Integrity360

your **security** in mind

2025

CYBER SECURITY TRENDS & PREDICTIONS

Integrity360

your security in mind

Integrity360
your security in mind

Message from the CTO

In 2025, the cyber security landscape is poised for significant changes, influenced by rapid technological advancements, evolving threat vectors and new regulations. The continued adoption of artificial intelligence (AI) and the possible coming of age of quantum computing will also create both opportunities and challenges.

AI's integration into cyber security has promised to revolutionise threat detection and response mechanisms. AI-driven systems can analyse vast datasets to identify anomalies and predict potential attacks, enhancing proactive defence capabilities. However, adversaries are also leveraging AI to develop more sophisticated attack methods, such as AI-generated phishing schemes and malware, which can bypass traditional security measures. This dual-edged nature of AI underscores the need for continuous innovation in defensive strategies.

The advent of quantum computing poses a substantial risk to current cryptographic standards. When Q-Day arrives, quantum computers have the potential to break widely used encryption algorithms, compromising data security across sectors. In response, **organisations need to start transitioning to quantum-resistant cryptographic methods now in order to safeguard sensitive information against future quantum-enabled threats.**

The adoption of Zero Trust Architecture (ZTA) is becoming increasingly critical. Once a buzz word but is now the reality of network & identity security, securing access to systems and data. ZTA operates on the principle that no entity, whether inside or outside the network, should be trusted by default. Implementing ZTA involves strict identity verification, continuous monitoring, and micro-segmentation to minimise attack surfaces and prevent lateral movement within networks.

As well as these new advanced threats, it is clear that the cyber security sector still has a lot to do in order to get organisations to get the basics right. Weak and re-used passwords combined with a lack of MFA, not keeping systems patched with the latest updates and other basics that we often take for granted are, by far, still the biggest threats organisations face in 2025.

Richard Ford
Integrity360 CTO

Organisations must prioritise understanding and mitigating their exposure to cyber threats. This involves identifying and securing potential vulnerabilities across all facets of operations. Simultaneously, building resilience is crucial in developing the capacity to withstand, respond to, and recover from cyber incidents. This dual focus will be instrumental in navigating the complex and evolving cyber threat landscape of 2025 and beyond.

The Human Cyber Equation

2025 will see the cyber security landscape increasingly embrace AI. While these innovations fortify defences and counter threats, they also pose significant challenges—particularly for the people on the frontlines. At the core of cyber security lies a critical, often overlooked element: the human aspect.

AI is not a silver bullet

Despite its potential, AI is not the magic solution that some proffered initially. Technologies like automated threat detection may be able to process data in real time, detect anomalies, and identify threats swiftly but AI is far from infallible. Its complexity and reliance on human oversight make the interplay between human and machine decision-making more crucial than ever. Professionals must still interpret and validate AI-generated insights, ensuring they are actionable and accurate.

The human cost of cyber security

Amid these advancements, the cost and consequences of cyber security breaches on people remains significant. Professionals face relentless pressure, with the stakes higher than ever. A single oversight can lead to catastrophic breaches, financial losses, or reputational damage.

This pressure, coupled with a persistent talent shortage, has led to widespread burnout. Long hours, high stress, and excessive workloads are common, undermining both individual well-being and team performance. AI is not a silver bullet

A human-first future

Addressing these challenges requires balancing AI's potential with human well-being. For example, automating repetitive tasks can free teams to focus on strategic decisions and problem-solving. Organisations must prioritise mental health through flexible work arrangements, counselling, and fostering a supportive culture. Equally important is putting humans at the centre—empowering the general user population to be part of the solution in defending company data, rather than part of the problem.

2025

will see the cyber security landscape increasingly **embrace AI**

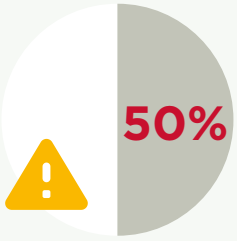
As the industry advances, the human cyber equation remains one of interdependence. Machines enhance human capabilities, but humans provide creativity, adaptability, and ethical oversight. By placing people at the centre of cyber security strategies, organisations can defend against threats while empowering their greatest asset: their people.

Integrity360
your security in mind

2024 in 24 statistics

In 2024 Integrity360 collated data from our internal tools and services. Below are some notable statistics our team gathered across a range of key subjects as well as some major statistics curated by the wider industry.

Integrity360 stats

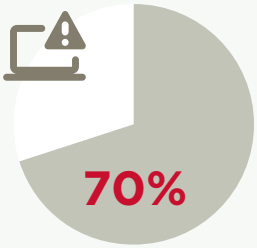


of vulnerabilities seen by Integrity360 were of high severity

3 years

on, Log4Shell is still one of the most common attacks

of recorded exploit attempts were targeting vulnerabilities from the 2010s

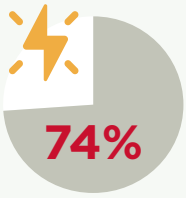


of recorded incidents were targeting high impact vulnerabilities

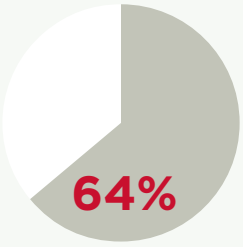
97 days

was the average time for organisations to patch critical vulnerabilities

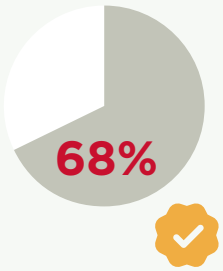
AI



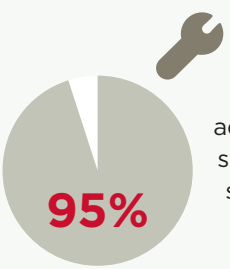
of IT security professionals report their organisations are suffering significant impact from AI-powered threats
- Darktrace



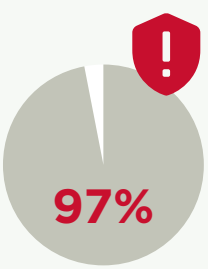
of organisations have adopted AI or machine learning in their cyber security measures as of 2024
- Gartner



of UK and Ireland based organisations will make AI their top deployed technologies in 2025
– Gartner



of security professionals anticipate that adopting AI cyber security tools will strengthen their security efforts
- Darktrace



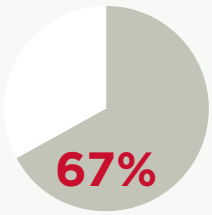
of cyber security professionals fear their organisations will face AI-generated security incidents
– Deep Instinct

Integrity360
your security in mind

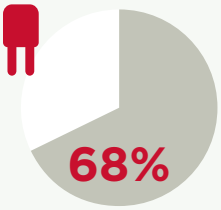
2024 in 24 statistics

Cyber attacks

year-over-year increase in the number of weekly cyber attacks recorded by organisations
– Check Point



of successful cyberattacks result from human negligence or human-based attacks, such as phishing
- ISACA Journal

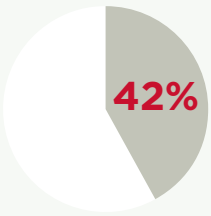


of breaches involved a human element in 2024
- Verizon

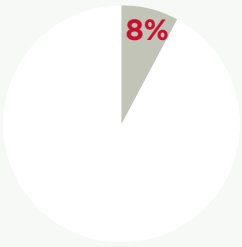
$2.73 million

was the average ransom demanded in a ransomware attack which is almost $1 million more than 2023
– Varonis

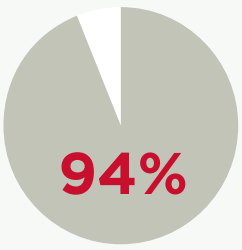
increase in cloud intrusions, highlighting the need for robust cloud security measures
- CrowdStrike



of companies reported suffering from cyber fatigue, or apathy to proactively defending against cyberattacks in 2024
- Cisco



of businesses who pay ransoms to hackers receive all of their data in return
– Sophos



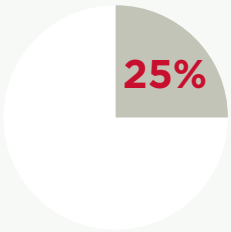
of all malware was delivered by email
– Varonis

Integrity360
your security in mind

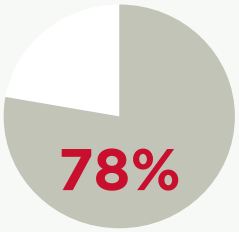
2024 in 24 statistics

Cyber industry

increase in Global expenditure on cyber security in 2024
– Gartner



increase in spending on cloud security products and services in 2024
– Gartner

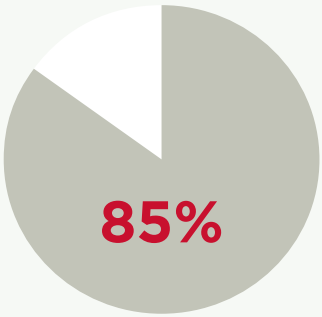


of organisations feel their cyber resilience is insufficient to meet their needs
– World Economic Forum

MDR and MSSPs

of organisations will utilise MDR services for threat monitoring, detection, and response functions in 2025
- Gartner

of organisations have outsourced at least part of their security operations to MSSPs in 2024
– MSSP Alert



was the customer satisfaction rate for MSSPs in 2024, indicating a high level of trust and reliance on managed security services
– **MSSP Alert**

Integrity360
your security in mind

The biggest cyber attacks of 2024

Dell data breach exposed information on 49 million customers in major cyber attack

In May, Dell warned customers about a significant data breach after a threat actor claimed to have stolen information on approximately 49 million individuals. Dell began sending out notifications, confirming that a portal containing customer data related to purchases had been compromised.

Exposed data included customer names, physical addresses, and order details

Dell's statement at the time revealed that the exposed data included customer names, physical addresses, order service tags, item descriptions, order dates, and warranty information. Fortunately, no financial or payment information, email addresses, or phone numbers were involved, which Dell believed helped reduce the potential risk to customers.

A threat actor identified as Menelik exploited Dell's partner portal by registering unverified accounts as resellers. Once approved, they brute-forced customer service tags over three weeks, extracting sensitive data. The breach exposed names, addresses, and order details of 49 million customers. Dell confirmed no financial information was compromised and discovered the breach post-hacker notification.

49

million customers

Menelik, had attempted to sell the stolen data on the Breach Forums hacking site, claiming it included records of purchases made between 2017 and 2024. Dell immediately launched an investigation and notified affected customers. The company reassured users that no highly sensitive information had been compromised.

560 million customer details stolen in Ticketmaster breach

In June 2024, Ticketmaster faced major scrutiny when its parent company, Live Nation, confirmed a massive data breach. Hackers known as ShinyHunters claimed they had stolen the personal information of 560 million customers and demanded a $500,000 ransom to prevent the sale of this data on the dark web. The stolen information included names, addresses, email addresses, usernames, and partial credit card details, leaving many customers vulnerable.

The ShinyHunters group targeted Ticketmaster via Snowflake, a third-party cloud data warehouse. Using stolen credentials obtained through malware, likely from phishing attacks, they accessed a Snowflake account. Lateral movement enabled the exfiltration of data on up to 560 million Ticketmaster customers. Snowflake denied responsibility but highlighted the risks of single-factor authentication.

This incident wasn't Ticketmaster's first security issue. In 2020, Ticketmaster admitted to hacking a competitor, resulting in a $10 million fine. More recently, in November 2023, an alleged cyberattack disrupted ticket sales for Taylor Swift's Era's tour. The incident underscores ongoing cyber security challenges within the entertainment industry.

Change Healthcare cyber attack exposed patient data, disrupted US healthcare system

First disclosed on 22 February, the cyberattack on Change Healthcare caused massive disruption in the US healthcare system for weeks. In response to the ransomware attack, an IT system shutdown was initiated, preventing many pharmacies, hospitals, and other healthcare facilities from processing claims and receiving payments. The Russian-speaking cybercriminal group known as BlackCat or ALPHV claimed responsibility. UnitedHealth Group CEO Andrew Witty confirmed in his Congressional testimony in May that the company paid a $22 million ransom following the attack.

Subsequently, another cybercriminal gang called RansomHub posted data it claimed was stolen from Change Healthcare. In late April, UnitedHealth revealed that data belonging to a "substantial proportion" of Americans may have been stolen in the attack against Change Healthcare, a unit of its Optum subsidiary. Witty testified that "maybe a third" of all Americans were impacted. In June, Change Healthcare disclosed that sensitive patient medical data was exposed, potentially including diagnoses, medicines, test results, images, care, and treatment.

The cyberattack stemmed from a legacy server lacking multifactor authentication, highlighting a compliance gap. While adherence to HIPAA Security Rule standards reduces risks, it cannot guarantee complete immunity from cyberattacks, underscoring the need for continuous improvements in security measures to address evolving threats.

Other major cyber attacks in 2024

Ransomware attack

- **Ascension Health system ransomware attack:** Ascension—a nonprofit health system with 140 hospitals operating across 19 states and Washington, D.C.—announced that its clinical operations were disrupted due to a ransomware attack. The breach severely impacted hospital operations across multiple states, disrupting Ascension's electronic health record (EHR) system MyChart. The ransomware attack was caused by an employee who had downloaded a corrupt file onto one of the organisation's devices.

270,000 military personnel data

- **UK military major data breach:** Hackers infiltrated the UK Ministry of Defence's payroll system, exposing sensitive personal information of 270,000 current and former military personnel. The breach included names, bank details, and other private data.

  Malicious actors accessed a segment of the armed forces payment network through an external system entirely separate from the Ministry of Defence's core network and unlinked from the primary military HR system.

$25 million ransom

- **CDK ransomware attack:** In June 2024, CDK Global, a leading US-based software provider for the automotive industry, suffered a significant ransomware attack. The BlackSuit ransomware gang, linked to Eastern Europe and Russia, claimed responsibility, demanding a ransom that escalated from $10 million to over $50 million. Reports suggest they paid a $25 million ransom to BlackSuit, however, the disruptions caused by the breach cost over $1 billion in financial losses. BlackSuit used phishing and software vulnerability exploits to compromise CDK. Phishing campaigns targeted employees, stealing credentials or deploying malware, while dealerships connected via always-on VPNs enabled further access. Once inside, attackers moved laterally, using credential dumping and exploiting weak permissions to infiltrate additional systems and steal sensitive data.

5,000 customers data

- **Transport for London cyber attack:** A cyberattack on Transport for London (TfL), saw attackers breach systems and access sensitive customer data. The compromised information included Oyster refund data, bank account numbers, sort codes, and personal contact details for around 5,000 customers. Police have arrested a teenager from Walsall in connection with the cyberattack highlighting the risks posed by script kiddies looking for easy targets.

Trends for 2025

The human element: Our greatest weakness but also our greatest strength

The divide between man and machine has never been smaller. We've seen this lead to the emergence of deepfakes, which are relatively trivial to create, that can fool users into thinking they are interacting with real human beings. As AI technology continues to improve its going to become even harder to discern between what is real and what is fake. We can expect to see phishing scams and authorised push payment fraud become more sophisticated, for instance, necessitating better security awareness training to build a culture of vigilance. Employees need to become the first line of defence, transforming them into active participants in safeguarding the organisation against evolving threats, while more advanced detection technologies help to look for such incidents.

The extent to which the cyber security culture is embedded within the organisation will depend upon effective leadership. As a sector we still need to refine the way in which we communicate cyber security risks and strategies at board level, and how we translate technical challenges into relatable business impacts. If we get that right, it will become easier to secure executive buy-in that then results in meaningful action.

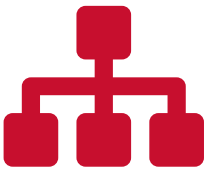
Integrity360
your security in mind

XDR to gain ground as a preferred alternative to SIEM

The Extended Detection and Response (XDR) market is finally reaching a consensus, enabling wider adoption and clear differentiation from traditional Security Information and Event Management (SIEM) platforms. XDR combines data collection across endpoints, cloud, identity, and networks to deliver comprehensive threat detection and response capabilities.

As SIEM platforms face criticism for being costly and rules-dependent, XDR is emerging as a more agile, scalable alternative. Its predictable pricing and unified approach make it an attractive option for organisations aiming to simplify security operations. By late 2025, XDR could become the default solution for most organisations, relegating SIEM to a niche role for larger enterprises with specific analytics needs.

The appeal of XDR lies in its capacity to provide full lifecycle security management—from threat protection to detection and response—offering an integrated approach that outpaces the often fragmented capabilities of SIEM. As AI becomes more embedded within security tools, XDR solutions are expected to surpass traditional SIEM systems, which may become increasingly niche, catering mainly to large enterprises requiring custom log analytics and extended retention.



XDR combines data collection across endpoints, cloud, identity, and networks

Integrity360
your security in mind

Time to patch and remediate will lengthen due to the complexity of IT/OT systems and unsupported IoT

2025 is expected to see a significant rise in patching and remediation times for cyber security vulnerabilities, driven by the growing complexity of IT/OT systems and the prevalence of unsupported IoT devices. Our 2024 findings reveal that it takes organisations an average of 97 days to address critical vulnerabilities and 146 days for low-impact ones, far above best practice recommendations of 7-30 days. These delays expose organisations to extended windows of risk, allowing attackers to exploit known vulnerabilities.

Several obstacles make timely patching challenging. Many vulnerabilities span interconnected IT and OT systems, which makes them difficult to isolate and repair without risking downtime for critical operations. Some IoT devices, no longer supported due to vendor bankruptcies or obsolete technology, further complicate efforts, as these devices lack patching capabilities or official updates. Additionally, many end-user devices fall through the cracks in patch cycles, either because they are not properly accounted for or due to the limitations of existing patching tools.

A worrying trend is that organisations often focus on new technologies rather than on fundamental cyber hygiene practices, leading to repeated patching delays. Until organisations prioritise system configuration, patch management, and vulnerability tracking, these extended remediation timelines will persist, leaving networks vulnerable to exploitation. Our research also indicates that Java, Zoom, Microsoft products, and Chrome are among the most frequently unpatched software, highlighting the need for improved visibility and exposure management to reduce overall threat levels effectively.

Integrity360
your security in mind

AI will mature, driving autonomous cyber security tools

As we move into 2025, trust in Generative AI is set to grow, accelerating its adoption. Despite early challenges such as data leaks and “hallucinated” results, the narrative is shifting as vendors refine their models and organisations establish governance frameworks to mitigate risks. These improvements will help organisations unlock AI’s potential and realise returns on their investments.

To date, Generative AI’s role in cyber security has largely been as an assistant—summarising data rather than analysing it deeply or responding independently. However, as the technology matures, it is poised to transition from augmentation to autonomy. By late 2025, organisations are likely to embrace AI-driven autonomous responses, marking a new era for Security Operations Centres (SOCs). The AI-augmented SOC will see machines sharing responsibility for decision-making and incident response, reducing reliance on human analysts for first-line actions.

The evolution of AI tools could transform the cyber security landscape, positioning them as more than assistants and advancing towards autonomous, decision-making roles. By automating routine tasks and providing more accurate threat analysis, AI-driven SOCs would free human analysts to focus on more complex, strategic tasks, potentially reshaping cyber security operations and response protocols in organisations across industries.

Integrity360
your security in mind

Budgets and spend will focus on driving vendor consolidation

As economic challenges continue, 2025 is expected to bring a strategic shift in how organisations allocate cyber security budgets, with a focus on vendor consolidation. While cyber security spending has generally been insulated from economic downturns, inflation and rising costs are now putting pressure on organisations to manage spending more carefully.

The squeeze on cyber security budgets, alongside competing pressures such as the availability of cash and credit, will continue to be felt in the vendor space resulting in more vendor consolidation.

Many organisations will look to consolidate their vendor portfolios or outsource security functions to managed security service providers (MSSPs). By reducing the number of platforms to monitor and simplifying vendor relationships, organisations aim to improve efficiency and streamline security management, often by consolidating with trusted providers that offer multi-layered, all-in-one solutions. Vendor consolidation can also lower costs associated with managing multiple vendor contracts and diverse systems, freeing resources to address core security concerns.

This drive for consolidation will also likely lead to increased mergers and acquisitions within the cyber security sector in 2025. Larger vendors may seek to gain market share and expand their capabilities through a cquisitions of smaller, innovative companies, creating comprehensive solutions that can address a range of security needs. The vendor landscape in cyber security will continue to evolve, favouring companies that can offer robust, consolidated platforms.

Just some of the mergers and acquisitions in 2024

- **Cisco - Splunk** ($28 billion)
- **Palo Alto – IBM QRadar** ($500 million)
- **Hewlett Packard Enterprise - Juniper Networks** ($14.3bn)
- **Rapid7 - Noetic Cyber** (no details released)
- **Fortinet – Next DLP** ($96 million)
- **Armis – Silk Security** ($150 million)

Quantum computing could become a reality and a threat to encryption

Quantum computing could become a transformative force in 2025, with significant implications for data security and encryption methods. Traditional cryptographic techniques, which have underpinned data protection for decades, may soon be rendered vulnerable by quantum computing's vast processing power. Unlike classical computing, which relies on binary states, quantum computing can perform calculations at speeds and complexities previously thought impossible, posing an existential threat to encryption algorithms that depend on complex mathematical problems for security.

As quantum technology becomes commercially viable, it will challenge current encryption methods, sparking a period of urgency among organisations to adapt their security strategies. Quantum-resistant encryption techniques are already in development, but the transition will be complex and costly. Organisations that rely heavily on embedded encryption, such as those in finance and healthcare, will be especially vulnerable, as retrofitting quantum-resistant solutions could require significant overhauls to infrastructure.

This shift will likely lead to a surge in demand for quantum-secure products and services, marking a new phase of investment and innovation in cyber security. Companies that act swiftly to adopt quantum-resistant encryption will be better positioned to maintain the integrity of their data assets, while those slow to adapt may face heightened risks as traditional encryption methods become easier to break. Quantum computing's entry into the mainstream will be a defining moment for cyber security, reshaping the landscape and setting new standards for data protection in the face of unprecedented computational power.

The National Institute of Standards and Technology (NIST) is advancing efforts to develop post-quantum encryption standards to protect against future quantum computing threats. Quantum computers could potentially break traditional cryptographic algorithms, jeopardising sensitive data. NIST's initiative includes rigorous testing of new algorithms designed to withstand quantum attacks. These advancements aim to future-proof global cyber security frameworks, ensuring robust encryption in the era of quantum computing.

Integrity360
your security in mind

Cloud security will evolve thanks to CNAPP and CTEM adoption

Cloud security is undergoing a transformation. The shift to native cloud applications is driving demand for Cloud Native Application Protection Platforms (CNAPPs), designed specifically to secure modern, cloud-centric environments and applications that run within them. This evolution is also reshaping security teams, placing greater emphasis on cloud expertise as a core competency.

Meanwhile, vulnerability management is evolving into Continuous Threat Exposure Management (CTEM), which goes beyond traditional practices to provide a continuous, proactive approach to mitigating cyber risks. CTEM reduces the time taken to address critical exposures, by focusing on key risk areas and leveraging automation. This integrated approach to managing vulnerabilities and risk will become a cornerstone of organisational security strategies moving forward.

CTEM reduces the time taken to address critical exposures

Integrity360
your security in mind

Navigating the Digital Operational Resilience Act (DORA)

By James Eason Integrity360 CRA Practice Lead

As DORA becomes enforceable in January 2025, financial entities across the EU must act swiftly to achieve compliance. With the deadline imminent, organisations need to prepare now to meet the regulation's stringent standards. This guide explores DORA's five core pillars.

What is DORA?

The Digital Operational Resilience Act (DORA) is a framework introduced by the EU to reinforce the resilience of the financial sector. Designed to address diverse digital risks, it mandates comprehensive measures for financial entities and their third-party providers to withstand and recover from cyber incidents and operational disruptions.

Why DORA compliance is urgent

The Digital Operational Resilience Act (DORA) is a framework introduced by the EU to reinforce the resilience of the financial sector. Designed to address diverse digital risks, it mandates comprehensive measures for financial entities and their third-party providers to withstand and recover from cyber incidents and operational disruptions.

Integrity360
your security in mind

The 5 Pillars of DORA

DORA's framework is structured around five key pillars, each fortifying distinct aspects of digital resilience within financial entities. Here's a look at these pillars and how Integrity360 can support your organisation's compliance journey.

1. ICT Risk Management

This pillar requires financial entities to identify, assess, and mitigate risks associated with Information and Communication Technology (ICT). It mandates robust internal governance and controls for effective risk management.

2. ICT-Related Incident Management

Organisations must establish processes for rapid detection, management, and notification of significant cyber incidents. Effective incident management is essential for maintaining operational continuity and regulatory compliance.

3. Digital Operational Resilience Testing

Regular resilience testing is essential for ensuring that organisations can withstand ICT-related risks. Comprehensive testing helps identify, address, and mitigate potential vulnerabilities.

4. Third-Party Risk Management

In an interconnected digital landscape, managing third-party risks is critical. DORA requires entities to conduct thorough assessments and maintain strong contractual agreements with their third-party service providers.

5. Information Sharing

DORA encourages the sharing of cyber threat intelligence within the financial sector to foster a collaborative approach to cyber defence. This pillar helps organisations stay vigilant and better prepared for emerging threats.

If you need assistance with becoming DORA compliant, contact our experts.

Integrity360
your security in mind

AI-driven security and compliance challenges in 2025

By James Eason, CRA Practice Lead at Integrity360

As artificial intelligence (AI) will become increasingly integral to business operations in 2025, James Eason, CRA Practice Lead at Integrity360, highlights the crucial steps organisations should take to navigate evolving cyber security and compliance demands.

Establish an AI governance team:

Assembling a diverse team across IT, cyber security, compliance, and business functions. “A cross-functional approach is essential to address AI risks from multiple perspectives,” he notes. Regular reviews will help the team stay responsive to new threats and comply with tightening regulations like GDPR, NIS2, and DORA.

Map AI systems and data flows:

The importance of an up-to-date inventory of AI systems. Documenting each AI system’s role and data interactions allows for a proactive approach to identifying and mitigating risks, especially with sensitive data.

Analyse technical, ethical, and compliance risks

The focus on data privacy and ethics will only intensify. “AI systems must be resilient against cyber threats, ethical pitfalls, and regulatory non-compliance.” Risk workshops and defined thresholds will enhance resilience against these threats, he suggests.

Stay current with AI regulations

As AI governance evolves, so must compliance efforts. Eason advises appointing a team member to track regulatory updates and ensure seamless integration of new compliance requirements. “Maintaining thorough documentation is critical for audits and fosters transparency,” he explains.

Foster organisation-wide AI awareness

“An informed team is your best defence,” Eason says, recommending training sessions across departments to heighten AI risk awareness and encourage a proactive reporting culture.

Gain a competitive advantage with strategic AI risk management

Organisations adopting a responsible AI approach will strengthen their market position in 2025. “Clients value privacy and ethical integrity; by aligning AI risk management with these principles, you build trust and reduce regulatory risks.”

In 2025, the organisations that prioritise AI responsibility and resilience will stand out as leaders in cyber security and compliance giving them a competitive advantage. By following these steps, companies can navigate the future of ethical and compliant AI deployment confidently.

Integrity360
your security in mind

Will Cloud Security Posture Management die in 2025? The evolution of CSPM

By Ahmed Aburahal, Technical Product Manager at Integrity360

In the fast-paced realm of cyber security, it's easy to assume that as new technologies emerge, the old ones fall away. Does this really apply to Cloud Security Posture Management (CSPM), with some questioning whether it's still relevant. Is CSPM dead, as some would suggest, or has it simply evolved into a more complex form? The short answer: CSPM is very much alive, but it now operates within a broader framework.

What is the objective of CSPM?

CSPM's objective is straightforward: continuously monitor cloud infrastructure for misconfigurations and security risks, flagging potential vulnerabilities before they can be exploited. It enforces cloud security best practices by identifying non-compliant assets and providing remediation guidance, or even better, auto-remediation capability.

CSPM as part of CNAPP

The rise of Cloud-Native Application Protection Platforms (CNAPP) has brought with it a shift in how cloud security is approached. CNAPP is a comprehensive solution designed to provide end-to-end security for cloud-native applications. It combines several capabilities, such as runtime protection, workload security, and identity management, into one platform.

While CNAPP expands cloud security coverage by incorporating features like workload protection and identity security, CSPM remains integral, addressing misconfigurations and compliance issues at the infrastructure level.

Think of CNAPP as a multilayered security framework, with CSPM acting as one of the foundational layers. CNAPP is designed to secure cloud-native applications from development to deployment, and it relies on CSPM's ability to manage the security posture of the underlying cloud infrastructure. Without CSPM's continuous assessment of cloud configurations, CNAPP's other features would be addressing a fundamentally insecure environment.

Remediation: the real challenge

Misconfigurations remain the top cause of cloud security incidents. CSPM automates detection and offers semi-automated remediation, combining speed with human oversight. It enforces preventive measures, reduces attack surfaces, ensures continuous compliance, and complements CNAPP capabilities. While cloud environments grow, CSPM remains essential for securing the foundational infrastructure of the cloud.

Integrity360
your security in mind

Why getting the basics right in 2025 has never been so important

Organisations across the globe continue to struggle with the basics of cyber security. Despite repeated warnings and education from cyber security firms and governments the message is still falling on far too many deaf ears. With threats advancing, getting the basics right is just the first vital step needed in defending an organisation.

In the UK cyberattacks have cost British businesses an estimated £44 billion ($55.08 billion)[1] in lost revenue over the past five years, with 52% of private sector companies reporting at least one attack during this period, according to insurance broker Howden.

Globally, the picture is similarly concerning with a study revealing that over 60%[2] of businesses worldwide experienced a cyberattack in the past year, and nearly 45% of small and medium enterprises reported being unable to recover from basic breaches due to insufficient defences.

60%

of businesses worldwide experienced a cyberattack in the past year

This continuing widespread gap in basic cyber security measures exposes organisations to significant risk, as the foundations of a secure environment remain weak. But it also highlights a critical opportunity: by addressing these gaps and going beyond the basics, businesses can transform their approach to defending against today's advanced cyber threats.

Where the basics go wrong

Fundamental measures like setting strong passwords (and better yet – Multi Factor Authentication (MFA), applying software updates, and limiting access to sensitive data are essential, yet many businesses fail to implement them consistently. The reasons are varied:

- **Skills gaps:** As highlighted by the UK government's findings, employees often lack the training and confidence to perform basic tasks.
- **Resource constraints:** Smaller businesses in particular struggle with the time and budget required to implement foundational measures effectively.
- **Underestimating the threat:** Many organisations mistakenly believe they are not targets, leaving them unprepared when an attack occurs.

Continuous monitoring

A key trend for 2025 is the shift from periodic security checks to continuous monitoring. “Cyber threats evolve in real-time, and so must our defences,” Ford notes. Continuous monitoring enables organisations to detect, control, and respond to risks as they emerge, rather than relying on outdated point-in-time assessments.

By embracing solutions like Extended Detection and Response (XDR), which revolutionise threat detection and response by providing wide visibility across environments, businesses can enhance their security posture. Combined with Managed Detection and Response (MDR), organisations gain the ability to prioritise critical risks and respond swiftly to minimise potential damage.

Addressing skills and confidence gaps

Bridging the cyber security skills gap is crucial for ensuring basic tasks are carried out effectively. Training employees and empowering them with the confidence to manage cyber security risks is a critical step. However, many organisations are turning to external providers to complement internal capabilities.

“Outsourcing cyber security tasks to managed providers can fill the gaps left by internal teams,” Ford suggests. “This not only enhances resilience and provides for critical security controls but also ensures access to expertise when it’s needed most.”

The role of incident response plans

Organisations that lack a robust incident response plan often find themselves scrambling when an attack occurs. Ford emphasises the importance of clear, actionable procedures for detecting, controlling, and recovering from threats.

“Your incident response plan should include employee training, right up to board level, as human error can exacerbate the impact of an attack,” Ford explains. “Combined with advanced detection tools, businesses can significantly reduce the likelihood and severity of breaches, nipping them in the bud before they become full blown incidents.”

Prioritising Vulnerability Management with CTEM

Continuous Threat Exposure Management (CTEM) is emerging as a must-have for organisations looking to go beyond the basics. CTEM provides prioritised insights into exposures, enabling organisations to strategically address vulnerabilities and allocate resources more effectively.

Ford highlights that CTEM shifts the focus from reactive to preventative measures, helping organisations strengthen their security posture before threats materialise.

Collaboration across teams

Cyber security is no longer the sole responsibility of IT departments. Effective protection requires collaboration across teams, ensuring that security measures are integrated throughout the organisation. Ford calls for stronger alignment between IT and security teams to create a unified defence strategy, but also between security teams and functions so each control is integrated ensuring the whole is greater than the sum of the parts.

2025 is the year to get it right

The statistics make it clear that too many organisations are still struggling with the basics of cyber security. But the path forward is equally clear. By addressing skills gaps, embracing continuous monitoring, implementing robust incident response plans, leveraging CTEM, and fostering cross-functional collaboration, businesses can build a more resilient defence against cyber threats.

“The fundamentals matter, but they must be paired with advanced strategies to stay ahead of evolving threats,” Ford concludes. In 2025, organisations that tackle these challenges head-on will be better equipped to protect their systems, data, and reputation in an increasingly complex cyber landscape.

1. YouGov survey
2. Bitdefender’s global Hacked Off! Study

Integrity360
your security in mind

How CTEM will help organisations with 5 major challenges in 2025

As we move into 2025, the cyber security landscape is growing more complex and demanding than ever. Threats evolve at an unprecedented pace, leaving traditional approaches such as Penetration Testing or Red Team Testing struggling to keep up. These essential methods often rely on periodic assessments, potentially leaving gaps in continuous visibility. Enter Continuous Threat Exposure Management (CTEM): a proactive approach designed to provide constant protection all year round.

Here's how CTEM will help businesses tackle five of the most pressing challenges in cyber security for 2025:

1. Volume of vulnerabilities

The sheer number of vulnerabilities that organisations must address is staggering. This is particularly challenging for businesses operating across on-premises, cloud, or hybrid environments, where distinguishing critical risks from less urgent ones can overwhelm security and IT teams.

How CTEM addresses this:

CTEM validates and prioritises exposures continuously, focusing on those that pose the highest risk. This prioritisation ensures IT resources are channelled into addressing vulnerabilities with the greatest potential to enhance security. Moreover, continuous scoping ensures every potential exposure across the organisation is accounted for, providing a comprehensive and focused security effort.

2. Fragmentation between security and IT teams

Security and IT teams often work in silos, with security prioritising risk elimination and IT tasked with maintaining operational efficiency. This disconnect can lead to delays, friction, and increased cyber risk.

How CTEM addresses this:

CTEM fosters collaboration by creating a unified programme with clearly prioritised actions based on risk. This alignment ensures both teams work towards shared goals, reducing tension and increasing efficiency. By leveraging CTEM as a service, organisations can also bring third-party providers into the fold, creating seamless collaboration and a stronger overall posture.

3. Limited internal resources for remediation

Resource constraints are a common challenge, especially for smaller organisations. Competing priorities can lead to critical exposures being overlooked, increasing the likelihood of breaches.

How CTEM addresses this:

CTEM offers more than just insights—it mobilises teams with validated, prioritised recommendations to tackle the most critical issues first. For businesses with limited resources, CTEM providers can augment internal teams or clear historic backlogs, ensuring exposures are addressed swiftly and effectively.

4. Adapting to emerging threats

Static, one-off security measures are no match for the constantly evolving nature of cyber threats. Organisations need a solution that adapts to new exposures and attack vectors in real time.

How CTEM addresses this:

CTEM operates on a continuous, iterative cycle. By staying updated with the latest threat intelligence and adapting dynamically to emerging risks, organisations remain resilient against evolving cyber threats. This approach ensures that the security posture is always improving, providing a robust defence against new challenges.

5. Fear of financial and reputational damage

A data breach can devastate an organisation, not only in financial terms but also by eroding customer trust. Many businesses pour resources into cyber security without a clear strategy, leading to inefficient investments.

How CTEM addresses this:

CTEM reduces the risk of breaches through its continuous exposure management. According to Gartner, organisations using continuous programmes like CTEM are three times less likely to experience a breach by 2026. This ensures businesses can protect their assets, enhance their reputation, and maximise the return on their security investments.

Adoption of CTEM will increase in 2025 as organisations increasingly recognise its value as a proactive and cyclical approach to addressing security challenges. CTEM enables businesses to prioritise risks effectively, align internal teams with strategic security goals, and adapt swiftly to the ever-evolving threat landscape. By continuously refining their security posture, organisations can not only reduce risk exposure but also enhance asset protection and resilience. In a year where cyber threats are expected to grow in sophistication and cost pressures could impact cyber security budgets, CTEM's cost-effective and targeted methodology will become indispensable for businesses wanting to pro-actively defend themselves from threats.

For more information on CTEM and the managed service provided by Integrity360 visit our website at https://www.integrity360.com/ctem-as-a-service

Integrity360
your security in mind

Related services

As a leading provider of end-to-end cyber security services, Integrity360 helps our clients solve complex challenges and drive business growth securely. Our industry-leading expertise and experience enable us to understand our clients' unique challenges and proactively protect them against the constantly evolving threat landscape.

Cyber Security Solutions

We provide you with the tools, practices, and strategies to ensure the confidentiality, integrity, and availability of your digital assets.

Technology Services

We help you identify, implement and operate the security platforms that can help your business fend off unique threats.

Cyber Risk & Assurance

We help you assess your security posture and apply structure to your cyber security strategy through policies and processes.

Cyber Security Testing

We keep your business safe against cyber threats by proactively uncovering vulnerabilities, preventing breaches and identifying weaknesses that attackers exploit.

Incident Response

As CREST Certified Cyber Security Incident Response (CSIR) Experts we quickly recognise and contain the threat, reducing your response time and minimising the business impact.

PCI Compliance

We take the pain out of PCI compliance, by identifying relevant controls, highlighting systems to protect, and addressing security and compliance gaps.

Managed Security Services

We give you the 24x7x365 cyber security expertise you need without the cost and complexity of having to provision and manage it in-house.

Integrity360

It's not enough to be secure. You need to stay secure.

Contact our advisor team today to learn how you can best protect your network, infrastructure and data.

integrity360.com

info@integrity360.com

Dublin, Ireland
+353 01 293 4027

London, UK
+44 20 3397 3414

Sofia, Bulgaria
+359 2 491 0110

Stockholm, Sweden
+46 8 514 832 00

Madrid, Spain
+34 910 767 092

Ludwigsburg, Germany
+49 7141 48799 80

Zurich, Switzerland
+41 44 421 3336