DATA SECURITY BREACHES: A GUIDE TO INCIDENT READINESS AND RESPONSE

BRYAN CAVE LEIGHTON PAISNER BCLP

www.bclplaw.com

News stories about high profile hacks and cyber incidents, as well as the advent of GDPR in 2018, have moved cyber-security up the agenda of many businesses, as they increasingly face the possibility of a security incident and its consequences.

In order to effectively respond to a data security incident, businesses must understand what a "security incident" entails, what they should do to prepare before an incident occurs, and what practical considerations will confront them when an incident arises. Effective response also requires understanding and preparing for the possibility that a data security incident may lead to regulatory investigations, litigation and public scrutiny.

This Guide provides a basic framework to assist in-house legal departments and incident response teams with thinking about how they would identify and handle a security incident and any subsequent legal, reputational and regulatory risks. As a preliminary to more tailored advice, we hope it helps your business ensure that it is as prepared as possible for an attack.

Oran Gelb
Partner, Commercial
Dispute Resolution
London, UK

Jena Valdetero
Partner, Commercial
Dispute Resolution
Chicago, USA

UNDERSTANDING THE NATURE AND SCOPE OF DATA EVENTS, INCIDENTS AND BREACHES

The GDPR defines a "data breach" as a situation where there is evidence of a breach of security which leads to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. In other words, unlike some of its international counterparts, the GDPR is concerned not only with breaches that impact the confidentiality of personal data, but also integrity and availability. It would trigger a legal obligation for an organisation to investigate the situation and potentially notify consumers, regulators, or business partners.

However, many of the situations that are referred to as "data breaches" in the media, and possibly by others within an organisation, do not in fact meet this definition. For the purposes of clarity, this Guide uses three terms to refer to security situations: a data security "event," "incident," and "breach".

It's more than just semantics: organisations should be careful to understand the lexicon, as clarity in identifying and describing what has occurred may prevent issues over (for example) the scope of insurance coverage, the triggering of any contractual obligation, and the scope of engagements of third parties including forensic investigators.

SECURITY EVENT:

An unauthorised attempt to obtain data or a situation in which data could, theoretically, be exposed. An event might be serious and turn into an "incident" or a "breach," but many events are automatically identified by an information security team or systems monitoring software and are resolved without requiring intervention or investigation.

Examples include a failed log-in that suspends an account, a phishing email that is caught in a spam filter, or an attachment that is screened and quarantined by an antivirus program.

SECURITY INCIDENT:

An event for which there is a greater likelihood that data has left, or will leave, the organisation, but it is not known whether unauthorised acquisition or access has occurred. For example, an organisation knows that a laptop has been lost, but not what information it contains or whether it has fallen into the hands of someone who might have an interest in misusing data.

Security incidents almost always necessitate a thorough investigation to test the suspicion that personal data has been improperly accessed or acquired.

SECURITY BREACH:

Where personal data has been accessed or acquired by an unauthorised party and that access or acquisition has created the possibility that an individual may be harmed, or where personal data has been unalterably changed or rendered unavailable.

For example, if a stolen laptop contained unencrypted bank account details of employees, the incident would fall under the definition of a "security breach".

DATA SECURITY INCIDENT PREPAREDNESS

As the number of attacks from third parties that exploit previously unknown software vulnerabilities (sometimes referred to as "zero-day exploits") has risen dramatically, most organisations now realise that even the best security is not a guarantee against a breach. Preparing in advance for how you will respond when a security incident or breach occurs is essential.

Where we have seen clients stumble in the course of responding to a breach usually relates to:

How fast did the organisation investigate and respond to the incident?

How well did the organisation communicate with stakeholders, including the public?

Performance in these two aspects is often directly linked to whether the organisation had prepared in advance how to handle a security incident.

Failure to prepare in advance can lead to an increase in certain costs often associated with a breach:	
Reputational Costs	The confidence of consumers or clients is eroded.
Business Continuity Costs	For example, a network has to be taken off-line to prevent further data-loss, disrupting normal business activity.
Competitive Disadvantage	If competitively sensitive information is leaked or lost.
Investigation Costs	Including IT forensic experts and legal assistance.
Contractual Costs	Contractual liability to business partners, for example if the breach affects data in your possession belonging to them.
Notification Costs	Direct notification costs such as the cost of printing and mailing notification letters; indirect costs of providing consumers with credit or identity monitoring, identity–theft insurance, or identity–theft restoration services.
Regulatory Costs	Legal expenses are associated with a regulatory investigation related to any type of authority or regulator; the regulators' (including ICO's) powers to levy significant fines in this space have been well-publicised.
Litigation Costs	Although the structure of the English litigation system and the difficulty of quantifying loss to individuals in a data breach may make litigation by those affected difficult to pursue in this jurisdiction, there is an increasing number of claims relating to data breaches. We anticipate that trend continuing as consumers become more aware, post-GDPR, of their data privacy rights. Organisations may be under pressure to settle complaints quickly before they escalate and set precedents.

KEY PLAYERS

Data security incident readiness will inevitably require engagement from and coordination with numerous individuals or teams forming the incident response team, including:

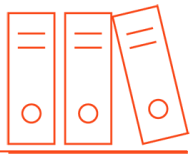
- senior management
- finance
- operations
- information technology and/or security
- legal
- public relations/communications
- human resources

Members from these groups will be crucial in deciding how the organisation will handle key business decisions that will arise.

And whilst internal resources are vital, organisations frequently also turn to external advisers (e.g. legal, forensic specialists, crisis PR firms) to assist both in the planning and training for an incident, and executing incident response plans when the time comes.

Identifying these partners in advance permits an organisation to vet expertise and negotiate price and the terms of engagement when it is not under the stress and time pressure of a breach. Generally, organisations should look for partners who have extensive experience responding to breaches and who will be able to leverage that experience to better and more cost-effectively assist you.

KEY DOCUMENTS



Most breaches will require reference to a few crucial documents, including a cyber insurance plan, written information security plan (WISP) and an incident response plan (IRP).

Understanding the contents of these documents and how they will come into play in a breach could be critical. Keep these documents readily available in hard copy or ensure they are accessible from a separate system in the event of an encryption or system shutdown.

Incident Response Plan

An incident response plan explains how an organisation handles security events, incidents and breaches. It helps employees understand the role that they are expected to play and those with whom they should be coordinating. It can also help educate employees concerning what they should and should not do when faced with a security incident.

There is no set structure for an Incident Response Plan but it should, at a minimum, include the following points:

- Define security event, incident and breach.
- Contain steps to internally escalate a security event that becomes an incident, or an incident that becomes a breach so that it can quickly be identified.
- Contain up-to-date internal and external contact details for key individuals on the incident response team and key vendors.
- Outline responsibilities for incident response team members when conducting an incident investigation, including a project manager who will hold each team member accountable for their action items.
- Include a record keeping protocol.
- Plan for post-incident reporting and reviewing to ensure a proper record is maintained and the team evaluates lessons learned from the incident response.
- Contain sufficient flexibility to deviate from the plan such that the organisation will not later be criticised for not strictly following the IRP.
- Identify key countries where there may be a breach reporting obligation and any timing requirements (e.g. 72 hours under the GDPR).
- For data processors or joint controllers, include a plan for notifying the controller without undue delay, as required by the GDPR, in the event of a breach of personal data. This may include a list of key business partners and their contact information.

Written Information Security Programme

After a security breach occurs, consumers, the media, regulators, and other interested parties routinely ask what measures were taken to prevent the breach in the first place. Consider, at a minimum, a written information security programme. A solid WISP will contain certain minimum administrative, technical, and physical safeguards to protect personal data. This will also help establish the technical and organisational measures required to be implemented by data controllers under Article 24 of the GDPR.

Generally, it will:

- designate an individual to maintain and be responsible for the programme;
- identify any reasonably foreseeable data security risks;
- protect and restrict access to paper and electronic forms of any personal information; and,
- oversee any third-party service providers and ensure that those service providers comply with the GDPR and other applicable regulations.

A WISP will need to be considered through the lens of any regulations, standards and particular risks that apply to the specific industry in which your business operates, to enhance the more generic requirements which will apply to any business – set out for example in well-known cybersecurity frameworks, like NIST or ISO.

Cyber Insurance Plan

Organisations increasingly recognise the value of cyber liability insurance, covering "first party" costs (i.e. costs incurred in responding to a breach) such as legal counsel and forensic investigations, and "third-party" costs, such as regulatory investigations or litigation. Coverage can vary quite dramatically depending on the policy, and it is not yet clear whether public policy will permit insurance coverage for regulatory fines and certain types of awards in litigation. Policies should be reviewed carefully to understand the degree to which the policy protects (or does not) from potential incident-related costs and liability. You will also need an awareness of any policy requirements to take specific actions such as notifying the insurer or using pre-approved data incident response resources (e.g. investigators, credit monitoring, mailing services, public relations firms, or external lawyers). Because data security law is rapidly evolving and changing, the policy should be reviewed annually to ensure it continues to align with changes in the legal landscape, coverage trends, and the organisation's operations. In the UK, there have already been some high profile disputes with insurers over whether a security incident is covered by the policy concerned.

Organisations should also decide whether they require cover for costs associated with average-size breaches (which can be significant but not necessarily financially threatening) or only for catastrophic "bet-the-company" breaches. The type of incident cover will affect the policy excess which is negotiated, as well as other key factors.

Training

The documents above pay no more than lip service if the organisation is not familiar with them and has not implemented training to ensure that they are understood and followed. Each training session inevitably identifies areas in which an organisation can improve its plan and/or provide additional training to improve its response.

The best way to test an organisation's response readiness is to create a mock data security breach in a controlled environment, also known as a tabletop exercise. The incident response team is presented with a fake breach scenario with changing facts designed to elicit discussion so that the team can adjust and refine its plan. The exercise can create "muscle memory" to help alleviate some of the "first time" fears that team members might feel in a real incident.

INCIDENT RESPONSE

Following a coherent Incident Response Plan is generally the best way to manage an incident. Ensuring that the incident response team knows the plan well, and is comfortable with how they might respond under the pressure of an incident, is as vital as the plan itself.

You should prepare to be flexible, however, and continue to take timely advice from lawyers, experts, law enforcement and IT professionals as the situation develops and changes.

Be aware also that there will be no set timeline or order of response steps – even as the incident is in its initial stages of investigation, you may start to face pressure from consumers, media, or regulators and you need to be able to meet that pressure head-on, in a controlled way.

The key best practice steps to respond to an incident, taking into account possible legal requirements and obligations will include:

- investigation and coordination;
- coordination between data controllers and data processors;
- communication with the Public/Media;
- communication with Law Enforcement; and,
- assistance for Affected Data Subjects.

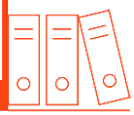
Investigation and coordination

Notify legal advisers as soon as possible, and include them within the incident response team. Although difficult to attain in English law, involving lawyers will maximise the possibility that aspects of the investigation are subject to legal professional privilege, which will give you more control over disclosure, for example in ensuing litigation or regulatory enforcement. Legal advisers will also ensure you are fully apprised, early on, of any regulatory notification obligations, including urgent notification deadlines, like the GDPR's 72-hour regulatory reporting requirement.

Form a core team of personnel to attend to the breach. Following the Incident Response Plan, this may include representatives from IT, legal/risk management, operations, marketing & communications, and human resources (Ideally, the team will have been identified and trained on data breach response prior to any incident.) The team should be prepared to convene as soon as possible to ensure everyone is aligned on the investigation and response plan.

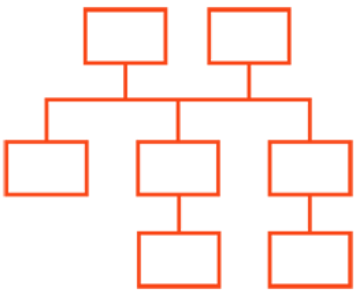
Retain a third-party forensic investigator. External forensic investigators will be experienced in acting quickly and comprehensively in a data breach crisis and can ensure no mistakes are made in containing the incident and preserving evidence. The investigator should be able to investigate the attack vector, decipher the scope of the breach—including what records were viewed or acquired and how many times the third-party gained access to the system—and identify whether and how data was removed from the organisation's IT environment.
A proactive organisation will identify and retain a forensic investigator before a breach occurs. Doing so will ensure that you can negotiate favourable terms and conditions in the retainer agreement before a crisis situation adversely affects your bargaining power.

Contain the breach and preserve evidence. The IT department should be advised to identify the source of the breach and isolate the compromised systems from the network. Evidence should not be destroyed or altered, and the system should be continuously monitored. In some instances, the legal team may need to help IT understand what it means to forensically preserve evidence, and to evaluate whether methods for copying and logging data would be defensible before a regulator or in court.



Assign a Crisis Manager. A pre-designated crisis manager that reports directly to, and has authority conferred from, senior management often facilitates the most efficient response. Take advice from appointed lawyers to ensure the flow of information takes place in privileged circumstances, where possible.

Coordination between data controllers and data processors



You probably rely on agreements with third parties to carry out various business operations. These agreements may authorise your business or the vendor to have access to or possess personal data owned by the other entity. Articles 33 and 34 of the GDPR place the obligations to notify regulators and affected individuals on the relevant data controller, but in many cases this will also require swift action from and cooperation by the processor. Thus, in advance of any security incident, it is important to have identified for each contract the nature of the role of each party – whether they are controllers or processors of data – and how that affects the practicalities and responsibilities for action and notification.

Even if you are the processor, however, the controller may look to you to satisfy its notification obligations, including paying for the costs associated. Accordingly, you should ensure that your cyber policy will provide coverage for notification expenses when you are not the controller.

Communication with the Public/Media

A proactive strategy assumes that your organisation has control concerning when, and what, information will be conveyed to the public, to the media, and to the affected individuals about the breach. It will also include who will make any statements and any key stakeholders (the board, key clients) who would need to be notified in advance of public statements.

Your plan should allow for consideration of the advantages and disadvantages of early notification in a given situation, weighing the need to present a coherent and accurate picture to the public whose personal data may have been compromised, against the risks of premature publicity which may do more harm than good. In many situations an organisation cannot control when the public becomes aware of a breach and it may be beneficial to have prepared holding statements in advance. You may see information about the breach disseminated in the media without your knowledge or input, or you may be asked by the media to comment about the breach. You should be prepared to work closely with the communications teams when determining how to respond to such reports.

Communication with Law Enforcement

Where a crime is being committed, you should consider reporting it to law enforcement, specifically the police via Action Fraud in England & Wales. Contacting law enforcement may result in assistance to stop the criminal behaviour, useful information that may help your own investigation of the incident, or prosecution of the culprit. It may also help demonstrate to the public that the organisation was diligent in investigating the incident and taking steps to protect consumers and that the organisation itself is the victim of a criminal attack.

Assistance for Affected Data Subjects

There are several factors to consider when choosing what (if any) services to offer affected individuals. Credit monitoring services (and to a lesser extent identity restoration services and identity theft insurance) may be offered in certain countries, but not all breaches involve data that would necessarily put a client's finances or credit history at risk. Nevertheless, businesses should be prepared to consider whether a failure to offer such services—even if unconnected to the breach—could be regarded by individuals and regulators as a failure to adequately protect data subjects.

If you choose to offer credit monitoring, identity restoration services, and/or ID theft insurance, you should carefully consider in advance the vendors that are selected to provide the services and any contractual limitations on those vendors.

DATA BREACH RESPONSE AT BRYAN CAVE LEIGHTON PAISNER

Bryan Cave Leighton Paisner has a world-class data breach response practice which has responded to more than two thousand significant breaches or incidents worldwide. We leverage that experience to help companies identify gaps in their readiness to respond to a breach, and to train companies on how to respond to breaches effectively, with the goal of mitigating risk.

Europe

Oran Gelb
Partner, Commercial Dispute Resolution
London
Tel: +44 (0)20 3400 4168
oran.gelb@bclplaw.com

Kate Brimsted
Partner, Technology & Commercial, Corporate
London
Tel: +44 (0)20 3400 3207
kate.brimsted@bclplaw.com

Sarah Delon-Bouquet
Counsel, Employment & Labor
Paris
T: +33 (0) 1 44 17 77 25
sarah.delonbouquet@bclplaw.com

Sarah McAtominey
Senior Associate, Commercial Dispute Resolution
London
Tel: +44 (0)20 3400 3345
sarah.mcatominey@bclplaw.com

Tom Evans
Associate, Technology & Commercial, Corporate
London
Tel: +44 (0)20 3400 2661
tom.evans@bclplaw.com

USA

Jena Valdetero
Partner, Commercial Dispute Resolution
Chicago
T: +1 312 602 5056
jena.valdetero@bclplaw.com

David Zetoony
Partner, Technology & Commercial, Corporate
Boulder/Washington
T: +1 303 417 8530 / +1 202 508 6030
david.zetoony@bclplaw.com

Kevin Scott
Counsel, Technology & Commercial, Corporate
Chicago
T: +1 312 602 5074
kevin.scott@bclplaw.com

24/7 DATA BREACH HOTLINE:
0800 260 6669

If a breach occurs, preventing liability often means analysing facts, identifying legal obligations, and taking steps to prevent or mitigate harm within hours of becoming aware of the breach. That's why a lawyer from our global data privacy and security practice is on call for clients whenever and wherever a data breach occurs, 24 hours a day, 7 days a week.

24/7

a lawyer from our data privacy and security practice is on call for clients whenever and wherever a breach occurs

2000+

significant breaches or incidents handled worldwide by the firm

"Highlighted for its 'knowledgeable, pragmatic and informed advice', Bryan Cave Leighton Paisner LLP's data and cyber security team has been described as providing 'a platinum service'."

Legal 500, 2019

With over 1,400 lawyers in 32 offices across North America, Europe, the Middle East and Asia, Bryan Cave Leighton Paisner LLP is a fully integrated global law firm that provides clients with connected legal advice, wherever and whenever they need it. The firm is known for its relationship-driven, collaborative culture, diverse legal experience and industry-shaping innovation and offers clients one of the most active M&A, real estate, financial services, litigation and corporate risk practices in the world.

www.bclplaw.com

BRYAN CAVE LEIGHTON PAISNER BCLP