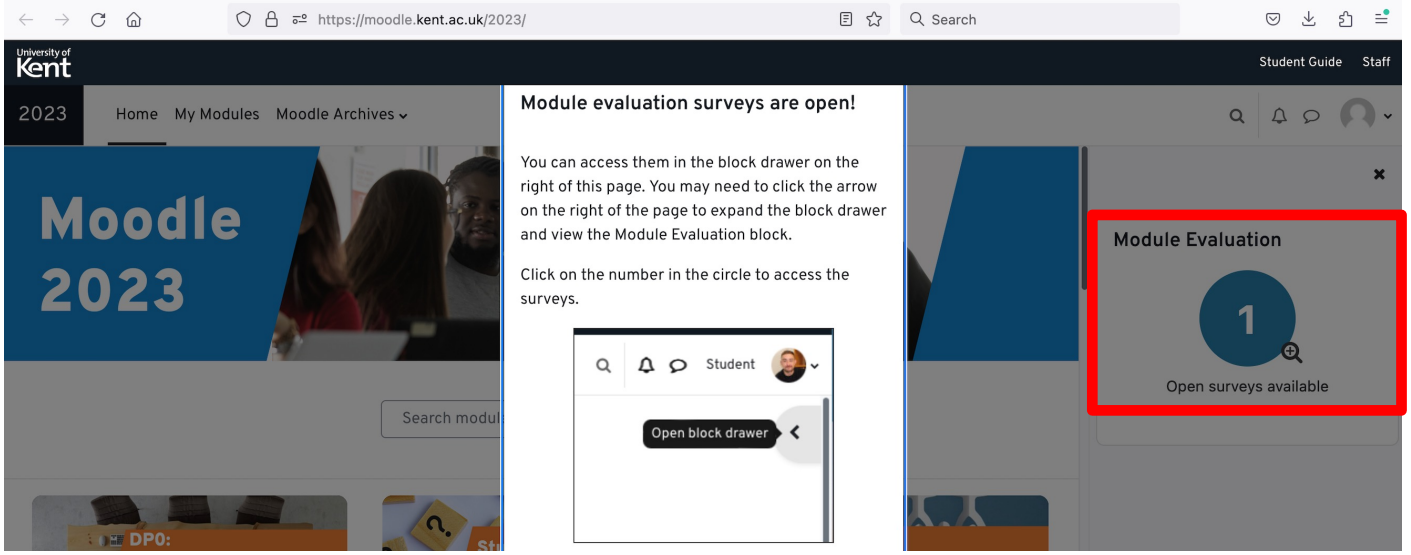
Accountability

Budi Arief
b.arief@kent.ac.uk

Based on slides by Shujun Li

Before we start…

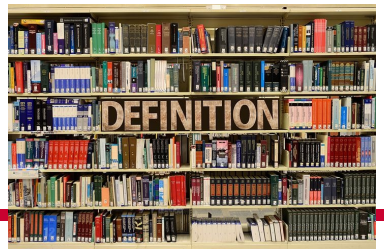
- Module evaluations are now live!
  - Please give us feedback on the delivery of COMP8760 (and other modules too) this year, so that we can improve for next year
  - The survey is open until **19 Jan 2024, 23:59:00**
  - You can access the survey from your Moodle homepage



Outline

- Basic Concepts
- Event Logging (Evidence Collection)
- Selected Techniques for Auditing and Incident Investigation
- Post-Incident Recovery
- Privacy Considerations
- Summary

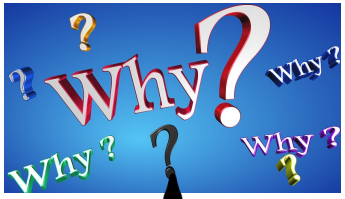
What is accountability?



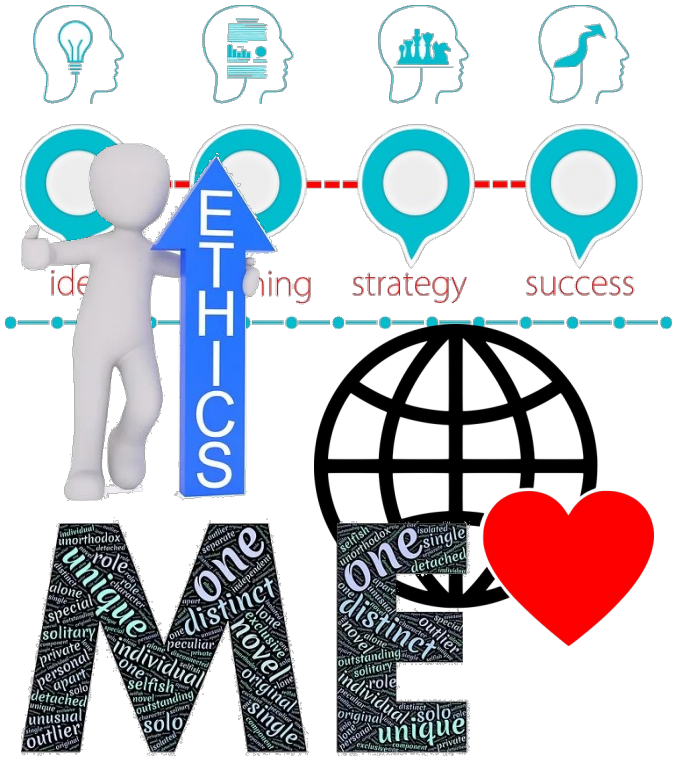
University of Kent

- Cambridge Dictionary
  - "the fact of being **responsible** for **what you do** and able to give a **satisfactory reason** for it, or the degree to which this happens"
- IETF RFC 4949 "Internet Security Glossary, Version 2" (2007)
  - "The property of a system or system resource that ensures that the **actions of a system entity** may be **traced** uniquely to that **entity**, which can then be held **responsible** for its actions."
- NIST CSRC (Computer Security Resource Center) Glossary
  - "… property that ensures that the **actions** of an **entity** may be **traced uniquely** to that entity."
  - There are more other definitions with different wordings, but the core messages are the same.

Reasons of accountability



- Legal compliance
- Contractual obligations
- Business needs
  - Quality assurance
  - Performance monitoring
  - Staff training and education
  - …
- Ethical requirements
- Social goods
- Personal needs or wishes
- …



Legal compliance: The case of GDPR

- GDPR = General Data Protection Regulation
  - The EU data protection law.
  - For the UK, the Data Protection Act 2018 is largely based on the GDPR and will still be valid after Brexit.
- One of the data protection principles in the GDPR.
  - "The controller shall be **responsible** for, and be able to **demonstrate** compliance with, paragraph 1 [the other data protection principles]"
- What should be done by organisations?
  - "you must implement **technical** and **organisational** measures to ensure, and **demonstrate**, compliance …"
  - "the measures should be **risk-based** and **proportionate**"
  - "you need to **review** and **update** the measures **as necessary**"

From accountability to auditing

- IETF RFC 4949
  Internet Security Glossary, Version 2 (2007)
  - **Audit service**: "A security service that records information needed to **establish accountability** for system events and for the actions of system entities that cause them."
  - **Security audit**: "An **independent review and examination** of a system's **records and activities** to determine the **adequacy of system controls**, ensure **compliance with established security policy and procedures**, detect breaches in security services, and recommend any changes that are indicated for countermeasures."
  - "**Audit trails** are examples of control measurements that are recorded as part of system operations."
  - Relevant for "archive", "attack sensing, warning, and response", "**controlled access protection**", "**Identification Protocol**", "intrusion detection", "**key management**", "**login**", "policy", "time stamp", …

Audit policies

- Sound audit policies are needed!
- Such policies can define
  - What **evidence** will be collected.
    - What events and information will be **logged**. ⇒ Event logging is a key element of auditing.
  - Who can access evidence collected.
  - Who are in charge of what.
  - When an investigation should be triggered.
  - When disciplinary and legal actions should be taken.
  - When external parties should be informed/involved.
  - What post-incident actions should be considered.
  - How staff training and communications should be organised.
  - …

SOCs

- SOC = Security Operations Centre
  - McAfee: “a centralized function within an organization employing people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents.”
- Key activities of an SOC
  - NCSC UK: **integration, management and review of traffic feeds**; **protective monitoring**; **initial triage and analysis**; vulnerability management; **alerting and response**; **incident management**; **root cause analysis**; patching & remediation; **correlation management**; **Security Information and Event Management (SIEM) tuning**; continuous improvement; **key management**
- A key unit for enabling accountability within an organisation
  - **Evidence** management is the key: **preserving** evidence, **analysing** evidence, and **assessing** evidence.

CSIRTs

- CSIRT = Cyber/Computer Security Incident Response Team
  - Also known as CERT (CMU's registered trade mark): Cyber/Computer Emergency Response Team
  - And as CIRT (ITU term): Cyber/Computer Incident Response Team
  - Many organisations and nations have set up such a team.
- CSIRTs vs SOCs
  - CSIRTs can have a narrower scope than SOCs.
  - A SOC often serves a single organisation, but a CSIRT can serve a sector, a nation or a region (e.g., CERT-EU for the whole EU).
  - The differences between them are not a clear cut.
  - There are often shared resources between the two teams.
  - CSIRTs as SOCs and vice versa

Outline

- Basic Concepts
- Event Logging (Evidence Collection)
- Selected Techniques for Auditing and Incident Investigation
- Post-Incident Recovery
- Privacy Considerations
- Summary

Who/What can/should do logging?

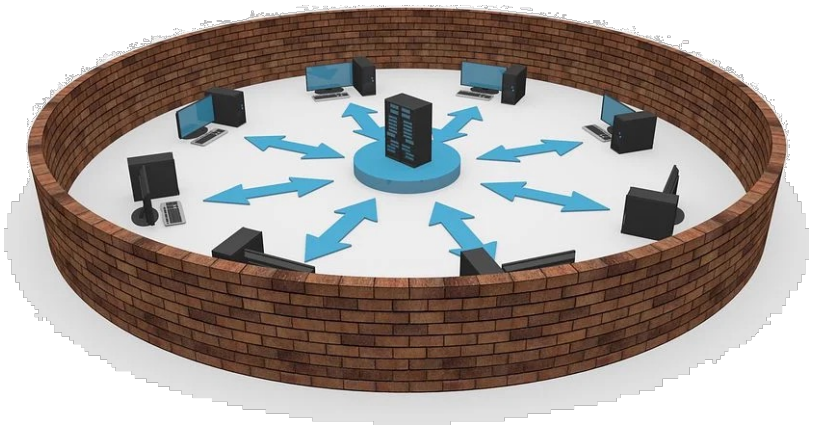
- Hardware
  - Networking devices (router, switches, firewalls, …), personal computers, mobile devices, …
- Software
  - Operating systems, local applications, mobile apps, cloud services, managed services, online services, …
- Organisations
  - Law enforcement agencies (LEAs), Internet service provides (ISPs), online service providers, identity providers (IdPs), employers, software and hardware vendors, …
- People
  - Supervisors, colleagues, parents, teachers, other users of online services, criminals, …

Where can logs be stored?

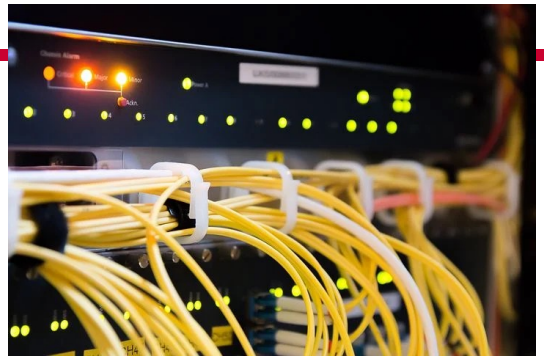
- External memory
  - Hard disk
  - Portable storage media
  - Permanent storage media (e.g., CD-R discs)
- Main memory @ Local devices
  - Such data can be recovered via memory dump.
- Cloud storage
- Databases
  - Local or distributed (e.g., a blockchain system)
- Remote servers (main or external memory)
- Special devices (main or external memory)
  - IoT devices, mobile devices, …
- …

Logging examples: Servers

- System local events
- Network connections
- Connections of external devices
- User management records
- Authentication events
- Authorisation events
- Access control events
- Hardware and software updates
- System configurations
- Application logs
- …



Logging examples: Networking devices



- Network flow logging
- IP packet inspection
- Routing records
- DNS requests and records (including caches)
- Network-level firewall records
- System configuration logs
  - Subnet configuration, IP address allocation, DHCP configuration, DNS servers, …
- Application layer monitoring and logging
  - Web (HTTP/HTTPS), email (POP3/SMTP/IMAP), FTP, SSH, VPN, VoIP, video conferencing, …
- …

Logging examples: End devices

- Monitoring tools on end devices
  - Anti-virus (AV) software
  - Firewall
  - Software scanner (e.g., for detecting license violations and installation of piracy software)
  - …
- All local applications
  - Including web browsers and extensions
- Local caches
  - Operating systems and local applications
- BYOD (Bring Your Own Device) policies and registration of user devices at workplace
- …

Outline

- Basic Concepts
- Event Logging (Evidence Collection)
- Selected Techniques for Auditing and Incident Investigation
- Post-Incident Recovery
- Privacy Considerations
- Summary

Authentication

- Authentication without auditing is dangerous!
  - We need to know who did what.
  - ⇒ **Accountability of all users**
  - ⇒ Audit trials of all user logins and logouts should be kept.
- Different authentication techniques can help!
  - Possession-based authentication: Can be used to identify hardware devices involved.
  - Inherence-based authentication: Can be used to identify people involved.
  - Context-based authentication: Can be used to identify contextual factors involved (e.g., geo-locations).
  - Risk-based authentication: Can be used to identify audit trials that require more attention.
  - Continuous authentication: Can be used to create a continuous audit trial of each user during login.

Authorisation

- Authorisation without auditing is dangerous!
  - The grantor (authoriser) should be responsible for all authorisation decisions.
  - ⇒ **Accountability of the grantor (authoriser)**
  - The grantor (authoriser) needs to know what the authorisee has been doing.
  - ⇒ **Accountability of the authorisee**
  - The access control policy makers should be responsible for any policy decisions made.
  - ⇒ **Accountability of the policy makers**
- Delegation without auditing is dangerous!
  - ⇒ **Accountability of the delegator and the delegatee**

Non-repudiation

- Non-repudiation = Source of origin verification
  - MACs (Message Authentication Codes)
  - Digital signatures
  - Biometrics
  - …

- **Trusted third parties** are often used as proxies.
  - Certificate authorities (CA) for issuing and verifying digital certificates
  - Identity providers (IdPs) for managing and verifying digital identities
  - Credential issuers for issuing verifiable credentials (VCs) and credential verifiers for verifying VCs
  - Governmental bodies for issuing and verifying passports and visas
  - …
- Non-repudiation gives a record of who did what.

Anti-virus (AV) software

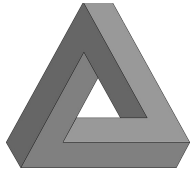
- What does it do?
  - Traditionally for detecting and removing computer viruses only
  - Nowadays for detecting and removing all kinds of malware
- Often extended to include other advanced features
  - Detecting phishing attacks, built-in VPN, parent control for child protection, software patching management, …
- Can also be used to identify those accountable and facilitating incident investigation.

How does AV software work?

- **Signature** based approach
  - A static signature is generated (mostly manually by malware analysts) to capture a specific piece of malware.
  - AI may help when static signatures fail.

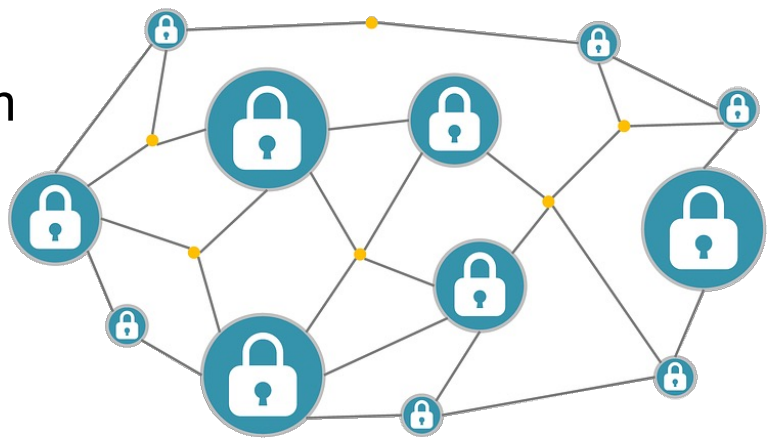
- **Static** (**code**) analysis
  - Analysing suspected binary code to look for signs of malware
  - Can be based on analysis of API calls

- **Dynamic** analysis (**sandbox**-based detection)
  - Putting suspected malware in a sandbox and analysing its **dynamic behaviour**



- Perfect AV software does not exist!
  - Researchers have demonstrated that it is **impossible** to design an algorithm capable of detecting **all** computer viruses (Cohen 1987, Chess & White 2000).

Network IDS (NIDS)



- IDS = Intrusion Detection System
  - ⇒ IPS = Intrusion Prevention System
  - Against various network attacks
- Network IDS
  - IDS at network traffic level
- Detection methods
  - **Misuse** (**signature**) based: for **known** attacks
  - **Anomaly** based: for **unknown** attacks (network traffic behaviours deviating from what is seen as normal)
    - Mostly **machine learning** based
- Can be used to record **network-level data flows** for identifying those accountable and facilitating incident investigation.

Host-based IDS (HIDS)

University of Kent

- A **local** IDS
  - IDS running on and for protecting an individual host
  - A piece of AV software can be seen an HIDS.
- What is being monitored?
  - **Network traffic** in and out of the protected host (similar techniques for NIDS can apply here)
  - **Local files** on the protected host ⇔ AV
  - **Internal processes** running in the main memory of the protected host ⇔ AV
  - **Behaviours** of human users and other local entities on the protected host ⇔ Detection of impersonators and insiders
- Can be used to record **host-level data flows** for identifying those accountable and facilitating incident investigation.

DLPs

- DLP = Data loss/leakage protection/prevention
  - Computing systems to prevent sensitive data leaking from a protected network (e.g., a company's intranet)
  - Data = Data at rest + Data in use + Data in motion
- Differences from NIDS
  - Normally target **unintentional** (**accidental**) data loss/leakage
  - Only care about **outbound data** (internal to external)
- Can be used to identify those accountable and facilitate incident investigation

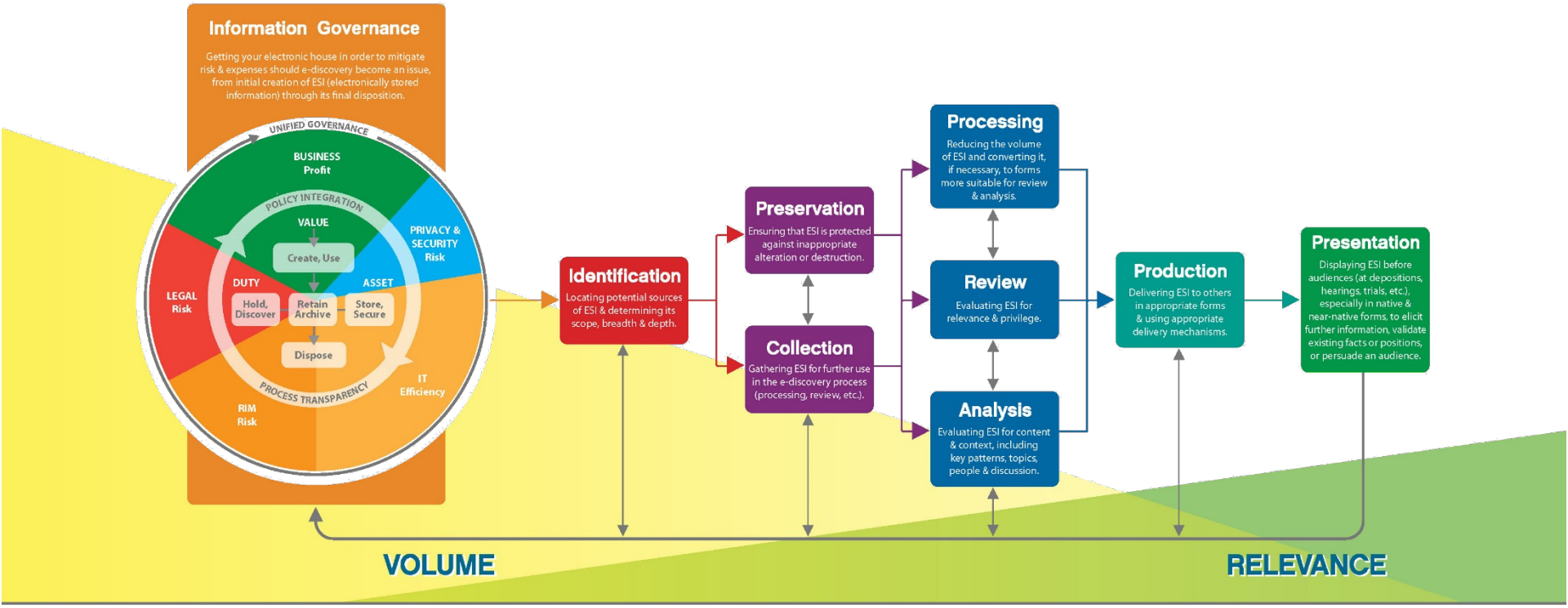
Insider threat detection

- What are “insiders”?
  - **Malicious insiders** (e.g., employees who collude with criminals)
  - **Negligent insiders** (e.g., employees who did not follow policies)
  - **Unintentional insiders** (e.g., employees who mis-communicate)
  - **Infiltrators**: external parties who gain access to internal systems therefore become an “insider”
- Is this a real problem?
  - Insider Threat Report 2018 (Veriato): “53% … have confirmed insider attacks against their organization in the previous 12 months”
- Identifying insiders = Identifying those accountable
- Monitoring insider threats
  - Require close monitoring and logging of all internal systems and interfaces with external systems
  - A.S. McGough, B. Arief, et al. “Detecting Insider Threats Using Ben-ware: Beneficial Intelligent Software for Identifying Anomalous Human Behaviour”, *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, Vol. 6, No. 4, pp. 3-46, 2015.

Digital forensics and e-discovery

- Digital forensics (DF)
  - ISO/IEC 31021:2015: "scientific tasks, techniques and practices used in the **investigation** of stored or transmitted **binary information or data** for **legal purposes**"
  - A closer but broader term: **digital investigation**
- Electronic discovery / e-discovery / eDiscovery
  - ISO/IEC 27050-1:2019: "discovery that includes the **identification**, **preservation**, **collection**, **processing**, **review**, **analysis**, or **production** of **Electronically Stored Information**"
  - Civil equivalent of digital forensics
- Many free and commercial tools and services are available.
  - See Wikipedia's list of DF tools, Gartner's e-discovery software list and Gartner's e-discovery report (2015)
- Both can be used for establishing accountability.

- EDRM = Electronic Discovery Reference Model
  - “practical global resources to improve e-discovery, privacy, security, and information governance”



Copyright © 2020, EDRM Global, Inc., Creative Commons Attribution 4.0 International, edrm.net

Security visualisation

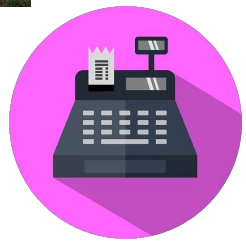
- SOCs and CSIRTs have to work with big data.
- Visualisation helps make more sense out of data!

https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

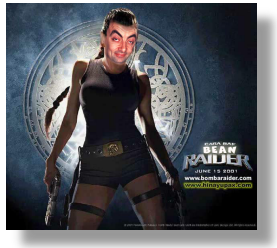
https://www.digitalattackmap.com/

Digital watermarking

- A digital watermark is a **<u>digital artefact embedded into</u>** a (digital) cover work.
- Relevant applications for accountability
  - **Transaction tracking**
    - A watermark is embedded as a fingerprint of each copy of a digital item: "Sold on 09/12/2019 to Alice."



  - **Content authentication / Tamper detection**
    - A watermark is used to preserve the integrity of a digital item.



  - **Persistent item identification**
    - A watermark is used to associate an identifier with a digital item, which can be used for various purposes.

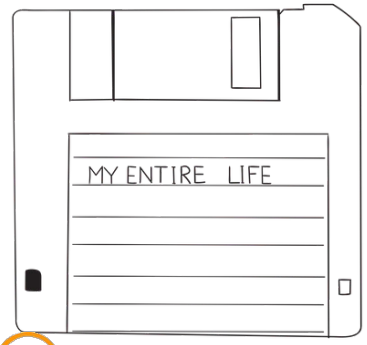
  - …

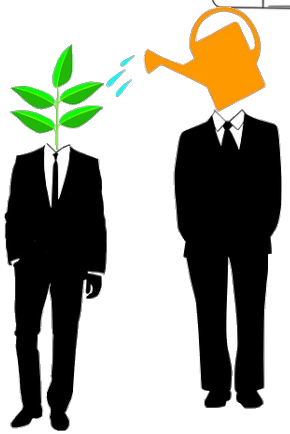
Outline

- Basic Concepts
- Event Logging (Evidence Collection)
- Selected Techniques for Auditing and Incident Investigation
- Post-Incident Recovery
- Privacy Considerations
- Summary

Proactive mechanisms

- Data backup
  - Real-time backup (e.g., automatic synchronisation with a remote cloud server)
  - Daily backup
  - Multi-site backups
  - Air-gapping
- Staff training and education
- Forensic readiness
  - Working with LEAs and security service providers
- Proactive threat monitoring
- …





Reactive mechanisms

- Incident investigation
  - Establish accountability
  - Learning from past failures
- System updates
- Communications
  - To staff, consumers, suppliers, partners, and the relevant authorities (e.g., for data breaches per the GDPR requirements)
- Staff (re-)training
- Policy reviews
- Disciplinary actions
- Legal actions
- …

“In-class” exercise

- Imagine some cyber incident happens on your laptop so that some of your important data are leaked, stolen, locked (e.g., encrypted by ransomware), hidden or erased.
  - What would you do to recover?
  - What should you have done before the incident to be better prepared for such an incident?

Outline

- Basic Concepts
- Event Logging (Evidence Collection)
- Selected Techniques for Auditing and Incident Investigation
- Post-Incident Recovery
- Privacy Considerations
- Summary

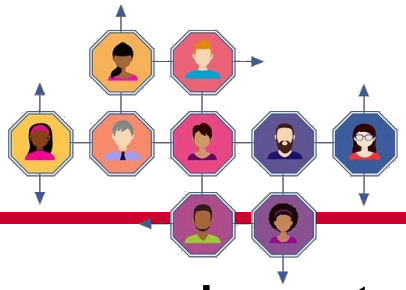
Privacy of employees

- Logging has immediate privacy implications on employees' privacy.
- Employment law may limit how closely an organisation can monitor its employees.
  - $\Rightarrow$ Some data may have to be anonymised, therefore limiting the usefulness of audit trails.
- **Distributed but cooperative logging** can help.
  - Example: Partial logs of an organisation + logs of an external website $\Rightarrow$ Identification of a malicious employee who attacked the external website from the organisation's work computer

Privacy of customers

- Many organisations hold a lot of personal data of individual customers.
- Accountability **for data protection** purposes
  - ⇒ Help better protect privacy of individual customers.
  - Example: DLP and IDS can both help reduce personal data breaches.
- **Aggregating data** from different sources and **presenting evidence** to relevant employees and external parties can potentially lead to **unwanted disclosures of personal data**.
  - **Data anonymisation** methods should be considered.

Privacy of other people



- People around employees and customers may also be affected.
  - Family members (including kids)
  - Friends
  - Other users of a shared computing device
  - Other users of a shared (internal or external) service
  - Other users of a shared communication session or platform (e.g., a remote meeting)
  - Those whose identities are stolen by criminals
  - …
- More on privacy was already covered in COMP8240.

Outline

- Basic Concepts
- Event Logging (Evidence Collection)
- Selected Techniques for Auditing and Incident Investigation
- Post-Incident Recovery
- Privacy Considerations
- Summary

Summary

- **A**ccountability (or Accounting) is the final piece of the “AAA” in information security.
  - It can be achieved through auditing.
    - **A**uthentication without auditing is dangerous.
    - **A**uthorisation without auditing is dangerous.
- Many reasons for the need of accountability:
  - Legal compliance, contractual obligations, business needs, ethical requirements, …
- Several related topics:
  - SOCs, CSIRTs, event logging, IDSs, DLPs, insider threats, digital forensics, and privacy (covered in COMP8240)
    - Some of these will be discussed further in COMP8920 next term.

Summary (contd.)

University of Kent

- And that's a wrap!
  - Authentication
    - User authentication: password and beyond password
    - Non-user authentication: product, message, server, software, humanness, …
  - Access control and authorisation
    - A zoo of access control terms, plus IdM, FIM, VC
  - Accountability

- Have a nice Christmas and New Year!