OPEN SECURITY SUMMIT

June | 2020

Open Information Security Risk Universe

Robin Oldham & Phil Huggins
Cydea & CISO Mentor

Instructions!

RISK SCENARIO:

<Please write a risk scenario>

1. Write the story of the risk.

Breakout Room 1 (click for your slide)

Breakout Room 2 (click for your slide)

Breakout Room 3 (click for your slide)

Breakout Room 4 (click for your slide)

Breakout Room 5 (click for your slide)

RISK STATEMENT:

SOURCE	EVENT	CONSEQUENCE
2. Who is the source of the risk?	3. What actually happens?	4. What is the actual harm when this risk occurs?

Risk statement components

Sources ↗

Events ↗

Consequences ↗

Source	Internal/External	Malicious/Non-Malicious
Disgruntled	Internal	Malicious
Accidental	Internal	Non-Mal
Ineffective	Internal	Non-Mal
Criminal	Internal	Malicious
Coerced	Internal	Malicious
Criminals	External	Malicious
Hacktivists	External	Malicious
Compromised suppliers	External	Non-Mal
State-Sponsored	External	Malicious
Competitor	External	Malicious
Press	External	Non-Mal
Researcher	External	Non-Mal
Regulator	External	Non-Mal

Level 1	Level 2	CIA
Abusive Content	Harmful Speech	
	Child / Sexual / Violent Content	
	Harassment	
Malware	Ransomware	Availability
	Worm	Confidentiality, Integrity, Availability
	Spyware	Confidentiality
	Rootkit	Confidentiality, Integrity, Availability
	Dialler	
Gathering		
	Network Scanning	

Level 1 Consequences	Level 2 Consequences
Operations	Reduced growth
	Business Disruption
	Ineffective Change
	Slow recovery
	Reduced access to staff / skills
	Loss of suppliers
	Environmental harm
	Safety failure
	Social harm
	Medical harm
	on-compliance
	or conduct / integrity

oisru.org

Breakout Room 1

Maersk / NotPetya Ransomware

RISK SCENARIO:

Major outage of global IT infrastructure due to a malware incident that disrupted business operations. Time to restore IT operations is out-of-tolerance.

The story… wired.com

- Maersk are a large international shipping company
- Attackers compromised an accountancy package
- That infected the whole IT landscape with ransomware
- The ransomware used ExternalBlue and Mimikatz to rapidly spread across their entire global network


WIRED

The Untold Story of NotPetya, the Most Devastating Cyberattack in History

Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world.

IT WAS A perfect sunny summer afternoon in Copenhagen when the world's largest shipping conglomerate began to lose its mind.

The headquarters of A.P. Møller-Maersk sits beside the breezy, cobblestoned esplanade of Copenhagen's harbor. A ship's mast carrying the Danish flag is planted by the building's northeastern corner, and six stories of blue-tinted windows look out over the water, facing a dock where the Danish royal family parks its yacht. In the building's basement, employees can browse a corporate gift shop, stocked with Maersk-branded bags and ties, and even a rare Lego model of the company's gargantuan Triple-E container ship, a vessel roughly as large as the Empire State Building laid on its side, capable of carrying another Empire State

RISK STATEMENT:

SOURCE	EVENT	CONSEQUENCE
Malicious actors, suspected Nation State APT via 3rd party compromise	Global IT outage	Reputational damage Business Disruption Increased costs Medical harm (damage to Ukrainian health system)

Breakout Room 2

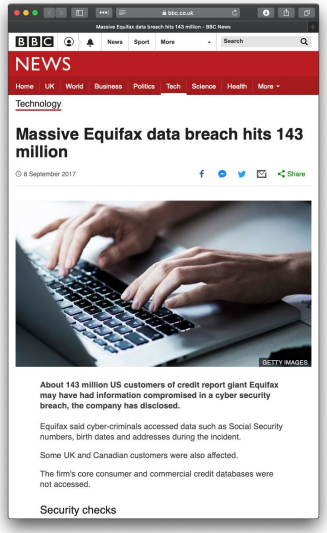
Equifax / Data breach

RISK SCENARIO:

<We hold personal information for our consumers, this may become available through the website if we have do not adequately protect our code or third party components. This may result in regulatory action/fines and reputational damage.>

The story… bbc.co.uk

- Equifax are a credit reference agency, holding large quantities of personal data
- An attacker exploited an unpatched vulnerability in Apache Struts to gain access
- Over 76 days they collated and exfiltrated information on 143 million U.S. citizens



RISK STATEMENT:

SOURCE	EVENT	CONSEQUENCE
1. External Malicious (criminal) 2. Internal Non-Malicious (ineffective/accidental)	<Information Breach - Unauthorised access to the system resulting in unauthorised access to data (confidentiality and integrity)>	<Regulatory Fines, Unexpected Costs and reputational damage>

Breakout Room 3

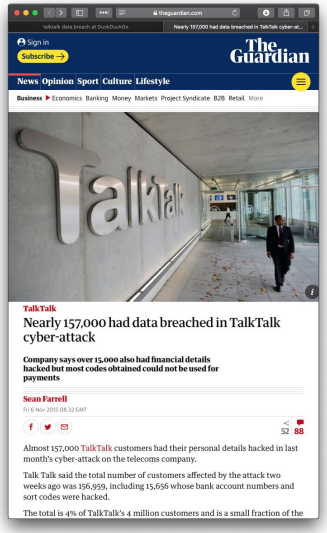
TalkTalk / Ransom breach

RISK SCENARIO:

External malicious actors, including organised cybercriminals or malicious hackers, and to a lesser extent- nation states and/or hacktivists, exploit known technical vulnerabilities on public-facing systems, gaining access to sensitive customer data records, resulting in a catastrophic data breach. A large-scale breach (10,000k records) could result in widespread disruption to business operations and customer access to services, reputational damage manifesting in a reduction of shareprice and loss of custom, legal costs and the potential for hefty regulatory fines.

The story… theguardian.com

- An ISP in the UK
- Someone found an SQL injection vuln in an old website.
- They stole 157,000 people's details, including full names, addresses, email addresses, dates of birth
- The attacker then sent a sample to the CEO demanding a ransom



Breakout Room 4

Australian Sewage H

RISK SCENARIO:

<Please write a risk scenario>

3. What actually happens?

1. Write the story of the risk.

4. What is the actual harm when this risk occurs?

The story... theregister.com

- Vitek Boden had conducted a series of electronic attacks on the Maroochy Shire sewage control system after a job application he had made was rejected by the area's Council.
- Boden made at least 46 attempts to take control of the sewage system during March and April 2000. On 23 April, the date of Boden's last hacking attempt, police who pulled over his car und radio and computer equipment.

RISK STATEMENT:

SOURCE	EVENT	CONSEQUENCE
Disgruntled external party	<Event(s)>	<Consequence(s)>

Breakout Room 5

German Steel Mill Cyber Attack

RISK SCENARIO:

Safety critical hack of control systems

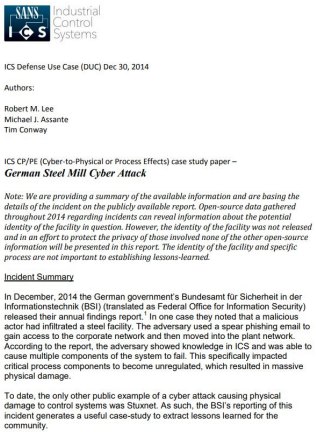
An employee opens targeted 'spear-phishing' email with a malicious attachment. The software exploit will give a sophisticated attacker access to our network where they can collect other information, such as credentials, that give them access to control software governing our smelting process. If the process is changed it may become unsafe and require us to shut down the furnace.

RISK STATEMENT:

SOURCE	EVENT	CONSEQUENCE
State-Sponsored	Phishing Software Exploit Stolen Credentials	Safety failure Business disruption Unplanned costs

The story… sans.org [PDF]

- In December, 2014 a malicious actor had infiltrated a steel facility
- The adversary used a spear phishing email to gain access to the corporate network and then moved into the plant network
- According to the report, the adversary showed knowledge in ICS and was able to cause multiple components of the system to fail
- This specifically impacted critical process components to become unregulated, which resulted in massive physical damage



SANS ICS Industrial Control Systems

ICS Defense Use Case (DUC) Dec 30, 2014

Authors:

Robert M. Lee
Michael J. Assante
Tim Conway

ICS CP/PE (Cyber-to-Physical or Process Effects) case study paper –
German Steel Mill Cyber Attack

Note: We are providing a summary of the available information and are basing the details of the incident on the publicly available report. Open-source data gathered throughout 2014 regarding incidents can reveal information about the potential identity of the facility in question. However, the identity of the facility was not released and in an effort to protect the privacy of those involved none of the other open-source information will be presented in this report. The identity of the facility and specific process are not important to establishing lessons-learned.

Incident Summary

In December, 2014 the German government's Bundesamt für Sicherheit in der Informationstechnik (BSI) (translated as Federal Office for Information Security) released their annual findings report.[1] In one case they noted that a malicious actor had infiltrated a steel facility. The adversary used a spear phishing email to gain access to the corporate network and then moved into the plant network. According to the report, the adversary showed knowledge in ICS and was able to cause multiple components of the system to fail. This specifically impacted critical process components to become unregulated, which resulted in massive physical damage.

To date, the only other public example of a cyber attack causing physical damage to control systems was Stuxnet. As such, the BSI's reporting of this incident generates a useful case-study to extract lessons learned for the community.