

TURN THE LATEST CYBERSECURITY TRENDS INTO ACTION

A practical guide to assessing emerging threats, strengthening defences and
building a prioritised security improvement plan.

1. Introduction

1.1 Purpose of the guide

Cybersecurity teams face a changing mix of threats and technology shifts. Attackers can use generative AI to produce convincing messages and impersonations; organisations are adopting AI agents that can take actions across business systems; employees may use unapproved AI services; and identity, cloud, supplier and cryptographic risks continue to require attention.

The purpose of this guide is to help organisations move from awareness to action. Each section explains the trend, highlights practical risk questions and provides an action checklist. The aim is to identify which changes matter most to your environment, what evidence is needed and who should own the next step.

1.2 Who should use this guide

CISOs, IT leaders and security managers setting priorities and allocating resources.

SOC analysts, incident responders and threat intelligence teams.

Identity, cloud, application, infrastructure and data protection teams.

AI product owners, developers and business teams deploying copilots or autonomous agents.

Risk, legal, compliance, privacy, procurement and vendor-management professionals.

People managers and learning teams responsible for security awareness and workforce capability.

1.3 How to use the guide

- ☐ Read each trend section and identify which risks are relevant to your organisation.
- ☐ Complete the action checklist using evidence, not assumptions.
- ☐ Record existing controls, unresolved gaps and dependencies.
- ☐ Assign an owner and priority to each material gap.
- ☐ Use the action plan and readiness scorecard to agree next steps with stakeholders.
- ☐ Review progress regularly and reassess after incidents, major technology changes or new requirements.

1.4 From cybersecurity trends to actionable security improvements

Step	What to do	Output
1. Understand	Translate the trend into realistic threats to your	Relevant threat scenarios.

	systems, people, data and operations.	
2. Assess	Review existing controls and collect evidence of how they operate.	Documented strengths and gaps.
3. Prioritise	Consider likelihood, impact, exposure, dependencies and current safeguards.	Ranked improvement backlog.
4. Implement	Assign accountable owners, resources, deadlines and completion criteria.	Owned action plan.
5. Validate	Test the control, check the evidence and confirm that the change reduced risk.	Verified improvement and updated rating.

A trend should not automatically become a project. Use risk and business context to decide whether a control needs to be introduced, improved, tested or simply monitored.

2. AI-Powered Attacks and Defence

Use this section to connect the trend to your own systems, workflows and risk exposure.

The questions are prompts for discussion; adapt them to the size, sector and technology environment of your organisation.

2.1 How AI is changing the cybersecurity landscape

AI can lower the effort required to research targets, personalise lures, generate code, translate messages and scale social engineering. Defenders can also use AI to summarise alerts, correlate events and support investigations. The technology changes the speed and scale of activity, but it does not remove the need for sound security fundamentals.

Questions to ask: Which critical systems rely on AI-enabled detection? Are analysts able to validate findings? Do existing incident playbooks address AI-assisted attacks?

2.2 AI-generated phishing, malware, and deepfake attacks

AI-generated messages may be fluent, personalised and context-aware. Synthetic voice or video can make impersonation more convincing. AI may assist malware development or adaptation, but defenders should focus on observable behaviour, identity signals, access patterns and layered controls rather than trying to identify whether content was generated by AI alone.

Questions to ask: Do employees know to verify unusual requests independently? Are email, endpoint and identity signals correlated? Can staff report suspicious content quickly?

2.3 Using AI for threat detection and automated response

AI-enabled security tools can help prioritise events, surface anomalies and reduce repetitive investigation work. However, model outputs can be incomplete or misleading, and automation can amplify mistakes if given broad permissions. Human oversight, tested playbooks, audit trails and rollback options are important for consequential decisions.

Questions to ask: What actions may automation take without approval? How is accuracy measured? Can analysts override a recommendation and reconstruct why an action occurred?

2.4 Action checklist

Action checklist item	Status / evidence / notes
Review AI-powered threat detection coverage and data sources.	☐ Not started ☐ In progress ☐ Complete Evidence / owner: _____

Establish human oversight and approval boundaries for automated security decisions.	☐ Not started ☐ In progress ☐ Complete Evidence / owner: _____
Test defences against AI-enabled phishing and impersonation scenarios.	☐ Not started ☐ In progress ☐ Complete Evidence / owner: _____
Define governance rules, logging, accuracy review and accountability for AI security tools.	☐ Not started ☐ In progress ☐ Complete Evidence / owner: _____

Priority gaps / observations:

Accountable owner: _____ Review date: _____

Cybersecurity Trends Action Guide | Page

3. Agentic AI Security and Governance

Use this section to connect the trend to your own systems, workflows and risk exposure.

The questions are prompts for discussion; adapt them to the size, sector and technology environment of your organisation.

3.1 Understanding agentic AI and autonomous actions

An AI agent can plan or execute multi-step tasks, use tools, call APIs, retrieve information or change systems. This creates a different risk profile from a tool that only returns text: an agent may have access to business data and operational capabilities, so its permissions and action boundaries matter.

Questions to ask: Which agents are deployed, who owns them, what tools can they call and what data can they access?

3.2 Risks associated with excessive AI agent permissions

Excessive permissions can turn a prompt injection, compromised credential, flawed instruction or model error into an operational incident. An agent with broad write access may alter records, expose information or make changes beyond its intended purpose.

Questions to ask: Could an agent access unrelated systems, export sensitive data, change production or take irreversible actions? Are permissions reviewed?

3.3 Securing AI agents and automated workflows

Treat agents as identities and software components. Use least privilege, scoped credentials, approved tool lists, input and output validation, logging, testing and human approval for high-impact actions. Monitor dependencies and provide a safe way to suspend an agent or revoke its access.

Questions to ask: Are agent actions logged? Are tools restricted by allowlists? Are dangerous actions gated? Is there a tested shutdown and credential-revocation procedure?

3.4 Action checklist

Action checklist item	Status / evidence / notes
Apply least-privilege access to each AI agent and restrict its available tools.	☐ Not started ☐ In progress ☐ Complete Evidence / owner: _____
Maintain activity logs and audit trails for consequential agent actions.	☐ Not started ☐ In progress ☐ Complete Evidence / owner: _____

Define human approval requirements for high-impact or irreversible actions.	☐ Not started ☐ In progress ☐ Complete Evidence / owner: _____
Assign clear business and technical ownership, including incident and retirement responsibilities.	☐ Not started ☐ In progress ☐ Complete Evidence / owner: _____

Priority gaps / observations:

Accountable owner: _____ Review date: _____

Cybersecurity Trends Action Guide | Page

4. Shadow AI and Data Protection

Use this section to connect the trend to your own systems, workflows and risk exposure.

The questions are prompts for discussion; adapt them to the size, sector and technology environment of your organisation.

4.1 What is Shadow AI?

Shadow AI is the use of AI services, browser extensions, integrations or models without the organisation's approval or oversight. It can occur when employees use personal accounts or unreviewed tools to solve legitimate work problems, sometimes without understanding where submitted data goes.

Questions to ask: Can the organisation identify AI services in use? Is there a practical route for employees to request an approved tool?

4.2 Risks of exposing sensitive data through unapproved AI tools

Prompts, uploads, transcripts and generated outputs may contain personal, customer, financial, source-code or confidential business information. Risks depend on provider settings, retention, access, contractual terms and how the service is used. Data minimisation and clear rules reduce avoidable exposure.

Questions to ask: Which data categories may be entered into each approved tool? Are retention, training use, access and deletion terms understood?

4.3 Establishing responsible AI usage practices

Effective policies should be practical: identify approved services, define prohibited data and use cases, explain review requirements, and provide an approval path for new needs. Training should explain both the risks and safe alternatives, so employees are not left to improvise.

Questions to ask: Are rules easy to find? Are they tailored to job roles? Are DLP controls and exception processes appropriate to the risk?

4.4 Action checklist

Action checklist item	Status / evidence / notes
Identify AI tools and integrations currently used across the organisation.	☐ Not started ☐ In progress ☐ Complete Evidence / owner: _____
Publish an approved AI tool list and a practical approval process.	☐ Not started ☐ In progress ☐ Complete Evidence / owner: _____

Define rules for handling confidential, personal, customer and regulated information.	☐ Not started ☐ In progress ☐ Complete Evidence / owner: _____
Train employees on safe AI usage and how to report accidental disclosure.	☐ Not started ☐ In progress ☐ Complete Evidence / owner: _____
Review data loss prevention controls and appropriate exception processes.	☐ Not started ☐ In progress ☐ Complete Evidence / owner: _____

Priority gaps / observations:

Accountable owner: _____ Review date: _____

Cybersecurity Trends Action Guide | Page

5. Zero Trust and Identity-First Security

Use this section to connect the trend to your own systems, workflows and risk exposure.

The questions are prompts for discussion; adapt them to the size, sector and technology environment of your organisation.

5.1 Understanding Zero Trust Architecture

Zero Trust is an approach in which access is explicitly verified and limited according to identity, device, context and resource sensitivity. It does not mean trusting nothing indiscriminately; it means avoiding implicit trust based solely on network location or a previous login.

Questions to ask: Are access decisions based on verified identity and context? Are sensitive resources segmented and access reviewed?

5.2 Identity, devices, applications, and AI agents as access points

Users are only one part of the identity landscape. Workloads, service accounts, APIs, devices and AI agents may hold credentials or permissions. Each identity needs an owner, a defined purpose and controls appropriate to its privileges.

Questions to ask: Is there an inventory of human and non-human identities? Are dormant accounts and unmanaged credentials identified?

5.3 Multi-factor authentication and least-privilege access

MFA reduces reliance on passwords alone, while least privilege limits the damage possible if an account or token is compromised. Privileged access, remote access, administrative consoles and sensitive AI integrations deserve particular attention.

Questions to ask: Are MFA exceptions justified and monitored? Are privileged permissions time-limited where feasible? Are API scopes narrow and credentials rotated?

5.4 Action checklist

Action checklist item	Status / evidence / notes
Enforce MFA for critical systems and privileged access.	☐ Not started ☐ In progress ☐ Complete Evidence / owner: _____
Review privileged accounts, roles and permissions.	☐ Not started ☐ In progress ☐ Complete Evidence / owner: _____

Verify device security before granting access to sensitive resources.	☐ Not started ☐ In progress ☐ Complete Evidence / owner: _____
Monitor unusual login, session and access activity.	☐ Not started ☐ In progress ☐ Complete Evidence / owner: _____
Audit service accounts, API keys and AI agent identities.	☐ Not started ☐ In progress ☐ Complete Evidence / owner: _____

Priority gaps / observations:

Accountable owner: _____ Review date: _____

Cybersecurity Trends Action Guide | Page

6. Ransomware, Phishing, and Deepfake

Prevention

Use this section to connect the trend to your own systems, workflows and risk exposure.

The questions are prompts for discussion; adapt them to the size, sector and technology environment of your organisation.

6.1 Understanding the evolving threat landscape

Ransomware and social engineering can combine technical compromise with pressure tactics, impersonation and data theft. Organisations should plan for prevention, detection, containment, communication and recovery rather than relying on a single security product.

Questions to ask: Which systems are business-critical? What attack paths could lead to widespread disruption? Who makes containment and recovery decisions?

6.2 Ransomware prevention and recovery

Defences commonly include patching, endpoint protection, segmentation, controlled administrative access, secure backups and tested restoration. Backups should be protected from the same compromised credentials or systems that could affect production. Recovery plans should address dependencies and business priorities.

Questions to ask: Can critical systems be restored within agreed objectives? Are backups isolated or otherwise protected? Have recovery steps been tested recently?

6.3 Detecting phishing and impersonation attempts

Look for unusual requests, mismatched context, unexpected attachments, suspicious links, changes to payment details and attempts to bypass established processes. Sender names, polished language, caller ID or familiar voices are not sufficient proof of identity.

Questions to ask: Do email and identity controls work together? Can employees verify requests through known contact details and report concerns?

6.4 Building employee awareness and verification habits

Training should reinforce behaviours: pause when a request is unusual, verify using an independent trusted channel, follow approval procedures and report suspected attacks promptly. Scenario-based exercises can reveal gaps in both employee knowledge and business processes.

Questions to ask: Do exercises test voice/video impersonation and urgent payment scenarios? Are results used to improve processes rather than merely score individuals?

6.5 Action checklist

Action checklist item	Status / evidence / notes
-----------------------	---------------------------

Maintain secure backups and test recovery of critical systems.	☐ Not started ☐ In progress ☐ Complete Evidence / owner: _____
Conduct phishing and deepfake awareness exercises.	☐ Not started ☐ In progress ☐ Complete Evidence / owner: _____
Verify financial and sensitive requests through trusted communication channels.	☐ Not started ☐ In progress ☐ Complete Evidence / owner: _____
Establish clear incident reporting and escalation procedures.	☐ Not started ☐ In progress ☐ Complete Evidence / owner: _____
Test ransomware response, containment and recovery plans.	☐ Not started ☐ In progress ☐ Complete Evidence / owner: _____

Priority gaps / observations:

Accountable owner: _____ Review date: _____

Cybersecurity Trends Action Guide | Page

7. Cybersecurity Governance and Regulatory

Compliance

Use this section to connect the trend to your own systems, workflows and risk exposure.

The questions are prompts for discussion; adapt them to the size, sector and technology environment of your organisation.

7.1 Integrating cybersecurity into organisational risk management

Cybersecurity decisions should connect to business impact, risk appetite, critical services and accountable owners. Risk registers, exception approvals and management reporting help leadership understand trade-offs and track whether important risks are being reduced.

Questions to ask: Are significant risks documented, owned, reviewed and escalated?

Are exceptions time-bound and formally accepted?

7.2 Understanding relevant regulatory obligations

Requirements vary by jurisdiction, sector, data type and contractual commitments.

Organisations should maintain an obligation register and obtain appropriate legal or compliance input rather than assuming one framework covers every duty.

Questions to ask: Who confirms applicability? Are reporting triggers, deadlines, evidence requirements and accountable contacts documented?

7.3 Incident reporting and accountability

Incident response needs clear severity definitions, decision rights, escalation paths, evidence handling and communication responsibilities. Applicable notification requirements should be integrated into the response process and validated with qualified advisers.

Questions to ask: Can responders determine who must be notified, by whom and within what timeframe? Are contact lists and playbooks current?

7.4 Third-party and supply-chain security

Providers, software dependencies, managed services and AI vendors can introduce risks through access, data processing, vulnerabilities or service disruption. Reviews should be proportionate to criticality and continue when services or dependencies change.

Questions to ask: Are critical suppliers inventoried? Do contracts address data handling, incident notification, access, resilience and exit arrangements?

7.4 Action checklist

Action checklist item	Status / evidence / notes
-----------------------	---------------------------

Identify applicable regulations, contractual obligations and reporting deadlines.	☐ Not started ☐ In progress ☐ Complete Evidence / owner: _____
Assign responsibility for compliance and incident reporting activities.	☐ Not started ☐ In progress ☐ Complete Evidence / owner: _____
Review third-party and supply-chain security risks.	☐ Not started ☐ In progress ☐ Complete Evidence / owner: _____
Document incident escalation, notification and decision procedures.	☐ Not started ☐ In progress ☐ Complete Evidence / owner: _____
Conduct periodic compliance assessments and track findings to closure.	☐ Not started ☐ In progress ☐ Complete Evidence / owner: _____

Priority gaps / observations:

Accountable owner: _____ Review date: _____

Cybersecurity Trends Action Guide | Page

8. Post-Quantum Cybersecurity Readiness

Use this section to connect the trend to your own systems, workflows and risk exposure.

The questions are prompts for discussion; adapt them to the size, sector and technology environment of your organisation.

8.1 Understanding the potential impact of quantum computing

A sufficiently capable quantum computer could undermine some widely used public-key cryptographic methods. The timeline and impact are uncertain, so organisations should follow trusted standards guidance and prepare systematically rather than assume an immediate universal break.

Questions to ask: Which systems rely on public-key cryptography? Who owns cryptographic architecture and technology decisions?

8.2 Risks associated with long-term sensitive data exposure

Data that must remain confidential for many years may face a longer-term risk if encrypted traffic or stored information can be collected now and decrypted later. The relevance depends on data sensitivity, required confidentiality lifetime and the cryptography used.

Questions to ask: Which datasets or communications have long confidentiality requirements? Are retention and encryption decisions aligned to that lifetime?

8.3 Preparing for post-quantum cryptography

Preparation begins with cryptographic discovery, dependency mapping, vendor engagement and an ability to change algorithms or libraries. Migration may require coordination across applications, devices, certificates, protocols and suppliers, so a phased plan is preferable to isolated changes.

Questions to ask: Can the organisation inventory algorithms, keys, certificates and dependencies? Are critical vendors tracking standards and migration options?

8.4 Action checklist

Action checklist item	Status / evidence / notes
Inventory encryption methods, certificates, keys and cryptographic dependencies across critical systems.	☐ Not started ☐ In progress ☐ Complete Evidence / owner: _____
Identify systems using vulnerable, outdated or difficult-to-replace cryptography.	☐ Not started ☐ In progress ☐ Complete Evidence / owner: _____

Prioritise long-lived sensitive data and critical infrastructure.	☐ Not started ☐ In progress ☐ Complete Evidence / owner: _____
Track recognised standards and migration guidance from trusted authorities.	☐ Not started ☐ In progress ☐ Complete Evidence / owner: _____
Develop a phased cryptographic migration plan with owners and dependencies.	☐ Not started ☐ In progress ☐ Complete Evidence / owner: _____

Priority gaps / observations:

Accountable owner: _____ Review date: _____

Cybersecurity Trends Action Guide | Page

9. Cybersecurity Skills and Workforce Readiness

Use this section to connect the trend to your own systems, workflows and risk exposure.

The questions are prompts for discussion; adapt them to the size, sector and technology environment of your organisation.

9.1 Evolving cybersecurity roles and responsibilities

Teams increasingly need to work across traditional security, cloud, identity, data governance and AI-enabled systems. Roles may evolve, but responsibility should remain clear: tools can assist specialists, not remove the need for judgement, accountability and communication.

Questions to ask: Which capabilities are essential to the organisation's threat profile?

Are responsibilities clear across security, IT, AI and business teams?

9.2 AI, cloud security, identity management, and threat intelligence skills

Priority capabilities may include cloud configuration, identity and access management, incident handling, threat analysis, secure AI integration, data protection and risk communication. The right mix depends on systems, sector and the organisation's operating model.

Questions to ask: Which skills are needed for current systems and planned AI adoption? Which tasks require internal expertise versus a trusted external partner?

9.3 Identifying organisational skills gaps

A useful assessment compares required capabilities with current evidence, such as practical exercises, incident outcomes, project experience and role expectations. Self-ratings alone may not show whether a team can perform under pressure.

Questions to ask: Can staff demonstrate the skills in realistic scenarios? Are gaps prioritised by risk and tied to development plans?

9.4 Action checklist

Action checklist item	Status / evidence / notes
Assess current team capabilities against organisational risk and planned technology changes.	☐ Not started ☐ In progress ☐ Complete Evidence / owner: _____
Identify priority technical, AI security and governance skills gaps.	☐ Not started ☐ In progress ☐ Complete Evidence / owner: _____
Develop role-based training and practical development plans.	☐ Not started ☐ In progress ☐ Complete Evidence / owner: _____

Conduct realistic incident response and cross-team exercises.	☐ Not started ☐ In progress ☐ Complete Evidence / owner: _____
Encourage continuous professional development and relevant certifications.	☐ Not started ☐ In progress ☐ Complete Evidence / owner: _____

Priority gaps / observations:

Accountable owner: _____ Review date: _____

Cybersecurity Trends Action Guide | Page

10. Cybersecurity Trends Action Plan

Use this worksheet to convert the guide into a prioritised, owned implementation plan.

Choose a status based on evidence and record the next concrete step. “To assess” is appropriate when the current position is not yet known.

Security area	Current status	Priority	Next action	Owner	Target date
AI threat detection	To assess / In progress / Implemented	High / Medium / Low	_____	_____	_____
Agentic AI governance	To assess / In progress / Implemented	High / Medium / Low	_____	_____	_____
Shadow AI controls	To assess / In progress / Implemented	High / Medium / Low	_____	_____	_____
Zero Trust and identity	To assess / In progress / Implemented	High / Medium / Low	_____	_____	_____

Ransomware readiness	To assess / In progress / Implemented	High / Medium / Low	_____	_____	_____
Regulatory compliance	To assess / In progress / Implemented	High / Medium / Low	_____	_____	_____
Post-quantum readiness	To assess / In progress / Implemented	High / Medium / Low	_____	_____	_____
Workforce skills	To assess / In progress / Implemented	High / Medium / Low	_____	_____	_____

10.1 How to prioritise actions

Priority	Use when	Expected handling
High	A gap could expose sensitive data, privileged access, critical services or	Contain urgent exposure; assign an owner promptly; agree a near-term

	create significant legal or operational impact.	milestone and monitor until resolved.
Medium	The gap matters but existing safeguards reduce immediate exposure or the impact is more limited.	Schedule work with a clear owner and target date; track dependencies and verify completion.
Low	The improvement would strengthen resilience or maturity but has comparatively limited immediate risk.	Place in the improvement backlog and revisit during planned reviews or when dependencies change.

10.2 Suggested implementation timeline

Period	Focus	Example outputs
First 30 days	Identify major risks, review access permissions and assess existing policies and inventories.	Top-risk list, initial AI tool/agent inventory, privileged-access findings, owners for urgent gaps.

Days 31–60	Address priority gaps, improve employee awareness and update incident response procedures.	Remediation underway, awareness exercise completed, response playbooks and escalation paths updated.
Days 61–90	Test controls, review progress and establish ongoing monitoring and improvement.	Control test results, recovery or tabletop exercise, updated scorecard and recurring review schedule.

Timeline note: adjust milestones to reflect risk, available resources, regulatory obligations and operational dependencies. Critical exposures should be addressed immediately rather than deferred to a 30-day milestone.

10.3 Action tracking and closure

Action ID	Success measure / completion evidence	Dependency / risk	Closure verified by	Date closed
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____

_____	_____	_____	_____	_____
_____	_____	_____	_____	_____

Cybersecurity Trends Action Guide | Page

11. Cybersecurity Readiness Scorecard

Rating scale

Rating	Status	Meaning
1	Not Implemented	No reliable control or repeatable process is in place.
2	Needs Improvement	Control exists but is incomplete, inconsistent or weakly evidenced.
3	Partially Implemented	Some elements are in place, but gaps in coverage or effectiveness remain.
4	Mostly Implemented	Control is broadly deployed and effective; limited gaps remain.

5	Fully Implemented	Control is evidenced, tested, maintained and periodically reviewed.
---	-------------------	---

Rate the current, evidenced state—not the intended future state. If a control is not applicable, document why and exclude it from the denominator. Do not count an unknown or unassessed control as implemented.

Area	Assessment question	Rating (1–5)	Evidence / notes
AI security	AI-powered threat detection is deployed for relevant systems and reviewed for effectiveness.	_____	_____
AI security	AI security tools have defined governance, human oversight and audit trails.	_____	_____

Agentic AI	AI agents have named owners, scoped permissions and approved tool access.	_____	_____
Agentic AI	High-impact agent actions require suitable approval and can be stopped or reversed where feasible.	_____	_____
Data protection	Approved AI tools and acceptable-use rules are documented and communicated.	_____	_____
Data protection	Controls reduce unauthorised sharing of sensitive	_____	_____

	information with AI services.		
Identity	MFA is enforced for critical and privileged access with exceptions reviewed.	_____	_____
Identity	Human and non-human identities are inventoried and granted least privilege.	_____	_____
Ransomware	Critical systems have protected backups and recovery is tested.	_____	_____
Ransomware	Incident response procedures include containment, escalation and	_____	_____

	recovery responsibilities.		
Phishing / deepfakes	Employees practise independent verification of sensitive or unusual requests.	_____	_____
Phishing / deepfakes	Employees can report suspicious messages and impersonation attempts quickly.	_____	_____
Governance	Relevant regulatory and contractual obligations have owners and documented reporting processes.	_____	_____
Third-party risk	Critical suppliers and AI providers are	_____	_____

	assessed and reviewed proportionately.		
Post-quantum	Critical cryptographic dependencies are inventoried or a discovery plan is approved.	_____	_____
Workforce	Priority skills gaps are assessed and supported by role-based development plans.	_____	_____

11.1 Calculate the score

☐ Total number of questions rated: _____ / 16

☐ Sum of ratings: _____

☐ Overall average = sum of ratings ÷ number rated: _____ / 5

☐ Questions rated 1 or 2: _____

☐ Critical gaps requiring action regardless of score: _____

11.2 Interpret the overall average

Average score	Suggested interpretation	Recommended focus
1.00–1.79	Foundational gaps	Address urgent exposure and establish essential controls.
1.80–2.79	Developing	Formalise ownership, extend coverage and improve consistency.
2.80–3.79	Reasonably prepared	Close important gaps and validate control effectiveness.
3.80–5.00	Strong and improving	Maintain testing, monitoring and continuous improvement.

Averages can hide high-impact weaknesses. Review individual low ratings and risk context before deciding what to address first. This scorecard is a self-assessment aid, not a certification or compliance determination.

Cybersecurity Trends Action Guide | Page

Conclusion: Make Cybersecurity a Continuous Priority

Cybersecurity trends matter when they change the organisation's exposure, the effectiveness of existing controls or the capabilities needed to manage risk. AI-powered attacks and defence, autonomous agents, Shadow AI, identity-first security, ransomware, deepfakes, regulatory expectations, post-quantum preparation and workforce capability are connected parts of the same security programme.

The most useful next step is not to tackle every trend at once. Establish an evidence-based view of current readiness, identify critical gaps, choose proportionate actions and assign clear ownership. Test whether changes work, document the results and adjust the plan as technology and threats evolve.

Commitments for the next review cycle

Commitment	Owner	Due date	Evidence of progress
Top risk to address: _____	_____	_____	_____
Control to test: _____	_____	_____	_____

Policy / process to update: _____	_____	_____	_____
Training / exercise to run: _____	_____	_____	_____

- ☐ Review the action plan at an agreed cadence and escalate overdue high-priority actions.
- ☐ Reassess after major incidents, new AI deployments, supplier changes or material technology shifts.
- ☐ Keep the scorecard, risk register and evidence current so leadership can make informed decisions.
- ☐ Treat cybersecurity as an ongoing operating discipline—not a one-time checklist exercise.

Final review and sign-off

Prepared by	Reviewed by	Date	Next review date
_____	_____	_____	_____

CERTIFIED CYBER SECURITY FOUNDATION (CCSF)

THE CERTIFIED CYBER SECURITY FOUNDATION PROGRAM IS GLOBALLY DESIGNED TO DEVELOP FOUNDATIONAL EXPERTISE IN CYBERSECURITY PRINCIPLES, RISK MANAGEMENT, AND SECURITY BEST PRACTICES TO HELP PROTECT SYSTEMS, NETWORKS, AND DIGITAL ASSETS FROM EVOLVING CYBER THREATS.



ABOUT GSDC CERTIFICATION



EBOOK

Extensive and exclusive Ebook created by world's experts to help you with understanding core concepts.



EBOOK

Extensive and exclusive Ebook created by world's experts to help you with understanding core concepts.



CREATED BY EXPERTS

GSDC certifications are created and authored by world's leading experts in the field.



LEARNING MATERIALS

Get access to learning materials such as videos, ebooks, templates, and practice exams, which will help you clear the certification exam.

LEARNING OBJECTIVE

- Explore ethical hacking fundamentals and their role in security.
- Establish a reputation as a sought-after cybersecurity expert
- Enhance the ability to protect organizational data and critical infrastructure.
- Build awareness of regulatory compliance and cybersecurity policies.

Enroll now with the
code **LEARN20** To
avail **20%** discount

Enroll Now



www.gsdcouncil.org