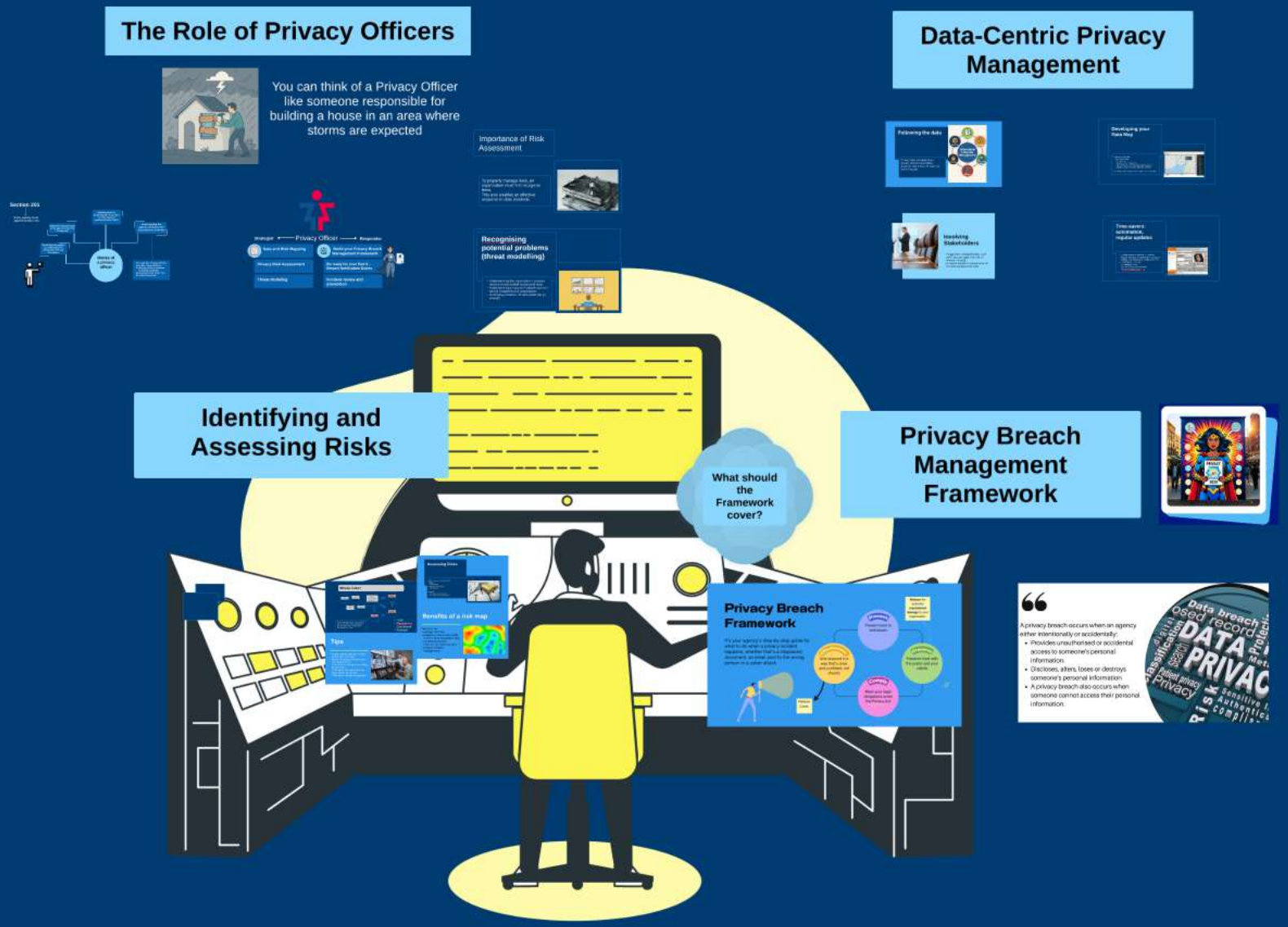
Privacy Officers Role: Getting Ahead of Risks Before They Become Breaches

A Practical Approach to Strengthening Privacy Assurances and Privacy Breach Management Frameworks

Dr. Marcin Betkier
Laura Rodriguez



The Role of Privacy Officers

You can think of a Privacy Officer like someone responsible for building a house in an area where storms are expected

Importance of Risk Assessment

To properly manage risks, an organisation must first recognise them.
This also enables an effective response to data incidents.

Recognising potential problems (threat modelling)

- Understanding the organisation's systems and processes (fueled by personal data)
- Understanding privacy and related legal and ethical obligations and expectations
- Identifying problems / threats (what can go wrong?)

Section 201

Every agency must appoint at least one

Duties of a privacy officer

- Working with the Commissioner in relation to investigations conducted under Part 5
- Deal with requests made to the agency under the Privacy Act
- Ensuring that the agency complies with the provision of the Act
- Encourage the agency to comply with the Information Privacy Principles

For example, Privacy Officers are often responsible for managing privacy breaches — including notifiable privacy breaches under Part 6 of the Privacy Act.

Privacy Officer

Strategist ⟵ ⟶ Responder

- Data and Risk Mapping
- Privacy Risk Assessment
- Threat Modeling
- Build your Privacy Breach Management Framework
- Be ready for your Part 6 – Breach Notification Duties
- Incident review and prevention

Importance of Risk Assessment

To properly manage risks, an organisation must first recognise them.
This also enables an effective response to data incidents.

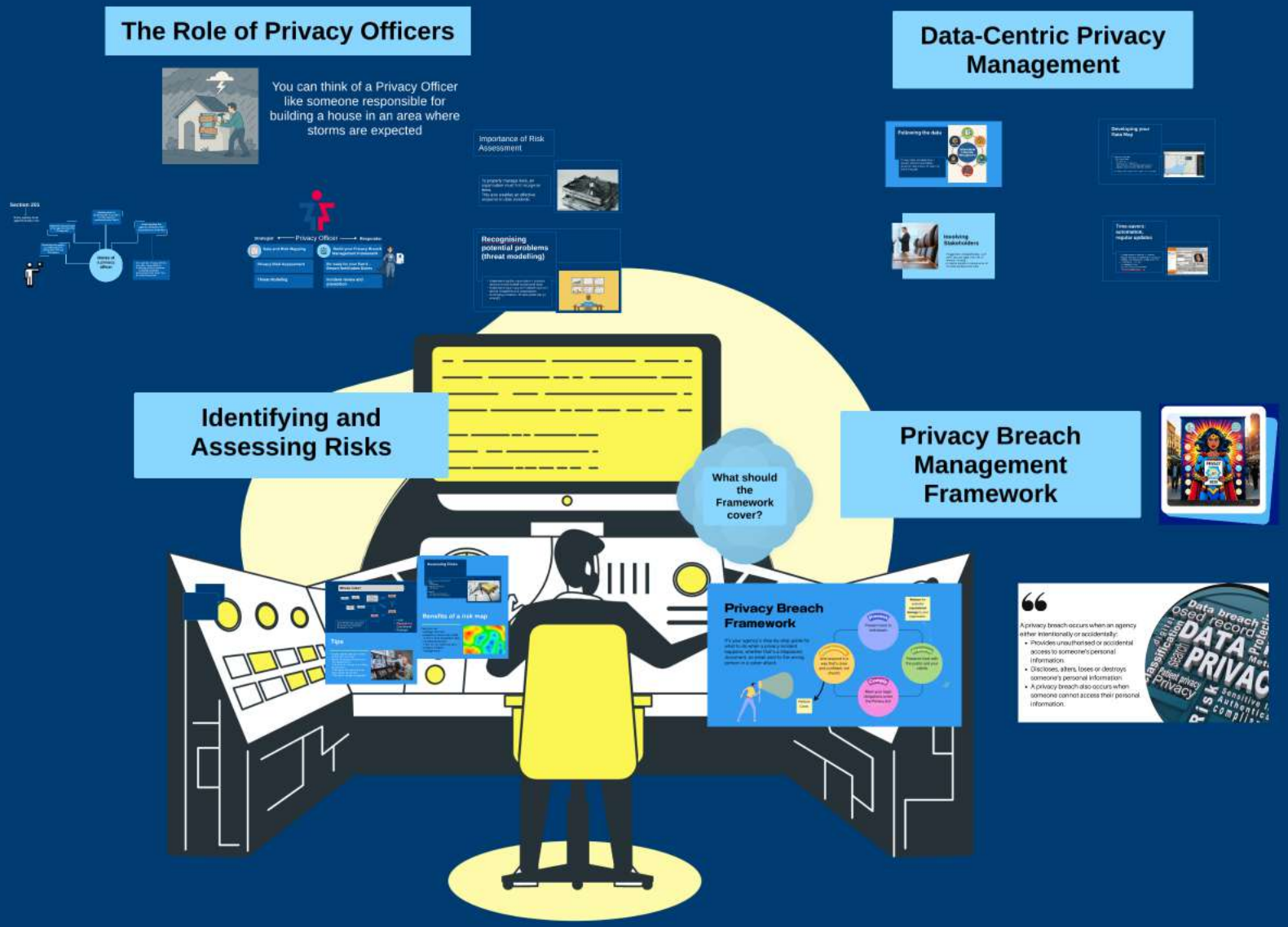
Recognising potential problems (threat modelling)

- Understanding the organisation's systems and processes (fueled by personal data)
- Understanding privacy and related legal and ethical obligations and expectations
- Identifying problems / threats (what can go wrong?)

Privacy Officers Role: Getting Ahead of Risks Before They Become Breaches

A Practical Approach to Strengthening Privacy Assurances and Privacy Breach Management Frameworks

Dr. Marcin Betkier
Laura Rodriguez



Data-Centric Privacy Management

Following the data

Privacy risks are data risks—privacy officers must follow personal data closely through its entire lifecycle.

Developing your Data Map

It needs to describe:
- all personal data
- full data cycle
- processing by third-parties
- relevant factors, like: locations, source of data, purposes, data sensitivity, "business owners"

Creating a data map does not need to be complicated!

Involving Stakeholders

- Engagement of stakeholders, such as IT, security, legal, risk, HR, or finance is crucial.
- it may be possible to reuse some of the existing data inventories

Time-savers: automation, regular updates

- Utilising software tools for information management can streamline the process of creating and maintaining a data inventory
- Updating the inventory:
  - ongoing projects
  - privacy risks assessments
  - 'environmental scanning'

Following the data

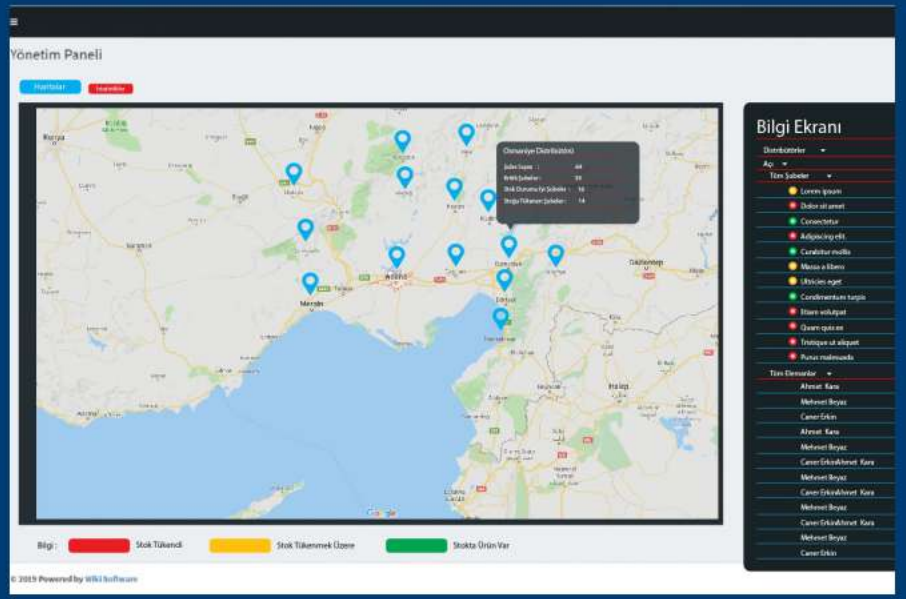
Privacy risks are data risks—privacy officers must follow personal data closely through its entire lifecycle.

Developing your Data Map

It needs to describe:

- all personal data
- full data cycle
- processing by third-parties,
- relevant factors, like: locations, source of data, purposes, data sensitivity, "business owners"

Creating a data map does not need to be complicated!



Involving Stakeholders

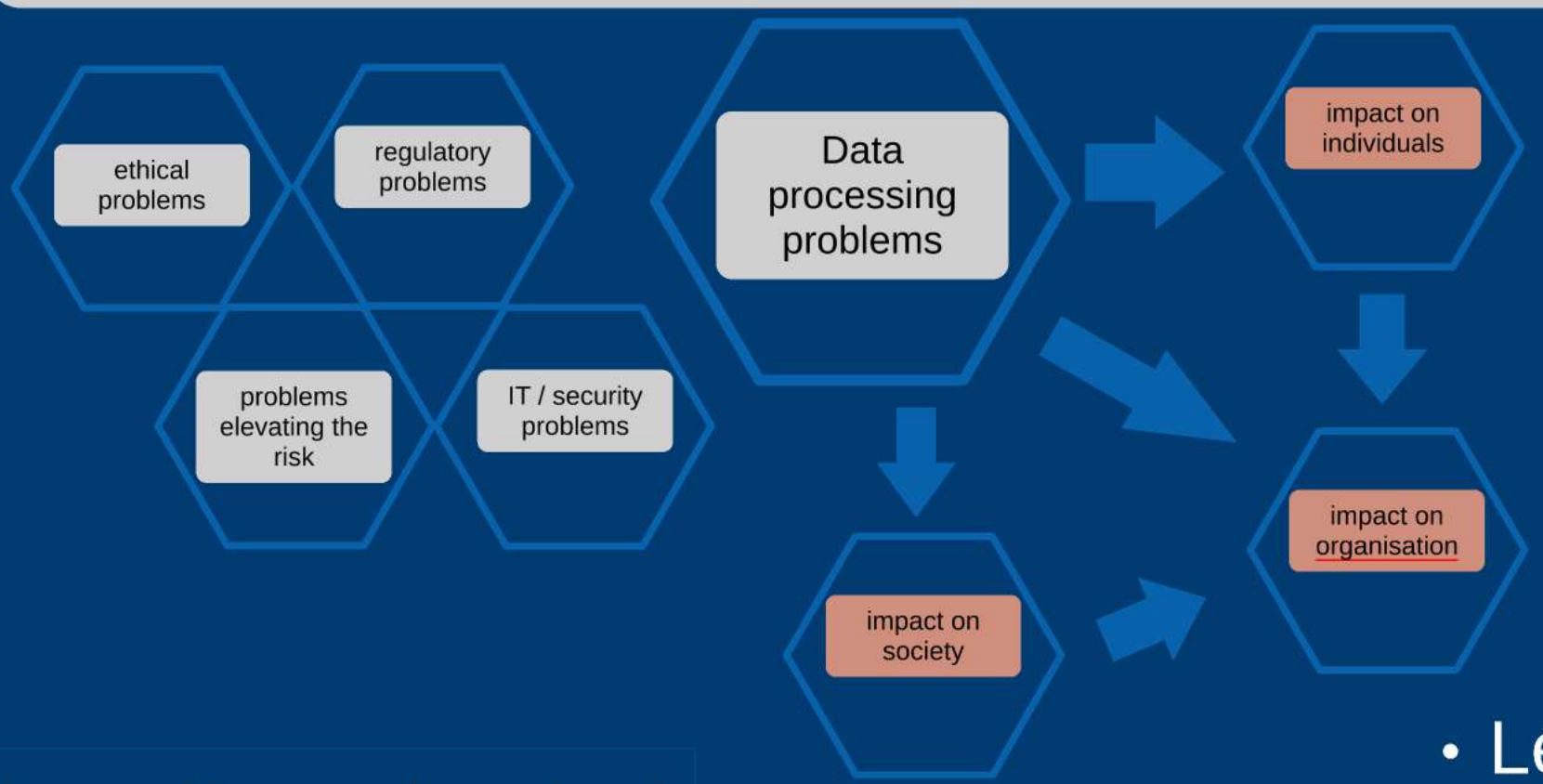
- Engagement of stakeholders, such as IT, security, legal, risk, HR, or finance is crucial.
- It may be possible to reuse some of the existing data inventories

Time-savers: automation, regular updates

- Utilising software tools for information management can streamline the process of creating and maintaining a data inventory
- Updating the inventory:
  - ongoing projects
  - privacy risks assessments
  - 'environmental scanning'

Identifying and Assessing Risks

Whose risks?



Privacy problems may have a broad origin, different nature and impact, but ultimately the organisation is responsible for them.

- Legal
- Reputational
- Operational
- Strategic

Assessing Risks

What can go wrong with data?
Inspect:

- technology
- people / employees
- processes

Include:

- 3rd parties and vendors
- privacy response processes

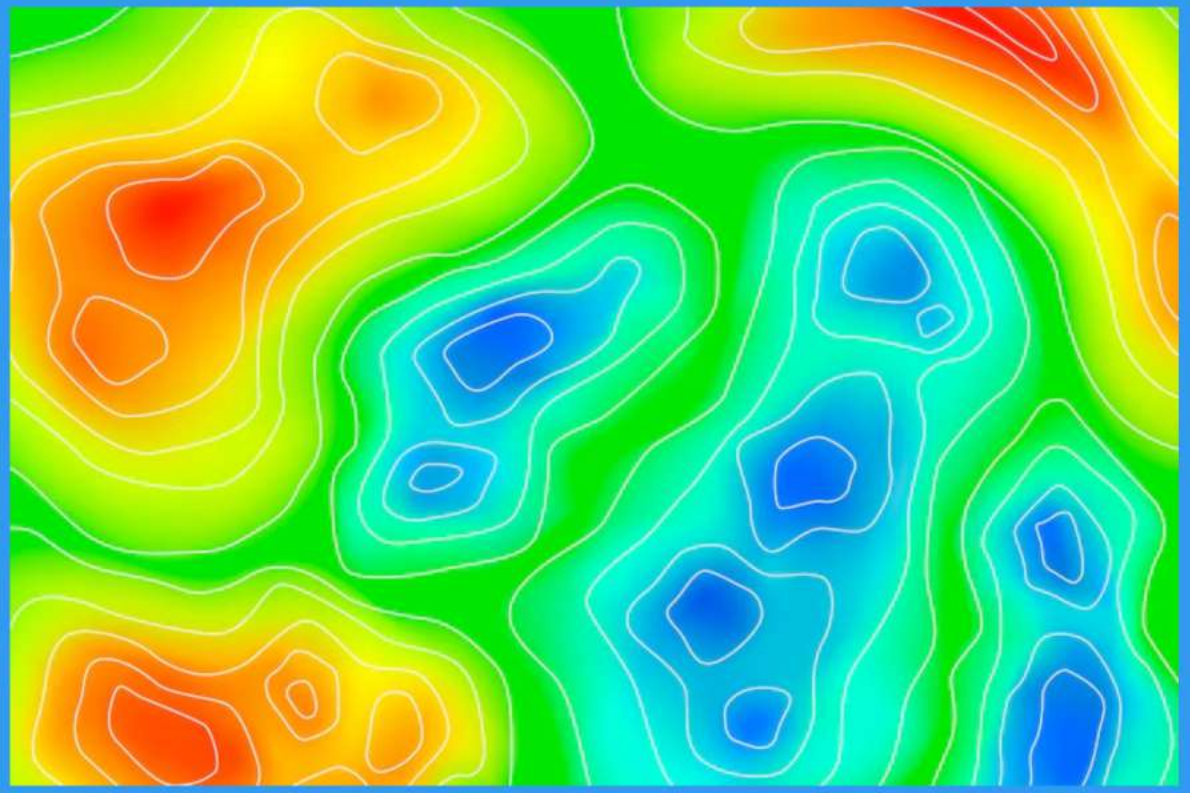
Tips

- Involve stakeholders (or let them do that with your help)
- Reuse the resources (web forms, risks descriptions)
- Find a way to leverage the existing assessments
- Think about the metrics (how to keep measuring the risk)
- Think about change management

Benefits of a risk map

Now you can:

- manage the risks
- prepare an action plan (start with the most important risks)
- develop assurance (monitoring, reporting, etc.)
- prepare incident management



Privacy Breach Framework

It's your agency's step-by-step guide for what to do when a privacy incident happens, whether that's a misplaced document, an email sent to the wrong person or a cyber attack.

Reduce the potential **reputational damage** to your organisation.

Prevent

Prevent harm to individuals

Preserve

Preserve trust with the public and your clients

Comply

Meet your legal obligations under the Privacy Act

Effectiveness

And respond in a way that's clear and confident, not chaotic

Reduce Costs

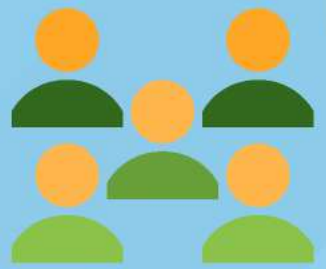
Breach Management Framework

TIPS ✓✓

Staff clearly understand what needs to happen in the event of a data breach

Document your framework clearly in writing

Run tabletop exercises or breach simulations



Available to all **staff**

How regularly?

Ensure it can be accessed quickly in an emergency

Review after major changes

- Nature of agency's operations
- Size of agency
- amount and sensitivity of the information you hold

Up to date framework

Key Elements Your Privacy Incident Response Framework Should Include

- **A clear explanation of what constitutes a privacy breach**
  - Train staff to recognise and report incidents
    - Make sure staff understand how to escalate concerns
- **A strategy for containing, assessing and managing breaches**
  - staff available to deal with the breach
    - Communications strategy that allows for the prompt notification of affected individuals
- **The roles and responsibilities of staff**
  - **Third-party providers**
    - Include them in planning and response testing Ensure contract terms require them to notify you quickly
  - Who should staff inform immediately if they suspect a breach
    - e.g Information and Communication Technology (ICT) support/forensics support
    - Clarify when a line manager can manage a breach, and when it must be escalated
      - Recommendation: All confirmed or suspected privacy breaches should be promptly escalated through the appropriate internal channels.
- **Metrics and documentation**
  - how your entity will record incidents
    - Have a plan for identifying and addressing weaknesses in how personal information is managed

Include The Fourth Step in your Framework

CONTAIN

Take immediate steps to limit the breach and prevent further compromise of personal information.

ASSESS

Gather the facts, evaluate the risks, including potential **harm to individuals,** and take action where possible to reduce that risk.

NOTIFY

Notify affected individuals and the Privacy Commissioner, if required. Notification is mandatory under the Privacy Act 2020 if the breach is likely to cause serious harm.

PREVENTION

After the incident is contained and managed, think long-term. What actions can you take to prevent this from happening again?

PREVENT HARM TO AFFECTED INDIVIDUALS

1. CONTAIN

- **Include possible containment measures , with practical examples in both your framework and staff training.**
  - For example, recalling an email, or requesting deletion by the recipient.
  - Questions to ask and include
    - Is the personal information still being shared, disclosed, or lost without authorisation?
    - Who currently has access to the personal information?
    - What can be done to secure the information, or stop the unauthorised access or disclosure, and reduce the risk of harm to affected individuals?
- **Identify the right people within the organisation**
- **Security measures**
  - NZ Police
  - Internal Security team

Limit the impact of the breach on affected individuals

Breach Assessment Process

Include it in your Framework

You will need this information

Assessment size and scope of the breach,

Assesing it as quickly as possible after the agency is made aware

What personal information was compromised

- About whom/Identify affected parties
- Sensitive/Non sensitive

What steps has your agency taken to reduce harm?

- How effective or successful were these steps?

Were the security measures strong enough to actually stop someone from accessing or using the information

- Was it encrypted or password protected? Could the device be remotely wiped?

Who accessed the information — and do they pose a risk?

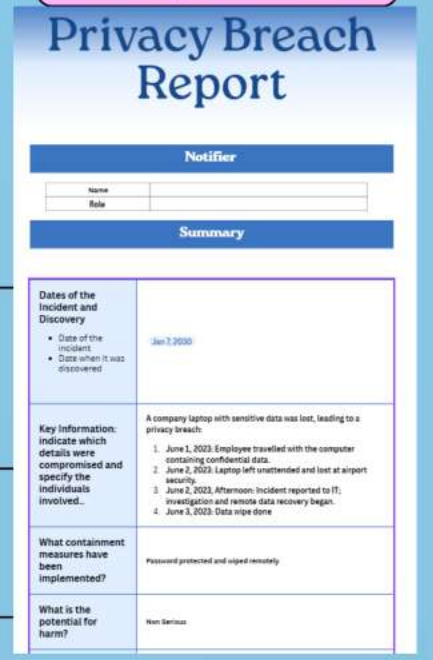
- Malicious Actor
- Someone unlikely to cause harm

Context matters.

Pro tip: Always request a timeline of events.

laurarodri26

Wheter Serious Harm is likely to occur



Privacy Breach Report

Notifier

Name	
Role	

Summary

Dates of the Incident and Discovery • Date of the incident • Date when it was discovered	Jan 7, 2030
Key information: indicate which details were compromised and specify the individuals involved..	A company laptop with sensitive data was lost, leading to a privacy breach: 1. June 1, 2023: Employee travelled with the computer containing confidential data. 2. June 2, 2023: Laptop left unattended and lost at airport security. 3. June 2, 2023, Afternoon: Incident reported to IT; investigation and remote data recovery began. 4. June 3, 2023: Data wipe done
What containment measures have been implemented?	Password protected and wiped remotely
What is the potential for harm?	Non Serious

Notification

Notification isn't just a legal requirement — it gives people a chance to protect themselves.

A well-handled notification shows respect, accountability, and manaakitanga.

THREE KEY POINTS TO INCLUDE IN YOUR FRAMEWORK

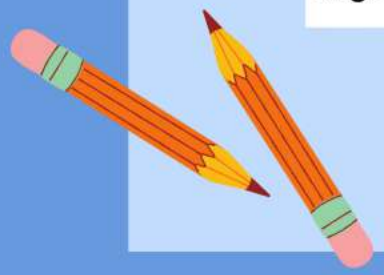
Why Notify?	Follow Section 117 (Part 6)	Make it part of your process
• Enables people to take action (e.g. replace ID, report to police) • Builds transparency and trust	Include all required information You must inform individuals of their **right to complain to the Privacy Commissioner**	• Use clear, consistent scripts • Frontline staff should know what to say • Train your teams — don't leave it to chance

Notifying the OPC

Include this in your Breach Management Framework:

Assess Risk of Harm

Once you've made the assessment and concluded that serious harm is likely, your framework should have a clear and urgent process that



Your framework should clearly set out:

- Highlights the importance of notifying the OPC without delay.
- Communicates to staff the legal obligation to notify
- Makes staff aware of the consequences of not notifying, including potential offences under section 212 of the Privacy Act

Pro Tip It's also really helpful to assign ownership of the OPC notification process. For example:
"If a notifiable privacy breach occurs, the Privacy Officer and only the Privacy Officer is responsible for contacting the OPC."

Prevention

Document and create data insights

NOTIFIER	DATE OF DISCOVERY	Date When It Happened	DESCRIPTION	IPP	Harm: SH/NSH	Notification to affected parties (date)

Privacy Officers Role: Getting Ahead of Risks Before They Become Breaches

A Practical Approach to Strengthening Privacy Assurances and Privacy Breach Management Frameworks

Dr. Marcin Betkier
Laura Rodriguez