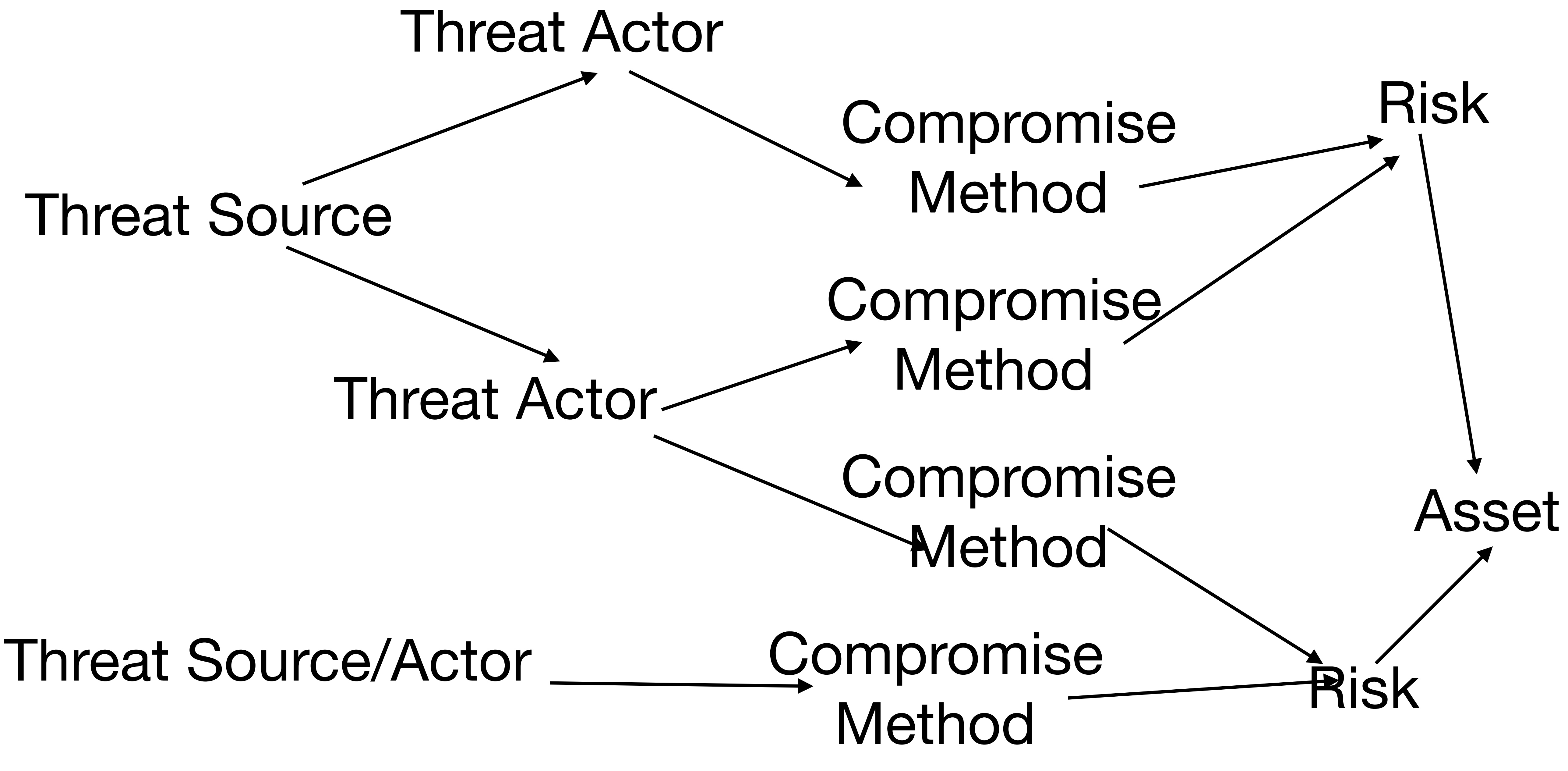
SSM Week 4: Risks and Threats

I.G.Batten@bham.ac.uk

Threats, Risks, Compromise Methods

- The language is confused, and the concepts are often treated in different ways
- I am going to use one set of definitions broadly from HMG IS1; other sources may use different definitions.
- In general:
  - **threats** are people who might do things
  - **compromise methods** are how they might do things
  - **risk** is the consequence to the defender of those things succeeding.

Overview



Threat Actor

Compromise Method

Risk

Threat Source

Compromise Method

Threat Actor

Compromise Method

Asset

Threat Source/Actor

Compromise Method

Risk

Threats

- A threat is something that an attacker ("threat actor") might attempt to do to an asset.
- One way to assess this is by looking at capability (**can** the attacker do this?) and intent (**will** the attacker do this?)
- Attackers need both to be a danger

HMG #1 says

- A **threat source** is a person or organisation that desires to breach security and ultimately will benefit from the breach in some way.
- A **threat actor** is a person who actually performs the attack or, in the case of accidents, will cause the accident.
- For example a criminal may wish to breach the confidentiality of some HMG data. The criminal wishes the breach of security to happen and thus is the threat source. If the criminal persuades a system user to release the desired information to them then the user is actually carrying out the attack. They are the threat actor.

What HMG #1 says

- The threat level is a value attributed to the combination of the capability and motivation of a threat actor or threat source to attack an asset. It takes into account any clearances that may apply to the threat actors and whether they are considered Deterrable.

Compromise Methods

- How an attacker might carry out an attack
- Can start at a high level (“Compromise Network”) and be refined to much more detailed level (“use CVE 1234 to penetrate system ABCD”).
- Only considers compromise methods that are plausible for identified threat sources.

What HMG #1 says

- A compromise method is the broad type of attack by which a threat actor may attempt to compromise the C, I or A of an asset. Once the threat actors' types have been determined it is straightforward to identify from Appendix C, the compromise methods they might use, and then consider which of those are actually plausible.
- We will look at Appendix C as an example of compromise methods on Thursday

Risks

- The risk to an asset is things that might happen to an asset, combining likelihood with impact.
- So a 1% chance per year of $10 000 of damage might be thought to be worth $100 per year (although it’s probably not as simple as that)
- Risks for ISO 27001 include things like accidental fire and flood which don’t have threat actors; **IS1 doesn’t consider this.**

HMG #1

- In general terms an information risk can be thought of as the likelihood that a threat will exploit a vulnerability leading to a business impact. IS1 aims to define all risks and estimate a risk level for each.
- Within IS1 a risk can be thought of as consisting of a number of components:
  - Threat actor and threat actor type;
  - Threat source;
  - Compromise method;
  - Property (C, I or A) of an asset … and business impact level associated with the compromise of that property.

Risk Assessment

- A Risk Assessment is a list of things that might happen to your assets, looking at likelihood and impact.
- Multiplication is OK, but breaks down for high impact / low likelihood events (cf. self-insuring)
    - Sometimes, you need to consider high impact events even if they are very low likelihood
- Idea is to weigh outcomes in the light of likelihood

But…

- Beware of claims to be precise and numeric, as there is too much uncertainty and subjecivity
- *“For the purposes of this Standard, risk level is defined on a six-point scale: Very Low; Low; Medium; Medium-High; High; Very High. The step-by-step process in Chapter 4 indicates how to estimate risk levels.”*
- Six point scale, eh?

Threat Assessment

- A threat assessment is a list of the people (groups of people) you think may attack you, looking at their capability and their motives.
- Nation states have (massive) capability, but for most people have limited intent (depends on the nation!)
- The guy you sacked yesterday has lots of intent, but probably fairly limited capability (assuming a competent exit process)

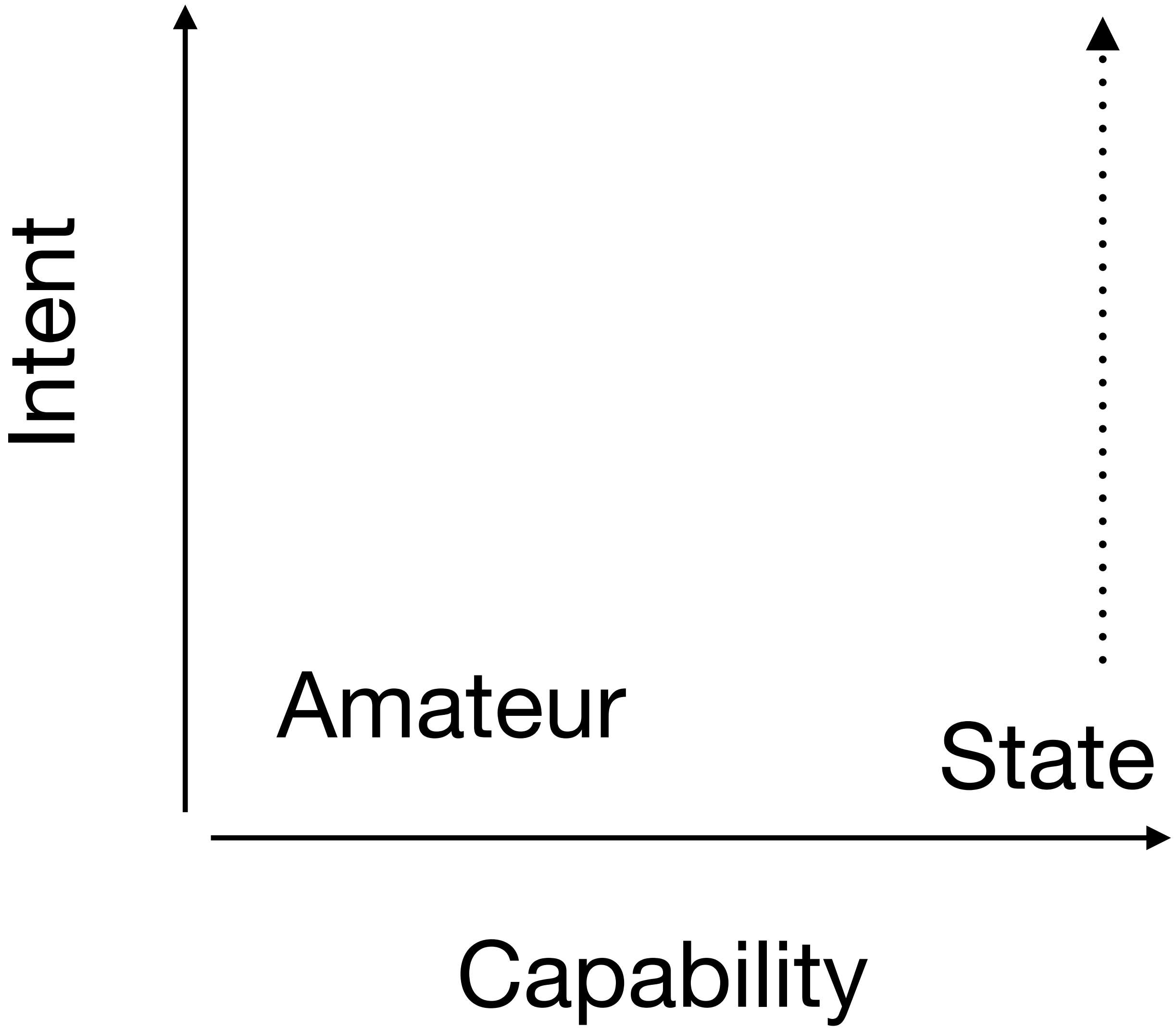
Exercise: Threat Actors

- Think about four different people or groups of people who might want to attack your business.
- Write down some statements about their capability: what can they do, and how well can they do it?
  - Think about this qualitatively (list the things) and informally quantitatively (how strong or weak?)
- Write down some statements about their intent: what might they want to do, and how likely are they to do it?

Examples

- Nation States: capability high, motive ?
- Fraud/Blackmail: capability medium, motive high
- “Script kiddies”: capability low, motive low
- Employees: capability medium, motive medium
- It’s difficult to enumerate them, isn’t it?

Examples



HMG #1 says

- Bystander (BY)
- Handler (HAN)
- Indirectly Connected (IC)
- Information Exchange Partner (IEP)
- Normal User (NU)
- Person Within Range (PWR)
- Physical Intruder (PI)
- Privileged User (PU)
- Service Consumer (SC)
- Service Provider (SP)
- Shared Service Subscriber (SSS)
- Supplier (SUP)

Bystander

- A Bystander is someone with authorised physical access to a place where the equipment within the focus of interest is located and/or account holders work, but with no business need to handle equipment or logically access the system. Typically this will include cleaners and visitors but could (for example) include hotel staff if portable equipment is left on hotel premises. (People with a need to physically handle equipment would normally be of type Handler).

Handler

- A Handler is someone whose business role requires physical access to the equipment within the focus of interest, but who is not a registered user and does not usually have logical access to the operational system, but may have temporary supervised access for test purposes. This includes people who transport equipment, test repair or replace hardware or dispose of obsolete or damaged equipment. This may also include postal or courier services.

Indirectly Connected

- An Indirectly Connected threat actor does not have legitimate or authorised business connectivity to the FoI. They may however, be able to access or make use of business or network connections because of onward connections from business partners or through networks to which the FoI has a direct connection e.g. the Internet. Where Departments have direct or indirect connections to the Internet this threat actor type could include all Internet users. This indirect connectivity could allow threat actors to mount business traffic-borne or network based attacks against the FoI.
- (FoI => Focus of Interest)

Information Exchange Partner

- An Information Exchange Partner is someone who needs, as part of their business, to exchange information with the focus of interest, whether through direct or indirect electronic connection or media exchange. The person may be an originator, recipient or both, of information in support of normal business. Note there must be a need to exchange information, not merely an ability to exchange information; people with the ability but not the need are Indirectly Connected.

Person Within Range

- A threat actor of type Person Within Range is someone who is in range of electronic, electromagnetic and any other emanations from the equipment within the FoI. This applies whether the emanations are unintentional, intentional or as the result of tampering, and hence is very broad ranging. In addition this threat actor type due to their presence within range of emanations, transmissions and communications may be in a position to jam communication paths. This type could be considered as including people who may:
- (TEMPEST, radio attacks, etc)

Normal User

- A Normal User is a registered user or account holder who uses the applications, services and equipment within the FoI to store, process, handle and exchange information in support of business objectives. These users would be provided with ‘standard’ facilities and system privilege as defined in the Departments [sic] policy.

Physical Intruder

- A Physical Intruder is someone who gains unauthorised physical access to equipment within the FoI, typically by breaking in to the premises in which the FoI equipment is sited. This may include the traditional office, data centres or locations where remote working is carried out.

Privileged User

- A Privileged User is a registered user or account holder who manages the applications, services, equipment and security defences within the focus of interest. A threat actor of this type can usually not be constrained in the same way as a Normal User and as such is modelled as a separate threat actor type.

Service Provider

- A Service Provider is someone who provides services to the FoI, including but not limited to, communications, shared databases, Internet access, web-site hosting, resource sharing, archive services or intrusion detection services and who by virtue of controlling that service could compromise any Security Property of the FoI.

Service Consumer

- A Service Consumer is someone who makes use of services advertised or provided by the FoI. Services provided by the FoI may require that consumers are registered for access control purposes or allow unregistered physical or logical access to a publically available service (e.g. an Internet website or ‘walk in’ kiosk). Service Consumers may use services provided by the system (such as view a website) but are not Normal Users.

Shared Service Subscribers

- A Shared Service Subscriber applies only where a shared service is within the reliance scope. A Shared Service Subscriber is someone who is an authorised user of services used by a FoI, but who is not a registered user of systems or services within the FoI. This threat actor could compromise the FoI by attacking the shared service. For example, a FoI may rely upon a shared service such as power distribution. If actions of other customers of that power distribution network make in unavailable, this could in turn affect availability of the FoI.
- Could this cover cloud tenants?

Supplier

- A threat actor of type Supplier is someone in the supply chain who provides, maintains or otherwise has access to software or equipment. This threat actor type may be aware of the system and its security characteristics and be in a position to provide equipment deliberately modified or configured to allow or facilitate compromise of any security property.