vulnerabilities. There are free scanners (like OpenVAS, Nessus Essentials) and paid ones that can monitor your network devices and systems for missing patches or misconfigurations. Running a monthly scan can identify forgotten exposures – for instance, that test server someone stood up last year that never got updated. Some managed security providers include regular vulnerability scanning in their packages for emerging and mid-sized companies. Also, consider utilizing free external scan services; for example, CISA offers a free vulnerability scanning service for US businesses, which can alert you if your internet-facing assets have known vulnerabilities.

- **ADDRESS "HIGH" AND "CRITICAL" VULNERABILITIES PROMPTLY:** Not all vulnerabilities are equal. Focus on addressing high-severity issues first, especially those with known exploits that have been actively used. The DBIR highlighted that exploitation of known vulnerabilities is up significantly, meaning attackers are actively looking for those unpatched critical flaws. Develop a patching SLA (service-level agreement) internal to your team: e.g., critical patches applied within seven days, high within 30 days. Lower severity can wait for standard maintenance windows. If a vital patch can't be used (due to compatibility or downtime constraints), implement compensating controls, such as temporarily disabling the vulnerable feature, increasing monitoring on the system, or isolating it from the internet until a fix can be applied. For instance, if an immediate patch isn't available for a critical bug, you might restrict access to the service via firewall rules as a stopgap.

The DBIR highlighted that exploitation of known vulnerabilities is up significantly, meaning attackers are actively looking for those unpatched critical flaws.



- **DON’T FORGET FIRMWARE AND SHADOW IT:** Ensure things like network equipment firmware (routers, IoT devices, printers) are also kept updated, as those can harbor vulnerabilities too. IoT and miscellaneous devices are often overlooked – create a checklist to review them periodically.

Conduct an inventory for any shadow IT – like an employee who set up a personal file-sharing server or a marketing team that uses an unvetted third-party SaaS tool. These unknowns can introduce vulnerabilities if not managed. Bring them into the fold or shut them down if unnecessary.

- **USE VIRTUAL PATCHING/SHIELDING IF AVAILABLE:** Some security tools and WAF (Web Application Firewalls) can provide virtual patching – rules that block exploitation of a vulnerability without patching the underlying software. For example, if your web server can’t be repaired immediately, a WAF might be configured to detect and block the specific attack signature targeting that flaw. This can buy you time. Similarly, endpoint security can sometimes thwart the exploitation of specific common vulnerabilities (like buffer overflow attacks, which overload the buffer’s allocated memory) generically. While not a substitute for real patching, these measures can reduce risk in the interim.

Remember, **vulnerability management is a continuous process, not a one-time project.** The dramatic breaches via unpatched systems (including many affecting emerging and mid-sized companies) show that “patch paralysis” can be fatal. Smaller companies may feel they lack time to patch, but the cost of not patching is far greater when an incident occurs. A pragmatic approach is to address the most critical issues first (those that are visible to the world) and establish a routine cadence for everything else. With cloud-based software and auto-updated features nowadays, patching can be more automated than in the past. Use those capabilities to your advantage so that staying up to date is the default. In doing so, you remove some of the easiest opportunities for attackers who breach your network.

Smaller companies may feel they lack time to patch, but the cost of not patching is far greater when an incident occurs.

6. Backup Data and Test Recovery (Prepare for Ransomware)

Reliable, accessible backups are the single most potent antidote to ransomware attacks. If you can quickly restore your data and systems from backups, you make the leverage of ransomware actors who try to extort you for decryption inefffective. However, achieving resilience through backups requires careful planning – modern attackers aim to **destroy or encrypt backups as part of their attack** (knowing this forces victims to pay). A survey found 94% of organizations hit by ransomware had their backups targeted by the attackers during the incident (Sophos, 2024). Emerging and mid-sized companies must implement backups in a way that anticipates these dirty tricks:

- **FOLLOW THE 3-2-1 BACKUP RULE:** This classic rule remains highly relevant: keep at least three copies of your important data (production data and two backups) on two different media, with one copy stored offsite (or offline). For example, you might have one backup on a local NAS device and another backup in a cloud storage service. The idea is to diversify so that a single event (like a fire or a ransomware infection) can't wipe out all copies. **One backup should be isolated** – either offline (disconnected except when running backups) or immutable (write-once storage that malware can't alter).

Many cloud backup providers now offer immutable backup options or retention locks that prevent deletion for a set period. Use these features so that even if an attacker gains domain admin rights, they can't simply delete all backup files.

- **USE CLOUD OR OFFSITE BACKUPS FOR REDUNDANCY:** For emerging and mid-sized companies, leveraging cloud backup services is often the easiest way to get an off-site, secure backup. For instance, back up critical servers or data to a cloud service like Amazon S3, Azure Backup, Backblaze, or specialized backup providers. Ensure the cloud backup account is secured with MFA and not broadly accessible. If you prefer physical backups, then rotate copies offsite (e.g., periodically copy data to an external drive and store it securely off-premises). The key is that a ransomware infection in your network should not be able to reach and encrypt every backup copy. Storing data in a different environment (cloud or offline) helps guarantee that.

- **AUTOMATE AND SCHEDULE BACKUPS FREQUENTLY:** Aim for daily backups (or more frequent incremental backups) of critical data. Ransomware can strike at any time; you don't want the only good backup to be two weeks old. Determine the Recovery Point Objective (RPO) that is acceptable – how much data could you afford to lose? For many businesses, losing even one day's worth of transactions or work is painful, so nightly backups are a minimum. There are many affordable backup solutions for emerging and mid-sized companies that can automate this process for files, databases, and even take full machine snapshots. Set them to run after hours or during low-use periods and regularly verify that the backup jobs complete successfully (monitor for failures).

- **PRACTICE RESTORATION AND RECOVERY:** A backup is only as good as your ability to restore it. You should periodically test restoring your backups to ensure the data is intact, and you are familiar with the process. It's not uncommon for businesses to think they have good backups, only to discover after a ransomware attack that the backups were corrupt, incomplete, or the team didn't know how to restore system X. Conduct fire-drills: for example, take a random file from backup and try to fix it, or spin up a server from a backup image in a sandbox environment. Time how long it takes and see if it matches your Recovery Time Objective (RTO) – the target window to be back up and running. Suppose restoring all systems from backup takes 3 days, and your business would suffer greatly from being down that long. In that case, you might need to invest in faster recovery solutions or prioritize plans.

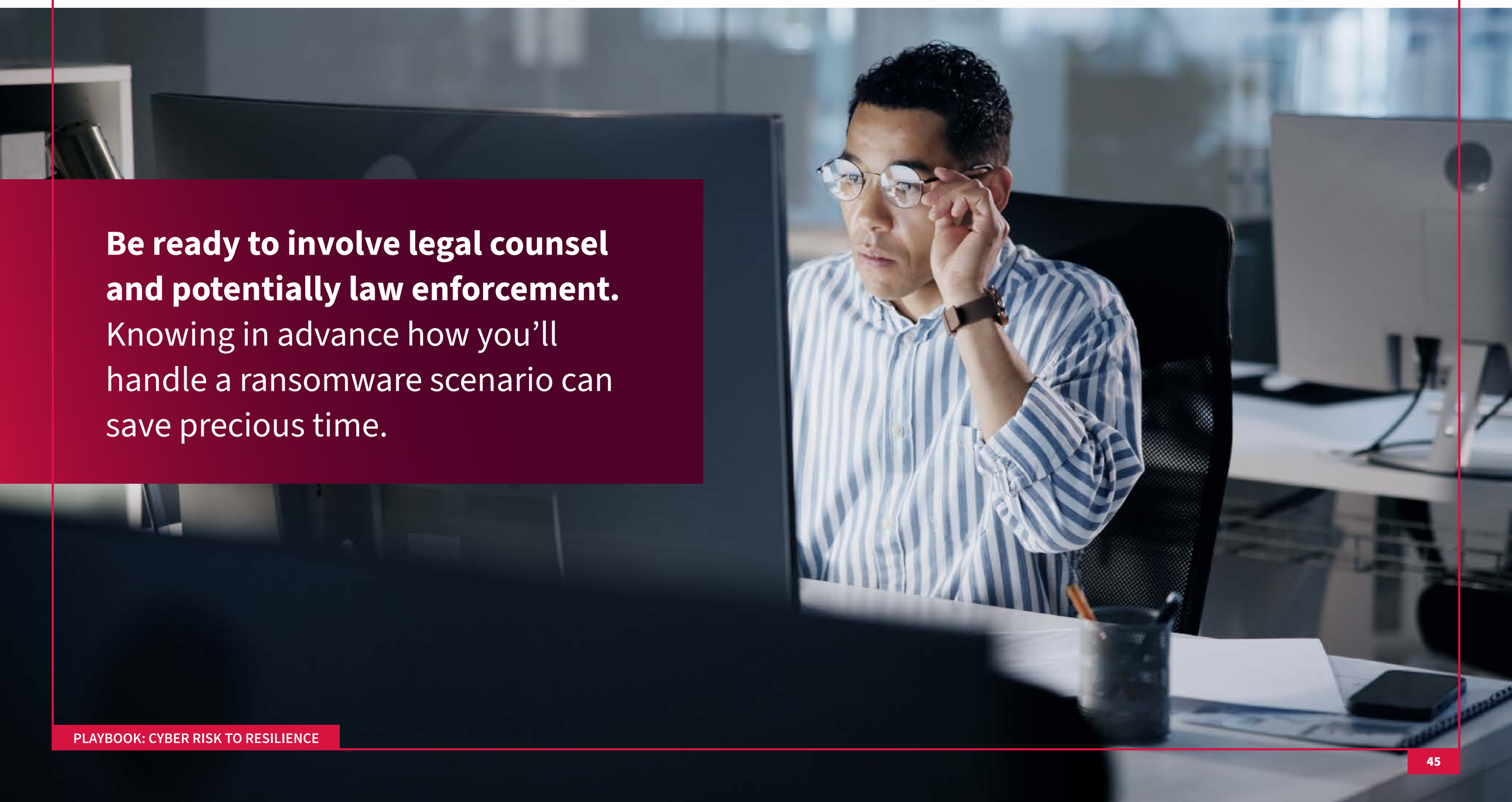
- **PROTECT BACKUP INFRASTRUCTURE:** Secure the accounts and systems involved in your backup process. Use a dedicated service account for backups that is not an administrative account on the network (so if an attacker gets domain admin, they still can't log into the backup system easily). Store backup credentials in a password manager or secure vault, not on a sticky note or an easily accessible script. If using a NAS or backup server, ensure it's properly segmented – ideally on a Virtual Local Area Network (VLAN) that regular workstations cannot access. Many ransomware strains specifically seek out network shares and connected backup drives to encrypt; if the PC that gets infected can't "see" the backup server due to network segmentation, the backups are safer. Also, update and patch your backup software – a few incidents have occurred where attackers exploited vulnerabilities in backup servers themselves.

Store backup credentials in a password manager or secure vault, not on a sticky note or an easily accessible script.

- **HAVE A RANSOMWARE RESPONSE PLAN:** In addition to backups, plan out the response steps if ransomware hits.
  - Who will declare an incident and make the call to start recovery?
  - What systems get restored first (identify your most critical applications to minimize business impact)?
  - Do you have cloud or alternate systems to fail over temporarily?

  Outline these in an incident response playbook. The plan should also address communication: Ransomware often comes with a data breach component (attackers steal data before encrypting). Be ready to involve legal counsel and potentially law enforcement. Knowing in advance how you'll handle a ransomware scenario can save precious time. As the saying goes, "it's not if but when" an incident happens, so have a blueprint ready to go.

Proper backups and rehearsed recovery procedures turn a potentially catastrophic ransomware event into a manageable IT issue. They give you the power to say "no" to extortion. The Verizon DBIR data indicates that more companies are refusing to pay ransoms, which is directly tied to the implementation of better backup strategies. To make that statistic personal: your business should aim to be among those who can refuse a ransom demand because you have confidence in your backups. It's worth noting that insurers also strongly encourage robust backups – one insurer's report found clients with offline backups and MFA saw far less business impact from ransomware (CISA, 2022). In summary, backup and recovery are your safety net. Strengthen it, test it, and keep it out of the reach of attackers.



Be ready to involve legal counsel and potentially law enforcement. Knowing in advance how you'll handle a ransomware scenario can save precious time.

7. Develop an Incident Response Plan and Practice It

Even with all preventative measures, breaches can still occur. Emerging and mid-sized companies need to be prepared to respond effectively when an incident happens – to minimize damage, recover faster, and fulfill any legal obligations. An Incident Response Plan (IRP) is a documented set of instructions for detecting, responding to, and recovering from incidents. Here's how to establish and improve this capability:

- **CREATE A SIMPLE, CLEAR INCIDENT RESPONSE PLAN:** At its core, an IR plan should answer: Who does what, and when? Define roles and responsibilities:
  - Who is the incident coordinator?
    (In a small business, it might be the IT manager or an external IT provider.)
  - Who contacts law enforcement or external responders?
  - Who communicates with employees and possibly customers?

  Include an escalation tree (e.g., when to notify the CEO/owner, when to bring in outside help). Outline key steps to take in everyday scenarios, e.g., for a suspected ransomware, steps might include isolate affected systems (unplug network cables, disable Wi-Fi), power off machines if malware is spreading, contacting your IT provider or IR firm immediately. For a suspected email account breach, reset the password, review mailbox rules, and alert the team to watch for potential fraud attempts. The plan doesn't need to be long; in fact, short checklists and decision trees are more usable during a crisis than a 100-page manual. Keep a printed copy accessible (in case you can't access it on the network during an incident).

- **PREPARE CONTACT INFORMATION AND RESOURCES:** As part of the plan, maintain an up-to-date contact list: key internal team members (with after-hours phone numbers), your cyber insurance claim hotline (if you have a policy), a preferred incident response firm or consultant, legal counsel, PR or communications contacts, and law enforcement contacts (like the local FBI office or cybercrime unit, if relevant). When "everything is on fire," you don't want to be scrambling to find phone numbers. Also, have ready any resources needed for response – for example, bootable clean USB drives with antivirus, lists of critical systems and their backups. Some emerging and mid-sized companies prepare an "IR go-kit" that contains tools and information that might be needed immediately when responding.

- **CONDUCT TABLETOP EXERCISES:** A highly recommended practice is to simulate an incident in a roundtable discussion, called a tabletop exercise. Gather the key players (even if that's just two or three people in a small company, along with your IT service provider) and walk through a hypothetical breach scenario. For instance, "It's Monday morning, all servers are encrypted, and there's a ransom note, what do we do?" Step through your plan: does everyone know their role? Are there unclear points, like whether we would ever consider paying a ransom? Who has the authority to make that decision? The exercise will reveal gaps or disagreements in your plan while the stakes are low, allowing you to adjust accordingly.

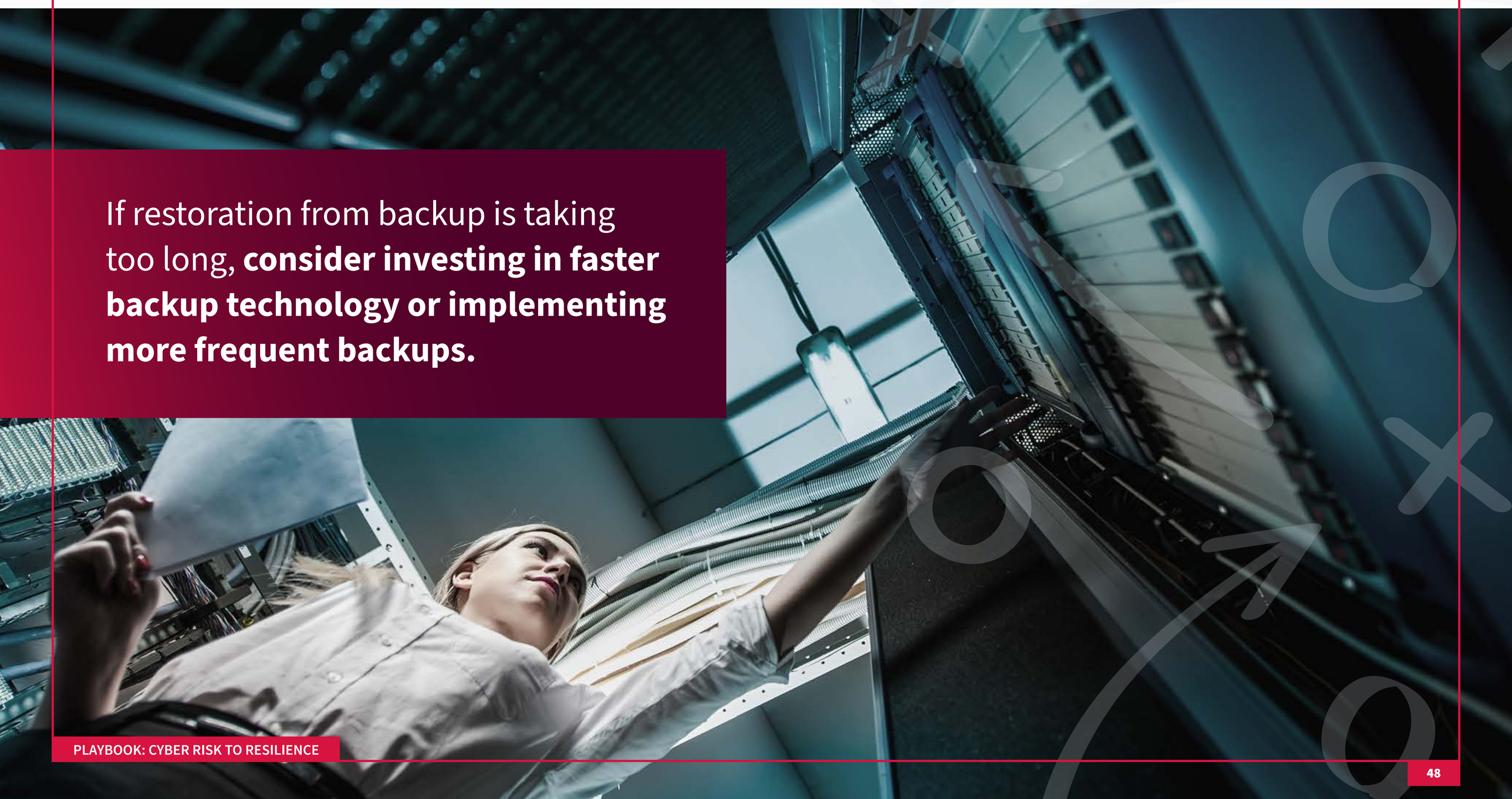
  It also familiarizes everyone with the process so that if a real event occurs, there's less panic and confusion. Verizon's incident experts noted that companies running regular tabletop simulations are far calmer and more effective when an actual incident happens – they approach it as something practiced rather than an unthinkable emergency. Even a yearly tabletop is hugely beneficial for emerging and mid-sized companies. If possible, incorporate scenarios beyond ransomware too (e.g., a lost laptop with sensitive data, or a malware outbreak, or a disgruntled insider stealing info) to broaden preparedness.

Determine ahead of time how you will handle notifications in the event of customer data compromise.

- **ESTABLISH EXTERNAL COMMUNICATION PLANS:** Part of incident response is managing communications to outside parties. Determine ahead of time how you will handle notifications in the event of customer data compromise – many jurisdictions have breach notification laws that require you to inform affected individuals and regulators within a specific timeframe. Your plan should identify when legal counsel will be involved (usually early, to guide breach notification and preserve legal privilege). **Draft some communication templates** in advance, such as a breach notification letter template and a press statement template, that can be quickly customized. Also, plan how to notify all employees in the event of a security lockdown (e.g., if everyone needs to disconnect from the VPN or stop using email). In a small business, word spreads informally, but it's still good to have an official channel (company-wide text alert or phone tree, for example).

- **LEARN AND IMPROVE (POST-INCIDENT REVIEWS):** After any security incident (even minor ones), do an analysis, a “post-mortem.” Document what happened, what was done to address the issue, and what could be improved. Identify root causes – if a phishing email led to a malware infection, the lesson might be to implement better email filtering or provide further training. If restoration from backup is taking too long, consider investing in faster backup technology or implementing more frequent backups. These continuous improvements will elevate your maturity. Share lessons learned with the team, so everyone grows more vigilant. Also, update the IR plan if new scenarios arise or if any aspect of the response process doesn’t work as expected. Treat the IR plan as a working document.

Having a practiced incident response capability can significantly reduce the **mean-time-to-recover** from breaches and limit damage. It’s often said that how you handle a breach is what defines the impact, perhaps even more than the fact that it occurred. A well-handled incident can reinforce trust (showing customers you take it seriously and respond quickly). In contrast, a bungled response can make a bad situation worse (think of breaches where companies took weeks to respond or issued confusing statements). **For small and scaling companies, demonstrating competent incident response can also be a selling point to clients in an era where supply chain security is scrutinized.** In essence, hope for the best, but prepare for the worst. An incident response plan is your playbook for the worst, and if you practice it, the worst will never catch you by surprise.



If restoration from backup is taking too long, **consider investing in faster backup technology or implementing more frequent backups.**

8. Protect and “Devalue” Sensitive Data with Cryptography

In the modern digital economy, data is a crown jewel for most businesses – and a prime target for attackers. One emerging strategy advocated by security experts is to “devalue the data” so that even if attackers steal it, they can’t exploit it. This is where **cryptography** – protecting information by turning it into a secret code – comes into play as a powerful tool in the emerging and mid-sized companies’ security arsenal. By encrypting sensitive data and using techniques like tokenization, emerging and mid-sized companies can mitigate the impact of a breach. Here’s how to apply cryptography to safeguard your critical information:

- **ENCRYPT DATA AT REST:** All sensitive data stored on servers, databases, or devices should be encrypted at rest. This means if someone gains unauthorized access to the storage (or if a device is lost or stolen), the data remains unintelligible without the decryption key. For example, if you host a customer database, enable the database’s encryption feature (many databases that use programming language like Structured Query Language (SQL) and Not Only SQL (NoSQL) offer transparent encryption). If you have file shares with essential documents, use disk-level encryption on the server or consider third-party tools to encrypt specific folders/files. Many emerging and mid-sized companies are already utilizing cloud services for tasks such as file storage (e.g., Dropbox, Google Drive) or email (Office 365).

These services typically encrypt data at rest by default, which is good. If you manage your on-prem storage, it’s on you to configure encryption. Fortunately, modern operating systems make it easy: Windows has BitLocker for drives, Linux has Linux Unified Key Setup (LUKS). Full-disk encryption should be standard for laptops and any portable drives, mainly to prevent data exposure if a device is lost. Some compliance standards require proving that data was encrypted to avoid reporting a lost device as a breach. Make sure to securely back up your encryption keys (e.g., BitLocker recovery keys in Active Directory or a safe escrow) to avoid losing access yourself.

Full-disk encryption should be standard for laptops and any portable drives, mainly to prevent data exposure if a device is lost.

- **ENCRYPT DATA IN TRANSIT:** This is a straightforward – ensure that all network communications, especially those over the internet, use encryption (like secure communication protocols Transport Layer Security/Secure Sockets Layer (TLS/SSL)). This includes your website (serving it over HTTPS only), emails (ensure your email provider supports TLS for mail transport), file transfers, Application Programming Interface (API) calls between systems. In practice, most modern services do this by default. Just avoid any unencrypted protocols within your control (for instance, don't let an outdated File Transfer Protocol (FTP) server run without TLS, or avoid using older email protocols like Post Office Protocol version 3 (POP3) without encryption). VPNs should be used for remote access to internal systems, which inherently encrypt that traffic.

Essentially, no sensitive data should be traversed through the network in clear text. Using strong encryption protocols prevents attackers from eavesdropping or manipulating data in transit – a fundamental but essential security layer.

- **TOKENIZATION AND DATA MASKING:** If your business handles sensitive information (such as credit card numbers, Social Security numbers, or health records), consider implementing tokenization or masking solutions. Tokenization means replacing a sensitive data element with a non-sensitive equivalent (a token) that has no exploitable meaning if compromised. The real data is stored securely in a separate vault, and you use the token (e.g., a reference number) in your database. For example, rather than storing actual credit card numbers, emerging and mid-sized companies can use a payment gateway that tokenizes cards – you store a token, and the gateway charges the card via token reference. This way, a breach of your system wouldn't expose the actual card numbers. Similarly, you can tokenize personal identifiers in databases and only translate them back when needed securely.

  Data masking is another approach for non-production environments: if you use production data in testing or analytics, mask or anonymize it so that even if those lower-security environments are breached, real personal data isn't exposed. The Bluefin report on the DBIR emphasizes that encryption and tokenization can render stolen data useless to attackers, essentially taking the "prize" out of the break-in. This strategy is particularly potent for emerging and mid-sized companies that hold valuable data troves (customer lists, personal info) but may not be able to prevent every intrusion; even if thieves get in, they can't monetize scrambled data.

- **PROPER KEY MANAGEMENT:** Encryption is only as strong as the protection of its keys. Use robust key management practices. For emerging and mid-sized companies, this may mean utilizing managed key services (such as AWS KMS or Azure Key Vault) to prevent storing encryption keys in plaintext on a server. If using built-in OS encryption like BitLocker, integrate it with your directory services to escrow keys. Restrict access to systems or personnel who can decrypt the data. Rotate encryption keys periodically (at least for data that changes; static archives can keep a single key but do have a process if you ever suspect a key is compromised). Avoid hard-coding credentials or keys in application code – if you develop software, use secure vaults for any secrets.

The goal is to prevent attackers from simply finding a key file or password and undoing all your encryption. Consider splitting knowledge of keys (no one person has full access) in especially sensitive situations.

- **LEVERAGE COMPLIANCE AND LEGAL SAFE HARBORS:** Many data breach notification laws provide a "safe harbor" if lost data was encrypted. This means if an emerging and mid-sized company's stolen laptop had encrypted files, they might not have to formally notify customers that their data was exposed (since it's assumed encrypted data is unreadable). This underscores a real business benefit: encryption can reduce regulatory burden and liability in a breach. It's worth understanding the laws that apply to you. For example, HIPAA (health data law in the US) doesn't require breach notifications if the data was encrypted. The same often applies under GDPR (Europe) and US state laws for personal data. Thus, **investing in encryption not only protects the data but could save your organization from the reputational damage of a public breach disclosure** (provided you're confident the encryption wasn't broken).

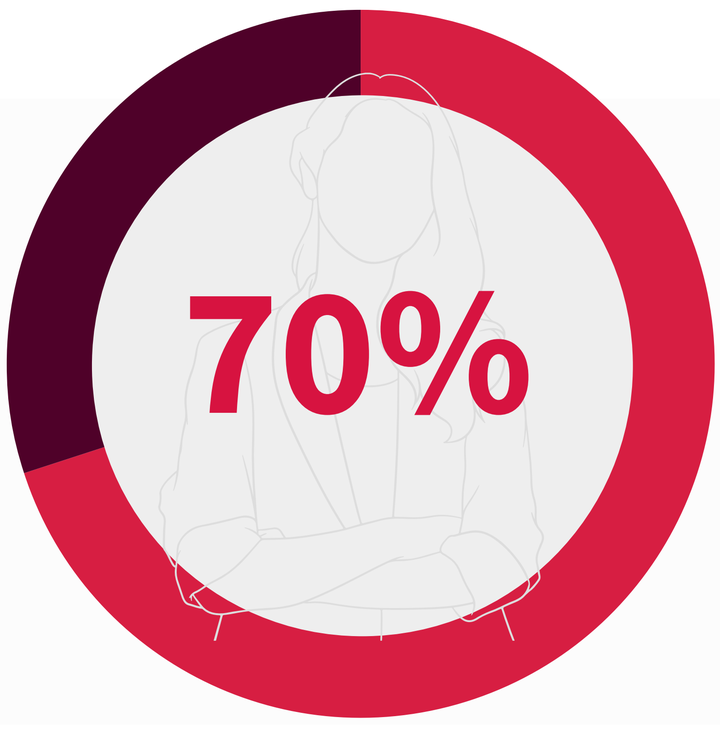
By implementing cryptographic protections, emerging and mid-sized companies should balance security with usability. Encrypt what's sensitive – not necessarily everything – to avoid complicating operations. But err on the side of caution: if you're unsure whether data is sensitive, it probably is to someone (customer or regulator). Modern systems have made encryption performance minimal for most use cases, so there are few downsides today beyond the need to manage keys and access. The mindset shift is essential: don't treat encryption as an exotic, enterprise-only control. It's very feasible for small businesses through cloud services and built-in tools. By incorporating encryption and tokenization, emerging and mid-sized companies can dramatically reduce the "data value" that an attacker would gain from a breach, thereby reducing the incentive to target them and the impact if they do. In essence, even if other defenses fail, cryptography can be a last line of defense.

9. Leverage External Security Expertise and Services

Most emerging and mid-sized companies do not have large internal security teams. But thegood news is that you don't have to go to it alone. There is a growing ecosystem of external services, providers, and even free public resources that smaller firms can leverage to bolster their cybersecurity. Engaging these can be a force multiplier, bringing enterprise-grade protection into reach:

- **MANAGED SECURITY SERVICE PROVIDERS (MSSPs) / MANAGED DETECTION & RESPONSE (MDR):** MDR was discussed in the context of endpoint monitoring. More broadly, MSSPs can handle a range of security functions: firewall management, intrusion detection, vulnerability scanning, incident response, compliance reporting, and more. Essentially, you outsource your security operations to specialists. For a monthly fee, an MSSP can serve as your 24/7 SOC and IT security department. When choosing providers, ensure they have experience with emerging and mid-sized company environments and check what technologies they use (some partner with top vendors like CrowdStrike, Splunk, under the hood).

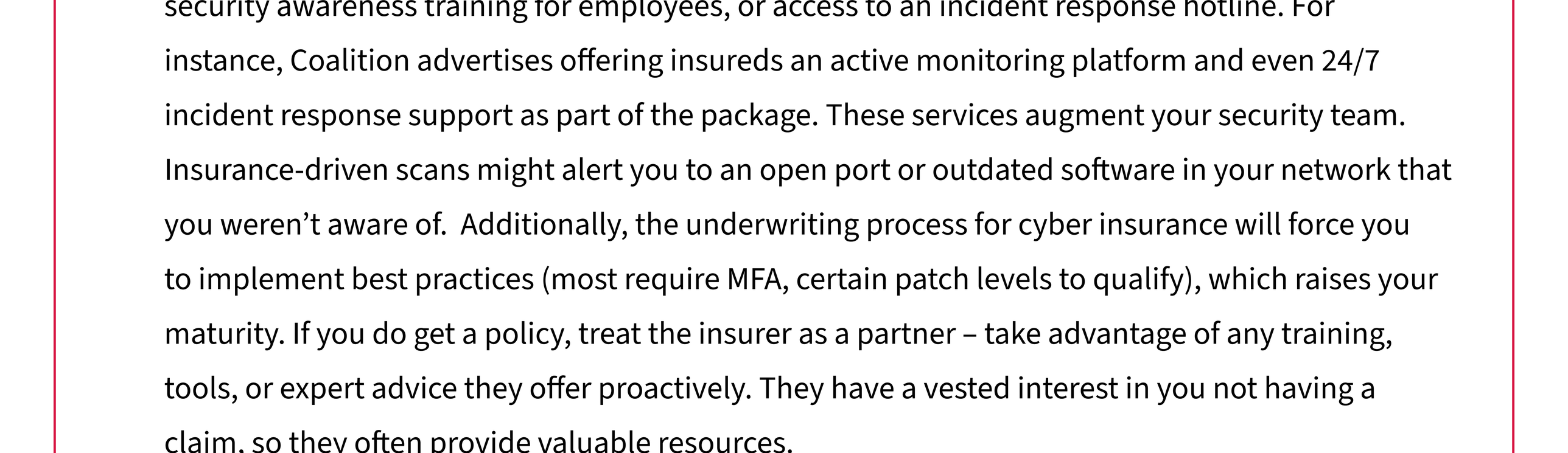
The CrowdStrike survey revealed that 70% of emerging and mid-sized companies rely on outside experts for security decisions, and this is often the model that makes sense. It allows you to focus on your core business while letting experts manage the cyber risk. Just treat selecting an MSSP like a critical hire – vet their reputation, SLAs (service-level agreements), and make sure they'll provide you with actionable reports and not just tech jargon. A good MSSP will help you interpret threat reports and will proactively advise on improvements (e.g., "We've seen multiple attempts to compromise Remote Desktop Protocol (RDP) on an old server; we recommend you disable or harden it").



of emerging and mid-sized companies rely on outside experts for security decisions

- **CONSULTING AND vCISO SERVICES:** If a full MSSP is beyond budget or need, at least consider consulting engagements for specific needs. For example, hire a consultant to do an annual security assessment or penetration test of your network – they will identify weaknesses before attackers do. You can also engage a **"Virtual CISO" (vCISO)** service: this is a part-time security executive who can help you develop strategy, policies, training programs, and ensure all the recommendations discussed are being implemented in a structured way. They essentially act as your Chief Information Security Officer (CISO) for a few hours a month, which is far more cost-effective than hiring a full-time employee but provides strategic oversight. vCISO services, often offered by security consulting firms or independent experts, are becoming increasingly popular among mid-sized organizations that require guidance but lack a dedicated CISO. They can also assist with compliance (e.g., preparing for audits) and with vendor risk management by evaluating the security of partners you work with.

- **CYBER INSURANCE AND ASSOCIATED SERVICES:** Cyber liability insurance is something every emerging and mid-sized company should at least evaluate. A policy can cover financial losses from a breach (ransomware payments, legal fees, customer notifications, business interruption). But beyond coverage, many insurers (like Coalition, Travelers) now bundle **preventive services for policyholders,** such as continuous attack surface monitoring, security awareness training for employees, or access to an incident response hotline. For instance, Coalition advertises offering insureds an active monitoring platform and even 24/7 incident response support as part of the package. These services augment your security team. Insurance-driven scans might alert you to an open port or outdated software in your network that you weren't aware of. Additionally, the underwriting process for cyber insurance will force you to implement best practices (most require MFA, certain patch levels to qualify), which raises your maturity. If you do get a policy, treat the insurer as a partner – take advantage of any training, tools, or expert advice they offer proactively. They have a vested interest in you not having a claim, so they often provide valuable resources.



Cyber liability insurance is something every emerging and mid-sized company should at least evaluate.

- **UTILIZE FREE GOVERNMENT AND NONPROFIT RESOURCES:** There are several free programs available to help emerging and mid-sized companies with cybersecurity. For example, the US. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency **(CISA)** provides a **list of free security services and tools** for emerging and mid-sized companies, ranging from vulnerability scanning to phishing test emails. They also have regional advisors who may assist businesses in improving their security posture.

The US Small Business Administration (SBA) and Federal Communications Commission (FCC) have guides and a "cyber planner" tool for small businesses. In the EU, agencies like the European Union Agency for Cybersecurity (ENISA) publish practical toolkits and even an online cyber maturity assessment for SMEs.

There are also nonprofit initiatives that pair small businesses with volunteer cybersecurity experts for basic advice (for example, some local Information and Sharing and Analysis Centers (ISACs) or community colleges run clinics). Stay informed through local business associations or chambers of commerce, which sometimes host cybersecurity workshops. The knowledge shared in these forums can be directly applied at minimal cost.

- **VENDOR SECURITY AND CONTRACTS:** When outsourcing any IT or adopting cloud services, scrutinize the security measures of those vendors. The chain is only as strong as its weakest link. MSPs and cloud providers have been targets for supply-chain attacks (e.g., the Kaseya VSA incident affected many MSP-served emerging and mid-sized companies). So, when you pick an IT provider or SaaS platform, ask about their security: Do they have SOC 2 or ISO 27001 certification? How do they handle data encryption? What is their incident response policy? And ensure your contract includes data protection language. It might sound like overkill for a small company to do "vendor risk management," but as DBIR data showed, 30% of breaches now involve a third-party. Even a brief questionnaire or conversation can flag potential issues. For critical vendors, consider contractual requirements that they notify you of breaches, carry their cyber insurance. Share some of the security responsibilities with those who support your operations.

When outsourcing any IT or adopting cloud services, scrutinize the security measures of those vendors. The chain is only as strong as its weakest link.

Engaging external expertise does come with a cost, but it can be cost-effective relative to building everything in-house or, worse, suffering a significant incident.

Think of it this way: just as many emerging and mid-sized companies hire an external accountant or lawyer rather than having full-time staff for those roles, using outside security experts is a smart way to get high-quality results on a budget. The key is to ensure the partner is aligned with your business goals and that you maintain oversight. Have regular check-ins, demand transparent reporting, and integrate their advice into your business planning (e.g., if the MSSP advises you to upgrade a firewall or segment your network, allocate a budget for that as part of your IT improvements).

By leveraging these external resources, small and scaling businesses can achieve a level of security maturity far beyond what their in-house capabilities might allow, effectively "punching above their weight" in cybersecurity. It's a classic force multiplier: a small team fortified by expert allies can defeat threats that would otherwise overwhelm them.

Final Thoughts

Emerging and mid-sized companies stand at a crossroads in 2025: cyber threats are escalating in sophistication and frequency, yet the tools and knowledge to combat them have never been more accessible. The breach analysis from the past year unequivocally shows that security is no longer optional for smaller businesses – it's a fundamental component of business resilience and trust. The idea that a company might be "too small to be noticed" by hackers has been thoroughly debunked; attackers, especially ransomware crews, are increasingly **indiscriminate in their targeting of victim size.** They often find emerging and mid-sized companies to be soft targets and will happily exploit that. The impact of a breach can be devastating, both to the company and to its customers or partners.

However, the narrative is not all doom and gloom. There are encouraging signs that with the right actions, emerging and mid-sized companies can significantly improve their security posture and outcomes:

- Companies are **getting better at handling ransomware** – more are refusing to pay ransoms because they have reliable backups and practiced response plans. This trend can continue if more emerging and mid-sized companies implement the backup and recovery strategies described.

- The availability of cloud-based security solutions and managed services means that enterprise-grade protection is within reach for emerging and mid-sized companies. You don't need a huge IT department to deploy EDR, 24/7 monitoring, or strong encryption – you can consume these "as a service" in a cost-effective way.

- Security **awareness among emerging and mid-sized companies' leadership is at an all-time high.** The gap is in execution, which is precisely what our action plan targets. By systematically addressing the gaps (training, MFA, patching), small and scaling companies can close the knowing-doing gap.

Crucially, taking a **maturity model approach** helps break the journey into manageable phases. Emerging and mid-sized companies don't transform from vulnerable to ironclad overnight. But through incremental improvements – moving from ad hoc to basic controls, then to managed and proactive practices – you can build layers of defense. Each layer (be it MFA, EDR, backups, or encryption) cuts down the risk a bit more, and together they dramatically reduce the likelihood of a successful breach, or at least the impact of one. The maturity model also provides a way to communicate with stakeholders (owners, boards, investors) about where the company is and where it needs to go in cybersecurity. This can justify budget and resources: for example, "We're at maturity level 2 now, but to effectively counter the ransomware and phishing threats noted in the DBIR, we need to reach level 3 by next year – that will require investing in an MDR service and formal training program." Framing it as a progression resonates more than piecemeal tool requests.

Crucially, taking a **maturity model approach** helps break the journey into manageable phases. Emerging and mid-sized companies don't transform from vulnerable to ironclad overnight.

It's nearly impossible to be 100% breach-proof (even top enterprises get breached), but you can aim to be resilient.

One theme that emerged is the idea of **resilience.** It's nearly impossible to be 100% breach-proof (even top enterprises get breached), but you can aim to be resilient – able to withstand attacks, recover quickly, and keep operating. For emerging and mid-sized companies, resilience means having robust backups, alternative processes in place in the event of system downtime, cyber insurance as a financial safeguard, and a well-practiced incident response plan.

There is also the concept of using **cryptography to devalue data,** which is a forward-looking strategy that might not yet be widespread among emerging and mid-sized companies. Embracing encryption and tokenization is a proactive move that could prevent a lot of grief down the line. It's a recommendation that stands up to academic analysis and real-world experience alike: data you encrypt is data criminals can't easily abuse. As more emerging and mid-sized companies adopt cloud services that offer built-in encryption, this should become a standard practice.

Remember that cybersecurity is a continuous journey, not a destination. Threats evolve – for instance, the rising use of AI by attackers to craft convincing scams means there is a need to innovate in response, perhaps with AI-driven defenses or new verification techniques for communications.

The regulatory landscape is also evolving, likely bringing more requirements even to smaller companies to protect data. By building a solid foundation now, emerging and mid-sized companies will be better positioned to adapt to whatever comes next. Think of it as building cybersecurity muscle memory: each new challenge can be met if the fundamentals are strong.

By applying the insights from breach reports and implementing the multifaceted action plan – from identity security and training to incident readiness and data encryption – growing businesses can dramatically reduce its cyber risk. The journey to higher maturity is achievable with deliberate steps, and the ROI is clear: avoiding costly breaches, preserving customer trust, and ensuring the longevity of the business. Cybersecurity may seem technical, but at its core, it’s about protecting the mission of your organization and the customers you serve. With the right strategy and support, even the smallest company can make itself a hard target and a cyber-resilient enterprise. The time to act is now – **the threats are real, but so are the solutions.**

References

Verizon. (2025a). 2025 Data Breach Investigations Report: Executive summary. Verizon Business.

Verizon. (2025b). 2025 Data Breach Investigations Report (web page). Verizon Business.

CrowdStrike. (2025a). 2025 Global Threat Report. CrowdStrike Holdings, Inc. SecurityWeek

CrowdStrike. (2025b). The CrowdStrike State of SMB Cybersecurity Survey. CrowdStrike

Security Magazine. (2025, March 5). Vishing attacks increased by 442% in the second half of 2024. Security Magazine

IBM. (2023, July 24). IBM Report: Half of breached organizations unwilling to increase security spend despite soaring breach costs. IBM Newsroom.

IBM. (2024). Cost of data breaches: The business case for security AI automation. IBM Think. IBM

National Institute of Standards and Technology. (2024). Digital Identity Guidelines: Authentication and Authenticator Management (SP 800-63B, Second Public Draft). NIST Publications

Cybersecurity and Infrastructure Security Agency. (2022). Implementing phishing-resistant multi-factor authentication (MFA). CISA

Sophos. (2024, March 26). The impact of compromised backups on ransomware outcomes. Sophos News

Reuters. (2024, June 30). Cyber insurance rates fall as businesses improve security, report says.
National Counterintelligence and Security Center. (2021, August 10). Kaseya VSA supply chain ransomware attack. ODNI

Qualys (2025, April 21). Qualys Midyear 2024 threat landscape analysis and insights.

Google Cloud. (2025). M-Trends 2025: Executive edition.

BlackFog. (2023, July 11). 61% of SMBs were victims of a successful cyberattack in the past year.

CrowdStrike. (2025, March 13). Zero Trust Security Explained: Principles of the Zero Trust Model.

CISA ZTMM Document – Cybersecurity & Infrastructure Security Agency. (2023, April). Zero Trust Maturity Model Version 2.0.

Tetrate. (2023, July 13). Accelerate Zero Trust Adoption with CISA's Zero Trust Maturity Model 2.0.

RCR Wireless (2025, April 23). Seven takeaways from Verizon's latest cybersecurity report.

Versa Networks Blog (2025, June 9). 2025 Verizon DBIR Inside: Cybersecurity Trends from 12,000+ Data Breaches.

TRM Labs. (2025, June 30). Inside the Nobitex Breach: What the Leaked Source Code Reveals About Iran's Crypto Infrastructure.

Hudson Rock. (2025, June 18). Nobitex Breach: Infostealers Expose Critical Employee Credentials in Latest Crypto Exchange Hack.

NIST. (2023). Cybersecurity Framework 2.0 Small Business Quick-Start Guide.

Coveware. (2025, January 31). Q4 Ransomware report.

ConnectWise. (2025). State of SMB cybersecurity report.

Coalition. (2022, May 24). How Coalition's incident response helps reduce risks during a cyber attack.

LastPass

Cyber Resilience Index (CRI)

for Emerging and Mid-Sized Companies:

A Quick Start Guide: Score it. Prove it. Improve it.

DR. CHASE CUNNINGHAM

The Origin and Rationale for the Cyber Resilience Index (CRI)

The Need for a New Model

Let’s be honest — the 1–5 maturity model has been a security industry comfort blanket for too long. You can score a ‘5’ and still get wrecked. What matters isn’t the shiny scorecard, it’s whether your business can take a punch and stay standing. That’s why the CRI exists.

Most security guidance stops at capability maturity — the classic 1–5 scale of how developed your controls are. While helpful, that approach has a central blind spot: it assumes perfect execution.

Breaches still happen even in “mature” environments, and the deciding factor in business survival isn’t just whether controls existed, but whether the business could recover quickly when they failed.

The Cyber Resilience Index (CRI) for emerging and mid-sized companies was designed to solve this gap. It’s not just about “Do you have MFA?” but “If MFA is bypassed, how much damage can be contained, and how fast can you return to normal operations?”

Behind the Build

Real-world breach cause data from high-credibility sources laid the foundation:

- **Verizon 2025 Data Breach Investigations Report (DBIR)** – provided the frequency of attack patterns by cause, broken down for smaller businesses vs. enterprises.
- **Coveware ransomware reports** – quantified the impact of backups, preparation, and incident response on ransom payment rates and downtime.
- **CrowdStrike Global Threat Report** – detailed the prevalence of “malware-free” intrusions, credential abuse, breakout times, and attacker tactics, techniques, and procedures (TTP).
- **Cybersecurity & Infrastructure Security Agency (CISA) and Zero Trust Maturity Model (ZTMM)** – informed control areas that map to current federal guidance.

The research dentified the five domains where the overwhelming majority of emerging and mid-sized company-impacting incidents occur:

- **Identity Assurance** – credential compromise was a top cause of breaches across DBIR categories, making identity security the single most leveraged attack vector for smaller firms.
- **Data Resilience** – ransomware prevalence (88% of smaller and mid-sized business breaches) makes backup, encryption, and recovery speed critical survival factors.
- **Threat Visibility** – detection delays drive impact; CrowdStrike data on breakout times (<1 hour) makes endpoint/network monitoring a necessity.
- **Vulnerability Velocity** – DBIR’s 34% YoY increase in vulnerability exploitation shows patch speed is as vital as patch coverage.
- **Supply Chain Security** – DBIR’s doubling of third party–origin breaches (now ~30%) makes partner/vendor security a real smaller business risk amplifier.

These domains were weighted based on relative frequency × average impact severity from DBIR and supporting reports, ensuring the CRI aligns with **where emerging and mid-sized companies are statistically most at risk.**

The Dual Scoring Concept

Don’t confuse maturity with survival. There are plenty of “mature” networks that end up in body bags after one phishing campaign. Resilience is what keeps the lights on. Think of it like boxing: maturity is your stance and guard. Resilience is whether you can recover when someone lands a clean shot. Most smaller companies only train for the stance, not the recovery.

Instead of only assigning a **Maturity Score** (1–5) to each domain, CRI also measures a **Resilience Factor** (0.0–1.0) — the realistic probability that the business will survive a major incident in that domain without catastrophic loss.

This approach is directly inspired by:

Business continuity research shows that post-breach survival depends as much on recovery time as on breach prevention.

Incident case studies from Coveware and Mandiant illustrate that businesses with high maturity but low resilience can still fail.

For example:

- A company with MFA everywhere but **no incident response plan** may still suffer catastrophic downtime after a credential phishing incident —
  Maturity: high; Resilience: low.
- Conversely, a growing business with average maturity but **bulletproof backups and tested failover** may bounce back from ransomware in hours —
  Maturity: mid; Resilience: high.

Why the CRI Is Evidence-Based and Actionable

The CRI is grounded in the most widely cited breach datasets in the industry (DBIR, CrowdStrike, Coveware) and designed to:

- Target the top 5 emerging and mid-sized company threat domains by prevalence and impact.
- Combine prevention and recovery in a single score.
- Be simple enough to calculate quarterly without consultants.
- Produce several metrics executives can track over time and link to ROI.

Because each domain is weighted by actual breach likelihood and impact severity, smaller companies using CRI aren't spending time on low-probability risks at the expense of high-impact gaps. This aligns directly with CISA's "risk-driven prioritization" guidance and NIST Cybersecurity Framework CSF's emphasis on outcome-based measurement.

A Framework You Can Own and Evolve

By branding and publishing the CRI, you establish a recognizable, repeatable emerging and mid-sized company security benchmark that can be:

- Released annually as an industry report.
- Used by MSPs, insurers, and business leaders as a quick health check.
- Enhanced over time with new threat vector weights as the landscape changes (e.g., AI-assisted phishing, deepfake fraud).

The CRI's strength is that it's both strategic and tactical:

- Strategic because it frames risk in terms of survival probability and business continuity.
- Tactical because it tells you exactly where to spend the next dollar for maximum CRI lift.

The Cyber Resilience Index (CRI) measures both your cybersecurity maturity and your ability to survive an attack. It focuses on five high-impact domains: Identity Assurance, Data Resilience, Threat Visibility, Vulnerability Velocity, and Supply Chain Security. Use this toolkit to score your business, visualize strengths/weaknesses, and plan improvements.

Purpose:

The CRI is a simple way to measure how ready your business is to survive a cyberattack — not just to prevent it. It combines:

Maturity – how strong your defenses are.

Resilience – how well you can recover if those defenses fail.

Step 1 – Score Each Domain

Rate yourself in **five critical areas** that account for most emerging and mid-size company breaches:

Domain	Examples of What's Included	Weight
Identity Assurance	MFA, password policies, credential monitoring	25%
Data Resilience	Backups, encryption, and tokenization	20%
Threat Visibility	Endpoint/network monitoring, 24/7 SOC/MDR	20%
Vulnerability Velocity	Patch speed, vulnerability scanning	20%
Supply Chain Security	Vendor risk reviews, breach notification clauses	15%

Maturity Score (1–5)

1 = Ad hoc / fundamental security

5 = Fully integrated, automated, and reviewed regularly

Resilience Factor (0.0–1.0)

Your realistic survival probability in that domain:

1.0 = Very likely to survive a major incident

0.5 = 50/50 chance

0.2 = Unlikely to survive without significant loss

Step 2 – Calculate CRI

Domain Score = Maturity × Resilience × Weight × 20

Add all 5 Domain Scores → CRI (0–500)

Score Ranges:

400–500: High Resilience – Strong defenses and recovery plans

300–399: Resilient but Evolving – Good in most areas, some gaps remain

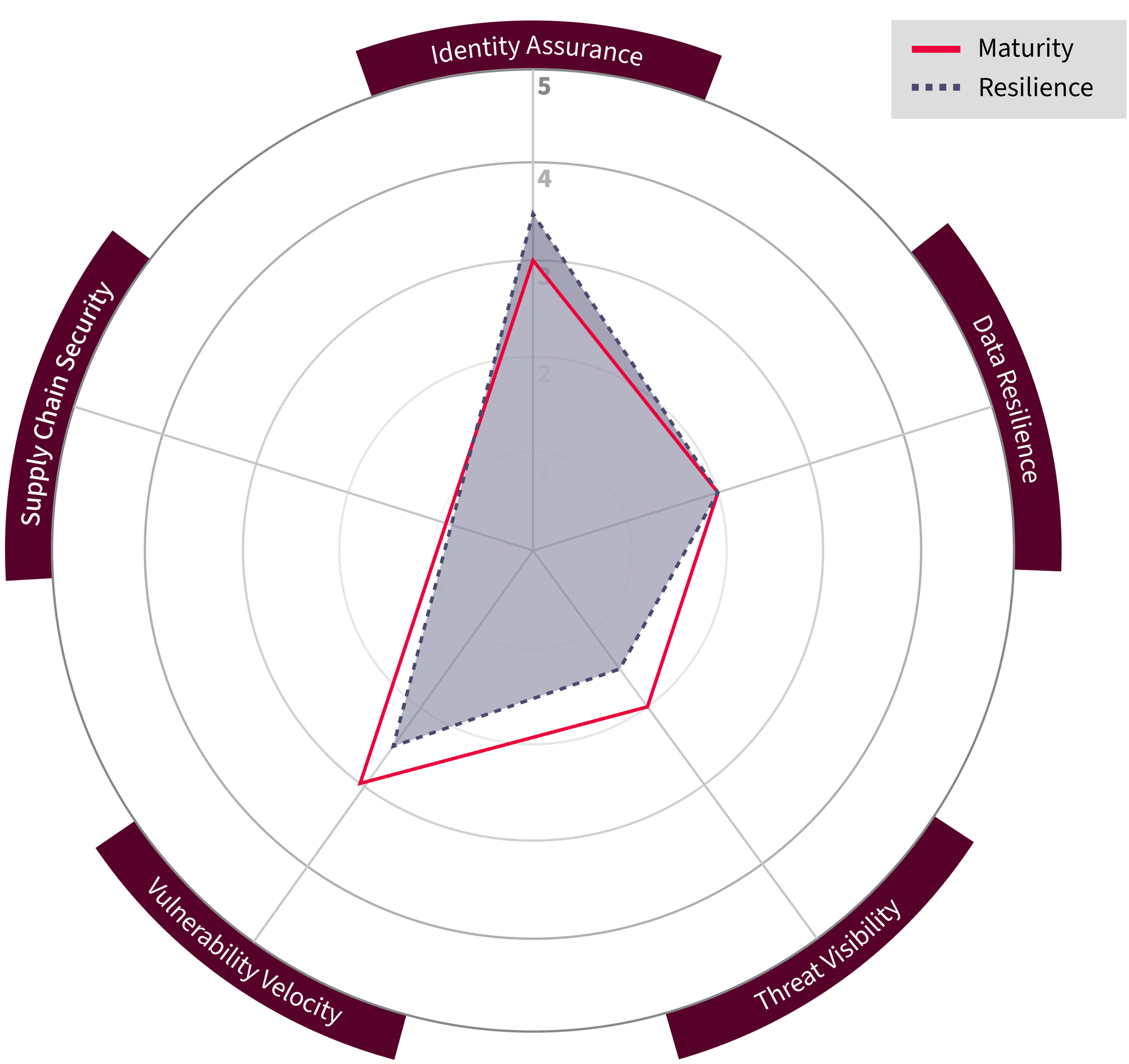
200–299: At Risk – Several weaknesses could be business-ending

Below 200: Vulnerable – Major overhaul needed

Step 3 – Visualize

Plot your **Maturity** and **Resilience** scores on a radar chart to see imbalances.

Cyber Resilience Index (CRI) Radar Chart



A balanced, outward-reaching shape is the goal.

Use this blank radar cart to plot your own maturity and resilience.

Download Chart

Step 4 – Take Action

Focus first on the **lowest-scoring domain** — raising that score often gives the most significant jump in CRI.

Typical fast wins:

- Use a password manager and set your minimum for the creation of new passwords to at least 12 characters with special characters and numbers
- Turn on MFA everywhere (Identity Assurance)
- Set up immutable cloud backups (Data Resilience)
- Add managed detection & response (Threat Visibility)
- Patch internet-facing systems first (Vulnerability Velocity)
- Add breach clauses to vendor contracts (Supply Chain Security)

Pro Tip: Recalculate your CRI quarterly to track improvement and justify your security budget. Cybersecurity isn't a one-and-done deal. Treat this like going to the gym. If you don't measure progress every quarter, you're just flexing in the mirror.

References

Verizon. (2025a). 2025 Data Breach Investigations Report: Executive summary. Verizon Business.

Verizon. (2025b). 2025 Data Breach Investigations Report (web page). Verizon Business.

CrowdStrike. (2025a). 2025 Global Threat Report. CrowdStrike Holdings, Inc. SecurityWeek

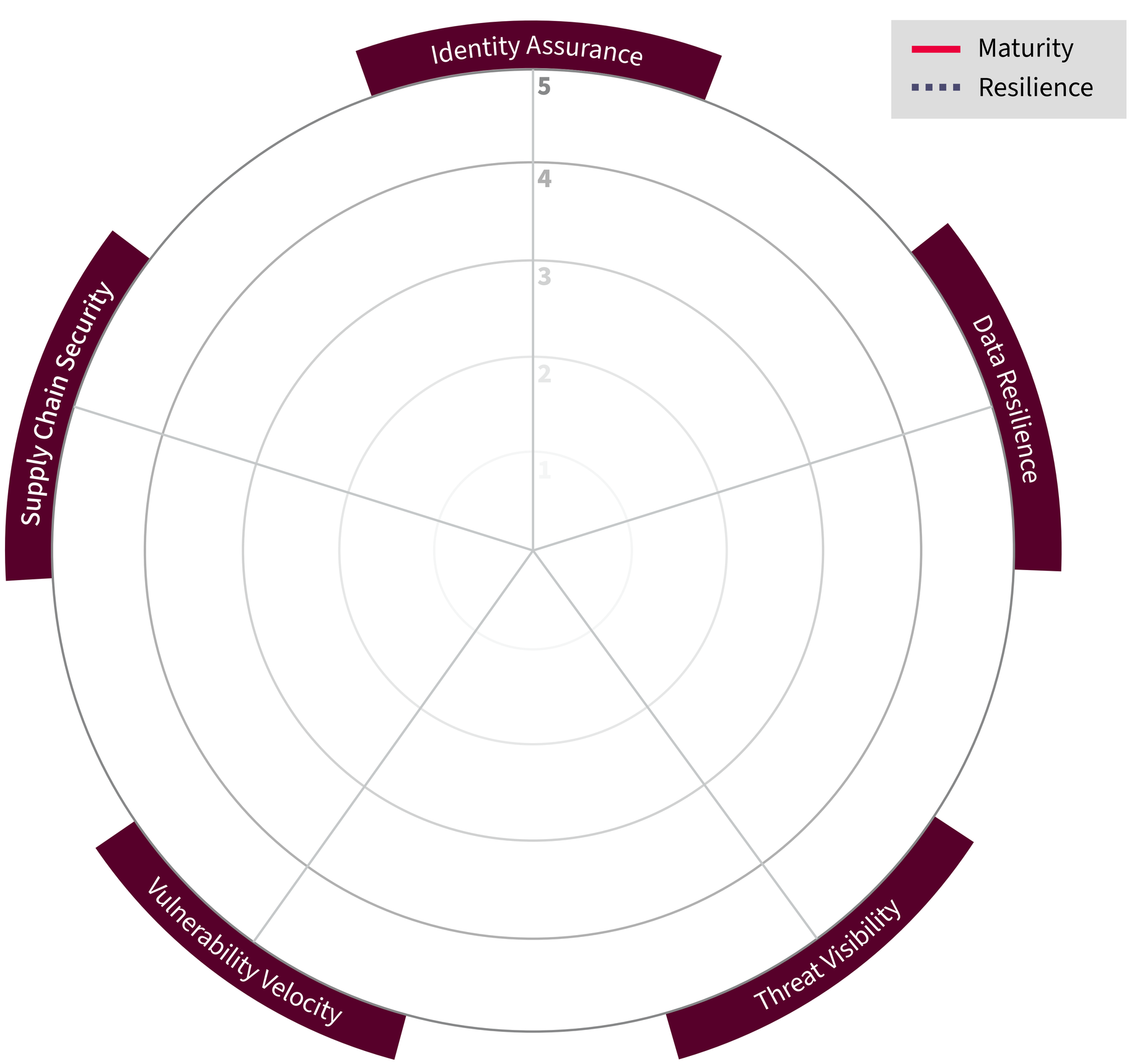
Coveware. (2025, January 31). Q4 Ransomware report.

CISA ZTMM Document – Cybersecurity & Infrastructure Security Agency. (2023, April). Zero Trust Maturity Model Version 2.0.

Download the full Cyber Resilience Playbook.

Plot your **Maturity** and **Resilience** scores on a radar chart to see imbalances.

Cyber Resilience Index (CRI) Radar Chart



A balanced, outward-reaching shape is the goal.