Data Breach Crisis - Checklist

STAGE 1

Containment and Recovery

RAPID RESPONSE NETWORK

The first five

- Immediate steps you must take should you identify or suspect a data breach has occurred.

01 **Don't turn the computer off**

Some valuable memory and running processes are lost with power loss, and if your computer has been infected with Ransomware, some variants will delete files if you attempt to restart your computer.

02 **Quarantine devices from the rest of the network**

If you have shared drives, remove the ability for users to write to them. If the network is segregated, separate the infected device to a different subnet/vlan so it cannot communicate with other devices. If you have a flat network, unplug the internet cable or turn off the Wi-Fi connection.

03 **Logging and monitoring**

Your logging and monitoring software will have tracked all the changes that it is configured to monitor. The logs should help identify which devices accessed which parts of the network and when and what data may have been lost.

04 **Warn third parties**

Assess if and which third parties may need to be notified of your concerns although you must be equally alive to the risk of tipping off.

05 **Set up alternative channels of communication**

If you are concerned that your network has been compromised you will need to notify other users via alternative, pre-approved channels of communication. This means any system external from your regular communication channels such as encrypted texts but could equally mean physically speaking to people or communicating via an app not connected to the network.

Data Security & Forensics

Contain and limit further damage. Isolate the affected parts of the system. Disconnect the relevant devices or servers from the internet. Suspend but do not delete remote access capability. Change access controls such as usernames and passwords. Quarantine but do not delete any malware identified. Ensure you have a separate way for the data breach management team to communicate that is separate from the email system.

Ensure forensic evidence is preserved intact. It should be done as quickly as possible - which is crucial to the entire process. Any evidence that is lost or tampered with risks jeopardising the entire response to an incident and can have significant judicial and regulatory consequences.

Ensure you have access to external support.

Strategic Communications

For context, if mistakes are made it is typically in the early hours or days of the crisis - hence the importance of getting answers to these questions below.

- What precisely has happened, to whom (organisations and individuals) and what has the impact on them been? Gather these facts and determine your confidence level in the accuracy of them based on the sources and your ability to verify them.
- What do you not know yet and how can you get that information? The answer is key for decision-making, avoiding mistakes, and scenario planning.
- Are you going to be purely reactive in your communications in the initial period or do you need to be proactive? With the latter, which audience is most important to communicate with, in what order, and what are you going to say and not say?

Things to bear in mind in your messaging:

- Convey that the organization is effectively managing the situation and knows the key steps and measures to take in order to limit the damage.
- Ensure that those impacted have been made aware of that and they know that the organization is acting accordingly to protect them.
- How much of what occurred has become public, by and to whom, and is it factually accurate? Do corrections of fact need to be made and if so how and with/ through whom?
- What steps need to be taken with external parties and which ones? (The media is not a constituency but a delivery system that has to be managed.)

Legal

Prioritise establishing the point at which your organisation became aware of the breach. Art. 33(1) of the GDPR sets out that the Controller shall notify the competent supervisory authority no later than 72 hours after having become aware of a data breach that may result in a risk to the rights and freedoms of natural persons. Note that the GDPR may also apply to non-EU based entities processing personal data of EU citizens.

If the Controller cannot provide all the information at the same time (typically this may be the case if a data breach has occurred due to a ransomware attack), it may provide it in phases. Processors shall notify controllers without undue delay (e.g., no later than 24 hours).

Keep in mind the importance of maintaining a breach log or record because Art. 33(5) obliges Controllers to document any personal data breach. Additionally, a breach log may contribute to comply with the accountability duties (see also Stage 4 below). Maintaining such a record will also help, both at a corporate level and at a general interest level, to have a better understanding of the causes of data breaches to implement more appropriate, effective, and sophisticated remedies in the future.

STAGE 2

Risk Assessment

RAPID RESPONSE NETWORK

Data Security & Forensics

It's a stressful time. Tension can build between the demands of the forensic investigators and other advisors (legal and communications). However, having some degree of tension can be a good challenge to self-evaluate the risk assessment process. It can become an issue if other advisors want to take action which is out of step with what facts are known.

There is a real risk to losing reputational integrity through advisors wanting to press ahead when all the evidence has not yet been forensically gathered or analysed. Of course, there is always going to be a measure of doubt, but it is far better to take steps with a higher degree of confidence based on evidential analysis then pressing ahead and being tripped up by questions customers and the media would ask which cannot be answered

Strategic Communications

You will be focussed on monitoring and media engagement (determining what to do off the record, on background, and on the record – who will public statements be attributed to?) and need to consider how what the media reports will impact internal/external stakeholders and business partnerships.

Think about what you need to do if the media coverage is factually inaccurate and, in some cases, damaging. While the media is a delivery system, engagement must be "high touch".

Consider who should be the 'face' for the Breach Management Team (BMT). The face of the team divides into two categories – first, to internal/external stakeholders and business partners; and second, to the media. Corporate leaders must be prepared to function in this role, working closely with the BMT.

You can almost never be too empathetic. Public statements of accountability must be carefully calibrated relative to potential liability: words matter.

Avoid expressing empathy without connecting it to accountability, and accountability without stating precisely what steps will be taken to fulfil responsibility

Legal

Notifying the Regulator and/or data subjects. The regulations state that Controllers will need to notify the relevant data protection authorities of a data breach unless the relevant data breach is unlikely to result in a risk to the rights and freedoms of data subjects.

This means that Controllers have to assess whether to notify the Regulator or not. The *Guidelines on personal data breach notification under Regulation 2016/679* and the *Guidelines 01/2021 on examples regarding personal data breach notification give some illustrations at this regard*. For instance, a controller shall not notify in case of losing an encrypted device, but it shall in case of a ransomware attack (except if the attack only affected encrypted systems).

Risk assessment criteria

- A simple set of questions to help evaluate the scale and severity of a data breach.

What type of data is involved?

What number of individuals' personal data is affected by the breach?

Can the individuals be identified whose data has been breached?
Whether they are staff, customers or suppliers will, to some extent, determine the level of risk posed by the breach.

How sensitive is the data?
Data can be sensitive because of its personal nature or because of the consequences of its misuse or both.

What information could the missing data reveal about an individual?

What has happened to the data?
Stolen data could be used for purposes which are detrimental to the individuals concerned, whereas damaged data may.

Can the individuals be harmed?
Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?

If data has been lost or stolen, are there any protections in place such as encryption?

Are there wider consequences of the data loss to consider such as a risk to public health or loss of public confidence?

STAGE 3

Notification

RAPID RESPONSE NETWORK

Information for the regulator and affected individuals

♦ The minimum information required when notifying the regulator of the data breach is as follows

01 The nature of the breach including where possible, the approximate number of individuals who are affected and the approximate number of records concerned.

02 The name and contact details of the data protection officer or other contact point where more information can be obtained.

03 The likely consequences of the breach.

04 The measures taken or proposed to be taken by the organisation to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

The following additional information should be provided to the affected individuals:

05 Specific advice to protect themselves from possible adverse consequences of the breach, such as resetting passwords.

Data Security & Forensics

In preparation for notification and setting out mitigation steps, a fully holistic approach should be considered. It isn't enough to only identify what has been technically exploited. A comprehensive strategy encompassing people, process, and technology, integrating lessons learnt with third parties, will go a long way to demonstrating you have grappled with the issues and the consequences on data subjects.

Being able to demonstrate this to regulatory bodies as well as data subjects shows your commitment to continually improving data security and placing emphasis on protecting sensitive information.

Strategic Communications

Assess whether multiple jurisdictions are involved. While some people in some jurisdictions may be impacted more than others, conveying the sense that everyone's experience is being acknowledged and respected and as much as possible treated equally in terms of notification and corrective action is essential. There are no "second class citizens" although there may be a sequencing issue in who is engaged with first and more than others.

Being proactive with regulators and law enforcement is vitally important. If they have to come to you first, then they've already reached preliminary conclusions about your liability without insight into key facts in your possession let alone your analysis of the situation.

Even if this means an enforcement action, it will very likely be less severe, and you'll have the opportunity to negotiate it in a more constructive way.

The optics of being proactive in this way has reputational benefits. It underscores the conviction to being accountable and taking responsibility for any mistakes/ oversights. You'll get more reputational dividends, short, medium and long-term, for "doing the right thing the right way".

Legal

Remember to notify the relevant authorities of a breach when you are required to do so. If not, the consequences can be costly and far-reaching

- Legal consequences: Art. 83(4) of the GDPR sets out that infringements of data breach provisions shall be subject to fines up to €10,000,000, or up to 2% of the total worldwide annual turnover (whichever is higher). In addition, depending on the consequences of data breach, the infringement could affect other GDPR provisions becoming a very severe infringement (where fines could reach up to €20,000,000 or 4% worldwide annual turnover, likewise whichever is higher).
- Reputational consequences: Beyond these administrative fines, a significant reputational crisis may result from a data breach since generally it involves a loss of trust that shall be properly managed and countered. In certain EU countries, sanctions may be subject to official publication (e.g., this applies in Spain vis-à-vis sanctions above €1,000,000) and the media is highly likely to track and report these.
- Financial consequences: These are closely related to legal and reputational consequences and may involve loss of clients, loss of profits, or recovery and restitution costs, among others.
- Other consequences: Further consequences may arise, particularly if the data breach affects a public institution (diplomatic, institutional, or governmental, among others).

STAGE 4

Evaluation and Response

RAPID RESPONSE NETWORK

Data Security & Forensics

Putting out the fires after an incident and data breach is important. However, just as important is being able to follow up with what is often the most overlooked and undervalued, yet important phase of the whole response cycle – a full evaluation and lessons learnt process. Neglecting this stage can lead to falling foul of the same type of incident again and thus losing reputational confidence both in the eyes of clients and regulatory authorities.

A thoroughly thought-out evaluation exercise will include changing processes and procedures, committing to undertaking regular (often annual) technical testing regimes and following up across the business with adequate planning and exercising to ensure teams are well equipped to swiftly deal with future incidents with minimal impact.

Strategic Communications

People remember not just what you did and said but what you didn't do and didn't say. While you can't "fall on your sword" because of the potential and actual liability issues, a degree of admission (carefully calibrated against liability issues) will do more to rebuild trust. Admission combined with taking the steps to protect people immediately and for the long-term will produce reputational benefits.

The greater the failure the more specific and meaningful the learnings must be defined and communicated. But there isn't always benefit in pushing too hard on all that was learned. Be selective. Focus on those that are most relevant to what happened, to whom it happened to, and how because of those learnings you create confidence that you've minimised the chances of it happening again.

Legal

Data breaches are in most cases unpredictable and unavoidable. Therefore, the Regulator does not require entities to be fully armoured against data breaches but requires them to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. In other words, these are best efforts obligations (i.e., having properly implemented the appropriate measures) and not result obligations (i.e., avoiding any potential data breaches).

Obviously, having a complete and updated security protocol is not sufficient. It has to be properly implemented. 'Tick-box compliance' is not an option when we talk about privacy.

It is important for you to have in place, technical and organisational measures to ensure the ongoing confidentiality, integrity, and availability of personal data and to be able to demonstrate, in the event a data breach occurs that such measures were implemented.

How would you do that? Consider having documented and structured the following measures, which are aligned with the GDPR provisions (particularly, with Art. 32 GDPR):

- prior security risk assessment of suppliers (i.e., processors);
- records of processing;
- data breach protocols;
- cybersecurity insurance;
- awareness program and in-house training;
- business continuity and recovery plan;
- encryption or pseudonymisation;
- access to the systems on a structured need-to-know basis;
- vulnerability management process;
- periodic vulnerability testing and/or external audit.

ASSERT your cyber-strength

♦ Follow this six-point plan to strengthen your resistance to a cyber attack and/or data breach.

A — **Awareness training**
Customised awareness training should be put in place along with internal support for the Incident Response Team.

S — **Simulation**
Attacks from Ransomware or phishing emails and other sorts of social engineering should all be periodically rehearsed to test infrastructure security as well as the incident.

S — **Scanning**
Your organisation's network and website should be regularly scanned for vulnerabilities as should the digital footprints of the senior leadership and primary stakeholders.

E — **Ethical hack**
An ethical hack should be commissioned to provide a real-time simulated attack on the company to assist in awareness training and ensure that all the employees appreciate the value of the data they are handling.

R — **Resilience**
An analysis of the risks associated with all the possible sources of the attack from bad leavers to competitors and cyber-criminals, and how they might be mitigated.

T — **Team**
The Incident Response Team should be regularly rehearsed and clear in their roles and reporting.

CONCLUSION

RAPID RESPONSE NETWORK

What should you be doing now?

- Assessing your ability to face up to a data breach incident.

01 Data should be stored with appropriate security measures determined by its sensitivity.

02 Clear internal policies and procedures for breach management and notification need to be drawn up and rehearsed.

03 An Internal Breach Register or Log needs to be set up.

04 All staff should be trained about what constitutes a data breach and to look out for suspicious behaviour and online activity.

05 Data protection clauses should be reviewed to ensure they require data processors and other third-party data handlers to proactively notify of breaches to you.

06 Insurance policies should be revisited to assess the extent of their coverage in case of breaches.

Conversely, a well-managed response to a data breach can engender trust and enhance a business' reputation. The focus of any cyber incident response plan should be on protecting individuals and their personal data. Data breach management must be integrated, rehearsed and adaptable.

In any event, the overriding principles of successful data breach management remain integration, accuracy, accountability, speed of response and consistency of communications.

Panellists

Magnus Boyd
Head of Legal and Partner, Schillings
magnus.boyd@schillingspartners.com

Montieth M. Illingworth
CEO and Global Managing Partner, Montieth & Company
montieth@montiethco.com

Sergio de Juan-Creix
Lawyer and Partner, Croma Legal
sergio.dejuancreix@croma.legal

Sachin Bhatt
Senior Associate - Cyber Security Advisory, Schillings
sachin.bhatt@schillingspartners.com