THE UNIVERSITY OF MELBOURNE

INFO30006
Information Security and Privacy

Week 03: Managing Information Security Risks

Dr Heidi Tscherning

Today's session

1. WEEK 02 AND FIRST WORKSHOP
2. INFORMATION ASSET, THREAT, VULNERABILITY AND RISK
3. SECURITY THREATS AND RISKS TODAY
4. RISK MANAGEMENT
5. CONCLUDING REMARKS / WORKSHOP

Today's session

1. WEEK 02 AND FIRST WORKSHOP
2. INFORMATION ASSET, THREAT, VULNERABILITY AND RISK
3. SECURITY THREATS AND RISKS TODAY
4. RISK MANAGEMENT
5. CONCLUDING REMARKS / WORKSHOP

Week 02 - information security practices

Assets, threats, vulnerabilities and risks

- Question: what do these concepts mean?

Security threat landscape

- 12 categories of security threats
- Question: what are some of the different types of threats?

Changing security threat landscape

- Question: what has changed the last decades?

Protection and control

- Question: four types – which?

Workshops

- Topic, presentation/facilitation?

Changing information security landscape I - shift

Last decade has seen a global shift in terms of information security threats in the media causing information security to become a main concern for businesses and nations: Video: The new Cyber threat:

Changing information security landscape II - examples

- 2015: US filing cyber espionage charges against Chinese military
- 2013: Snowden reveals US hackers targets China, North Korea, Hong Kong
- 2013: US charged Russian/Ukranian hackers with hacking into computers of major retailers, payment processors and banks stealing customers' credit card numbers.

Today's session

1. WEEK 02 AND FIRST WORKSHOP
2. INFORMATION ASSET, THREAT, VULNERABILITY AND RISK
3. SECURITY THREATS AND RISKS TODAY
4. RISK MANAGEMENT
5. CONCLUDING REMARKS / WORKSHOP

Revisiting terms: threat, vulnerability, risk

Threats

- Threats can NOT be controlled, e.g. terrorist groups, hurricanes and other natural disasters
- Need to be identified!

Vulnerabilities

- CAN be treated
- Weaknesses need to be identified
- Proactive measures should be taken to correct vulnerabilities

Risks

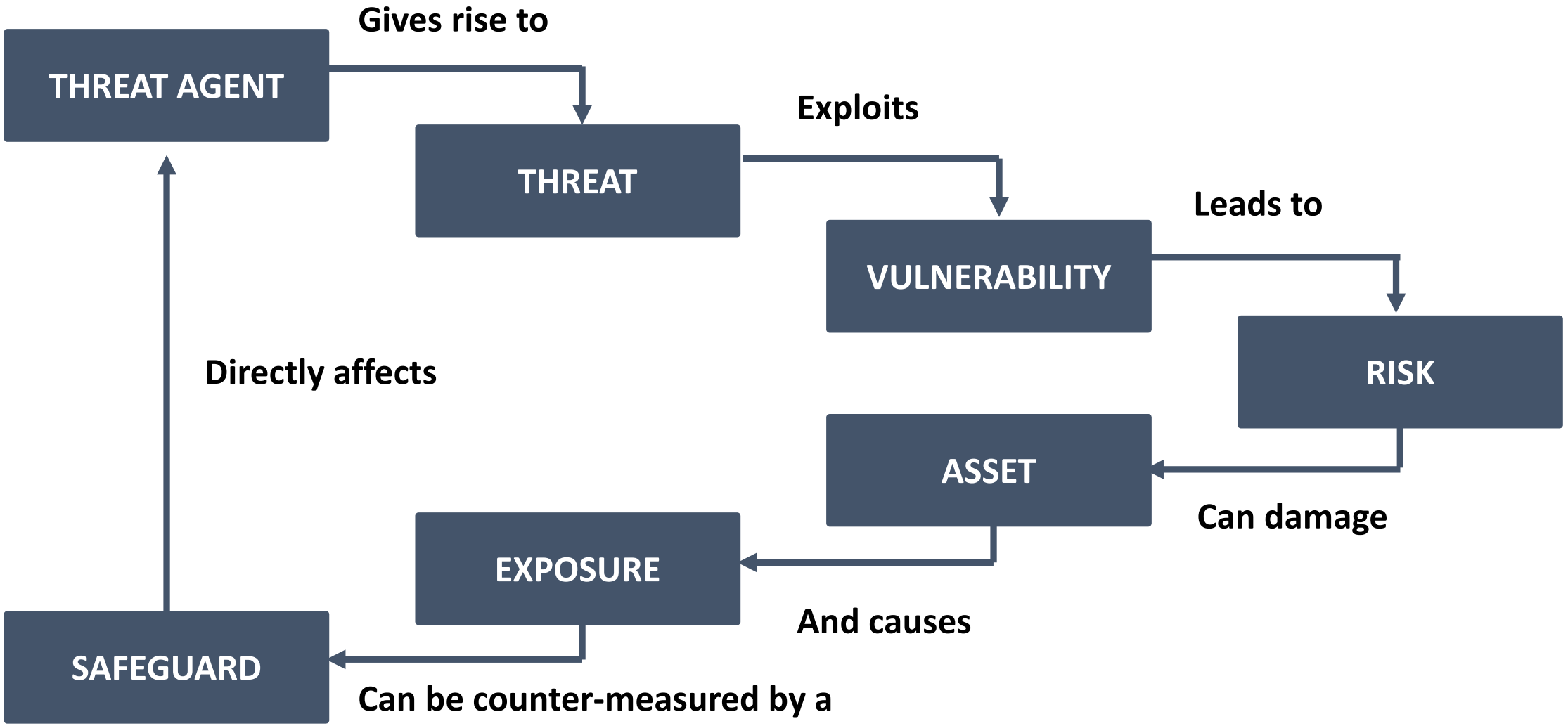
- CAN be mitigated or managed to lower vulnerability or overall impact
- Risk assessment -> identification of critical assets

So what is a risk?

A risk is an *asset* that has a *vulnerability* that can be exploited by a *threat*, measured in terms of consequence and likelihood.

Standards Australia, HB 231: 2004:
Information security risk management guidelines

Concept relationships



NB! Added 12 August 2017

Evolving information security threat landscape

Exercise – 5 minutes:

Discuss in small groups: what are the biggest information security threats and risks today: anno 2017?

- Identify different types of threats and risks

SECURITY IS MOSTLY A SUPERSTITION. LIFE IS EITHER A DARING ADVENTURE OR NOTHING.

Helen Keller,
American author, political activist,, and lecturer

Today's session

1. WEEK 02 AND FIRST WORKSHOP
2. INFORMATION ASSET, THREAT, VULNERABILITY AND RISK
3. SECURITY THREATS AND RISKS TODAY
4. RISK MANAGEMENT
5. CONCLUDING REMARKS / WORKSHOP

Security threats and risks today

Emerging technologies: consumer drones becoming weaponised

- Such as…
- Consumer drones becoming weaponised
- Why?

Security threats and risks today

ET: consumer drones becoming weaponised

'There are many ways to kill a drone. But what's the cheapest and most effective way to do it? A cybersecurity consultancy is testing various ways to defend against rogue drones'.

Read more: Wired: 'The Army Grounds its DJI Drones Over Security Concerns'

Source: Wired 1 Feb, 2017: https://www.wired.com/2017/01/biggest-security-threats-coming-2017/

Security threats and risks today

Encryption clash between governments and tech companies

- Such as…
- Turnbull government and backdoor
- Why?

Security threats and risks today

Encryption clash between governments and tech companies

'The Turnbull government has not explicitly laid out what it wants in terms of encrypted messaging, but both Turnbull and Shorten spoke on Tuesday about the need for social media and messaging companies to engage in cooperation and "collaboration" with police investigations'.

Read more: Wired: 'The Apple-FBI Fight isn't About Privacy cs. Security'

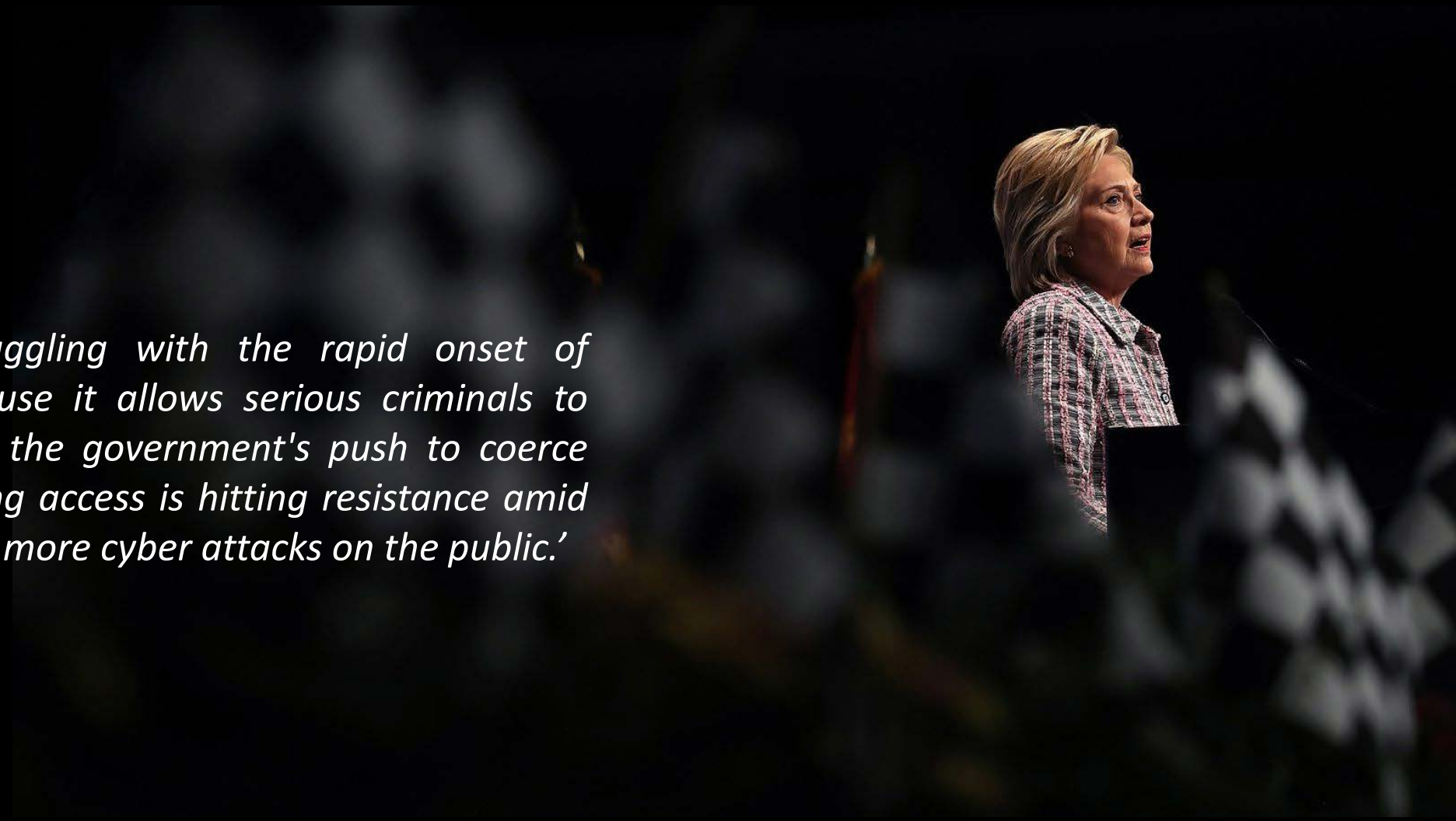
Security threats and risks today

Russians hack US election

- Kremlin's hacking of US election
- US Homeland security reveal to Washington Post
- Why?

Read more: Esquire: 'Hoe Russia Pulled Off the Biggest Election Hack in U.S. History'

Security threats and risks today



Russians hack US election

'Security agencies are struggling with the rapid onset of encrypted data online because it allows serious criminals to communicate in secret. But the government's push to coerce tech companies into providing access is hitting resistance amid fears it could actually lead to more cyber attacks on the public.'

Source: BBC.com: 21 June 2017: Read more:
https://www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections

What about 2019?

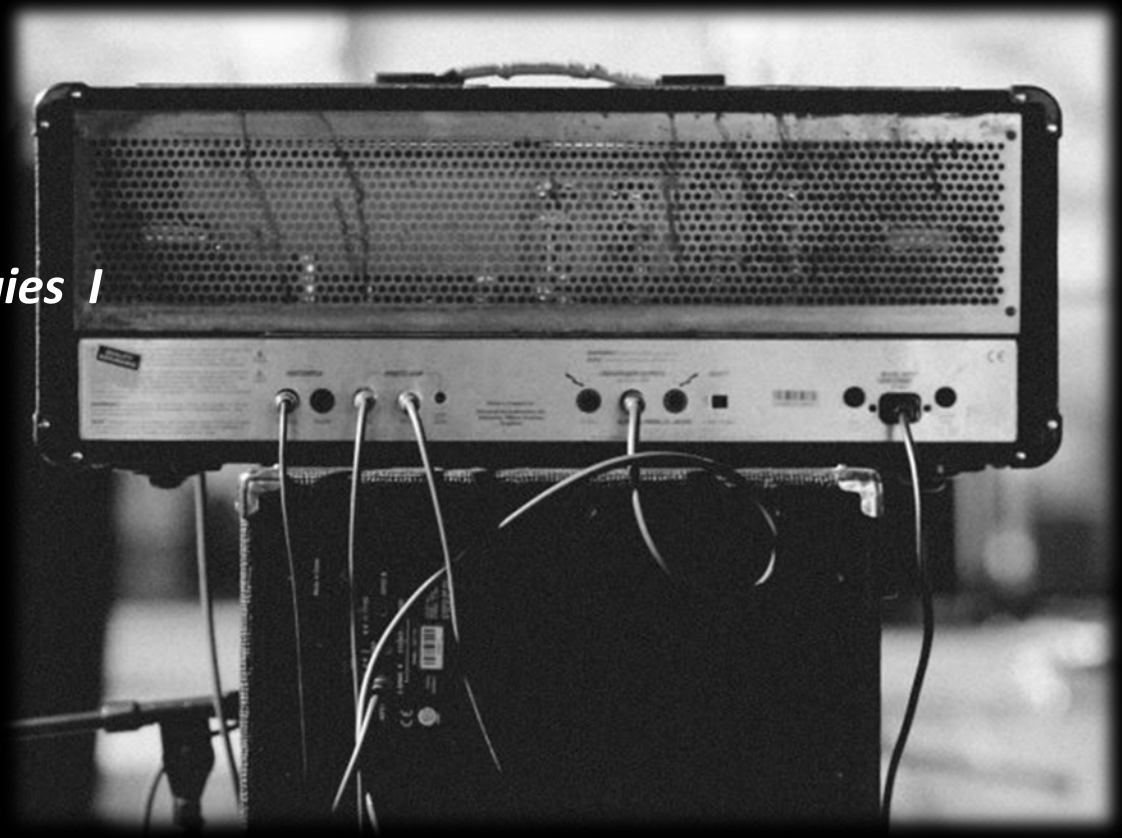
Disruption - over-reliance on Internet-of-Things (IoT) technologies I

- Malicious attacks global scale: Internet outages create conflicts globally -> nation chaos

What about 2019?

Disruption - over-reliance on Internet-of-Things (IoT) technologies I

- Twitter is down. Skype is down. Tumblr is down. Facebook is down. Twitter is down again.
- WhatsApp down for two hours



What about 2019?

Disruption - over-reliance on Internet-of-Things (IoT) technologies II

- Such as…
- Ransomware hijacks IoT: encryption of victim's data -> demanding payment for encryption key
- Why?

What about 2019?

Hi to all mankind.

The greatest leak of cyber space era is happening.

Disruption - over-reliance on Internet-of-Things (IoT) technologies

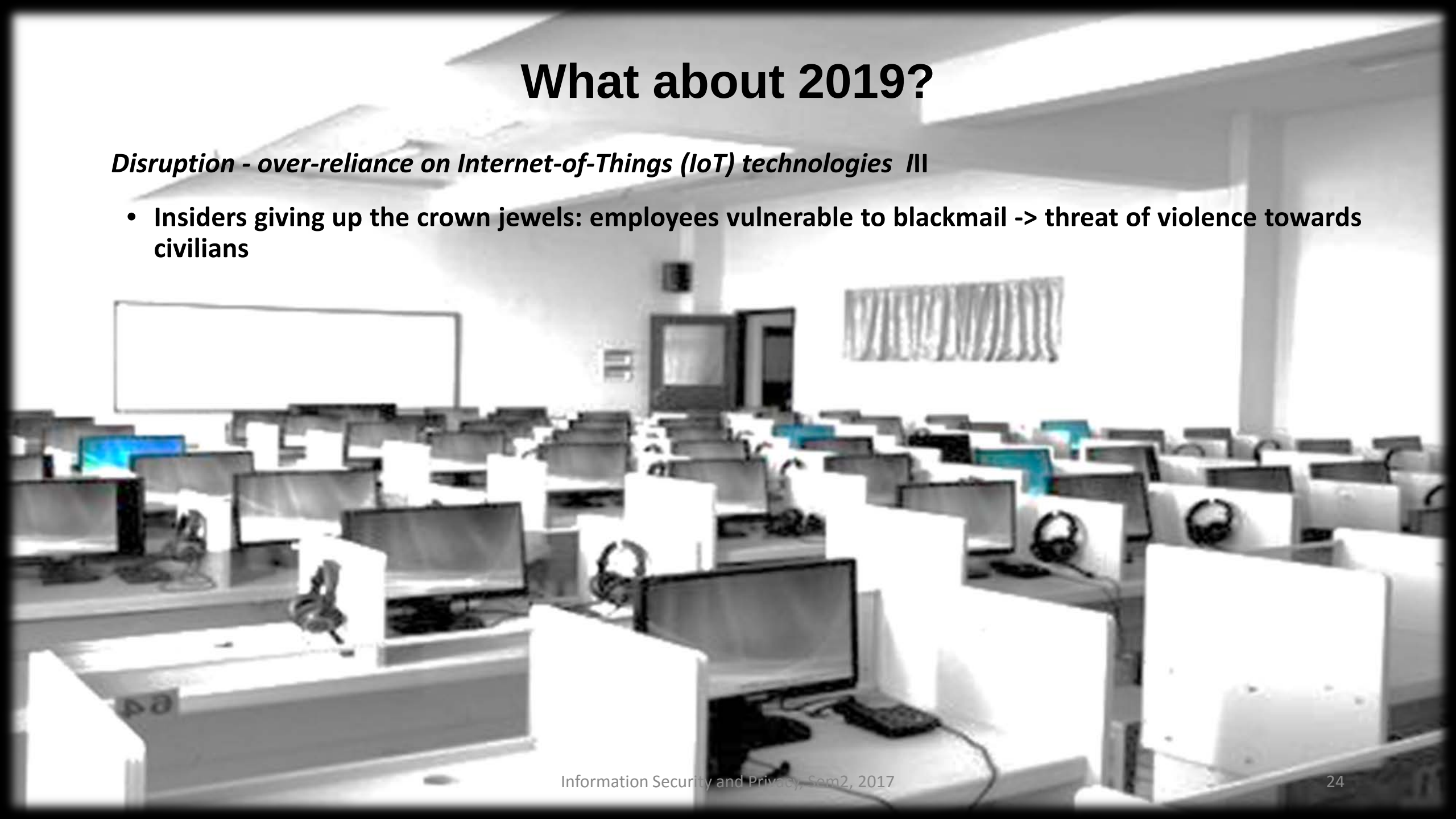
- Ransomware: Hacking group targets Game of Thrones from HBO:
  - Latest hack: 0.5 GB stolen
  - Total: 1.5 terabyte
  - Watermarked with hacker motto: "HBO is Falling."
  - Ransomware letter

Read more: Wired: 'HBO Hackers Release Ransom Note and New Trove of Stolen Data'

What about 2019?

*Disruption - over-reliance on Internet-of-Things (IoT) technologies I*II

- **Insiders giving up the crown jewels: employees vulnerable to blackmail -> threat of violence towards civilians**



What about 2019?

Integrity of information

- Automated misinformation (e.g. fake news) gains credibility
- Falsified information a compromise (e.g. counterintelligence or data distortion)

THE BIGGEST RISK IS NOT TAKING ANY RISK… IN A WORLD THAT'S CHANGING REALLY QUICKLY, THE ONLY STRATEGY THAT IS GUARANTEED TO FAIL IS NOT TAKING RISKS.

Mark Zuckerberg,
Co-founder Facebook

Today's session

1. WEEK 02 AND FIRST WORKSHOP
2. INFORMATION ASSET, THREAT, VULNERABILITY AND RISK
3. SECURITY THREATS AND RISKS TODAY
4. RISK MANAGEMENT
5. CONCLUDING REMARKS / WORKSHOP

Information security risk management

Risk management is the process of identifying and controlling risks facing an organisation. Security risk management consists of the following steps:

1. **Risk identification**: process of examining an organisation's current information security situation
2. **Risk assessment**: determination of consequence and likelihood
3. **Risk control**: applying controls to reduce risks to an organisations data and information systems

Security risk management

Security risk management

A word on terminology

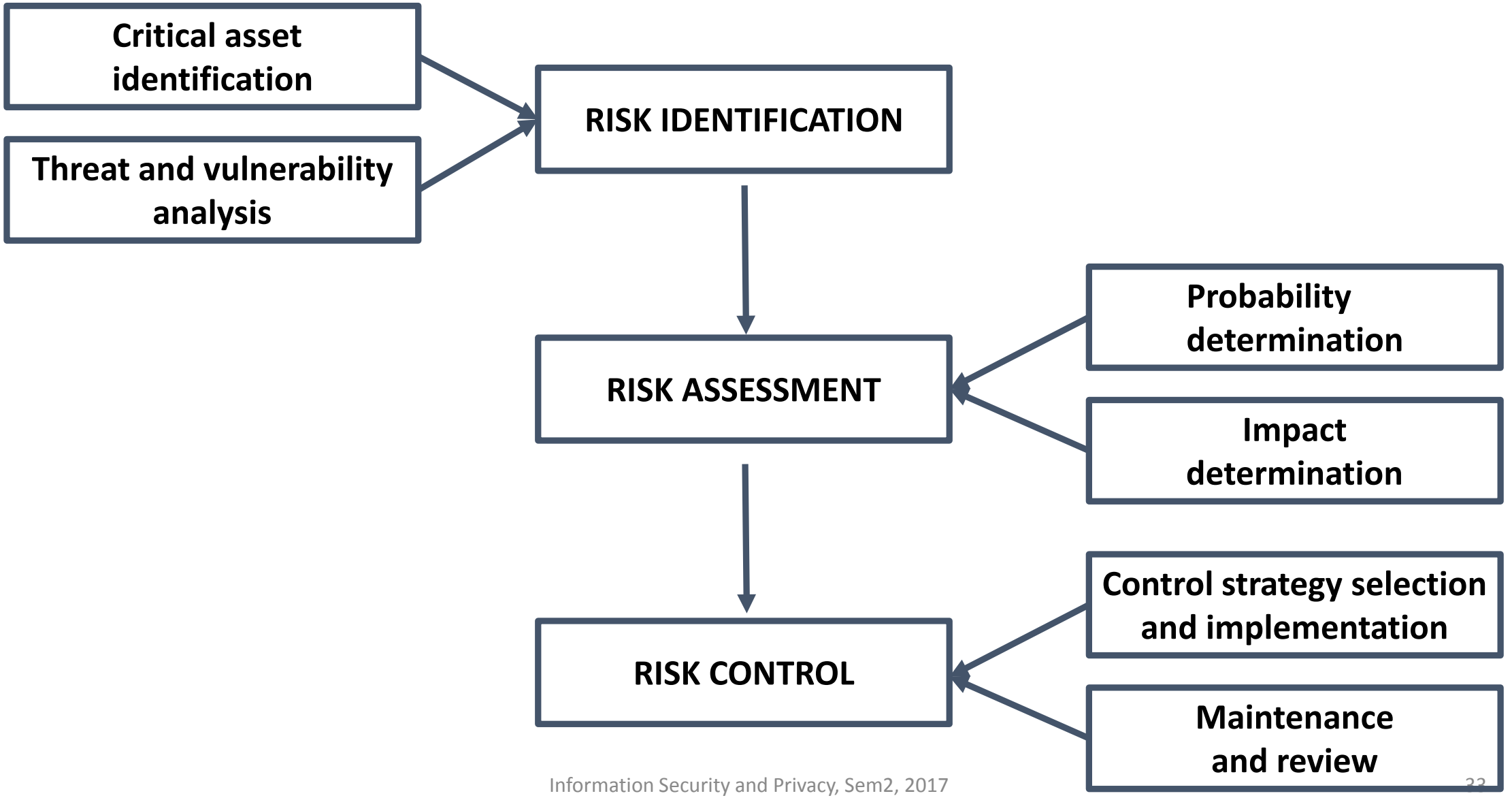
- There are many different methodologies, with different uses for the same words
- Different areas refer to risk management and its phases interchangeably
- Some commonly used variations:

    1. Risk analysis
    2. Risk assessment
    3. Risk evaluation
    4. Risk estimation

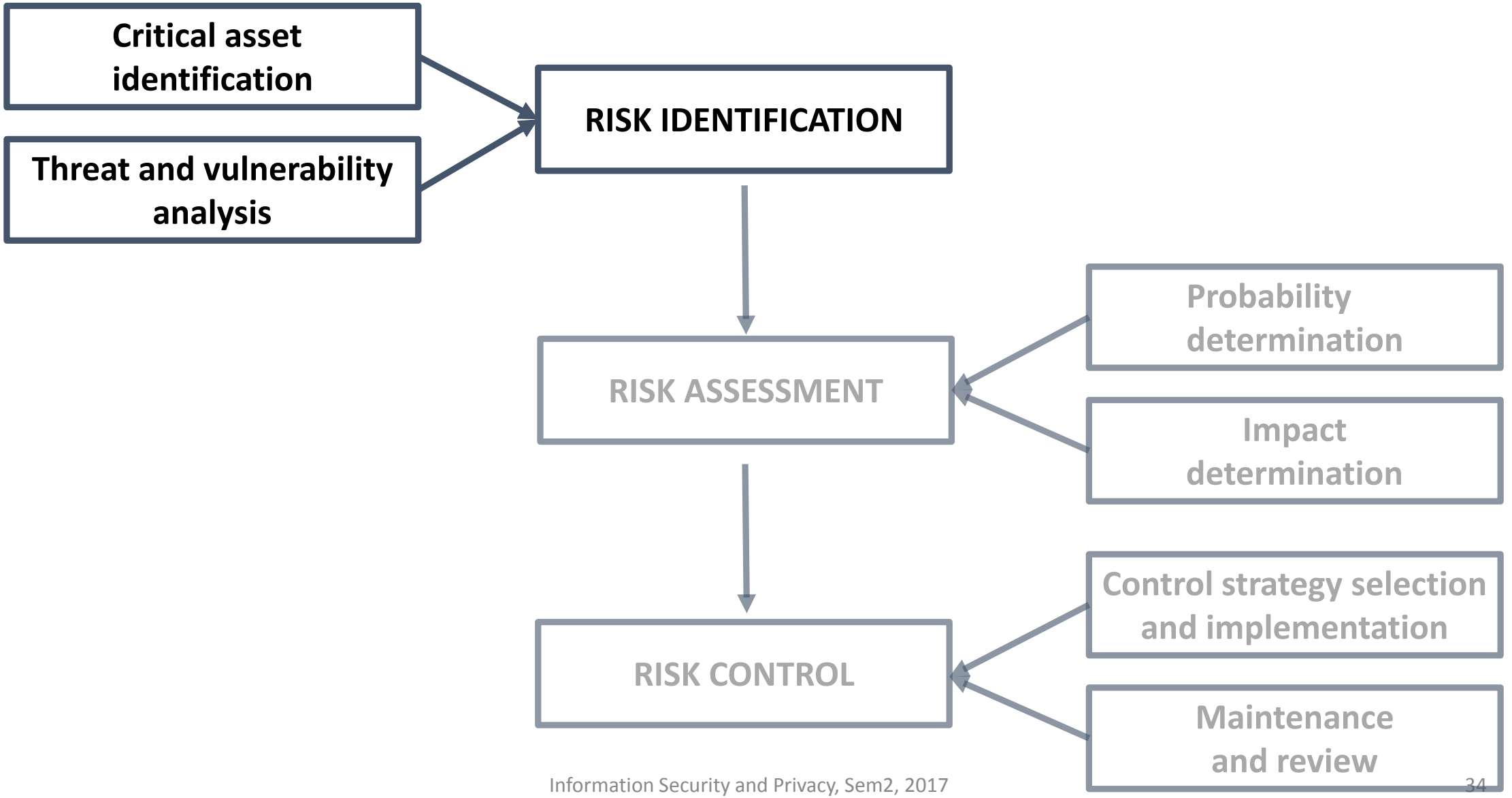
Steps in the information security risk management process

1. **Risk identification**
   - Context establishment
   - Identification and valuation of assets
2. **Risk assessment**
   - Consequence and likelihood determination
3. **Risk control**
   - Control strategy selection and implementation
   - Maintenance and review

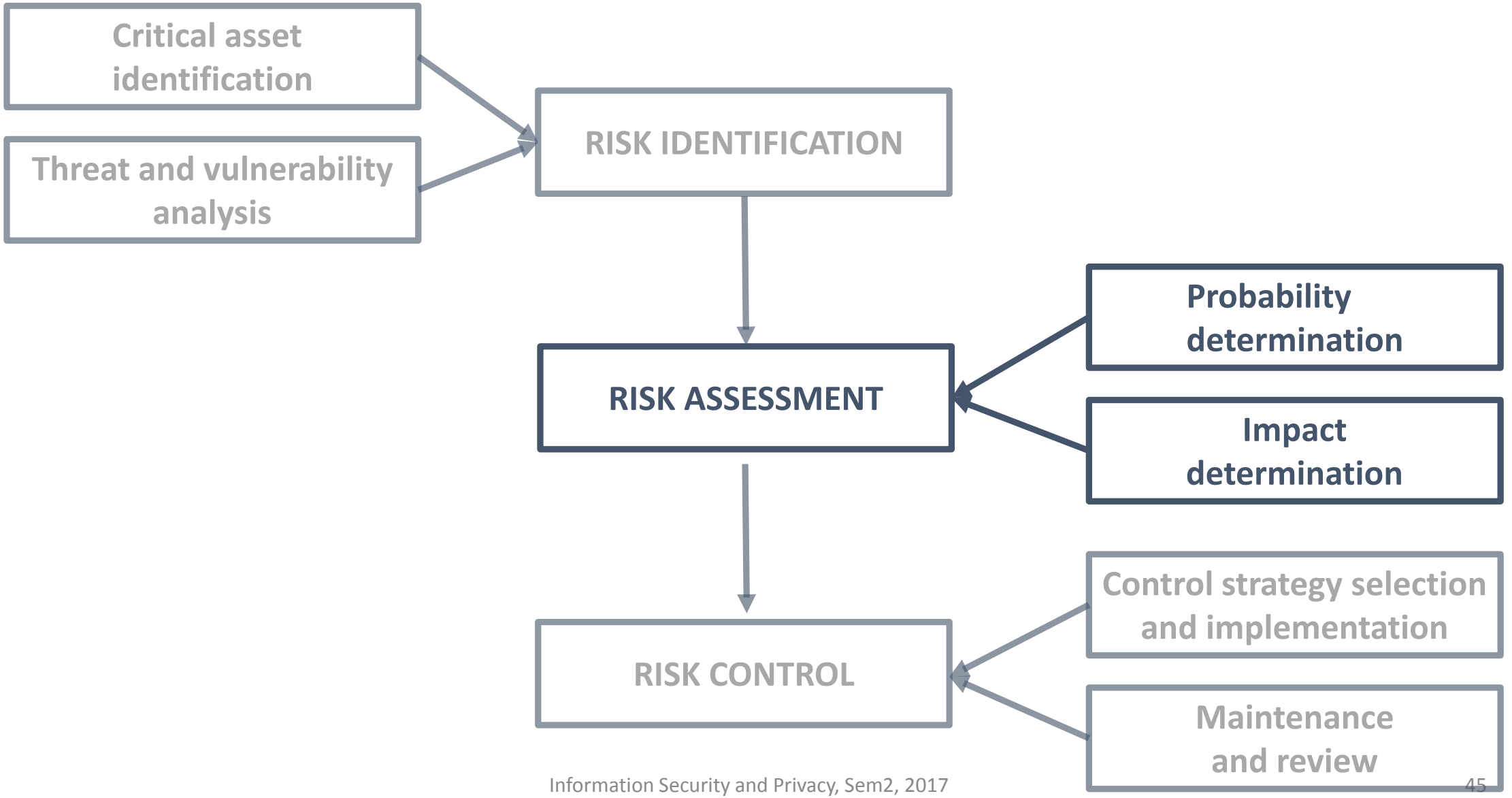
Security risk management



Security risk identification



Security risk management



Risk assessment

- Risk assessment evaluates the relative risk for each vulnerability
- Assigns a risk rating or score to each information asset
  - Textbook is quantitative (ie. numerical scores)
  - There are qualitative avenues, as well (ie. measured as CRITICAL, HIGH, MEDIUM, LOW, etc.)

Impact of an attack:

- Measured in dollars and cents
- Cost depends on the risk not the asset
  - Cost of confidentiality attack on a document asset is different to an availability attack
- Multiple avenues of impact:
  - Direct cost in dollars and cents
  - Productivity cost in regaining asset or reputation
  - Penalties for example if confidentiality has been breached

Risk assessment

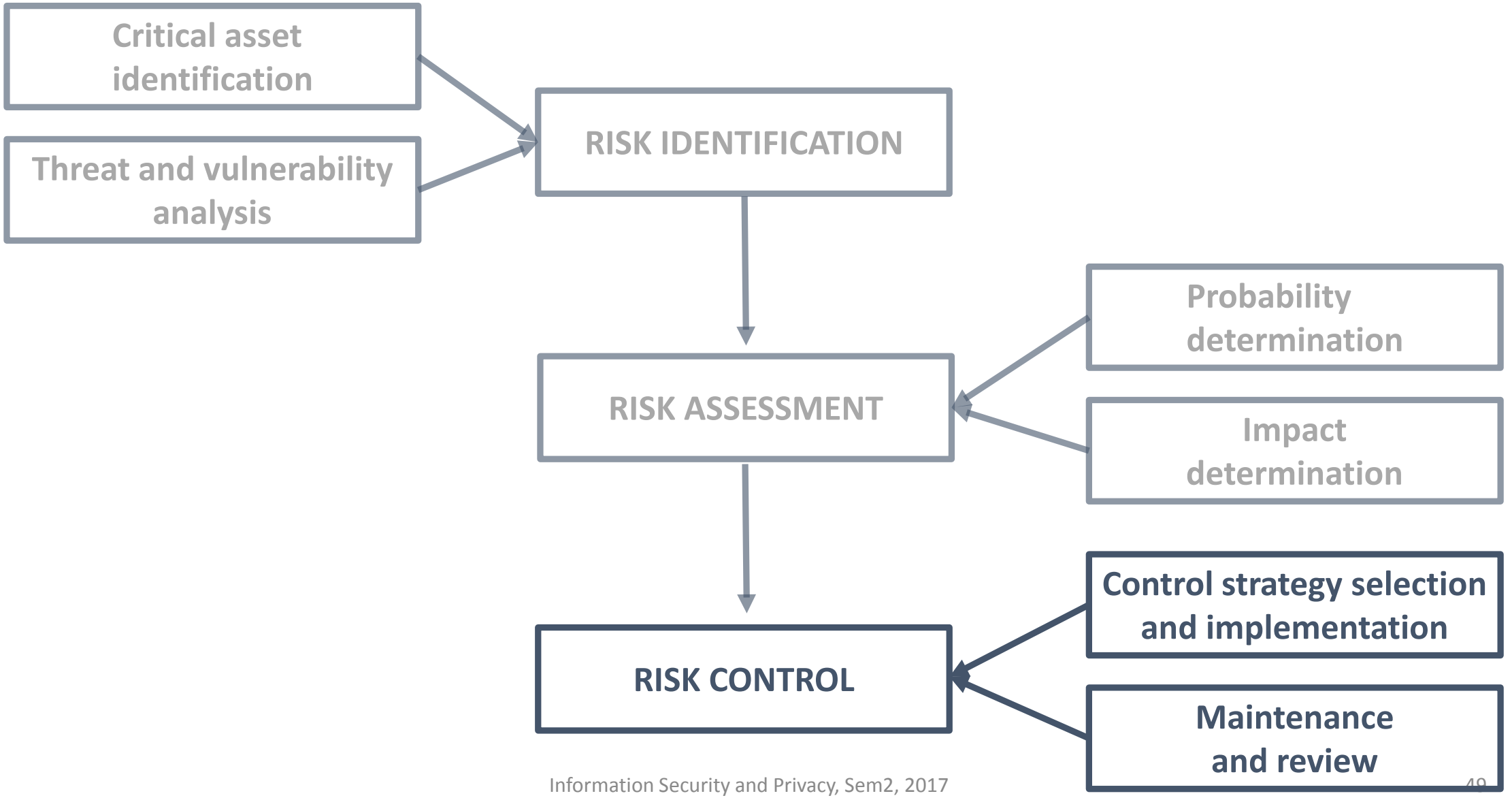
Likelihood of an attack:

- Likelihood of the threat manifesting, considering:
  - Asset value
  - Vulnerability
- Can be calculated from a number of sources, including:
  - Past records
  - Experience
  - Simulations
  - Experimentation
  - Specialist and expert judgements

Risk determination

LIKELIHOOD	IMPACT			
	CRITICAL	HIGH	MEDIUM	LOW
ALMOST CERTAIN	High	High	Medium	Low
LIKELY	High	High	Medium	Low
MODERATE	High	High	Medium	Low
UNLIKELY	Low	Low	Low	Low

Security risk management



Identify possible controls

Possible controls:

- For each threat and associated vulnerabilities that have residual risk, create preliminary list of control ideas
- Control categories:
- Formal: risk management, policy, etc.
- Informal: SETA
- Technical: Firewalls, VPNs, access control, etc.

Access controls:

- Specifically address admission of a user into a trusted area of organisation
- Access controls can be:
- Mandatory
- Discretionary
- Other

Identify possible controls

Types of access controls:

Mandatory access controls (MAC): give users and data owners limited control over access to information

Discretionary access controls (DAC): implemented at discretion or option of data user

Other type of controls: managed by a central authority in organisation; can be based on individual's role (role-based controls) or a specified set of assigned tasks (task-based controls)

Risk control strategies:

Once we know the risks for each asset must choose one of four strategies to control each risk:

- Prevent by applying safeguards (avoidance)
- Transfer the risk (transference)
- Reduce impact by Incident Response (mitigation)
- Understand consequences and accept risk (acceptance

Avoidance

- Attempts to prevent exploitation of the vulnerability
- Preferred approach; accomplished through countering threats, removing asset vulnerabilities, limiting asset access, and adding protective safeguards
- Three common methods of risk avoidance:
  - Application of policy
  - Training and education
  - Applying technology

Transference

- Control approach that attempts to shift risk to other assets, processes, or organisations
- If lacking, organisation should hire individuals/ firms that provide security management and administration expertise
- Organisation may then transfer risk associated with management of complex systems to another organisation experienced in dealing with those risks

Mitigation

- Attempts to reduce impact of vulnerability exploitation through planning and preparation
- Approach includes three types of plans:
  - Incident response plan (IRP)
  - Disaster recovery plan (DRP)
  - Business continuity plan (BCP)
- IRPs describe the actions to take the while incident is in progress
- DRP details the steps to take in order to recover from an incident just after it has occurred
- BCP encompasses continuation of business activities if catastrophic event occurs

Acceptance

- Doing nothing and accepting the outcome of an asset's exploitation
- Valid only when the particular function, service, information, or asset does not justify cost of protection
- Risk appetite describes the degree to which the organisation is willing to accept risk as trade-off to the expense of applying controls

Selecting a risk control strategy

- Level of threat and value of asset play major role in selection of strategy
- Rules of thumb on strategy selection can be applied:
  - When a vulnerability exists and can be exploited
  - When attacker's cost is less than potential gain
  - When potential loss is substantial
  - When cost of control < cost of impact

Redefining security in terms of risk

‘SECURITY IS A WELL-INFORMED SENSE OF ASSURANCE THAT THE RISKS AND CONTROLS ARE IN BALANCE’

Ronin background

- In this short clip the character Deidre (Natascha McElhone) describes the broad outlines of a mission:
- The main characters are:
  - Sam (Robert De Niro): an American
  - Grigor (Stellan Skarsgard): an Eastern European Telecoms expert
  - Vincent (Jean Reno): a Frenchman
  - Spence (Sean Bean): an Englishman
  - Larry (Skipp Suduth): a professional driver

Ronin

1. What is the mission (in security terms)?
2. What is going on in each character's mind?
3. Which one of the characters is thinking like a risk manager?
4. Explain his questions and behaviour

Today's session

1. WEEK 02 AND FIRST WORKSHOP
2. INFORMATION ASSET, THREAT, VULNERABILITY AND RISK
3. SECURITY THREATS AND RISKS TODAY
4. RISK MANAGEMENT
5. CONCLUDING REMARKS / WORKSHOP

Concluding remarks

1. Risk identification
   - A risk management strategy enables identification, classification, and prioritisation of organisation's information assets
   - Residual risk: risk that remains to the information asset even after the existing control is applied
2. Risk assessment
   - Consequence and likelihood evaluation
   - Quantitative (as per textbook) or qualitative methods
3. Risk control: four strategies are used to control risks that result from vulnerabilities:
   - Apply safeguards (avoidance)
   - Transfer the risk (transference)
   - Reduce impact (mitigation)
   - Understand consequences and accept risk (acceptance)

Workshop 03: Will be published over the weekendn

Headline

TAKE CALCULATED RISKS.
THAT IS QUITE DIFFERENT FROM BEING RASH.

George S. Patton,
Senior Officer, US Army