Playbook for a Forensic Data Investigation

By Simon Taylor and Matt Bedan[1]

October 2019

Against the current backdrop of both emerging external risk and heightened enforcement trends, any organization that interfaces with personal data must have a well thought-out plan for investigating and responding to potential data breaches and allegations of misuse. 100% security and compliance is not a practical objective. Properly scoped and executed forensic investigations coupled with robust and defensible compliance programs are an organization's best bet for reducing eventual fines, limiting regulatory attention, and restoring investor and consumer confidence in the event of an incident. FRA's Simon Taylor and Matt Bedan discuss the more significant mitigating factors to consider in advance when planning your company's incident response, and the key steps to incorporate into that process.

The Cybersecurity/Data Privacy Landscape

It is estimated that by 2020, 1.7MB of data will be created and stored, every second, for every person on the planet[2]. Personal data of all types is being captured, stored and put to commercial use at a staggeringly accelerating pace. Equally staggering, it seems, is the acceleration of financial and reputational risk associated with this data.

According to a recent Cybersecurity Ventures report, cybercrime is expected to cost global consumers over $6 trillion a year by 2021.[3] For perspective, this would be more financially damaging than all of the natural disasters on the planet combined in 2018, and would even exceed the value of the global illegal drug trade.[4] A recent report by IBM Research noted that data breaches in 2019 cost U.S. companies approximately $242 per lost record, with an average impact to the business of nearly $8.2 million.[5]

In response, governments across the globe are moving quickly to enact and enforce an increasingly complex regime of overlapping data protection requirements. Emblematic of this new landscape is the EU General Data Protection Regulation (GDPR), which represents a significant change in the protections afforded to personal data in the EU. The GDPR imposes strict penalties for non-compliance, with potential fines up to €20 million or 4 percent of the organization's worldwide revenue, whichever is higher. The penalties were deliberately set in order to attract C-suite attention to the issue

[1] Simon Taylor (staylor@forensicrisk.com), Partner, FRA (London), and Matt Bedan (mbedan@forensicrisk.com), Associate Director (Washington DC)
[2] IBM Marketing Cloud study, 2017.
[3] https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
[4] https://www.cpomagazine.com/cyber-security/11-eye-opening-cyber-security-statistics-for-2019/
[5] https://www.cshub.com/attacks/articles/quantifying-the-enterprise-cost-of-a-cyber-security-data-breach

and drive home the message that data security and privacy are no longer simply IT issues – they are enterprise risks.

In addition, although GDPR represents an effort to harmonize data privacy regulation generally, the enforcement landscape remains complex. For example, German data protection authorities recently announced a new model for how they will interpret and apply fines under GDPR. A recent case decided under this new model included a 24-page fine calculation, which applied a convoluted set of "daily rates" within certain "fine corridors", set against a subjective infringement score multiplier. Although it remains unclear how this methodology will be applied in practice, it brings the potential to skew more infractions toward GDPR's top tier of fines than was previously anticipated.

Finally, there is now the real risk of company executives becoming exposed to criminal charges and intense public scrutiny, such as in the case of the US Senate hearings for Facebook and the UK Parliamentary Select Committee inquiries into Cambridge Analytica. Beyond the prevalence of outsider threats, it is also important for organizations to understand the various forms of misuse of data that can lead to fines and reputational damage.

In the Cambridge Analytica example, Facebook collected data from users who provided 'informed consent' as well as the members of those users' networks who had not provided any form of consent. The wrongfully collected data was then used to attempt to influence voters in multiple countries around the world. Perhaps reflecting public outrage over this and similar incidents, the highest penalty tier of GDPR was reserved for misuse of data, not security breaches. Following the Cambridge Analytica scandal, Facebook was fined £500,000 by the ICO (the maximum fine available at that time). Had the misuse occurred after the enactment of the GDPR, the fine could have been as high as £1.4 billion.

Against this backdrop of both emerging external risk and heightened enforcement trends, any organization that interfaces with personal data must have a well thought out plan to investigate and respond to potential data breaches and allegations of misuse. Because 100% security and compliance is not a practical objective, properly scoped and executed incident investigations, coupled with a robust and defensible compliance programme, may be an organization's only opportunity to reduce fines, limit regulatory attention, and restore investor and consumer confidence in the event of an incident.

An adequate response to a data breach means looking far beyond the immediate technical issues of how the breach occurred or how the data was misused. As with any other situation involving allegations of corporate wrongdoing, it is important to establish a clear narrative through a comprehensive forensic investigation in order to mitigate damage, plan effective remediation, and meet the expectations of management, customers, the public, and not least, the regulators.

In this respect, the UK's Information Commissioner's Office (ICO) has provided instructive guidance regarding what factors should be taken into account when setting out an investigation plan. These factors provide insight into the elements used to assess a breach and justify fines, and are largely consistent with approaches laid out by other regulators (e.g. CMA, FRC, Bribery Act – UK, US sentencing guidelines). They include the following:

- the seriousness of the breach or potential breach (including, for example, whether any critical national infrastructure or service is involved);
- the gravity and duration of a breach or potential breach;

- the categories of personal data affected (including whether any special categories of personal data are involved) and the level of any privacy intrusion;
- the intentional or negligent character of the failure;
- any action taken by the controller or processor to mitigate the damage or distress suffered by data subjects;
- the number of individuals affected, the extent of any exposure to physical, financial or psychological harm, and, where it is an issue, the degree of intrusion into their privacy;
- whether the issue raises new or repeated issues or concerns that technological security measures are not protecting the personal data;
- any relevant previous failures by the controller or processor, including whether the organisation or individual involved is representative of a sector or group, raising the possibility of similar issues arising again across that group or sector if not addressed;
- whether, and to what extent, the company self-disclosed the incident to the ICO;
- the extent to which the organization has complied with previous enforcement or penalty notices;
- adherence to approved codes of conduct or certification mechanisms and the degree of co-operation with the Commissioner to remedy the failure and mitigate the possible adverse effects of the failure; and
- any other aggravating or mitigating factor applicable to the case, including financial benefits gained, or losses avoided, as a result of the failure (whether directly or indirectly).

By demonstrating that these factors have been carefully considered and controls have been put in place to attempt to mitigate the associated risks, an organization can not only demonstrate that it is striving to comply with the spirit of the legislation, but also provide mitigating factors as a basis for reducing penalties.

Whilst some of these factors require a technical analysis of the mechanics of the breach, others require a different approach that would be more closely aligned to the investigation of corporate wrongdoing. In our view, the factors that need to be established through a forensic investigation – such as mitigation measures, whether the breach was intentional or negligent, whether the breach was indicative of systemic failure, whether the organisation complied with recognized standards and whether the organisation has cooperated with the regulator – are likely to be the most significant in terms of the reduction in financial penalties.

The Forensic Investigation Playbook

The data forensics process can broadly be broken down into three steps (i) Detection and Analysis; (ii) Investigation, Containment, Mitigation; and (iii) Reporting, Notification and Post-Incident Review.

I. Detection and Analysis

The goal of the Detection and Analysis phase is to determine the scope and impact of the incident, and prioritize the investigative plan. Before declaring a data breach, conduct a thorough analysis of the type of data that has been impacted, being careful to consider terms that may have legal import (e.g. "breach" vs. "incident"), as well as compliance requirements

such as the Health Insurance Portability and Accountability Act (HIPAA) and GDPR. The severity of a data breach should also be documented as it becomes clear.

People, Process and Technology
Your employees should know how to report any type of suspected security incident, have several methods of reporting, and be incentivized to do so. Your organization should also have a comprehensive security program with policies, procedures, and processes which serve as guides on behaviour, specifically around how users interact with company data and systems in a secure fashion. Technology's role cannot be understated in this respect. All hosts on your network should be updated with the latest patches and secured using best practice configurations. Controls such as antivirus and appropriate firewall rules should be in place and configured correctly, along with appropriate authentication methods utilized.

Risk Management
Conducting risk assessments of your network, systems, and applications provides insight into the most important threats and vulnerabilities, and will help you identify the data breach risks in your organization. Data breach risks should be prioritized by criticality and impact, and reviewed for mitigation, transfer, or acceptance.

Scope/Impact
A data breach is one of the most significant events that can happen to an organization. Although news headlines tend to focus on the financial impacts, the impact to morale, productivity, and reputation can have lingering effects for years. It is important to be able to quickly determine the scope and impact of a data breach. This is a crucial point in the response process as actions will need to be prioritized based on the scope and impact of the breach.

Breach Impact Analysis
The impact of a data breach can be felt immediately, but there are additional direct, indirect and systemic costs to consider and document. Revenues may decline due to declining customer confidence. There may be a drop in productivity as resources are reallocated to deal with the breach. Reputational damage often results in a drop in share value. According to the Ponemon Institute's 2018 Cost of a Data Breach Study, the average cost of a data breach was $3.8 million and the average cost of a lost or stolen record was $148. It is important to consider the ongoing maintenance cost of dealing with a data breach.

Chain of Custody
During this phase, you'll want to establish a chain of custody as you gather and document evidence of a breach. The purpose is to serve as a paper trail for electronic evidence. The chain of custody should specify the data collected, sequence of control, transfer, and analysis along with the name of each person who handled the evidence, with the appropriate timestamps for collection or transfer. This is required to ensure the integrity and authenticity of the evidence and prevent contamination, which is paramount if the evidence is needed in court.

II. Investigation, Containment, Mitigation

A proper incident response would address the immediate need to close the existing gap(s) that allowed the data breach to occur, as well as determine the root cause, path and method of exploitation, and the extent of the breach.

The logical first step in determining the root cause of a data breach is typically to ensure a comprehensive understanding of the data that resides within the network. After a thorough mapping of the data and network has been confirmed, vulnerability scanning tools should be used to help identify weaknesses in the network. Audit and logging trails should also be reviewed for anomalous activity.

Audit findings and other similar recommendations should be requested (e.g., stemming from other controls reviews or risk assessments), along with the status of remediation of those findings. In many cases, another party may have already identified a weakness or gap in the control environment that is suspected to have failed.

Conduct network forensics to identify active malware in your environment, the source of attack, and attacker attribution. A host forensics examination is also critical to determine key information for future remediation and reporting, including:

- how many systems have been accessed or compromised
- what data may have been impacted or exfiltrated
- how long the breach has been active
- the initial attack vector, and
- persistence mechanisms in your environment

GDPR Impact on Investigations

Companies should additionally take note of the following GDPR issues in potential breach or misuse investigations:

- **Data governance** – This includes knowing what data is being considered, the jurisdiction where the data resides, any applicable data privacy regulations, and what clearance may be required.
- **Collection and preservation** – This involves ensuring that appropriate risk management tools have been engaged and steps have been taken to ensure compliance with data regulations and the jurisdictional source of any relevant data.
- **Training and escalation** – This would include up-to-date training regarding transfer protocols and jurisdictional data privacy regulations for all personnel involved in investigations and data transfers.
- **Data transfer strategy** – This is a specific strategy that takes into consideration the nature of the data, its origin, data privacy and other data-related constraints.
- **Jurisdictional and data privacy issues** – This includes the overall logistics of processing, hosting and reviewing the data.

III. Remediation, Reporting and Notification

Remediation

A well-designed remediation plan should clearly articulate the specific actions the company needs to take to address the identified issues. The plan should be pragmatic and risk-based, anticipating the cost benefit of the control and potential resourcing constraints. Once defined, the remediation plan needs to be tested. All internal control systems, including remediation plans, need to be monitored. Remedial measures, the status of their implementation and the process to test the effectiveness of implementation should be memorialized and tracked. There should also be a process in place to test the effectiveness of implementation before considering a remediation 'complete'.

Notification to Shareholders and the Public

Communication to external parties should occur after all the facts are known. It should be forward-focused on the improvements that have been implemented to address the previous deficiencies, and be shared in a timely manner. A report to the board should provide context to by answering the following questions:

- What was the root cause of the data breach?
- Were policies/procedures/tools in place to prevent the breach? If not, why not?
- If adequate policies/procedures/tools were in place, what went wrong?
- Which data was compromised?
- Were all necessary, legally required notifications provided?
- Have the underlying root causes of the breach been corrected?
- If an Incident Response Plan (IRP) was in place, did it function as intended?
- What were the lessons learned that can be applied in the future?

Post-Incident Review

The report should describe the incident in detail, including a summary of actions performed to address the data breach. It should additionally reference all information and assumptions relied upon to form the ultimate conclusions (e.g., deposition, transcripts, digital evidence items, etc.), and describe the process under which all evidence was acquired. The report can be used to inform future control enhancements and other preparation against data breaches, as well as serve as confirmation of the remediation for regulators.

Conclusions

The opportunities available for organisations arising out of the mass accumulation of data on human activity and behaviours are immense. Up until now, regulation of how data is collected, stored and used by companies has been at best 'light touch', as have been the penalties available for violations. These benign conditions allowed many companies to capitalize on freely available data and no effective regulation. It is clear that this environment has now irrevocably changed. Governments in all jurisdictions are giving regulators new powers and encouraging them to push these powers to the limits.

Organisations wishing to take advantage of the opportunities offered by technology and data need to develop compliant ways of handling and using data. Additionally, when (not if) things go wrong, whether as a result of data breaches or the misuse of data, companies should learn from the hard lessons in other regulated areas such as financial services, bribery, sanctions, and money laundering, to name but a

few. A full forensic investigation is essential to ensure reduction of financial penalties and reputational damage through cooperative engagement with regulators and an effective compliance remediation of the problem.

Forensic Risk Alliance

Audrey House

16-20 Ely Place

London EC1N 6SN

+44 (0)20 7831 9110