

2026 Cyber Resilience Benchmark Report



Contents

1	Introduction	Page 3
2	About the Cyber Resilience Benchmark Report	Page 4
3	Breakdown of survey participants	Page 5
4	Analysis and discussion of survey findings	Pages 6-32
4.1	<i>Governance and Strategy</i>	Pages 6-10
4.2	<i>Regulatory Compliance and Standards</i>	Pages 11-12
4.3	<i>Risk Management</i>	Pages 13-15
4.4	<i>Data Protection and Privacy</i>	Pages 16-17
4.5	<i>Incident Response and Recovery</i>	Pages 18-21
4.6	<i>Technical Controls</i>	Pages 22-27
4.7	<i>People and Culture</i>	Pages 28-30
4.8	<i>Future Outlook</i>	Pages 31-32
5	Closing thoughts and looking ahead	Page 33
	Appendix – List of acronyms and abbreviations used	Page 34

1. Introduction

The UK cyber security threat landscape has undergone a profound transformation over the past two years, marking a decisive shift in both the nature and severity of attacks facing UK organisations. Sophisticated ransomware gangs are increasingly targeting critical infrastructure and essential services, while nation-state actors from Russia, China, Iran, and North Korea demonstrate unprecedented persistence in pursuing UK economic and strategic assets. The National Cyber Security Centre reports that cyber attacks against UK organisations have increased significantly in both volume and sophistication, with financial services, healthcare, manufacturing, and professional services sectors experiencing particularly acute pressure.

Compounding these threats, the regulatory environment is experiencing its most significant overhaul in a decade. European initiatives such as the Digital Operational Resilience Act and the NIS2 Directive, expand regulatory scope to encompass thousands of organisations having European operations, introducing stringent security requirements, mandatory 24-hour incident reporting, and substantial financial penalties for non-compliance. Simultaneously, the UK government's Cyber Security and Resilience Bill signals further legislative action, whilst sector-specific regulators including the FCA, Ofcom, and ICO intensify their cyber security oversight and enforcement activities.

The convergence of escalating threats and sweeping regulatory change creates an inflection point for UK organisations. Technology leaders face the dual challenge of strengthening defences against increasingly capable adversaries whilst simultaneously ensuring compliance with complex, evolving regulatory frameworks. Understanding where UK CIOs, CTOs, CISOs and other Information Security leaders stand in their cyber resilience maturity has never been more vital. This survey captures the current state of preparedness across organisations in the UK, providing directional benchmarking data to inform strategic decisions and investment priorities during this critical period of transformation.

2. About the Cyber Resilience Benchmark report

Xcina Consulting surveyed 33 organisations in the first semester of 2026. The survey was addressed to CIOs, CTOs, CISOs and other senior managers having responsibilities relating to information security in their organisations.

While not statistically representative of the UK market, the objective of the survey was to assess the current state and provide directional insights on cyber resilience practices in UK organisations. It provided participants with the opportunity to benchmark their own practices against those of other survey participants.

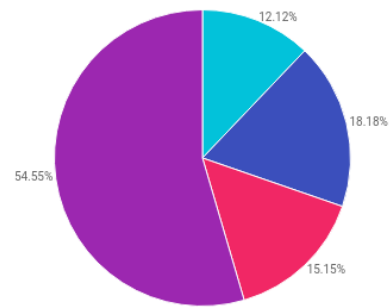
The survey benchmark report aligns with the structure of the survey questionnaire. It consolidates the participants' responses on an anonymised basis across the 31 domains and questions covered by the survey. The report aims to provide context around each of the topics and to highlight and comment on the emerging and better practices, as well as any areas for improvement identified through the participants' responses. Organisations should tailor their security strategy based on risk, size and regulatory landscape.

This report is provided on a complimentary basis and does not constitute formal advice or assurance. Unless we provide express prior written consent, no part of this report should be reproduced. Xcina Consulting does not accept any liability if this report is used for any purpose other than that for which it is intended.

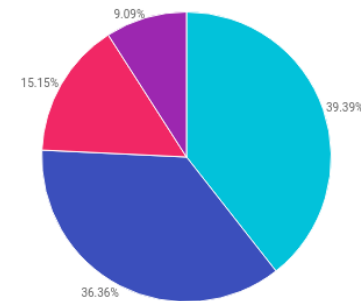
3. Breakdown of Survey Participants

Respondents held senior technology or security roles including CTO, CIO, CISO or their equivalent in some of the organisations that did not necessarily use these specific formal job titles.

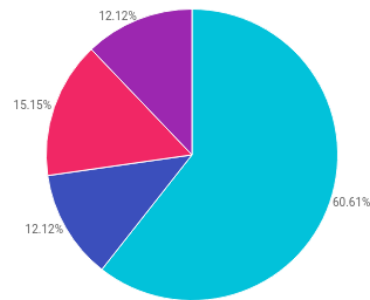
70-75% of the participants had revenues under £100 million and less than 1,000 staff. Financial services, technology and telecommunications represented 79% of the organisations surveyed.



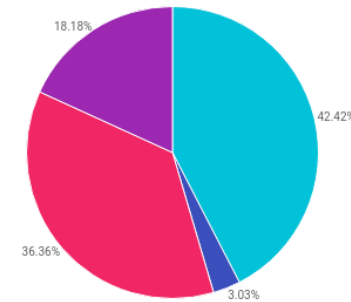
● A. Chief Information Officer (CIO) ● B. Chief Technology Officer (CTO)
● C. Chief Information Security Officer (CISO) ● D. Other senior technology or security role



● A. Under £10 million ● B. £10 million - £100 million
● C. £100 million - £1 billion ● D. Over £1 billion



● A. 1 - 250 ● B. 251 - 1,000
● C. 1,001 - 5,000 ● D. Over 5,000



● A. Financial services, insurance, or professional services ● B. Healthcare, pharmaceuticals, or life sciences
● C. Technology, telecommunications, or media ● D. Manufacturing, retail, energy, or other sectors

4. Analysis and Discussion of Survey Findings

Q5. Does your organisation have a formal cyber resilience strategy aligned with business objectives?

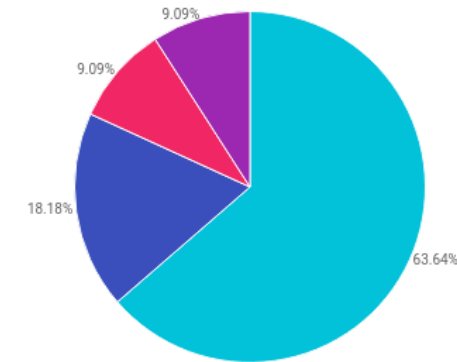
Why it's important

A documented cyber resilience strategy ensures cybersecurity is aligned with business objectives, adequately resourced, and consistently executed. Without formal strategy, organisations react to threats rather than proactively managing risk, leading to security gaps and inefficient spending.

64% of participants have a documented cyber resilience strategy which is regularly reviewed. 27% have a strategy which is in development or needs updating. 9% of the organisations do not have a formal strategy.

Good Practices commonly seen across industry:

- Developing a 3-year cyber resilience strategy reviewed annually
- Aligning strategy with business objectives and risk appetite
- Including specific, measurable objectives with clear ownership
- Addressing people, process, and technology dimensions
- Incorporating supply chain and third-party risk
- Defining success metrics and KPIs
- Ensuring executive sponsorship and board approval
- Regular communication of the strategy to all stakeholders



- A. Yes, fully documented and regularly reviewed
- B. Yes, but it needs updating
- C. Currently in development
- D. No formal strategy exists

Emerging Trends according to industry sources include:

- A shift from "cybersecurity" to "cyber resilience", emphasising service and business continuity
- The integration of cyber risk into enterprise risk management (ERM) frameworks
- An increase in board-level accountability for cyber risk following high-profile breaches
- Strategy documents focusing to a greater extent on supply chain resilience and third-party risk
- Adoption of frameworks like the NIST Cybersecurity Framework for strategic planning

4. Analysis and Discussion of Survey Findings

Q6. How frequently does your board or executive review cyber resilience matters?

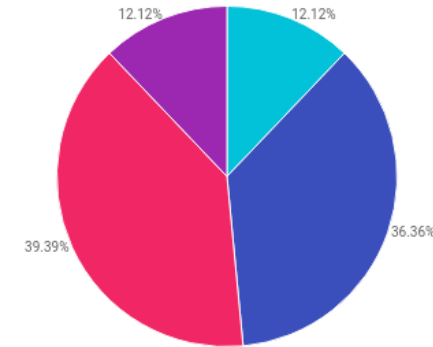
Why it's important

Board and executive oversight ensure adequate resources, accountability, and strategic alignment. Regular board and executive engagement indicates that cybersecurity is treated as a business risk, not just an IT issue. The frequency of board and executive review correlates with organisational maturity and preparedness.

48% of the participants conduct board or executive reviews at least quarterly.

Good Practices commonly seen across industry include:

- Board reporting on cyber resilience at least quarterly as a minimum
- Monthly reporting for high-risk sectors (e.g. financial services, critical infrastructure)
- Executive summary format which minimises technical jargon
- Reporting includes threat landscape, incidents, control effectiveness, and strategic initiatives
- Presenting cyber risk in business impact terms (financial, reputational, operational)
- Board papers including trending over time, not just point-in-time snapshots
- Board members receiving regular cyber awareness briefings
- Annual deep-dive sessions on emerging threats and technologies



- A. Monthly or more frequently
- B. Quarterly
- C. Bi-annually or annually
- D. Only when incidents occur or ad-hoc

Emerging Trends according to industry sources include:

- UK boards increasingly establishing dedicated cyber/technology committees
- Financial services and other regulators expecting quarterly cyber risk reporting
- Non-executive directors with cyber expertise being appointed to boards
- Cyber risk dashboards becoming standard board reporting tools
- Integration of cyber metrics into enterprise risk reporting

4. Analysis and Discussion of Survey Findings

Q7. What percentage of your IT budget is allocated to cyber security and resilience?

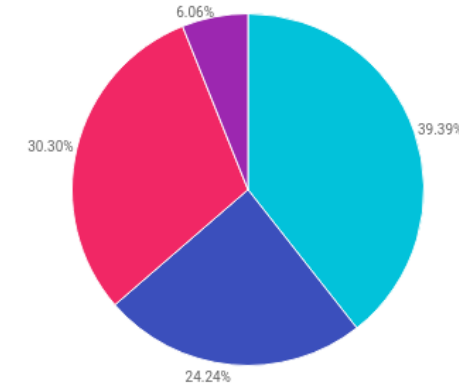
Why it's important

Budget allocation reflects organisational commitment to cybersecurity. Industry benchmarks help assess whether investment is adequate relative to risk. Underfunding can lead to security gaps, whereas an appropriate level of investment enables proactive risk management.

64% of survey participants allocate at least 10% of their IT budget to cybersecurity, in line with good practice.

Good Practices commonly seen across industry include:

- Allocating 10-15% of IT budget as a baseline, adjusting for sector and risk profile
- Financial services and critical infrastructure typically allocating 12-18%
- Balancing spending across prevention, detection, and response capabilities
- Prioritising spending based on risk assessment outcomes
- Including a budget provision for incident response and recovery
- Budgeting for continuous improvement, not just maintaining current state
- Tracking security spending ROI through risk reduction metrics
- Reserving a contingency budget (5-10%) for emerging threats



● A. More than 15%

● C. 5-10%

● B. 10-15%

● D. Less than 5%

Emerging Trends according to industry sources include:

- UK organisations averaging 10-15% of IT budget for cybersecurity in 2024-2025
- Shift from capital expenditure (tools) to operational expenditure (services, skills)
- Increased spending on cloud security as cloud adoption accelerates
- Growing investment in security automation and orchestration
- Rising costs of cyber insurance contributing to driving increased security investment

4. Analysis and Discussion of Survey Findings

Q8. Does your organisation have cyber insurance coverage?

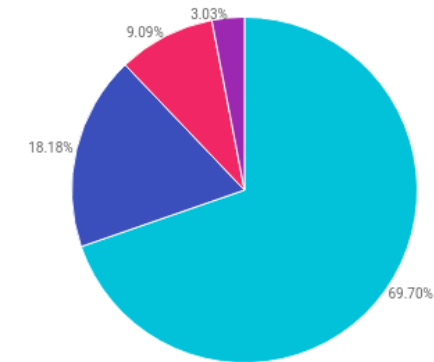
Why it's important

Cyber insurance provides financial protection against incidents and increasingly serves as an external validation of security controls. Insurers now require specific security measures before providing coverage, effectively raising the security baseline. Insurance also provides access to incident response resources.

70% of participants have comprehensive insurance cover, which is evaluated on a regular basis. 18% have basic insurance only. The remaining 12% don't have cyber insurance in place yet.

Good Practices commonly seen across industry include:

- Obtaining cyber insurance appropriate to the organisation's risk exposure
- Reviewing cyber insurance policy annually to ensure coverage matches current risk landscape
- Understanding exclusions, sub-limits, and coverage triggers
- Ensuring the policy includes incident response services, legal support, and PR crisis management
- Meeting all insurer security requirements to avoid coverage disputes
- Maintaining evidence of security controls for underwriting and claims
- Considering first-party (own losses) and third-party (liability) coverage
- Testing incident response procedures, including insurance notification processes



- A. Yes, comprehensive coverage regularly reviewed
- B. Yes, basic coverage
- C. Currently evaluating or procuring
- D. No cyber insurance

Emerging Trends according to industry sources include:

- Premium increases in the range of 30-50% year-on-year due to rising claims
- Insurers imposing stricter security requirements (e.g. MFA, EDR, offline backups)
- Coverage exclusions expanding, particularly for ransomware and nation-state attacks
- "Silent" (or non-affirmative) cyber clauses being added to traditional policies
- Incident response retainers being bundled with insurance policies
- Some insurers requiring continuous security posture monitoring

4. Analysis and Discussion of Survey Findings

Q9. How is the cyber security function structured in your organisation?

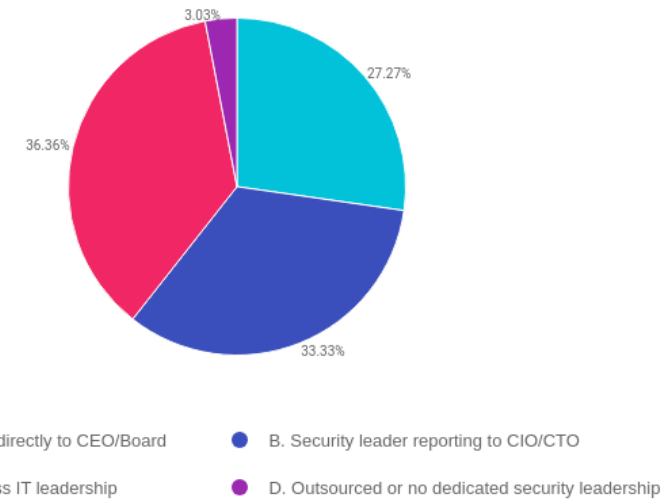
Why it's important

The cybersecurity reporting structure influences the independence, authority, and effectiveness of the security function. Direct reporting to CEO/Board provides greater authority and visibility, while reporting through IT may create conflicts of interest when security requirements conflict with operational objectives.

27% of participants have a dedicated CISO reporting to the CEO or Board, whereas 33% have the role covered by a security leader reporting to the CIO or CTO.

Good Practices commonly seen across industry include:

- CISO reporting directly to CEO or Board for organisations over £100M revenue
- CISO with dotted-line reporting to board risk/audit committee
- Security function being independent from IT operations to avoid conflicts
- Clear delineation between security policy (CISO) and implementation (IT)
- Adequate security team resourcing based on organisational size and complexity
- Security being represented in all major business initiatives and projects
- Regular CISO participation in executive leadership meetings
- A federated security model with security champions in business units



Emerging Trends according to industry sources include:

- CISO increasingly reporting directly to CEO or Board rather than to the CIO/CTO
- Separation of security and IT operations becoming standard in larger organisations
- Growth in virtual CISO (vCISO) services for mid-sized organisations
- Security operations centres (SOCs) being established or outsourced
- Integration of physical and cyber security functions under the Chief Security Officer

4. Analysis and Discussion of Survey Findings

Section 4.2 – Regulatory Compliance and Standards

Q10. Which cyber security frameworks does your organisation currently comply with?

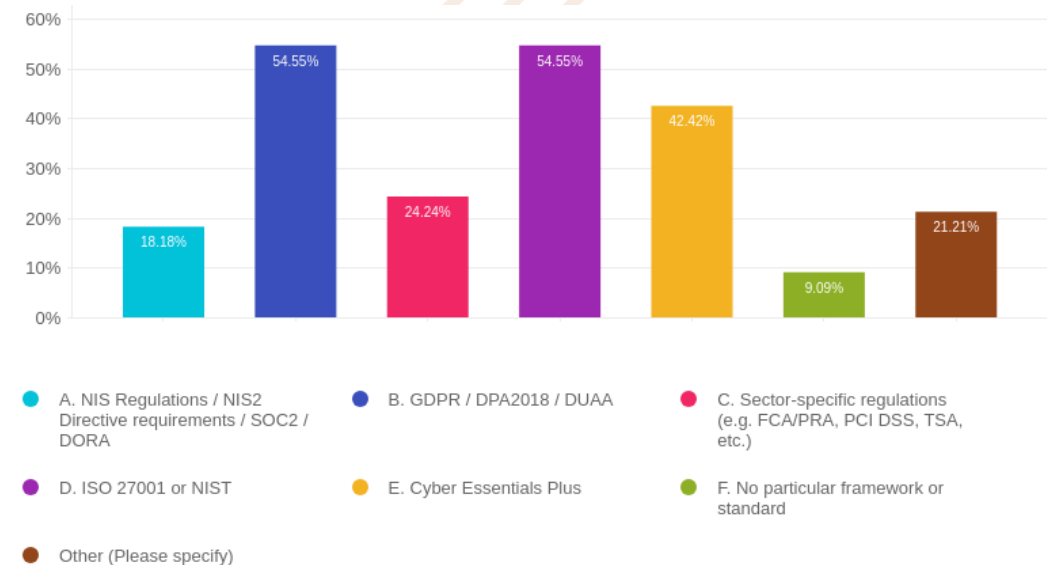
Why it's important

Understanding regulatory obligations is fundamental to compliance risk management. Different sectors face varying requirements, and failure to comply may result in significant fines, reputational damage, and loss of operating license. Frameworks drive baseline security practices.

55% of participants have adopted ISO 27001 or NIST. Equally, 55% report adherence to GDPR, which appears relatively low as every organisation must legally comply. 42% adhere to Cyber Essentials Plus. Other notable frameworks reported by participants include SOC 2, CREST, and Cyber Essentials Basic.

Good Practices commonly seen across industry include:

- Maintaining a comprehensive regulatory requirements register
- Mapping controls to multiple regulatory frameworks simultaneously
- Assigning compliance ownership to specific individuals
- Conducting annual gap assessments against regulatory requirements
- Maintaining audit trail evidence of compliance activities
- Monitoring regulatory developments and assessing their impact
- Engaging external advisors for complex regulatory interpretation
- Participating in regulatory industry forums and working groups



Emerging Trends according to industry sources include:

- Increasing requirement for SOC 2 reports to streamline supplier security assurance
- NIS2 Directive and UK Cyber Security and Resilience Bill implementation significantly expanding the scope of compliance
- The UK's own cyber regulations evolving post-Brexit, with potential EU divergence
- Sector-specific regulations intensifying (e.g. financial services and telecoms)
- Increased regulatory focus on supply chain security
- More proactive cyber assessments by regulators, not just reactive investigations
- Significant increase in financial penalties for breaches

4. Analysis and Discussion of Survey Findings

Q11. How prepared is your organisation for the upcoming Cyber Security and Resilience Bill or NIS2 Directive requirements (whichever is applicable)?

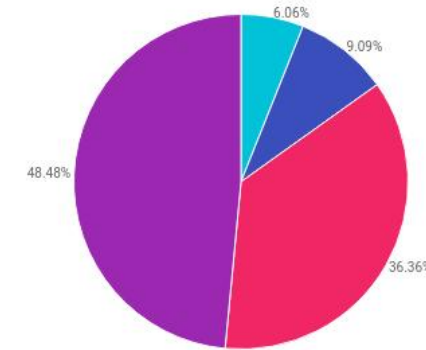
Why it's important

NIS2 significantly expands regulatory scope compared to its predecessor NIS1, covering more sectors and smaller organisations. It introduces stricter security requirements, incident reporting obligations, and enforcement measures which may include personal liability. Non-compliance may result in substantial fines and operational disruption. The Cyber Security and Resilience Bill (CSR) which applies to UK organisations aligns closely to the NIS2 scope and requirements.

15% of respondents have completed or are currently completing their implementation, and another 36% are in the initial assessment phase.

Good Practices commonly seen across industry include:

- Conducting NIS2/CSR applicability assessment without undue delay
- Performing a gap analysis against new requirements
- Implementing 24-hour incident detection and reporting capabilities
- Establishing incident classification process aligned with NIS2/CSR definitions
- Enhancing the third-party/supply chain risk management programme
- Implementing the required governance structures (CISO, board oversight)
- Documenting all security measures and controls
- Establishing relationships with relevant authorities
- Conducting regular compliance reviews and readiness assessments



- A. Fully prepared with implementation complete or underway
- B. Gap analysis completed, implementation planning in progress
- C. Initial assessment phase
- D. Not yet started or not applicable

Emerging Trends according to industry sources include:

- EU transposition deadline driving urgent preparation efforts
- Scope expansion capturing thousands of UK organisations previously unregulated
- 24-hour incident reporting requirements leading to operational challenges
- Supply chain security requirements driving vendor management improvements
- Personal liability for directors driving increased board engagement
- Overlaps with other sectoral frameworks creating regulatory complexity

4. Analysis and Discussion of Survey Findings

Q12. How often does your organisation conduct formal cyber risk assessments?

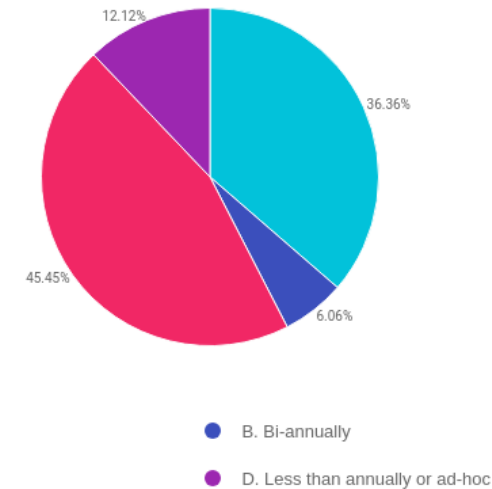
Why it's important

Regular cyber risk assessments ensure that security controls address the current threats and business context. As the threat landscape evolves rapidly, annual assessments may leave organisations vulnerable to emerging risks. The frequency of risk assessments should align with the pace of organisational and threat landscape changes.

36% of respondents conduct cyber risk assessments continuously or at least quarterly and another 6% assess cyber risk bi-annually.

Good Practices commonly seen across industry include:

- Conducting formal comprehensive risk assessments at least annually
- Quarterly reviews for high-risk sectors or rapidly changing environments
- Continuous automated risk monitoring for technical vulnerabilities
- Triggering risk re-assessment for significant changes (M&A, new systems, major threats)
- Using recognized methodologies (e.g. ISO 27005, NIST, FAIR)
- Documenting risk acceptance decisions by appropriate authority
- Maintaining risk register with clear ownership and treatment plans
- Presenting risk in business impact terms, not just technical vulnerabilities
- Tracking risk trends over time to measure programme effectiveness



Emerging Trends according to industry sources include:

- Shift from annual to continuous/quarterly risk assessments
- Integration of threat intelligence into risk assessment processes
- Automated risk assessment tools using asset discovery and vulnerability data
- Risk quantification methodologies (e.g. FAIR framework) gaining adoption
- Board-level risk appetite statements becoming more sophisticated
- Integration of cyber risk into enterprise risk management (ERM)

4. Analysis and Discussion of Survey Findings

Q13. How does your organisation identify and prioritise cyber threats?

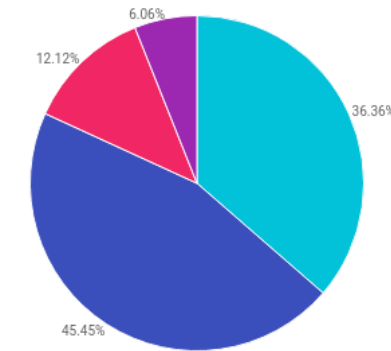
Why it's important

Understanding relevant threats enables focused defence investment. Generic threat models waste resources on irrelevant risks while missing critical exposures. Threat intelligence informs risk-based security strategies and enables proactive defence.

36% of respondents use external threat intelligence feeds with automated risk scoring. 45% conduct their own regular threat assessments internally.

Good Practices commonly seen across industry include:

- Subscribing to relevant threat intelligence feeds (commercial and government)
- Participating in information sharing communities (e.g. NCSC CISP, sector groups)
- Maintaining threat model specific to organisation's sector and profile
- Mapping threats to assets and assessing realistic impact scenarios
- Prioritising based on likelihood and business impact, not just technical severity
- Regular threat briefings to leadership team
- Conducting threat-informed penetration testing
- Document threat actor Tactics, Techniques and Procedures (TTPs) relevant to the organisation
- Updating threat model quarterly or when significant threats emerge



- A. Threat intelligence feeds with automated risk scoring
- B. Regular threat assessments by internal security team
- C. Annual reviews with external consultants
- D. Reactive approach based on incidents

Emerging Trends according to industry sources include:

- Threat intelligence platforms integrating multiple feeds for contextualization
- AI/Machine Learning enhancing threat detection and priority scoring
- Sector-specific threat intelligence sharing increasing (NCSC CISP, sector ISACs – Information Sharing and Analysis Centers)
- Focus on nation-state threats particularly from Russia, China, Iran, North Korea
- Ransomware-as-a-service lowering barriers to entry for criminals
- Supply chain attacks becoming more sophisticated and common

4. Analysis and Discussion of Survey Findings

Q14. How mature is your organisation's third-party/supply chain risk management?

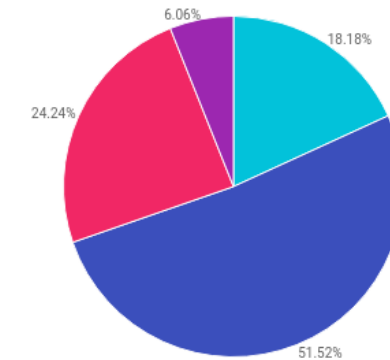
Why it's important

Third-party breaches are becoming the leading attack vector. Organisations remain accountable for vendors' security failures affecting their and their customers' data. Supply chain attacks can be devastating as demonstrated by multiple recent high-profile incidents. Regulatory requirements such as NIS2, DORA and CSR have mandatory supply chain risk management requirements.

Only 18% of the participants have a comprehensive third-party management programme with risk-based continuous monitoring. 6% do not have a formal process and 24% only focus on basic contractual requirements.

Good Practices commonly seen across industry include:

- Conducting risk-based vendor assessments before onboarding
- Tiering vendors by risk and applying appropriate due diligence
- Including specific security requirements and right-to-audit in contracts
- Requiring critical vendors to maintain appropriate certifications
- Using software composition analysis and requiring SBOMs
- Conducting annual vendor security reviews and audits
- Maintaining vendor inventory with risk classifications
- Monitoring critical vendor security posture continuously where possible
- Vendor incident response procedures and notification obligations
- Testing vendor disaster recovery and business continuity capabilities
- Maintaining vendor offboarding procedures ensuring data return/destruction



- A. Comprehensive programme with continuous monitoring
- B. Standard due diligence for critical suppliers
- C. Basic contractual requirements only
- D. Limited or no formal process

Emerging Trends according to industry sources include:

- Supply chain attacks increasing significantly year-on-year
- Regulations requiring continuous supplier monitoring, not just onboarding due diligence
- 4th and 5th party risk gaining increasing attention
- Automated vendor risk assessment platforms maturing
- Cyber rating services being used for continuous monitoring

4. Analysis and Discussion of Survey Findings

Section 4.4 – Data Protection and Privacy

Q15. How does your organisation ensure compliance with UK GDPR, Data Protection Act 2018 and Data (Use and Access) Act 2025?

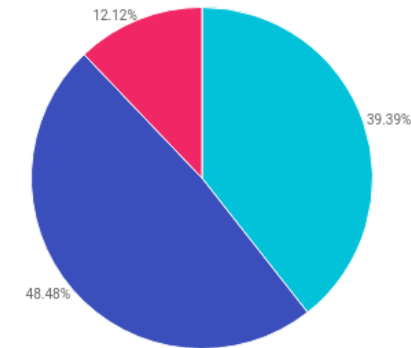
Why it's important

GDPR and UK data protection laws have been around for some time and require comprehensive data governance. Proper management prevents costly breaches (up to 4% global turnover fines), legal liability, and reputational damage. Data protection is increasingly integrated with cybersecurity as breaches are a primary cause of data protection violations.

39% of respondents reported having a comprehensive privacy programme with a dedicated DPO and regular audits. A further 48% have established data compliance processes with periodic reviews.

Good Practices commonly seen across industry include:

- Considering appointing a qualified Data Protection Officer (DPO) or equivalent
- Maintaining an accurate record of processing activities (ROPA)
- Conducting DPIAs for high-risk processing
- Using automation to support data subject rights request (DSAR) handling
- Establishing 72-hour breach notification capabilities
- Deploying data discovery and classification tools
- Regular privacy awareness training for all staff
- Documenting legitimate interest assessments and consent mechanisms
- Conducting annual compliance health checks and gap assessments
- Establishing an internal network of privacy champions.



- A. Comprehensive privacy programme with dedicated DPO and regular audits
- B. Established compliance processes with periodic reviews
- C. Basic compliance measures in place
- D. Minimal compliance efforts or unsure

Emerging Trends according to industry sources include:

- Assessing AI use and training for compliance with data protection requirements
- ICO enforcement activity increasing with larger fines being issued
- Data protection impact assessments (DPIAs) being required for an increasing number of processing activities
- Increased complexity of international data transfers post-Brexit
- Increasing adoption of ISO 27701 as a best practice template
- Growing adoption of privacy-enhancing technologies (PETs)
- Integration of privacy-by-design into development processes
- Automated GDPR compliance tools and platforms emerging.

4. Analysis and Discussion of Survey Findings

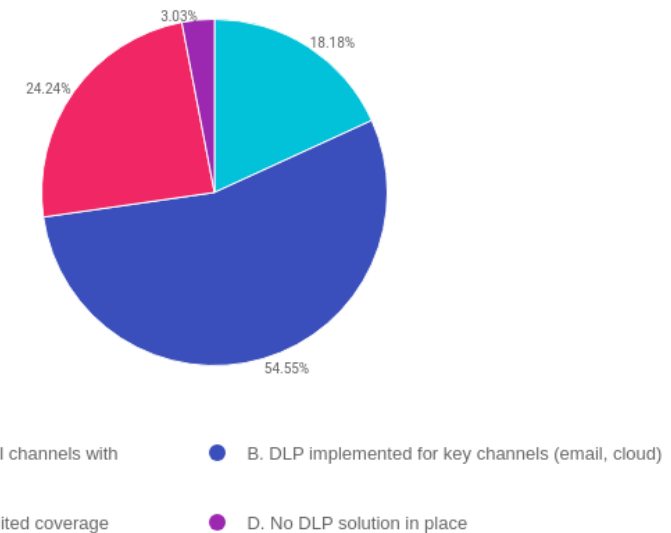
Q16. How mature is your data loss prevention (DLP) programme?

Why it's important

Data Loss Prevention protects organisational data from unauthorised access, exfiltration, or accidental disclosure. Data loss can lead to lasting reputational damage, competitive disadvantage through IP theft, regulatory sanctions and financial losses. DLP is particularly critical in hybrid work environments where data flows across multiple devices, networks, and cloud services. Insider threats—both malicious and accidental—account for a substantial portion of breaches, making DLP visibility and controls essential for prevention. 18% of respondents have a comprehensive DLP programme, with active monitoring and a further 55% have it implemented for key channels such as email and cloud.

Good Practices commonly seen across industry include:

- Deploying automated data discovery and classification across all repositories
- Implementing layered DLP controls (network, endpoint, cloud, email, web)
- Starting monitoring mode before enforcing blocks
- Creating context-aware, risk-based policies balancing security with usability
- Integrating DLP with SIEM and identity management
- Monitoring insider threats using User Entity and Behaviour Analytics (UEBA)
- Tuning policies quarterly reducing false positives
- Mapping to regulatory requirements, maintaining 24-month audit logs
- Extension to emerging technologies (e.g. AI tools, collaboration platforms)
- Conducting regular awareness training.



Emerging Trends according to industry sources include:

- Cloud-native DLP integrating with SaaS and multi-cloud environments
- Using AI/ML to improve detection speed
- Risk of shadow AI usage leaking corporate data
- Automated data discovery replacing manual classification
- Integration with Zero Trust architectures
- UEBA detecting insider threats through behavioural analytics
- Unified platforms consolidating DLP with Cloud Access Security Broker (CASB) and encryption.

4. Analysis and Discussion of Survey Findings

Q17. Does your organisation have a documented and tested major incident response plan?

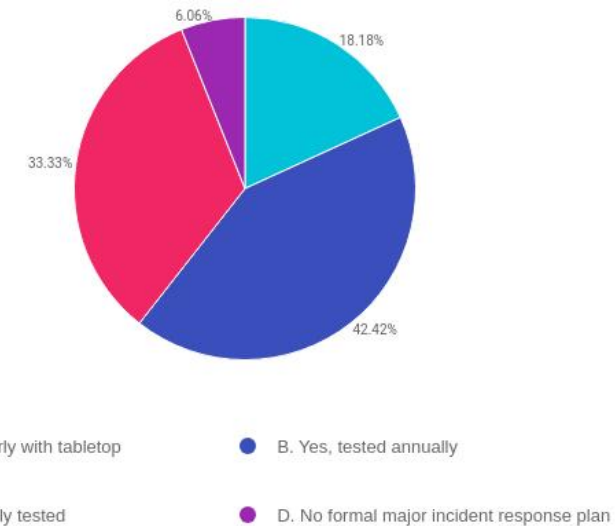
Why it's important

Incident response plans untested in realistic scenarios often fail during real incidents. Testing identifies gaps, validates procedures, trains responders, and builds muscle memory. Regulatory requirements increasingly mandate regular testing. Poor incident response magnifies the impact of a breach.

18% of participants test plans at least quarterly, including tabletop exercises. 42% test them annually. 39% of respondents do not test plans or do not have a formal major incident response plan. Incident response testing for SMEs often focuses on tabletop rather than live-play.

Good Practices commonly seen across industry include:

- Continual improvement, leading to improved efficiency and risk reduction
- Testing incident response plans at least quarterly for high-risk environments
- Annual full-scale exercises simulating major incidents
- Including technical, communications, legal, and executive teams in exercises
- Testing specific scenarios (e.g. ransomware, data breach, DDoS, insider threat)
- Documenting lessons learned and update plans accordingly
- Testing 24-hour incident reporting capabilities (regulatory requirement)
- Conducting surprise exercises to test actual readiness, not just prepared responses
- Engaging external Incident Response firms to validate capabilities
- Test communication plans including customer, regulator, and media notification



Emerging Trends according to industry sources include:

- Shift from annual to quarterly tabletop exercises
- Purple team exercises combining red and blue teams
- Cyber crisis simulations including board and executive participation
- Automated incident response (SOAR platforms – Security Orchestration, Automation and Response) reducing response times
- Integration of incident response with business continuity planning
- Third-party Incident Response retainers becoming standard

Q18. How frequently does your organisation conduct business continuity or disaster recovery testing?

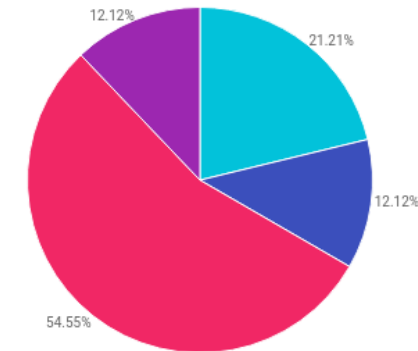
Why it's important

Business continuity and disaster recovery capabilities degrade over time due to changes in systems, personnel, and processes. Regular testing validates that recovery procedures work and meet defined RTOs/RPOs. Untested plans frequently fail when needed most. Testing also helps identify dependencies and single points of failure.

21% of respondents conduct BC or DR testing at least quarterly and a further 12% do so bi-annually. 55% conduct testing on an annual basis.

Good Practices commonly seen across industry include:

- Continual improvement, leading to improved efficiency and risk reduction
- Testing BC and DR at least annually (quarterly preferred)
- Testing different scenarios (site loss, ransomware, cloud provider outage, multiple simultaneous failures)
- Including full end-to-end testing, not just infrastructure restoration
- Involving business users in the validation of recovered systems
- Testing the recovery of the most critical systems more frequently
- Documenting detailed test results, actual recovery times and lessons learned
- Including data integrity validation in testing
- Updating BC/DR plans based on test findings before next tests.



- A. Quarterly or more frequently
- B. Bi-annually
- C. Annually
- D. Less than annually or never

Emerging Trends according to industry sources include:

- Shift from annual to quarterly BC/DR testing
- Automated DR testing capabilities in cloud platforms
- Chaos engineering approaches (deliberately breaking production systems)
- Integration of DR testing into CI/CD (continuous integration/continuous delivery) pipelines
- Business continuity and disaster recovery testing combined in single exercises
- Increasing use of cloud for DR reducing costs and improving capabilities

4. Analysis and Discussion of Survey Findings

Q19. In the past 12 months, has your organisation experienced a significant cyber incident?

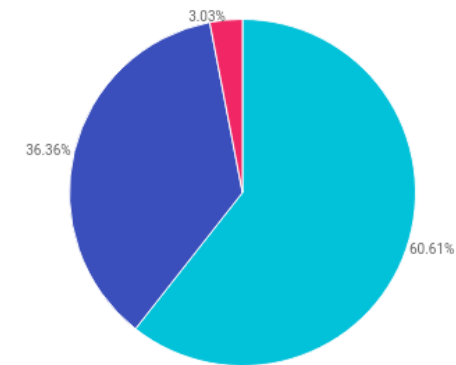
Why it's important

Incident history indicates current security posture effectiveness and attack targeting. Multiple incidents suggest systematic weaknesses. Understanding incident patterns helps prioritise improvements. Organisations learning from incidents improve resilience; those with repeating incidents are more likely to have cultural or resource issues.

97% of participants reported no incidents or minor incidents only in the past 12 months.

Good Practices commonly seen across industry include:

- Maintaining a comprehensive incident log with detailed root cause analysis
- Classifying incidents by type, severity, and business impact
- Tracking incidents against industry benchmarks
- Conducting thorough post-incident reviews identifying root causes
- Implementing corrective actions preventing recurrence
- Sharing appropriate incident details with sector peers on an anonymised basis
- Reporting qualifying incidents to regulators as required
- Using incident data to improve security controls and monitoring
- Briefing the board and executive on significant incidents and lessons learned
- Tracking mean time to detect and respond trends over time



- A. No incidents
- B. Minor incidents only
- C. Yes, one significant incident
- D. Yes, multiple incidents

Emerging Trends according to industry sources include:

- Ransomware incidents becoming more targeted and impactful
- Business email compromise and phishing remaining the top attack vectors
- Supply chain compromises affecting multiple organisations simultaneously
- Increasing nation-state attacks against targets including UK critical infrastructure
- Insider threats (intentional and accidental) increasing with remote work
- Cloud misconfigurations causing data exposures

Q20. How long would it take your organisation to fully recover from a ransomware attack?

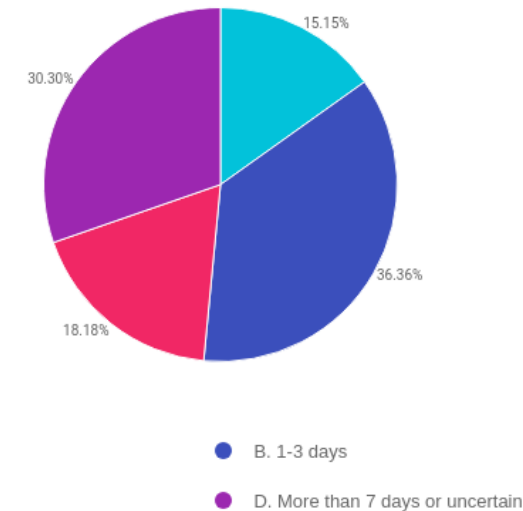
Why it's important

Ransomware is one of the most significant cyber threats to organisations. Recovery capabilities determine the business impact and ransom payment pressure. A fast recovery requires specific preparations (e.g. offline backups, tested procedures, tabletop exercises). The recovery time correlates directly with the financial and operational impact.

15% of respondents estimate it would take them less than 24 hours to fully recover from a ransomware attack, whereas 30% would take more than 7 days or are uncertain as to how long it would take them to fully recover.

Good Practices commonly seen across industry include:

- Maintaining immutable, offline, or air-gapped backups
- Testing ransomware scenarios including communication plans quarterly
- Implementing 3-2-1 backup rule (3 copies, 2 media types, 1 offsite)
- Deploying anti-ransomware capabilities (e.g. EDR, email filtering, network segmentation)
- Maintaining forensic capabilities to understand attack scope before recovery
- Establishing a clear decision framework for ransom payment consideration
- Pre-positioning an Incident Response firm retainer for expert assistance
- Implementing detection for lateral movement and backup deletion attempts
- Maintaining offline documentation of recovery procedures



Emerging Trends according to industry sources include:

- Attackers specifically targeting backups before deploying ransomware
- Dwell times increasing (weeks of access before encryption)
- Double and triple extortion (encryption + data theft + DDoS)
- Ransomware-as-a-service lowering attacker skill requirements
- Recovery times improving as organisations prepare better
- Insurance companies requiring specific anti-ransomware controls

4. Analysis and Discussion of Survey Findings

Q21. What is your organisation's approach to multi-factor authentication (MFA)?

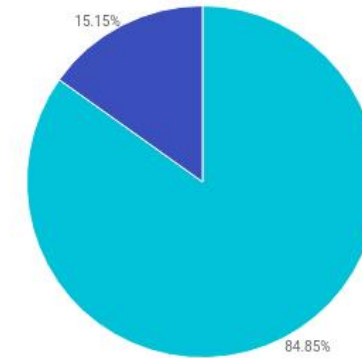
Why it's important

Microsoft reports that MFA can block 99.9% of automated attacks. Password-only authentication is obsolete given prevalent credential stuffing, phishing, and password reuse. Many compliance frameworks now mandate MFA. Lack of MFA is increasingly indefensible after a breach.

85% of respondents have mandated MFA for all users and all systems. The remaining 15% require MFA for privileged accounts and remote access.

Good Practices commonly seen across industry include:

- Deploying MFA at least for VPN, cloud applications, email, and administrative access
- Mandating MFA for all users and all systems
- Deploying phishing-resistant MFA (e.g. FIDO2, hardware keys, certificate-based)
- Avoiding SMS-based MFA, using authenticator apps as minimum. Where SMS cannot be avoided, compensating anti SIM swap measures are recommended.
- Implementing conditional access adjusting requirements based on context
- Requiring MFA for privileged access without exception
- Blocking legacy authentication protocols not supporting MFA
- Educating users on MFA fatigue attacks
- Maintaining MFA backup procedures for device loss
- Monitoring and alerting on MFA-related anomalies



- A. Mandatory for all users and all systems
- B. Mandatory for privileged accounts and remote access
- C. Optional or available but not enforced
- D. Not currently implemented

Emerging Trends according to industry sources include:

- Shift from MFA for "some systems" to "all users, all systems"
- SMS-based MFA being phased out due to SS7 vulnerabilities and SIM swapping
- Passwordless authentication emerging (e.g. passkeys, biometrics)
- Conditional access policies adjusting MFA requirements based on risk
- MFA fatigue attacks targeting push notification approvals
- Hardware security keys gaining adoption for highest-risk users

4. Analysis and Discussion of Survey Findings

Q22. How does your organisation manage software patching?

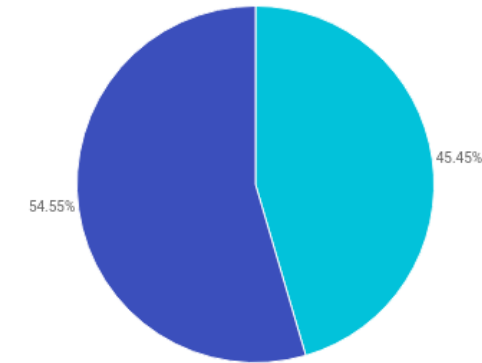
Why it's important

Unpatched vulnerabilities are leading cause of breaches. Attackers exploit vulnerabilities within hours of disclosure. Effective patch management balances security urgency against operational stability. Cyber compliance and regulatory frameworks increasingly mandate cybersecurity patching Service Level Agreements (SLAs).

45% of respondents use automated patching with defined SLAs for critical vulnerabilities. 55% have a regular patching schedule with manual prioritisation.

Good Practices commonly seen across industry include:

- Establishing risk-based patching SLAs (e.g. critical: 7-15 days, high: 30 days, medium: 90 days, factoring in risk and system criticality) and tracking patching metrics (time to patch, coverage). OT environments often have materially slower patch windows.
- Automated patch management for endpoints and standard applications
- Maintaining a comprehensive asset inventory enabling complete patch coverage
- Conduct monthly vulnerability scanning verifying patch deployment
- Prioritising patching internet-facing and crown jewel systems
- Monitor vulnerability intelligence sources
- Documenting and approving exceptions for unpatchable systems with compensating controls
- Maintaining out-of-band (OOB) emergency patching procedures



- A. Automated patching with defined SLAs for critical vulnerabilities
- B. Regular patching schedule with manual prioritisation
- C. Reactive patching when issues are identified
- D. No formal patching process

Emerging Trends according to industry sources include:

- Zero-day vulnerabilities increasing, requiring faster response
- Virtual patching via WAF/IPS while testing permanent patches
- Risk-based patching prioritising actively exploited vulnerabilities
- Supply chain vulnerabilities requiring a rapid, comprehensive response
- Patch Tuesday causing a monthly crisis for many organisations
- Automated patching for endpoints and standard applications

4. Analysis and Discussion of Survey Findings

Q23. What level of network segmentation does your organisation maintain?

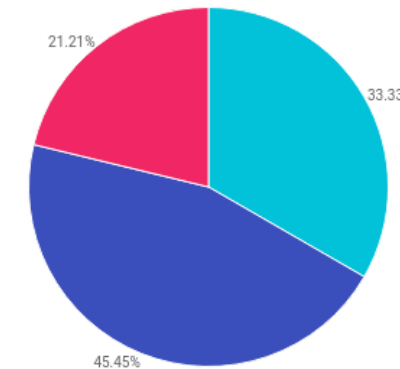
Why it's important

Segmentation divides networks into isolated zones, limiting lateral movement for attackers who breach perimeter defences. Without segmentation, a single compromised device provides access to the entire network, all data and systems. Effective segmentation contains breaches and reduces incident blast radius. Regulatory frameworks including NIS2 mandate segmentation and cyber insurers increasingly require it.

33% of respondents employ extensive microsegmentation and 45% use moderate segmentation separating critical systems. Microsegmentation maturity is still low in most mid-market organisations.

Good Practices commonly seen across industry include:

- Implementing tiered architecture separating production, development, and corporate networks, isolating high-risk environments (guest WiFi, IoT, DMZ)
- Applying microsegmentation for crown jewel assets
- Segmenting by function (HR, finance, development, third-party) and enforcing OT/IT separation.
- Deploying internal firewalls with default-deny policies, SIEM-monitored inter-segment traffic, and jump servers for sensitive access.
- Extending segmentation to cloud workloads via security groups and ACLs.
- Regularly testing segmentation through penetration testing
- Verifying segmentation doesn't create continuity single points of failure.



- A. Extensive micro-segmentation with zero-trust principles
- B. Moderate segmentation separating critical systems
- C. Basic segmentation (e.g., guest vs. corporate networks)
- D. Minimal or no network segmentation

Emerging Trends according to industry sources include:

- Replacing traditional VLANs with software-defined microsegmentation
- Zero Trust application-level access, and identity-based rules
- Cloud-native security groups, service mesh, and container/Kubernetes policies enforcing workload isolation
- East-West traffic inspection and OT/IT separation maintaining operational security
- Dynamic segmentation adjusting based on real-time threat intelligence and risk scores.

4. Analysis and Discussion of Survey Findings

Q24. How frequently does your organisation conduct penetration testing of critical systems and infrastructure?

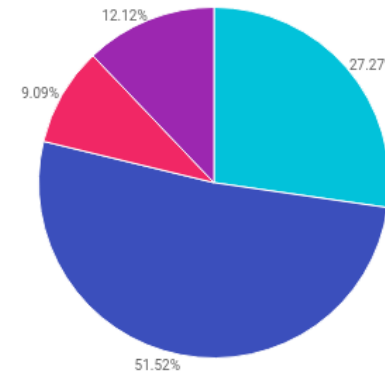
Why it's important

Penetration testing validates that the security controls actually prevent real-world attacks. It identifies vulnerabilities that scanners have missed and tests detective/response capabilities. External testing provides independent validation. Many compliance frameworks require regular penetration testing, depending on sector, regulatory exposure and criticality.

27% of participants conduct pentesting at least on a quarterly basis, covering all critical assets. 52% carry out pentesting annually, with a comprehensive scope.

Good Practices commonly seen across industry include:

- Conducting external penetration testing at least annually
- Testing internal network at least annually
- Testing web applications before major releases and annually as a minimum
- Engaging reputable penetration testing firms (CREST, CHECK, ISO 9001/27001)
- Defining clear rules of engagement and scope
- Testing social engineering and phishing resilience
- Conducting application security testing throughout the development lifecycle
- Prioritising remediation of critical/high findings within 30 days or an acceptable remediation timeframe
- Re-testing after remediation, verifying fixes
- Briefing board/executives on penetration testing results



- A. Quarterly or more frequently, covering all critical assets
- B. Annually with comprehensive scope
- C. Annually with limited scope or ad-hoc when significant changes occur
- D. Rarely or not conducted

Emerging Trends according to industry sources include:

- Shift from annual to continuous/quarterly testing
- Bug bounty programmes complementing traditional penetration testing
- Red team/purple team exercises to test detection and response
- Cloud-focused penetration testing addressing cloud-specific risks
- Adversary simulation based on real threat actor Tactics, Techniques, and Procedures
- Automated penetration testing tools enabling more frequent assessment

Q25. How frequently does your organisation conduct vulnerability scanning of its assets?

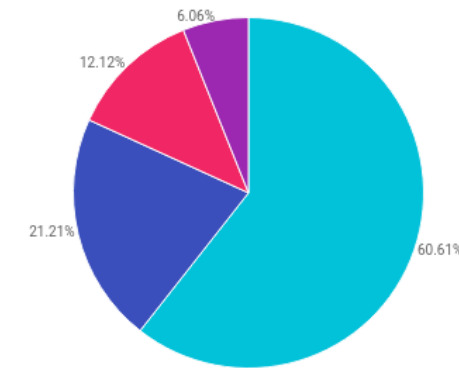
Why it's important

Regular vulnerability scanning identifies security weaknesses before attackers exploit them, providing visibility into your attack surface. It enables risk-based prioritisation of remediation efforts, demonstrates compliance due diligence, and reduces exposure windows to emerging threats that cybercriminals actively target.

61% of survey respondents employ continuous scanning or agent-based monitoring. 21% scan for vulnerabilities at least on a quarterly basis.

Good Practices commonly seen across industry include:

- Scanning internet-facing assets weekly and internal systems monthly using automated tools
- Using authenticated scans to identify deeper vulnerabilities beyond surface-level issues
- Deploying multiple scanning tools/vendors to increase coverage
- Prioritising remediation by risk score, exploitability, and asset criticality, not just vulnerability count
- Integrating scanning into change management process (e.g. after updates)
- Maintaining current asset inventory to ensure comprehensive coverage
- Covering all environments: cloud infrastructure, containers, APIs, and traditional systems



- A. Continuous scanning or agent-based monitoring
- B. Quarterly or more frequently
- C. Annually or following a significant change
- D. Rarely or not conducted

Emerging Trends according to industry sources include:

- Shift to continuous, real-time scanning rather than periodic schedules
- Integration with threat intelligence to prioritise actively exploited vulnerabilities
- Adoption of risk-based vulnerability management considering business context, not just technical severity
- Increased use of cloud-native tools integrated with DevOps pipelines
- Growing focus on OT and IoT device vulnerability management
- Regulatory and cyber insurance pressure driving more frequent scanning requirements, particularly from regulations such as NIS2

4. Analysis and Discussion of Survey Findings

Q26. How does your organisation monitor and detect security threats?

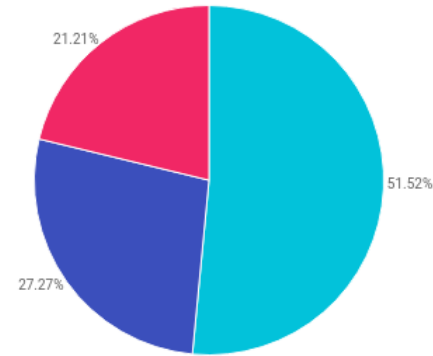
Why it's important

The speed of detection determines the impact of a breach. Speedy detection enables faster response and damage containment. Many breaches remain undetected for months, allowing extensive damage to occur. Effective monitoring requires appropriate tools, skilled analysts, and well-defined processes.

52% of participants run a 24/7 Security Operations Centre with a SIEM and advanced threat detection capabilities. A further 27% use security tools and regular monitoring only during business hours.

Good Practices commonly seen across industry include:

- Deploying SIEM or security data lake collecting logs from all sources
- Implementing 24/7 monitoring (in-house SOC or managed security services)
- Defining use cases and detection rules for known threats
- Employing threat hunting proactively searching for unknown threats
- Deploying EDR/XDR solutions on all endpoints
- Integrating threat intelligence feeds into detection tools
- Monitoring cloud environments with CSPM and CWPP tools
- Tiered alert handling (automated, SOC analyst, senior analyst, IR team)
- Measuring and improving MTTD and MTTR metrics
- Tuning detection rules quarterly reducing false positives



- A. 24/7 SOC with SIEM and advanced threat detection
- B. Security tools with regular monitoring during business hours
- C. Basic logging and periodic reviews
- D. Limited or no active monitoring

Emerging Trends according to industry sources include:

- 24/7 Security Operations Centres (SOC) becoming standard for larger organisations
- SIEM platforms evolving into unified security platforms
- AI/ML improving threat detection and reducing false positives
- Mean time to detect (MTTD) decreasing to ranges such as 16-24 days
- Extended Detection and Response (XDR) correlating signals across security tools
- Managed Detection and Response (MDR) services for organisations lacking internal capacity or capabilities

Q27. How frequently does your organisation provide cyber security awareness training to employees?

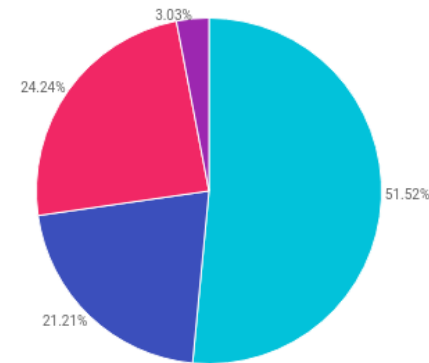
Why it's important

Humans remain the weakest link in security. Phishing and social engineering are among the top attack vectors. Regular training builds a security culture and reduces risky behaviours. One-time training is ineffective as behaviour change requires ongoing reinforcement. Regulatory requirements increasingly mandate security awareness training.

52% of participants conduct continuous training with regular simulated phishing exercises. A further 21% carry out training on a quarterly or bi-annual basis.

Good Practices commonly seen across industry include:

- Deploying a continuous security awareness programme all year round
- Conducting formal training at least quarterly
- Running monthly simulated phishing campaigns (common in mature programmes), providing immediate feedback and coaching for phishing clicks
- Tailoring training to roles (e.g. developers, executives, general staff)
- Covering specific threats e.g. phishing, password security, physical security, data handling
- Track metrics: phishing click rates, training completion, incident reports
- Making training engaging (short videos, interactive modules, gamification)
- Rewarding security-conscious behaviour and incident reporting
- Briefing executives separately on targeted threats (e.g. CEO fraud, whaling)
- Testing effectiveness through periodic security culture assessments



- A. Continuous training with regular simulated phishing exercises
- B. Quarterly or bi-annually
- C. Annually or during onboarding only
- D. Infrequent or no formal training

Emerging Trends according to industry sources include:

- Shifting to continuous micro-learning replacing annual training sessions
- Gamification improving learning engagement and retention
- Simulated phishing campaigns with real-time feedback
- Role-based training tailoring content to job functions
- Measurement of behaviour change, not just training completion
- AI-generated phishing simulations adapting to user performance

4. Analysis and Discussion of Survey Findings

Q28. Does your organisation conduct simulated cyber attack exercises (e.g., red team/purple team)?

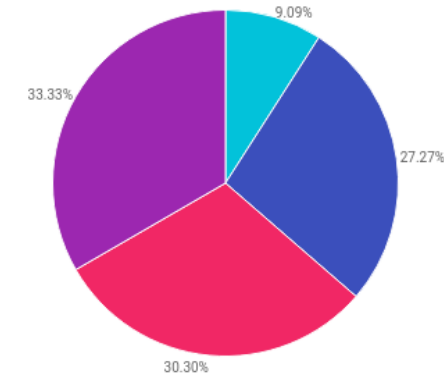
Why it's important

Simulated attacks test actual defence capabilities under realistic conditions. They validate that tools, processes, and people work together effectively. Purple team exercises improve coordination between offensive (red) and defensive (blue) teams. Realistic testing identifies gaps that compliance audits may miss, , providing a wholistic/wider picture of the organisation cybersecurity posture.

9% of the respondents conduct simulated cyber attack exercises on a quarterly basis. 27% do so annually. 63% of participants never conduct such exercises or only do so on an ad hoc basis.

Good Practices commonly seen across industry include:

- Conducting red team/purple team exercises at least annually
- Testing specific threat scenarios relevant to the organisation (e.g. ransomware, state-sponsored, insider)
- Including technical, process, and people elements in testing
- Focusing on detecting and responding, not just preventing
- Engaging external red teams providing unbiased assessment
- Conducting purple team workshops to translate findings into improvements
- Testing crown jewel protection with assumed breach scenarios
- Including executives in crisis simulation components
- Documenting lessons learned and tracking remediation
- Sharing appropriate findings with the board and audit committee



- A. Yes, at least quarterly
- B. Yes, annually
- C. Occasionally or ad-hoc
- D. No, never conducted

Emerging Trends according to industry sources include:

- Purple team exercises (collaborative) replacing pure red team (adversarial)
- Adversary emulation based on specific threat actor TTPs
- Automated adversary simulation tools enabling more frequent testing
- Focus shifting to detection and response speed, not just prevention
- Increasing board participation in cyber crisis simulations
- Integration of physical security testing (facility access)

4. Analysis and Discussion of Survey Findings

Q29. What is your biggest challenge in building cyber resilience?

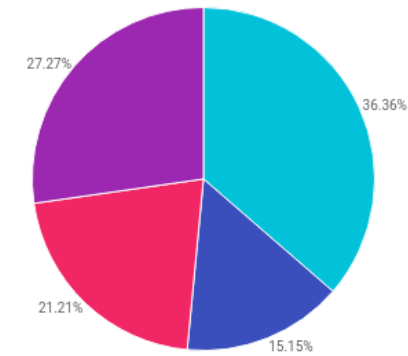
Why it's important

Understanding primary challenges enables targeted resource allocation and strategic planning. Identifying common barriers across organisations may reveal systemic industry issues requiring collaborative solutions. This insight helps boards and senior management justify investments, prioritise initiatives, and benchmark against peers facing similar obstacles in their cyber resilience journey.

36% of participants cited budget constraints and the ability to secure investment as the biggest challenge. 27% cited organisational culture and user awareness. Legacy systems and technical capabilities were the main challenge for 21% and 15% cited a shortage of skills and difficulties in recruiting talent.

Good Practices commonly seen across industry include:

- For budget challenges: quantifying cyber risk in financial terms; demonstrating ROI through prevented breach costs; benchmarking spending against peers; presenting security as business enabler.
- For culture: securing executive sponsorship; demonstrating business value; celebrating security wins; embedding security champions across departments.
- For legacy systems: developing a modernisation roadmap with risk-based priorities; implementing compensating controls; establishing sunset timelines.
- For skills shortages: investing in training existing staff; using managed security services; implementing automation and orchestration; offering competitive compensation; creating clear career paths.



- A. Budget constraints and securing investment
- B. Skills shortage and difficulty recruiting talent
- C. Legacy systems and technical capabilities
- D. Organisational culture and user awareness

Emerging Trends according to industry sources include:

- Skills shortage intensifying with 50% unfilled UK cybersecurity positions; salaries increasing 15-20% annually
- Budget constraints despite rising threats; executives demanding demonstrable ROI and risk quantification
- Legacy system retirement accelerating but technical debt persisting in critical infrastructure
- Cultural resistance declining with increasing awareness following high-profile breaches
- Managed security services and automation addressing skills gaps
- Security-by-design adoption reducing technical debt in new systems

4. Analysis and Discussion of Survey Findings

Q30. Which emerging technologies pose the greatest cyber risk and challenge to your organisation in the next 12 months? (multiple responses allowed)

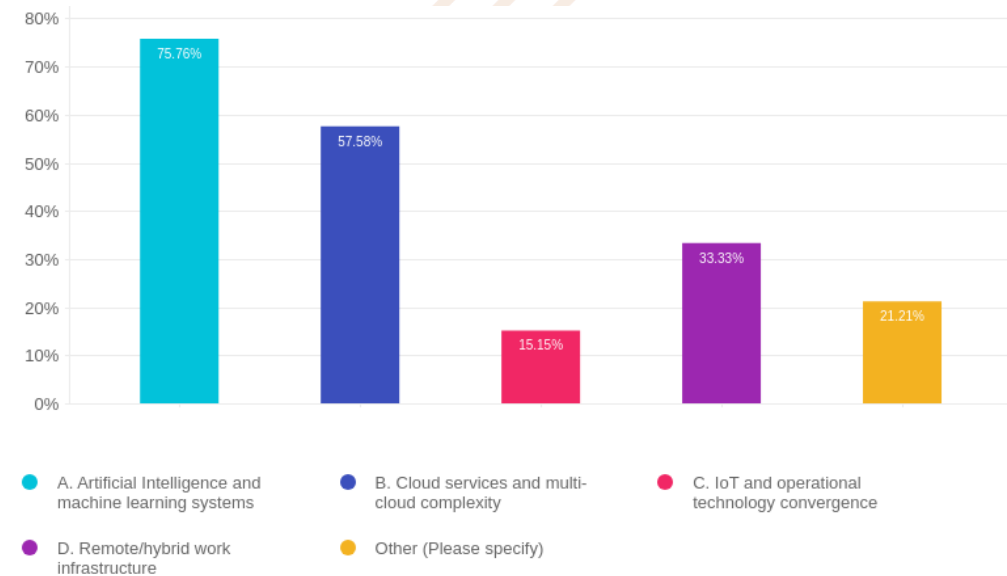
Why it's important

Understanding which emerging technologies pose the greatest risk enables proactive preparation. Different technologies require different security approaches and skills. Resource allocation should anticipate upcoming risks, not just address current ones. Board and executive concern about emerging risks drives investment.

AI/ML, cloud services and complexity, and remote/hybrid work infrastructure were the most frequently listed emerging technologies, with respectively 76%, 58% and 33% of the participants citing these. Other notable items mentioned include quantum computing.

Good Practices commonly seen across industry include:

- AI/ML: Establishing governance for security and ethics; assessing AI threats (deepfakes, automated attacks); implementing AI-specific controls; training teams on vulnerabilities; monitoring for adversarial attacks.
- Cloud: Deploying CSPM and CWPP; establishing architecture standards; training on shared responsibility model; implementing CASB for visibility.
- Remote/Hybrid: Implement zero-trust architecture; secure endpoints; enforce MFA; monitor remote access; provide security awareness training for workers.
- IoT/OT: Segmenting networks; deploying OT-specific monitoring; conducting assessments; managing patching; implementing physical security.
- Quantum: monitoring developments; planning migration to post-quantum cryptography; inventory of cryptographic assets requiring future updates.



Emerging Trends according to industry sources include:

- AI/ML evolving rapidly and lowering technical barrier for entry for offensive capabilities, creating new attack vectors while also improving defences
- Generative AI enabling sophisticated phishing and deepfakes
- Cloud complexity increasing with multi-cloud and hybrid strategies
- IoT/OT convergence expanding attack surface
- Quantum computing threatening current encryption (preparing for post-quantum cryptography)
- Remote work attack surface remaining a significant concern

4. Analysis and Discussion of Survey Findings

Q31. What are your organisation's primary cyber resilience investment priorities for the next 12 months?

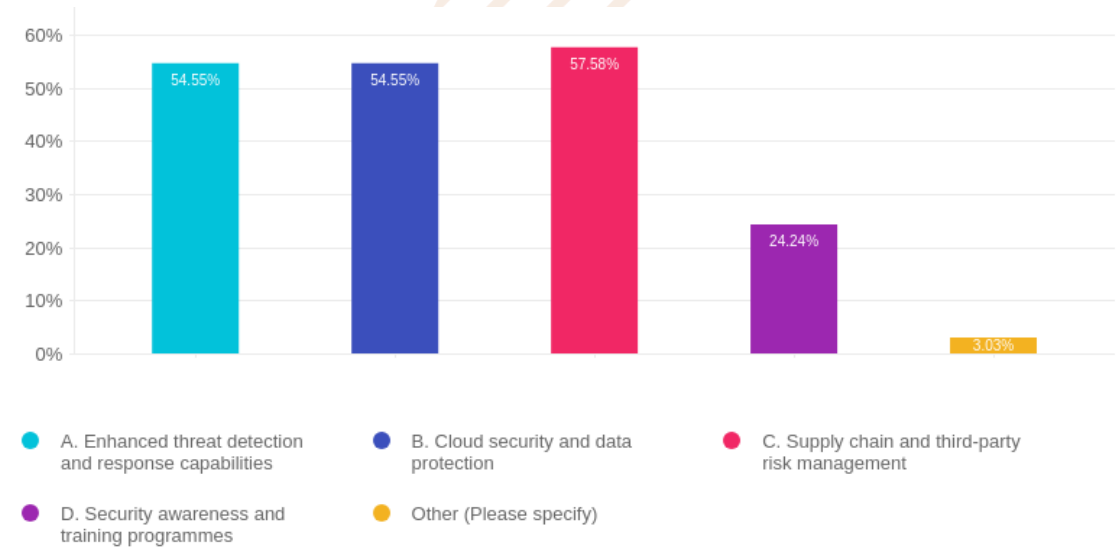
Why it's important

Investment priorities reveal the strategic focus and threat perceptions across organisations. Understanding where leaders allocate resources helps benchmark spending patterns, identify emerging security paradigms, and validate investment decisions. This insight enables organisations learn from peers, avoid under-investing in critical areas, and align spending with industry best practices and evolving threat landscapes.

TPRM, enhanced threat detection and response, and cloud security and data protection are the primary investment priorities cited by participants.

Good Practices commonly seen across industry include:

- Balancing spending across prevention (40%), detection (30%), response (20%), and recovery (10%) capabilities
- Prioritising based on risk assessment outcomes, not vendor marketing or peer pressure
- Addressing identified gaps from recent incidents, audits, and penetration tests first
- Investing in automation to reduce manual security operations burden and address skills shortage
- Allocating budget for emerging threats: AI security, cloud protection, supply chain risk
- Reserving contingency (10-15%) for urgent threats or regulatory requirements
- Measuring ROI through risk reduction metrics and time-to-detect/respond improvements



Emerging Trends according to industry sources include:

- Enhanced detection and response are leading priorities with XDR, MDR, and SOAR platform investments accelerating
- Cloud security spending has been surging as organisations adopt multi-cloud strategies; CSPM and CWPP deployment are increasing
- Supply chain risk management investment rising following high-profile breaches
- Zero Trust architecture projects expanding beyond initial pilots to enterprise-wide deployment
- AI-powered security tools gaining budget share for threat detection and automation
- Security awareness training investment increasing with focus on continuous, behaviour-changing programmes

5. Closing Thoughts and Looking Ahead

This survey provides a snapshot of UK cyber resilience at organisations at a pivotal moment in the evolution of digital security. The findings reveal an ecosystem in transition: organisations are increasingly recognising cyber risk as a fundamental business imperative, yet significant gaps remain between aspiration and implementation across people, process, and technology dimensions.

Several themes emerge as critical priorities for the year ahead. First, the maturity of governance structures—particularly board engagement and strategic planning—directly correlates with the overall resilience posture. Second, the shift from compliance-driven to risk-driven security represents a fundamental mindset change that separates mature organisations from their peers. Third, the persistent challenge of skilled resource acquisition demands creative solutions including managed security services, automation, and strategic partnerships.

Looking forward, UK technology leaders face a demanding agenda. The Cyber Security and Resilience Bill implementation will test organisational preparedness and incident response capabilities. Supply chain security will require sustained attention as attackers increasingly exploit third-party relationships. The integration of artificial intelligence into both attack and defence paradigms will reshape the threat landscape. Meanwhile, the ongoing challenge of maintaining security in hybrid work environments continues to stretch traditional security models. Success in this environment requires sustained executive commitment, adequate resource allocation, and cultural transformation positioning security as an enabler rather than impediment to business objectives. The organisations that thrive will be those treating cyber resilience not as a destination but as a continuous journey of adaptation and improvement. Organisations should seek external expertise as required to implement relevant frameworks and obtain independent assurance through internal or external reviews that the appropriate framework is in place and operating effectively.

We hope that the insights provided in this benchmark report will provide a useful basis for continuous improvement, navigating the challenges ahead and building truly resilient security programmes fit for an increasingly digital future.

Feel free to contact us if you have any questions or would like to discuss the report with our Cyber Maturity team (free of any costs and without obligation).

We thank you for taking the time to read through this report including our analysis of your responses.

We would also like to thank all of those who have responded to our survey questions.

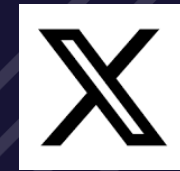
Appendix – List of Abbreviations and Acronyms used

AI: Artificial Intelligence
ACL: Access Control List
BC/DR: Business Continuity / Disaster Recovery
CASB: Cloud Access Security Broker
CI/CD: continuous integration/continuous delivery
CREST: Council of Registered Ethical Security Testers
CSPM: Cloud Security Posture Management
CSR: Cyber Security and Resilience Bill
CWPP: Cloud Workload Protection Platform
DDoS: Distributed Denial of Service
DLP: Data Loss Prevention
DORA: Digital Operational Resilience Act
DPIA: Data Protection Impact Assessment
DMZ: Demilitarized Zone
EDR: Endpoint Detection and Response
ERM: Enterprise Risk Management
FAIR: Factor Analysis of Information Risk framework
FIDO2: Fast IDentity Online 2
IoT: Internet of Things
IPS/IDS: Intrusion Prevention System / Intrusion Detection System
IR: Incident Response
ISAC: Information Sharing and Analysis Center

MDR: Managed Detection and Response
MFA: Multi-Factor Authentication
ML: Machine Learning
MTTR: Mean time to respond
MTTD: Mean time to detect
NCSC CISP: Cyber Security Information Sharing Partnership
NIS 2: Network and Information Security Directive 2
NIST: National Institute of Standards and Technology
OSCP: Offensive Security Certified Professional
PCI DSS: Payment Card Industry Data Security Standard
ROI: Return On Investment
RPO: Recovery Point Objective
RTO: Recovery Time Objective
SBOM: Software Bill of Materials
SIEM: Security Information and Event Management
SOAR: Security Orchestration, Automation and Response
SOC: Security Operations Centre
SOC 2: System and Organization Controls 2
TTP: Tactics, Techniques and Procedures
UEBA: User Entity and Behaviour Analytics
WAF: Web Application Firewall
XDR: Extended Detection and Response

For further information

info@xcinaconsulting.com



www.xcinaconsulting.com

bc
brookcourt
A Shearwater Group plc Company

xcina
Consulting