The Strategic Business Leader's Framework for Defensible Data Incident and Breach Response

FROM AD-HOC INCIDENT RESPONSE TO A DEFENSIBLE ORCHESTRATED BREACH MANAGEMENT PROCESS

exterro®

INTRODUCTION

Organizations significant and small have experienced privacy incidents and breaches in the last 10 years. From regulatory scrutiny and the public nature of breaches to the emerging private right of action supported by very vocal privacy advocacy groups, there is no denying that the incident and breach landscape has been visibly changing.

Regulators expect organizations to maintain logs of their incidents and demonstrate due diligence and the capability to address risks before a breach occurs. This expectation demands a different approach to incident and breach management and response, and signals to the market that it is no longer acceptable to deal with such events as a "one-off." Organizations operating in multiple jurisdictions or those planning expansions into global markets feel the amplified effect. The impact of a breach is no longer isolated but rather meaningful to the community at large (see Equifax, Marriott, etc.).

Public confidence and trust, especially in the time of a pandemic, are of paramount importance. To maintain a position of trust in the eyes of consumers, employees, customers and suppliers, organizations not only must comply with breach notification laws and contractual commitments but must also show that they are good stewards of stakeholder data. Everyone will admit that, even with a solid information security program, breaches will occur. But only those who can demonstrate a strategic and systematic approach to incident and breach response can manage the reputational fallout from it.

"Both regulatory enforcement actions and litigation risks force organizations to think of a strategic and defensible approach to responding to breaches, and no longer treat it as a one-time event."

"To maintain a position of trust in the eyes of consumers, employees, customers, and suppliers organizations must show that they are good stewards of stakeholder's data."

Setting The Stage

Today's breach landscape is unprecedently complex. Every organization is facing potential enforcement of many interconnected and overlapping laws in multiple jurisdictions. Requirements for what constitutes a privacy breach or legal privilege, or what thresholds regulators are setting to hold organizations to account vary significantly, yet there are no exceptions made based on the inability to keep the pace. Executing the basics, by simply discovering the incident or breach and going through the motions to investigate and make the correct decisions to notify the parties affected is no longer sufficient.

This paper identifies the **six key reasons** why incidents and breaches need to have your full immediate attention:

1 **BREACH SEVERITY HAS EVOLVED YET RESPONSE IS STILL AD-HOC**

2 **REGULATORY FINES HAVE INCREASED AND ARE GETTING BOARD ATTENTION**

3 **REGULATORS GENERALLY DO NOT OPT FOR SEVERE PUNISHMENTS WHEN THEY SEE DILIGENCE AND RESPONSIVENESS**

4 **PRIVATE RIGHT OF ACTION IS GAINING MORE TRACTION IN ADDITION TO PRIVACY, CYBERSECURITY AND COMPETITION LAWS**

5 **CLASS-ACTION LAWSUITS ARE CHANGING DUE TO THE EVOLVING INTERPRETATIONS OF HARM**

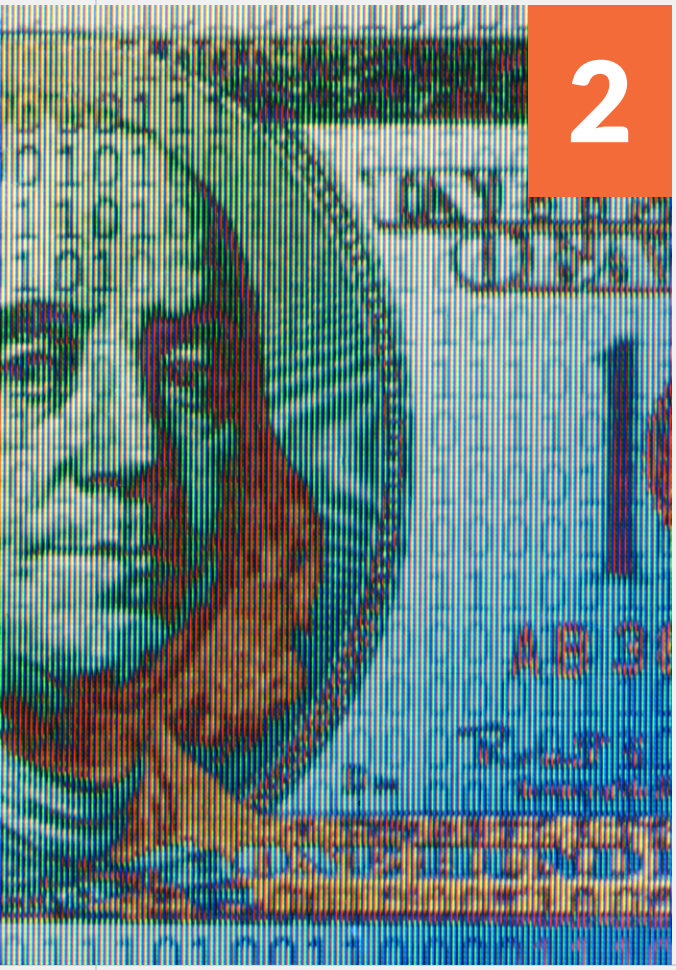
6 **PANDEMIC HAS PUT BREACH RESPONSE IN THE SPOTLIGHT**

1

Breach severity has evolved yet response is still ad-hoc

Breach is an area of privacy that tends to get a lot of attention from corporate management, consumers and regulators due to its often very public nature. What is surprising, given the frequency and impact of corporate incidents and breaches, is that organizations have not yet achieved a level of maturity in their response enabling them to present a documented, repeatable and defensible approach that demonstrates due diligence to stakeholders. Instead, most organizations are attempting to implement response and mitigation with portfolios of disjoint tools, manual processes and ad-hoc approaches.

Because of this approach, organizations are slow at identifying incidents that can turn into breaches, not realizing that the incidents themselves can lead to unwanted and negative attention. This is compounded by poor and incorrect communication across all levels of the organization, and when an event occurs the teams involved seem to be reinventing the wheel, therefore putting the organization at risk of liability and possibly litigation.



2

Regulatory fines have increased and are getting Board attention

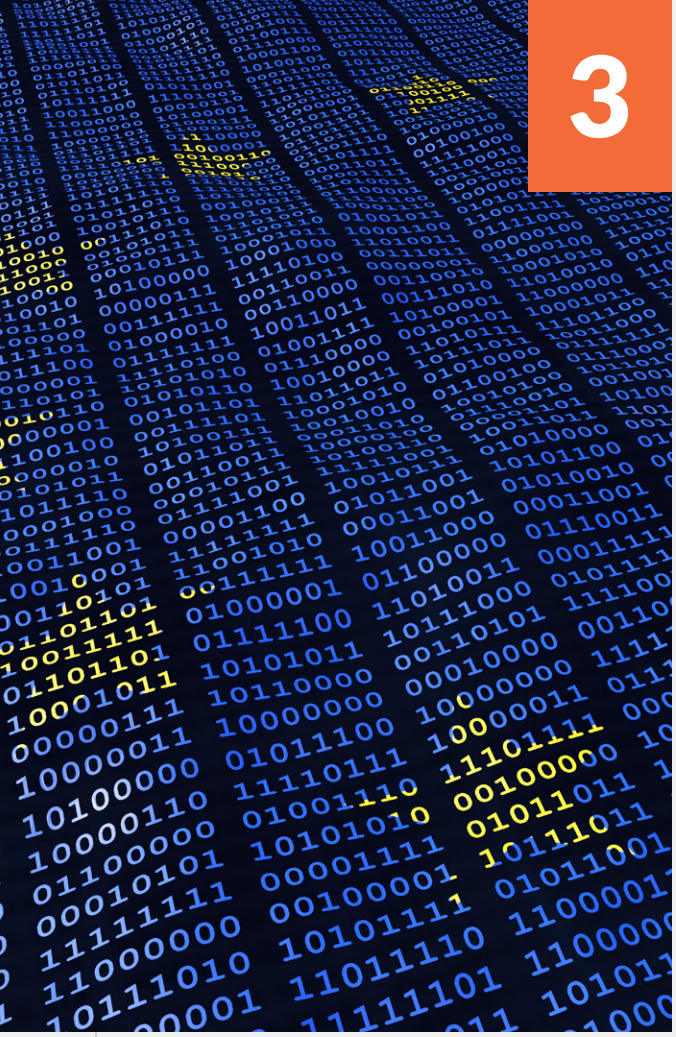
Fines for data breaches have increased in the past few years. More and more regulations stipulate fines as a proportion of the organizations' revenue. In addition to the privacy regulators, there are other forces at play, such as cybersecurity and competition law regulatory regimes which can also impose fines for the same breach. Yet executives tend to focus on the risk of fines instead of what the breach states about the organization's ability to manage regulatory data risk. So, do breaches get the right kind of attention or are they being treated with a band-aid?

90% of class-actions claim negligence or non-data breach claims as the primary cause[1]

Nearly half (48%) of consumers said they have stopped using services of an an organization post-breach. Nearly half of those consumers were impacted by the breaches[2]

[1] https://ccpa-info.com/wp-content/uploads/2019/08/2019_Litigation_Report.pdf

[2] https://info.rippleshot.com/blog/data-breach-customer-trust



3

Regulators generally do not opt for severe punishments when they see diligence and responsiveness

EU Regulators have demonstrated a readiness to hand out fines for breaches of security safeguards and data protection violations, but equally have shown restraint when organizations have been able to demonstrate a quick, thorough and well-documented response to data incidents.

This is an opportunity for Legal Counsel and Privacy Officers to use the amounts and the reasoning in the fines awarded as a means to get the attention of the Boards of Directors, to obtain their commitment for an appropriate response capability that is adequately resourced.

4

Private right of action is gaining more traction in addition to privacy, cybersecurity and competition laws

Perhaps more concerning than the threat of the regulatory enforcement actions, a new challenge has surfaced in the form of private right of action, whereby individuals can pursue claims. This right is championed by strong advocacy groups such as None of Your Business (NOYB), Privacy International, and European Center for Digital Rights (to name just a few), all of whom are very active and are leveraging representations actions in the EU, most notably against tech-giants like Google, Facebook and Apple. To make matters even more thorny, class proceedings are gaining momentum in the U.S. with the introduction of California Consumer Privacy Act and its very recent update in the California Privacy Rights Act, and with the proposed updates in the privacy legislation at provincial and federal levels in Canada.

5

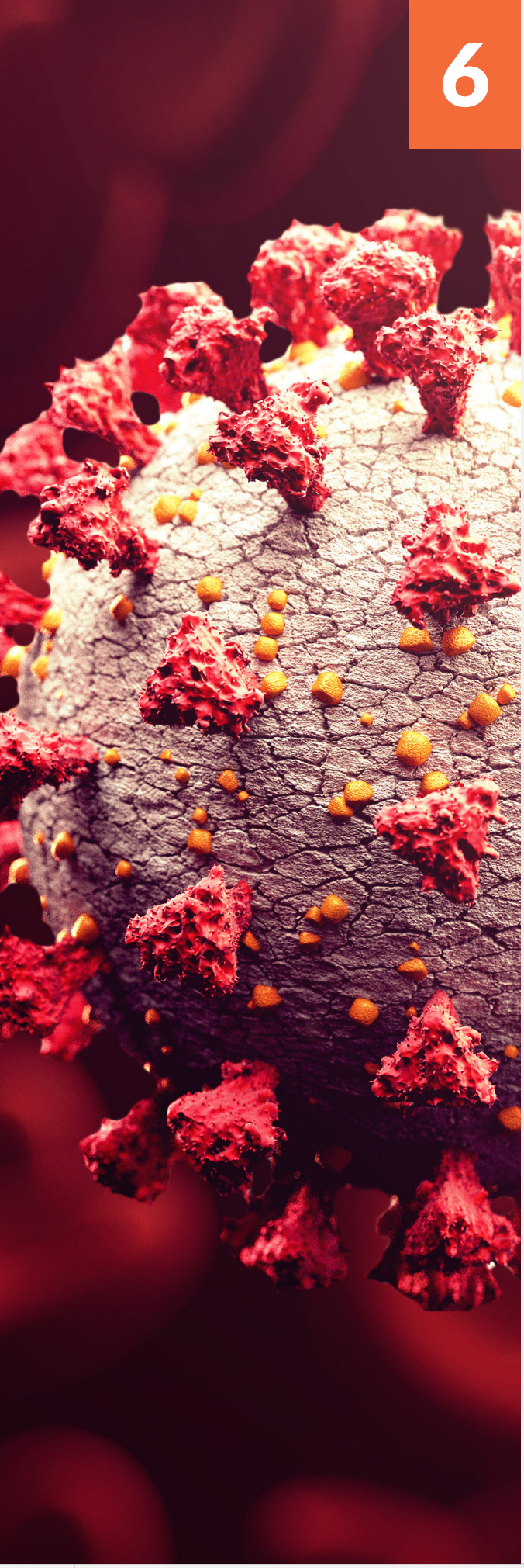
Class-action lawsuits are changing due to the evolving interpretations of harm

The U.S. has a long history of shareholder actions, and as data becomes increasingly recognized as an asset, class actions by shareholders that focus on management failures to address breaches will become increasingly common as the connection between breaches and share value are realized.

Another very important change is in what is considered a "harm". Traditionally, in the U.S., it has been difficult to launch class proceedings because harm has been considered from a financial aspect, which led to two problems for initiating class actions:

- **first, in many cases where the harm resulted in credit card fraud, banks and financial institutions would absorb the losses; and**
- **second, it was always very difficult to establish a causal link between a breach, and identity theft or other consequences.**

What has changed? First, statutorily defined damages such as in California, eliminate this hurdle. Second, "harm" itself is being broadened; in the EU and Canada, non-financial harms have always been a part of the law, such as embarrassment or humiliation; and the U.S. is moving to this broader notion of harm as well. The threshold for establishing a cause of action is therefore being reduced; this makes the recognition, analysis and remediation of breaches a critical activity for organizations dealing with data breaches. Given the consequences, the "project management" of breaches, is a key area of failure that will inevitably impact the assessment of the organization's Duty of Care to affected individuals — a duty that continues even during and after a breach.



6

Pandemic has put breach response in the spotlight

The recent **COVID-19** pandemic has in many ways fundamentally altered how organizations do business. With remote working becoming the norm, the number of attack surfaces that malicious actors can take advantage of has increased. Many employees (and consumers) do not have the sensibilities that can be imposed in nicely contained, structured work environments where cybersecurity experts have protected the systems. Organizations are learning how to do this, and companies are setting up mechanisms such as VPNs to secure the transmission of information from remote workers. Undoubtedly mistakes and failures of understanding will come to light over the next 12 to 24 months. Employees sometimes share computers with others in their household and may not have up-to-date antivirus and anti-malware technology. They will likely make mistakes in inadvertently sending data insecurely via email to the wrong parties. They will have unencrypted laptops and computers stolen and will print materials that are not stored in locked cabinets or shredded securely.

While organizations are adapting to the extended workplace, it is questionable whether their breach response capabilities have adapted to these new realities. We have already heard about some of the ways in which these security capabilities have been compromised by malicious actors (for instance, with ransomware attacks), but the larger portion of events have typically risen from human error. There is no reason to think that this is not continuing. Defensibility for the organization requires addressing this new reality and putting in place mechanisms to deal with it. If the pandemic has taught us anything, it is that we must anticipate and plan for adverse events.

Introducing the 6 guiding principles of the Strategic Incident and Breach Response Framework™ that will help organizations meet the demands of today's breach landscape.

Threats of litigation and stringent regulatory requirements demand an orchestrated response that is synchronized across your organization. The Strategic Incident and Breach Response Framework™ outlines the principles you must follow to create consistent, compliant, defensible protocols.

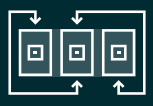
1 IT'S NOT ABOUT THE WHAT — IT IS ABOUT THE HOW

2 MANAGE PRIVACY BREACH RESPONSE LIKE A PROJECT — APPOINT A PM FROM THE LEGAL TEAM

3 PREPARE YOUR RESPONSE WITH "LEGAL PRIVILEGE" IN MIND

4 ESTABLISH STRONG COMMUNICATION GOVERNANCE

5 REMEDIATE AND APPLY LESSONS LEARNED TO IMPROVE



6 OPERATIONAL CONSIDERATIONS TO PREPARE A CONSISTENT DEFENSIBLE RESPONSE EVERY TIME

1

Organizations are expected to manage multiple legal, regulatory and compliance obligations and be able to demonstrate how they responded to an event that may affect potentially a large number of individuals in more than one jurisdiction. With a strong regulatory network, actions taken by an organization in one jurisdiction and the ability to demonstrate that those were appropriate, can set a good or bad precedent for the aftermath of a breach.

To strengthen the defensibility of your breach response:

- ❑ Document the legislative requirements that apply to your organizations
- ❑ Document the facts in the light of all the applicable legal obligations (consider law enforcement, works councils, etc.)
- ❑ Document the process by which the analysis of the event has led to conclusions of notice (or no notice)
- ❑ Document the timeframes for which respective parties are required to be given notice
- ❑ Retain evidence that notice has been given, with the requisite information and in the form required by regulators
- ❑ Record and manage the interactions with the parties who have been given notice

It's not about the what — it is about the how

Over the last five years serious data breaches have occurred with increasing frequency. The publicity surrounding the infamous Sony, Equifax and Capital One breaches compounded by the actions of privacy advocates, have shown that regulators and the public are holding organizations to a higher standard. The world is watching, comparing and judging especially when the impact is multinational.

"Incidents can no longer be managed as a one-off because they can be the signal of many issues that could turn into a much bigger problem"

Organizations face several additional challenges when law enforcement and other bodies are involved, which may impact their ability to meet the notifications timelines. This is due to the nature of the investigations and stakeholders involved. Additional consideration needs to be given to the 'no notice' scenario. In order to make a defensible decision not to give notice, enough information must be collected and documented in order to allow for that decision to be justified, on its face. This is an explicit obligation under some laws (such as Canada's mandatory breach reporting framework) but is arguably implied under any breach regime.

Additional complications arise from contractual obligations that may have stricter timelines and definitions than found in legislation. In many business-to-business contexts, the client organization ("data controller" in EU parlance) has the obligation to provide notice, within a limited period of time, and must rely on their service provider ("data processor") to be notified of events. Careful consideration must be given to the imputed knowledge of the client in this context. The EU regards its 72-hour period for notification to a regulator as a starting point when a data processor becomes aware of the event. Therefore, clients' contracts typically demand 24 or 48 hours notice (if not immediate) of an event in order to meet their own obligations.

When it comes to data breaches, organizations face the compounded pressures of warding off legal action, demonstrating due diligence internally, and complying with multiple breach notification laws. The only approach that puts businesses in a winning position is to get the entire breach management and response process planned, organized, and documented in advance, to execute it diligently, and then to continuously improve it.

A well-defined, repeatable process with set steps assigned to the appropriate stakeholders empowers the organization to meet the specific pressures and timelines of a breach response. The obvious benefits to implement such an approach is consistency and to reliably demonstrate that the organization was prepared. Accurate execution shows that training and resources were properly allocated as part of a plan and were not an afterthought.

2

Manage Privacy Breach Response like a Project — appoint a PM from the Legal Team

While a breach is initially investigated by IT and Cybersecurity, it is often lost on organizations that the real impact is of a legal nature.

It is often difficult to understand what in fact has happened early in the assessment process. Facts that might lead to the conclusion an event is a breach (or not), may be corrected or altered as the investigation proceeds. Event response will require the support of information technology to understand and diagnose what exactly has gone wrong when an event arises from information technology.

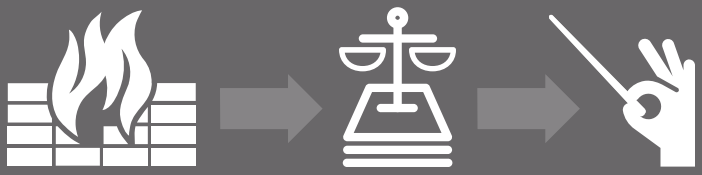
A breach is a conclusion of law; while responding to a data breach is a multidisciplinary, team sport, it is the Legal Department that must play the role of coach. It must plan the response, and then ensure that all the team players fulfill their roles. IT and cybersecurity cannot tell you how the affected data was being used, why it was collected in the first place, and what obligations or commitments were made (contractually or through notice) regarding its handling.

The Privacy Office and/or Legal Department will conclude whether an "event" or "incident" is actually a breach. It is essential that the internal incident response team members understand that this is the Legal Department or external Counsel's call, and refrain from using the term "breach" unless and until Legal has made this diagnosis.

To orchestrate cohesive response project management:

- ❑ Create a central project tracking mechanism early on, and the appropriate awareness with employees to report any event that contravenes your policies
- ❑ Allow the IT and cybersecurity teams to conduct their own investigation and follow their process to maintain chain of evidence custody and not interfere with forensics
- ❑ Appoint a Project Manager (PM) and give them the mandate to take charge and verify whether an event is an incident or a breach as not all incidents will become breaches and be subject to extensive breach reporting and notification laws
- ❑ Record events part of a log because many regulatory authorities expect it. The added advantage is that a log can inform senior management as to root causes and these can be early indicators into some misunderstood practices which can be corrected
- ❑ Guide employees through the process because employees will not know what incidents and breaches are, but they will likely know what they must do at the right time, if they are engaged and feel part of the process
- ❑ Verify that the employees involved in the incident response process record the steps they took to answer to the obligations, to understand, investigate and ultimately repair the cause of the breach. Such a track record is invaluable in the eyes of an auditor or regulator

Creating an incident and breach response process that involves the appropriate key stakeholders early-on leads to developing a culture. This creates a defensible strategy that is future and jurisdiction-proof.



Breach is a conclusion of the Law, therefore breach response needs to be strategically orchestrated by the General Counsel to demonstrate accountability and defensibility

3

To truly take advantage of legal privilege:

- ❑ Verify that business-as-usual records and activities are not included in the incident or breach response documentation, as they are not normally covered by privilege
- ❑ Exercise "accountability on demand": understand and document obligations (such as under GDPR and other regimes) to demonstrate the existence and effectiveness of your data privacy program and controls to the regulators
- ❑ Coordinate a response to limit liability. The goal is to document the appropriate response by jurisdiction. Keep in mind to not minimize the importance of cross jurisdictional activity and maintaining privilege
- ❑ Manage the scope of the entire project as opposed to disjointed efforts which also reduces risk
- ❑ Document situations where you must defer notice or decide to take a "no notice" approach
- ❑ Establish a secure and confidential pathway with Legal that preserves privilege and allows for segregated legal analysis and opinion from facts. Key to maintaining privilege is that it be **(1)** kept confidential and **(2)** that the legal counsel is the originator or recipient of the communication
- ❑ Document a complete, well thought-out and integrated response to include situations like law enforcement or other legal confidentiality restrictions that make it more complex) etc. that make it more complex
- ❑ Integrate processes to produce information with other legal information response processes and document these engagements and the directions as well as maintain certain facts and conversations under legal privilege
- ❑ Find a communication platform that allows the segregation of the factual underpinnings of the event from the conclusions and advice reached by counsel, in order to avoid compromised confidentiality of conversation or having to release information under subpoena, which may happen when using corporate messaging tools, word processing or spreadsheet documents

Leading incident and breach response with legal privilege in mind has never been more important. An organization may experience an incident or a breach that can affect other external stakeholders and their response may be delayed. How well these decisions are orchestrated, protected and justified, can make the difference between a defensible response that benefits from legal privilege and unwanted complications.

Prepare your response with "legal privilege" in mind

Ultimately, the goal of any incident and breach management system is to coordinate a response that contains the damage, and limits the organization's legal liability. To do this, it is important that the response process, including all the steps, information, and decisions, be regarded as potential evidence in a lawsuit. This means that they must be gathered in a way that will preserve legal privilege over them. While the specific requirements to maintain privilege will vary in different jurisdictions, it is important to design your breach response process such that privilege is maintained. These observations can only be at a high level and advice from your own counsel should be sought to structure your use of breach response to effectively leverage privilege.

A key area to be cognizant of is the reason that might prevent one from providing notice or deferring it. In some cases, law enforcement may be engaged as a result of the event, such as where it arises from malicious third parties, or from a rogue insider. This may cause your organization to have to defer notifications in order to avoid compromising an investigation and it is important to understand how to address this.

One should note that not everything can be protected by privilege. Typically, privilege protects legal advice (attorney or solicitor-and-client privilege) or advice given in the context of anticipated or pending litigation (litigation privilege).

It is not surprising that some organizations will go as far as having their outside counsel license their incident and breach response software instance in order to preserve privilege and support the maintenance of privilege in the diverse operational jurisdictions. This will also help to support communications with third parties and experts, who must also be typically brought in to help preserve privilege.

"In an increasing number of jurisdictions regulators are demanding to see evidence of a data privacy program, and holding companies accountable for its rigor — accountability on demand"

4

Establish strong communication governance

Poor and disjointed, immature processes can instigate rumour-mongering and labelling an "event" as a "breach" prematurely, and can negatively impact the organization's liability and reputation.

Having a defined process and technology which encapsulates specific incident or breach related communications also serves the purpose of supporting your legal team in their efforts to preserve certain aspects of the breach as legally privileged.

An important consideration for a breach response process is the need-to-know and the ability to segregate information so it only reaches the appropriate stakeholders. If you consider a breach that involves multiple jurisdictions, this aspect of the process becomes even more important. It is very possible that additional information is required in a certain jurisdiction and the timeline is significantly shorter. By having a centralized system, stakeholders can leverage information from other jurisdictions with advice from the legal team and meet the timelines.

The opposite of this is not relying on a centralized system and process, including communication but instead manually reviewing incidents, correlating information across continents or state lines, while feeling the pressure of regulator or other stakeholder reporting requirements and timelines with an underlined, increased probability of potential manual errors and omissions.

To maintain control of communications:

- ❑ Use a separate communication channel and be aware that privileged information can be communicated by accident to the wrong stakeholders, possibly creating additional breaches of confidentiality
- ❑ Include critical internal and/or external stakeholders in the conversation with the clarity of what is communicated to whom and by whom, and who needs to be in that conversation
- ❑ Involve third parties in a timely manner but be careful to not include them in any company confidential and privileged communications
- ❑ Maintain a role-based chart of all the stakeholders to ensure these and critical information were not omitted from the process
- ❑ Make every effort to obtain all the pertinent information in a timely manner so that decisions (such as a "no notice") are weighed and consequences are documented and understood

Communications from the moment an incident is discovered and declared a breach, through to resolution and closure, must be well controlled and orchestrated. Knowing what communication goes to what audience, the timing, as well as who needs to approve them is of paramount importance. A strong legal leader is required to be in charge of the entire communication process to provide need-to-know oversight and limit liability.

5

Remediate and apply lessons learned to improve

Response has become a more sophisticated area for defensible breach handling than in the past. Using the time-honored practice of sending notices by mail is not always desirable in a breach, and doing so doesn't necessarily achieve defensibility, since that could vary with the potential harms associated with the event.

Key of course is to do what the laws — and applicable contracts — tell you. Understanding the applicable rules may be easier for organizations which operate in a few jurisdictions. However, multinationals must rely on legal databases which detail the obligations and typically include notice to applicable regulators, notice to individuals and notice to third parties, who may be relevant to help prevent harm to individuals or otherwise mitigate risks.

› After the Event: Defensible Breach Response Doesn't End with Notification and Remediation

In the relief and exhaustion that follows a stressful event such as a major data breach, many organizations want to return to "business as normal" as quickly as possible. However, determining the root cause, documenting and incorporating lessons learned into the response process, and evaluating the process itself and making any changes if deficiencies are found are vital. These steps are essential to defensibility. Most jurisdictions, particularly in the U.S., require that notifications to individuals highlight what has been done to prevent the recurrence of the event. Apart from these requirements, lessons learned is an area to which regulators pay particular attention. It is also fundamental to building a learning organization. Like any business process, managing incident response will need to change as the business, environment, laws and regulations change. If this change is built-in, it will not be disruptive.

The post breach fatigue opens up another area for potential risk that is addressed by defensible breach management. Data events, particularly those resulting in breaches of personal information, create reputational damage and legal risk for the organization. The costs, fines, and notice obligations attract the attention of shareholders, and plaintiff's counsel, who seek damages based on the failure of management of the organization to ensure that a critical asset — personal data — is preserved and protected.

"What every organization must be able to demonstrate is that they learned from the event, and have responded reasonably"

To prevent mis-steps or incident/ breach re-occurrences:

- ❑ Establish the organization's methodology to document and then record the organization's understanding of the root cause and lessons learned
- ❑ Maintain an action plan with owners and ensure that participants in the event follow up and act on the lessons learned
- ❑ Document that the organization is constantly improving the response process and it will not repeat the same mistakes
- ❑ Conduct training, run simulations of response process and include new participants that may prove critical to the incident or breach response
- ❑ Provide reports to senior management and propose ways to actively involve them in the breach response simulations, so they can become part of the due care and due diligence over personal data which needs to be continuously safeguarded

Regulators understand that organizations make mistakes but they expect continuous learning so that the same mistake or a side-step does not lead to the same or larger consequences. Demonstrating appropriate responses does not stop once the legal obligations are met. Negative or adverse data events will impact every business large and small, and often these cannot be anticipated or prevented easily. Continuous improvement is beneficial for organizations because it allows for changes to be absorbed and integrated with the business activities without significant disruptions or costly shifts in the ways of working.

6

To ensure consistency of breach response in action:

- ❑ Train all involved stakeholders to not disclose assessments, analyses, or forensics reports to other third parties, either purposely or accidentally
- ❑ Use secure and confidential communications portals outside the common corporate channels in order to preserve the confidentiality of incident or breach related information
- ❑ Plan for the eventuality that documents may still be disclosed if privilege is waived or if the opposing party is able to prove that they need the information
- ❑ Maintain a forensically complete documentation and evidence preservation model for the breach investigation process, as you may be called to provide any document even under privilege as this may be waved
- ❑ Continuously document lessons learned to ensure that they are not lost or skewed significantly due to lack of input from stakeholders or unavailable information (due to multiple decentralized repositories with limiting access controls) preventing cross-jurisdictional collaboration
- ❑ Track "near misses" and how well understood or not they are by key stakeholders, which then can become evidence of neglect should the organization have a repeat situation instead of knowing how to avoid it
- ❑ Consider cultural differences in expectations, response and danger of "exclusion" by omission

From multi-jurisdictional nuanced effect of regulations, to cultural differences and lessons learned from one incident to the next, privacy leaders need to provide auditable and defensible evidence to put in front of litigators and regulators: to show due diligence, robust decision making, and meeting notification requirements and timelines. Evidence shows to a regulator there is a systemic approach and therefore a breach is more likely to be seen as an exception rather than a systemic problem.

Operational considerations to prepare a consistent defensible response every time

Breach response requires collaboration between IT/cybersecurity, legal/privacy, human resources, and critically, business people. This group may include sales, marketing, operations, public relations/communications, and other departments depending on the nature of the information that was affected. GDPR, CCPA and a host of new regulations demand an understanding of how the information was being used, with whom it was being shared, and the business purposes.

Breach handling requires good project management and collaboration between departments, and a shared responsibility in managing a data event.

IT and Cybersecurity teams have their unique role and importance, including forensic investigation, preserving chain of custody and involving cyber-investigators and insurers to demonstrate due diligence in understanding what caused the incident or breach and how it can be prevented from occurring in the future.

It is important to clarify and educate stakeholders of their roles in incident response and how to preserve confidentiality of communications. To do so manually requires a lot of resources time and possibly (for multinational organizations) a dedicated full-time resource to document, train, collect feedback and lead the process while still being subject to errors and omissions. What is of utmost importance and not emphasised enough is avoiding activities that may jeopardize the position of the organization and inadvertently lose protection of legal privilege.

Multi-jurisdictional breaches present some additional challenges to the ones discussed in the third principle [Prepare your response with "legal privilege" in mind]. Notification requirements and periods can and do differ, and what is a breach in one jurisdiction, may not be in another. Experience has shown that individuals do not like being treated differently based on where they happen to live; it is difficult to explain to employees, for instance, why their colleagues received notice of a breach while they did not. Treating consumers or employees equally may mean giving notice (and performing associated remediations) even where not legally required. Also, consider the impact of giving notice to one regulator, and having another find out about the event through the news. In some instances, it may be desirable to provide formal or informal notice in order to forestall concerns or investigation.

Responses also have to be tailored for cultural as well as legal differences. Breaches disclosing financial information such as salary, while embarrassing, may not by themselves trigger notification obligations in some jurisdictions; yet in some countries, may create a risk of kidnapping. Cultural differences may also dictate different responses; apologies are sometimes expected and will go a long way to resolving a data event. In North American organizations there is recognized reluctance to admit fault as it may become the basis of legal action.

Only an orchestrated incident response process and a centralized system can consolidate the effort, anticipate the risks of miscommunication and streamline the unfolding of a stressful event in an organized, consistent, confidentiality preserving and compliant manner.

It is clear that organizations' leaders must commit to continuous improvement in handling data breaches. You cannot improve that which you do not measure. However, what can you measure if you have sporadic documentation in disparate repositories that you cannot correlate?

CONCLUSION

Every organization will have data events that will challenge consumers and employees, and the privacy leaders need to provide auditable and defensible evidence to put in front of litigators and regulators to show due diligence, robust decision making, and meeting notification requirements and timelines. Evidence shows to a regulator there is a systemic approach and therefore a breach is more likely to be seen as an exception rather than systemic problem. Enterprises will attract, at some point, the attention of a regulator, a data protection commissioner, or a class action lawyer and if they are planning to expand, they will likely have to undergo reviews from external auditors.

How well your organization responds to the task of analyzing and responding to an event will serve to mitigate the risks associated with these events, preserve reputation and trust, minimize costs to the organization and maximize its value in the eyes of stakeholders.

Incident management and response relies on the defensibility of process from engaging their employees early on to reporting incidents the organization can learn from, effectively becoming an awareness and education resource that helps reduce future occurrences while continuously improving the breach response process.

To orchestrate a strong defensible response process, organizations need their own automated and encrypted incident and breach management system, configurable workflows and defined tasks for stakeholders, where the evidence of defensibility is generated by the activities associated with the response to a data event. The same centralized solution should contain libraries of extensive global breach notification requirements to support the legal team with intelligence-based triggers for obligations under multiple breach laws and contractual obligations, and encrypted channels of communications to preserve confidentiality.

Authorship:

Amalia Barthel,
CIPM, CIPT, CDPSE

Constantine Karbaliotis,
CIPP/C, CIPE, CIPM, CIPT, CDPSE

Daniel Sholler,
Product Marketing Manager, Exterro