# RESKILLING LAB
# DT-02 TRAINING & SELF-LEARNING PACK

**CYBERSECURITY**

*From Digital User to Cybersecurity-Aware Professional*

Beginner → Intermediate | Recommended learning time: 40–60 hours
Expanded Learner Handbook | Version 1.0 | September 2026

# How to Use This Handbook

DT-02 is designed for self-learning, blended learning and trainer-supported delivery. It develops practical cybersecurity competence for employees, SME staff, VET learners, jobseekers and career changers. The handbook combines theoretical explanations, guided exercises, safe simulations, SME cases, risk-assessment activities, incident-response practice and a capstone project.

All practical work must be performed only on systems, accounts, networks and training environments that the learner owns or is explicitly authorised to use. The pathway teaches defensive cybersecurity and risk reduction; it does not require intrusive testing of third-party systems.

# 1. Pathway Overview

| Item | DT-02 Specification |
|---|---|
| Pathway | Cybersecurity |
| Target level | Beginner → Intermediate |
| Recommended workload | 40–60 hours |
| Target groups | Employees; SME staff; VET learners; jobseekers; career changers; trainers; administrative, business and junior IT personnel |
| Entry requirements | Basic digital literacy and routine use of computers, web browsers, email and online services |
| Possible target roles | Cybersecurity Support Technician; Junior Security Analyst; SME Cybersecurity Coordinator; Security-aware IT Support Specialist |
| Learning mode | Self-learning, blended learning or trainer-supported |
| Main evidence | Asset inventory; risk register; phishing analysis; access-control checklist; backup plan; incident playbook; capstone SME security improvement plan |

## 1.1 Learning Outcomes

- Explain cybersecurity, information security, cyber risk, threats, vulnerabilities, controls and resilience.
- Identify common SME assets, attack surfaces and threat scenarios.
- Recognise phishing, social engineering, malware, credential attacks and common online fraud patterns.
- Explain basic network, endpoint, cloud and wireless-security concepts.
- Apply practical controls including MFA, secure passwords, patching, least privilege, backups and secure configuration.
- Classify information and apply basic privacy, confidentiality and data-protection precautions.
- Perform a simple cybersecurity risk assessment using likelihood, impact and control effectiveness.
- Describe incident-response stages and prepare a basic incident playbook.
- Recognise supply-chain, cloud, remote-work and AI-enabled cyber risks.
- Use NIST CSF 2.0 concepts to structure SME cybersecurity improvement.
- Relate learning to European cybersecurity skills and regulatory context.
- Create a realistic cybersecurity improvement plan for a small organisation.

## 1.2 Framework Alignment

The handbook uses NIST Cybersecurity Framework (CSF) 2.0 as a practical risk-management backbone. CSF 2.0 is designed for organisations of any size, sector or maturity and organises cybersecurity outcomes around six functions: Govern, Identify, Protect, Detect, Respond and Recover. The European Cybersecurity Skills Framework (ECSF) is used as a career and competence reference. ENISA describes ECSF as the EU reference point for cybersecurity professional skills and role profiles.

| Reference | How DT-02 uses it |
|---|---|
| NIST CSF 2.0 | Risk-management structure: Govern, Identify, Protect, Detect, Respond, Recover. |
| ENISA ECSF | Career awareness, professional-role language and competence development. |
| NIS2 | European context for cybersecurity risk-management and incident-reporting obligations in covered sectors/entities. |
| DigComp | General digital-safety and security competence context for citizens and workers. |

## 2. Initial Skills Check

Before training, rate each statement: 0 = No, 1 = Partly, 2 = Yes. Repeat the same check after completing DT-02.

| # | Statement | 0 No | 1 Partly | 2 Yes |
|---|---|---|---|---|
| 1 | I can explain the difference between a threat, vulnerability, risk and security control. | ☐ | ☐ | ☐ |
| 2 | I can identify the most important digital assets in a small organisation. | ☐ | ☐ | ☐ |
| 3 | I can recognise common phishing and social-engineering warning signs. | ☐ | ☐ | ☐ |
| 4 | I use strong authentication practices, including MFA where available. | ☐ | ☐ | ☐ |
| 5 | I understand why software updates and patching are security controls. | ☐ | ☐ | ☐ |
| 6 | I can explain least privilege and why administrator rights should be limited. | ☐ | ☐ | ☐ |
| 7 | I understand the purpose of firewalls, secure Wi-Fi and network segmentation. | ☐ | ☐ | ☐ |
| 8 | I can explain the 3-2-1 backup principle and why recovery testing matters. | ☐ | ☐ | ☐ |
| 9 | I know what to do first when I suspect a cybersecurity incident. | ☐ | ☐ | ☐ |
| 10 | I can distinguish confidentiality, integrity and availability. | ☐ | ☐ | ☐ |
| 11 | I can perform a simple likelihood-impact risk assessment. | ☐ | ☐ | ☐ |
| 12 | I understand basic cloud, supply-chain and AI-related cybersecurity risks. | ☐ | ☐ | ☐ |

Indicative formative interpretation: 0–8 Foundation needed; 9–16 Developing; 17–20 Functional; 21–24 Ready for intermediate practice. This is not a formal professional certification.

## 3. Cybersecurity Foundations: Assets, Threats, Vulnerabilities and Risk

Cybersecurity is the protection of digital systems, networks, devices, services, applications and information against events that could compromise their confidentiality, integrity, availability or legitimate use. Cybersecurity is broader than installing antivirus software. It combines people, processes, technology, governance and continuous risk management.

An asset is anything of value that an organisation needs to protect. Assets include laptops, servers, cloud accounts, websites, customer databases, intellectual property, credentials, operational technology, business

processes and reputation. Effective security starts by knowing what exists, who owns it, where it is located and how important it is to operations.

A threat is a potential cause of harm. A vulnerability is a weakness that a threat may exploit. Risk reflects the possibility that a threat exploits a vulnerability and produces an adverse consequence. A control or safeguard reduces likelihood, impact or both. These terms should not be used interchangeably: an unpatched application is a vulnerability; ransomware is a threat; loss of operations and data is an impact; patching and tested backups are controls.

The CIA triad provides a foundational model. Confidentiality means information is accessible only to authorised people or systems. Integrity means information and systems remain accurate, complete and protected from unauthorised alteration. Availability means authorised users can access information and services when needed. Many incidents affect more than one dimension.

Risk is contextual. The same technical weakness can create different levels of risk in different organisations. A temporary outage of a public brochure site may be inconvenient; an outage of a production-control or healthcare system can be severe. Security decisions therefore require understanding business processes, dependencies and consequences.

### Key Learning Points

- Relate the concepts to a real SME or workplace process.
- Identify at least one preventive, one detective and one recovery control.
- Record one example of how human behaviour and organisational process affect the technical risk.

### Practical Activity

Apply the concepts to the fictional company 'Northstar SME', a 25-person organisation using cloud email, laptops, a public website, online banking, shared cloud storage and an outsourced IT provider. Record the relevant assets, risks, controls and improvement actions for this chapter.

## 4. The Cyber Threat Landscape and Attacker Behaviour

Cyber threats come from different actors with different motives and capabilities. Criminal groups may seek money through ransomware, fraud or data theft. Insiders may cause harm intentionally or accidentally. Competitors may seek commercial intelligence. State-linked actors may pursue espionage or disruption. Opportunistic attackers may simply exploit exposed systems at scale.

Attackers frequently choose the easiest path rather than the most technically sophisticated path. Weak passwords, reused credentials, unpatched software, exposed remote-access services, misconfigured cloud storage and successful social engineering can provide an entry point. This is why basic controls remain strategically important.

A typical attack can be viewed as a sequence: reconnaissance, initial access, execution, persistence, privilege escalation, credential access, lateral movement, collection, exfiltration and impact. Not every incident follows every stage, but thinking in stages helps defenders identify opportunities to prevent, detect or contain an attack.

For SMEs, concentration risk is important. One administrator account, one cloud tenant, one outsourced IT provider or one backup location may become a single point of failure. Small organisations should therefore

focus on business-critical dependencies rather than attempting to copy the security architecture of a large enterprise.

### Key Learning Points

- Relate the concepts to a real SME or workplace process.
- Identify at least one preventive, one detective and one recovery control.
- Record one example of how human behaviour and organisational process affect the technical risk.

### Practical Activity

Apply the concepts to the fictional company 'Northstar SME', a 25-person organisation using cloud email, laptops, a public website, online banking, shared cloud storage and an outsourced IT provider. Record the relevant assets, risks, controls and improvement actions for this chapter.

## 5. Social Engineering, Phishing and Business Email Compromise

Social engineering exploits human trust, urgency, authority, curiosity or fear. The attacker tries to influence a person into revealing information, opening malicious content, transferring money, changing payment details or bypassing a normal procedure. Technical controls help, but organisational procedures and employee confidence to verify unusual requests are equally important.

Phishing messages may impersonate banks, cloud services, colleagues, suppliers or senior managers. Warning signs can include unusual urgency, unexpected attachments, mismatched sender details, suspicious links, requests for credentials, payment changes or attempts to move the conversation away from established channels. However, modern phishing can be grammatically polished and highly personalised, so poor spelling is no longer a reliable indicator.

Business Email Compromise (BEC) targets business processes, especially payments and supplier relationships. An attacker may compromise or imitate an email account and request a change in bank details or an urgent transfer. A strong defence is procedural: independently verify payment-detail changes using a known contact method rather than relying on the email thread itself.

Generative AI can increase the scale and quality of social-engineering content, including personalised messages, translated scams and synthetic voice or images. The defensive response is not to assume that realistic content is genuine. Verification procedures should be based on trusted channels, approval thresholds and known identities.

### Key Learning Points

- Relate the concepts to a real SME or workplace process.
- Identify at least one preventive, one detective and one recovery control.
- Record one example of how human behaviour and organisational process affect the technical risk.

### Practical Activity

Apply the concepts to the fictional company 'Northstar SME', a 25-person organisation using cloud email, laptops, a public website, online banking, shared cloud storage and an outsourced IT provider. Record the relevant assets, risks, controls and improvement actions for this chapter.

# 6. Malware, Ransomware and Endpoint Security

Malware is malicious software designed to disrupt, spy, steal, manipulate or provide unauthorised access. Categories include ransomware, spyware, trojans, worms and information stealers. Modern attacks often combine malware with stolen credentials and legitimate administration tools, making simple file-based detection insufficient.

Ransomware typically seeks to make data or systems unavailable, often through encryption, and may also steal information for extortion. Resilience depends on prevention, detection, containment and recovery. Tested offline or otherwise protected backups are critical, but backups alone do not prevent data theft or reputational damage.

Endpoint security includes secure configuration, supported operating systems, prompt patching, endpoint protection, application control where appropriate, restricted administrator privileges, disk encryption and secure disposal. Organisations should maintain an inventory so that unsupported or unmanaged devices do not become invisible weaknesses.

Patching is a risk-management process rather than a mechanical update task. Critical internet-facing vulnerabilities may require urgent action, while other changes may need testing to avoid operational disruption. SMEs need ownership, priorities and evidence that important updates have actually been applied.

## Key Learning Points

- Relate the concepts to a real SME or workplace process.
- Identify at least one preventive, one detective and one recovery control.
- Record one example of how human behaviour and organisational process affect the technical risk.

## Practical Activity

Apply the concepts to the fictional company 'Northstar SME', a 25-person organisation using cloud email, laptops, a public website, online banking, shared cloud storage and an outsourced IT provider. Record the relevant assets, risks, controls and improvement actions for this chapter.

# 7. Identity, Passwords, MFA and Access Control

Identity is a primary security boundary in cloud-based work. If an attacker obtains valid credentials, malicious activity may look like legitimate use. Strong identity security therefore combines unique accounts, secure authentication, multi-factor authentication, controlled privileges, monitoring and timely removal of access.

Password security is improved by using long, unique passwords or passphrases and a reputable password manager. Reusing passwords across services creates credential-stuffing risk: compromise of one service can lead to compromise of another. Default passwords should be changed immediately.

Multi-factor authentication requires more than one factor, such as something the user knows, has or is. MFA substantially reduces risk from stolen passwords, although not every MFA method provides the same resistance to phishing. Organisations should enable the strongest practical methods supported by their services and prioritise administrator, email, financial and remote-access accounts.

Least privilege means users and systems receive only the access needed for their role. Administrative privileges should be separated from routine work where feasible. Joiner-mover-leaver processes are essential: access should be created deliberately, adjusted when roles change and removed promptly when people leave.

### Key Learning Points

- Relate the concepts to a real SME or workplace process.
- Identify at least one preventive, one detective and one recovery control.
- Record one example of how human behaviour and organisational process affect the technical risk.

### Practical Activity

Apply the concepts to the fictional company 'Northstar SME', a 25-person organisation using cloud email, laptops, a public website, online banking, shared cloud storage and an outsourced IT provider. Record the relevant assets, risks, controls and improvement actions for this chapter.

## 8. Network, Wi-Fi and Remote-Work Security

A network connects devices and services and therefore creates pathways that defenders must control. Basic network-security concepts include addressing, routing, ports, protocols, firewalls, segmentation and secure remote access. Learners do not need to become network engineers to understand that unnecessary exposure increases attack surface.

A firewall controls network traffic according to defined rules. It is not a guarantee of security: permitted services can still contain vulnerabilities and users can still be deceived. Firewalls work best as one layer in a defence-in-depth strategy.

Network segmentation separates systems so that compromise of one area does not automatically provide access to everything else. Even a small business can benefit from separating guest Wi-Fi from internal devices and isolating sensitive or operational systems where practical.

Remote work extends the security boundary into homes, travel environments and personal networks. Organisations should use managed devices where possible, secure remote-access methods, MFA, encrypted connections, device-locking, patching and clear procedures for lost devices. Public Wi-Fi should be treated as untrusted.

### Key Learning Points

- Relate the concepts to a real SME or workplace process.
- Identify at least one preventive, one detective and one recovery control.
- Record one example of how human behaviour and organisational process affect the technical risk.

### Practical Activity

Apply the concepts to the fictional company 'Northstar SME', a 25-person organisation using cloud email, laptops, a public website, online banking, shared cloud storage and an outsourced IT provider. Record the relevant assets, risks, controls and improvement actions for this chapter.

# 9. Data Protection, Encryption and Information Handling

Security controls should reflect the value and sensitivity of information. A simple classification model might distinguish public, internal, confidential and highly restricted information. Classification helps determine who may access information, where it may be stored, whether it may be shared externally and what protection is required.

Encryption protects information by transforming it so that it cannot be read without the appropriate key. Encryption at rest protects stored data; encryption in transit protects data moving across networks. Encryption reduces risk but does not solve every problem: an authorised but compromised account may still access decrypted information.

Data minimisation reduces both privacy and cybersecurity exposure. Organisations should avoid collecting or retaining information without a clear need. Sensitive information should not be copied into unmanaged services, personal accounts or unapproved AI tools.

Secure deletion and retention matter because forgotten copies remain an attack target. Backup archives, exported spreadsheets, old shared folders and former employee accounts can preserve sensitive data long after the original business purpose has ended.

## Key Learning Points

- Relate the concepts to a real SME or workplace process.
- Identify at least one preventive, one detective and one recovery control.
- Record one example of how human behaviour and organisational process affect the technical risk.

## Practical Activity

Apply the concepts to the fictional company 'Northstar SME', a 25-person organisation using cloud email, laptops, a public website, online banking, shared cloud storage and an outsourced IT provider. Record the relevant assets, risks, controls and improvement actions for this chapter.

# 10. Backups, Business Continuity and Cyber Resilience

Cybersecurity is not only about preventing incidents. Resilience is the ability to continue or restore critical operations when prevention fails. Business continuity identifies essential services, dependencies, acceptable downtime and alternative ways of working. Disaster recovery focuses on restoring technology and data.

The 3-2-1 backup principle is a useful baseline: maintain at least three copies of important data, on two different types of storage, with one copy off-site or otherwise isolated. Modern ransomware risk makes immutability, offline protection and restricted backup administration particularly valuable.

A backup is useful only if it can be restored. Organisations should test recovery, document recovery steps and know how long restoration takes. Recovery Time Objective (RTO) expresses how quickly a service should be restored; Recovery Point Objective (RPO) expresses how much recent data loss may be tolerable.

Continuity planning should include people and suppliers, not only servers. If the only person who knows the recovery process is unavailable, the plan is fragile. Contact lists, escalation routes, alternative communication channels and supplier responsibilities should be documented.

### Key Learning Points

- Relate the concepts to a real SME or workplace process.
- Identify at least one preventive, one detective and one recovery control.
- Record one example of how human behaviour and organisational process affect the technical risk.

### Practical Activity

Apply the concepts to the fictional company 'Northstar SME', a 25-person organisation using cloud email, laptops, a public website, online banking, shared cloud storage and an outsourced IT provider. Record the relevant assets, risks, controls and improvement actions for this chapter.

## 11. Cloud Security and Shared Responsibility

Cloud services can improve security by providing professionally managed infrastructure, but moving to the cloud does not transfer all responsibility to the provider. The customer remains responsible for areas such as identities, permissions, data handling, configuration and appropriate use, depending on the service model.

Software as a Service (SaaS) gives users an application managed largely by the provider. Platform as a Service (PaaS) provides a managed application platform. Infrastructure as a Service (IaaS) gives the customer more control over virtual infrastructure and therefore more security responsibility. The exact division varies by provider and service.

Common cloud risks include weak administrator accounts, excessive permissions, exposed storage, insecure sharing links, lack of logging, unmanaged third-party integrations and incomplete offboarding. Cloud security therefore depends heavily on identity and configuration management.

SMEs should maintain an inventory of cloud services and owners, review administrator roles, enable MFA, restrict external sharing, configure logging where available, and understand backup/export options. Business continuity should consider what happens if a cloud service or account becomes unavailable.

### Key Learning Points

- Relate the concepts to a real SME or workplace process.
- Identify at least one preventive, one detective and one recovery control.
- Record one example of how human behaviour and organisational process affect the technical risk.

### Practical Activity

Apply the concepts to the fictional company 'Northstar SME', a 25-person organisation using cloud email, laptops, a public website, online banking, shared cloud storage and an outsourced IT provider. Record the relevant assets, risks, controls and improvement actions for this chapter.

## 12. Vulnerability Management and Secure Configuration

Vulnerability management is the continuous process of identifying, evaluating, prioritising and addressing weaknesses. Vulnerabilities may exist in software, firmware, configuration, identity settings, processes or third-party components. A scanner can help identify technical weaknesses but does not replace risk analysis.

Prioritisation should consider more than a severity score. Important factors include whether the system is internet-facing, whether exploitation is known, the value of the affected asset, available mitigations and business impact. A critical weakness on an isolated test machine may be less urgent than an actively exploited weakness on a public service.

Secure configuration reduces unnecessary functionality and exposure. Examples include disabling unused accounts and services, changing defaults, restricting macros, limiting external sharing, enforcing screen locks and applying baseline settings consistently. Configuration drift should be reviewed over time.

Asset inventory is the prerequisite. An organisation cannot reliably patch, monitor or retire devices and software that it does not know it owns. The inventory should identify owner, purpose, criticality, support status and relevant dependencies.

### Key Learning Points

- Relate the concepts to a real SME or workplace process.
- Identify at least one preventive, one detective and one recovery control.
- Record one example of how human behaviour and organisational process affect the technical risk.

### Practical Activity

Apply the concepts to the fictional company 'Northstar SME', a 25-person organisation using cloud email, laptops, a public website, online banking, shared cloud storage and an outsourced IT provider. Record the relevant assets, risks, controls and improvement actions for this chapter.

## 13. Cybersecurity Risk Assessment and NIST CSF 2.0

Risk assessment translates technical concerns into business priorities. A simple approach identifies assets and processes, describes plausible threat scenarios, records vulnerabilities and existing controls, estimates likelihood and impact, and decides how to treat the risk. Treatment options include reducing, avoiding, transferring or accepting risk.

NIST CSF 2.0 provides a common language for cybersecurity outcomes. Govern establishes organisational context, strategy, roles, policy and oversight. Identify covers assets, risks and improvement opportunities. Protect focuses on safeguards. Detect concerns discovering and analysing adverse events. Respond addresses incident management and communication. Recover focuses on restoration and resilience.

The functions are not a chronological checklist. Governance influences every other function, and learning from incidents feeds back into risk decisions. An SME can use the framework without implementing every possible control: the objective is to define a current profile, desired target outcomes and prioritised actions.

Risk registers should be living documents. Each meaningful risk should have an owner, treatment decision, target date and status. Residual risk is the risk remaining after controls are applied. Management needs to understand and accept significant residual risk rather than assuming that the IT provider has eliminated it.

### Key Learning Points

- Relate the concepts to a real SME or workplace process.
- Identify at least one preventive, one detective and one recovery control.
- Record one example of how human behaviour and organisational process affect the technical risk.

### Practical Activity
Apply the concepts to the fictional company 'Northstar SME', a 25-person organisation using cloud email, laptops, a public website, online banking, shared cloud storage and an outsourced IT provider. Record the relevant assets, risks, controls and improvement actions for this chapter.

## 14. Security Monitoring, Logging and Detection
Detection reduces the time between compromise and response. Useful security logs may come from identity systems, endpoints, firewalls, cloud services, email platforms and critical applications. Logging without review creates little value, while excessive logging without priorities can overwhelm a small team.

SMEs should identify high-value events: repeated failed logins, impossible travel, new administrator accounts, disabled security controls, unusual data downloads, unexpected forwarding rules, malware alerts and changes to critical configurations. Managed security services may help where internal monitoring capacity is limited.

An alert is not the same as an incident. Alerts require triage: what happened, which asset or account is involved, whether the activity is expected, what evidence exists and what immediate containment may be required. Maintaining accurate time settings and retaining relevant logs supports investigation.

Detection engineering should evolve from incidents and near misses. If an organisation discovers that a specific event would have revealed an attack earlier, it should consider adding or improving monitoring for that event.

### Key Learning Points
- Relate the concepts to a real SME or workplace process.
- Identify at least one preventive, one detective and one recovery control.
- Record one example of how human behaviour and organisational process affect the technical risk.

### Practical Activity
Apply the concepts to the fictional company 'Northstar SME', a 25-person organisation using cloud email, laptops, a public website, online banking, shared cloud storage and an outsourced IT provider. Record the relevant assets, risks, controls and improvement actions for this chapter.

## 15. Incident Response and Reporting
An incident is an event that compromises or threatens the confidentiality, integrity or availability of information or systems, or otherwise violates security policy. Incident response aims to limit harm, preserve evidence, restore operations and learn from what happened.

A practical lifecycle includes preparation; detection and analysis; containment; eradication; recovery; and post-incident improvement. In reality, these stages overlap. For example, recovery may begin for one service while investigation continues elsewhere.

The first response should avoid destroying evidence or making the situation worse. Employees need a simple reporting route and should know whom to contact. Organisations should record times, affected accounts or devices, observed symptoms, actions taken and people involved.

Communication is part of incident response. Depending on the event and jurisdiction, organisations may need to involve customers, insurers, data-protection authorities, sector regulators, law enforcement or national cyber authorities. Legal notification requirements should be determined with appropriate professional advice.

Post-incident review should focus on improvement rather than blame. Ask how the incident entered, why it was not prevented or detected earlier, which controls worked, what slowed response, and what changes are required.

### Key Learning Points

- Relate the concepts to a real SME or workplace process.
- Identify at least one preventive, one detective and one recovery control.
- Record one example of how human behaviour and organisational process affect the technical risk.

### Practical Activity

Apply the concepts to the fictional company 'Northstar SME', a 25-person organisation using cloud email, laptops, a public website, online banking, shared cloud storage and an outsourced IT provider. Record the relevant assets, risks, controls and improvement actions for this chapter.

## 16. Supply-Chain and Third-Party Cybersecurity

SMEs depend on software vendors, cloud providers, accountants, payment services, managed IT providers and other suppliers. A supplier with privileged access or sensitive data can become part of the organisation's attack surface. Cybersecurity therefore extends beyond direct technical control.

Third-party risk assessment should be proportionate. Critical suppliers deserve more scrutiny than low-impact services. Questions may cover MFA, breach notification, backups, data location, subcontractors, security certifications, access controls, vulnerability management and exit arrangements.

Contracts can support cybersecurity by defining responsibilities, incident notification, data handling, service continuity and return or deletion of information. However, contractual wording does not replace operational verification.

Concentration risk occurs when many critical functions depend on one provider or platform. Organisations should understand alternatives, export capabilities and recovery options before a crisis occurs.

### Key Learning Points

- Relate the concepts to a real SME or workplace process.
- Identify at least one preventive, one detective and one recovery control.
- Record one example of how human behaviour and organisational process affect the technical risk.

### Practical Activity

Apply the concepts to the fictional company 'Northstar SME', a 25-person organisation using cloud email, laptops, a public website, online banking, shared cloud storage and an outsourced IT provider. Record the relevant assets, risks, controls and improvement actions for this chapter.

# 17. AI-Enabled Cyber Threats and Security of AI Use

Generative AI can assist defenders with summarisation, awareness content, analysis and documentation, but it can also help attackers scale social engineering, translate fraudulent messages, generate convincing pretexts and accelerate reconnaissance. The key change is often scale and accessibility rather than the invention of entirely new attack categories.

Employees should treat AI-generated voice, images and text as potentially synthetic. Sensitive actions such as payment changes, password resets or disclosure of confidential information should use independent verification procedures rather than relying on apparent familiarity.

Using AI tools also creates security risks: confidential data leakage, unapproved integrations, insecure generated code, malicious prompt injection and excessive agent permissions. AI security therefore intersects with identity, data governance, software security and supplier management.

When AI is connected to tools or organisational data, least privilege and human approval become especially important. A system that can read documents poses different risk from one that can also send messages, change records or execute transactions.

## Key Learning Points

- Relate the concepts to a real SME or workplace process.
- Identify at least one preventive, one detective and one recovery control.
- Record one example of how human behaviour and organisational process affect the technical risk.

## Practical Activity

Apply the concepts to the fictional company 'Northstar SME', a 25-person organisation using cloud email, laptops, a public website, online banking, shared cloud storage and an outsourced IT provider. Record the relevant assets, risks, controls and improvement actions for this chapter.

# 18. European Cybersecurity Context and Career Development

The European Cybersecurity Skills Framework provides a common language for cybersecurity professional roles, tasks, skills, knowledge and competences. It can help learners understand how foundational skills connect to professional pathways and helps training providers relate learning outcomes to workplace roles.

NIS2 establishes a common EU framework for cybersecurity across a broad set of critical sectors and introduces risk-management and incident-reporting requirements for entities within scope. Not every SME falls within scope, and applicability depends on sector, size, role and national implementation. Learners should therefore treat NIS2 as an important governance context rather than assume that every organisation has identical legal duties.

Cybersecurity careers are diverse. Technical paths include incident response, security operations, penetration testing, architecture and digital forensics. Other roles emphasise governance, risk, compliance, awareness, project management or security leadership. Foundational cybersecurity literacy is also increasingly valuable in ordinary IT, management, finance, HR and operations roles.

Professional development should combine theory with evidence of practice. A learner portfolio can include risk assessments, incident playbooks, asset inventories, security-awareness materials, backup plans and documented labs. These artefacts demonstrate applied competence while remaining safe and defensive.

### Key Learning Points

- Relate the concepts to a real SME or workplace process.
- Identify at least one preventive, one detective and one recovery control.
- Record one example of how human behaviour and organisational process affect the technical risk.

### Practical Activity

Apply the concepts to the fictional company 'Northstar SME', a 25-person organisation using cloud email, laptops, a public website, online banking, shared cloud storage and an outsourced IT provider. Record the relevant assets, risks, controls and improvement actions for this chapter.

## 19. Practical Lab Series

| Lab | Activity | Evidence |
|---|---|---|
| Lab 1 – Asset Inventory | Create an inventory of 15–20 assets for a fictional SME; assign owner, criticality and support status. | Asset register |
| Lab 2 – Phishing Triage | Review fictional emails for sender anomalies, urgency, link risk, attachment risk and verification needs. | Phishing analysis sheet |
| Lab 3 – Identity Hardening | Audit fictional account settings for MFA, privilege, shared accounts and offboarding. | Identity checklist |
| Lab 4 – Secure Wi-Fi & Remote Work | Design a small-office network separating internal and guest access; define remote-work rules. | Network sketch + rules |
| Lab 5 – Backup & Recovery | Design a 3-2-1 backup approach and a restore-test schedule. | Backup plan |
| Lab 6 – Risk Register | Score ten fictional risks using likelihood × impact and propose treatments. | Risk register |
| Lab 7 – Incident Tabletop | Respond to a fictional compromised email account and suspicious payment request. | Incident timeline + decisions |
| Lab 8 – Cloud Security Review | Review a fictional cloud tenant for external sharing, MFA, admin accounts and logging. | Cloud review checklist |
| Lab 9 – Supplier Risk | Assess an outsourced IT provider and SaaS supplier using a proportionate questionnaire. | Supplier assessment |
| Lab 10 – Capstone | Prepare a cybersecurity improvement plan for a small organisation. | Portfolio + presentation |

## 20. Safe Practice Exercises

These exercises require no attack against real systems. Use fictional data, local documents, screenshots, diagrams or authorised training environments.

1. Create a phishing-reporting checklist that a non-technical employee can follow in under two minutes.
2. Draft a password and MFA policy for a 20-person SME.
3. Create an employee offboarding checklist covering accounts, devices, shared secrets and cloud access.
4. Design a simple data-classification table with Public, Internal, Confidential and Restricted categories.
5. Prepare a monthly patch-management checklist.

6. Create a quarterly restore-test record for critical backups.
7. Draft an incident contact tree and escalation matrix.
8. Map one business process to NIST CSF 2.0 functions.
9. Create a one-page remote-work security guide.
10. Prepare five cybersecurity questions to ask a critical SaaS supplier.

# 21. SME Case Studies

## Case 1 – Invoice Fraud

A finance employee receives a realistic message from a supplier asking to change bank details. The sender name is familiar, but the domain contains a subtle spelling difference.

**Task:** Design the verification and escalation procedure. Identify which control could prevent payment loss.

## Case 2 – Ransomware Morning

Several employees report that shared files cannot be opened and one laptop displays an extortion message.

**Task:** Identify immediate containment priorities, communication needs, evidence to preserve and recovery dependencies.

## Case 3 – Lost Laptop

A manager loses a company laptop during travel. It contains synced business documents and active browser sessions.

**Task:** Identify controls that reduce impact before loss and actions required after loss.

## Case 4 – Departing Administrator

An outsourced technician with administrator access ends the contract.

**Task:** Prepare the access-removal and credential-rotation checklist.

## Case 5 – Cloud Sharing

A confidential spreadsheet is accidentally shared through a public link.

**Task:** Identify containment, investigation, notification and prevention steps.

## Case 6 – AI-Assisted Impersonation

A manager receives a voice message that appears to come from the CEO requesting an urgent payment.

**Task:** Design a verification procedure that remains effective even when audio or video appears authentic.

# 22. Cybersecurity Risk Assessment Template

| Field | Guidance |
|---|---|
| Asset / Process | What business resource is at risk? |
| Threat scenario | What could happen and who/what could cause it? |
| Vulnerability | What weakness enables the scenario? |
| Existing controls | What currently reduces likelihood or impact? |
| Likelihood | 1 Rare – 5 Almost certain |

| | |
|---|---|
| Impact | 1 Minor – 5 Severe |
| Risk score | Likelihood × Impact |
| Treatment | Reduce / Avoid / Transfer / Accept |
| Owner | Who is accountable for action? |
| Target date | When should treatment be completed? |
| Residual risk | What remains after treatment? |

## 23. Incident Response Mini-Playbook

11. Recognise and report: capture what was observed, by whom and when.
12. Triage: identify affected accounts, devices, services and business processes.
13. Contain: isolate affected assets or revoke access where authorised and appropriate.
14. Preserve evidence: avoid unnecessary deletion or reinstallation before required evidence is secured.
15. Escalate: involve responsible management, IT/security, legal/privacy and external providers as appropriate.
16. Eradicate: remove malicious persistence, reset compromised credentials and correct exploited weaknesses.
17. Recover: restore from trusted sources, monitor closely and confirm business functionality.
18. Communicate: use approved channels and meet applicable contractual or legal notification duties.
19. Learn: conduct a post-incident review and update controls, procedures and training.

## 24. Capstone Project – SME Cybersecurity Improvement Plan

Select a real organisation for which you have permission to work, or use a fictional SME. Produce a practical improvement plan that management could understand and act upon.

### Required Deliverables

20. Organisation profile and critical business processes.
21. Asset inventory with at least 15 assets.
22. Top ten cybersecurity risks and risk register.
23. Current-control assessment mapped to Govern, Identify, Protect, Detect, Respond and Recover.
24. Priority improvement plan: immediate (0–30 days), short term (1–3 months), medium term (3–12 months).
25. Identity and MFA improvement actions.
26. Backup and recovery plan.
27. Incident-response mini-playbook.
28. Supplier/cloud-security review.
29. Employee-awareness action.
30. One-page management summary with five priority decisions.

### Capstone Assessment Rubric

| **Criterion** | **Weight** |
|---|---|
| Asset and business understanding | 15% |
| Risk identification and prioritisation | 20% |
| Technical and organisational controls | 20% |
| Incident response and resilience | 15% |
| Identity, data, cloud and supplier security | 15% |
| Feasibility for an SME | 10% |

| | |
|---|---|
| Clarity and evidence | 5% |

## 25. Final Knowledge Assessment

1. What is a vulnerability?

2. Which three objectives form the CIA triad?

3. Why is MFA important?

4. What does least privilege mean?

5. Why is a backup not enough by itself?

6. What is phishing?

7. What is residual risk?

8. What is the purpose of segmentation?

9. What are the six NIST CSF 2.0 functions?

10. What should happen after a significant incident?

11. Why are suppliers part of cybersecurity risk?

12. What is prompt injection in an AI-security context?

### Answer Key

1. A weakness that can be exploited by a threat.

2. Confidentiality, Integrity and Availability.

3. It reduces reliance on a password as the only authentication factor.

4. Granting only the access required for a role or task.

5. It must be protected and tested for successful restoration.

6. Social engineering using deceptive communications to influence a target.

7. Risk remaining after controls are applied.

8. To limit unnecessary connectivity and reduce lateral movement/impact.

9. Govern, Identify, Protect, Detect, Respond, Recover.

10. Recovery plus a post-incident review and improvement actions.

11. They may hold data, provide critical services or possess privileged access.

12. Untrusted instructions intended to manipulate an AI system's behaviour.

## 26. Post-Training Skills Check and Reflection

Repeat the Initial Skills Check and compare results. Use practical evidence—not only self-confidence—to judge progress.

- Which three security controls would you implement first in a small organisation and why?
- Which business process would create the greatest impact if unavailable for three days?
- Which incident would your current organisation find hardest to detect?
- Which account or identity would cause the greatest harm if compromised?
- What is the most important improvement you would make to backup and recovery?
- What further cybersecurity role or learning pathway interests you?

## 27. Career Transition Guide

| Starting profile | Possible direction | Portfolio evidence |
|---|---|---|
| General employee / administration | Cybersecurity-aware business professional | Awareness guide; phishing checklist; data-classification exercise |
| IT support | Cybersecurity Support Technician | Asset inventory; hardening checklist; incident playbook |
| Junior technical learner | Junior Security Analyst | Risk register; alert triage exercises; incident tabletop |
| SME manager | SME Cybersecurity Coordinator | CSF-based improvement plan; supplier assessment; policy set |
| Compliance / quality staff | Cyber risk & governance pathway | Risk assessment; control mapping; governance documentation |
| Career changer | Entry-level cybersecurity pathway | DT-02 portfolio plus further networking, operating-system and security-operations study |

## 28. Glossary

| Term | Definition |
|---|---|
| Asset | Anything of value to an organisation that requires protection. |
| Threat | A potential cause of an unwanted cybersecurity event. |
| Vulnerability | A weakness that can be exploited. |
| Risk | Potential adverse effect arising from uncertainty, commonly considered through likelihood and impact. |
| Control | A safeguard that modifies risk. |
| CIA Triad | Confidentiality, Integrity and Availability. |
| Attack Surface | The collection of points through which an attacker might attempt access or influence. |
| Phishing | Deceptive communication intended to manipulate a recipient. |
| BEC | Business Email Compromise; fraud involving compromised or impersonated business communications. |
| Malware | Software designed for malicious purposes. |
| Ransomware | Malware or related extortion activity that disrupts access to systems/data, often combined with data theft. |
| MFA | Multi-Factor Authentication. |
| Least Privilege | Providing only the access required for legitimate duties. |
| Patch | An update intended to correct software defects or vulnerabilities. |

| | |
|---|---|
| Firewall | A control that permits or blocks network traffic according to rules. |
| Segmentation | Separating networks or systems to limit access and propagation. |
| Encryption | Cryptographic protection of information against unauthorised reading. |
| RTO | Recovery Time Objective. |
| RPO | Recovery Point Objective. |
| Incident | An event that compromises or threatens security or violates security policy. |
| Containment | Actions to limit the spread or impact of an incident. |
| Residual Risk | Risk remaining after controls are applied. |
| NIST CSF 2.0 | A cybersecurity risk-management framework organised around six functions. |
| ECSF | European Cybersecurity Skills Framework. |
| NIS2 | EU Directive 2022/2555 on measures for a high common level of cybersecurity across the Union. |
| Prompt Injection | Manipulative instructions embedded in untrusted content to influence an AI system. |

## 29. Curated Learning Resources

**NIST Cybersecurity Framework 2.0**
https://www.nist.gov/cyberframework
Primary framework for organisational cybersecurity risk management.

**NIST CSF 2.0 Quick-Start Guides**
https://www.nist.gov/cyberframework/quick-start-guides
Includes guidance for small businesses and other implementation contexts.

**ENISA – European Cybersecurity Skills Framework (ECSF)**
https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf
European role and competence framework for cybersecurity careers and training.

**ENISA – ECSF Role Profiles**
https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles
Twelve professional role profiles with missions, tasks, skills and knowledge.

**ENISA – ECSF Video Hub**
https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/ecsf-video-hub
Short videos and webinars explaining the framework and cyber skills.

**European Commission – NIS2 Directive**
https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
Official EU overview of the NIS2 cybersecurity framework.

**CISA – Secure Our World**
https://www.cisa.gov/secure-our-world
Practical cybersecurity awareness resources for individuals and organisations.

**CISA – Cyber Guidance for Small Businesses**
https://www.cisa.gov/audiences/small-and-medium-businesses
Practical resources oriented to small and medium-sized businesses.

**Cisco Networking Academy / Skills for All**
https://skillsforall.com/
Introductory networking and cybersecurity learning; course availability and credentials should be checked on the current site.

**Microsoft Learn – Security learning**
https://learn.microsoft.com/training/browse/?products=security
Modular security learning; filter by role and level.

**TryHackMe**
https://tryhackme.com/
Optional hands-on learning environment. Use only authorised platform labs and follow platform rules.

**OWASP**
https://owasp.org/
Open resources on application security; useful as a next-step resource after foundational DT-02 learning.

## 30. Suggested 40–60 Hour Delivery Plan

| Component | Indicative hours |
|---|---|
| Orientation and initial skills check | 2 |
| Cybersecurity foundations and threat landscape | 6 |
| Phishing, malware and endpoint security | 7 |
| Identity, network and remote-work security | 7 |
| Data, backup, cloud and vulnerability management | 8 |
| Risk assessment and NIST CSF 2.0 | 6 |
| Monitoring and incident response | 6 |
| Supply chain, AI-related risk and EU context | 4 |
| Labs and case studies | 6 |
| Capstone, assessment and reflection | 8 |
| Total | 60 hours; compressible to approximately 40 hours by reducing guided practice |

## 31. Trainer / Facilitator Notes

- Keep all exercises defensive and use fictional, local or explicitly authorised environments.
- Use SME examples and avoid assuming enterprise-level budgets or staffing.
- Assess the learner's reasoning and evidence, not only terminology.
- Ask learners to connect each technical control to a business risk.
- Use incidents and near misses as learning scenarios without encouraging blame.
- Update legal and threat examples before delivery; distinguish general training from legal advice.
- Encourage a portfolio containing the asset register, risk register, incident playbook and capstone plan.

## 32. References

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29.

National Institute of Standards and Technology. (2024). NIST Cybersecurity Framework 2.0: Resource and Overview Guide (SP 1299).

European Union Agency for Cybersecurity (ENISA). (2022). European Cybersecurity Skills Framework (ECSF): User Manual.

European Union Agency for Cybersecurity (ENISA). (2022). European Cybersecurity Skills Framework Role Profiles.

European Union Agency for Cybersecurity (ENISA). (2025). Cybersecurity roles and skills for NIS2 Essential and Important Entities.

European Union. (2022). Directive (EU) 2022/2555 (NIS2 Directive).

Cybersecurity and Infrastructure Security Agency (CISA). Secure Our World and Small/Medium Business cybersecurity resources.

OWASP Foundation. Open Web Application Security Project resources.

## 33. Website Publishing Structure

For ReskillingLab, publish DT-02 as modular learning content. Each unit should use the same visible structure: Learn | Practice | Check Your Understanding | Resources.

- Overview & Initial Skills Check
- Cybersecurity Foundations
- Threat Landscape
- Phishing & Social Engineering
- Malware & Endpoint Security
- Identity & Access
- Network & Remote Work
- Data & Encryption
- Backup & Resilience
- Cloud Security
- Vulnerability Management
- Risk & NIST CSF 2.0
- Monitoring & Detection
- Incident Response
- Supply Chain
- AI-Enabled Cyber Risks
- European Context & Careers
- Labs & Cases
- Capstone
- Assessment
- Resources & Glossary