ISOM 5280:
Risk Management;
Contingency Planning; Law

Prof. Weiyin Hong

Department of ISOM, HKUST Business School

Fall 2024

Reading

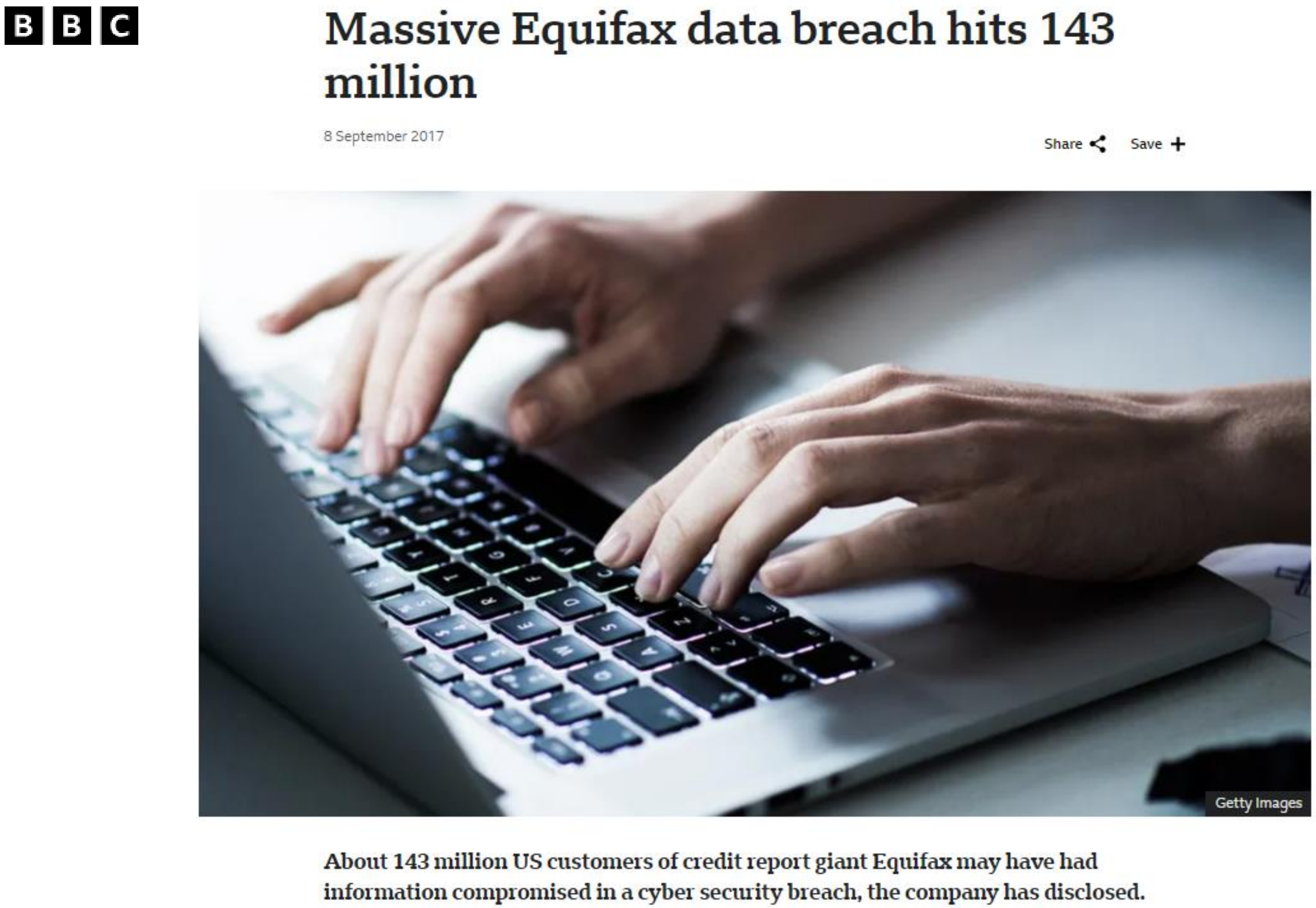
- [WM] – Chapters 4, 5, 6

Table of Contents

- Risk Management
- Contingency Planning

Risk Management

Data Breach - The Equifax Case



BBC

Massive Equifax data breach hits 143 million

8 September 2017

About 143 million US customers of credit report giant Equifax may have had information compromised in a cyber security breach, the company has disclosed.

Funded in 1899, Equifax is one of the three major credit reporting companies in the US. It is responsible for collecting and providing information on credit-worthiness to organization and individuals.

Before the incident…

- “We are regularly the target of attempted cyber and other security threats” – had a number of security lapses
- Security was managed by the chief legal officer (CLO), who manages chief security officer (CSO), while IT was managed by CIO
- Security alerts from Deloitte, Mandiant, Cyence, and an independent researcher, who warned about unpatched system and misconfigured security policies
- No evidence of data breach plans or regular audits of information security policies and systems

“Every time there was a discussion about doing something, we had a tough time to get management to understand what we were even asking.” – a former employee at Equifax

How it happened…

- A security vulnerability of Apachi (used to build web applications) were discovered on March 6 and warning message sent to Equifax CSO and his team on March 8 and then about 430 employees on March 9
- Failed to patch the system within 48 hours as security policy stipulated
- On March 16, the vulnerability was discussed at the monthly security meeting, but most senior managers typically did not attend it

How it happened…

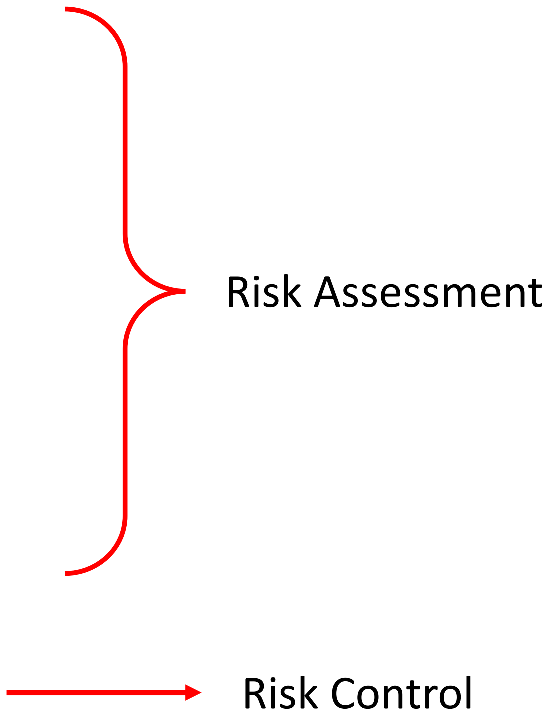
- Hackers scanning for the unpatched vulnerability discovered it on March 10, then created 30 backdoors into Equifax's systems
- On March 13, hackers began collecting personally identifiable information (PII)
- On March 14, the patch was installed and immediately blocked a significant number of attempts

Discover and Respond to the breach…

- On July 29-30, Equifax's security team noticed the data breach and shutdown the malware
- On July 31, CSO informed CIO
- On August 2, Equifax retained Mandiant, law firm, and FBI.
- On August 24-25, the full board was notified by telephone.
- On Sept 1, the board met to discuss the breach.
- On Sept 7, Equifax publicly announces the breach.

The Risk Management Framework

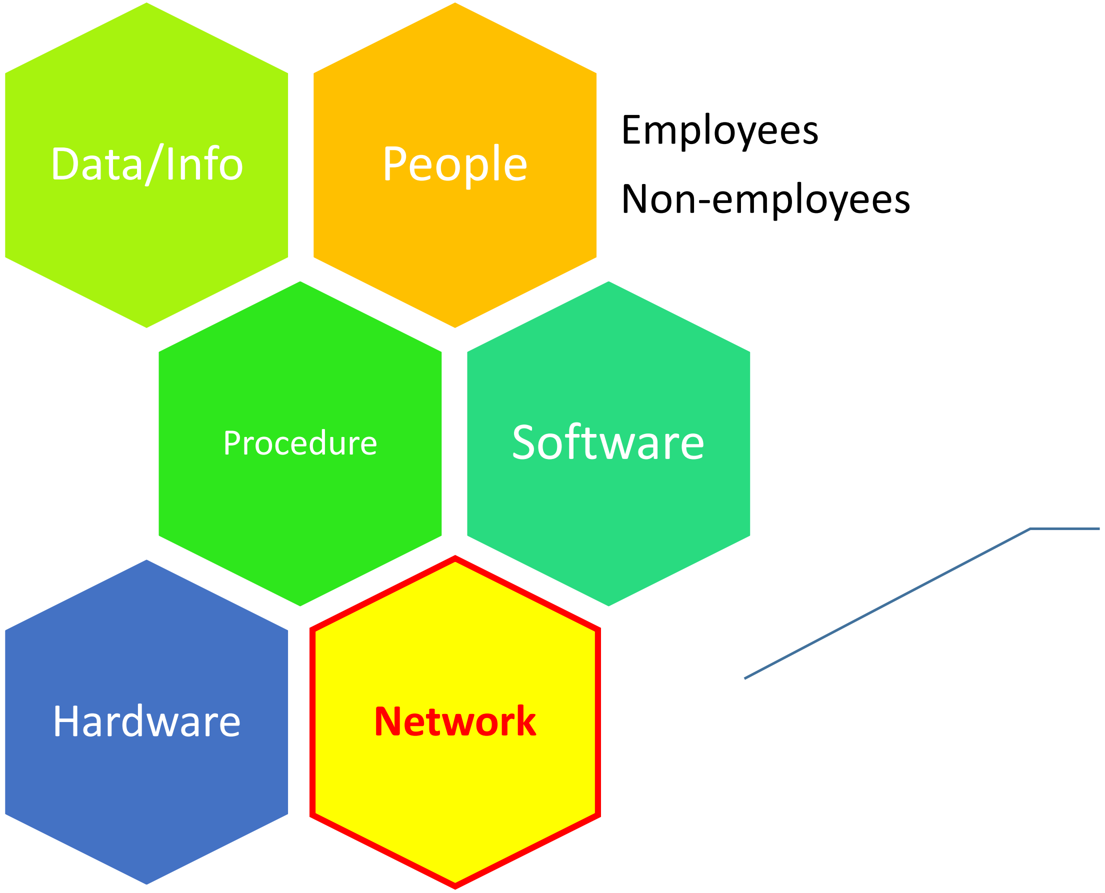
- Where and what is the risk (risk identification)? - Identifying assets
- How severe is the current level of risk (risk analysis)? - Identifying vulnerabilities
- Is the current level of risk acceptable (risk evaluation)?
  - Threat/Asset matrix (qualitative)
  - Quantitative risk assessment
- What do I need to do to bring the risk to an acceptable level (risk treatment)?



Risk Assessment

Risk Control

1. Identifying Assets

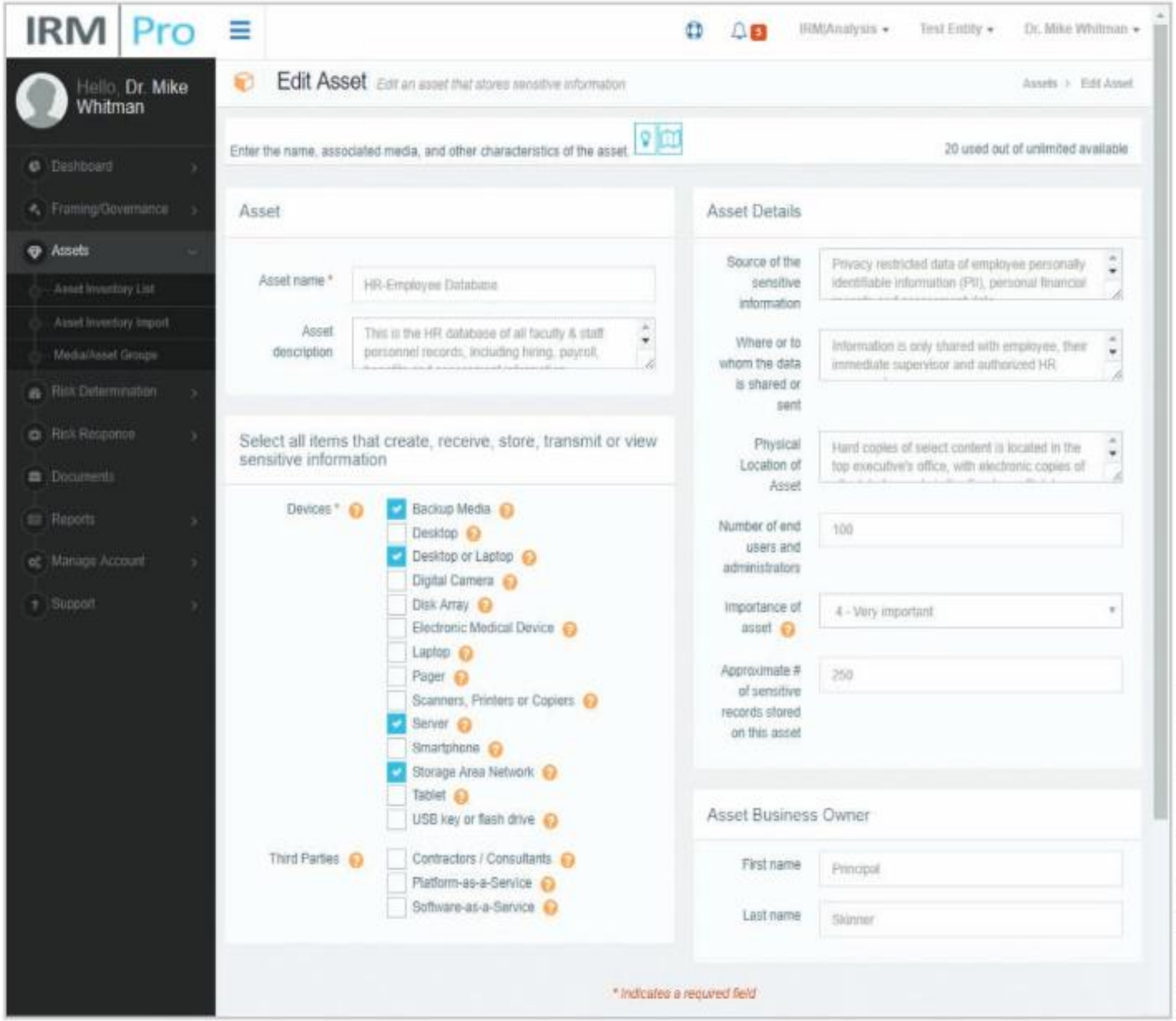


Employees

Non-employees

- Name
- Asset tag
- Asset type
- IP address
- MAC address
- Serial number
- Manufacture
- Manufacture model or part number

ClearWater IRM Information Asset Description



Edit Asset *Edit an asset that stores sensitive information*

Enter the name, associated media, and other characteristics of the asset.

20 used out of unlimited available

Asset

Asset name *: HR-Employee Database

Asset description: This is the HR database of all faculty & staff personnel records, including hiring, payroll,

Select all items that create, receive, store, transmit or view sensitive information

Devices *
- ☑ Backup Media
- □ Desktop
- ☑ Desktop or Laptop
- □ Digital Camera
- □ Disk Array
- □ Electronic Medical Device
- □ Laptop
- □ Pager
- □ Scanners, Printers or Copiers
- ☑ Server
- □ Smartphone
- ☑ Storage Area Network
- □ Tablet
- □ USB key or flash drive

Third Parties
- □ Contractors / Consultants
- □ Platform-as-a-Service
- □ Software-as-a-Service

Asset Details

Source of the sensitive information: Privacy restricted data of employee personally identifiable information (PII), personal financial

Where or to whom the data is shared or sent: Information is only shared with employee, their immediate supervisor and authorized HR

Physical Location of Asset: Hard copies of select content is located in the top executive's office, with electronic copies of

Number of end users and administrators: 100

Importance of asset: 4 - Very important

Approximate # of sensitive records stored on this asset: 250

Asset Business Owner

First name: Principal

Last name: Skinner

* Indicates a required field

Source: Clearwater Compliance IRM.

Figure 4-2 Clearwater IRM information asset description

✓ *How critical is the asset to the success of the organization?*

✓ *How much does the information asset contribute to profit generation?*

✓ *How expensive is the information asset to replace?*

✓ *How expensive is the information asset to protect?*

✓ *How much embarrassment or liability would the asset’s loss or compromise cause?*

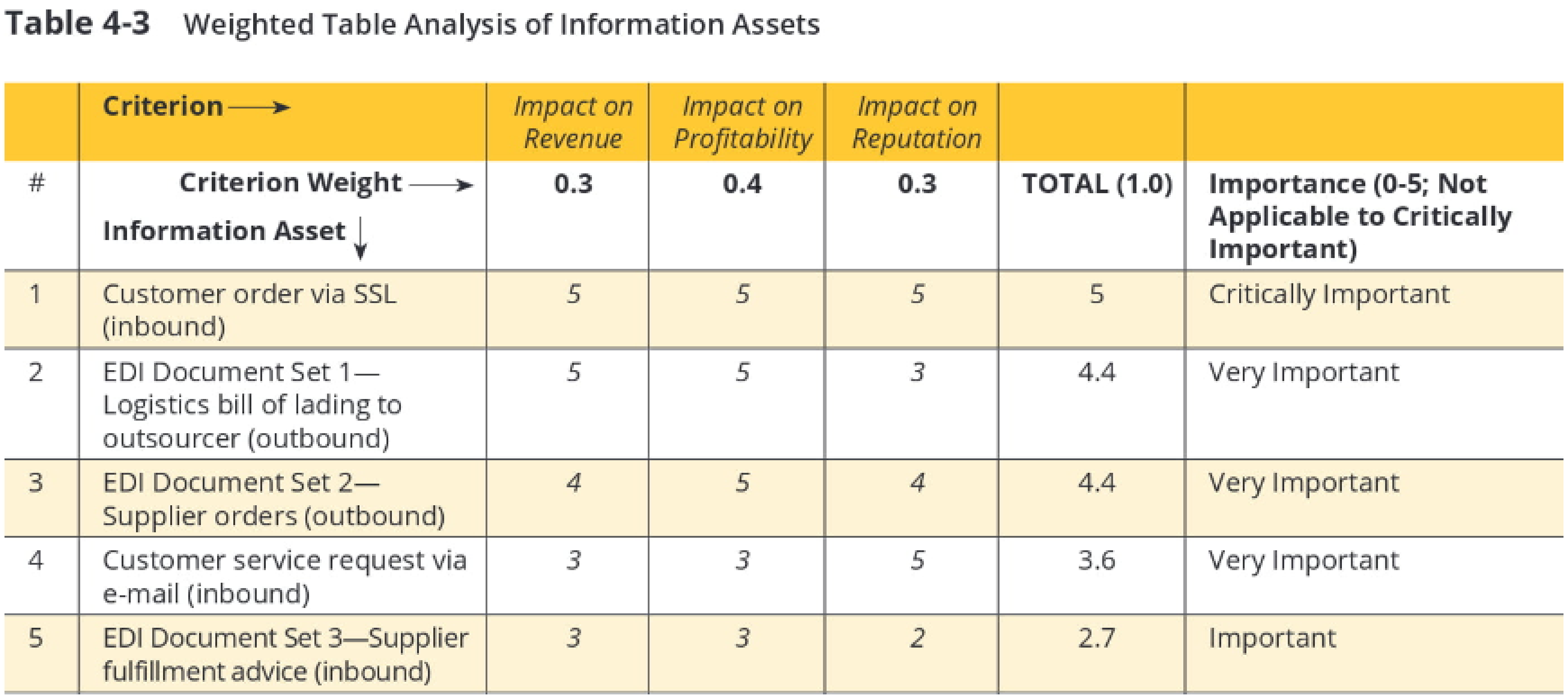


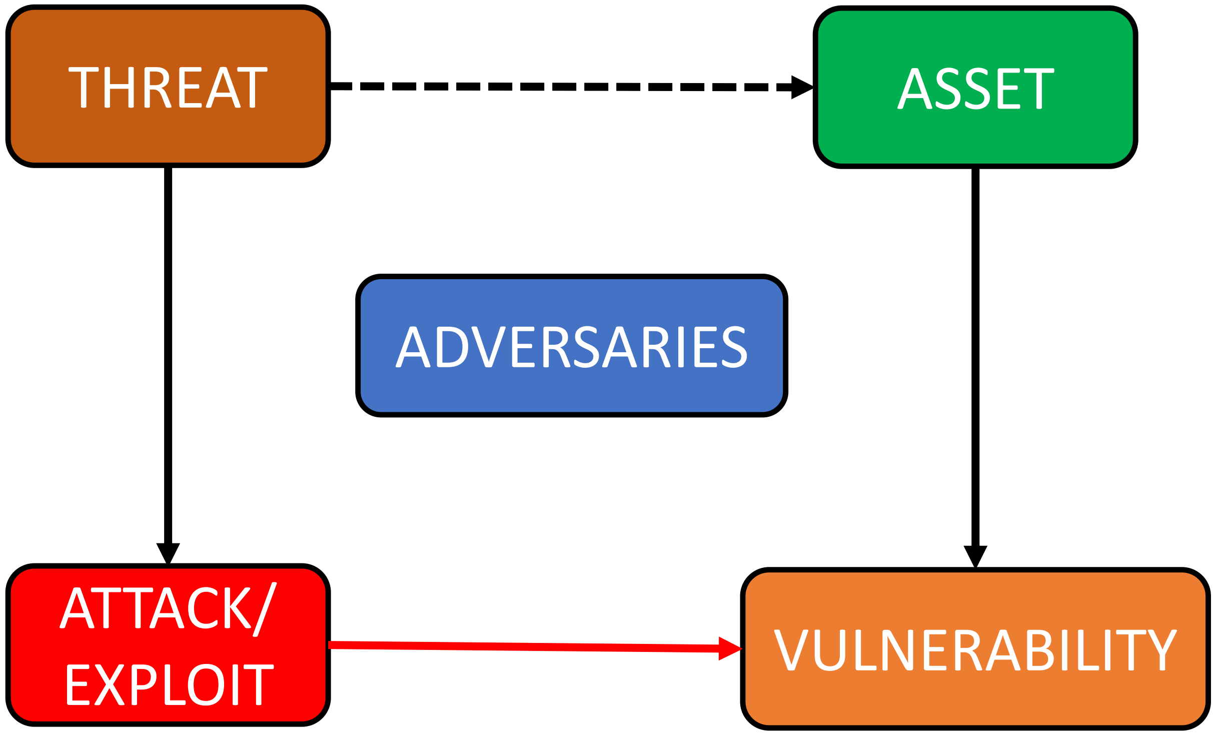
Table 4-3 Weighted Table Analysis of Information Assets

	Criterion →	*Impact on Revenue*	*Impact on Profitability*	*Impact on Reputation*		
#	**Criterion Weight →** **Information Asset ↓**	**0.3**	**0.4**	**0.3**	**TOTAL (1.0)**	**Importance (0-5; Not Applicable to Critically Important)**
1	Customer order via SSL (inbound)	*5*	*5*	*5*	5	Critically Important
2	EDI Document Set 1—Logistics bill of lading to outsourcer (outbound)	*5*	*5*	*3*	4.4	Very Important
3	EDI Document Set 2—Supplier orders (outbound)	*4*	*5*	*4*	4.4	Very Important
4	Customer service request via e-mail (inbound)	*3*	*3*	*5*	3.6	Very Important
5	EDI Document Set 3—Supplier fulfillment advice (inbound)	*3*	*3*	*2*	2.7	Important

2. Identifying Vulnerabilities

Threat is an event that are able to cause negative impact to an organization.

An Asset is anything of value to your company or organization.

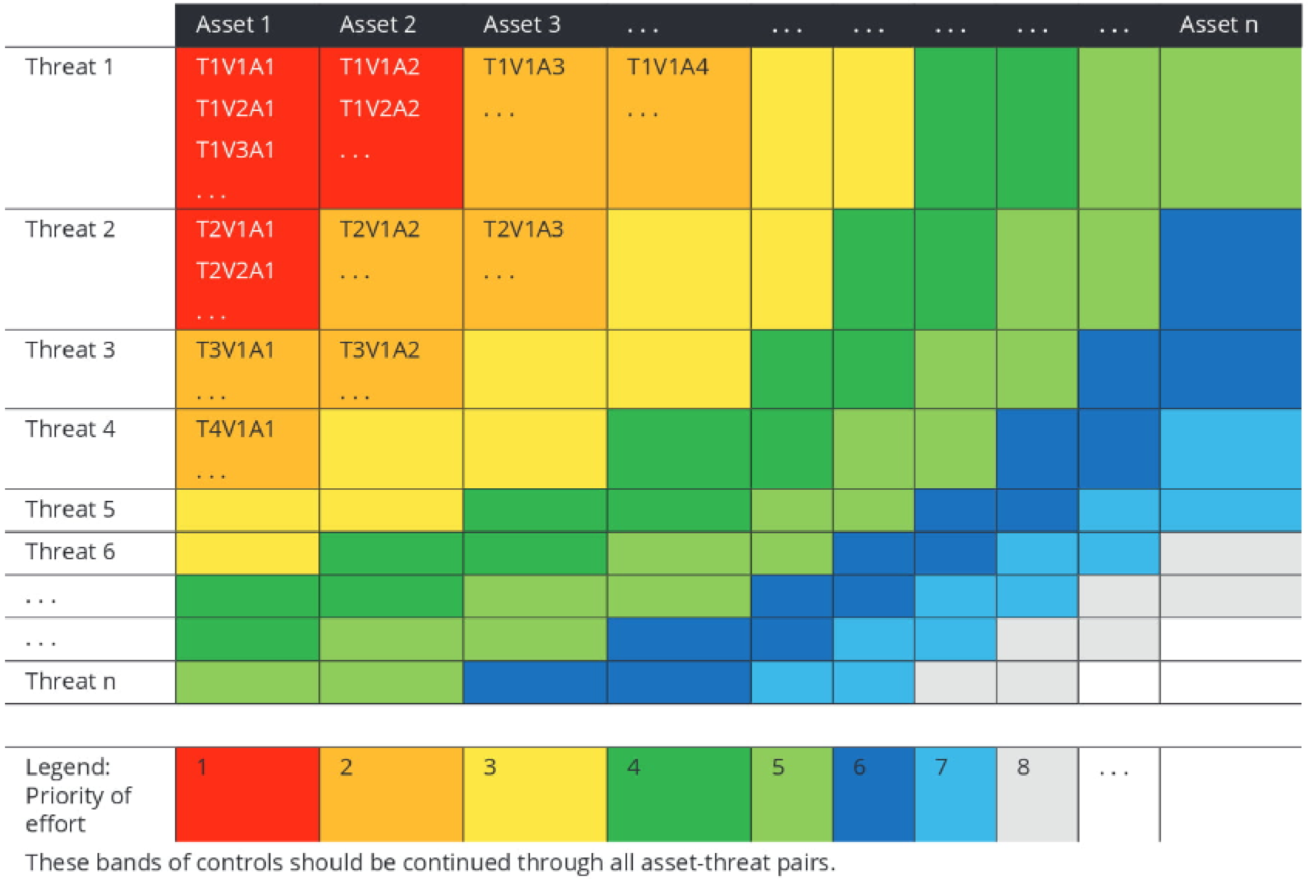


Attack/Exploit is a way to breach the security of an IT system through a vulnerability.

Vulnerability is a potential weakness in an asset or its defensive control system(s).

Threats-vulnerabilities-assets (TVA) Worksheet

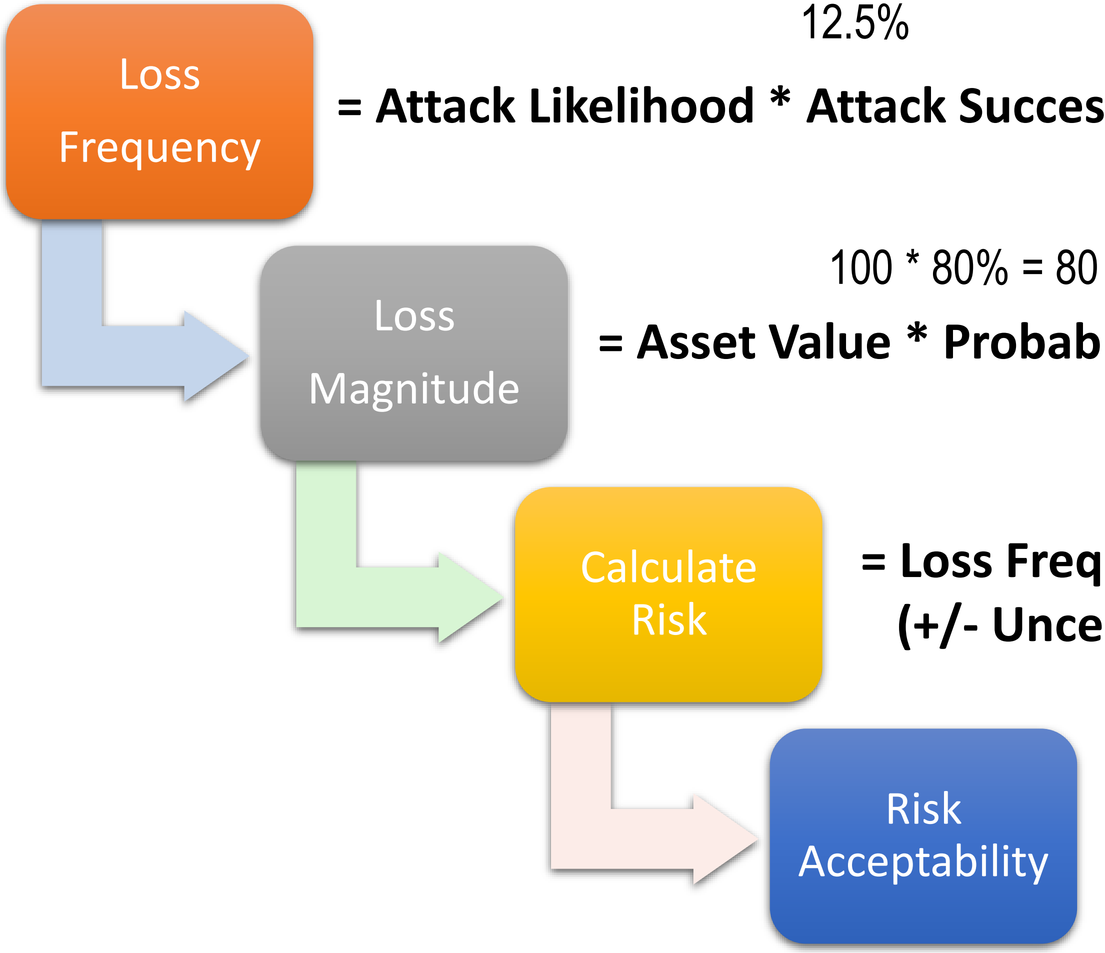
- A prioritized asset list
- A prioritized threat list:
  - Malware infection
  - Phishing message
  - Laptop/hardware theft/loss
  - Bots/zombies in organization
  - Insider abuse of Internet access or email
  - DDoS
  - Unauthorized access or privilege escalation by insider
  - …
  - …
  - …



	Asset 1	Asset 2	Asset 3	. . .	. . .	. . .	. . .	. . .	. . .	Asset n
Threat 1	T1V1A1 T1V2A1 T1V3A1 . . .	T1V1A2 T1V2A2 . . .	T1V1A3 . . .	T1V1A4 . . .						
Threat 2	T2V1A1 T2V2A1 . . .	T2V1A2 . . .	T2V1A3 . . .							
Threat 3	T3V1A1 . . .	T3V1A2 . . .								
Threat 4	T4V1A1 . . .									
Threat 5										
Threat 6										
. . .										
. . .										
Threat n										
Legend: Priority of effort	1	2	3	4	5	6	7	8	. . .	

These bands of controls should be continued through all asset-threat pairs.

3. Quantitative Risk assessment



Loss Frequency

12.5%

= Attack Likelihood * Attack Success Probability

Loss Magnitude

100 * 80% = 80

= Asset Value * Probable Loss

Calculate Risk

12.5% * 80 = 10

= Loss Frequency * Loss Magnitude (+/- Uncertainty of all estimates)

10 +/-10% = 9~11

Risk Acceptability

Calculated Risk vs. Risk Appetite

1 in 4 years = 25% chance of happening

×

50% chance of success if got attacked

=

12.5% chance of Loss from a DDoS attack

4. Select Control Strategies

Strategy	Description	Measures
Defense	Prevent exploitation of the vulnerability	Countering threats, removing vulnerabilities, limiting asset access, and adding protective safeguards
Transference	Shift risks to others	Hire individuals/firms with expertise to provide security management services
Mitigation	Reduce the impact of the attack instead of the success of the attack	CP (Contingency planning): IR (Incident response), DR (Disaster recovery), BC (Business continuity)
Acceptance	Do nothing to protect and accepting the outcome of its exploitation	Valid only when the particular function, service, information, or asset does not justify the cost of protection
Termination	Avoid business activities that introduce uncontrollable risks	May seek an alternate mechanism to meet the customer needs

Which is the most passive strategy?

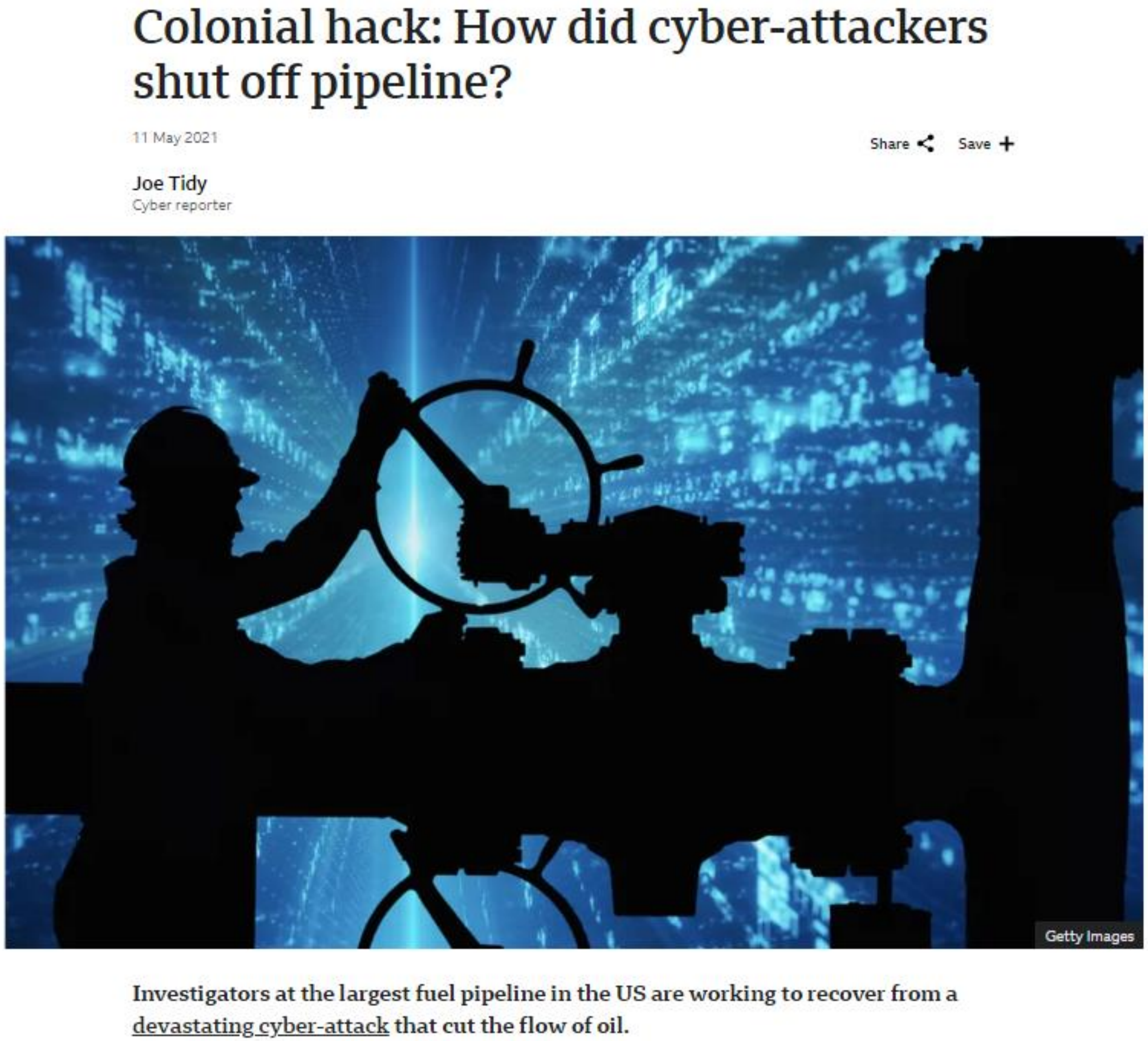
-- Acceptance

What factors would affect your choice?

As any other business decision, it depends on the size the company, technical capability, value of the application or asset, the risk appetite, available options, law and compliance, etc.

Contingency Planning (CP)

- In case of adverse events, there must be contingency plans in place.
- To prepare the organization to anticipate, react to, and recover from events that threaten the security of information.



Colonial hack: How did cyber-attackers shut off pipeline?

11 May 2021

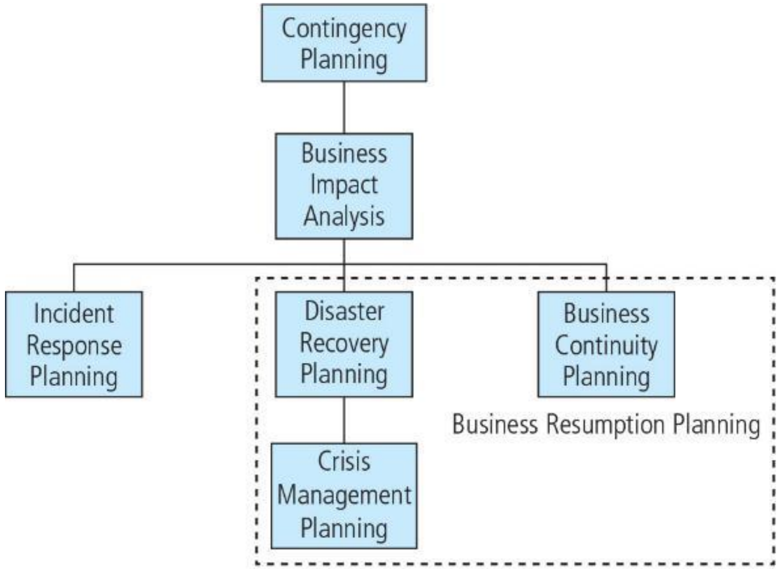
Joe Tidy
Cyber reporter

Investigators at the largest fuel pipeline in the US are working to recover from a devastating cyber-attack that cut the flow of oil.

- On May 7, 2021, a ransomware attack was launched on the largest refined oil products pipeline in the United States.
- A five-day shutdown of the pipeline, which disrupted the delivery of gasoline, diesel fuel, and jet fuel across the East Coast.
- Significant consequences, including reputational damage, legal ramifications, and recovery costs.
- Highlight the vulnerability of critical infrastructure to cyber attacks.

NIST CP Methodology

- Once formed, the **contingency planning management team (CPMT)** begins developing a CP document, for which NIST recommends using the following steps:
  1. Develop the CP policy statement.
  2. Conduct the BIA.
  3. Identify preventive controls.
  4. Create contingency strategies.
  5. Develop a contingency plan.
  6. Ensure plan testing, training, and exercises.
  7. Ensure plan updates and maintenance.



Contingency Planning
Business Impact Analysis
Incident Response Planning
Disaster Recovery Planning
Business Continuity Planning
Business Resumption Planning
Crisis Management Planning

Figure 5-1 Contingency planning hierarchies

1. Business Impact Analysis

- Business impact analysis (BIA) helps determine which business functions and information systems are the most critical to the success of the organization.
  - Maximum tolerable downtime (MTD)
    - The maximum time a business can tolerate the absence or unavailability of a particular business function
  - System recovery time (RTO) – Time to recover system
  - Work recovery time (WRT) – Time to recover data/work

2. Incident Detection

Level 1

Presence of unfamiliar files

Presence or execution of unknown programs or processes

Unusual consumption of computing resources

Unusual system crashes

Level 2

Activities at unexpected times

Presence of new accounts

Reported attacks

Notification from IDPS

Level 3

Use of dormant accounts

Changes to logs

Presence of hacker tools

Notifications by partner or peer

Notification by hacker

Level 4

Loss of availability

Loss of integrity

Loss of confidentiality

Violation of policy

Violation of law

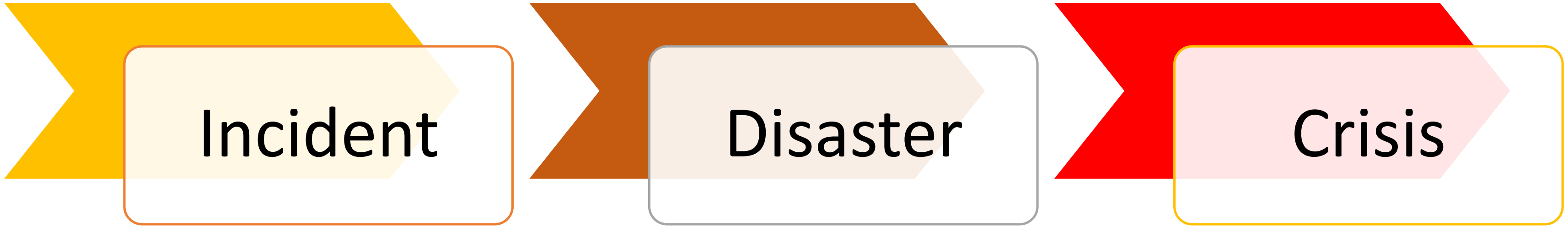
3. Incident Reaction

- Incident Reaction
  - Notification of key personnel (alert roster)
  - Document an incident
  - Incident containment strategies
    - “Cut the wire”
    - Disable compromised accounts
    - Reconfigure firewall rules to block certain traffic
    - Disable compromised services
    - Disable compromised server (e.g. email server)

- Incident Recovery
  - Damage assessment using computer forensics
  - Identify vulnerabilities and resolve them
  - Install, replace, or upgrade safeguards
  - Evaluate monitoring capabilities
  - Restore data, services, processes, and confidence!
  - After-action review

4. Disaster

- Unable to mitigate the impact of an incident while it is occurring; and the level of damage is so severe that the organization is unable to recover quickly.
- Recovery process similar to that of Business Continuity Planning (BCP)



5. Business Continuity Planning (BCP)

- Hot sites: duplicate facilities
- Warm sites: with computing equipment but not applications
- Cold sites: Just a room with A/C and electricity. Might as well rent on spot.
- Time-shares: Few organizations to share a site
- Service bureaus: a rental car clause in a car insurance policy
- Mutual agreements: organizations help each other out when needed

6. Ensure plan testing, training, and exercises

Digital Forensics

- Identifying relevant items of evidence
- Acquire the evidence without alteration or damage (special software and skills needed)
- Take steps to assure the authenticity and integrity of evidence at every step
- Report findings to the proper authority