skillcast

Cybersecurity Toolkit

About Cybersecurity

Cybersecurity threats such as phishing, ransomware, and social engineering continue to put organisations at risk. Employees play a critical role in protecting systems and information, which is why training is essential. They need to understand how to recognise and respond to threats, follow internal policies and procedures, and report incidents quickly and correctly.

Failing to address these risks can result in financial loss, operational disruption, and serious reputational damage. Beyond technology and controls, an informed and vigilant workforce is your strongest defence.

This toolkit provides resources to support your cybersecurity compliance and resilience efforts.

Did you know...

95% of cyber incidents involve human error, and half of UK organisations suffered an attack in 2024

Contents

Why Cybersecurity Matters

Understanding cybersecurity is essential for every organisation. It is not merely a technical requirement - it is a critical framework for safeguarding information, ensuring business continuity, and building trust with stakeholders.

Strong cybersecurity practices help mitigate risks of attacks and breaches, protect sensitive data, and enhance your organisation's resilience and reputation. By recognising and implementing effective cybersecurity measures, your organisation can:

- **Protect Information Assets:** Safeguard data, systems, and networks from unauthorised access and misuse.
- **Build Trust:** Demonstrate to customers, partners, and stakeholders that security is a top priority.
- **Reduce Risk:** Minimise financial, operational, and reputational damage caused by cyber incidents.
- **Promote Best Practices:** Embed secure behaviours and procedures across the organisation.
- **Enable Business Growth:** Operate with confidence in an increasingly digital and interconnected world.

Understanding the significance of cybersecurity equips your organisation to remain compliant, protect its reputation, and maintain the trust of those you serve.

Cybersecurity Desk Aid

Staff Checklist

Always report issues promptly to IT, including unauthorised access attempts or malware, suspected data breaches, accidentally sharing sensitive information, and lost or stolen devices.

Don't hesitate to ask your IT department or security team for help if you're unsure.

1. **Create strong, unique passwords.** Mix lower and uppercase letters, numbers, and symbols. Avoid dictionary words and personal information, and do not reuse passwords.

2. **Enable multi-factor authentication (MFA).** This adds an extra layer of login security, requiring a code beyond your password.

3. **Never share your logins.** This includes usernames, passwords, and security codes.

4. **Keep work devices secure.** Use strong passwords for screen locks, encrypt sensitive data, and update software regularly.

5. **Don't mix personal and work use.** Avoid accessing personal accounts and do not download unauthorised software on work devices.

6. **Take care when accessing public.** Where possible, use a VPN for added security when connecting to public Wi-Fi networks.

7. **Think before you download.** Only download files from trusted sources. Be cautious of attachments, especially from unknown or unfamiliar senders.

8. **Beware of social engineering.** Don't share confidential or personal information in response to unsolicited calls, emails, or messages. It is a common technique used by fraudsters.

9. **Beware of phishing attempts.** Don't click on suspicious links or attachments in emails or messages. Be sceptical about links in branded emails. Always verify senders before responding.

10. **Understand and follow data-sharing rules.** Follow company policies on data handling, and don't share sensitive information without authorisation.

Training Aid

Email Phishing Checklist

There are no fool-proof methods to prevent phishing. But you can reduce the risk by installing anti-phishing tools and making your employees aware of the risks.

Workplace malware protection tools may not always succeed. That's why it is important to try and avoid the risks by following a few simple guidelines.

1. **Keep your software up-to-date!** Ensure that you keep the software updated and mitigate the consequences of any mistake you might make
2. **Be sceptical about links in branded emails.** If you receive an email from a recognised brand, be sceptical if it asks you to click a link, provide your personal information or passwords.
3. **Avoid oversharing personal information on social media.** Avoid sharing your position, job title, location, company and even age on social media.
4. **Train yourself to recognise personal styles.** Make yourself familiar with how colleagues and suppliers communicate with you.
5. **Notify your IT team of suspicious emails.** If you are suspicious of an email, then forward it to your IT team.
6. **Be wary of requests from generic addresses.** If you receive an email from a generic address, e.g., customerservice@, help@, hr@ itsupport@, or payroll@, always be suspicious.
7. **Know the red flags.** Be wary of generic greetings, unusual sender information, poor formatting, spelling/grammar mistakes, dire warnings, incorrect facts, financial rewards or penalties and a lack of legally required links to subscribe.
8. **Trust your instincts.** If it sounds too good to be true, it usually is. If it sounds too bad, it also usually is. Cybercriminals are experts at making up extreme scenarios.

Cybersecurity tips

Preventing a cyber attack

Carrot, stick – and training
Carrot: Rewards people for getting it right.
Stick: Penalties for those who get it wrong (anything from poor practices to negligence).
Training: Introduce courses on common threats and how to look out for them.

- Dr John Kingston, cybersecurity expert, shares his tips for avoiding a cyber attack

Businesses should already be implementing intrusion detection systems, firewalls and other security measures to protect against technical risks. There are also several other ways organisations can reduce the risk:

- **Penetration Testing**
  Carry out controlled attacks on your own systems to uncover weaknesses before cybercriminals do. This proactive approach highlights vulnerabilities and helps strengthen overall security

- **Self-Phishing Exercises.**
  Send simulated phishing emails to staff. Anyone who clicks receives immediate feedback, turning mistakes into teachable moments. Regular exercises help employees recognise real threats and respond correctly.

- **Two-Factor Authentication (2FA)**
  Strengthen logins by adding a second layer of protection. Avoid SMS codes, which are vulnerable to interception. Instead, use secure methods such as authenticator apps or encrypted platforms like WhatsApp.

- **Clear Security Policies**
  Document clear prevention policies and assign responsibility for ensuring they're followed. A well-structured policy, backed by accountability, builds stronger habits across the organisation.

- **Password Testing & Passphrases**
  Run password cracking tools internally to reveal weak choices. Many employees still rely on predictable patterns. Encourage the use of passphrases (a string of random words), which are far harder to break and easier to remember.

Cybersecurity tips

Expert FAQs

Real questions from our recent cyber seminar, answered by our experts:

Q: ChatGPT is used a lot by our staff. How safe is this?
A: Most people have come to rely on AI for some reason or another, it's a useful tool, however, it is not recommended entering personal or sensitive/confidential information into any third-party services such as ChatGPT etc. If you must, then use the Enterprise version. Data inserted to tools like ChatGPT is not private. It must be stored somewhere and with OpenAI, in this case, it is primarily the US. Your organisation should conduct its own risk review and consider any relevant legal or regulatory requirements e.g. GDPR. You are responsible for the security of that data and by using tools such as ChatGPT you are assuming/trusting that OpenAI has the necessary controls in place to protect that data.

How secure is your data:

- It depends on what type of account you are using (free or not).
- OpenAI have stated that data is encrypted at rest and in transit.
- If chat history is enabled, conversations are stored longer and may be used to model training of the AI.
- It is your responsibility to turn off "Chat History & Training" in settings, if you don't want conversations being used for model improvements.
- If chat history is disabled, conversations are stored for about 30 days for security and abuse monitoring and then deleted.
- Authorised personal within OpenAI can access stored data (conversation history) which is done so in accordance with their internal procedures.
- No third-parties have direct access unless you connect via an external plugin or API, which then you are trusting the security another third-party as well.

Q. Are there any stats on the likely proportion of companies that pay ransomware attackers to protect their data vs those that don't?
A: There is no overarching stats on the likely proportion of companies that pay the ransom. Some organisations do have their own statistics, but this is based on their experiences and their client base. It is highly likely that organisations do not want to admit they paid a ransom because it would have an impact on the organisation (financial/ reputation). You will see that most governments around the globe are trying to make it mandatory for certain organisations such as public sector to report if they pay a ransom.

Cybersecurity tips

Expert FAQs

Q. Is using a password manager a risk? Is it safer to rely on it or will it just make it easier for attackers to access all passwords in one place?
A: With or without a password manager there is always a risk. Using a password manager is less of a risk. We should be employing good password hygiene which includes using different passwords across different platforms. Without a password manager it makes it harder for humans to remember these passwords unless you are using a similar passwords or a weak passwords. By using a password manager, you are trusting that the password manager is secure and regularly updated as necessary but by remembering just one secure password is far easier than remembering multiple. This can be improved with the use of MFA.

It should also be highlighted; password managers will be target for threat actors so make sure you keep the password to it and the backend database secure.

Q. How robust is the cyber essentials certification, is it a good foundation to support cyber security?
A: Cyber essentials is a good fundamental certification to have in place for your organisation and is required in some industries, however, it shouldn't be the only controls in place. Security by compliance isn't great, but it's a start. Organisations should take a risk-based approach when it comes to security, the aim is to be minimise the risk to business while still operating securely. Implementing cyber essentials does not guarantee that your organisation will not be compromised.

Q. 65% of companies have not recovered from a cybersecurity attack in the last 12 months - what are the main reasons for the slow recovery?
A: Poor incident planning/preparation or lack of documentation when it comes to recovery of critical systems. Unfortunately, some incident response can take time due to the complexity and nature of the incident. It is crucial that you find and remediate the initial root cause because you don't want to be dealing with the same incident again just after recovering your business IT systems.

Q. Training is essential due to most incidents happening because of human error, but what about human errors that stem from things like cognitive overload etc?
A:Training is essential but it shouldn't be an organisation's only line of defence. Unfortunately, humans do make mistakes, but organisations should also consider security controls across people, process, technology, and physical. Getting the balance right for training is difficult because humans learn differently, what might work for an individual doesn't necessarily work for someone else. Training should be provided regularly but not cognitive overload

Cybersecurity tips
Expert FAQs

Q. Should passwords be changed cyclically (30/60/90 days etc) if secure and not breached?
A: No. Approach to password management has changed over the years. By changing your password regularly for no reason can have negative effect. When mandated to change passwords regularly, people tend to use easy to remember passwords such as adding a number to the end of their existing password or using something like the month or season. This is why using a password manager is a better approach. Password should only be changed if there is a risk that they have been compromised. Passwords should be different across all platforms.

Q. Under Cyber Essentials this brings devices into scope under BYOD and staff may not want monitoring tools. What are the best practices for employers whose staff access data (emails & teams etc) on personal devices?
A: Where possible, personal devices and business devices should be separate. By including personal devices these need to include the same or better security controls as used on business devices. The organisation needs to take a risk-based approach to what devices they allow to store and process sensitive or confidential data.
You also need to consider what happens if there is an incident. Who is responsible for the incident response or investigation on that device? This brings in additional privacy concerns as that individual might not want a third-party to go through their personal data on their device.

Did you know...

Cybercrime costs the UK government £27 billion each year

Cybersecurity tips

Expert FAQs Summary

Using ChatGPT Safely

- Don't enter personal, sensitive, or confidential information into free/public versions.
- Use enterprise editions if business use is essential.
- Switch off Chat History & Training to limit retention.
- Data is stored in the US and accessible to authorised OpenAI staff – assume nothing is fully private.

Paying Ransomware Demands

- No reliable global stats – many cases go unreported.
- Governments are pushing for mandatory reporting (esp. public sector).
- Experts advise: don't pay. But some organisations may see no choice – it's a business decision that should be planned for before an incident.

Password Managers

- Safer than reusing or creating weak passwords.
- Choose a trusted provider and keep it updated.
- Secure the master password with MFA.
- Remember: password managers are high-value targets, so guard access carefully.

Cyber Essentials – How Far Does It Go?

- A solid foundation and often required for contracts.
- But compliance ≠ security. Treat it as a starting point and layer on risk-based controls.

Why Recovery Takes So Long

- Often due to poor incident response planning and documentation.
- Root cause analysis takes time but is crucial to avoid repeat attacks.

Human Error vs Cognitive Overload

- Training is essential but not enough on its own.
- Build layered defences: people, process, technology, physical.
- Avoid "training fatigue" – mix up formats and keep sessions digestible.

Password Rotation

- Don't force 30/60/90-day changes unless breached.
- Frequent forced changes lead to weak patterns (e.g. Winter2025!).
- Use unique passphrases and change only if compromised.

Personal Devices (BYOD)

- Business vs personal should be kept separate where possible.
- If BYOD is allowed, apply the same or stricter controls as business devices.

Training Aid

PCI DSS Checklist

PCI DSS is a set of standards designed to improve card data security. There are six goals and 12 requirements. To ensure PCI compliance, companies must have a rigorous and robust security policy. This requirement is often presented at the end of the PCI DSS framework, but it is the basis of all PCI DSS compliance.

1. **Install & maintain a firewall**
2. **Don't use defaults for system passwords & security parameters**
3. **Protect stored cardholder data**
4. **Encrypt the transmission of cardholder data**
5. **Use and regularly update anti-virus software**
6. **Develop and maintain secure systems and applications**
7. **Restrict access to cardholder data by business need to know**
8. **Assign a unique ID to each person with computer access**
9. **Restricting physical access to cardholder data**
10. **Track and monitor all access to network resources and cardholder data**
11. **Test security systems and processes regularly**
12. **Maintain cybersecurity and information security policies**

Cybersecurity Training

Cybersecurity is critical for protecting your organisation against threats that can damage revenues, reputation, and consumer trust. Our courses cover everything from information security and phishing to emerging risks like ransomware, deepfakes, and business email compromise.

Example Topics Covered

Information Security: How to safeguard sensitive data and prevent information loss or theft.

Phishing: Spot the signs of phishing attempts and know how to respond.

Business Email Compromise: Understand how attackers exploit email systems and how to defend against them.

Ransomware: Learn what ransomware is, how it spreads, and how to protect your organisation.

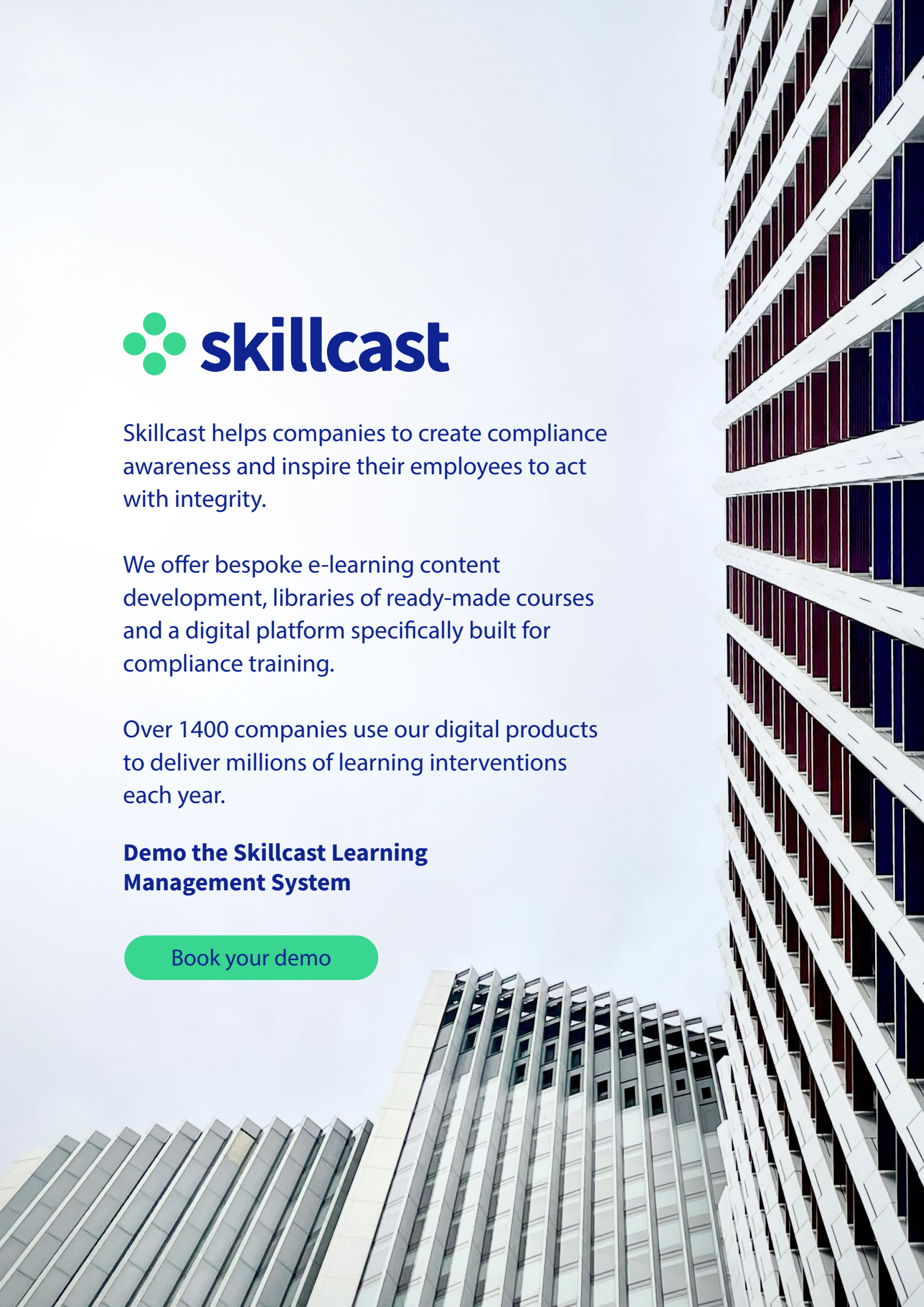
Deepfake Awareness: Recognise deepfake technology and its potential misuse.

Zero Trust Cybersecurity: Introduction to the zero-trust approach to protecting networks and data.

Why Our Cybersecurity Training?

Comprehensive: Over 30 courses covering core and emerging cyber risks.
Flexible: In-depth modules, refreshers, and microlearning formats.
Up-to-Date: Regularly reviewed and aligned with the latest regulations, including DORA.

Start your free trial to see how we make cybersecurity compliance simple.



skillcast

Skillcast helps companies to create compliance awareness and inspire their employees to act with integrity.

We offer bespoke e-learning content development, libraries of ready-made courses and a digital platform specifically built for compliance training.

Over 1400 companies use our digital products to deliver millions of learning interventions each year.

Demo the Skillcast Learning Management System

Book your demo