Information Security Risk Management

Dan Ionita

UTwente, Services and cybersecurity (scs.utwente.ewi.nl)

Information security

“The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. “

~SANS Institute

Information security goals

Information security aims to provide:

- **Confidentiality –** allowing only authorized access to information;
- **Integrity –** preventing undesired modification or destruction of information;
- **Availability** - ensuring timely and reliable access to the information.

Access control

The security of an information system is largely determined by its ability to **control access.**

Access control consists of:

- **Identification:** claiming identity
  Who are you?
- **Authentication:** verifying identity
  Are you really who you say you are?
- **Authorization:** providing access
  What rights do you have?

Identification

- Digital identification is most often based on entering a pseudonym:
  - Username, e-mail address, etc.
- It is only used to differentiate (types of) users from each other.
- There are increasing numbers of identity providers, e.g. login with Facebook or Google.

Authentication

Single-factor authentication:

- **Proof of knowledge**: something you know
  - e.g. PIN, password, secret
- **Proof of ownership:** something you have
  - e.g. key, card, device
- **Proof of inheritance:** something you are
  - e.g. fingerprint, voice, DNA

Two-factor authentication (2FA) or multi-factor authentication (MFA):

- Combinations of the above

Authorization

- Can be binary (access or no access)
- But most often it is gradual:
  - E.g. No access, Read, Write, Execute, Delete, Change, Full control.
- And often relies criteria to help manage permissions
  - Role-based
    - E.g. Wordpress distinguishes between administrators, editors, authors, contributors, subscribers.
  - Group-based
    - E.g. financial dept, HR department, IT department, etc.
- Should be periodically reviewed to prevent authorization creep.
  - By the manager, not the administrator!

Risk in the information age

Several factors make cyber-crime much harder to manage:

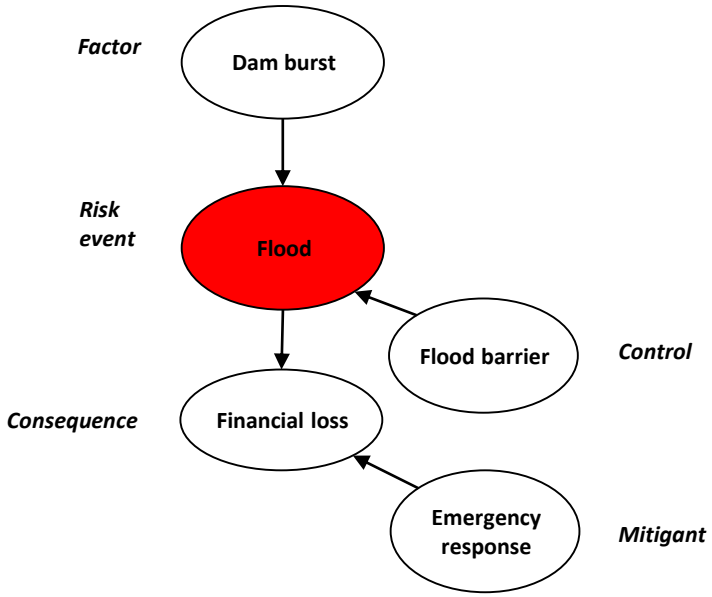
- Availability of hacking tools and tutorials
- Computation power of modern computers
- Anonymity provided by the Internet
- Complexity and diversity of modern computer networks

- Real-time cyber-attack map: http://map.norsecorp.com
- Estimated annual cost of cyber-crime: **$400 billion***
- Cost of cyber-crime projected to reach **$2 Trillion****

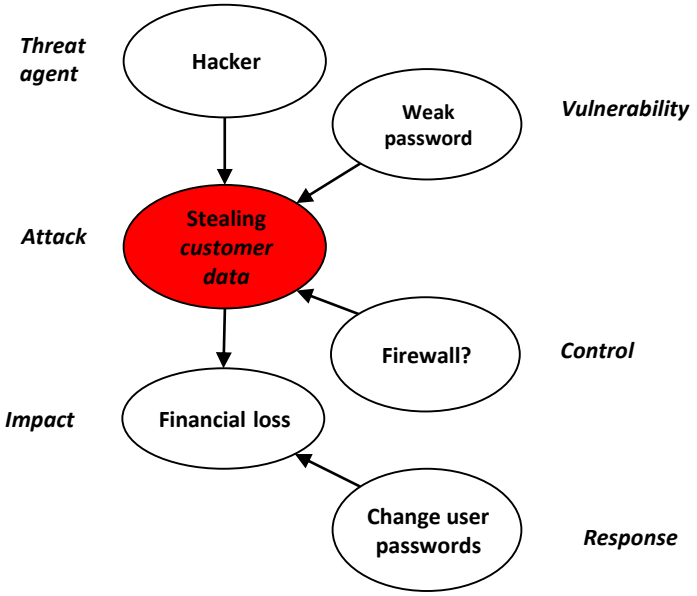
**Intel Security & McAfee, "Net Losses: Estimating the global cost of cybercrime", Center for Strategic and International Studies.*
*** Juniper research, "Cybercrime will cost businesses over $2 trillion by 2019"*

A slightly different taxonomy

Traditional risk

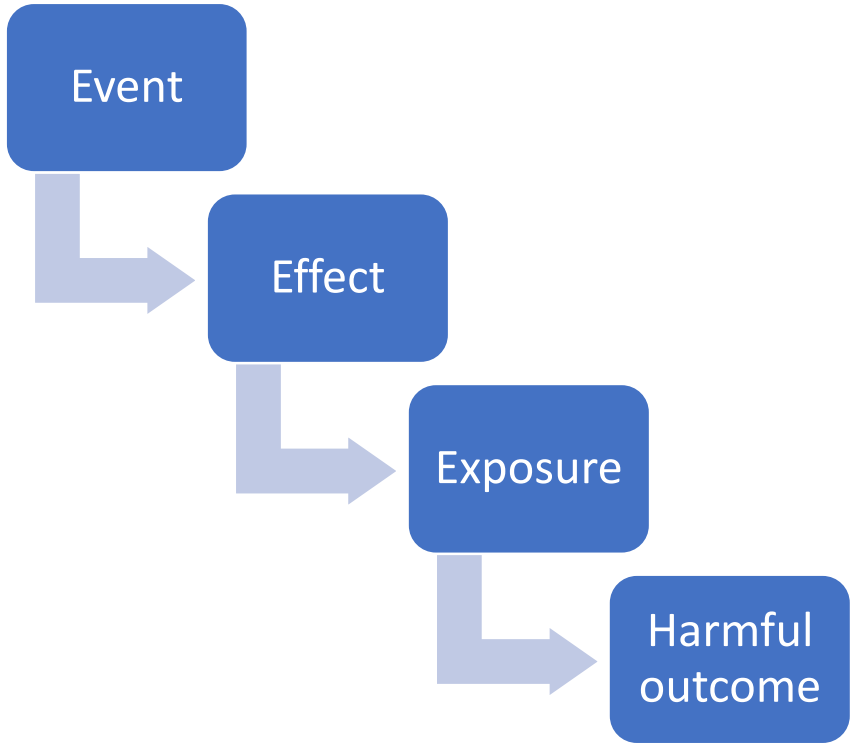


Cyber-security risk

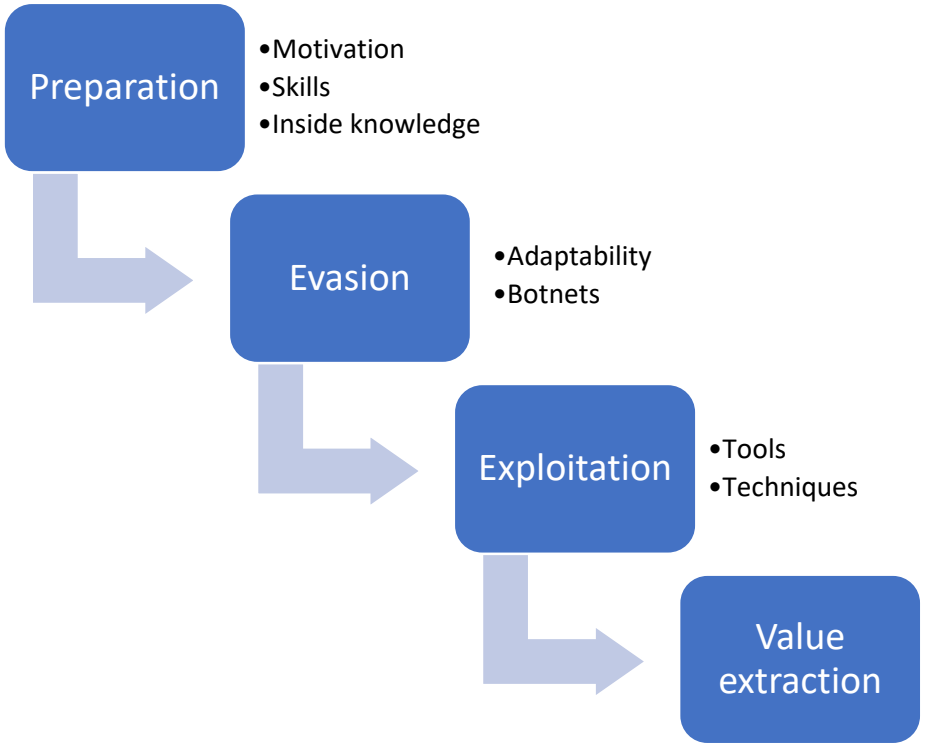


And an attacker perspective

Traditional incident



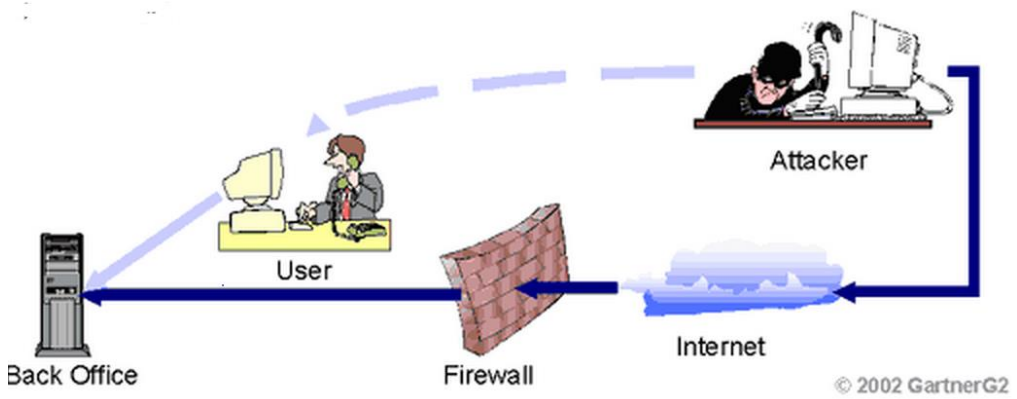
Cyber-security incident



Cyber-insecurity

Attackers can exploit all kinds of vulnerabilities:

- Vulnerable software or hardware
- Poor configuration
  - Weak encryption
  - Short or guessable passwords
- **Social Engineering**
  - Phishing
  - Tailgating
  - Impersonation
  - Malicious insiders
  - …



What is social engineering?

Hackers (1995)

Social engineering

- 70-90% of cyber-attacks exploit the human element*.
- Social engineers use phycological principles to manipulate another person:


Reciprocity


Consistency / Commitment


Consensus (previously Social Proof)


Authority


Liking


Scarcity

ENISA Threat Landscape 2018

Interactive version:
https://etl.enisa.europa.eu/

Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	→	1. Malware	→	→
2. Web Based Attacks	↑	2. Web Based Attacks	↑	→
3. Web Application Attacks	↑	3. Web Application Attacks	→	→
4. Phishing	↑	4. Phishing	↑	→
5. Spam	↑	5. Denial of Service	↑	↑
6. Denial of Service	↑	6. Spam	→	↓
7. Ransomware	↑	7. Botnets	↑	↑
8. Botnets	↑	8. Data Breaches	↑	↑
9. Insider threat	→	9. Insider Threat	↓	→
10. Physical manipulation/ damage/ theft/loss	→	10. Physical manipulation/ damage/ theft/loss	→	→
11. Data Breaches	↑	11. Information Leakage	↑	↑
12. Identity Theft	↑	12. Identity Theft	↑	→
13. Information Leakage	↑	13. Cryptojacking	↑	NEW
14. Exploit Kits	↓	14. Ransomware	↓	↓
15. Cyber Espionage	↑	15. Cyber Espionage	↓	→

Vulnerabilities

- A vulnerability is a weakness in a piece of software which can be abused by malicious actors.
  - Most often cause by a mistake of the programmer.
  - Fixed by patches (or updates), once *discovered.*

Zero-days

- **Zero-day** vulnerabilities are unknown to those interested in mitigating it.
  - developers, users, security researchers, etc
- Zero-day vulnerabilities can be exploited at will with minimal risk and very high chances of success.
- Zero-days can be sold for up to **$1.5 million**!
- Often, companies offer bounties for zero-days but they often cannot compete with the **zero-day black markets.**
- **Examples:**
  - Siguza's macOS priviledge escalation vulnerability (exploitable since 2002, disclosed Jan 2018)
  - HeartBleed (affected 2/3 web servers globally)

Malware

Malware = **mal**icious soft**ware** specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

- Many types:
  - Viruses and worms, e.g. Stuxnet
  - Trojans and bots, e.g. Srizbi
  - Ransomware, e.g. WannaCry
  - Spyware, e.g. keyloggers
  - Adware, e.g. search bars

- Usually delivered as an e-mail attachment, with pirated software, via infected USB sticks or via compromised or malicious websites.
  - Malware infections almost always happen as a result of a user action.

Web-based and web-application attacks

- Web-based attacks exploit the Internet infrastructure and attack websites.
- Attacks:
  - SQL injection: entering in malicious code instead of text into online forms.
  - XSS (Cross-Site Scripting): injecting malicious scripts into web pages.
  - Man-in-the-middle attacks: intercepting (and possibly modifying) traffic.
  - Infected browser or malicious extensions.
- Tools:
  - Network exploration, e.g. NMap
  - Vulnerability probing, e.g. Nessus
  - Traffic sniffing, e.g. WireShark
  - Password cracking, e.g. John the Ripper
  - Malware

Phishing

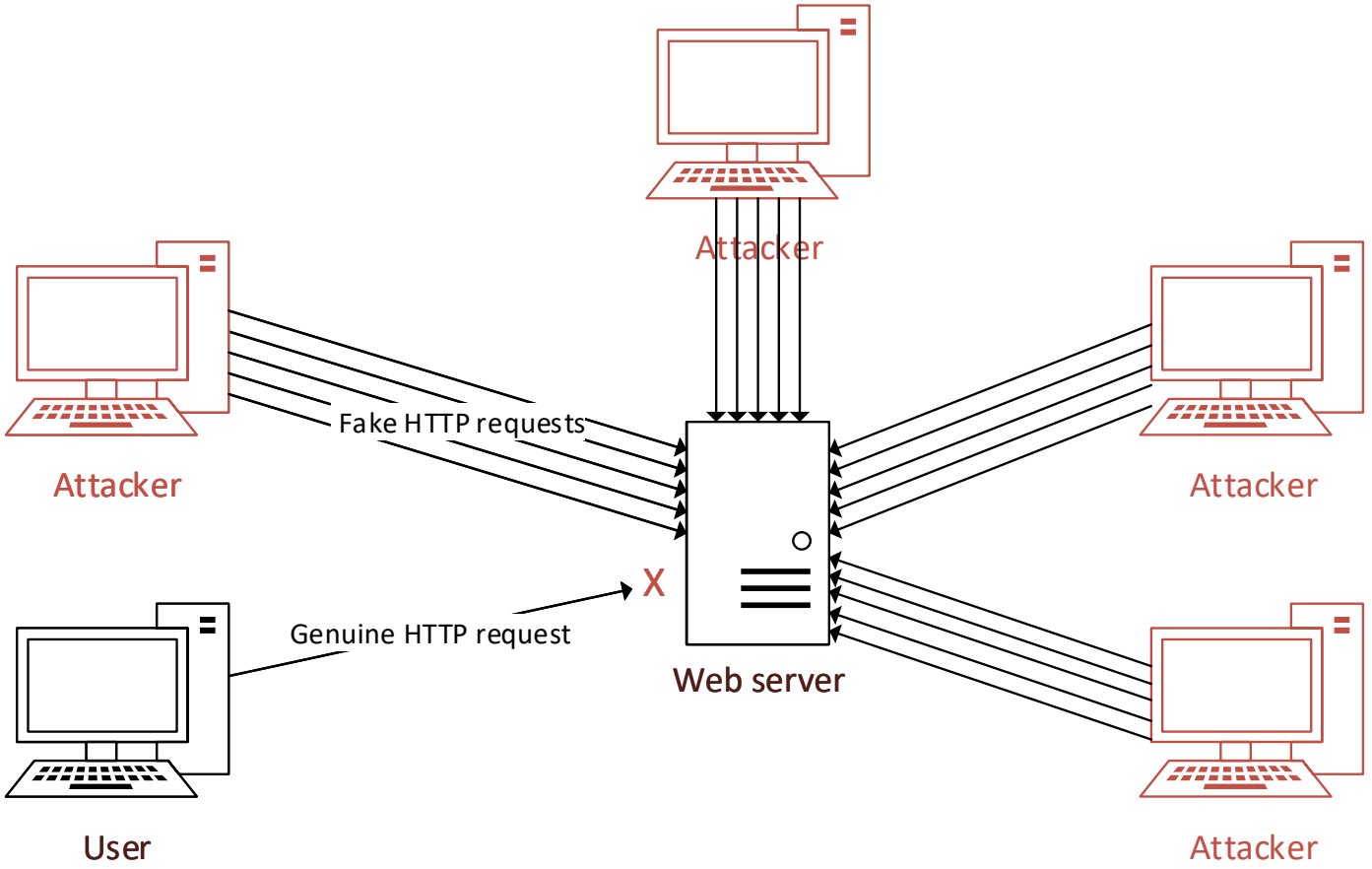
Phishing = malicious e-mail masquerading as legitimate

- Up to 90% of cyber-attacks start with phishing
- Also used for scams, credit card fraud, identity theft, etc.
- Estimated 156 million phishing emails sent daily
- Open rate of up to 30% (average newsletter has only 25%)

Spear phishing = targeted phishing using previously gathered information (e.g. OSINT)

- E.g. using your real name, or even the names of people you know
- Open rate of 70% or higher

(Distributed) Denial of Service



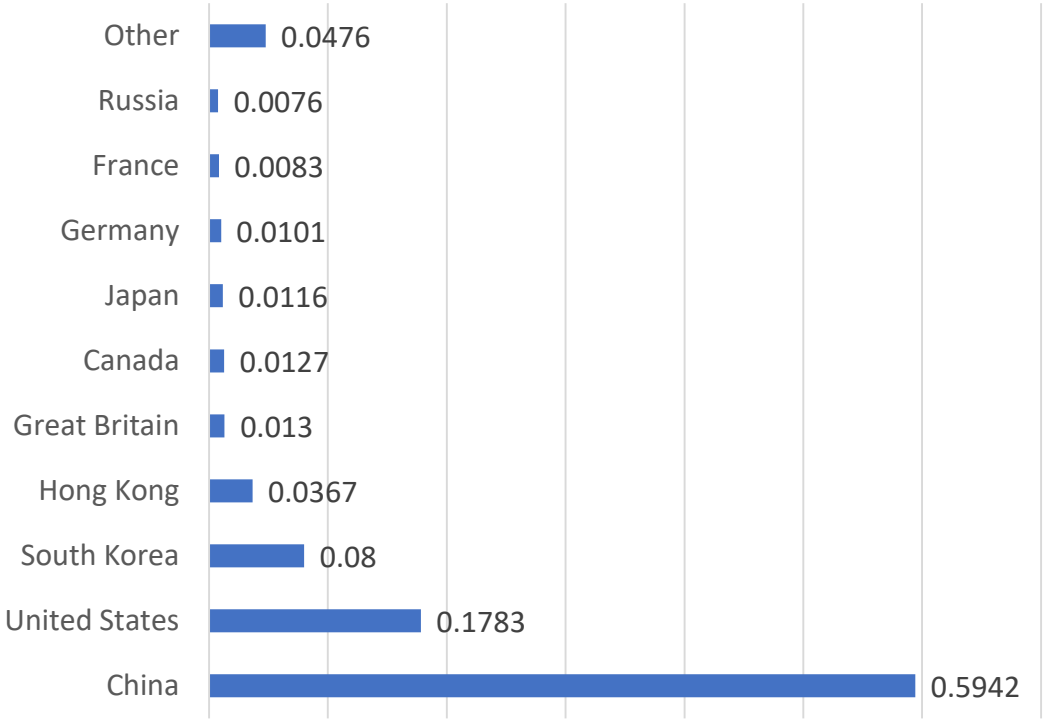
(Distributed) Denial of Service

- Most DDoS attacks are to and from China
- Longest sustained attack: 12 days *
- Main motivations: Online Gaming, attackers presenting their niche capabilities and extortion**.

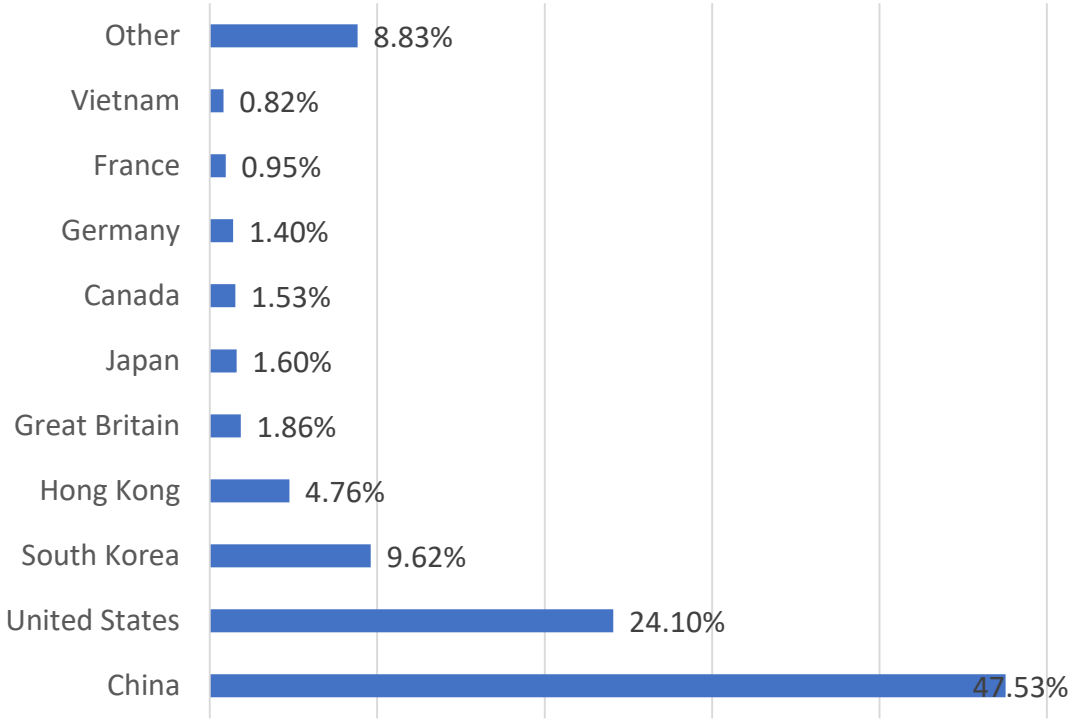
** https://securelist.com/ddos-report-in-q1-2018/85373/*
*** https://pages.arbornetworks.com/rs/082-KNA-087/images/13th_Worldwide_Infrastructure_Security_Report.pdf*

DDoS attacks by country (Q1 2018)

Origin



Target



SOURCE: https://securelist.com/ddos-report-in-q1-2018/85373/)

Spam

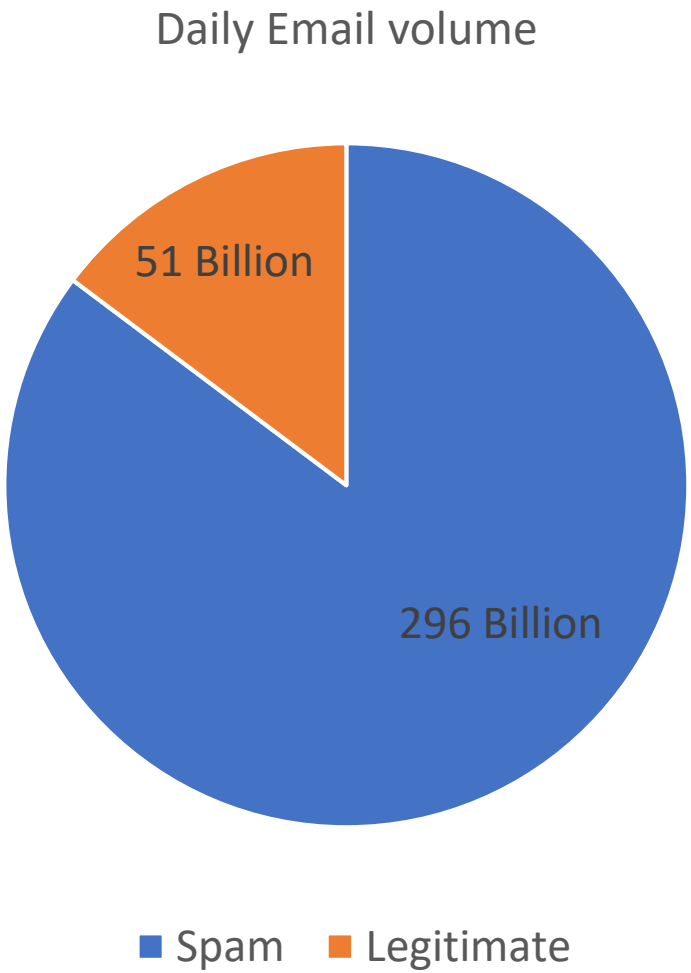
88% of spam comes from botnets

Top categories:

1. Health related spam (26,6%),
2. Spam delivering malware (25,7%)
3. Spam for online dating sites(21,4%)

Easy to mitigate:

- Spam filters
- SPF, DMARC, DKIM
- Awareness training



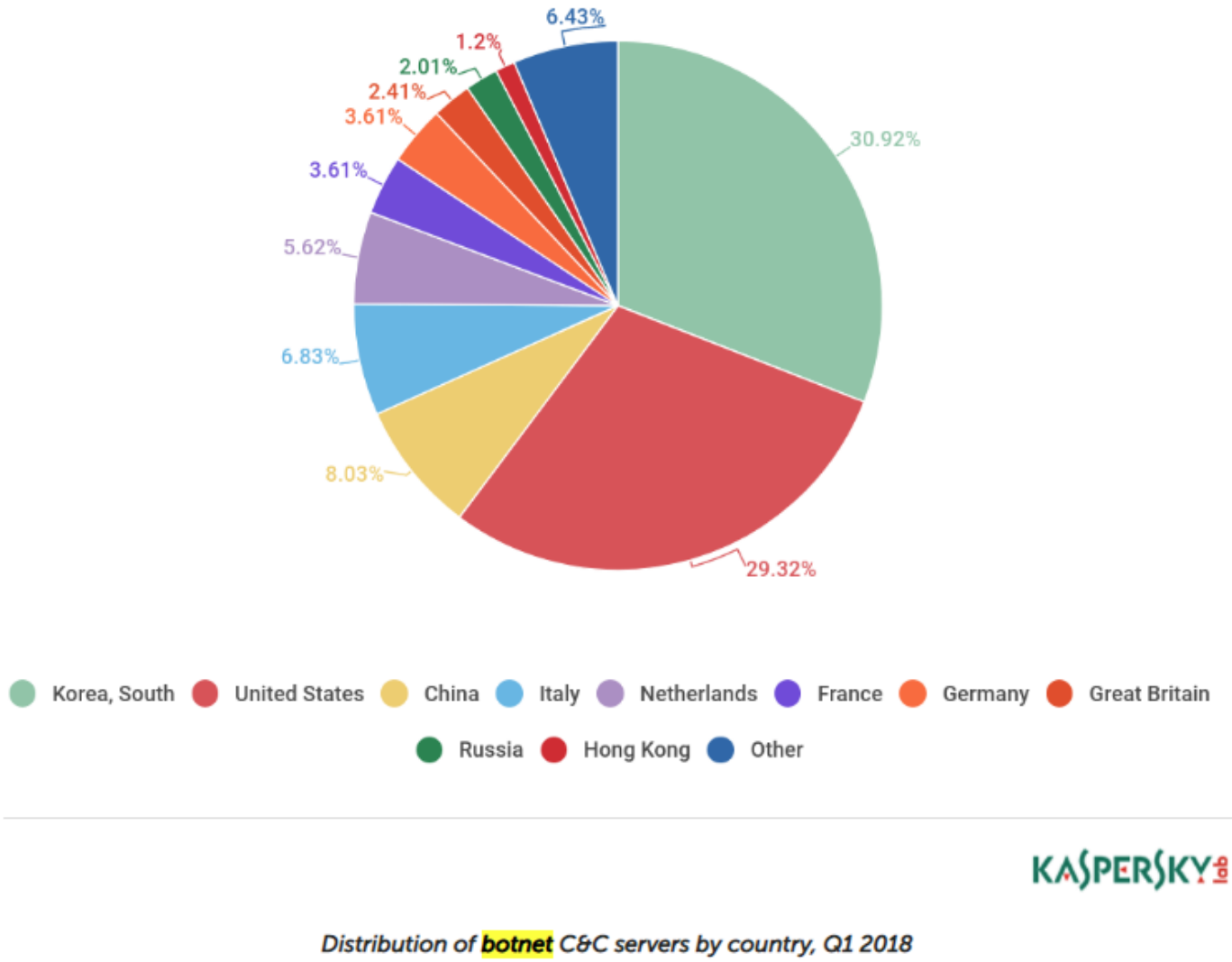
Source: https://www.talosintelligence.com/reputation_center/email_rep#global-volume, accessed October 2018.

Botnets

- 60-90% running Linux
- Many are IoT devices

Botnets are mostly used for DDoS and Spam

- 88% of *spam* comes from botnets



Distribution of botnet C&C servers by country, Q1 2018

Data breaches

25 million records were compromised or exposed every day for the first six months of 2018*; 1% were encrypted.

73% were carried out by malicious actors:

- Organized crime 50%
- State actors 12%

Most common attack vectors:

- SQL injection
- Phishing
- Insider threat
- Physical theft and loss

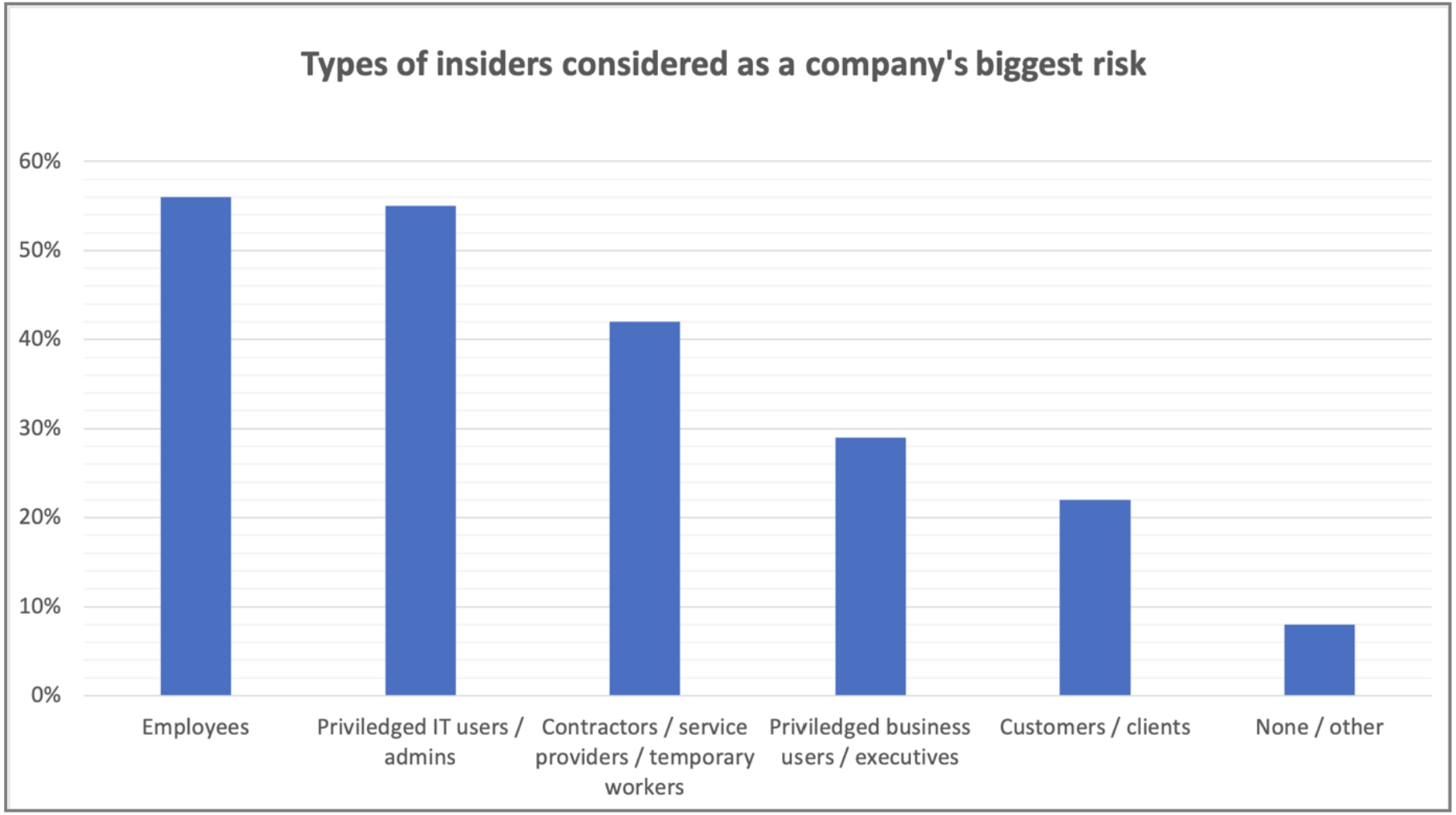
** https://www.gemalto.com/press/pages/data-breaches-compromised-4-5-billion-records-in-first-half-of-2018.aspx,*

Insider threat

- 77% of the companies' data breaches involve insiders*
  - Either willing:
    - Malicious
    - Disgruntled
    - Coerced
  - Or unwilling:
    - Phishing
    - Weak or reused passwords
    - Unlocked devices
    - Password sharing practice
    - Unsecured Wi-Fi
- Enabling factors:
  - Excessive privileges
  - Increasing number of devices with access to sensitive data
  - Increasing complexity of information technology
  - Increasing amount of sensitive data
  - Lack of training/awareness

** https://www.forcepoint.com/sites/default/files/resources/files/whitepaper_practical_executives_guide_data_loss_prevention_en.pdf,*

Insider threat



** https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf,*

Cryptojacking

- AKA malicious cryptomining
- Mines cryptocurrencies on infected machine
- Often aimed at datacenters, supercomputers or critical infrastructure
- Can also infect Android devices, browser extensionsand even websites

Ransomware

Ransomware encrypts data or changes passwords to block access to data.

Often with a ransom in cryptocurrency.

- Various goals:
  - Ransom
  - Extorsion
  - Reputation damage
  - Sabotage / destruction
- Enabling factor: Outdated or unpatched software and Oss

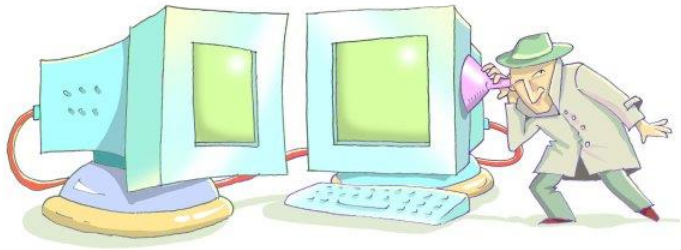
- Nations are getting involved
  - North Korea – WannaCry
  - Russia - NotPetya

The internet of things

- IoT Devices must meet strict requirements:
  - Size
  - Price
  - Energy usage
  - Complexity
- Therefore, there is not much room for security.
  - Proper authentication and configuration requires a GUI
  - End-to-end encryption is resource intensive
  - Secure software and frequent updates are expensive

The IoT provides hackers with plenty of low-hanging fruit: www.shodan.io

Side-channel attacks



- **Side-channel attacks** = extracting information from the physical characteristics rather than by compromising the software
  - e.g. timing, power consumption, EM leaks, sound, etc.

- Side-channel attacks often require less time and resources.
  - E.g. Cracking MyFare (OV-chipkaart) in minutes using optical recognition

- Many Internet-connected devices => many side-channels

Return on security investment

- Security is often an after thought or ignored completely
- Because **ROSI (Return on Security Investment)** is hard to estimate:
  - Dynamic threat landscape
    - Tools, motivations,
  - Zero-days
  - Lack of historical data
    - E.g. frequency of attacks
  - Damage is hard to quantify
    - Often reputational
- And because security often comes at **high cost** (not only financial)

Good enough security

- **100% cyber-security is impossible.**
- Therefore one should aim for **good-enough security**:
  - Based on well-defined risk-acceptance criteria
    - Do not invest in things you do not need
  - Proportional to that of similar organizations
    - Build a fence higher than your neighbor
  - In-line with best-practice guidelines
    - Avoid script-kiddies and automated tools (95% of attacks)

Conclusions

Cyber-risk management:

- Is as much about the technology as it is about the humans using it
  - Social engineering is used in over 2/3 of all attacks by hackers, hacktivists and nation states.*
- Is as much about prevention as it is about detection:
  - A new zero-day vulnerability was discovered every week in 2015**
- Is difficult and expensive
  - Requires technical knowledge and constant investment in time&money
- Is absolutely essential for the modern enterprises.
  - Even “offline” companies rely on IT systems internally.

* social-engineer.org

** 2016 Symantec Internet Security Threat Report

Information Security Risk Management in organisations (ISRM)

"ISRM is a process aiming at an efficient balance between realizing opportunities for gains while minimizing vulnerabilities and losses"

~European Network and Information Security Agency (ENISA)

Information Security Risk Management (ISRM)

Risk management is a continuous (cyclical) process concerned with:

1. Risk assessment
2. Risk treatment
3. Monitoring and control

Risk assessment

Risk Assessment = phase of Risk Management

1. Analyze an infrastructure,
2. Identify vulnerabilities,
3. Select countermeasures.

Qualitative ISRA method

		Likelihood		
		Low	Medium	High
Consequence	High	Medium	High	High
	Medium	Low	Medium	High
	Low	Low	Low	Medium

Semi-qualitative ISRA method

			Likelihood				
			Rare	Unlikely	Possible	Likely	Certain
			<0.0001	0.001	0.01	0.1	1
Consequence	Catastrophic	$50,000,000					
	Major	$5,000,000					
	Significant	$500,000					
	Minor	$50,000.00					
	Insignificant	< $5000					

Quantitative ISRA

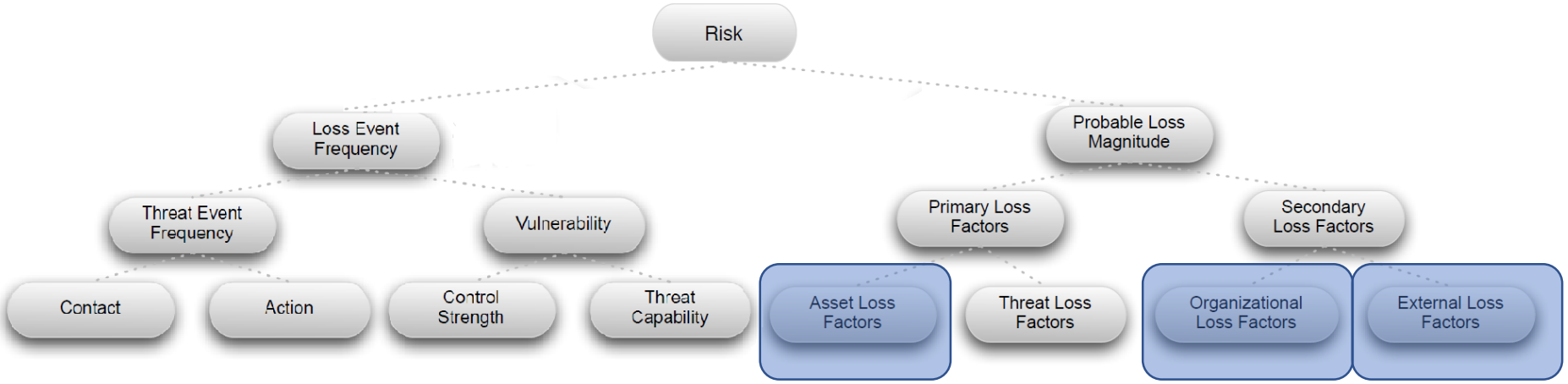
ITEM	Possible Risk Factor	QUALITATIVE ANALYSIS				QUANTITATIVE ANALYSIS		REMARKS
		L	I	D	RPN	RISK	PR	
1	Substructure	7.93	7.94	8.06	507.49	0.63	0.11376	HR
2	Floor space designation	5.4	5.4	5.40	157.46	0.29	0.05269	Irrelevant
3	Structural framework	6.02	6.98	6.02	252.96	0.42	0.07592	MR
4	Block work	6.85	6.85	6.85	321.42	0.47	0.08478	HR
5	Carpentry	5.02	5.02	5.02	126.51	0.25	0.04553	Irrelevant
6	Joinery	5.44	5.44	5.44	160.99	0.30	0.05347	Irrelevant
7	Roofing	6.49	6.49	6.49	273.36	0.42	0.07610	MR
8	Finishes	7.65	7.64	7.75	452.96	0.58	0.10560	VR
9	Electrical and IT	7.83	7.9	7.90	488.67	0.62	0.11176	HR
10	Mechanical installations	7.89	7.86	7.77	481.86	0.62	0.11205	HR
11	External works	6.83	6.82	6.78	315.82	0.47	0.08416	MR
12	Furniture/ Fenestration/ Installations	6.83	6.82	6.78	315.82	0.47	0.08416	Irrelevant

Source: Joseph Ignatius Teye Buertey, "Project Cost Risk and Uncertainties: Towards a Conceptual Cost Contingency Estimation Model", International Journal of Construction Engineering and Management, 2014

Criticism of quantitative approaches in IS risk assessment

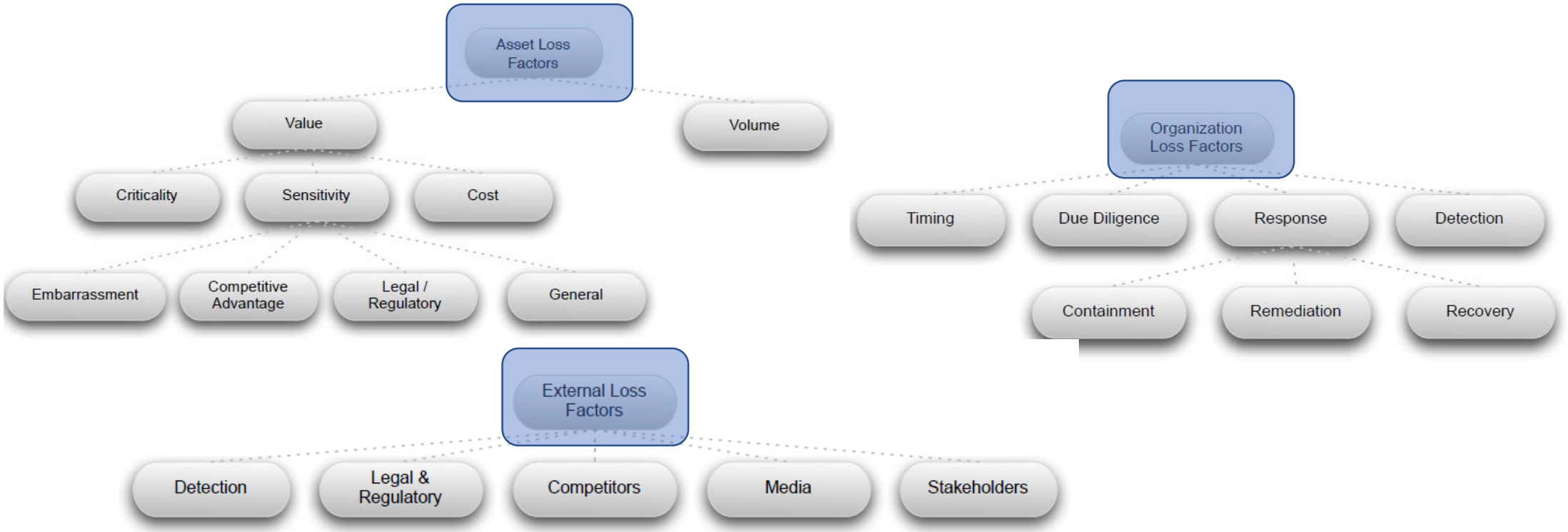
- While qualitative approaches are more accurate in traditional risk management, their utility is questionable when applied to Information Security Risk Management:
  - Limited historical data:
    - Many cyber-attacks are new
    - Breaches are not always reported
  - And the data that is there is rarely applicable
    - Likelihood depends on many other factors
    - Zero-days

Factor analysis of information risk (I)



Source: Jack A. Jones, An Introduction to Factor Analysis of Information Risk (FAIR), Risk Management Insight LTD.

Factor analysis of information risk (II)



Source: Jack A. Jones, An Introduction to Factor Analysis of Information Risk (FAIR), Risk Management Insight LTD.

Risk treatment

There are four ways to treat risk:

- **Accept** the risk as it is;
- **Mitigate** the risk by implementing countermeasures or controls;
- **Avoid** the risk altogether by eliminating the vulnerable activity or component;
- **Transfer** the risk to a third-party (e.g. insurance)

Monitoring and control

“Security Monitoring is the process by which organizations perform (real-time), threat prioritized collection, normalization and analysis of data generated by users, applications and infrastructure, put in context by organizational information and cyber threat intelligence.”

~ Deloitte

Why monitor and control?

- It is impossible to prevent all attacks!
  - You might not be aware of all attacks:
    - Because modern interconnected systems are too complex to thoroughly analyze;
    - Because new vulnerabilities are discovered all the time (one per week in 2015**).
  - You might not be able to defend against all attacks:
    - Because some countermeasures might be too expensive
    - Because the risk was not considered severe enough

*** 2016 Symantec Internet Security Threat Report*

Monitoring and control goals

- Provide actionable alerts and comprehensive insights;
  - which can be used to reduce the impact of attacks;
  - or reduce the likelihood of future attacks.

- A secondary goal is assessing the efficiency of existing countermeasures and security policy.

Monitoring and control tools and techniques

Monitoring:

- Security information and event management (SIEM) software provides real time analysis of security events;
- Intrusion Detection Systems (IDS):
  - Network Intrusion Detection Systems (NIDS) monitor network traffic
  - Host Intrusion Detection Systems (HIDS) monitor system activity
- Intrusion Protection Systems (IPS) block malicious activity based on IDS;

Control:

- Pen testing and red teaming

Response and recovery

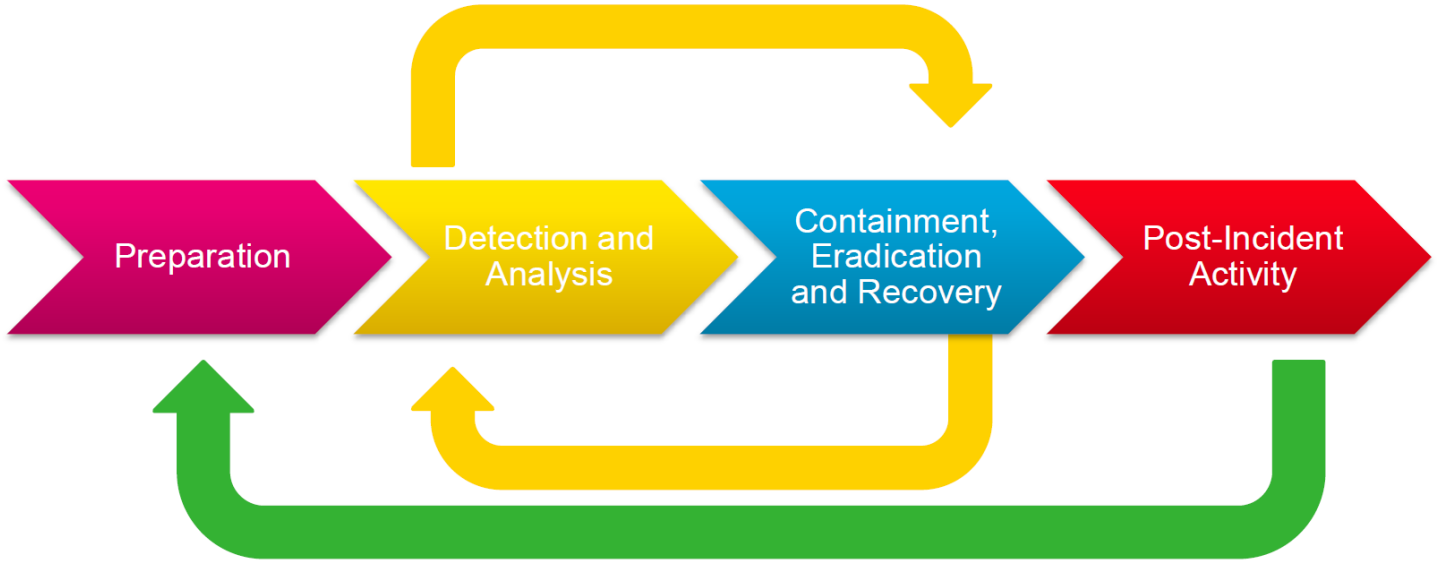
What is an incident?

- And incident is a chain of events leading to what Colin Sheppard called the **breach triad:**
  - **Infiltration** (i.e. obtaining access)
  - **Aggregation** (i.e. obtaining something valuable)
  - **Exfiltration** (i.e. escaping with the valuable asset)

The kill chain

Source: novainfosec.com

Response and recovery process



Source: NIST Computer Security Incident Handling Guide – SP 800-61 Rev2

Response and recovery phases

1. **Prepare** incident readiness:
   - Know and understand your systems, data;
   - Define teams, responsibilities and means of communication;
   - Set up incident detection measures and incident response plans;
   - Perform training.

2. **Detect and analyze** events:
   - Examine IDSs and “crime scene”;
   - Gather and store all available data about incidents;
   - Analyze data to determine cause, who/what is affected.

Response and recovery phases

3.Contain incident:

- Execute incident response plan;
- Implement impact reduction measures;
- Get the business back to normal;

4.Post-incident:

- (re-)test if the threat was eliminated;
- Recommend more structural changes.