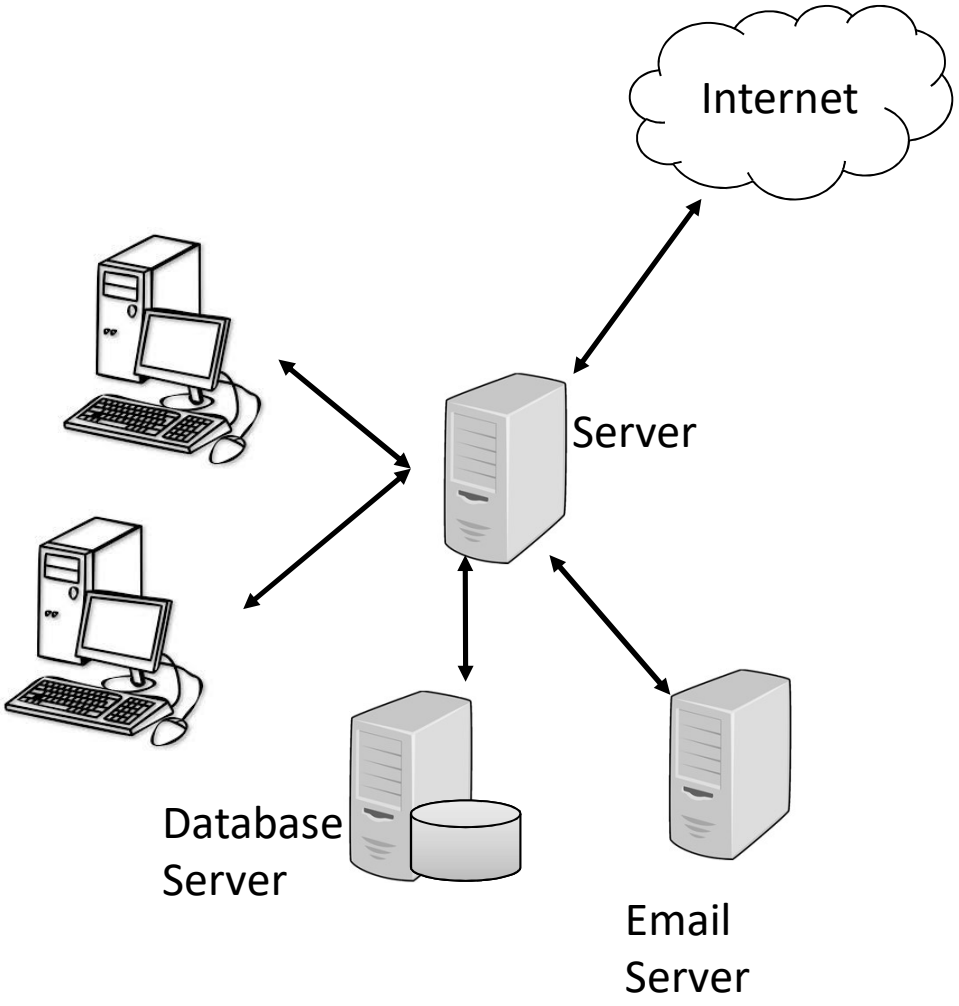
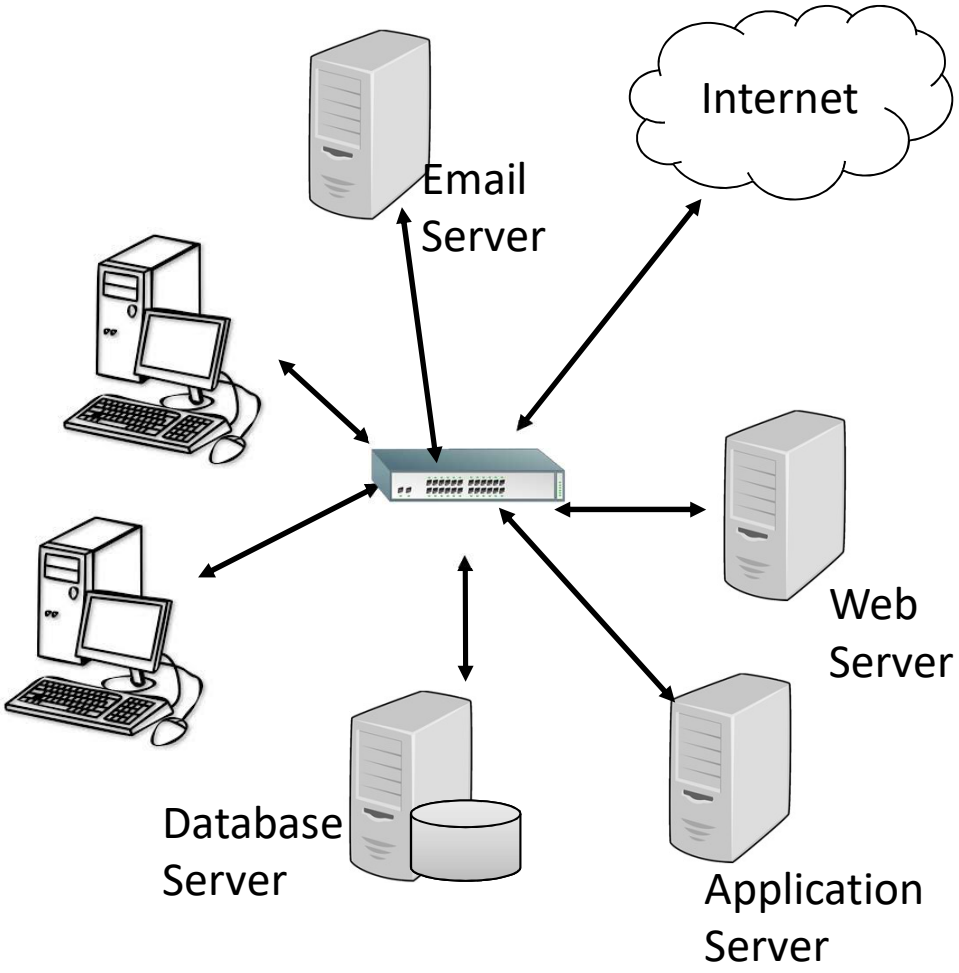
CMT116 Business and Security

Threats to Business



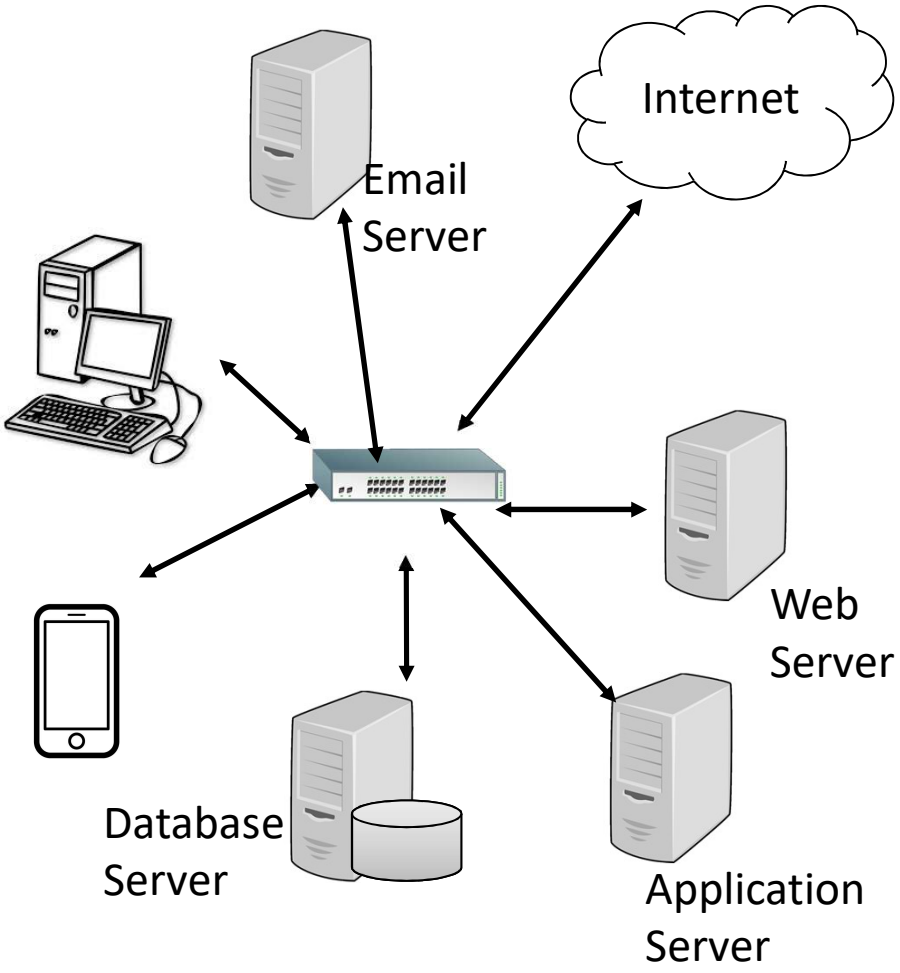
- Employee are more like to be hit by Email Threat
  - Phishing (1 in 3,207)
  - Spamming (55% of email analysed by Symantec in 2018 as spam)
  - Email – can be of two type, as attachment or as link. Microsoft Office users are the most at risk of falling victim to email-based malware, with Office files accounting for 48 percent of malicious email attachments.
- Malware Threat
  - Self propagating financial trojans (Emotet and Qakbot)
  - Execution of Powershell Script such as VBS.Downloader and JS.Downloader
- Cryptojacking – Ransomware.

Threats to Business



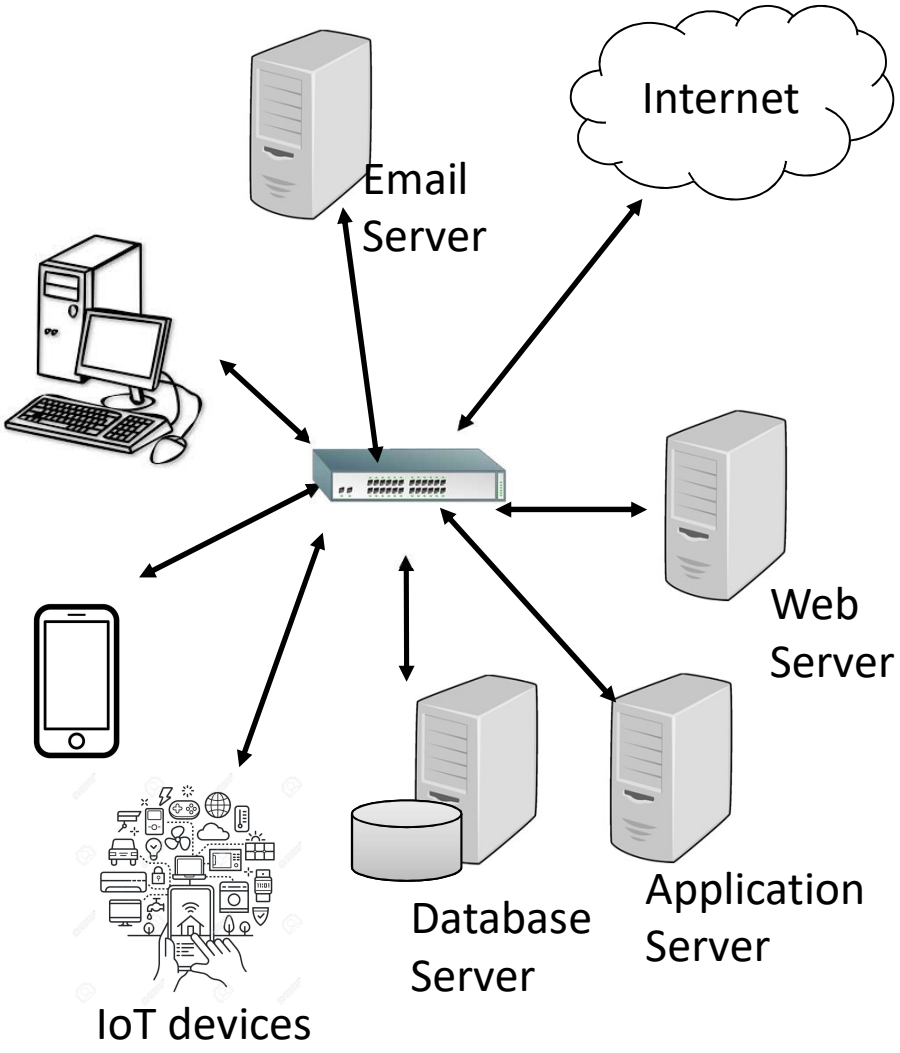
- Web attacks
  - 1 in 10 URL pointing to malicious web server
  - 1.3 million unique web attacks reported by Symantec in 2018
  - Exploit Kits to carry out web attacks
  - On average 4,800 website compromised by Formjacking.

Threats to Business



- Mobile malware
  - Ransomware for mobile. (63% of companies in US got affected by ransomware malware)
  - 1 in 36 devices in organisation were considered as high risk. Why ?
  - Devices that were rooted or jailbroken, along with devices that had a high degree of certainty that malware had been installed.

Threats to Business

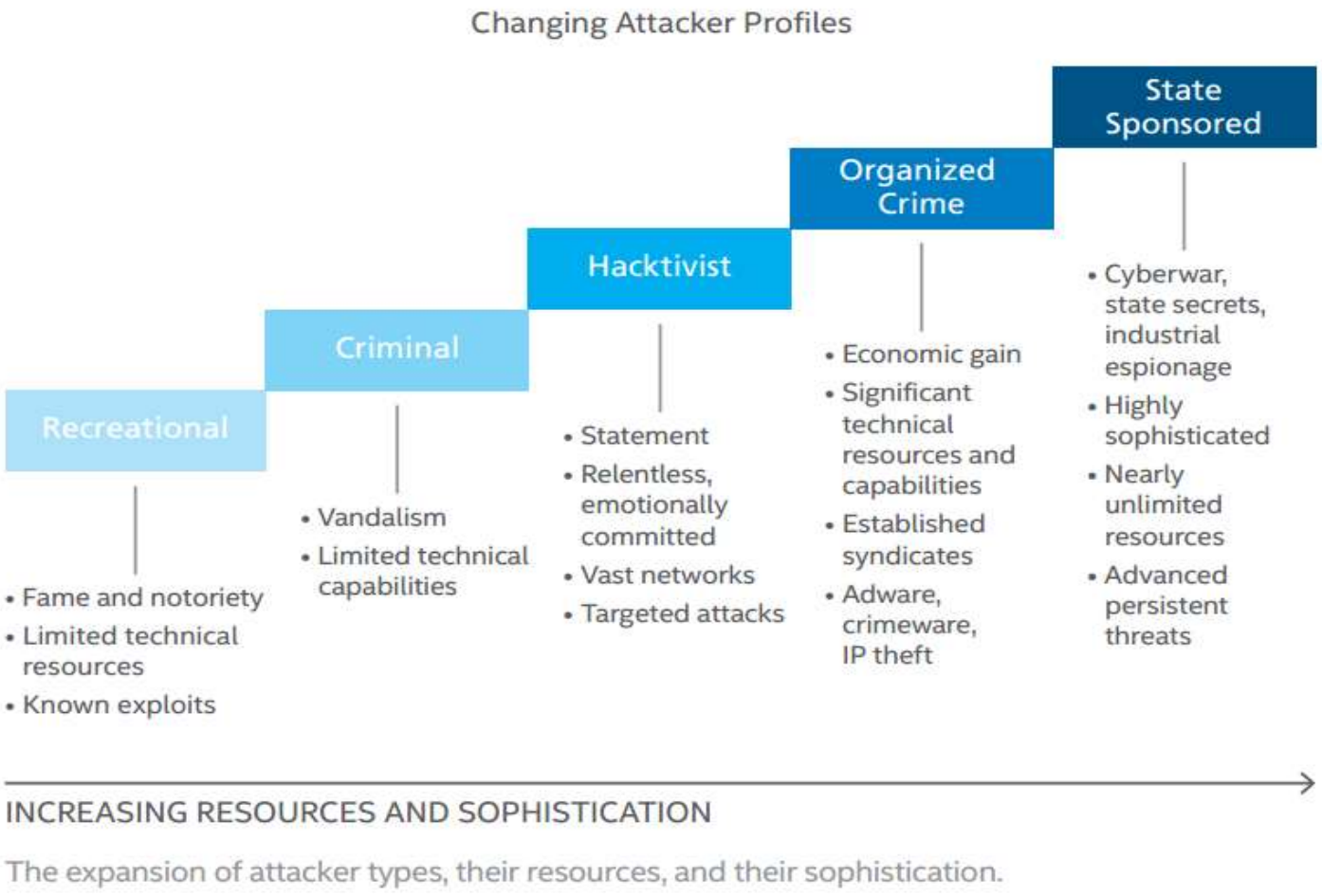


- IoT
  - On average 5,200 IoT based attacked reported by Symantec in 2018.
  - Routers and connected cameras were by far the main source of IoT attacks.
  - Attackers were also increasingly focused on Telnet as an avenue for attack and accounted for over 90 percent of attempted attacks.

Company Size and Attack relationship

EMAIL SPAM RATE BY ORGANIZATION SIZE (YEAR)			
ORGANIZATION SIZE	SPAMMING RATE	PHISHING RATE (1 IN)	MALICIOUS EMAIL RATE (1 IN)
1-250	55.9	2,696	323
251-500	53.6	3,193	356
501-1000	54.5	3,203	391
1001-1500	56.9	6,543	823
1501-2500	53.7	3,835	440
2501+	54.9	4,286	556

The actors targeting businesses



The expansion of attacker types, their resources, and their sophistication.

Underground Economy

ACCOUNTS

- Restaurant gift cards- 15–40% of value
- Online retailer gift cards- 15–50% of value
- Online banking accounts (depending on value & verification)- 0.5%–10% of value
- Video and music streaming accounts- $0.10–10
- Cloud service account- $5–10
- Gaming platform account- $0.50–12
- Hacked email accounts (2,500) -$1–15
- VPN services- $1–20
- Hotel loyalty (reward program accounts with 100,000 points) $10–20
- Online payment accounts (depending on value & verification) $1–100

Underground Economy

IDENTITIES

- Stolen or fake identity (name, SSN, and DOB) - $0.10–1.50
- Medical notes and prescriptions - $15–20
- Mobile phone online account - $15–25
- Stolen medical records - $0.10–35
- ID/passport scans or templates $1–35

MALWARE

- Office macro downloader generator - $5–10
- DDoS bot software $1–15
- Spyware $3–50
- Ransomware toolkit $0–250

SERVICES

- Airline ticket and hotel bookings -10% of value
- Hacker for hire- $100+
- Custom phishing page service -$3–12
- DDoS service, duration >24h (medium and strong protected targets) $10–1,000
- Single credit card with full details - $1–45

Today's Challenge

There is an increased risk for wide-scale or high-consequence cyber event that could cause harm or disrupt services upon which our economy and the daily lives of millions of peoples depend.

- Vulnerabilities
- Motivations
- Tools and services

Companies must constantly identify exposures; assess risks; prioritize actions; and test and apply security patches faster than ever before. All of this must be done without disruption to daily operations.

This is a challenging task and one that requires constant evolution

Cybersecurity as a Business Enabler

1. Strong security will enable you to win customers and retain customer loyalty
    1. A survey by Vodafone where 90% of businesses said strong cyber security would help their reputation in the market, attract new customers, and improve customer loyalty.
2. A detection and response program will relax restrictive preventative controls, increase productivity, and reduce shadow IT.
    1. Gartner forecast that 60% of business is shifting towards detect and respond than prevent.
3. Strong security will give confidence to the business when expanding into new territories or markets.
4. Modern security is reliant on vast quantities of data that can optimize the wider business
5. A well-handled security breach can actually boost brand equity
    1. Cloudflare data breach

Note : *http://www.vodafone.com/business/press-release/global-vodafone-survey-shows-strong-cyber-security-helps-businesses-to-grow*

Information Technology Infrastructure Library

- Information Technology Infrastructure Library (ITIL) first published in 1980's and last revised in 2019.
- Introduces a framework for IT Service Management lifecycle and highlights outcomes that must be achieved to successfully implement and manage IT services
- It is a library that contains a set of five books and 26 different processes inside different phases of its lifecycle that describes the processes that need to be implemented in an organization and provides a systematic approach in the area of IT Governance, management, operations and control of IT services.
- The books gives the best practices for providing IT services efficiently and effectively and
  - Identify IT service needed by the organization and understand how these services will be delivered.
  - IT units can deliver quality services, meet all the enterprise requirements by alignment of IT and business needs.
  - Contributes to perform the day-to-day operation of the processes that manage the IT services.
  - To identify and evaluate institution needs and implement improvements to IT services to support institutional

Incorporating ITIL into Business Model

- **Business Execution**
  - This is based on the idea that business strategy is a driver of organizational design choice and IS infrastructure design.
  - the top management formulate business strategy and IT managers design and implement ITIL for a better strategic alignment between IT and the business.
- **Technology transformation**
  - This evaluates the implementation of business strategy through appropriate IT strategy and IS infrastructure and processes..
  - It examines the implementation of a chosen business strategy through IT strategy and the required IT infrastructure and ITIL processes
- **Competitive potential**
  - It focuses on the utilisation of IT capabilities to impact on products and services (business scope), the key strategy attributes (distinctive competencies) and to create new forms of relationships (business governance).
- **Service level:**
  - The strategic fit enables organizations to meet IS customers' needs by implementing resources that can respond to their fast changing demands

Benefits of Aligning IT with business objectives using ITIL

- Strategic alignment is achieved by enhancing the communication between IT and business, as well as improving service delivery to business.
- ITIL breaks down barriers and enables people in an organization to share knowledge.
- ITIL has the ability to support business strategy, improve IT strategy and competency and impact significantly on organizational infrastructure.
- It provides consistency in the way things can be done throughout the organization.
- It improves quality of services as well as availability of services, which results in having more satisfied customers and gaining competitive advantage

Security Management

- We saw the challenges companies face with the introduction of technology, how to do cope with it.
- Computers have been integrated into the business and individual daily fabric, and their sudden unavailability would cause great pain and disruption.
- Security is more than just the technical controls we put in place to protect the organization's assets and it practices focus on the continuous protection of an organization's assets and resources.
- Security management encompasses all the activities that are needed to keep a security program up and running and evolving.

Risk Management

Risk in the context of security is the possibility of damage happening and the ramifications of such damage should it occur.

Information risk management (IRM) is the process of identifying and assessing risk, reducing it to an acceptable level, and implementing the right mechanisms to maintain that level. There

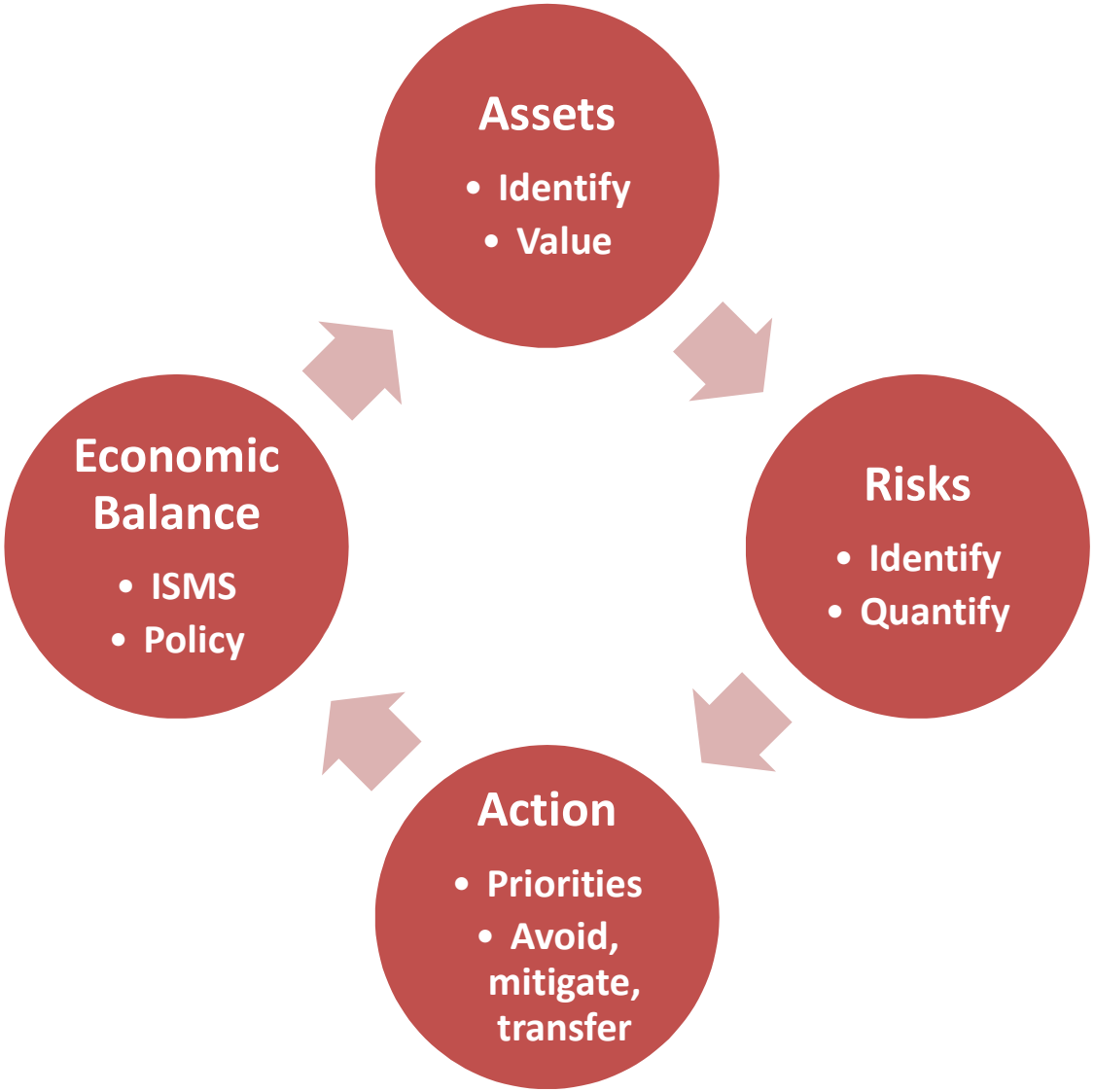
Types of Risk

- **Physical damage** Fire, water, vandalism, power loss, and natural disasters
- **Human interaction** Accidental or intentional action or inaction that can disrupt productivity
- **Equipment malfunction** Failure of systems and peripheral devices
- **Inside and outside attacks** Hacking, cracking, and attacking
- **Misuse of data** Sharing trade secrets, fraud, espionage, and theft
- **Loss of data** Intentional or unintentional loss of information to
- unauthorized receivers
- **Application error** Computation errors, input errors, and buffer overflows

Information Risk Management Policy

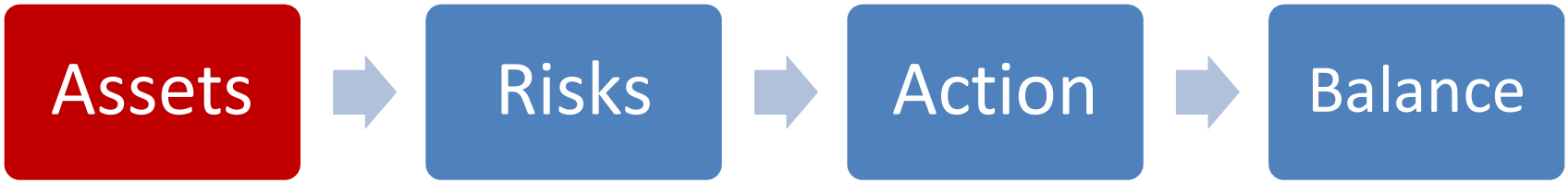
- The objectives of the IRM team
- The level of risk the organization will accept and what is considered an acceptable level of risk
- Formal processes of risk identification
- The connection between the IRM policy and the organization's strategic planning processes
- Responsibilities that fall under IRM and the roles to fulfil them
- The mapping of risk to internal controls
- The approach toward changing staff behaviours and resource allocation in response to risk analysis
- The mapping of risks to performance targets and budgets
- Key indicators to monitor the effectiveness of controls

Risk Assessment and Analysis



1) Identify assets and their value to the organization.
2) Identify vulnerabilities and threats.
3) Quantify the probability and business impact of these potential threats.
4) Provide an economic balance between the impact of the threat and the cost of the countermeasure.

Risk management – In context



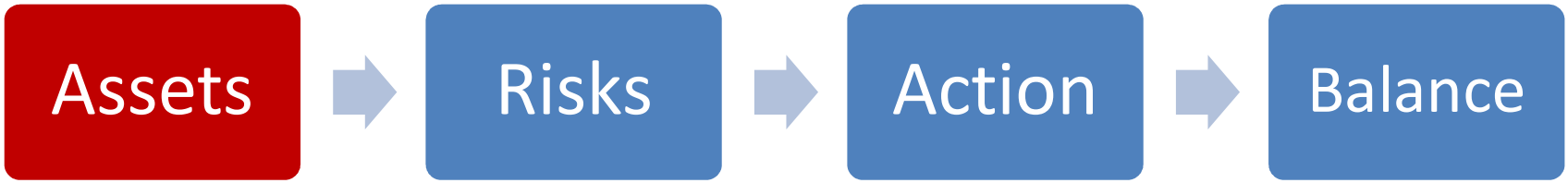
Identify

- Not just data
  (but we will mainly be looking at data)
- Network mapping
  What assets? Who owns them?

Value

Valued in terms of their importance to the business operation
Similarly to risk assessment, asset valuation is usually as organisations): Low, Medium, High or Very high

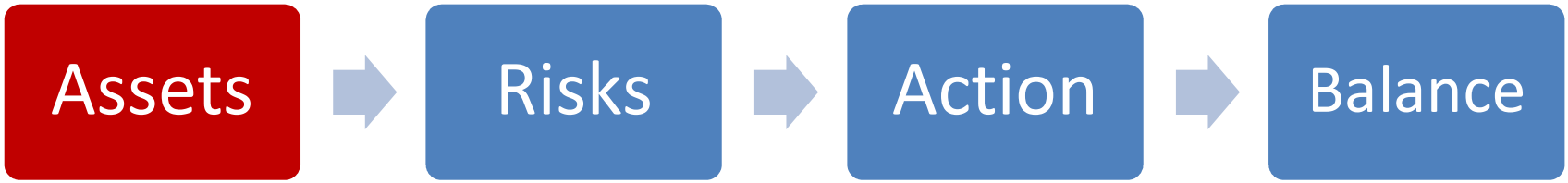
Risk management – In context



Cost that make up the Value

- Cost to acquire or develop the asset
- Cost to maintain and protect the asset
- Value of the asset to owners and users
- Value of the asset to adversaries
- Price others are willing to pay for the asset
- Cost to replace the asset if lost
- Operational and production activities affected if the asset is unavailable
- Liability issues if the asset is compromised
- Usefulness and role of the asset in the organization

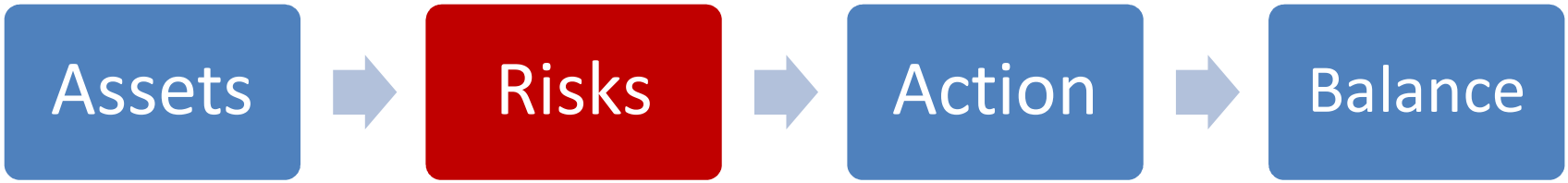
Risk management – In context



Benefit of identifying value of assets

- To perform effective cost/benefit analyses.
- To select specific countermeasures and safeguards.
- To determine the level of insurance coverage to purchase
- To understand what exactly is at risk
- To comply with legal and regulatory requirements

Risk management – In context



- Identify threats
  - Not just adversaries
    (user actions, lack of resources e.g. electrical supply, natural disaster)
  - Network mapping - who has access to what?
- Assess Risk
- Treat

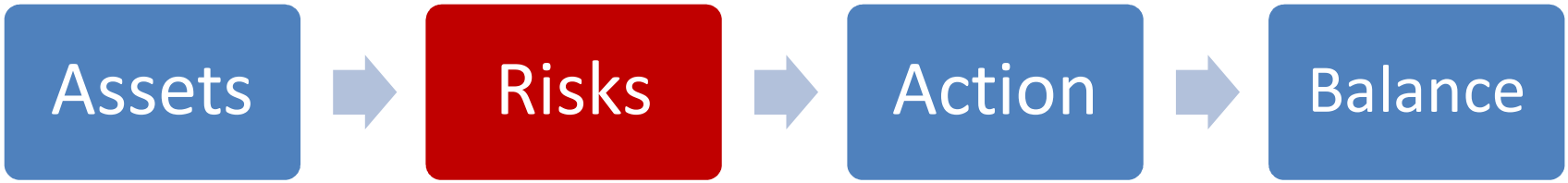
Risk management – In context

Assets → **Risks** → Action → Balance

Threat Agent	Can Exploit This Vulnerability	Resulting in This Threat
Malware	Lack of antivirus software	Virus infection
Hacker	Powerful services running on a server	Unauthorized access to confidential information
Users	Misconfigured parameter in the operating system	System malfunction
Fire	Lack of fire extinguishers	Facility and computer damage, and possibly loss of life
Employee	Lack of training or standards enforcement Lack of auditing	Sharing mission-critical information Altering data inputs and outputs from data processing applications
Contractor	Lax access control mechanisms	Stealing trade secrets
Attacker	Poorly written application Lack of stringent firewall settings	Conducting a buffer overflow Conducting a denial-of-service attack
Intruder	Lack of security guard	Breaking windows and stealing computers and devices

Risk management – In context

Mapping the network architecture

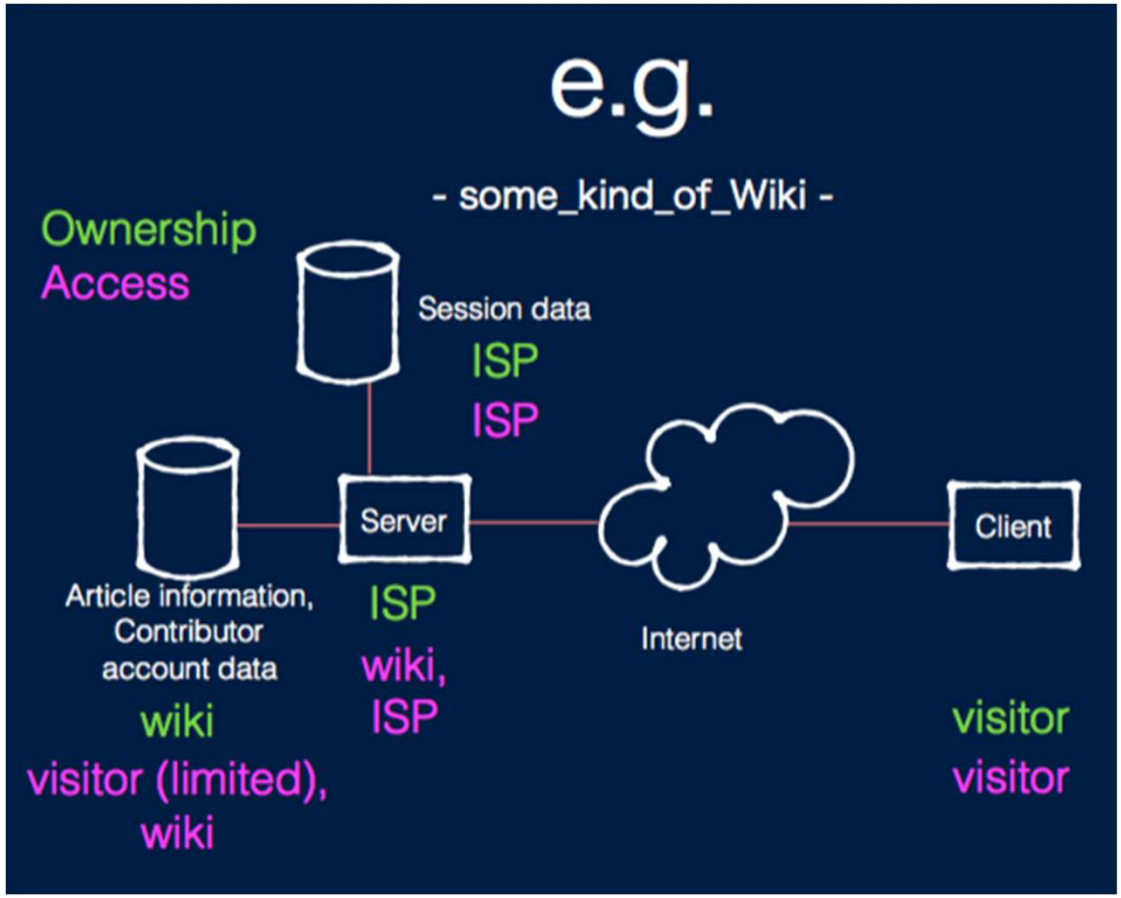


A risk is:

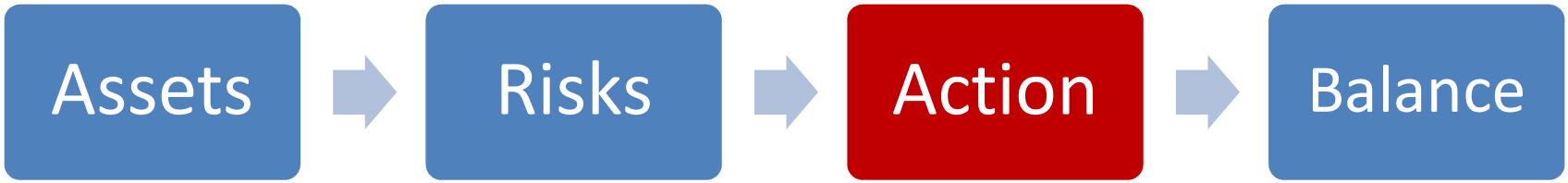
- The likelihood of an event (threat occurring) combined with its consequence.
- For something to be a risk there needs to be a vulnerability and a threat.
- Can be represented as impact /likelihood = risk
- Must look at ***delayed loss*** when assessing the damages that can occur.

Risk management – In context

Assets → **Risks** → Action → Balance



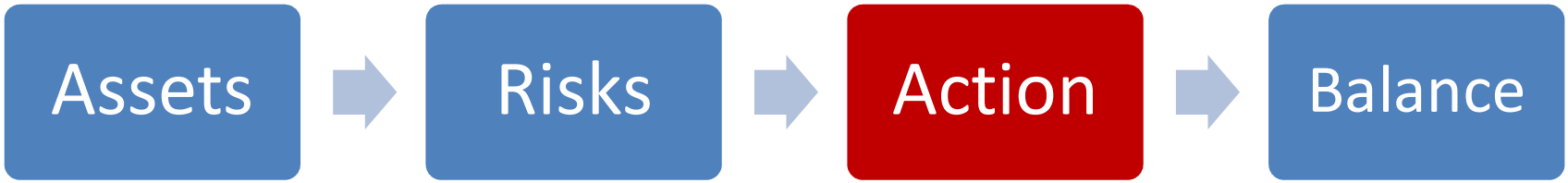
Risk management – In context



- Prioritise by doing Risk analysis
  - Rank risks *f*(likelihood, impact)
  - Residual risk
  - Legal compliance
  - Company priorities (business needs)
- Handle Risk
  - Avoid- e.g. all employees stop using cloud storage provider ‘x’
  - Mitigate- e.g. put a firewall in place
  - Transfer- e.g. get insured
  - Accept- do nothing

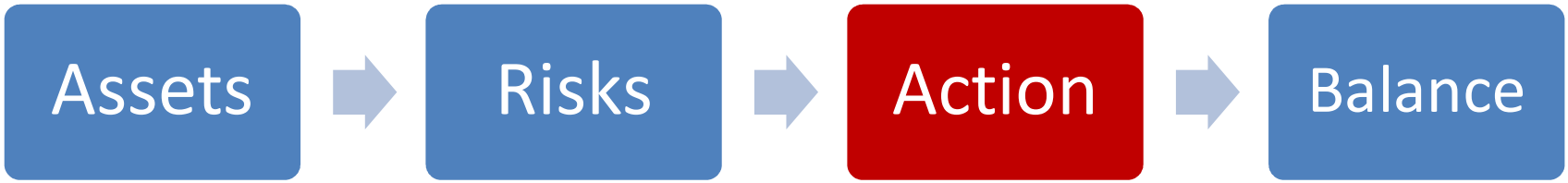
Risk management – In context

Mapping the network architecture



- Risk Analysis
  - Quantitative Risk is used to assign monetary and numeric values to all elements of the risk analysis process.
  - Qualitative risk analysis uses a “softer” approach to the data elements of a risk analysis. It does not quantify that data, which means that it does not assign numeric values to the data so that they can be used in equations.

Risk management – In context



- Quantitative Risk Analysis
  1. We have identified the assets that are to be assessed
  2. Associated a value to each asset, and
  3. Identified the vulnerabilities and threats that could affect these assets.

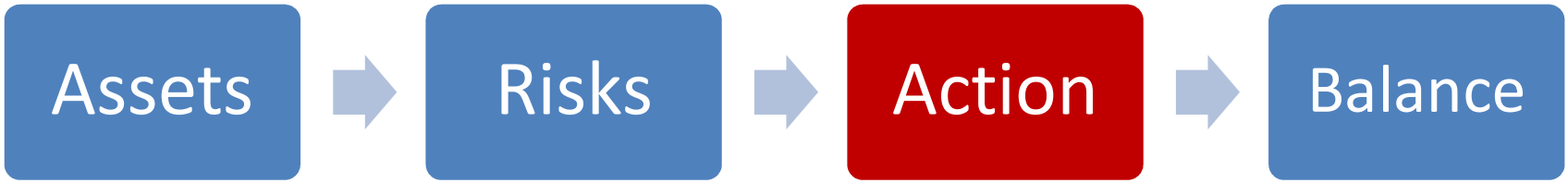
Important terms to calculate

The Single Loss Expectancy (SLE) is the amount that is assigned to a single event that represents the company's potential loss amount if a specific threat were to take place.

Asset Value × Exposure Factor (EF) = SLE

Where**,** the ***exposure factor (EF)*** represents the percentage of loss a realized threat could have on a certain asset.

Risk management – In context

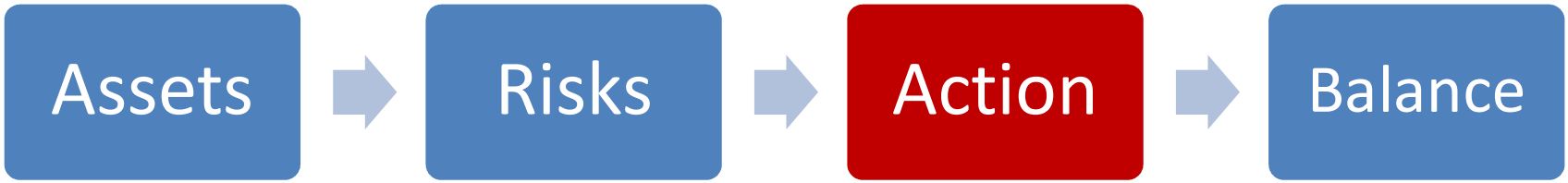


Example if a data warehouse has the asset value of £150,000, it can be estimated that if a fire were to occur, 25 percent of the warehouse would be damaged, in which case the SLE would be

Asset Value × Exposure Factor (EF) = SLE

Asset Value (£150,000) × Exposure Factor (25%) = £37,500

Risk management – In context



The ***annualized rate of occurrence (ARO)*** is the value that represents the estimated frequency of a specific threat taking place within a 12-month timeframe.

The range can be from 0.0 (never) to 1.0 (once a year) to greater than 1 (several times a year) and anywhere in between.

SLE × Annualized Rate of Occurrence (ARO) = ALE

For example, if the probability of a fire taking place and damaging our data warehouse is once every five years, the ARO value is 1/5= 0.2

Then the ALE value is £7,500 (£37,500 × 0.2 = £7,500).

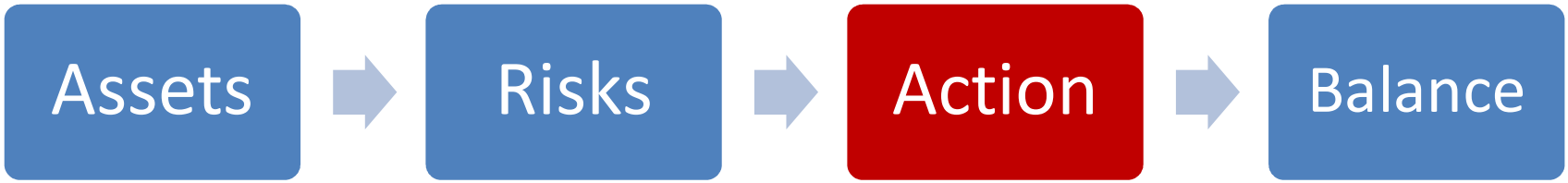
Risk management – In context

Assets → Risks → **Action** → Balance

Asset	Threat	Single Loss Expectancy (SLE)	Annualized Rate of Occurrence (ARO)	Annualized Loss Expectancy (ALE)
Facility	Fire	$230,000	0.1	$23,000
Trade secret	Stolen	$40,000	0.01	$400
File server	Failed	$11,500	0.1	$1,150
Data	Virus	$6,500	1.0	$6,500
Customer credit card info	Stolen	$300,000	3.0	$900,000

the company can make intelligent decisions on what threats must be addressed first because of the severity of the threat, the likelihood of it happening, and how much could be lost if the threat were realized.

Risk management – In context



Return on Security Investments (ROSI)
The ROSI equation integrates the risks and costs associated with a security incident, and combines that with the impact of a security solution.

$$ROSI = \frac{ALE * mitigation\ ratio - Cost\ of\ solution}{Cost\ of\ Solution}$$

Risk management – In context

ROSI Example:

Echo Inc. has been suffering from increased security breaches for the last few years and is considering investing in a user behaviour analytics (UBA) solution. However, the executive suite is not convinced the investment is worth it. The new CIO has decided to run some numbers.

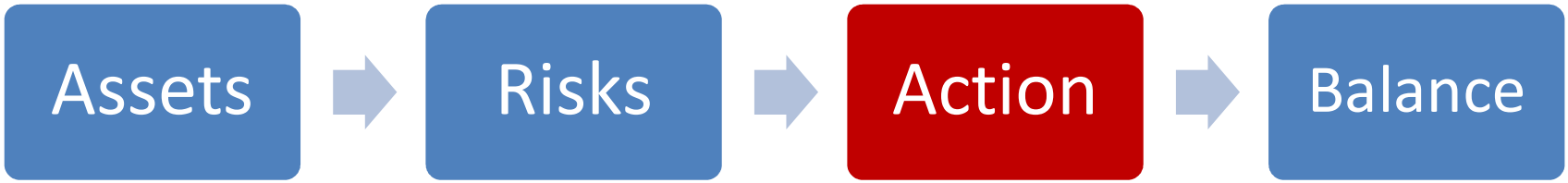
Echo's CIO estimates that Echo has been suffering about 10 (ARO=10) security incidents per year for the last three years. These incidents seem to cost about $20,000 (SLE=20,000) in data loss, fine, and productivity. The UBA solution is projected to block about 90% (mitigation ratio = 90%) of the attacks. However, the costs are causing the solution is an estimated $50,000 per year.

ARO=10, SLE=20,000,mitigation ratio = 90, Cost of Solution $50,000 per year.

ROSI = ((10 * 20000) * 0.9 - 50,000) / 50,000 = 260%

The investment in this example of $50,000 per year would save Echo Inc. an estimated $130,000 per year. Put simply the saving produced from the investment would provide a 260% payback on the security investment

Risk management – In context



Qualitative Risk Analysis

- Qualitative analysis techniques include judgment, best practices, intuition, and experience.
- Examples of qualitative techniques to gather data are Delphi, brainstorming, storyboarding, focus groups, surveys, questionnaires, checklists, one-on-one meetings, and interviews.
- A scenario of each identified vulnerability and how it would be exploited is explored.
- The “expert” in the group, who is most familiar with this type of threat, should review the scenario to ensure it reflects how an actual threat would be carried out.
- Safeguards that would diminish the damage of this threat are then evaluated, and the scenario is played out for each safeguard.

Risk management – In context

Assets → Risks → **Action** → Balance

Likelihood	Consequences				
	Insignificant	Minor	Moderate	Major	Severe
Almost certain	M	H	H	E	E
Likely	M	M	H	H	E
Possible	L	M	M	H	E
Unlikely	L	M	M	M	H
Rare	L	L	M	M	H

Qualitative Risk Assessment

- The exposure possibility and loss possibility can be ranked as high, medium, or low on a scale of 1 to 5 or 1 to 10.
- Once the ranking is complete, best possible counter measure is installed and report is generated to be presented to management.

Risk management – In context

Qualitative Risk Assessment Example

Scenario

The risk analysis team presents a scenario explaining the threat of a hacker exploiting a web vulnerability in the website of the company and accessing confidential information held on the five file servers within the company.

Steps

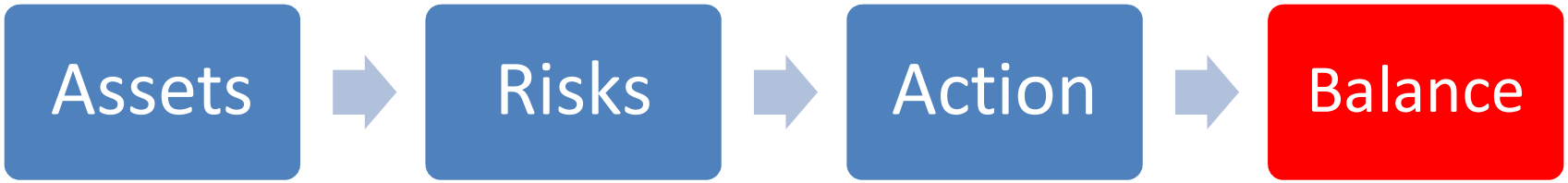
1) The risk analysis team then distributes the scenario in a written format to a team of five people that would be affected by the threat example
    1) the IT manager,
    2) database administrator,
    3) application programmer,
    4) system operator,
    5) and operational manager
2) They are also given a sheet to rank the threat's severity, loss potential, and each safeguard's effectiveness, with a rating of 1 to 5, 1 being the least severe, effective, or probable

Risk management – In context

Threat = Hacker Accessing Confidential Information	Severity of Threat	Probability of threat Taking Place	Potential Loss to the company	Effectiveness of a firewall	Effectiveness of a IDS
IT Manager	4	2	4	4	3
Database Administrator	4	4	4	3	4
Application Programmer	2	3	3	4	2
System Operator	3	4	3	4	2
Operational Manager	5	4	4	4	4
Results	3.6	3.4	3.6	3.8	3

Recommendation to CSO

Risk management – In context



- Update the ISMS
- Provide an economic balance between the impact of the threat and the cost
- of the countermeasure.
- Recommend counter measures to the board

Protection Mechanism

- Access Control
- Software application and Data malfunctions
- Threats arising from Fire, power loss, equipment malfunction
- Telecommunication and networking issue
- Business continuity and Disaster recovery.
- Computer Systems

Control Selection

- A security control must make business sense
- It should be cost effective
- A cost/benefit analysis must be conducted before implementing a control

(**ALE before implementing safeguard) – (ALE after implementing safeguard) – (annual cost of safeguard) = value of safeguard to the company**

Example :

For example, if the ALE of the threat of a hacker bringing down a web server is £12,000 prior to implementing the suggested safeguard, and the ALE is £3,000 after implementing the safeguard, while the annual cost of maintenance and operation of the safeguard is £650, then the value of this safeguard to the company is £8,350 each year

Control Selection

Things to consider while calculating cost for countermeasures.

- Product costs
- Design/planning costs
- Implementation costs
- Environment modifications
- Compatibility with other countermeasures
- Maintenance requirements
- Testing requirements
- Repair, replacement, or update costs
- Operating and support costs
- Effects on productivity
- Subscription costs
- Extra man-hours for monitoring and responding to alerts

Assessing Functionality and Effectiveness of Control

Characteristic	Description
Modular	It can be installed or removed from an environment without adversely affecting other mechanisms.
Provides override functionality	An administrator can override the restriction if necessary.
Defaults to least privilege	When installed, it defaults to a lack of permissions and rights instead of installing with everyone having full control.
Asset protection	Asset is still protected even if countermeasure needs to be reset.
Easily upgraded	Software continues to evolve, and updates should be able to happen painlessly.
Testable	The safeguard should be able to be tested in different environments under different situations.
Must be able to reset safeguard	The mechanism should be able to be reset and returned to original configurations and settings without affecting the system or asset it is protecting.

Risk company is exposed to

Total Risk , is the risk the company faces if it chooses not to apply control

Total Risk = Threats * Vulnerability * Asset Value

Which is possibility of a vulnerability being exploited multiply by assets value.

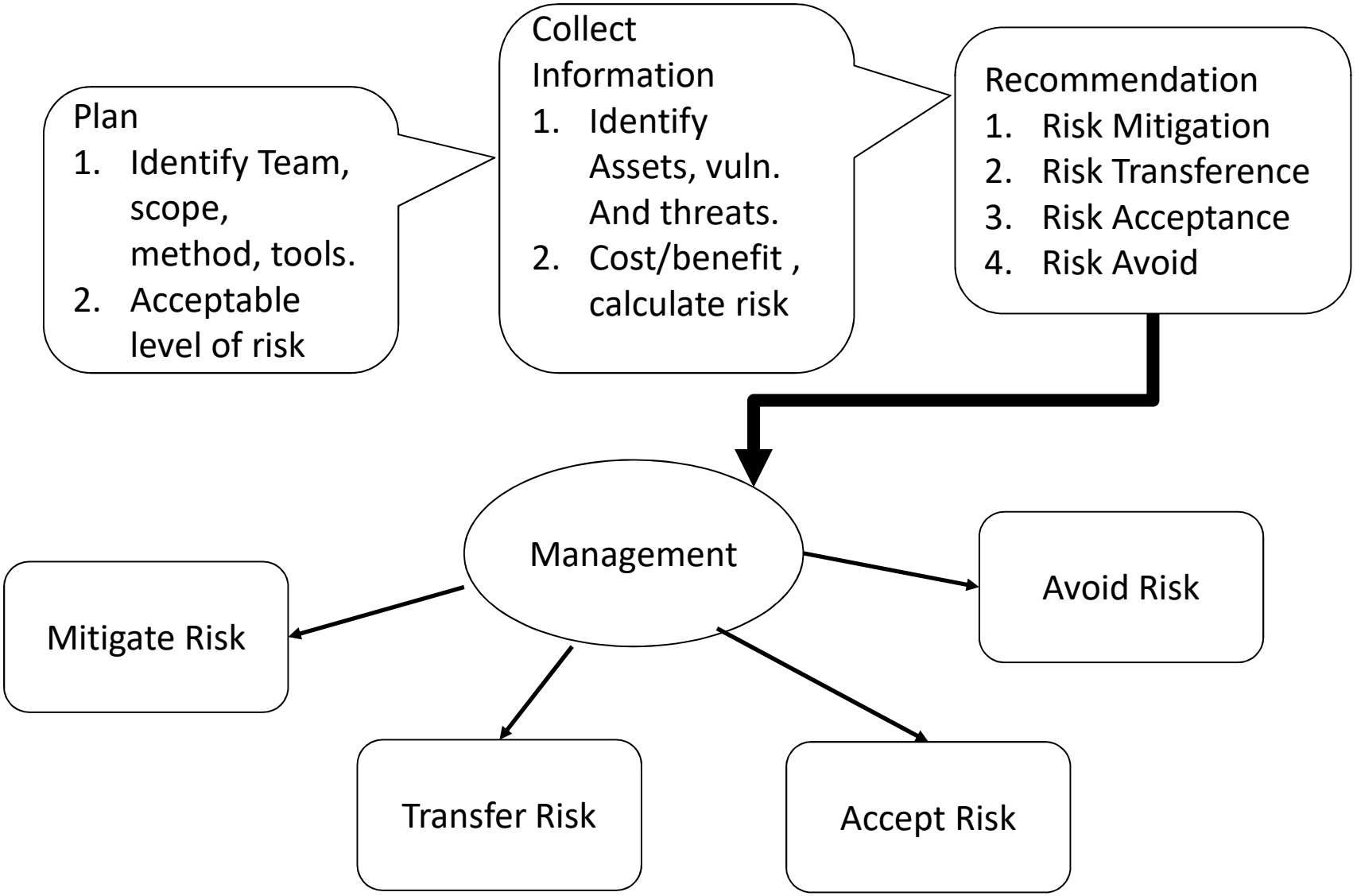
Residual risk is the risk left after control is places.

Total Risk – Countermeasure = Residual Risk

Handling Risk

- **Risk Mitigation**
  - Control Selection
  - Implementation
  - Monitoring
- **Risk Transference**
  - Purchase insurance
- **Risk Acceptance**
  - Do nothing
- **Risk Avoidance**
  - Discontinue Activity

Steps in Risk Management Program



Legal and Regulatory Environment

- Computer Misuse Act
- Data Protection Act
- GDPR

Computer Misuse Act 1990

Background

- The law was introduced following the 1987 case of *Regina v Gold and Schifreen.*
- The hackers were charged and convicted under Frogery and Counterfeiting Act 1981 however, their conviction was overturned on appeal, where they demonstrated that they hadn't attempted to profit from hacking.

This lead to the design and introduction of Computer misuse act

- Unauthorised access to computer material, punishable by twelve months' imprisonment (or six months in Scotland) and/or a fine "not exceeding level 5(unlimited) on the standard scale"
- Unauthorised access with intent to commit or facilitate commission of further offences, punishable by twelve months/maximum fine (or six months in Scotland) on summary conviction and/or five years/fine on indictment;
- Unauthorised modification of computer material, punishable by twelve months/maximum fine (or six months in Scotland) on summary conviction and/or ten years/fine on indictment

Data Protection Act 1998

The **Data Protection Act 1998** was a United Kingdom Act of Parliament designed to protect personal data stored on computers or in an organised paper filing system.

It was superseded by the Data Protection Act 2018 and supplements the GDPR which regulates the collection, storage and use of personal data significantly more strictly.

Data Protection Act 1998
Principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. About the rights of individuals e.g. personal data shall be processed in accordance with the rights of data subjects (individuals).
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

General Data Protection Regulation

- Companies have to fully compliant with GDPR from 25 May2018
- Personal Data
  - Is defined as any information relation to a person that can be used to identify the person directly or indirectly.
  - Included online identifiers such as IP and cookies, if they are capable to be linked back to user.
  - There is no distinction between personal data about an individual in their private, public or work roles.
- Penalties
  - 10 million Euro's or two percent of global gross turnover for violation of record keeping, security breach notification and privacy impact assessment obligation.
  - 20 million Euro's or 4% of turnover for violation related to legal justification for processing, lack of consent, data subject rights and cross-border data transfer.

General Data Protection Regulation

- Companies are required to implement appropriate technical and organisational measures in relation to the nature, scope, context and purpose of handling and processing personal data.
- These safeguards must be appropriate to the degree of risk and might include
  - Encryption of personal data
  - Ensuring CIA and resilience of system
  - Restoring data in a timely manner
  - Process to test, assess and evaluate the effectiveness of system.
- Consent to be taken by individual whose data is held.
  - Organisation must be able to show how consent was obtained
  - Data obtained must be specific, explicit and of legitimate purpose
  - User must be able to withdraw consent
- Individual must have full access to information on how their data is processed.
- Companies must report breaches of security.
  - In the event of personal data breach companies must notify the appropriate supervisory authority with 72 hours.

Group Discussion

- Use Betterbuy scenario to
  - Draw a network diagram
  - Identify the threats
  - Assets
  - Do Qualitative analysis on at least 2 threats identified by you.