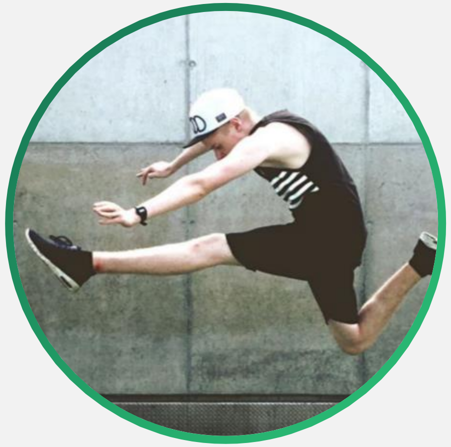
What is cyber resilience?

Cyber resilience



- Focus on the human factor
- The ability of any organization to prevent, detect, respond, recover

Cyber security

- More secure IT systems and infrastructure
- Controls and testing/management of vulnerabilities

Key Challenges Faced by an Organization

The Shock

Timing of the discovery of the breach vs. initial breach

In 50% of major breaches, breach is revealed by an outsider (law enforcement, client)

Help from authorities

Who can help? which authorities?

Do you have established relationships with the right people?

The chain of command

Challenged by ambiguity during a suspected breach

The only fact will be that you won't know all the facts

Opinions may fill the gap where facts are missing

Legal and moral responsibilities

They might not be immediately clear

Law enforcement may ask you not to notify clients

Conflicting notification requirements

Serious decisions require money

Is the breach covered by your cybersecurity insurance?

Breach notification to individuals typically require credit monitoring in some countries

Surge in enquiries and criticism

Irate calls from clients

List of stakeholders is long: regulators, clients, staff, press, social media

Organization are criticised even if criminal attack

Key areas for Legal

Response

a business' immediate response to a cyber attack is crucial

Investigation

examining how the attacker was able to penetrate the system and gathering evidence

Communication

is essential – from discovery to resolution

Response

1. Identify
2. Assemble team
3. Establish and maintain privilege
4. Document preservation
5. Contain the incident – eradication – recovery
6. Insurance

Investigation

1. Internal investigation
2. Third party forensics
3. External investigation

Communication

1. Transparency vs evaluation
2. Contractual reporting obligations
3. Regulatory reporting obligations

10 key things you need to do in an data incident I

Legal tasks/role identified in orange

Establish a “privileged” communication channel

Establishing a privileged reporting channel maintains the confidentiality of the investigation

- Legal establish with crisis team a clear reporting protocol : provide instructions to team members to ensure that any communication should include Legal to ensure privilege
- Legal counsel should provide legal advice, retain cyber security experts and direct responses every step of the way to protect the privilege of the investigation and of applicable internal communications.
- BCG Incident response team members should label documents (including email traffic) as **“Attorney-Client Privilege/Work Product Communications.”**
- Email traffic communications between BCG Incident response team members should be with outside counsel cced.
- Communications between the client and the external firm/expert should be through outside counsel or in the presence of outside counsel.
- External firm/expert should label documents (including email traffic) as “Attorney-Client Privilege/Work Product Communications.”

Incident assessment

what Legal needs to know from IT Security:

- What incident?
  - Who accessed the data and how
  - How the data may be used
  - Whether the data is encrypted
  - If there is a risk of identity theft
- What data?
  - Number of people affected, if any
  - From which countries (if not possible to identify this from the data, need to involve the owner of the data (project team or relevant function)
  - What are the exact categories of data

Avoid referring to the incident as a breach, at least until you have determined that a breach has occured. Instruct the team to refer to the matter as an "incident"

With respect to countries, ask for the data subjects residency in addition to the citizenship.

Use independent experts

- **Forensic experts, pre-vetted by IT security, retained and directed by outside legal counsel,** can verify the depth and extent of the breach, advise how to stop data loss, secure evidence and prevent further harm. They are also trained to preserve evidence (including that which may exist only in temporary memory)
- **Hire external legal counsel that will support in the assessment of regulatory and contractual risk,** best resource to work with regulators, law enforcement and forensic experts as they should have established relationships

Identify outside counsel contact details

10 key things you need to do in an data incident II
Legal tasks/role identified in orange

Assessment of regulatory and contractual risk

Based on information provided by IT Security response team and external counsel advice, Legal to determine:

- Identify applicable law
- Whether reported incident legally qualifies a breach
- Whether notification to the affected individuals is required by local law
- Whether notification to the affected individuals is required as part of a contractual obligation
- When to notify, how to notify and who notifies the affected individual and/or client
- What to include in the notification notice
- Notifying other relevant third parties - for example: National Data Protection Authority / Credit card companies or credit reporting agencies
- Contacting/notifying Law enforcement authorities :

Capture and document notification decision and rationale

Stop additional data loss

If the breach is ongoing,

- IT security to consult with forensic and cyber security experts and trained IT staff about taking affected systems offline by disconnecting them from the network and using tools to dynamically image affected systems to preserve evidence prior to any such action.

Secure evidence and data logs

Secure and prevent physical access to affected systems such as servers and workstations to maintain the integrity of the evidence and

- ensure that only selected forensic experts and law enforcement (if applicable) have access.
- Preserve all security access devices (tokens, badges, key cards, etc), logs and surveillance tapes.
- **Legal to send evidence preservation letters to service and cloud providers. Track the chain of custody for all physical and digital evidence and take an inventory of any missing hardware.**

Preserve all affected system log files including firewall, VPN, mail, network, weband intrusion detection system logs as logs are critical for assessing the origins of the incident, its duration and the volume of data exfiltrated

Document the data breach

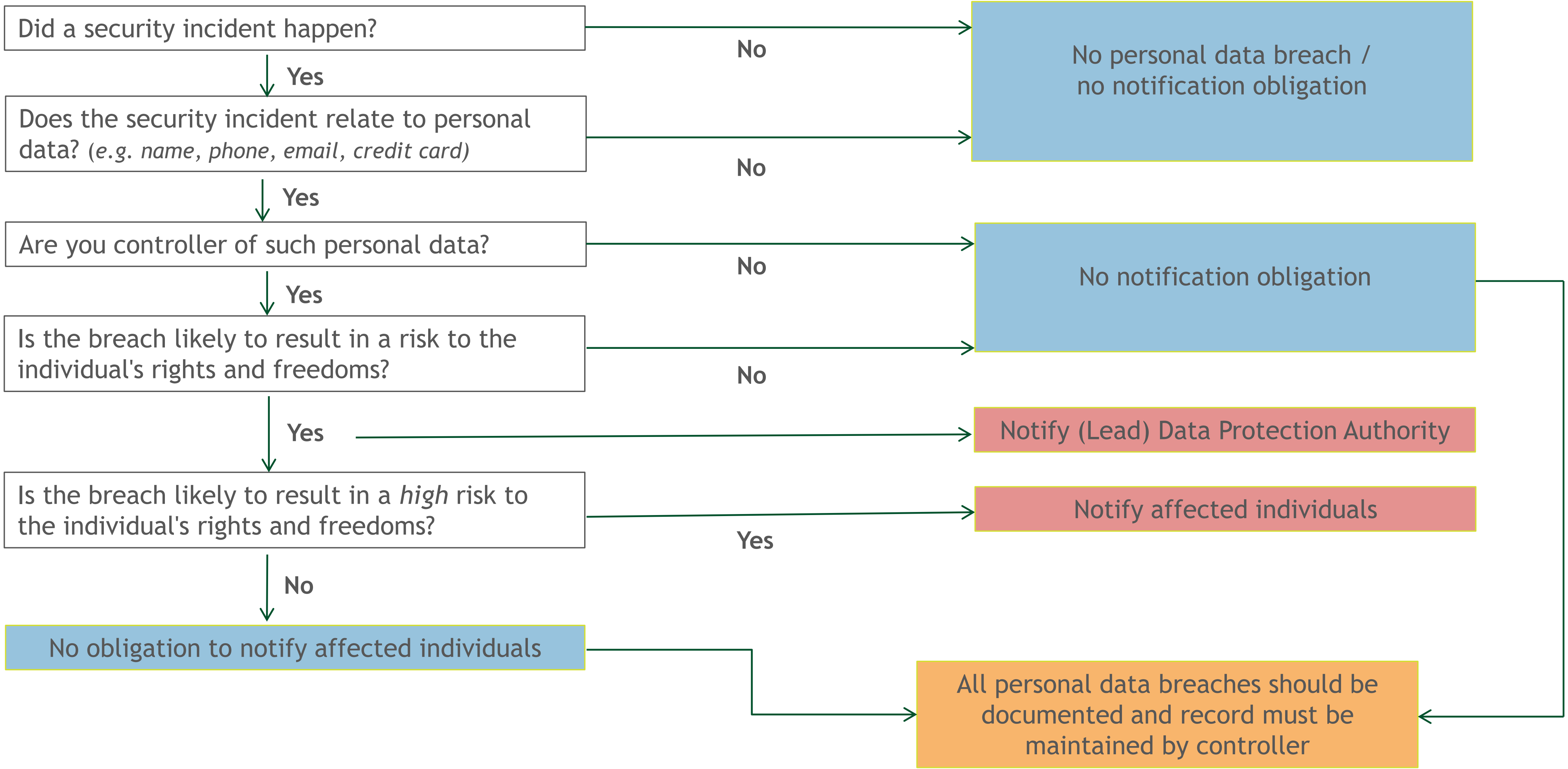
Legal to instruct IT security that there is a record in as much detail and as precisely as possible

- the date and time of the data breach, the personnel who discovered the breach,
- the nature of the breach, the kinds of data stolen/lost,
- when the response efforts began and all of the employees who had access to the affected systems

Insurance and long term PR

- **Notify insurance broker (with Treasury support)**
- Manage ongoing PR activities on the longer term : communicate on remediation plan

EU GDPR: Breach notification analysis flowchart



Did a security incident happen?

No

Yes

Does the security incident relate to personal data? *(e.g. name, phone, email, credit card)*

No

No personal data breach / no notification obligation

Yes

Are you controller of such personal data?

No

Yes

Is the breach likely to result in a risk to the individual's rights and freedoms?

No

No notification obligation

Yes

Notify (Lead) Data Protection Authority

Is the breach likely to result in a *high* risk to the individual's rights and freedoms?

Yes

Notify affected individuals

No

No obligation to notify affected individuals

All personal data breaches should be documented and record must be maintained by controller