⚠️ Managing Risk

Author(s): Hayden Smith

(Download as PDF)

🧐 Risk

What in the world is risk?

What do you think of when you think of risk?

🧐 Risk

There are many definitions, but the Association for Project Management defines risk management as *"a process that allows individual risk events and overall risk to be understood and managed proactively, optimising success by minimising threats and maximising opportunities and outcomes."*

🧐 Risk

Risk management isn't about trying to avoid risk, it's actually about trying to **engage with more risk** but in an accountable and sustained way.

Without proper risk management, theoretically businesses would take less risks as they might seem too scary.

🧐 Risk

Good examples of times we might consider risk management are:

- What speed do you set on the highway or roads?
- How much money do you invest into the quality of a piece of engineering (e.g. a plane engine)

What are other times we might want to consider risk?

🧐 Risk

Risks don't have to be technical!

Risks can be technical (e.g. vulnerabilities, data loss, cyber attacks).

Risks can be human (people leaving a business, people posting dumb things on social media).

Risks can be business-oriented (running out of money, key employees incapacitated)

Risk can be anything!

🧠 Understanding Risk

How serious is the risk of something?

Risk is fundamentally about finding appropriate **controls** to manage the risk based on the risk's seriousness. A risk's seriousness typically come from two primary dimensions:

- **probability** of the risk occurring
- **impact** of the risk occurring

⚖️ Impact V Probability

Risk severity can be understood more visually:

		Impact				
		Trivial	Minor	Moderate	Major	Extreme
Probability	Rare	Low	Low	Low	Medium	Medium
	Unlikely	Low	Low	Medium	Medium	Medium
	Moderate	Low	Medium	Medium	Medium	High
	Likely	Medium	Medium	Medium	High	High
	Very likely	Medium	Medium	High	High	High

⚖️ Impact V Probability

What is an example of:

1. Low probability, low impact risk?
2. Low probability, high impact risk?
3. High probability, low impact risk?
4. High probability, high impact risk?

⚖️ Impact V Probability

One reason this approach is useful is stakeholder management too, for example only high severity issues get discussed/approved by exec/board.

🎛️ Controls

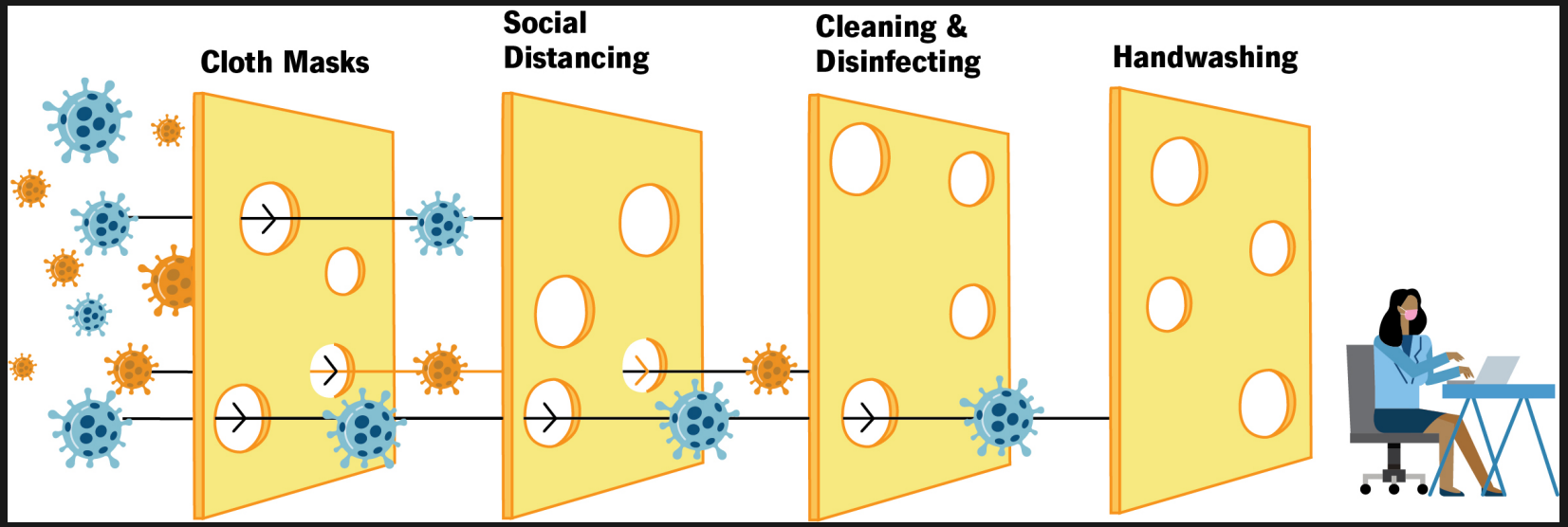
Once we understand the severity of a risk, the next step is look at how to **control** the situation in order to help us get comfortable that the risk can be managed.

In general we can try and put in controls to either:

🛑 Prevent; or

🤕 Mitigate

🧀 Swiss Cheese Model



Likens controlling risk well to multiple slices of Swiss cheese, which has randomly placed and sized holes in each slice, stacked side by side, in which the risk of a threat becoming a reality is mitigated by the differing layers and types of defenses which are "layered" behind each other.

✈️ Example: Jetstar

Passengers on a Jetstar flight wandering off as they walk on the tarmac to board the back of the plane.

✈️ Example: Jetstar

Passengers on a Jetstar flight wandering off as they walk on the tarmac to board the back of the plane.

What is the probability and impact?

✈️ Example: Jetstar

Passengers on a Jetstar flight wandering off as they walk on the tarmac to board the back of the plane.

What is the probability and impact?

- 🛑 Prevent: Only board front of plane

✈️ Example: Jetstar

Passengers on a Jetstar flight wandering off as they walk on the tarmac to board the back of the plane.

What is the probability and impact?

- 🛑 Prevent: Only board front of plane
- 🤕 Mitigate: Extra cameras / extra security staff

Example: Employee SaaS Access

Employee has access to 30 different services (e.g. Google, Slack) as part of their employment.

Example: Employee SaaS Access

Employee has access to 30 different services (e.g. Google, Slack) as part of their employment.

What is the probability and impact?

🖥️ Example: Employee SaaS Access

Employee has access to 30 different services (e.g. Google, Slack) as part of their employment.

What is the probability and impact?

- 🛑 Prevent: Revoke or restrict access (least privilege)

🖥️ Example: Employee SaaS Access

Employee has access to 30 different services (e.g. Google, Slack) as part of their employment.

What is the probability and impact?

- 🛑 Prevent: Revoke or restrict access (least privilege)

Drawbacks of this?

🖥️ Example: Employee SaaS Access

Employee has access to 30 different services (e.g. Google, Slack) as part of their employment.

What is the probability and impact?

- 🛑 Prevent: Revoke or restrict access (least privilege)

Drawbacks of this?

- 🤕 Mitigate: Password Manager, SSO

🖥️ Example: Employee SaaS Access

Employee has access to 30 different services (e.g. Google, Slack) as part of their employment.

What is the probability and impact?

- 🛑 Prevent: Revoke or restrict access (least privilege)

Drawbacks of this?

- 🤕 Mitigate: Password Manager, SSO

Does Password Manager + SSO just create more risks?

🖥️ Example: Employee SaaS Access

Employee has access to 30 different services (e.g. Google, Slack) as part of their employment.

What is the probability and impact?

- 🛑 Prevent: Revoke or restrict access (least privilege)

Drawbacks of this?

- 🤕 Mitigate: Password Manager, SSO

Does Password Manager + SSO just create more risks?

Benefits of zero knowledge password manager?

Example: Customer Data Access

Employee requires access to customer data in order to do their job (e.g. to debug an account).

Example: Customer Data Access

Employee requires access to customer data in order to do their job (e.g. to debug an account).

What is the probability and impact?

🖥️ Example: Customer Data Access

Employee requires access to customer data in order to do their job (e.g. to debug an account).

What is the probability and impact?

- 🛑 Prevent? How
- 🤕 Mitigate? How

Example: Customer Data Access

Employee requires access to customer data in order to do their job (e.g. to debug an account).

Example: Customer Data Access

Employee requires access to customer data in order to do their job (e.g. to debug an account).

What is the probability and impact?

🖥️ Example: Customer Data Access

Employee requires access to customer data in order to do their job (e.g. to debug an account).

What is the probability and impact?

- 🛑 Prevent? How
- 🤕 Mitigate? How

🏦 Example: Direct Debits

Direct Debit is the process whereby you can "pull" money from one account into a merchant account. It runs on the BECS rails.

- Merchant account: A business like account
- BECS: Bulk Electronic Clearing System - an old Australian payment system used between banks

 Example: Direct Debits

1. You collect a direct debit authorisation form from a client
2. You provide a bank with a BSB / Account Number
3. You request an amount to be "pulled" into your merchant account
4. The funds appear on T+1
5. On T+2, if the funds were legitimate, they stay in your account. If they weren't, they are removed.
6. At any point in the next 7 years, a customer can "dispute" that transaction, and the onus is on the merchant to prove that it was legitimate.

So What Can Go Wrong?

So What Can Go Wrong?

Customer attempting to falsely pretend they didn't authorise the transaction.

🏦 So What Can Go Wrong?

Customer attempting to falsely pretend they didn't authorise the transaction.

Fraudster using someone else's bank account details.

So What Can Go Wrong?

How can we manage those risks?

💂 Example: Atlassian Envoy

Last week (around 16th Feb 2023) Atlassian had a lot of employee data (names, profile pictures, seating locations) sitting in a third party service called **Envoy**.

- Hacker found valid credentials, not a technical vulnerability
- Company device compromised? Personal information posted?

Managing secrets is tricky:

- Hide too much, people can't do their work
- Show too much, things like this happen

See this link for more info.

Documentation

Sometimes we document our risks through a risk assessment, or a risk matrix.

SOC2 and ISO27001 are common Infosec specific certifications that help demonstrate an industrial degree of risk management.

🤷 Identifying Is A Good Start

Don't be scared of needing to find controls in order for you to feel validated in highlighting a risk. For example, the following are hard to control for a business:

- Economic collapse
- Regulatory changes
- New competitor launched

Thank You!!

🦻 Feedback

Or go to the form here.