

# DIGITAL HEISTS UNCOVERED

**How elite hackers break in, and how  
cybersecurity tries to stop them**

Dr Keith L Mannock  
Birkbeck, University of London  
1 October 2026 · BK30228



# A safe investigation

- 01** **We examine real incidents without recreating harmful techniques.**
- 02** Use only fictional data. Never test another person's account, device or network.
- 03** The goal is to think like a defender: notice, question, contain and recover.

# The 90-minute route

- 01** 00-15 How a digital heist works
- 02** 15-31 The Lazarus Heist case files
- 03** 31-43 Activity: reconstruct the attack
- 04** 43-52 Activity: phishing detective
- 05** 52-56 Short reset
- 06** 56-68 How defenders break the chain
- 07** 68-83 NCSC-style incident tabletop
- 08** 83-90 Study route and Immersive Learning Lab

# What counts as a heist?

- 01 Money can move without cash ever changing hands.**
- 02 Data can be stolen, altered, encrypted or used for leverage.
- 03 Disruption can become the objective: services stop, trust falls and recovery costs grow.

# The attacker's problem

## Access is only the beginning

A successful heist also needs a route through the system, enough time to act, and a way to avoid or delay detection.

# Four jobs in one incident

- 01 Gain a foothold: persuade a person or exploit a weakness.
- 02 Expand access: reach accounts, devices or systems that matter.
- 03 Achieve the objective: steal, alter, encrypt or disrupt.
- 04 Survive the response: hide, return or create confusion.

# Security protects three different things

## CONFIDENTIALITY

**Who may see it?**

Example: customer records

## INTEGRITY

**Who may change it?**

Example: payment instructions

# Availability

## Can the service still work?

Hospitals, transport, shops and banks can suffer even when attackers steal no data. Keeping essential services available is a security goal.

# Case file: Lazarus

**BBC Cyber Hack and The Lazarus Heist turn complex incidents into human stories: pressure, improvisation, missed clues and global consequences.**

# Hacking Hollywood

## Sony Pictures, 2014

The incident exposed data and disrupted work. The useful question for us is not 'Who typed fastest?' It is 'Which layers failed together?'

# A breach becomes a crisis

- 01 A person or system grants initial access.
- 02 Weak separation allows access to spread.
- 03 The attacker collects data or affects operations.
- 04 The organisation must investigate while continuing to work.

# The quiet clue

## A printer stops working

At Bangladesh Bank, a faulty printer became part of a much bigger story about suspicious payment messages and delayed detection.

# Bangladesh Bank: the defender's questions

- 01 Which transaction is unusual for this organisation?
- 02 Which independent signal could confirm or contradict it?
- 03 Who can pause the process, and how quickly can they act?
- 04 What evidence must be preserved for investigation?

# Bangladesh Bank payment chain



**Where could an independent check stop a fraudulent instruction?**

# The printer clue



**A mundane failure can remove a monitoring signal**

Defender question: what second route would confirm that the process is healthy?

# Global ATM cash-outs

## Digital instructions, physical cash

Coordinated withdrawals show how a cyber incident can cross software, banking networks, time zones and people on the street.

# ATM cash-out at scale



**The operation depends on synchronising software, people and money movement**

# Digital heists cross boundaries

## INSIDE THE SYSTEM

### **Accounts and permissions**

Messages and transaction rules

Logs and alerts

## OUTSIDE THE SYSTEM

### **People under pressure**

Cash machines and payment networks

Law, communications and public trust

# Kill switch

## Small discoveries can change global events

WannaCry disrupted hospitals and organisations worldwide. A researcher found a technical clue that helped limit its spread.

# Common pattern across the cases

- 01 A normal-looking event creates the opening.
- 02 The attacker depends on connected systems and delayed detection.
- 03 A small clue can reveal the larger incident.
- 04 Recovery requires technical work and human decisions.

# Anatomy of a digital heist



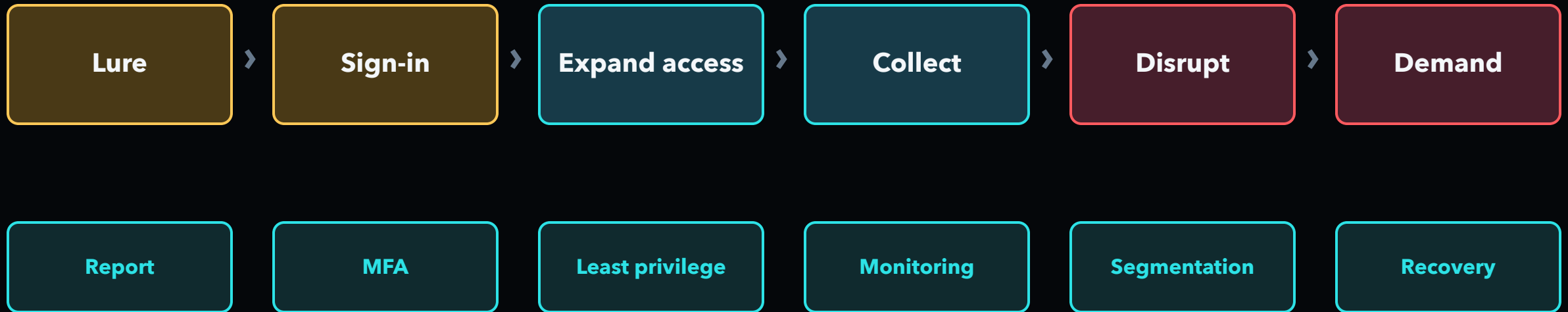
**Which stage would create the first useful clue?**

# The first warning



**A new sign-in can be a clue, but context decides what it means**

# Break points across the chain



**Every stage gives defenders another chance to interrupt the incident**

# Activity 1: attack reconstruction

- 01 Work in groups of three or four.
- 02 Put the evidence cards in the most plausible order.
- 03 Mark one point where a defender could have broken the chain.
- 04 Prepare a 20-second explanation.

# Evidence cards A and B

- 01**    **A 08:42: an employee receives an urgent request that appears to come from a trusted supplier.**
- 02**    B 09:16: a sign-in occurs from a device the organisation has not seen before.

# Evidence cards C and D

- 01 **C 10:03: a large archive of files begins moving to a rarely used internal location.**
- 02 D 10:21: the finance team cannot open a shared folder needed for payments.

# Evidence cards E and F

- 01 E 10:37: a supplier reports receiving strange messages from the employee's account.**
- 02 F 11:05: a note demands payment to restore access.**

# Group decision

## CHOOSE ONE ACTION NOW

**Disable or restrict the affected account**

Isolate a device or system

Pause a risky business process

## CHOOSE ONE QUESTION

**What changed first?**

Which accounts were used?

What still works safely?

# A plausible sequence

**A B C D E F**

The order matters less than the reasoning. Strong teams distinguish facts from assumptions and name the evidence that would change their decision.

# Break points

- 01 Before access: make suspicious requests easier to report.
- 02 At sign-in: require stronger authentication and notice unusual context.
- 03 During movement: restrict permissions and monitor abnormal behaviour.
- 04 During response: contain carefully, preserve evidence and communicate.

# Level up: competing explanations

- 01** **Could the unknown sign-in be legitimate travel or a new phone?**
- 02** Could the file archive be an approved backup?
- 03** Which extra evidence separates a fault, a mistake and an attack?

# Social engineering

## The interface is a person

Attackers use urgency, authority, curiosity or fear to make a risky action feel reasonable.

## Activity 2: phishing detective

- 01 Read the fictional message on the next slide.
- 02 Find four warning signs.
- 03 Choose a safe way to verify the request.
- 04 Do not click, reply or use any real password.

# Fictional message

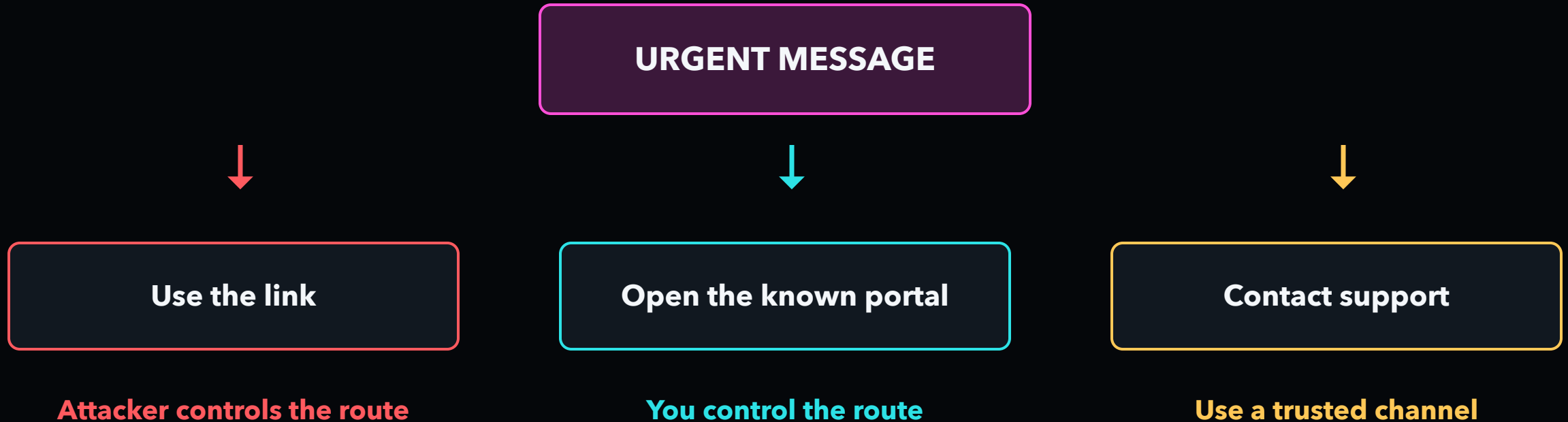
From: IT Helpdesk <support@university-security.example>  
Subject: FINAL WARNING: mailbox closes in 20 minutes

We detected a problem with your student account.  
Use this link now to keep your files:  
<https://login-check.example/verify>

Reply with the six-digit code if the page does not work.  
IT Service

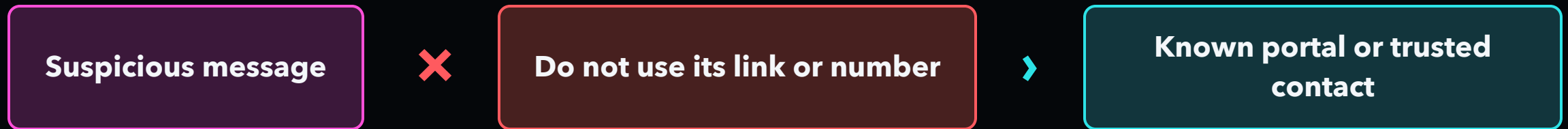
**The .example addresses are deliberately fictional.**

# Phishing decision point



**Vote before the answer appears: which action creates independent evidence?**

# The safest route



**Independent verification breaks the attacker's control of the conversation**

# Warning signs and safer choices

## WARNING SIGNS

### Urgent deadline

Unfamiliar sender or link

Request for a sign-in code

## SAFER CHOICES

### Open the known portal yourself

Contact support through a trusted route

Report the message promptly

# A positive reporting culture

## People are sensors

NCSC guidance treats staff reports as an early warning system. Blame makes people hide mistakes. Fast reporting gives defenders options.

# Level up: AI-assisted phishing

- 01 **Better spelling removes one familiar warning sign.**
- 02 Personal details can make a message feel credible.
- 03 Verification through a trusted route still works.

# Four-minute reset

## Stand, stretch, breathe

When we return: how defenders make attacks harder, noisier and less damaging.

# Ransomware has several stages

1

## Entry

A person, account or  
exposed service

2

## Data theft

Files may leave before  
disruption

3

## Encryption

Systems and data  
become unavailable

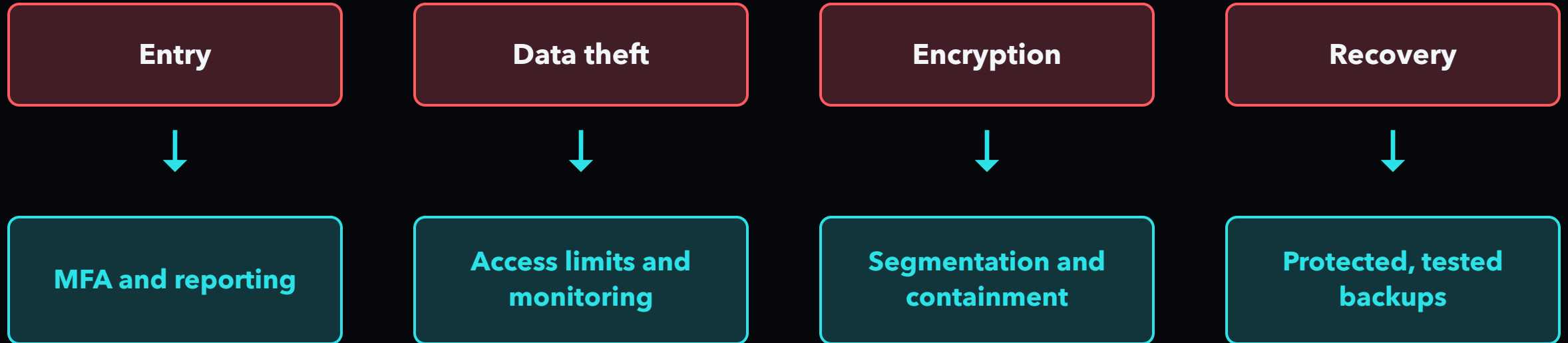
4

## Pressure

Payment demands and  
leak threats

**Encryption may be the loudest moment, but the incident often  
began earlier**

# Ransomware break points



**No single control carries the whole defence**

# Defence is teamwork

**Security brings together software, networks, data, human behaviour, law, communication and business continuity.**



# Defence in layers

- 01 Reduce the chance of initial access.
- 02 Limit what one account or device can reach.
- 03 Detect unusual behaviour early.
- 04 Recover essential services safely.

# Stronger sign-in

## A stolen password should not be enough

Multi-factor authentication and passkeys reduce the value of a password alone. Recovery routes need protection too.

# Least privilege

## Access should match the job

When one account can reach everything, one mistake has a larger blast radius.  
Review access as roles change.

# Segmentation

## Connected does not mean unrestricted

Separating systems can slow movement and protect essential services while an investigation continues.

# Backups

**A backup matters only if it restores**

Keep protected copies, test restoration and know which service must return first.

# Logging and detection

## Turn events into evidence

Useful logs answer who did what, when and from where. Teams still need baselines, context and people who can act.

# Zero trust

## Verify each request in context

Identity, device, location, data sensitivity and behaviour can affect the decision.  
Trust does not last forever just because someone is inside the network.

# Encryption

## WHAT IT CAN PROTECT

### Data travelling across a network

Stored data if a device is lost

Integrity when used with authentication

## WHAT IT CANNOT FIX ALONE

### A compromised authorised account

A user sending data to the wrong place

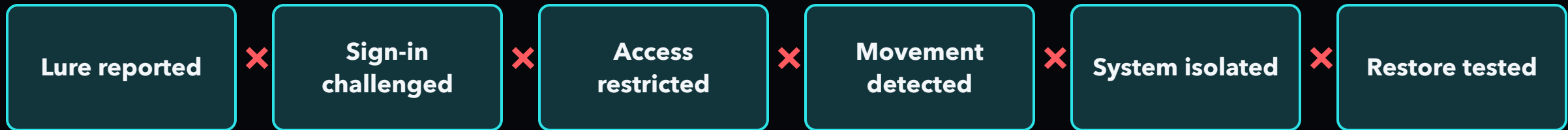
Poor recovery and response

# Secure software

## Design decisions become security decisions

Input checks, careful error handling, updates and testing reduce opportunities for attackers and mistakes.

# The attack chain replayed



**Each layer limits the next move and creates time for people to act**

Ask: which layer depends most on preparation before the incident?

# Level up: access-control matrix

- 01 Student: view own profile; submit work.
- 02 Tutor: view class list; mark assigned work.
- 03 Administrator: manage enrolment; no automatic access to submitted work.
- 04 Which permission would create the largest unnecessary risk?

# The UK threat picture

## 204 nationally significant incidents

The NCSC handled 204 nationally significant incidents in the 12 months to August 2025, up from 89 the previous year. Eighteen were highly significant.

# Critical systems

## More than 200 incidents in one year

The NCSC reported more than 200 incidents affecting UK critical national infrastructure or its supporting ecosystem in the year to May 2026. Around 75% were believed linked to state actors.

# Ransomware changes daily life

- 01 Recent UK incidents affected retailers, aviation and automotive manufacturing.**
- 02 Effects spread to customers, staff and suppliers.
- 03 The NCA describes ransomware as the highest-harm serious and organised cybercrime threat affecting the UK.

## Activity 3: incident tabletop

- 01 Your group runs a fictional ticketing company called Northstar Live.
- 02 You will receive three incident updates, called injects.
- 03 After each update, choose one priority action and one message.
- 04 There is no perfect information and no single correct answer.

# Tabletop roles

- 01 Incident lead: decides priorities and keeps the team focused.
- 02 Technical lead: explains what can be isolated, checked or restored.
- 03 Communications lead: prepares clear messages without guessing.
- 04 Evidence recorder: separates confirmed facts, assumptions and open questions.

# Inject 1

## 09:10: unusual sign-ins

A staff account signs in from two countries within eight minutes. Customers report that password-reset emails have arrived without being requested.

# Inject 1 decision

- 01** **What can you restrict without stopping the whole service?**
- 02** Which evidence would confirm account takeover?
- 03** How will legitimate staff regain access safely?

# Inject 2

## 09:35: checkout failures

Payment attempts are failing. A supplier says its remote-support account has been locked. Social media claims customer data has leaked, but you have not confirmed this.

# Inject 2 decision

- 01 Which business process should pause?**
- 02 What evidence must be preserved before systems change?
- 03 What can you tell customers now without overclaiming?

# Inject 3

## 10:20: the recovery dilemma

A ransom note appears on several staff devices. Yesterday's backup completed, but nobody has tested a full restore this month. A major event goes on sale at noon.

# Inject 3 decision

- 01 Which service must return first, and why?
- 02 How will you test that restored systems are safe?
- 03 Who decides whether the noon sale can proceed?
- 04 Which regulator, law-enforcement or cyber-response routes might apply?

# Model response priorities

## FIRST HOUR

### **Protect people and essential services**

Contain affected access and systems

Preserve evidence and record decisions

## NEXT PHASE

### **Communicate confirmed facts**

Restore from trusted sources

Review causes and improve controls

# The purpose of exercising

## Practise decisions before pressure arrives

NCSC Exercise in a Box provides free scenarios covering ransomware, phishing, supply chains, passwords, vulnerabilities and more.

# Tabletop debrief

- 01 Which clue changed your plan?
- 02 Where did the team disagree?
- 03 Which preparation would have saved the most time?
- 04 What would you measure to know recovery is real?

# Level up: supply-chain twist

- 01 **Northstar's own systems look clean.**
- 02 A software supplier reports that its update service may be compromised.
- 03 Which connections, updates and credentials should Northstar review first?

# Study the whole system

**Birkbeck's BSc Computer Science for Cybersecurity combines core computing with information security, secure software, networking, governance, threat response and a final project.**



# BSc Computer Science for Cybersecurity

- 01 Three years full-time on campus.
- 02 Four years part-time on campus.
- 03 A four-year full-time route with Foundation Year is also listed.
- 04 The University of London awards the degree.

# Today's activities map to the degree

## TODAY

### Reconstruct an incident

Judge suspicious evidence

Balance containment and recovery

## COURSE TOPICS

### Information Security

Secure Software Development

Cyber Threat Management and  
Response

# Cybersecurity careers

- 01 Security analyst and incident responder
- 02 Secure software developer and security engineer
- 03 Digital forensics and threat intelligence
- 04 Governance, risk, audit and security consulting
- 05 Research, policy and roles still emerging

# Immersive Learning Lab

Take a defender's questions next door: What does the system sense? What does it trust? What happens if a signal is wrong, missing or malicious?

# Five ideas to keep

## Security is a chain of decisions

People create clues. Layers limit harm. Logs support evidence. Recovery must be tested. Clear communication belongs in the response.

# Listen and explore

- 01 BBC Sounds: Cyber Hack and The Lazarus Heist
- 02 NCSC: guidance, alerts and Exercise in a Box
- 03 Birkbeck: BSc Computer Science for Cybersecurity
- 04 University of London: taster-course information

# Optional extension: Caesar cipher

- 01 **Shift each letter three places: A becomes D.**
- 02 Decode: VHF~~X~~ULWB QHHGV PRUH WKDQ D VHFUHW  
DOJRULWKP
- 03 Why does frequency and repetition make this weak?

# Optional extension: threat model the room

- 01 Assets: what matters in an immersive environment?
- 02 Inputs: cameras, controllers, microphones or accounts.
- 03 Failures: what if a signal is wrong, missing or malicious?
- 04 Controls: how could the design limit harm and protect privacy?

# Optional extension: ethical red teaming

- 01 Permission defines the system and time window.
- 02 Rules of engagement define allowed and prohibited actions.
- 03 Evidence supports a clear report and safe remediation.
- 04 Testing stops when safety or scope is uncertain.