Cyber Secure

Module 1

Human Risk in Cybersecurity

Author: George Nicholl

Student ID: 50095130

Cybersecurity threats are constantly evolving, and while organisations invest heavily in technical defence, human error remains as one of the biggest vulnerabilities. A single mistake – whether intentional or accidental – can lead to data breaches, system compromises and financial loss. This module examines the concepts of human risk in cybersecurity, the types of common errors that are made by individuals, real world examples and key strategies for mitigating this risk.

This content compliments the video training for Module 1 and provides additional depth, examples and context to reinforce learning.

What is Human Risk?

Human risk in cybersecurity refers to the potential for security incidents caused by human behaviour, including negligence, ignorance, or intentional malicious actions. Despite the presence of sophisticated firewalls, encryption, secure networks and advanced monitoring tools, human users are often the entry point of attack.

Examples include falling for phishing attacks, using weak passwords, sharing sensitive information or failing to follow protocols. Reducing human risk requires a cultural shift in how organisations view security:

Not an IT Issue alone, but as a shared responsibility.

Common Threats or Mistakes

A. Neglecting Security Protocols

- Ignoring company policies or security procedures
- Using unauthorised or outdated software
- Failing to lock devices when unattended
- Mishandling sensitive data

B. Weak Password Practices

- Using easily guessed passwords like “123456” or “password”
- Reusing the same password across multiple services
- Avoiding Multi-Factor Authentication (MFA)

C. Falling for Phishing or Social Engineering

- Clicking on suspicious links in emails
- Downloading malicious attachments
- Providing credentials to fake login pages

D. **Accidental Information Disclosure**

- Sending emails to the wrong recipients
- Discussing sensitive data in public or insecure channels
- Oversharing personal details or organisational information on social media

Together these examples illustrate the diverse ways in which human actions can undermine even the most advanced cybersecurity systems. Whether intentional or accidental, these behaviours pose real and measurable risks to organisational security. Recognising these vulnerabilities is the first step toward implementing more effective protection and building a culture of cyber awareness throughout the workforce.

Real-World Examples

- **2017 Equifax Data Breach** – An unpatched vulnerability and lack of proper security practices led to the exposure of 147 million records, including sensitive financial information.
- **2014 Sony Pictures Hack** – A Phishing attack compromised employee's credentials, leading to massive data leaks and reputational damage.
- **2020 Twitter Bitcoin Scam** – Attackers used social engineering to manipulate employees, gaining access to high-profile accounts to conduct a cryptocurrency scam.

These examples highlight how even large organisations can be compromised by common human behaviours.

Reducing Human Risk

Organisations and individuals can take proactive steps to minimise human risk through training, policies and awareness initiatives:

A. **Training & Awareness**

- Deliver regular cybersecurity awareness sessions to educate people about common cyber threats
- Simulate phishing attacks to test the ability to recognise suspicious emails
- Make the training relevant and interactive
- Stay updated on emerging threats and new attack methods.

B. **Technical Safeguards**

- Require the use of password managers
- Enable Multi-Factor Authentication across all platforms
- Restrict access to sensitive systems based on roles

C. Organisational Policy

- Encourage reporting of suspicious activity
- Recognise employees who follow best practices
- Ensure leadership sets the tone by prioritising cybersecurity

Key Takeaway

Humans remain the weakest link in cybersecurity, but through education, awareness and proactive security measures, organisations can significantly reduce the risks that are posed by human error.

Cybersecurity is not just an IT issue – It is a shared responsibility across all levels of an organisation.

Why This Matters for You

This module is designed to help employees, managers and non-technical staff and individuals build safer habits. Understanding human risk reduces the likelihood of falling victim to common attacks and improves the overall organisational security.

Quick Recap: Human Risk Best Practices

DO:

- ✓ Lock your screen whenever you step away – even for just a moment
- ✓ Use complex, unique passwords for each service & account and enable Multi Factor authentication
- ✓ Regularly complete cybersecurity awareness training and apply what you learn
- ✓ Double-check recipient email addresses before sending sensitive information

DON'T

- X Don't use the same passwords across work and personal accounts
- X Don't assume only IT is responsible for cybersecurity
- X Don't click on unexpected links or download unverified attachments
- X Don't ignore system update prompts or postpone security patches

References

IBM Security Services (2014) 'IBM Security Services 2014 Cyber Security Intelligence Index'. Available at: https://newsroom.ibm.com/2023-07-24-IBM-Report-Half-of-Breached-Organizations-Unwilling-to-Increase-Security-Spend-Despite-Soaring-Breach-Costs (Accessed: 1 April 2025).IBM Newsroom+1Cisco Duo+1

PwC (2019) 'COI on SingHealth Cyber Attack 2019'. Available at: https://www.pwc.com/sg/en/risk-assurance/assets/coi-on-singhealth-cyber-attack-201901.pdf (Accessed: 1 April 2025).PwC+1维基百科，自由的百科全书+1

Breachsense (2024) 'How human error causes data breaches'. Available at: https://www.breachsense.com/blog/data-breach-human-error/ (Accessed: 1 April 2025).Breachsense

Duo Security (2014) 'Human Error Accounts for Over 95% of Security Incidents, Reports IBM'. Available at: https://duo.com/blog/human-error-accounts-for-over-95-percent-of-security-incidents-reports-ibm (Accessed: 1 April 2025).Cisco Duo

Usecure (2019) 'The Role of Human Error in Successful Cyber Security Breaches'. Available at: https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches (Accessed: 1 April 2025).usecure Blog