Simple Bowtie for a common top event: unauthorised access to live/online confidential data

Threats (left):

- Malware
- Remote intruder e.g. hacker
- Physical intruder
- Malicious Internal User
- Non-Malicious Internal User

Central:

Confidential data stored in live/online computing environments

Unauthorised access to data

Barriers / controls (threat side):

- Up-to-date anti-malware software on all devices
- Staff security awareness training (e.g. Computer Use Policy, handling suspicious files, portable media advice or usage banned)
- Logical access controls at all levels (e.g. network, server drive, folder, file, application role)
- Firewall
- Intrusion detection and prevention system
- Logical access controls at all levels (e.g. network, server drive, server console, folder, file, application role)
- Naming conventions (defence by obscurity)
- Decoy environment (honeypot)
- Staff security awareness training (e.g. Computer Use Policy, social engineering, screen locking, password complexity)
- Staff security awareness training (e.g. Computer Use Policy, social engineering, screen locking, printer output, password complexity)
- Logical access controls at all levels (e.g. network, server drive, server console, folder, file, application role)
- Intrusion detection and prevention system
- Naming conventions (defence by obscurity)
- Decoy environment (honeypot)
- Physical access controls (e.g. biometrics, keys, key pad combinations)
- Tamper proof hardware seals
- Encryption of hard drives
- HR procedures for: vetting, reference checking, staff grievances and employee exits
- Logical access controls at all levels (e.g. network, server drive, server console, folder, file, application role)
- Physical access controls (e.g. biometrics, keys, key pad combinations)
- Tamper proof hardware seals
- Encryption of hard drive
- Staff security awareness training (e.g. Computer Use Policy, social engineering, screen locking, printer output, password complexity)
- Intrusion detection and prevention system
- Staff security awareness training (e.g. Computer Use Policy, screen locking, printer output)
- Competency in the use and navigation of networked computing environments
- Logical access controls at all levels (e.g. server drive, folder, file, application role)

Barriers / controls (consequence side):

- Warning 'banner' before entering confidential data store
- Backup and recovery process/procedures
- Effective DR process
- Backup and recovery process/procedures
- Availability of replacement hardware with equivalent specifications and configuration
- Advise affected parties to initiate mitigation, e.g. changing their passwords, blocking accounts
- DR Communications Plan (periodically reviewed)
- Compliance with applicable security standards

Consequences (right):

- Exposure of sensitive/confidential data
- Data loss through deletion or corruption
- Lost productivity
- Exploitation of sensitive/confidential data
- Reputational damage, including lost clients
- Legal or regulatory action, including fines