arcX Cyber Threat Intelligence 101 part 4

Day 17/365

Threat vectors

Threat vector

- 'A path or method via which a threat gains access to a victim computer or network'

Vulnerability

- 'A flaw in a system (people, technology or business logic) that a threat can exploit to create an effect on the victim'

Threats can exploit vulnerabilities in

- Emails
- Users
- Remote access portals
- Software
- Networks (intranet and internet)
- Hosts

Security Controls

- 'countermeasures that a company can implement to detect, prevent, reduce or counteract security risk(s)'
  -Isolating legacy systems
  -Education and training
  Physical security (i.e. no USB)

Threat vector types

Attack Surface

- All the technology of an organization put together (people, computers, networks, accounts)
- The combined sum of the different points within an organisation that a malicious cyber actor can use to mount an attack

In order for the threat to have an impact on the organization there has to be a vulnerability being exploited

Email

#1 exploited threat factor in the past

- Inexpensive to mount
- Low risk
- Multiple attempts to compromise

Points to note

- Don't assume every malicious email contains malware
- Specific tactics are linked with this threat vector

Users

Directly

- Spear Fishing

Indirectly

- Watering hole attack
  - 1. Attackers find a suitable website (the watering hole)
  - 2. Attackers compromise the website
  - 3. User visits the website and malicious script is downloaded
  - 4. Script exploits vulnerabilities and delivers malware to the user
  - 5. Attackers have access to the network and continue trying to reach their objective
- Insider Threat
  - STUXnet

VPN or Remote Desktop Protocol (RDP)

- Logging as an actual user
- No malware - much smaller trace for defenders to detect
- Critical element of many ransomware attacks

Software

- Vulns
- The most exploited
- CVE - Standardised method for recording vulnerabilities

Network

- Hardware issues
- Firewall
- Wi-Fi access
- Internet of Things

- Bring your own Device

Hosts

- End devices

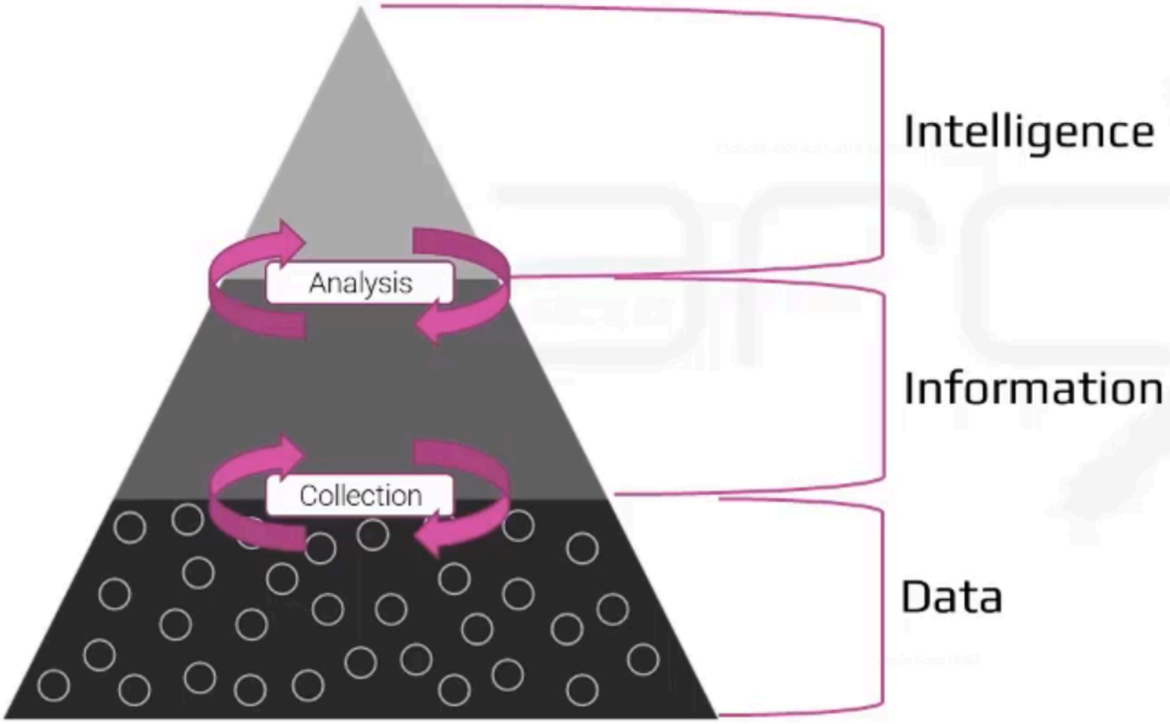
Additional points

- Threat vectors don't exist in isolation
- i.e. Business email compromise typically leverages
  - 1. Remote access portal compromise
  - 2. People
- The way that a threat can exploit vulnerabilities is potentially infinite
- Supply chain vulnerabilities have the ability to sit behind all of the threat vectors that we have discussed -> Software that you bought and are using could be already compromised i.e. solarwinds
- Reducing the attack surface by providing less end devices to employees is not as easy since you need to balance security, functionality and ease of use when building a system. It can be useful to separate the responsibilities by teams, one team responsible of each type of end device, can elaborate on the threat on more detail

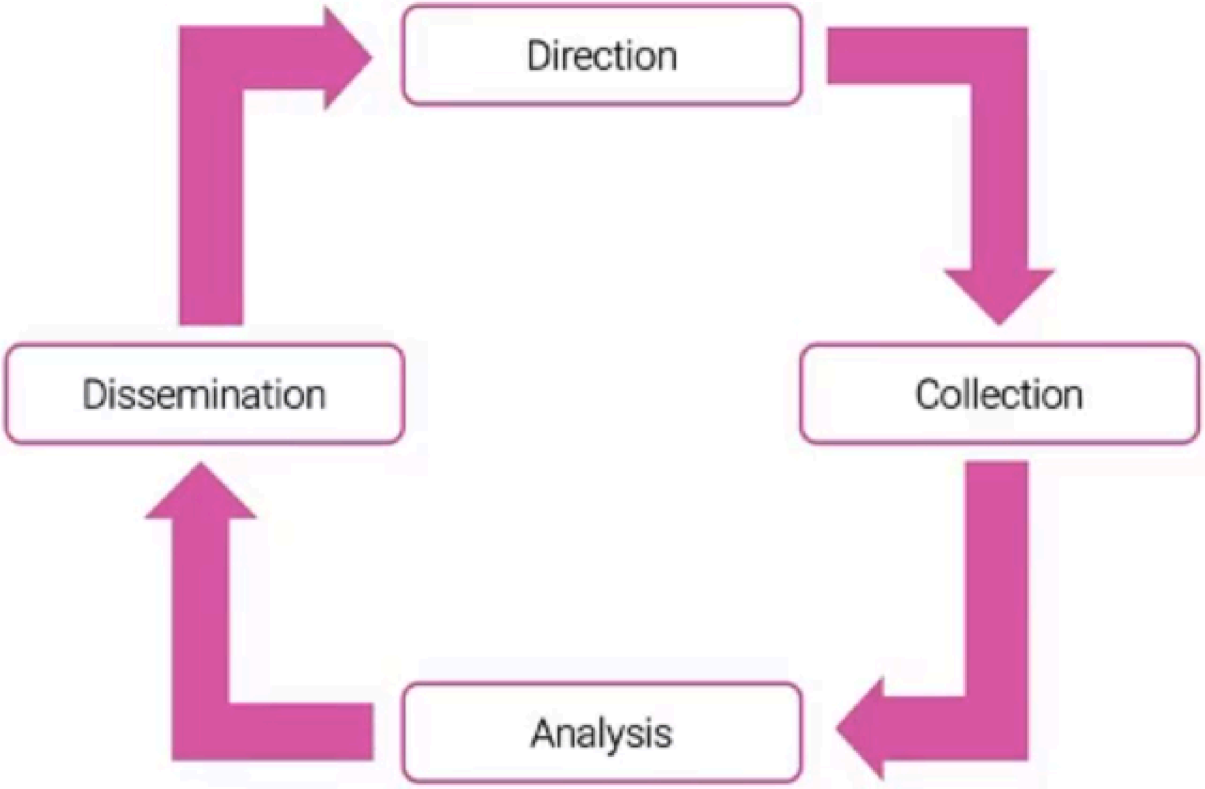
---

The Intelligence Cycle

CTI is about turning data into intelligence, and the Intelligence Cycle is the process that allows us to do this



Transforming data into Intelligence



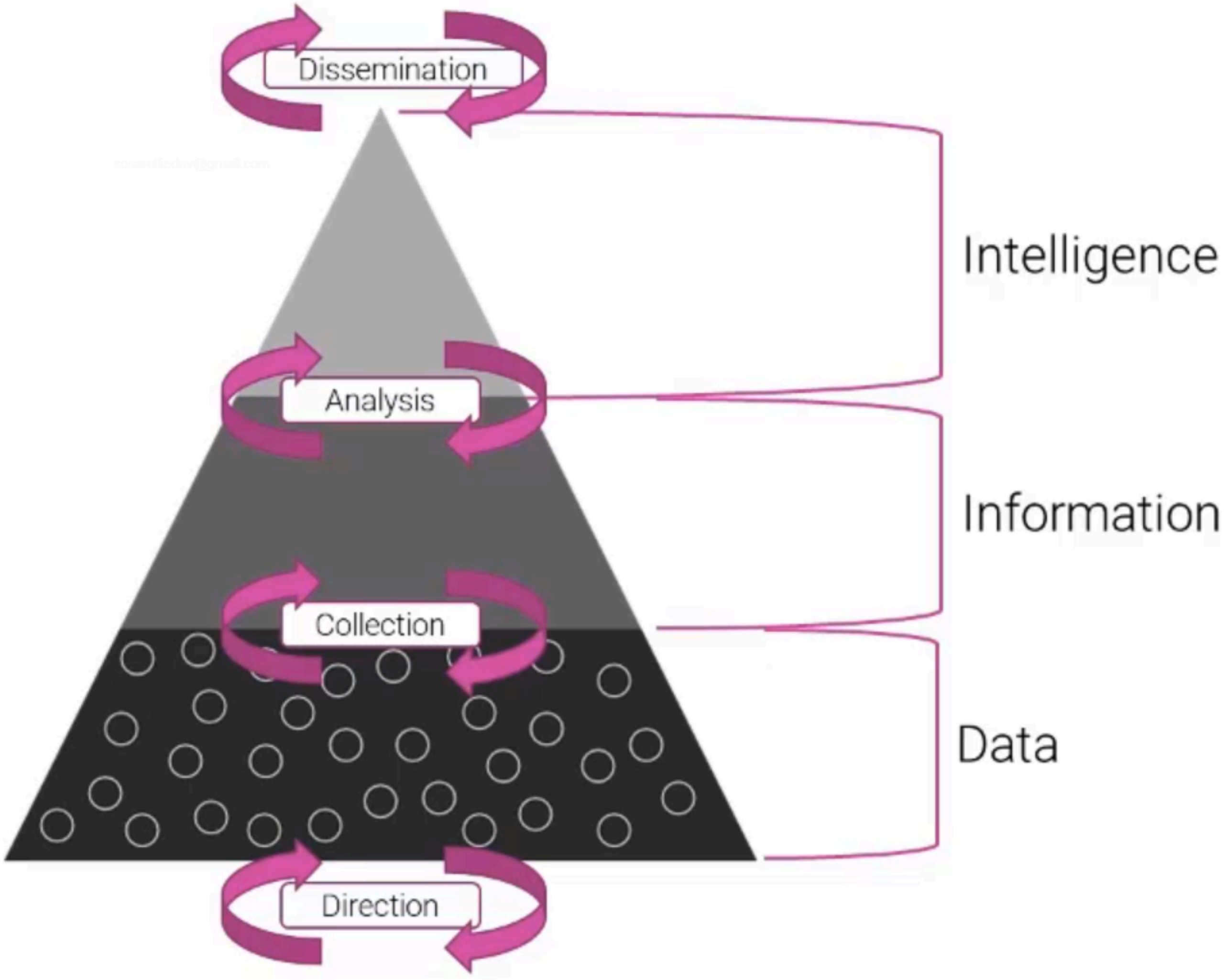
The Intelligence Cycle

The cycle starts with direction

The cornerstone of CTI is the Intelligence Cycle

- Direction
  - Where the intelligence team takes direction from the customer. - Intelligence Requirements
- Collection
  - This is where the intelligence team collects data and turns into information. - tasking to Sources and Agencies(SandA)
- Analysis
  - Where information is turned into intelligence
- Dissemination
  - This is where the intelligence is handed back to the client, which in turn stimulates new Direction

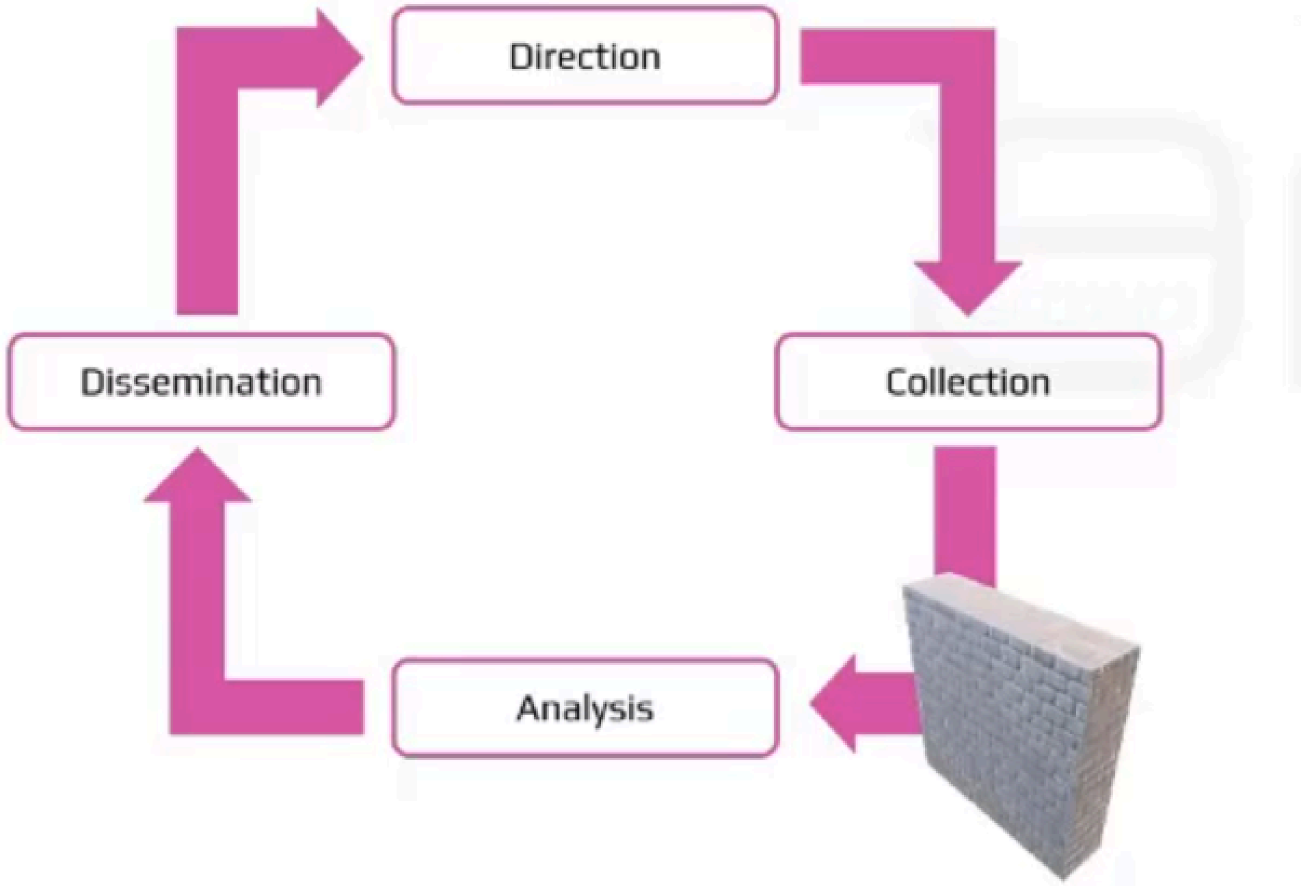
If you get the cycle right it will go on "forever"



Model integrated into pyramid

Why is it useful?

- Intelligence work can be demanding
- Many specialisations exist within each step of the Intelligence Cycle
- It is often desirable to explicitly separate the steps within the cycle - 'Sterile Corridor' (A deliberate separation between phases of the intelligence cycle, with the objective of obscuring aspects of an intelligence activity to other members of the intelligence team) - Based on a principle called Need to know and Source protection, mostly exists between the collection and the analysis phase



Sterile corridor visualized

The intelligence cycle is at the core of cyber threat intelligence because it provides a structured framework for collecting, processing, analysing, and disseminating information about potential cyber threats. The intelligence cycle and its steps can be communicated in different ways dependent on who you speak with but some of the key elements that everyone can agree with sit below:

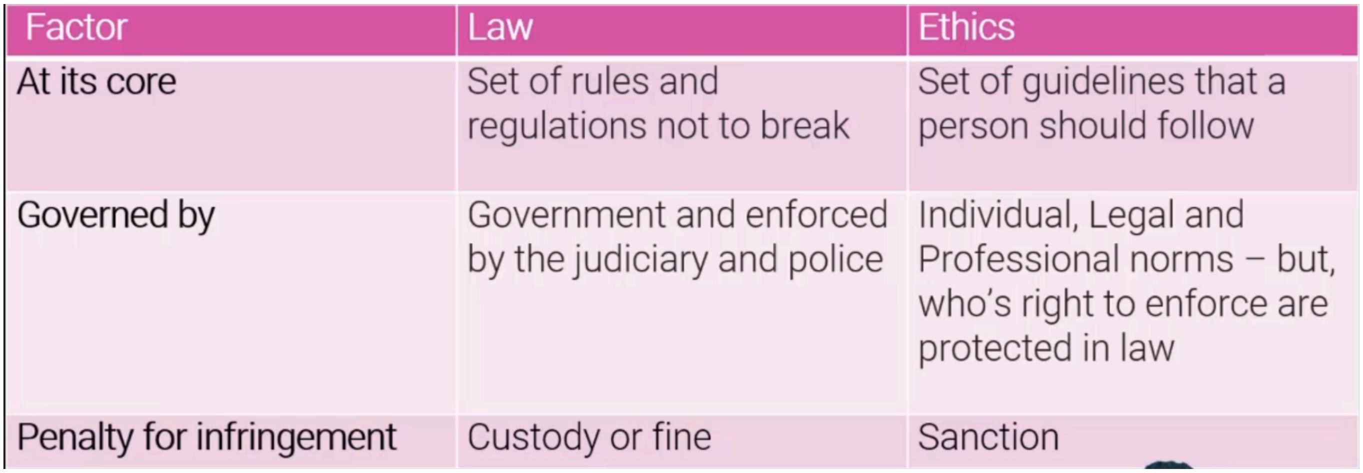
- Defining what information is needed to support decision-making and security operations.
- Gathering data from various sources, such as open source intelligence (OSINT), proprietary databases, and sensor networks.
- Converting raw data into usable information by verifying, validating, and fusing it into a coherent picture.
- Assessing the significance of the information and identifying patterns, trends, and potential threats.

- Sharing the results of the analysis with stakeholders who need it to make informed decisions and take appropriate actions.
- Using the results of the analysis to inform future collection and analysis efforts, as well as to validate the accuracy and reliability of the information.

By following this structured process, organisations can ensure that they have a complete and up-to-date understanding of the cyber threat landscape, and can take effective steps to protect themselves from potential threats.

Introduction to Law and Ethics

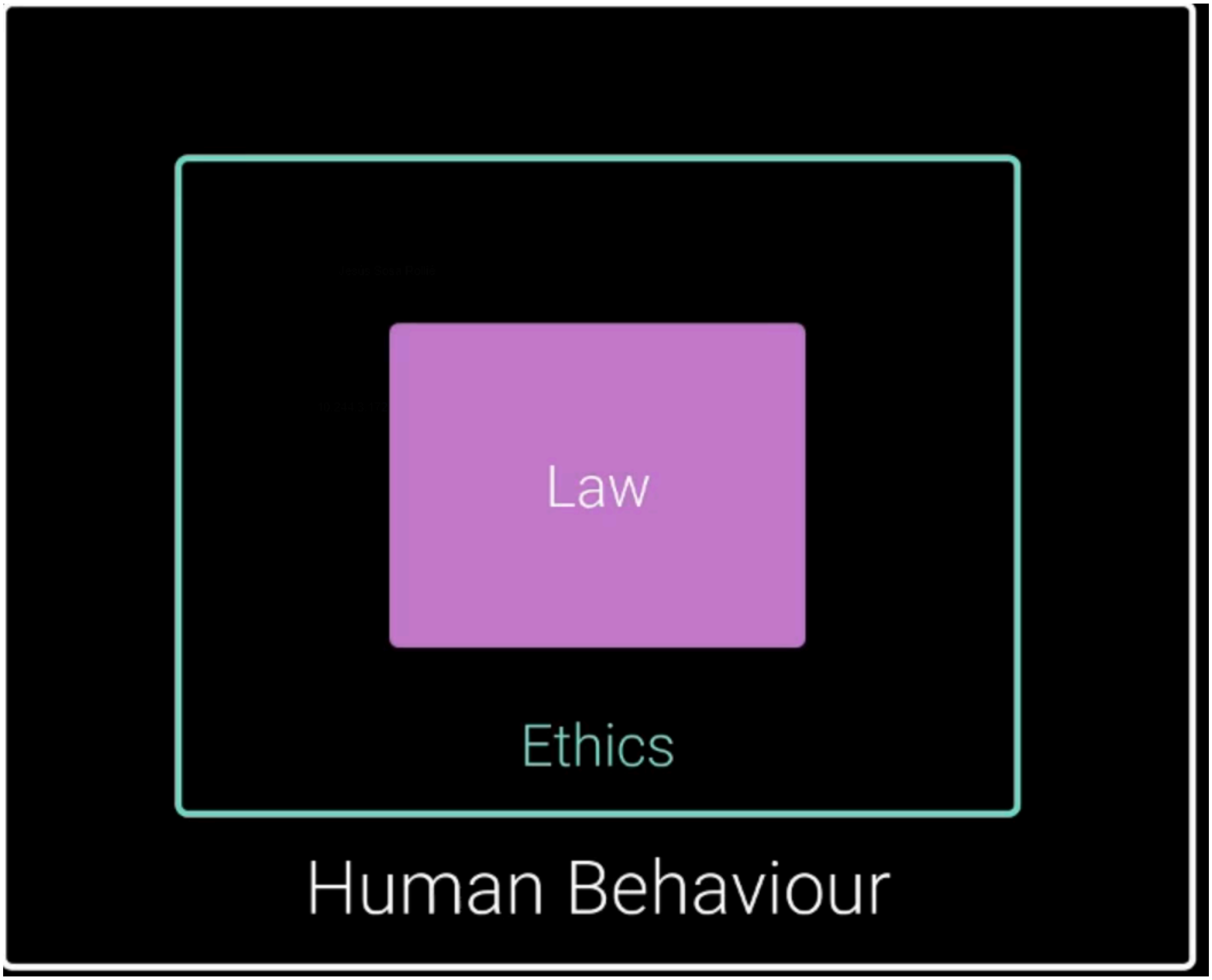
- CTI is not a regulated industry
- There are wider sets of laws that can be applied
- There's an emergent set of ethical norms that you should consider
- Difference between law and ethics



Factor	Law	Ethics
At its core	Set of rules and regulations not to break	Set of guidelines that a person should follow
Governed by	Government and enforced by the judiciary and police	Individual, Legal and Professional norms – but, who's right to enforce are protected in law
Penalty for infringement	Custody or fine	Sanction

Laws and ethics chart

Note that ethics is the collection of the community, not as individually guided as morals.



Ethics and law graphic

Specific legal articles that you should be aware of include (UK but relevant to the practice)

- Data Protection Act 1998
- Computer Misuse Act 1990
- Police and Justice Act 2006
- Bribery Act 2010
- Regulation of Investigatory Powers Act 2000
- Proceeds of Crime Act 2002
- Official Secrets Act 1989
- Telecommunications 2000
- Human Rights Act 1998

Data breaches example

- Fixture of the IT security landscape
- Happen every day and have been thousand cumulatively
- Breach victims typically invest heavily in security after a breach

- Responsible disclosure vs ambulance chasing

Responsible disclosure is, if you find something potentially sensitive about an organization and they are not your client, what do you do with that data?
Ambulance chasing is using that mechanism to try to make a sale.