CYBER INCIDENT RESPONSE:

PERSPECTIVES FROM
INSIDE THE RISK ECOSYSTEM

Featuring insights from:

Global insurer AXA XL | International law firms BakerHostetler and Osborne Clarke | Ransomware specialist Coveware | S-RM senior advisor Giles Cockerill, CBE | S-RM's ethical hacking team, cyber security consultants and incident responders
MOUNTING ACCOUNTABILITY

The cybersecurity regulatory and legal landscape has grown in complexity, attracting increased scrutiny from both governmental agencies and the public over recent years. Part of this complexity is due to the globalisation of liabilities. Organisations today must comply with data privacy and data usage regulations across multiple regions, covering not only their own physical locations or jurisdictions of incorporation, but also those of the individuals and businesses they serve. Similarly, the list of potential claimants against businesses who fail to protect their data is a long one. It includes:

- Regulatory bodies with the power to impose significant fines;
- Consumers or employees whose personally identifiable and/or financial information has been exposed;
- Shareholder groups who may sue a company in response to a drop in share price, or even hold management personally responsible for failing to meet their fiduciary duties;
- Financial institutions, who may seek reparations from the targeted company if they have had to compensate customers for fraudulent transactions on the back of a data breach; and,
- Companies doing business with a breached entity, where the breach causes disruptions in another company’s business operations or results in the loss of information owned by another company.

Against this backdrop, the fact that law firms globally now form a core part of an organisation’s cybersecurity planning and incident response frameworks is unsurprising.

THE RIGHT REPRESENTATIVE

S-RM spoke with Partners from two leading law firms in the US and UK to get their perspectives on the role of legal counsel in cyber incident response. A number of core tenets emerge:

Experience is key. When it comes to a cyber incident, a swift response is important, and your legal counsel should not be learning on the job. The more cases your legal representative has worked on, the more likely they are to have already dealt with an incident such as the one you are facing now. This means they can apply cumulative learnings quickly to an often highly charged and dynamic situation.

Strong coordination and communication. Your legal counsel is likely to be liaising with and often directing not only key internal stakeholders, from senior management through to IT and HR, but also a range of third parties. These include forensics teams, insurers, PR firms and even the authorities and regulatory bodies.

There from start to finish. When it comes to incident response your legal counsel will play a central role throughout the crisis. Your lawyer will likely be one of your first - if not your first - call at the point of incident detection, and they will guide you through the implementation of mitigation measures that minimise the prospect of subsequent legal action, and support you through any fallout in the aftermath of an attack.
TWO PERSPECTIVES

The Q&A below covers the role of legal counsel in a cyber incident from the US and UK perspectives in greater detail, focusing on how your legal representative forms a part of your broader incident response team.

Theodore J. Kobus III, BakerHostetler (US)

Ted Kobus stands at the forefront of cyber protection. He has earned authority in the areas of privacy, data security and cyber security, leading clients to entrust him with more than 5,000 data breach responses.

Businesses, government and other organisations turn to Ted for sound advice on compliance, developing response strategies, breaches implicating domestic and international laws, and defence of both class action litigation and regulatory actions. Ted is the firmwide chair of BakerHostetler’s Digital Assets and Data Management Group and a member of the firm’s Policy Committee.

Charlie Wedin, Partner, Osborne Clarke (UK)

Charlie is a partner in Osborne Clarke’s commercial disputes team, and handles large, complex, commercial disputes and investigations, normally with a cross-border element. He has particular expertise in resolving disputes concerning technology and the digital / online world.

He is an expert on contentious privacy and cyber security issues and advises businesses on investigations, regulatory issues, litigation, and risk and reputation management strategy, in the immediate (and longer-term) aftermath of cyber security incidents, including major cross border data security breaches.
In the US, the role of the law firm is often referred to as “outside counsel,” “privacy counsel” or “breach coach.” No matter how you refer to the outside attorneys assisting the company during a data security incident or cyber event, the role is (or should be) essentially the same.

The advice we provide sometimes goes beyond what we traditionally view as “legal advice” and relates to advice around generally managing the crisis. Accordingly, we help manage the retention and direction of all vendors often involved in the response efforts: forensics, public relations/crisis communications, information systems restoration, notification and call centre, and credit monitoring. We also walk through the response journey with the various stakeholders at the company involved in the response, and do not focus solely on the legal aspects. Distilling the findings of forensics to something that is understandable so that the company can weigh the risk to its business reputation and operations is just one example of the critical role privacy counsel fills.

Application of privilege protection in the US focuses on the legal advice being provided. We take great care to document that any information being reviewed and analysed is being done so for the purpose of providing legal advice to the client. In many instances, the forensics investigation can be cloaked under privilege. Many courts, however, are narrowing the scope of the privilege. It is therefore critical that privacy counsel make clear how the information is being used to give legal advice, i.e., regulatory scrutiny, application of data breach notification laws, etc. The courts are moving towards not protecting advice that is more around the company’s operations, and not actual legal advice.

Cyber breaches can lead to huge financial loss and reputational exposure. The involvement of the right legal team can help minimise that loss and exposure significantly.

First, many cyber breaches will trigger regulatory obligations (whether under the GDPR, if personal data is involved, or through sector and industry specific regulators). Where regulatory obligations may have been breached, there is a risk for enormous regulatory fines (e.g. unlimited fines for FCA-regulated entities, or up to the higher of 4% of global worldwide turnover or EUR 20,000,000 for breach of the GDPR). Law firms can advise on regulatory obligations (including as to any applicable notification requirements), as well as help to structure the breach response in a way that minimises the chance of regulatory enforcement action (including by making appropriate representations to the relevant regulator).

Secondly, there is the risk that follow-on claims may be brought against the affected entity including, where third parties (such as employees, customers or data subjects) are affected by the cyber breach, the potential for group legal claims for damages for “distress”. Law firms can help to navigate the incident response in a way which minimises the risk of such claims materialising and, if they do materialise, they will be able to assist in the robust defence of such claims before they gain momentum.

Finally, the role of a law firm in project managing and overseeing incident response cannot be underestimated. In particular, law firms can also help advise on privilege, and set up privilege structures which may help protect the documents created in the aftermath of a breach (such that those documents do not need to be shared with regulators or potential claimants).

“Law firms can advise on regulatory obligations as well as help to structure the breach response in a way that minimises the chance of regulatory enforcement action”
WHAT DOES THE RELATIONSHIP BETWEEN THE TARGET OF A CYBER ATTACK AND THEIR LEGAL COUNSEL LOOK LIKE DURING AN ATTACK?

Privacy counsel should bring the experience of helping clients manage thousands of data security incidents. Our team has managed more than 5,000 incidents and has worked on some of the largest incidents that ever occurred.

We also work on a number of incidents that hit small and medium-sized companies, too. The compromise intelligence that we bring to the client during incident response helps them weigh the risks at each decision point so that they can make the decision that is right for their company.

Lawyers with expertise in crisis management tend to provide a measured and steadying presence during a tumultuous response process. More often than not, the lawyers will have dealt with the same or similar issues previously (including both the legal and practical considerations involved in any given issue). The right lawyers can often be used to as a sounding board or filter during the decision making process, and are approached for advice on whether a proposed course of action might bring about unnecessary risk (or unintended consequences).

Lawyers will often also fulfil a project management or “quarterback” role during the response process, as the typical ordered skillset of a lawyer lends itself to distilling large quantities of information and evidence into actionable points even in times of intense pressure.

WHAT RELATIONSHIPS AND STAKEHOLDER MANAGEMENT PROCESSES MATTER MOST WHEN IT COMES TO CYBER INCIDENT RESPONSE?

The answer to that question really depends on the type of company involved in the data security incident. Incident response, and incident response preparation, is an enterprise issue, and key stakeholders should have a seat at the table, including legal, human resources, compliance, privacy, information security (IS), information technology (IT), customer/patient advocacy, public relations, finance and physical security. Not everyone needs to participate at the beginning of every incident – for example, an incident may be related to HR only. Or it could be a paper incident, and IT does not need to be involved. If the incident expands, additional stakeholders can be added on an as-needed basis.

The first question to ask is who should lead the response. The incident response team leader should be someone who has strong organisational skills and good people management skills and is respected in the company. The title of the person matters less than the skill set of the person. The incident response team lead is going to need to organise calls and lead the agenda. The person is also going to need to reach out to stakeholders outside the incident response team to get tasks completed. The one caveat to all of this comes into play if the company is a highly regulated business. With a highly regulated business, we recommend that the legal representative partner with the team lead to ensure that regulatory requirements or triggers are considered.

Following the response, the team does not need to be as robust, and only members addressing the closing issues need to participate. Depending on the resulting media response and the extent of the clean-up efforts, legal, IS, IT, finance, privacy and compliance may continue to convene for another 30 days to three months.
In the run-up to an incident it is important that a potential target has firmly got to grips with: the data it holds; the way in which it holds it; and its incident response (and business continuity) processes. On the incident-readiness side, entities need to know who their points of contact will be to convene a crisis management team when an incident hits. This includes knowing which IT forensics you would call for support, whether you have insurance and the notification requirements to meet that policy; the lawyers you would call; and the public relations support you may draw upon. Knowing how to effectively escalate and address an issue with the right group of decision-makers is a large part of an effective response.

During and after the incident, effective communication is absolutely key. Appropriately spaced and planned crisis management team calls or meetings can ensure that the various stakeholders remain abreast of the ongoing issues to ensure that the various proposed elements to the response do not cut across each other. Some of the immediate response activities can be driven by legal requirements, for example the 72 hour window for an expected notification to the ICO in the event of a personal data breach. Other activities have knock-on effects: where an entity is legally obliged to notify affected customers, it is important to properly coordinate the public messaging campaign that will follow, perhaps including website FAQs or a call-centre to assist with the management of queries. Each of these will need to be reviewed from a legal perspective to avoid statements that unintentionally attract liability.

In addition to liaising with the affected entity, the legal team will co-ordinate communications with the IT / cyber forensics team, the public relations advisors (whether internal or external), customers and regulators. One of the key tenets of an effective response is to ensure joined-up and consistent messaging and communications, as well as to avoid responses or communications which are factually incorrect, misleading, or increase liability. That’s one of the reasons why the legal team will often act as a central hub for messaging.

“We deal with regulators and law enforcement frequently. We also know what information is most valuable to them and ways to get them the information they need without hurting privilege or work product arguments.”
Clients often panic after the news of the event is released, and providing them with the information around why certain decisions were made and how other clients have fared when they approached the media a certain way ends up being tremendously helpful. Some companies believe the more information they provide, the better the outcome. The reality is that we do not always have all of the answers to the questions being asked – and that’s ok.

We need to focus on answering the four basic questions that everyone wants answered: what happened, how did it happen, what are you doing to protect me, and what are you doing to stop this from happening in the future.

In the longer-term aftermath of the breach, the role of the legal representative will usually ease from hands-on crisis management to a more traditional advisory role. Once “business as usual” is achieved following the event, the focus on the legal side will turn to how to manage any ongoing investigations (including by any notified regulators) and liaison with third parties (including any claims against responsible third parties or claims by affected third parties).

Finally, legal advice may also be necessary to ensure that any necessary revisions to policies and procedures take place (by way of “lessons learned” from the cyber breach).