From pawns to queens: Why 581 breached SAP systems prove identity management needs strategic elevation

4:00 AM -- London: A security operations centre is lit by the glow of alerts. The Chief Information Security Officer jolts awake to a phone call: **their SAP ERP system has been breached.** Within minutes, they learn their company is among the 581 organisations compromised by a critical SAP vulnerability (CVE-2025-31324). This zero-day flaw -- scored a perfect 10.0 in severity -- allowed hackers to upload malicious files and **gain remote control of SAP servers** [1][2]. Investigators later trace the attack to a **nation-state hacking group** exploiting the gap in basic access controls [1][2]. In that moment of crisis, the company's **defences** were as vulnerable as pawns scattered across a chessboard -- their **"pawn-level" controls** had failed to block an enemy queen from slicing through. The nightmare is no abstract exercise: late last year, Stoli Group's US business filed for bankruptcy after a cyberattack **disabled its SAP systems** and forced months of manual operations [10]. In the high-stakes game of modern cybersecurity, **losing control of your pawns can mean checkmate for the entire organisation**.

The harsh reality is that traditional approaches to SAP identity and access management are reaching their **endgame**. This article uses the metaphor of chess to explore why organisations must **strategically elevate their identity management -- promoting their "pawns" into "queens"** -- to survive in today's threat landscape. We follow a narrative arc from the current crisis (the problem), through the struggle with outdated defences (the challenge), toward a strategic transformation (the resolution), and finally actionable steps (the call to action). It's a story of urgency and evolution, written in clear terms for both executives and technical teams. Just as Jeff Bezos insists on simple, narrative-driven communication, we'll cut the jargon, use vivid examples, and focus on what really matters: **securing your SAP environment before it's too late**.

The endgame is approaching for traditional SAP identity management

The SAP security landscape of 2024--2025 looks like a **chessboard mid-turn**, and the old defensive strategies are running out of moves. **SAP Identity Management (IdM)**, the on-premises user provisioning tool many organisations have relied on for over a decade, is now on a ticking clock. SAP has announced it will **end maintenance for SAP IdM on 31st December 2027** -- essentially signalling the product's end-of-life [4]. Companies can pay for limited extended support until 2030, but **there will be no like-for-like successor from SAP** [4]. In other words, a core component of many organisations' access infrastructure will retire in about **36 months**, with no direct replacement in the lineup. Experts recommend completing any migration at least six months before the deadline, meaning **the real window for transition is closer to 30 months** -- an instant

on a strategic timeline [4]. The clock is ticking, and every organisation still using SAP IdM faces an imminent decision: **advance to a new identity solution or be left defenceless on an unsupported platform**.

At the same time, the **threat environment has become unforgiving**. Sophisticated attackers are treating SAP systems as high-value targets. The **CVE-2025-31324** breach described earlier was not an isolated incident -- it was part of a coordinated campaign by **China-linked APT groups** that infiltrated hundreds of SAP instances worldwide [1]. They didn't breach these systems by *hacking around* strong defences; they walked straight through weaknesses in basic access management. This vulnerability allowed them to **place their pieces anywhere on the board without following the rules**, as one analyst put it. The result: **581 SAP systems compromised and backdoored** with malicious webshells, giving attackers persistent control [1]. Energy companies, water utilities, government agencies -- all found themselves in jeopardy from what started as a single unchecked pawn in their security strategy [1].

The **fallout from such breaches is devastating**. A recent study found the **average cost of a data breach reached £3.9 million in 2024**, up 10% from the previous year [6]. In the financial sector it's even higher -- about **£4.9 million per breach** on average [6]. And for smaller enterprises, a major cyberattack can be an existential threat: **60% of small companies go out of business within six months of a cyber-attack** [7]. These aren't abstract statistics; they are cautionary tales. The bankruptcy of Stoli's subsidiaries in the wake of an SAP ransomware attack underscored that point -- a breach can literally bring a company to its knees [10].

All of this signals **"Day 2" for legacy identity management** -- to borrow Jeff Bezos's terminology. Day 1 is vitality and innovation; Day 2 is stasis followed by irrelevance or death. Clinging to ageing access management tools and perimeter-focused security is a **Day 2 strategy**. It means operating with a false sense of safety whilst adversaries manoeuvre around your static defences. Just as a chess player who refuses to adapt their opening strategy will be outmatched by a more dynamic opponent, an organisation that assumes yesterday's IAM practices are good enough today is **setting itself up for checkmate**. The **status quo is not static** -- it's deteriorating. Every unpatched SAP vulnerability, every orphaned account with excessive privileges, every delay in modernising your identity platform is an opponent's move against you.

Strategic positioning beats reactive defence every time

So how do we respond to this crisis? The answer is by **changing the game** -- moving from a reactive, defensive crouch to a **proactive, strategic stance**. In cybersecurity, as in chess, **strategy beats tactics**. It's no longer sufficient to simply react to threats as they arise (patch this system, revoke that user, comply with this audit finding). Organisations need to be thinking **several moves ahead**, deliberately positioning their security controls like a grandmaster controlling the centre of the board.

One strategic shift gaining momentum is the adoption of **Zero Trust architecture** -- an approach that treats **identity as the new security perimeter**. Instead of the old paradigm (trust anything inside our network), Zero Trust assumes **every access request could be malicious** until verified. This philosophy mirrors the chess principle of **"control the centre"**: rather than just fortifying the edges of the network (the equivalent of castling and hiding behind pawns), you assert control over identity, authentication, and authorisation at the core of every interaction. It's a strategic posture that forces attackers into a much more difficult battle. And it's rapidly becoming the norm -- according to Gartner, **63% of organisations worldwide have now fully or partially implemented a Zero Trust strategy** [5]. Security leaders recognise that old castle-and-moat defences are outdated; in modern chess terms, purely defensive play from the back rank won't win the game when the adversary is already amongst your pieces.

Consider how this plays out with a real-world example of strategic positioning: **"castle early."** In chess, players often castle their king early in the game to tuck it safely behind defensive pawns and a rook. In cybersecurity, **"castling early" means implementing strong protective measures at the outset** -- multi-factor authentication (MFA), strict role-based access controls, and compliance controls -- **before** your organisation suffers an attack. Early adoption of frameworks like **Digital Operational Resilience Act (DORA)** in finance or **PCI-DSS 4.0** in commerce can actually bolster your security posture rather than just tick boxes. Yes, compliance is a requirement (and often a complex one), but it can be approached as an opportunity to strengthen your overall defence. Think of regulations as the rules of the game -- you can either meet them minimally, or you can leverage them to **reinforce your king's safety behind a wall of well-configured controls**. For example, when DORA took effect in early 2025 requiring comprehensive ICT risk management, leading banks used it as a catalyst to **upgrade their identity governance and incident response processes** rather than treating it as a paperwork exercise. They effectively castled: moving their "king" (critical systems) to a safer position and bringing a "rook" (robust oversight) into play.

Meanwhile, strategic positioning also involves understanding the **opponent's moves** -- the threat actors' tactics -- and countering them proactively. We know, for instance, that **advanced threat groups exploit privileged access** as a quick path to control. They target users and admins with high-level permissions, or exploit flaws that give them such access. A reactive stance would be, "We'll reset passwords when they're compromised and apply patches when we can." A proactive strategy says, **"We will minimise the chances of a compromise in the first place, and limit the blast radius if one occurs."** Concretely, that means **principle of least privilege** at all times, dynamic privilege management, continuous monitoring for anomalies, and segmented access zones so that a breach of one account doesn't open the whole kingdom. These are core ideas in Zero Trust and modern identity management. When implemented, it's like having extra queens and knights on the board anticipating and countering every enemy advance.

Real-world data validate this strategic approach. IBM's analysis of breaches shows that stolen or abused credentials are the top initial attack vector, and breaches involving compromised credentials take the longest to detect. What's the remedy? Assume every credential is untrusted until proven otherwise. Many organisations now use **risk-based authentication** that steps up verification if anything seems off (location, device, time of access). It's the equivalent of a chess player saying "I suspect that piece might not be what it seems, so I'm going to challenge it early." One CISO recently shared how implementing risk-based login checks thwarted an attempted intrusion: when an attacker used valid but compromised credentials at 2 AM from an unusual location, the system automatically prompted for an extra factor and then locked the account, **preventing a breach**. As he put it, *"Our pawns spotted the queen and blocked her path."* This is **strategic defence in action** -- not waiting for an incident, but anticipating it and **positioning your pieces to mitigate it**.

In summary, organisations must pivot from a mindset of *"Respond to the breach when it happens"* to *"Assume the breach is coming and shape the battlefield now."* In cybersecurity terms, that means **architecting your SAP environment for resilience**: adopt Zero Trust principles, make identity and access the centre of your security strategy, and put strong defences in place **before** the attackers strike. It's proactive risk management. And it works. Studies show companies with mature identity-centric security see significantly lower breach costs and dwell times than those relying on perimeter firewalls alone. As the saying goes, *offence is the best defence* -- by taking the offensive in designing a secure identity framework, you drastically reduce the opportunities for attackers. **Strategic positioning beats reactive defence every time.**

Executing the pawn promotion to transform your identity security

Understanding the need for strategic change is one thing; **executing it is another**. In chess, even when you've formulated a brilliant plan, you still have to make the sequence of moves that brings a pawn to promotion. In the context of SAP security, "**pawn to queen**" represents the transformation of a basic, limited capability (your current identity management) into a powerful, agile, and comprehensive solution. How do you actually do that in practice? What are the moves that turn theory into reality? This section lays out the key elements of **modernising your SAP identity management** -- effectively, how to achieve that pawn promotion and gain a queen on your side of the board.

1. Plan your migration early and strategically. The end-of-life of SAP IdM in 2027 is not just an IT upgrade issue; it's a strategic inflection point. Organisations should treat it as an opportunity to **reimagine their entire approach to user access**. This begins with choosing the right successor platform. Since SAP isn't providing a one-for-one replacement, you'll need to evaluate alternatives. Many companies are looking at solutions like **SAP Cloud Identity Services** (which include Identity Authentication, Identity Provisioning, and Identity Access Governance) or hybrid approaches that integrate **Microsoft Entra ID (formerly Azure AD)** for broad enterprise identity combined with SAP-specific governance tools [4]. The key is to choose a path that supports **both your SAP and non-SAP environments**, as the old SAP IdM often did. **There is no one perfect tool** -- experts note that most IAM suites have converging features [4]. What matters is selecting one that aligns with your future-state architecture (cloud, on-prem, or hybrid) and can enforce the security principles we've discussed (least privilege, continuous validation, etc.). And don't delay: Gartner's guidance, echoed by KPMG, suggests that **IAM migration projects take 24--36 months** on average. That means if you haven't started by now (mid-2025), you're already behind the ideal schedule. The **aim should be to complete your migration well before SAP IdM's support ends** [4]. Like a chess player who sees the endgame approaching, you must start advancing that pawn now if you want it to reach the eighth rank in time.

2. Implement Just-in-Time access and granular privilege control. One of the most powerful modern practices in access management is **Just-in-Time (JIT) provisioning of privileges**. Instead of giving users standing admin rights "just in case" they need them, JIT elevates a user's privileges only for a short, approved window and then automatically revokes them. This concept directly parallels controlling pawn promotion -- you only allow that transformation when absolutely necessary, under strict conditions. Analysts predict that by the mid-2020s, a significant portion of privileged

activity will rely on JIT access workflows (one Gartner survey put it at **40% of privileged access using JIT by 2025**). Many organisations are already seeing the benefit: for example, a global manufacturer implemented JIT for all SAP Basis administrators. When an admin needs to perform a sensitive task, they request elevation, which triggers an approval and logging process. They get the needed rights for, say, 2 hours, and then those rights expire. The result? They have **virtually eliminated permanent super-user accounts** and drastically reduced the risk of internal misuse or credential theft leading to disaster. JIT, coupled with **policy-based role management**, ensures you're not accidentally **"promoting all your pawns to queens"** and giving too much power to too many users. Each privilege elevation is deliberate and transient -- a controlled pawn promotion rather than an unchecked one.

3. Embrace intelligent automation and analytics. Modern identity platforms bring in the big guns -- **AI and machine learning** -- to help manage complexity. Remember the earlier analogy of having a "chess coach" who can see all possible moves? Solutions like **SAP Cloud Identity Access Governance (IAG)** and others now incorporate machine learning to analyse user behaviour, recommend roles, and flag anomalies. For instance, these systems can learn what normal access patterns look like across your SAP landscape and then detect when someone is accessing data in a way that's highly unusual (much like noticing a knight making an impossible move). In 2024, **78% of organisations globally are using AI in at least one business function**, and security is a prime area benefiting from this. By applying AI-driven analytics, companies have achieved **40--60% reductions in manual access management efforts** (such as user access reviews and compliance reporting) because the system intelligently highlights what matters. An example: a large retailer using an identity governance tool found that the AI suggested removing a certain access role from dozens of users because they never actually used it. Doing so tightened security and also cleaned up their licensing costs. Automation also speeds up incident response -- when a breach attempt happens, AI can isolate affected accounts or systems faster than any human, essentially **moving your pieces on the board at lightning speed to counter an attack**. Embracing these advanced capabilities is like augmenting your chess-playing with a powerful engine: you still set the strategy, but you have rapid, data-driven insights to execute it flawlessly.

4. Develop a migration and training playbook. Transforming your identity management isn't a one-off project; it's an ongoing programme that involves technology, process, and people. You need a **clear playbook**. On the technology side, this means charting out how you will integrate new identity services, what the interim coexistence with SAP IdM looks like (if any), and how you will cut over with minimal

disruption. On the process side, it means updating your policies -- for example, revising your **joiner-mover-leaver** process for user provisioning, re-defining how access requests are approved in the new system, and ensuring **segregation-of-duties checks** are built-in (so you don't inadvertently create toxic combinations of privileges). But perhaps most importantly, on the people side, it means **training and change management**. Your IT administrators need to become fluent in the new tools (often cloud-based interfaces instead of the old SAP IdM console). Your business role owners and auditors need to understand the new review dashboards and certification workflows. And every user should be educated on enhanced security practices (for instance, if you implement passwordless authentication or stricter MFA, users must know how to use these new methods). Ongoing education is vital -- remember, **the threat landscape evolves as rapidly as chess openings**. Regular training sessions, simulated phishing drills, and tabletop exercises for incident response will keep your team sharp. The organisations that excel in SAP security treat it as a continuous improvement journey. As one CIO put it, *"We didn't just train our people for the transformation; we trained them for the new game that follows -- because the game never really ends."*

By executing these steps, you effectively **promote your pawn**: your basic, perhaps neglected identity management process transforms into a robust, intelligent, and strategic function of the business. You go from playing draughts with access controls to playing chess. And when done correctly, it **feels like magic** -- suddenly you can see threats coming earlier, you can address compliance requirements with a few clicks, and you can grant or revoke access in hours rather than weeks. It's not easy (just as coordinating a real pawn promotion requires surviving a tough middlegame), but the payoff is immense. You'll have turned a weak point -- user access -- into one of your strongest security assets. **That pawn becomes a queen**, ready to dominate the board for your side.

Mastering the new game with continuous adaptation and vigilance

Promoting a pawn is a major achievement in chess, but it's not the end of the game -- it's the beginning of a new phase. Likewise, once you've modernised your SAP identity management and fortified your security posture, you enter a **new game**. The challenge now is to **master this new game by continuously adapting and staying ahead of emerging threats**. Cybersecurity is not a one-and-done victory; it's an ongoing contest against intelligent, evolving opponents. This means our strategies must also evolve. In this final section, we discuss how to sustain and build upon your gains -- how to ensure

that, having transformed your pawns into queens, you use them effectively and keep them safe.

Adapt to emerging technologies and threats: The tech landscape that supports your business is changing rapidly, and each innovation brings new security considerations. Take **authentication methods** as an example. We are witnessing the rapid rise of **passwordless authentication** -- methods like **passkeys** that use device biometrics and public-key cryptography instead of traditional passwords. In fact, passkey adoption has surged by **400% in 2024 alone** [8]. Today, roughly **95% of global devices support the WebAuthn standard** for passwordless login (thanks to ubiquitous support in browsers and smartphones) [9]. This is a hugely positive development for security -- it's like fundamentally improving the "locks on your doors" across the organisation. **Mastering the new game** means embracing such advancements. Companies should be planning pilot programmes for passkeys or other passwordless tech for SAP and other applications, especially for privileged users who are high-priority targets. Early adopters report smoother user experiences and fewer phishing compromises. The lesson: **don't cling to old techniques (like static passwords) out of habit if better ones are available**. Evolve your authentication and authorisation models as the industry progresses -- whether that's passkeys, biometric logins, or continuous behavioural authentication. Each of these, if implemented wisely, is another move that keeps attackers off-balance.

Looking further ahead, **quantum computing** appears on the horizon as the ultimate game-changer. Whilst still experimental, experts warn that within a decade or so, quantum computers could crack current encryption schemes that underpin everything from SAP logins to bank transactions. A leading research institute recently estimated there's a **17--34% chance of a quantum computer capable of breaking RSA-2048 by 2034** [3]. That probability leaps to nearly 80% by 2044 [3]. What does this mean for an SAP security executive? It means **quantum readiness** must enter our plans. NIST has already published three new post-quantum cryptographic standards as of August 2024 (algorithms designed to resist quantum attacks), and governments are pushing organisations to inventory and eventually upgrade their cryptography. Whilst it's not an immediate crisis, mastering the security endgame means **planning your defences years ahead**. Forward-thinking companies are starting to **encrypt their most sensitive data with quantum-resistant algorithms** (or at least have a roadmap to do so) and working with vendors to ensure future software versions will be quantum-safe. It's akin to studying new chess openings that might become relevant in future tournaments -- you prepare now so you aren't caught off guard later.

Foster a culture of continuous improvement: Modern security is as much about mindset as tools. To stay ahead of adaptive adversaries, your organisation itself must be adaptive. This involves instituting feedback loops and continuous improvement cycles for your security programme. For example, conduct **regular security drills** in your SAP environment: simulate an insider privilege abuse scenario or a ransomware attack on an SAP system, and practise your incident response. Each exercise will reveal gaps or delays that you can then fix (maybe you discover a particular system wasn't being monitored, or the response team wasn't aware of a certain data recovery procedure). Top-performing security teams often follow a model of **"practise, learn, adjust, repeat."** They treat security incidents -- whether real or simulated -- not as failures but as **lessons** that make them better. Over time, this builds a resilience and agility that tools alone can't provide. In effect, the whole team and organisation learn to **play the game at a higher level**. A useful mental model here is to think of your security programme like a biological immune system: it must constantly learn to recognise new pathogens. That means encouraging open communication when employees spot suspicious activity, blameless post-mortems when something goes wrong, and celebrating the identification of a new vulnerability as much as the blocking of an attack. When your company culture treats security as everyone's responsibility and continuously evolves knowledge, you've achieved something powerful -- **you've made your organisation a moving target that adapts faster than the threats**.

Measure success and keep executive focus: One Bezos-style principle to borrow is the importance of metrics and narratives in tandem. Executives respond to clear, concrete metrics, so develop some to track the progress of your identity and access transformation. It could be quantitative metrics like "number of privileged accounts reduced" or "percentage of access requests auto-approved by AI with no incidents," or risk metrics like "time to detect and disable unauthorised access." According to Gartner, nearly **79% of organisations implementing Zero Trust have developed strategic metrics to measure progress** [5] -- and doing so helps keep the momentum. Alongside the numbers, keep telling the narrative of security in business terms to leadership. For instance, frame the outcome of your pawn-to-queen transformation as **"we have significantly reduced the risk of a costly breach, and here's how"**. Use comparisons and stories: "Six months ago, a user could accumulate excessive access over years; now our system flags and removes it within a week, closing a door that could have led to a multimillion-pound incident." Executives in 2025 are increasingly savvy to cyber risks (boards today often ask, "Are we safe from being the next Stoli Group scenario?"). By demonstrating continuous improvement and alignment with business goals (like stability, compliance, and customer trust), you will keep them

invested in supporting security initiatives. That support, in turn, ensures you have the resources -- budget, people, priority -- to keep adapting and innovating. This forms a virtuous cycle: management support drives better security, which reduces incidents, which proves value and garners more support.

In sum, **mastering the new game** of SAP security means never resting on your laurels. You have to think and act like a grandmaster: always several moves ahead, always learning from each play, and always ready to innovate a new tactic when the situation demands. The combination of strong foundations (Zero Trust, modern IAM), agile adoption of new tech (AI, passkeys, post-quantum crypto), and a culture of continual learning is what separates the leaders from the laggards. Security is an infinite game -- but if you approach it with the right mindset, it's a game you can keep **winning**.

Conclusion: Turning strategy into action -- your move

We've travelled from the opening moves (recognising the urgent threats and outdated tools) through the middle game (implementing strategic defences and modern solutions) and into the endgame (continuous adaptation to stay ahead). The chess metaphor isn't just a gimmick -- it's a useful way to understand that **SAP security is a strategic endeavour, not a checklist**. Like chess, it's about seeing the whole board, planning your moves, and executing with skill. But unlike chess, in the cybersecurity game the stakes are **measured in jobs, reputations, and millions of pounds**, not merely points on a scoreboard. This is why all the narrative and analysis we've presented boils down to a simple, urgent message: **elevate your identity management from a pawn to a queen, or risk losing the game.**

The 581 breached systems, the bankruptcy, the multimillion-pound losses -- these are vivid signals that **traditional approaches have reached their limit**. Yet, this is not a doom-and-gloom finale; it's a call to action. Organisations that **act decisively** can turn these challenges into an advantage. The pending end-of-life of SAP IdM in 2027 is not just a deadline to dread; it's a chance to **rebuild stronger** with the latest technology and a fresh strategy. The relentless attacks by APTs can actually galvanise support for security initiatives that may have been hard to justify before ("Remember those 581 systems? We need to make sure we're never on that list."). And the evolution of tools -- from AI-driven analytics to passwordless auth -- means we have an expanding arsenal to draw upon.

Let's end with a **future-forward vision**: imagine a year from now, you're a security leader reading your board a brief report. It starts like this: *"Last year we faced serious risks in our SAP environment. Since then, we migrated to a modern identity platform,*

implemented Zero Trust for all critical access, and cut our standing privileged accounts by 90%. We have real-time analytics watching over our crown jewels. This quarter, whilst others in our industry suffered attacks, we quickly neutralised an attempted breach with zero impact. Our auditors gave us a clean bill of health, noting our improved controls. Most importantly, we've woven security into every business process -- it's now part of our company's DNA." That kind of progress is achievable -- but only if you take the initiative now.

The board is set, the pieces are in motion. **It's your move.** To ensure you're not checkmated by the next wave of threats, take the lessons from this narrative and put them into practice. Here are the key action steps to get started:

Key action steps

1. **Elevate Identity Management Now:** Initiate your migration away from SAP IdM without delay. Evaluate modern identity solutions (e.g. SAP Cloud Identity Services, Microsoft Entra ID) and plan a **36-month migration** with clear milestones [4]. Treat this as a strategic overhaul -- include integration with Zero Trust and cloud architectures from the design stage.
2. **Implement "Pawn to Queen" Controls:** Strengthen your access controls so that no user gets unchecked promotion. Enforce **least privilege and Just-in-Time access** for all high-level accounts. Review and recertify roles regularly -- use analytics to strip away excess rights. This prevents minor accounts from turning into major threats.
3. **"Castle" Your Defences Early:** Don't wait for an incident to harden your security. Deploy strong authentication (MFA or passkeys) universally, segment your network, and ensure compliance mandates (DORA, GDPR, PCI-DSS) are met **proactively** through robust controls. By securing your "king" (critical systems) now, you build resilience against inevitable attacks.
4. **Invest in Intelligence and Training:** Leverage **AI-driven security tools** to monitor behaviour and flag anomalies -- let machine speed augment your defence. At the same time, invest in your people. Conduct regular training on new threats and run breach simulations. Create a culture of security awareness where every employee becomes a sensor and every incident drives improvement.
5. **Continuously Adapt and Lead:** Establish metrics and governance to keep security efforts on track. Brief senior leadership regularly using clear narratives and data. Stay informed on emerging risks (e.g. quantum threats) and update your strategies accordingly [3]. **Security is a continuous game** -- commit to ongoing evolution, so you always stay a few moves ahead of the adversaries.

By taking these steps, you transform your SAP security posture from reactive to proactive, from vulnerable to resilient. In chess, the player who masters both strategy and tactics wins. In SAP security, the organisation that combines visionary strategy with diligent execution will not only thwart today's attacks but also **thrive amid tomorrow's challenges**. The pawn promotion principle teaches us that with the right approach, even your lowest-value pieces can become your greatest strength. It's time to apply that principle and ensure that every "pawn" in your security programme is on a path to becoming a queen -- powerful, agile, and firmly on your side of the board. **Your organisation's security, success, and survival depend on it.**

Annotated Bibliography

Ref	Publication & date	Key point cited
[1]	**The Hacker News** (13 May 2025) *"China-Linked APTs Exploit SAP CVE-2025-31324 to Breach 581 Critical Systems Worldwide."*	CVE-2025-31324 breach details and 581-system figure.
[2]	**Onapsis Threat Intelligence Brief** (May 2025) *"Active Exploitation of SAP Vulnerability CVE-2025-31324."*	CVSS 10.0 rating and Visual Composer upload vector.
[3]	**SecurityWeek** (Jan 2025) *"Cyber Insights 2025: Quantum and the Threat to Encryption."*	17--34% probability of a CRQC by 2034; 79% by 2044.
[4]	**IBsolution Blog** (3 Jan 2024) *"End of maintenance 2027 for SAP IdM -- what companies need to do now."*	SAP IdM EoM date, absence of successor, 36-month migration guidance.
[5]	**Dark Reading** (Apr 2024) *"Zero Trust Takes Over: 63% of Organisations Implementing Globally."*	Global 63% zero-trust implementation statistic.
[6]	**IBM Press Release** (30 Jul 2024) *"Escalating Data Breach Disruption Pushes Costs to New Highs."*	USD 4.88 million global breach cost; USD 6.08 million for finance.
[7]	**Cybersecurity Ventures** (undated) *"60% of Small Companies Close Within Six Months of Being Hacked."*	Statistic on small-business failure after cyber-attack.
[8]	**The Verge** (30 Jul 2024) *"Dashlane says passkey adoption has increased by 400 percent in 2024."*	400% surge in passkey authentications.
[9]	**Descope Blog** (May 2025) *"WebAuthn traction: 95% of global devices support passwordless."*	95% global device/browser support for WebAuthn.
[10]	**BleepingComputer** (3 Dec 2024) *"Vodka maker Stoli files for bankruptcy in US after ransomware attack."*	Stoli Group bankruptcy and SAP ERP disruption.