Information Security from Risk Management and Design

Build a Secure Cyberspace 2019
“Phishing scams? No more!” Seminar
May 3rd 2019 @ Hong Kong

Albert Hui
GREM, GCFA, GCFE, GNFA, GCIA, GCIH, GXPN, GPEN, GAWN, GSNA, GSEC, CISA, CISM, CRISC

Who am I?

Albert Hui

GREM, GCFA, GCFE, GNFA, GCIA, GCIH, GXPN, GPEN, GAWN, GSNA, GSEC, CISA, CISM, CRISC

SECURITY RONIN

albert@securityronin.com

- Spoke at **Black Hat**,
  ACFE Asia Pacific Fraud Conference,
  HTCIA Asia Pacific Forensics Conference, and
  Economist Corporate Network.
- Risk & Security Consultant for
  Banks, Government and Critical Infrastructures.
- Digital Forensic Analyst & Fraud Investigator.
- Co-designed Hong Kong's first
  Digital Forensics course
  for the HK Police Force and ICAC by HKUST.

Security pitfalls #1: Inappropriate controls

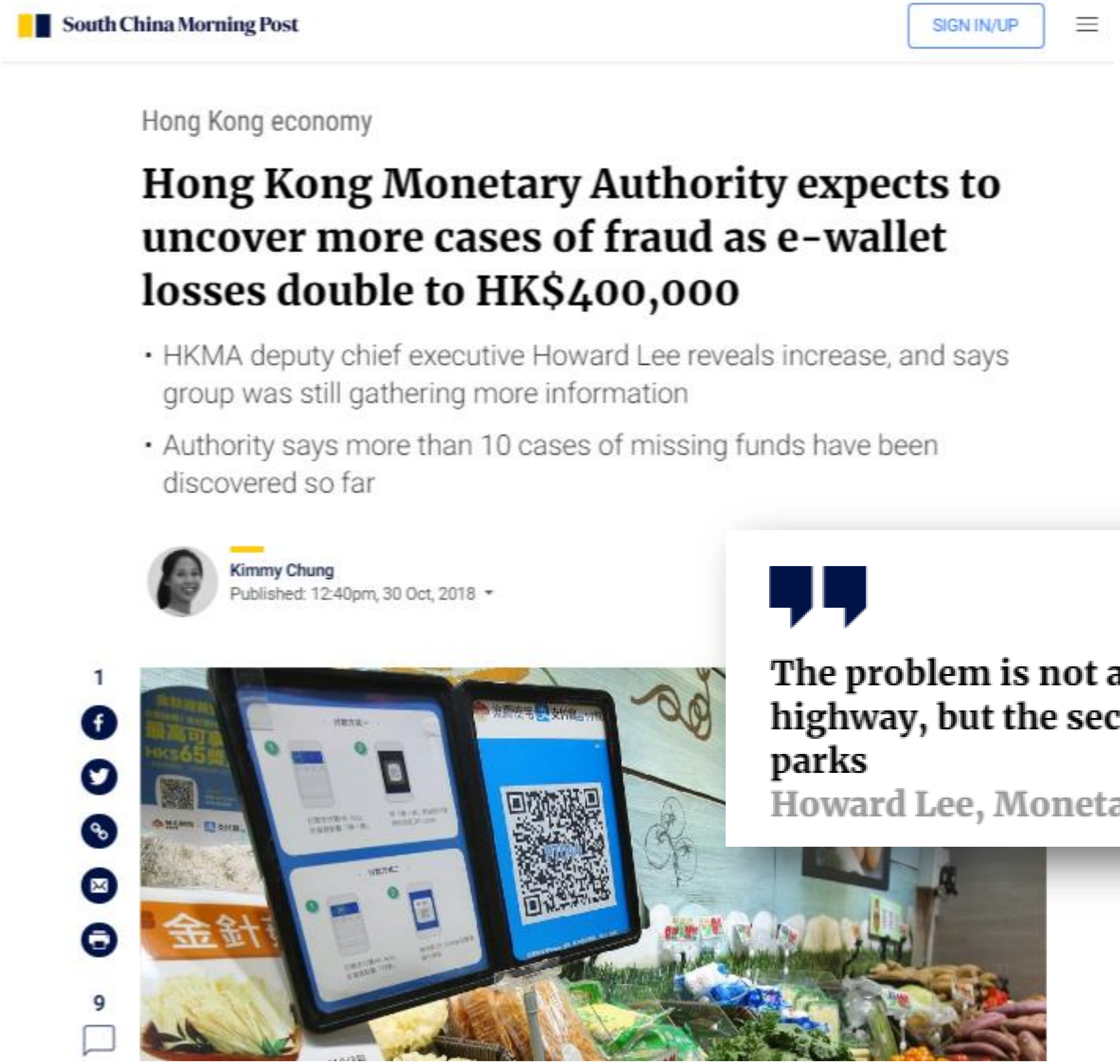
Source: https://www.redbubble.com/people/memecentral/works/21912648-question-mark-guy-meme-transparent?p=sticker

Security pitfalls #2: Inadequate threat modeling

Source: https://getyarn.io/yarn-clip/80499338-efe7-43e5-970e-5e7a79cbf3a2

Security pitfalls #2: Inadequate threat modeling

Case Study



Hong Kong economy

Hong Kong Monetary Authority expects to uncover more cases of fraud as e-wallet losses double to HK$400,000

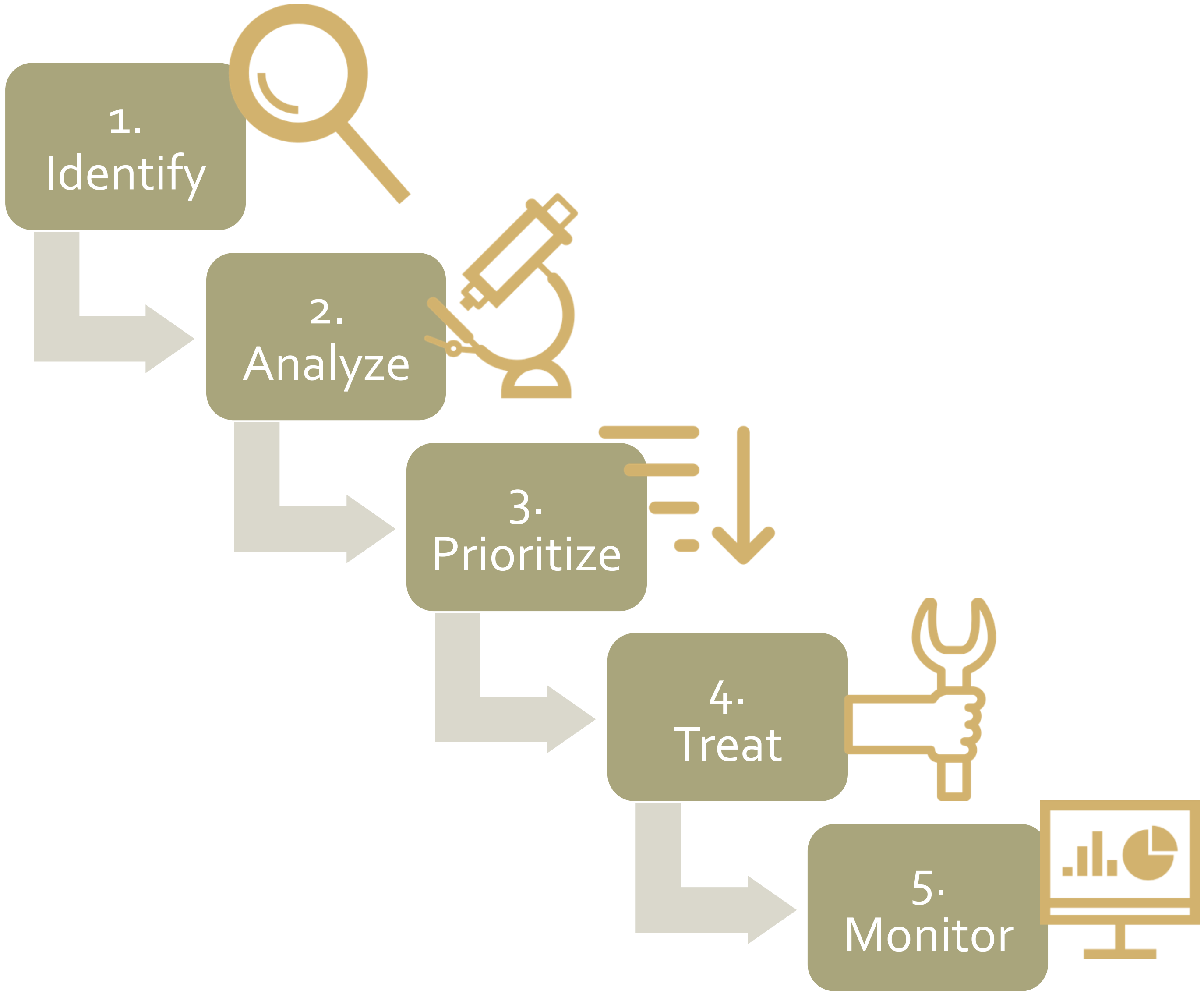
- HKMA deputy chief executive Howard Lee reveals increase, and says group was still gathering more information
- Authority says more than 10 cases of missing funds have been discovered so far

Kimmy Chung
Published: 12:40pm, 30 Oct, 2018

> **The problem is not about the highway, but the security of the car parks**
> **Howard Lee, Monetary Authority**

Source: https://www.scmp.com/news/hong-kong/hong-kong-economy/article/2170803/hong-kong-monetary-authority-expects-uncover-more

5 Steps of Risk Management



1. Identify

2. Analyze

3. Prioritize

4. Treat

5. Monitor

Asset Identification: What do you want to Protect?

Identify your important assets (mission-critical / business-critical / crown jewel):

Data

Examples:
- Customer information
- Supplier procurement records
- Design blueprints
- …

Process

Examples
- e-Commerce / Shopping Cart operations (for online shops)
- Power generation (for power plants)
- …

Possible Loss Identification: What can you Possibly Lose?

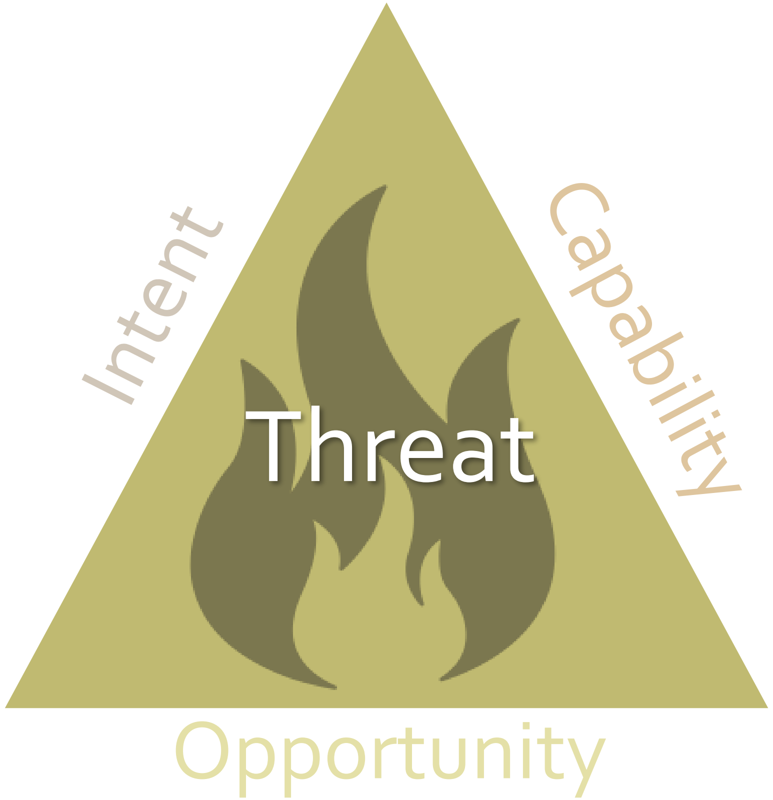
Primary losses:

- Money
- Customer data (e.g. credit card data)
- Proprietary information (design blueprints, strategic plans, etc.)
- Goodwill, brand damage and reputation loss
- …

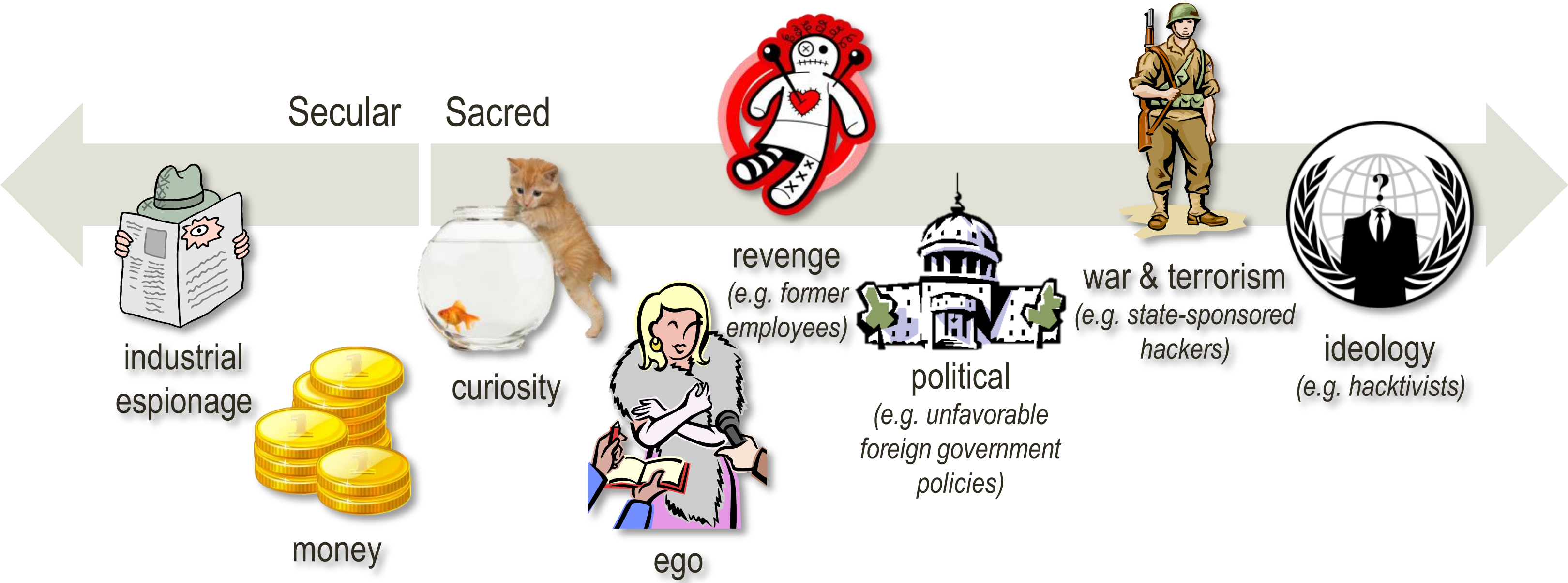
Secondary losses:

- Fines & penalties, loss of license, insurance premium
- Victim compensation (e.g. monetary compensation, credit monitoring)
- Cleanup cost (e.g. investigation and remediation)
- …

Threat Identification: What is Threat?



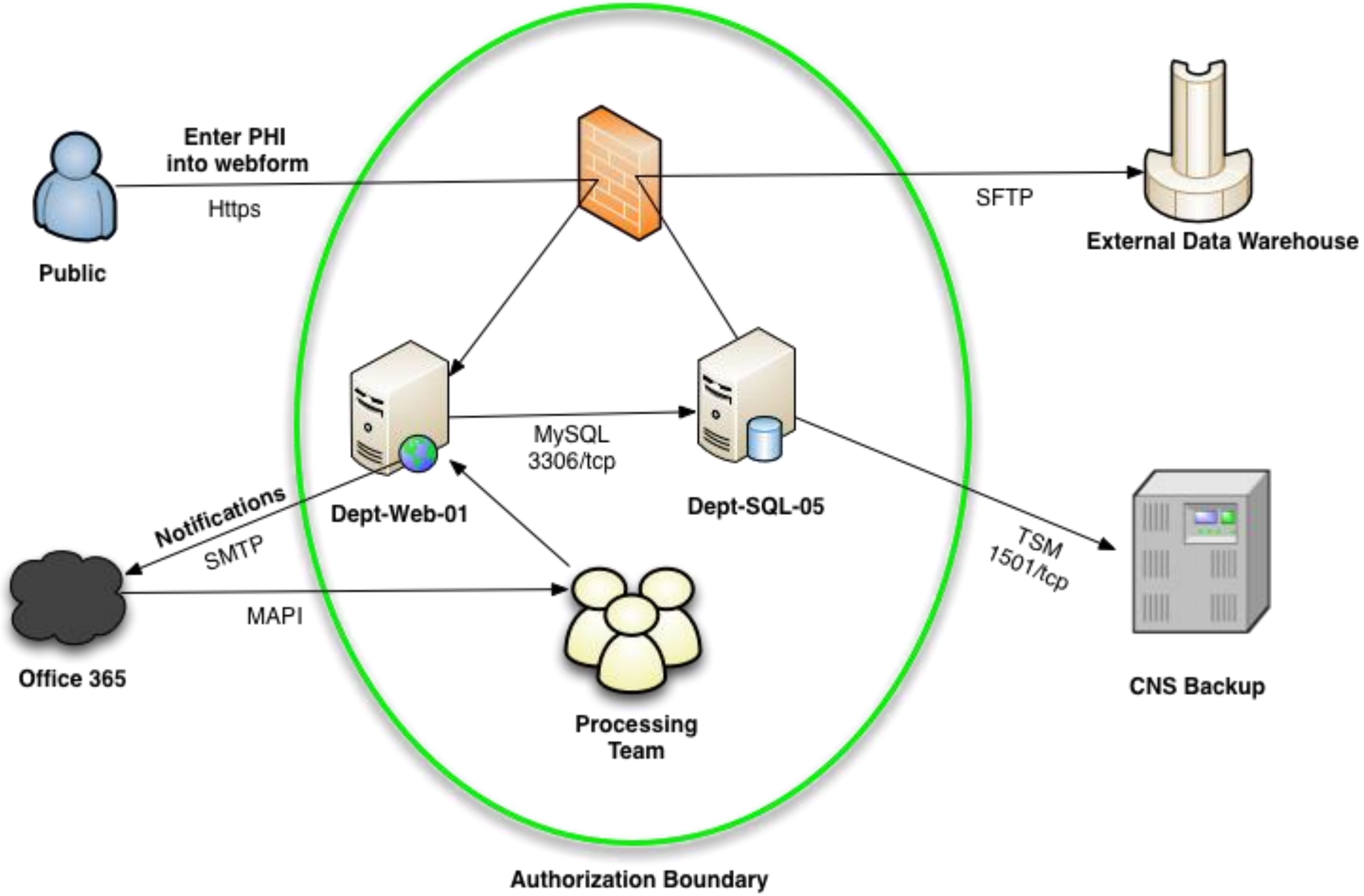
Threat Modeling: Threat Actors



Secular
Sacred
industrial espionage
money
curiosity
ego
revenge (e.g. former employees)
political (e.g. unfavorable foreign government policies)
war & terrorism (e.g. state-sponsored hackers)
ideology (e.g. hacktivists)

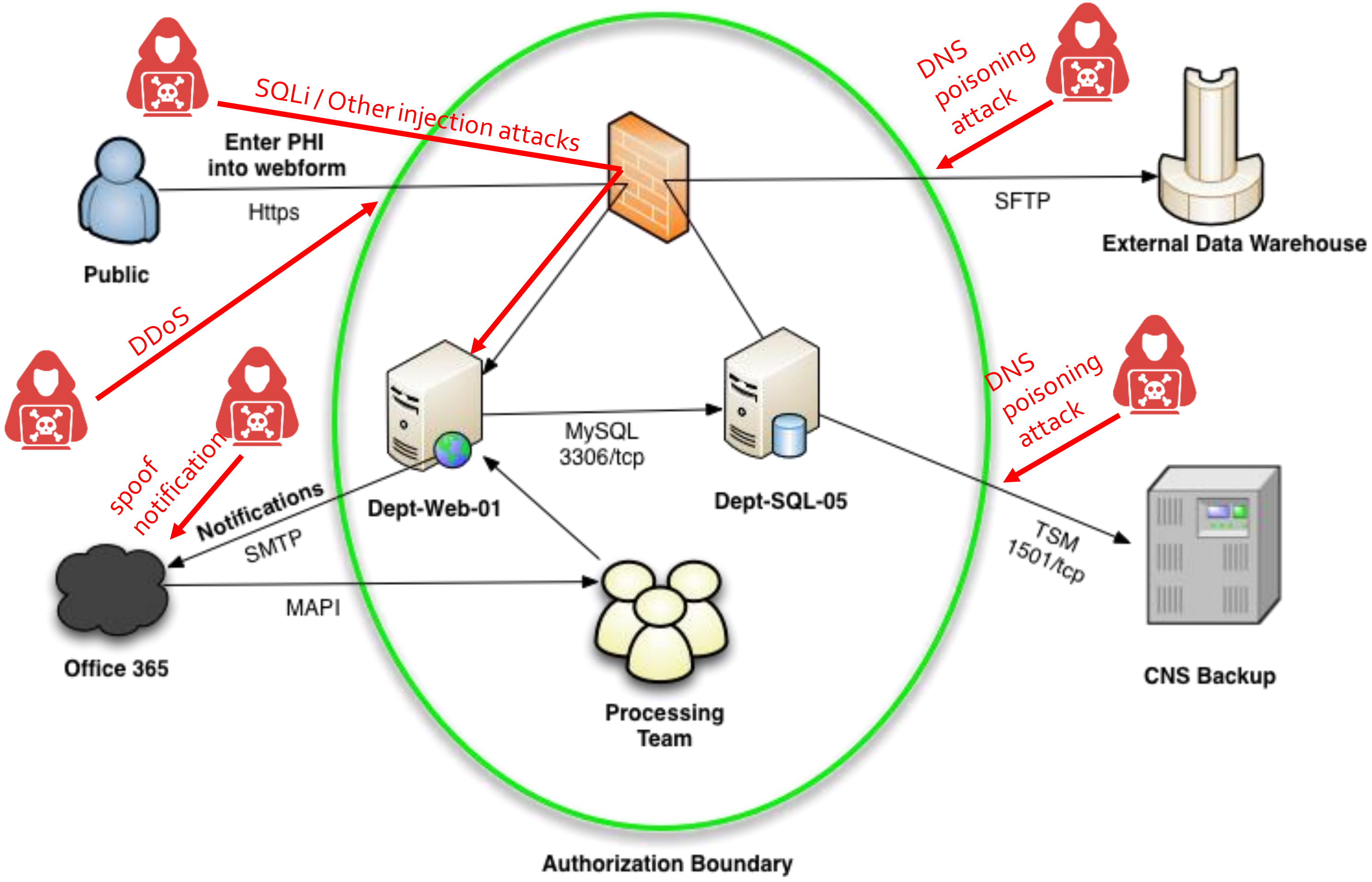
Threat Modeling: Dataflow Diagram (DFD)

Example of a good DFD



Source: https://security.ufl.edu/it-workers/risk-assessment/creating-an-information-systemdata-flow-diagram/

Threat Modeling: Plausible Attacks



Source: https://security.ufl.edu/it-workers/risk-assessment/creating-an-information-systemdata-flow-diagram/

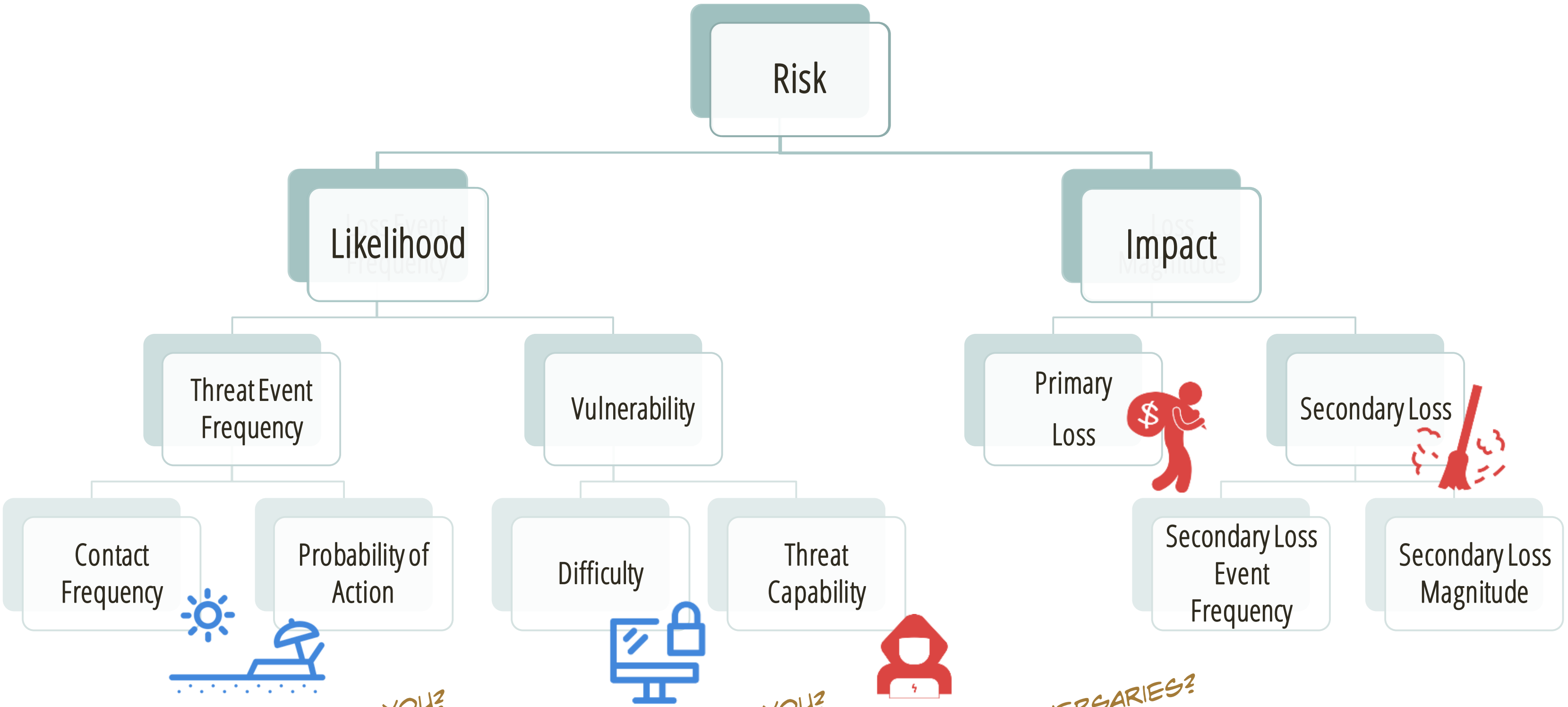
Threat Modeling: Threat Actions

STRIDE Model

- **S**poofing identity
- **T**ampering
- **R**epudiation
- **I**nformation disclosure
- **D**enial of service
- **E**levation of privilege

Risk Identification: What is Risk?

FAIR (Factor Analysis of Information Risk) Risk Ontology



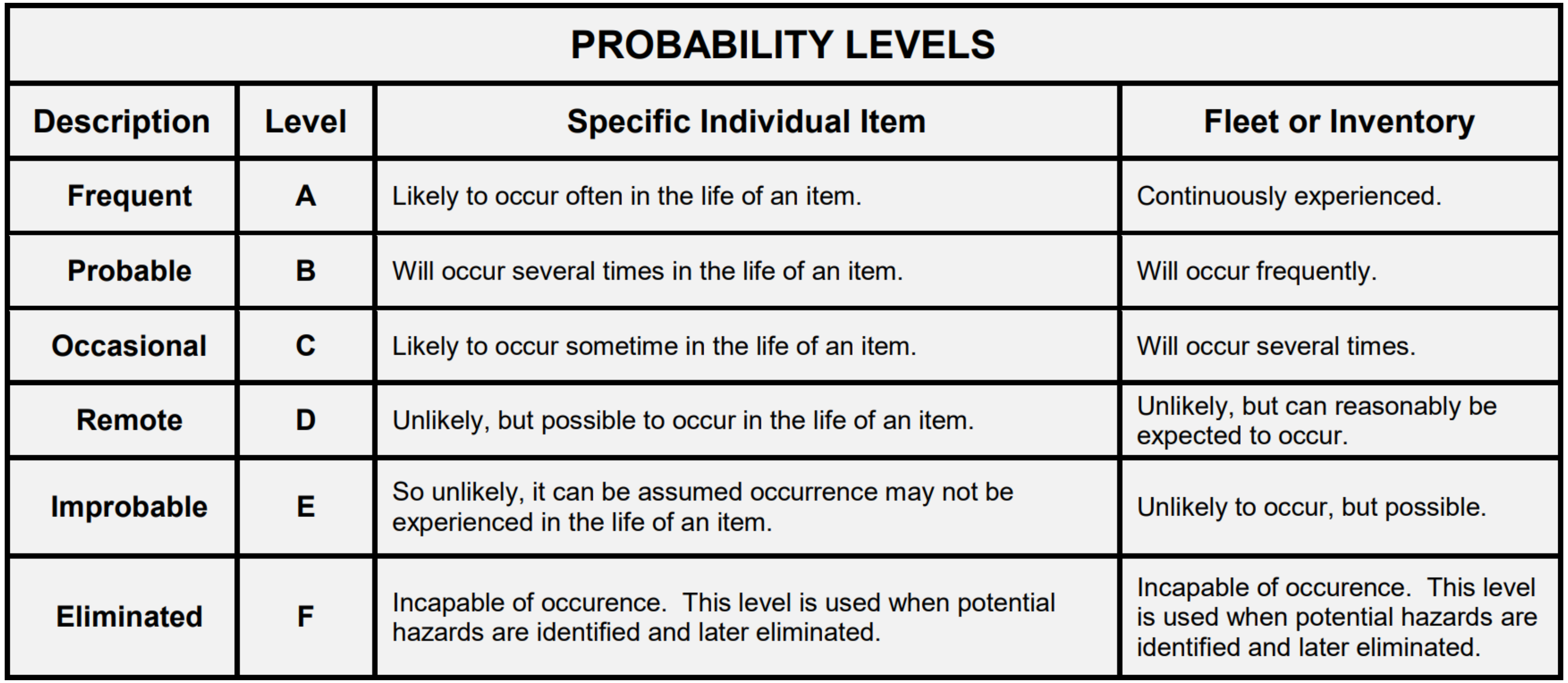
HOW EXPOSED ARE YOU?

HOW VULNERABLE ARE YOU?

HOW STRONG ARE YOUR ADVERSARIES?

Risk Analysis: Likelihood

MIL-STD-882E

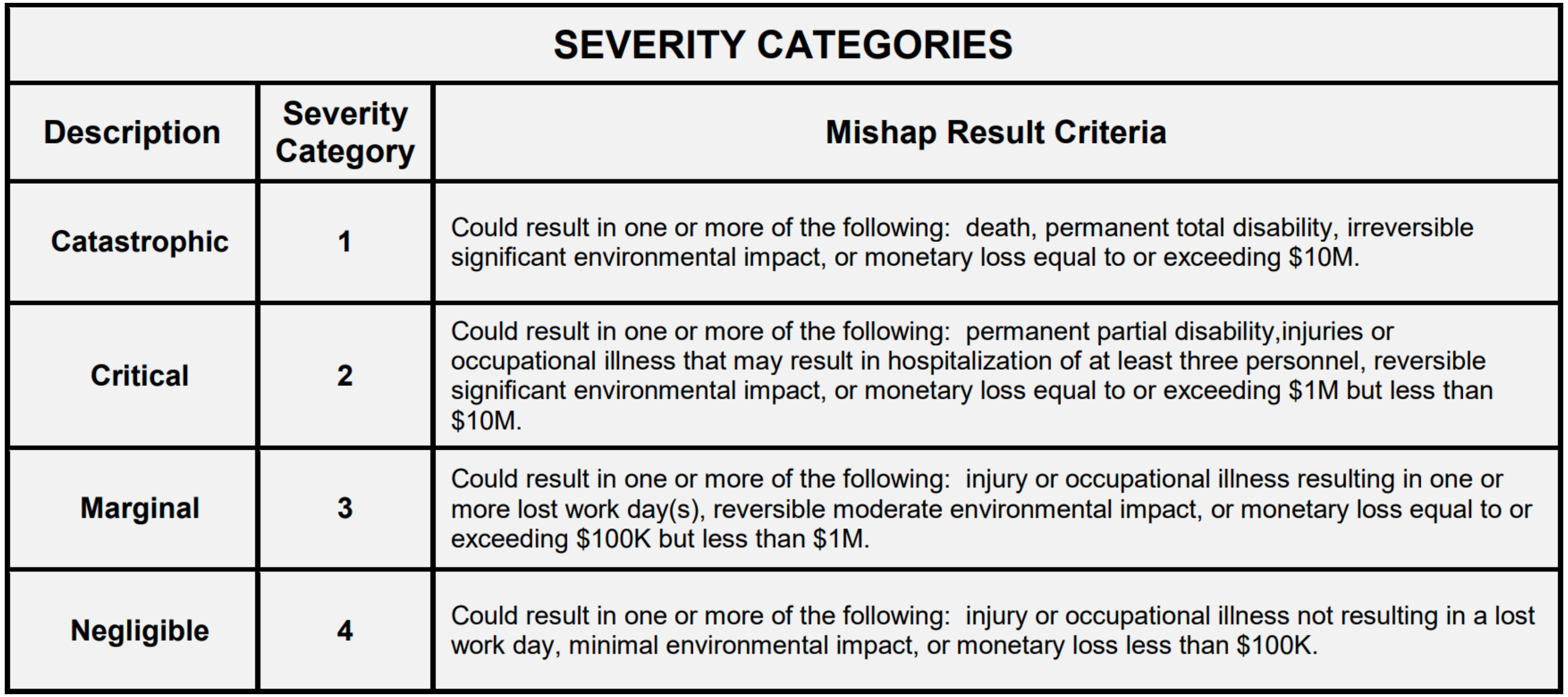


PROBABILITY LEVELS			
Description	**Level**	**Specific Individual Item**	**Fleet or Inventory**
Frequent	**A**	Likely to occur often in the life of an item.	Continuously experienced.
Probable	**B**	Will occur several times in the life of an item.	Will occur frequently.
Occasional	**C**	Likely to occur sometime in the life of an item.	Will occur several times.
Remote	**D**	Unlikely, but possible to occur in the life of an item.	Unlikely, but can reasonably be expected to occur.
Improbable	**E**	So unlikely, it can be assumed occurrence may not be experienced in the life of an item.	Unlikely to occur, but possible.
Eliminated	**F**	Incapable of occurence. This level is used when potential hazards are identified and later eliminated.	Incapable of occurence. This level is used when potential hazards are identified and later eliminated.

Source: https://www.system-safety.org/Documents/MIL-STD-882E.pdf

Risk Analysis: Impact

MIL-STD-882E



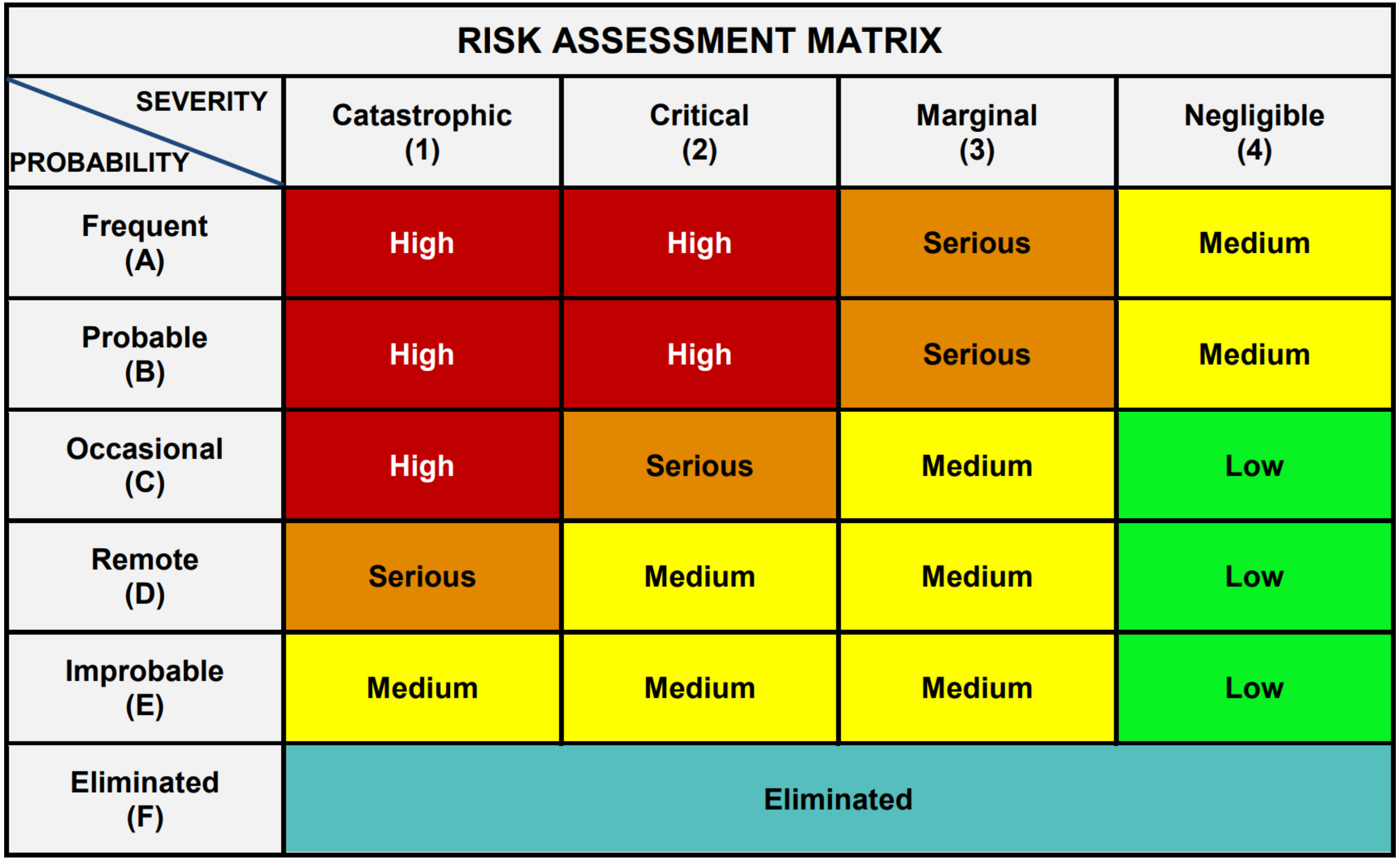
SEVERITY CATEGORIES

Description	Severity Category	Mishap Result Criteria
Catastrophic	1	Could result in one or more of the following: death, permanent total disability, irreversible significant environmental impact, or monetary loss equal to or exceeding $10M.
Critical	2	Could result in one or more of the following: permanent partial disability,injuries or occupational illness that may result in hospitalization of at least three personnel, reversible significant environmental impact, or monetary loss equal to or exceeding $1M but less than $10M.
Marginal	3	Could result in one or more of the following: injury or occupational illness resulting in one or more lost work day(s), reversible moderate environmental impact, or monetary loss equal to or exceeding $100K but less than $1M.
Negligible	4	Could result in one or more of the following: injury or occupational illness not resulting in a lost work day, minimal environmental impact, or monetary loss less than $100K.

Source: https://www.system-safety.org/Documents/MIL-STD-882E.pdf

Risk Analysis: Risk Matrix

MIL-STD-882E

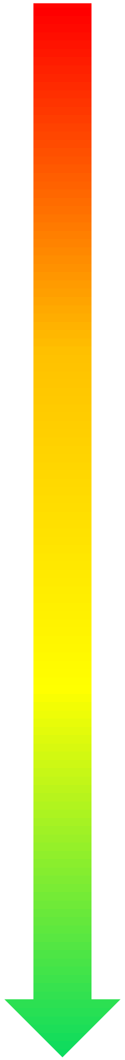


RISK ASSESSMENT MATRIX

SEVERITY PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

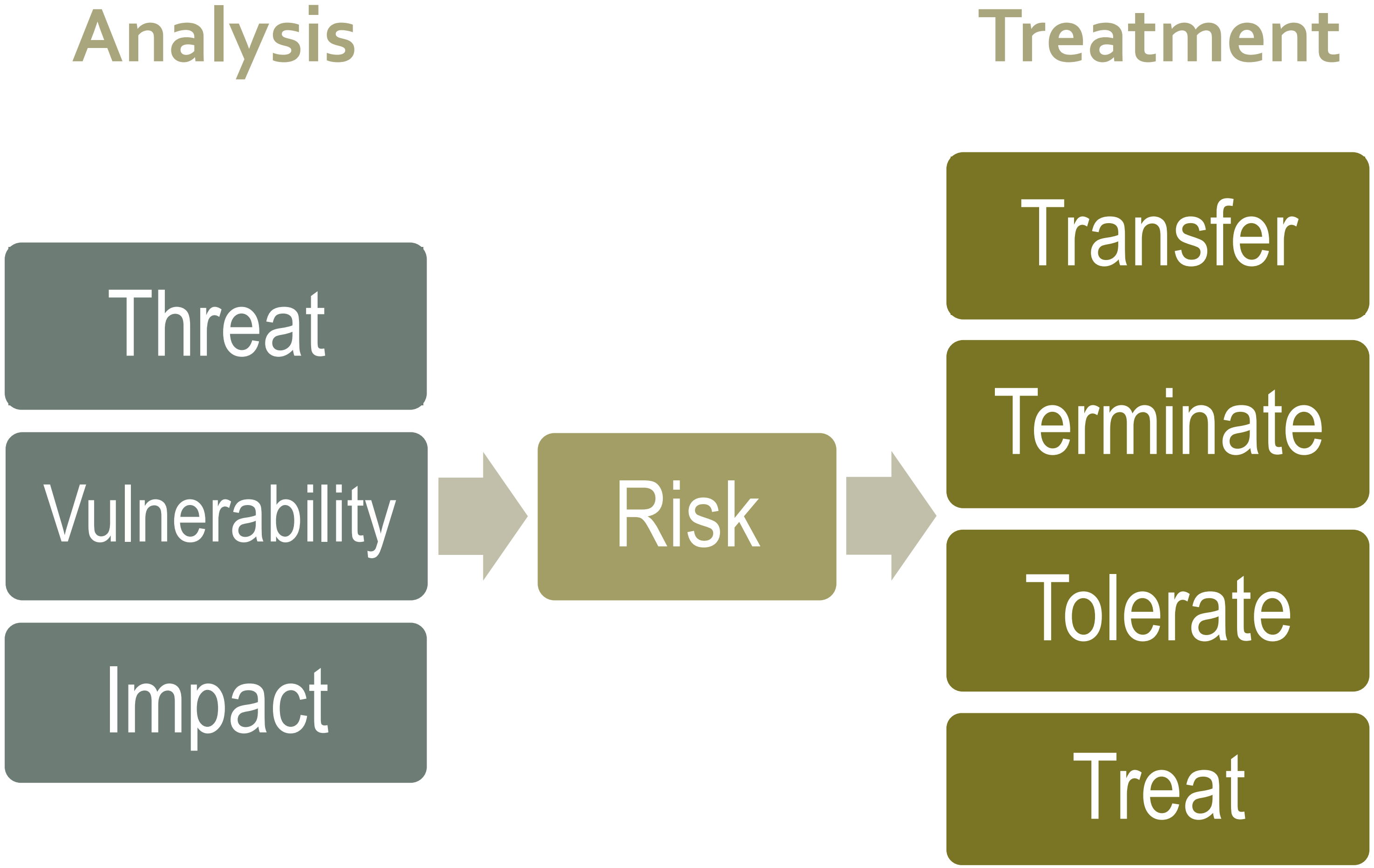
Source: https://www.system-safety.org/Documents/MIL-STD-882E.pdf

Risk Prioritization



Risk Level	
High	•......
High	•......
Serious	•......
Serious	•......
Serious	•......
Medium	•......
Medium	•......
Low	•......
Low	•......
Low	•......
Low	•......
Low	•......
Low	•......
Low	•......
Low	•......
Low	•......
Low	•......

Risk Treatment: Overview



Analysis

Threat

Vulnerability

Impact

Risk

Treatment

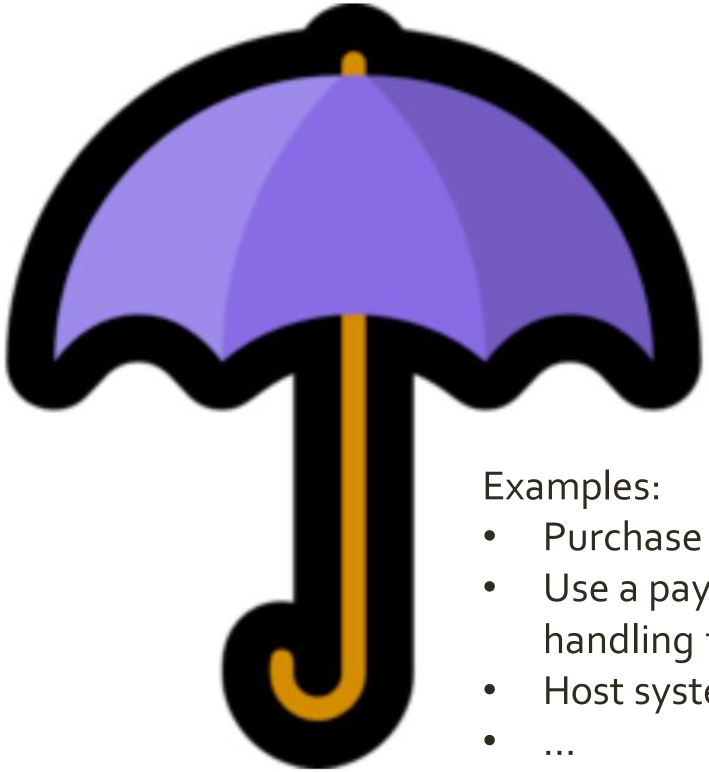
Transfer

Terminate

Tolerate

Treat

Risk Treatment: Option 1: Transfer



Examples:

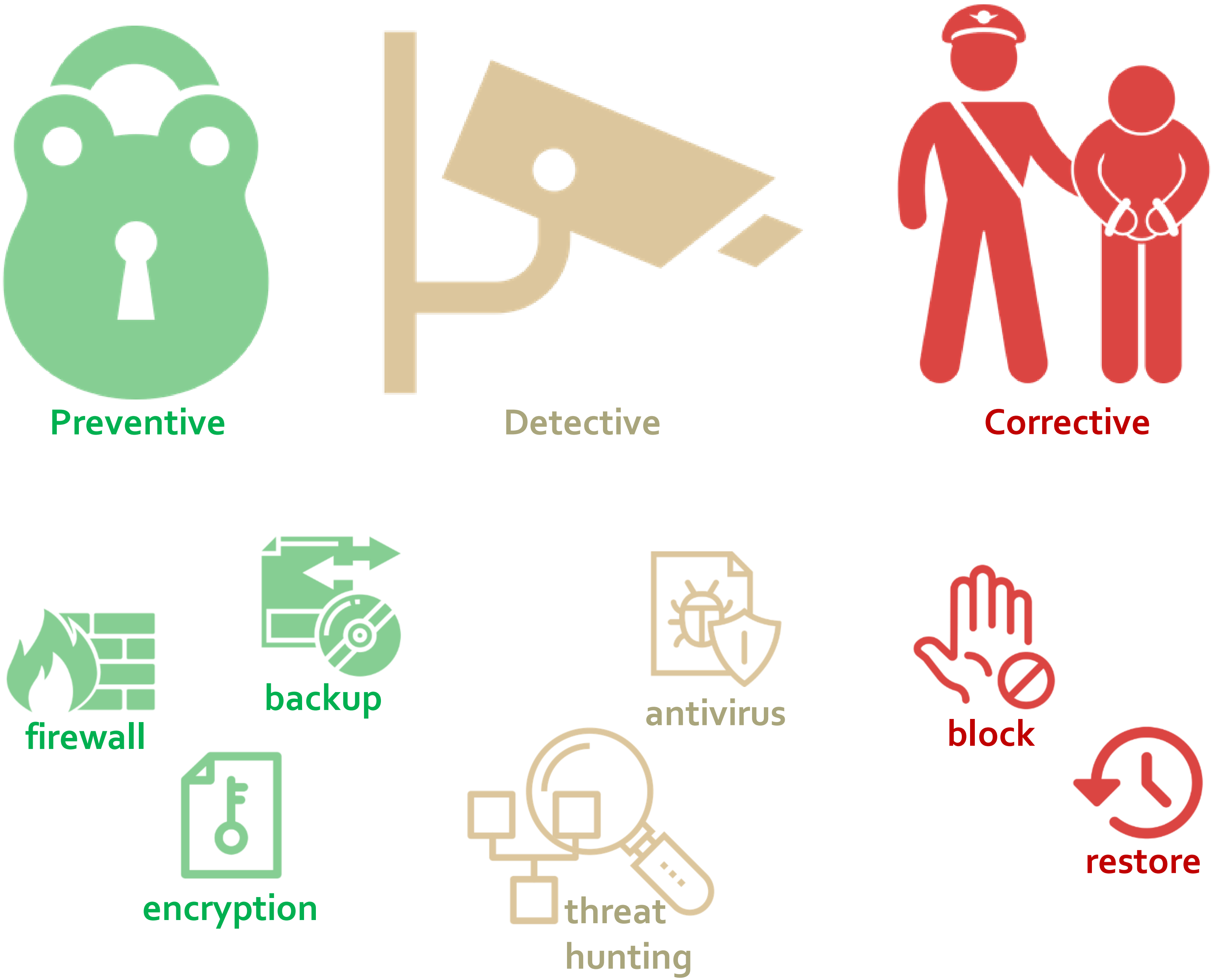
- Purchase an insurance policy
- Use a payment processor instead of handling transactions on your own
- Host system on a cloud platform
- …

Risk Treatment: Option 2: Terminate

Risk Treatment: Option 3: Tolerate

Risk Treatment: Option 4: Treat (Mitigate)

Risk Treatment: Mitigation controls



Preventive

Detective

Corrective

firewall

backup

encryption

antivirus

threat hunting

block

restore

Examples

Example 1:

Asset at Stake:	Shopping cart operations
Plausible Compromise:	Hacker gain access to DB and destroy data
One Possible Mitigation Control:	Deploy WAF

Example 2:

Asset at Stake:	Shopping cart operations
Plausible Compromise:	System / DB goes down and corrupt data
One Possible Mitigation Control:	Daily backup

Example 3:

Asset at Stake:	Shopping cart history
Plausible Compromise:	Backup lost (due to hacking or accident)
One Possible Mitigation Control:	Backup to write-only media

Risk Monitoring

Key Takeaways

1. Know your assets
2. Know your threats
3. Rank your risks
4. Design corresponding controls

Thank you

albert@securityronin.com