1495 UNIVERSITY OF ABERDEEN

CELEBRATING
525 YEARS
1495 – 2020

ABERDEEN 2040

Network Security Technology

Security management

September 2025

Outline of lecture

1. Motivation.
2. Governance.
3. Concepts.
4. Standardisation.
5. Risk.
6. C.I.A triad.
7. Management of people.
8. Human issues in control.

What you need to know and how you manage it all

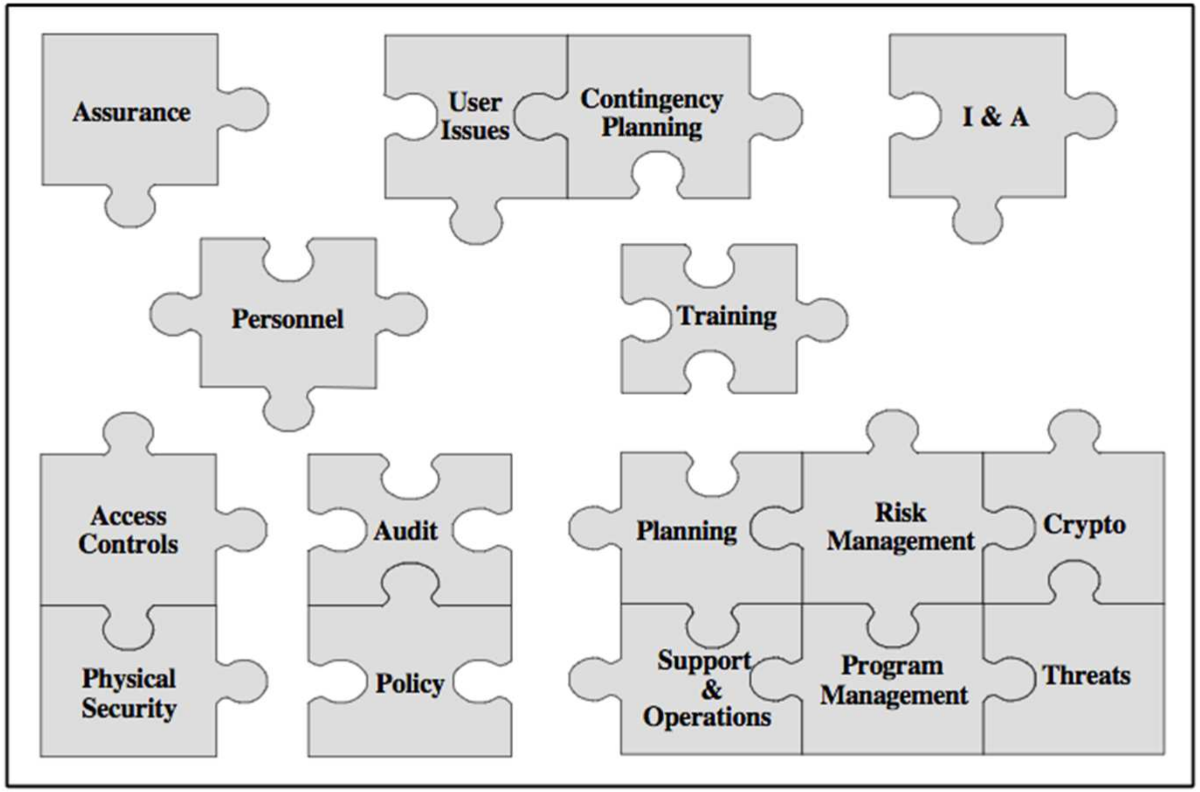


Figure: [NIST SP800-12]

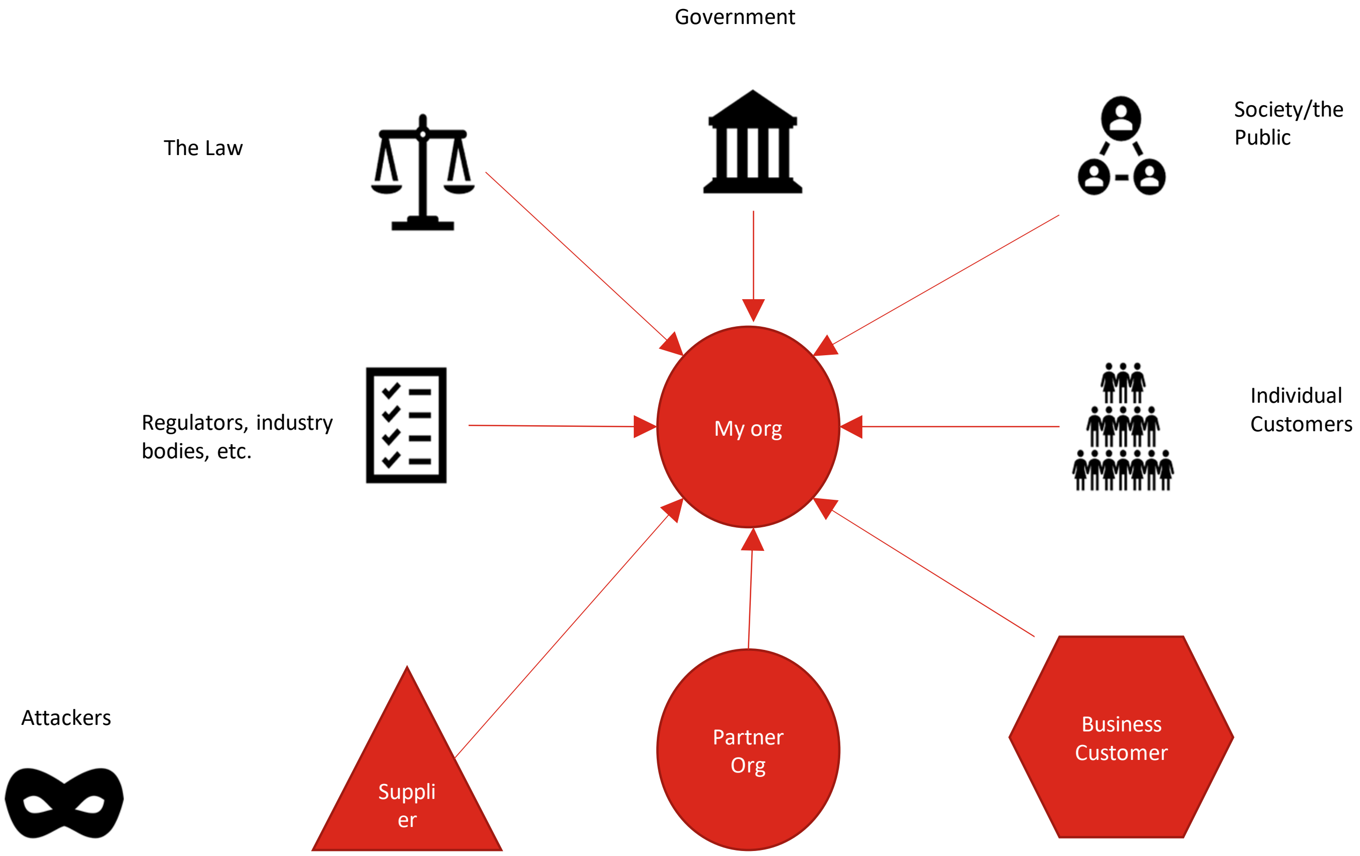
Objective and a motivating question

1. The objective for these lectures is to think about protecting an organization. The organization is presumed to be not very small.
2. Suppose that you were in charge of the cybersecurity for a large organization. Where would you even start?

Context: a top-down approach

1. IT systems are part of larger organizational systems:
    1. IT hardware and software.
    2. People (and other resources).
    3. Business processes.
2. Organizations are embedded within a larger eco-system:
    1. Customers
    2. Other organizations (as suppliers and customers)
    3. Attackers who want to disrupt our processes.

Context: ecosystem



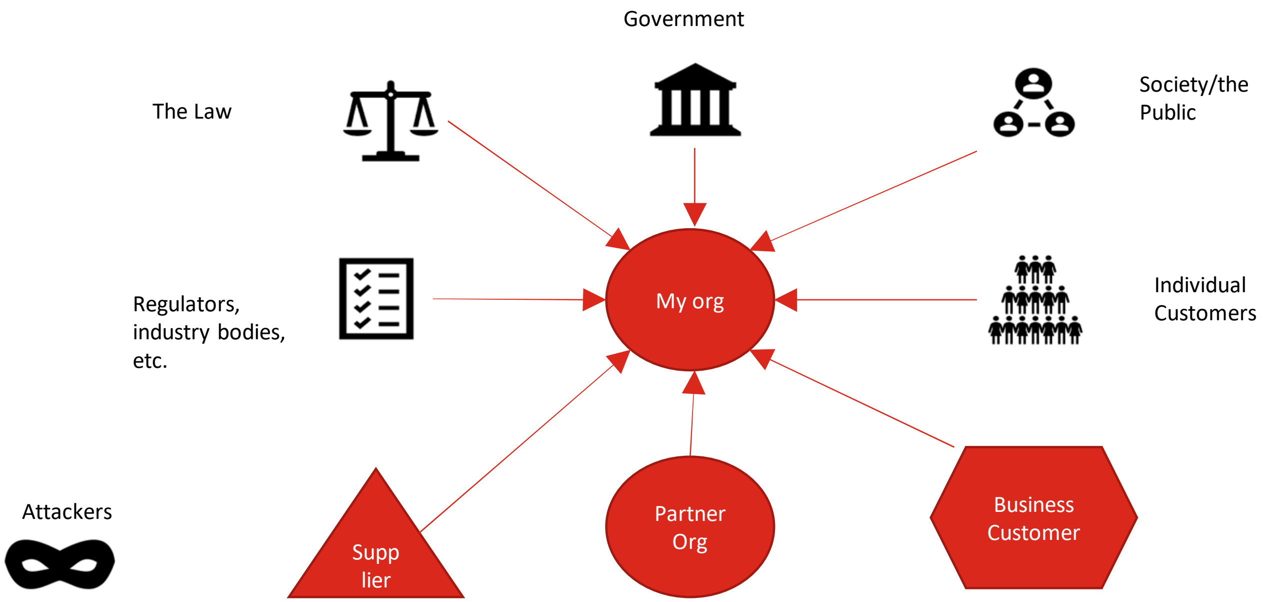
To achieve security for the organisation…

1. We need to **secure our business processes** (inc. services & supporting tech.):
    1. Cost to us, and value to attacker, often depends on disruption.
2. We need good **business processes for security**. Examples include:
    1. Ensure that standard security controls are applied (e.g. device configuration, patching).
    2. Network monitoring, use of monitoring, reporting.
    3. Incident management.
    4. User training, information, alerts, …
3. We need to **make best use of our resources:**
    1. This includes getting people, ordinary users and IT administrators, to make the best security decisions and to act securely.
    2. We also need to orchestrate (coordinate) their actions.

Motivation

1. Much of this is broadly about **security management**. This is the point at which technical security meets management.
2. Many jobs, and many of the most highly paid jobs, in security are in security management.
3. Security managers often:
   1. orchestrate the use of resources,
   2. run the people who run the security operations,
   3. assess risk, and are a key part of decisions about where to put protection efforts,
   4. make resourcing and strategic recommendations to `top management' relating to security.

Governance



1. **Top managers** and **governors** (these are sometimes different roles) of an organization have overall responsibility for ensuring that an organization is dealing with security appropriately.

Governance (cont'd)

1. Governance requires delivery of **value** to the business from IT investments, and oversight of **risk**.
2. The organization needs to balance **opportunity** against **risk**.
3. Security helps to manage risk, but security needs to be of value.

risk
opportunity

Challenges to maintaining the right balance

1. **Opportunity costs**:
    1. Risk reduction from security needs to be balanced against loss of opportunity as side-effects of security controls.
2. **Investment trade-offs with short-run vs long-run returns**:
    1. Investment in security needs to be of value.
    2. In the short-term, investing in security often means not investing in something else.
    3. The value of security might only be estimated over the longer term.
3. **Observability of benefit**:
    1. The value of security is often not fully observable.
    2. For example, if an attack is deterred by a control, then we may never know how bad things might have been without it.

What is data protection?

"Data protection is the fair and proper use of information about people. It's part of the fundamental right to privacy – but on a more practical level, it's really about building trust between people and organisations. It's about treating people fairly and openly, recognising their right to have control over their own identity and their interactions with others, and striking a balance with the wider interests of society."

- Source: https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-dpa-2018/some-basic-concepts/#1

GDPR: General Data Protection Regulation

1. Law that applies across the EU and the UK.
2. Addresses processing of personal data.
3. Very large fines are possible for non-compliance.
4. Now drives a lot of security investment!
5. In the UK, the relevant governmental body is the **Information Commissioner's Office** (**ICO**).

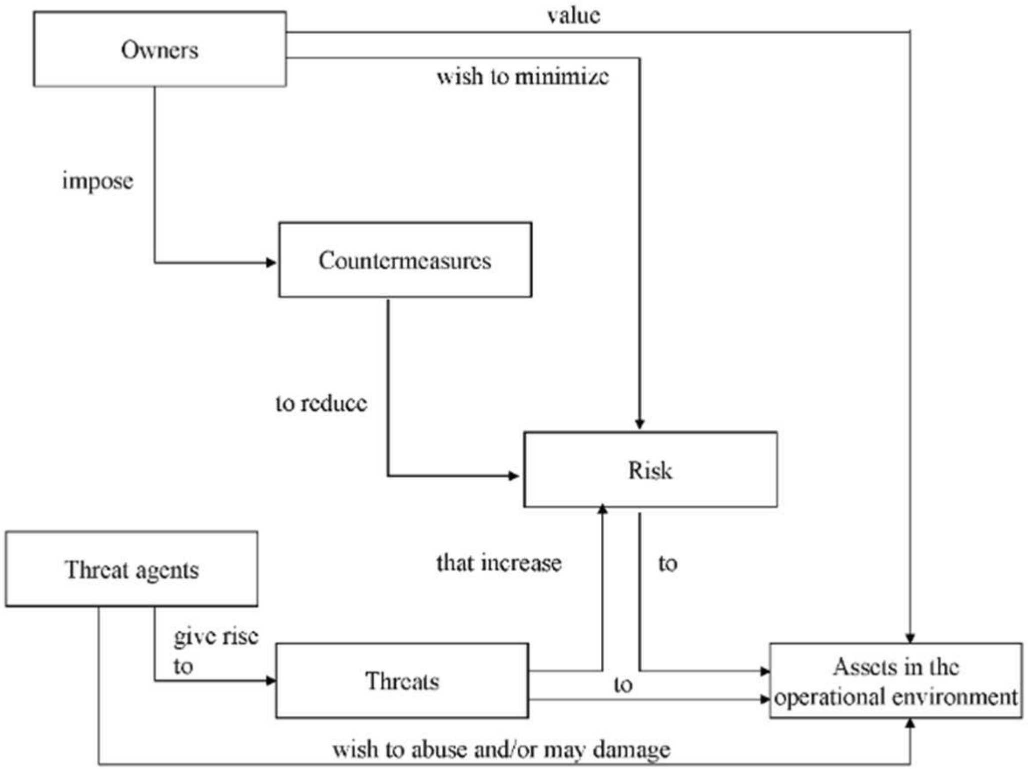
Standardisation

1. People in security management try to work with standardized terminology.
2. This is to try to be clear about objectives, descriptions of the current state, etc.
3. The reason to be clear is to minimize confusion, since multiple people will be involved in security tasks and operations. Confusion could lead to vulnerabilities arising or attacks not being addressed quickly.

Common (criteria) language

1. **Assets** are things owned by some **owner(s).**
2. They have some **value** to the owner.
3. **Threats** are posed to assets by **threat agents.**
4. The owner thus carries some **risk** (associated with the asset) if there is a threat to the asset.
5. Owners use **countermeasures** (**controls**) to mitigate the risk.

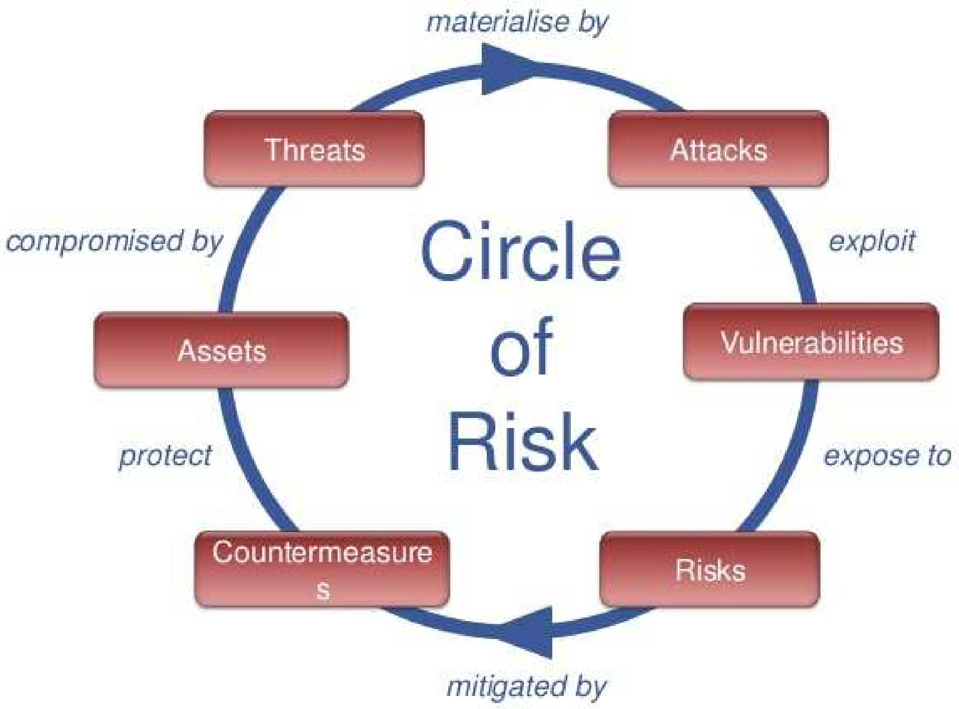
Common criteria ontology for risk etc.



Vulnerabilities, exploits and attacks

1. A **vulnerability** is a potential way into a system.
    1. These often start with **defects** and **bugs** in systems and software.
2. An **exploit** is a way of using that way in.
3. An **attack** implements the exploit and seeks to get into the system.

The “cycle of risk”



Risk

1. Risk is the potential for harm.
2. It might be justified to take a risk, by opportunity or necessity.
3. Risk includes the harm/impact if the event occurred, and the chance of occurrence.

The risk equation

$$\boxed{\text{Risk} = \text{Impact} \times \text{Probability}}$$

1. This equation/definition encapsulates many underlying ideas about the risk of an event.
2. It isn’t always exactly the concept needed, but it is a useful starting-point and you should remember it.
3. Note that you have two ways to reduce risk of an event: reduce the impact or reduce the probability.

System and information risk

1. Decompose risk into two concepts.
2. **Information risk**:
    1. Risk to the information itself.
3. **System risk**:
    1. Risk to information processing systems, machines, networks, communications, processes.

The C.I.A triad

1. Core concepts of information security:
    1. **Confidentiality.**
    2. **Integrity.**
    3. **Availability.**

Extending C.I.A to the Parkerian Hexad

1. **Authenticity:**
   1. Is the information authentic?
   2. Does it come from the purported source?
2. **Possession** (a.k.a. **Control**):
   1. Somebody may have possession of your data but may not look at it.
   2. Is your confidentiality breached?
3. **Usefulness (**a.k.a. **utility):**
   1. Your data might be securely encrypted, but useless if the encryption key is lost.

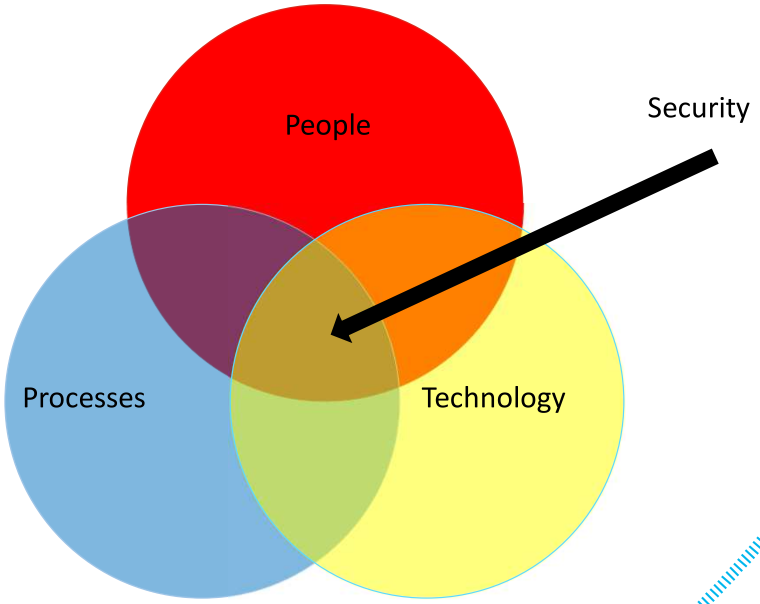
Sensitivity and Criticality (S.C)

1. The S.C approach to information assurance focus not purely on properties of resources (like C.I.A), but rather on how information resources relate to the function of a business (or other entity).
2. This might sometimes be more useful language than C.I.A for thinking through the relation of security to business function.
3. **Sensitivity**: *"A measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection."*
4. **Criticality**: *"A measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function."*

Sources: NIST SP800-60: Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories

People, process and technology

1. Achieving security involves properly coordinating:
    1. **People,**
    2. **Process**, and
    3. **Technology**.
2. In the end, a lot of management is about managing people.
3. This raises a great many human issues in security.

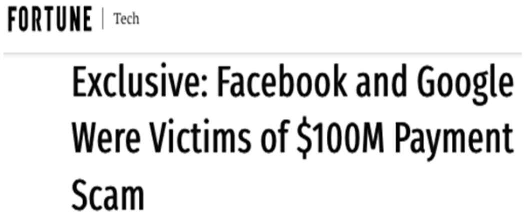


ABERDEEN 2040

High-impact attacks

Russia was behind 'malicious' cyber attack on Ukraine, Foreign Office says

2018

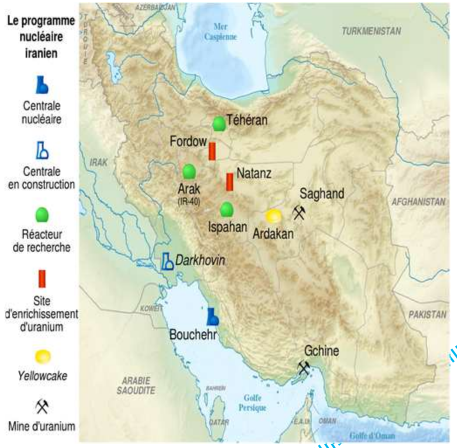


FORTUNE | Tech

Exclusive: Facebook and Google Were Victims of $100M Payment Scam

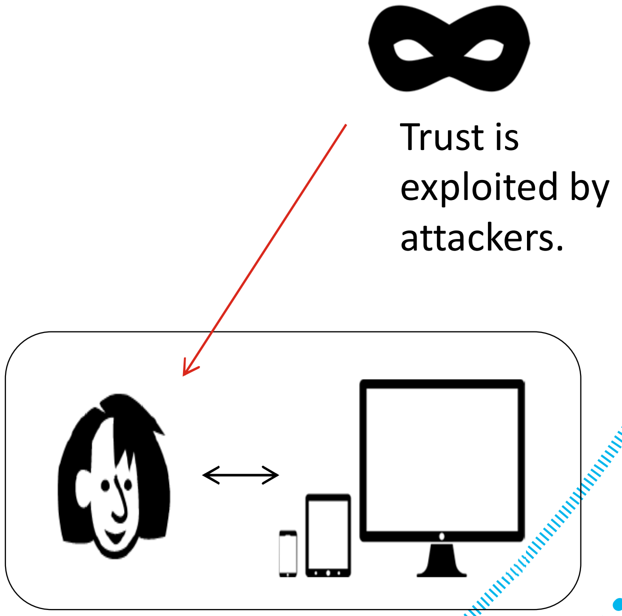
Target Agrees to Pay $18.5 Million to End Data-Breach Probes

Booz|Allen|Hamilton
Edward Snowden
Sys Admin
TOP SECRET CLEARANCE



Why employee behaviour matters

1. People are part of the attack surface of organizations:
    1. Trusted use of IT systems
    2. Trusted management of IT systems
    3. Trusted roles in workflows
    4. Trusted communications.
2. *Sometimes* people are the weakest link:
    1. Can be deceived
    2. Mistakes, accidents
    3. Are almost set up to fail in a poor environment: policy, support, …
    4. Insiders.



Trust is exploited by attackers.

Human issues in control

1. We need to be aware of human limitations and human behaviour when selecting controls and managing people.
2. How will behaviour change within the people, process, technology environment if we change a control?
    1. Example: password complexity or frequency of change.
3. Will it result in a net gain in security?
4. What will be the net effect on productivity of the organization, or on the work environment?

From management science to behavioural science

1. To manage people effectively for security, we'd like to understand and be able to predict their behaviour under the application of different security controls.
2. This suggests input from the behavioural and social sciences, particularly psychology.
3. There are many relevant theories to draw on for ideas, but it often remains difficult to predict behaviour in new contexts.

Determining behaviour

1. The COM-B model and Behaviour Change Wheel [BCW] is one theory of the determinants of behaviour, rooted in a systematic review of many other theories.
2. Used for understanding things like controlling smoking and diet. Similarities with an older criminological theory.
3. It posits the three determinant types for behaviour:
   1. **Capabilities** (physical, psychological).
   2. **Opportunity** (physical, social).
   3. **Motivation** (reflective, automatic).

Capability issues: Examples

1. Does a user have fingerprints for a biometric system? Can a user remember a random 26-character password?
2. Can users detect the difference between phishing and legitimate emails?
3. Can users properly apply encryption tools that require significant manual configuration and input?
4. Do admins have enough understanding to enable them to make the right choices about automated security settings?
5. What skills and knowledge does an attacker need to exploit a vulnerability?

Opportunity issues: Examples

1. Does a user have time to think about whether email attachments might be a security risk?
2. Does an admin have time to properly configure security settings?
3. Does a user know of a security policy that says that certain sensitive information cannot be taken off site?
4. From the attacker perspective, are there vulnerabilities to exploit?
5. Does an insider have access to unlocked machines?
6. Is there a time that the attacker can launch an attack, and be likely to succeed or not be detected?

Compliance from the user perspective

1. Must be aware of compliance situation (opportunity).
2. Must be given time and resources to comply (opportunity).
3. Must be able to be aware (capability).
4. Must be able to understand how to comply (capability).
5. Must know how to comply (capability).
6. Must have the skills to comply (capability).
7. For automatic behaviours, user environment must be configured correctly ("motivation")
8. For reflective behaviours, must invest time and resources in complying, choosing over other activities (motivation).

Issues with motivation

1. Is a user interested in protecting the organization? Are they aligned in that respect?
2. Does a user believe that their management really cares enough about security for it to be a problem if the user does not comply with security policy?
3. Is an employee motivated to become an insider attacker? Greedy? Angry? A vandal?

Human limitations: awareness issue and error

1. Are users adequately aware of security risks?
2. How likely is it that users know enough to enable our controls to be effective?
3. **Humans** make errors and security mistakes.
4. How tolerant are our systems to the following:
    1. Prediction?
    2. Detection?
    3. Containment?
    4. Procedures for self-reporting of error?

Human limitations: usability

1. Do our controls make it very difficult or time-consuming for users to accomplish their primary tasks?
2. Do they make reasonable demands on user’s cognitive, physical and social abilities and attributes?
3. Do they support users to make the right security decisions?

Motivation, task priority and usability

1. For most users, security is a **secondary task**, not a **primary task**. That is, they are required to "do" security simply in order to enable them to be allowed to get on with their primary task:
    1. Security will not interest many/most users.
    2. Many users will understandably find security an irritation as it may be perceived to be getting in the way of their primary task(s).
2. Possible solutions (may or may not be feasible and work):
    1. Make controls near-invisible to the user.
    2. Make controls usable and unobtrusive.
    3. Change user perceptions (e.g., of security within task structure).
3. *Sometimes* there may be unavoidable **trade-offs** between security and usability of systems.
    1. A decision must be taken about balance.

Accountability

1. Without accountability, it is hard to ensure that people will behave appropriately.
2. We often have the technical means for “accountability”. We have logs relating to the usage of systems, including user authentication and access control logs.
3. However, meaningful accountability still requires:
    1. The ability to prove that actions were really performed by some individual with sufficient certainty, and this may require forensic investigations, and
    2. Organizational (and legal) policies and HR/personnel processes that do hold individuals accountable for inappropriate actions.

Culture

1. Each organization has a different culture.
2. This is especially true for security.
3. Examples:
   1. Is tailgating (right) acceptable?
   2. Is it normal for users to be expected to report phishing emails?
   3. Do users share authentication credentials?
   4. Is usage of work IT equipment for personal purposes acceptable?
   5. Do users even believe that security is significant to their role?

NO
TAILGATING
Each person must present his/her Apple I.D. Badge to the card reader to confirm valid access.

Employee expectations

1. People have rights as employees and individuals (under the law).
2. They have contracts of employment.
3. They have expectations within the organizational culture.
4. Security policies and processes will need to work alongside these constraints, e.g.
    1. Can’t use arbitrary force to secure physical site.
    2. Can’t arbitrarily dismiss someone on suspicion without evidence.
    3. Monitoring of employees while at home is likely not acceptable.
    4. May not be acceptable to ask employees to spy on their co-workers.
    5. May have to balance accessibility against security or make adjustments in security systems.
    6. Is it reasonable to force reset of an employees’ personal phone if they agree to use work email from it and a risk is detected?

Ethics

1. In some cases, the law delimits what you can’t do in managing employees.
2. In some cases, social norms, and the potential cost of violating them may constrain management.
3. In other cases, **ethical considerations** may play a role:
    1. E.g., even if you are allowed to monitor employees’ use of IT equipment at home, and there are no clear social norms relating to this, *should* you do it, from an ethical perspective?
    2. How do you deal with matters if you find out they visited a porn or other risky site?

Frameworks, guidelines and standards

1. One tool for handling the complexity of security management is to follow external frameworks, standards and guidelines.
2. There are major standards for security management such as ISO27001, as well as overlapping standards for other things (IT governance, security architecture, business continuity).
3. An organization can use these in two ways:
    1. As guidelines (to help them).
    2. As something to be certified against by an external auditor.
4. Most large organizations will be following major standards in structuring their entire management process.

Baselines and risk approaches to control choice

1. There are two basic approaches:
    1. Apply a set of **baseline controls** that almost every organization uses to meet similar security objectives (follow `**best-practice**’).
    2. Use **risk management** to provide additional insight into which controls really need to be used and what type of implementation should be chosen.
2. Which approach is better is controversial, and many real standards and organizations mix-and-match both**.**

Policies

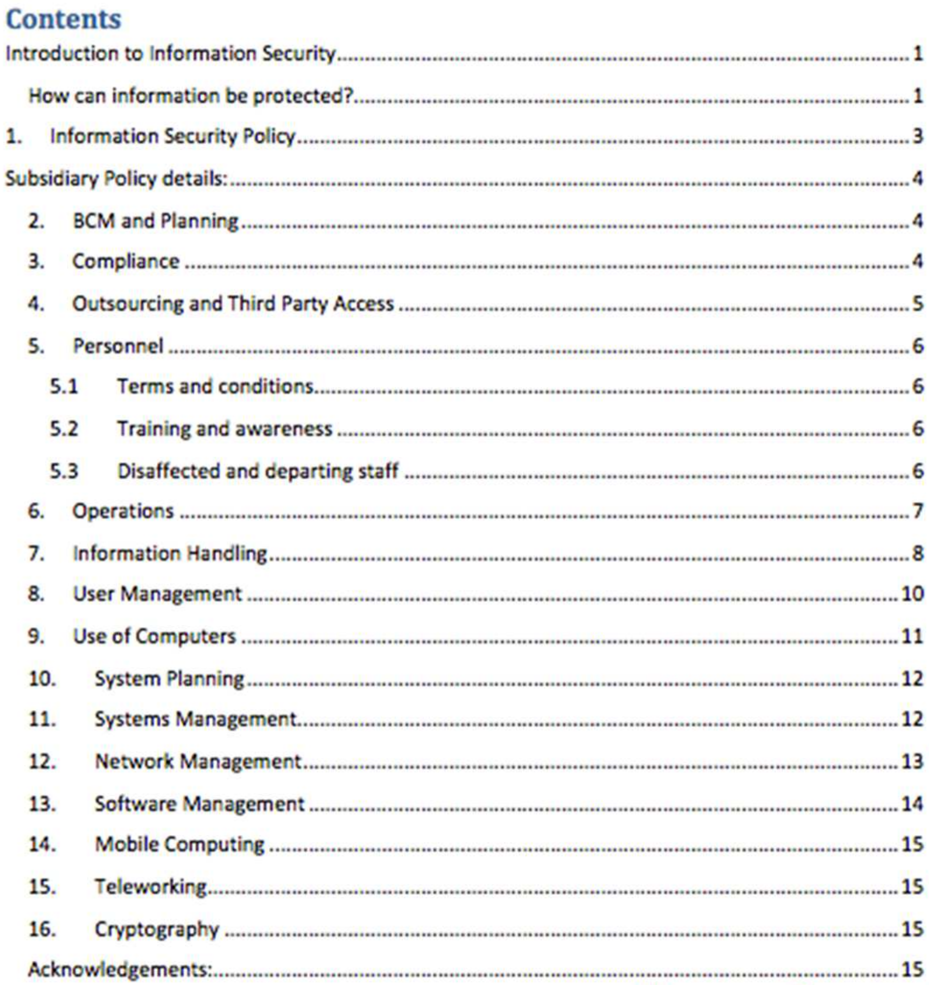
1. An organization will likely need its own policies in addition to following external frameworks and guidelines.
2. These are usually collated in a set of documents that state *the* security policy.
3. Frameworks like ISO27001 require there to be a policy.
4. These policies are not the same thing as automated security policies (firewall rules, access control rules, etc.) although the automated policy should really align with the organizational policy.

Typical security policy contents

1. **Security policy objectives**:
    1. Statement of intent to provide security for particular resources.
2. **The security policy:**
    1. A statement that defines the security policy objectives of an organization
    2. It must state what needs to be protected
    3. The security policy will often also indicate how this is to be done, including what controls are to be used, but most often not in complete detail.

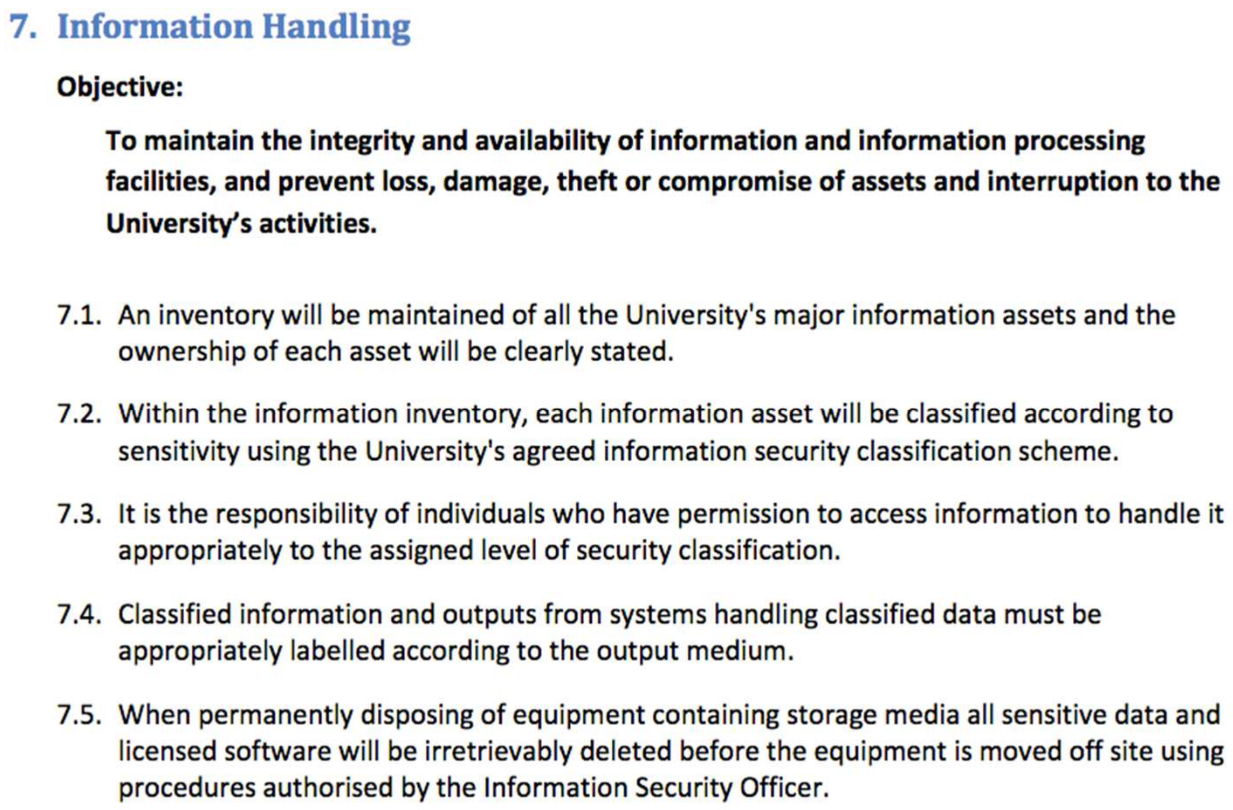
Policy example

- UoA Information Security Policy (2015, now withdrawn and updated)



Contents

Policy example: information handling



7. Information Handling

Objective:

> **To maintain the integrity and availability of information and information processing facilities, and prevent loss, damage, theft or compromise of assets and interruption to the University's activities.**

7.1. An inventory will be maintained of all the University's major information assets and the ownership of each asset will be clearly stated.

7.2. Within the information inventory, each information asset will be classified according to sensitivity using the University's agreed information security classification scheme.

7.3. It is the responsibility of individuals who have permission to access information to handle it appropriately to the assigned level of security classification.

7.4. Classified information and outputs from systems handling classified data must be appropriately labelled according to the output medium.

7.5. When permanently disposing of equipment containing storage media all sensitive data and licensed software will be irretrievably deleted before the equipment is moved off site using procedures authorised by the Information Security Officer.

Problems with policy

1. Is it ambiguous or vague?
2. Is it self-contradictory?
3. Is it feasible?
    1. Is it resourced?
    2. Is it **usable**?
4. Who is going to read the policy document?
5. Who is going to understand it?
6. How can you align individuals, and the culture, with the policy?

Policy compliance

1. A policy isn’t much use if people don’t comply with it.
2. If people don’t comply, then processes and technology security controls will often fail.
3. Examples:
    1. Cryptographic keys are not handled properly.
    2. Hosts are not up-to-date and fully patched.
    3. Business processes are using software and services that have not been through procurement processes (including security vetting).
        1. E.g. `Shadow IT’: a business unit is using a cloud IT service without authorization, and this subjects the organization to unknown and uncontrolled risk.

Compliance in the round

1. Compliance is good:
   1. Ensures baselines applied. E.g., Every security control on a check-list is applied.
2. Compliance is not enough:
   1. People and organizations stop thinking, and just comply at the minimum level with the letter of the policy.
   2. E.g., Your server room has a door and a certain grade of strong lock on the door because the standard says so. It also has an open window ..
   3. Your data is encrypted by AES 256 in GCM, but the keys are not kept securely.
   4. Danger: stop thinking about risk and being accountable; just follow check-list.

Procedures

1. Procedures are simple routines that can be run, with limited thought.
2. Examples:
    1. How to report or respond to a security incident.
    2. How to properly acquire and secure data for forensics.
    3. What to do if encrypting ransomware is suspected.
    4. Steps to secure your personal machine for home working.
    5. How to encrypt or append a digital signature to an email.
3. Advantage: usually reduces the chance for mistakes; makes compliance easy.
4. Problem: Non-standard situations do arise (e.g., zero-day malware), and may be mistaken for standard ones.

Security awareness, education and training

1. We can support good security behaviour and compliance by campaigns and programmes aimed at delivering to users:
2. **Awareness**: users and administrators need to be aware of risks
3. **Training**: Provide specific instruction on what to do in particular situations (e.g., how to report incidents, or how to use secure software to complete a task).
4. **Education:** Support the development of insight into risks, and how to mitigate them.

ABERDEEN 2040