**Litigators and Privacy: The Last People You Want to See, or the First?**

In their consideration of possible worst-case cyber attack scenarios, organizations often focus on the various types of attacks and their relative severity. But, the worst-case scenario is not the breach, it's the reputational damage, regulatory enforcement action, the business interruption, and the inevitable litigation that follows a poorly handled breach from an unprepared organization. Given this reality, it is important to adjust planning assumptions and response scenarios to focus on addressing these drivers of post-breach exposure.

**By Michael Bahar, Sarah Paul, Matt Gatewood and Andrew Weiner**

It is hardly news that cyber incidents are front of mind for companies. Whether costly data thefts, pernicious data manipulation attacks, or crippling ransomware or disruptive denial of service attacks, cyberattacks are trending toward greater frequency, severity and sophistication. Geopolitical tensions have further increased the risk. In fact, the New York State Department of Financial Services recently warned its regulated entities to be alert for an increased risk of malicious cyber activity directed at United States industries and government agencies by highly cyber-capable Iranian actors and proxies. The New York Times reports a 41% increase in 2019 in the number of files hacked in ransomware attacks, and notes that according to American authorities, several of these attackers have operated with the protection of their governments and have helped their governments by passing along hacked files.

When it comes to cybersecurity risks and breaches, organizations know they should plan for the worst, and hope for the best. In their consideration of possible worst-case scenarios, however, organizations often focus on the various types of attacks and their relative severity. In other words, they focus on the day of, not the day after.

But, the worst-case scenario is not the breach, as bad as a breach can be for the organization and its affected associates. In fact, the worst-case scenario is the reputational damage, regulatory enforcement action, the business interruption, and the inevitable litigation that follows a poorly handled breach from an unprepared organization. Given this reality, it is important to adjust planning assumptions and response scenarios to focus on addressing these drivers of post-breach exposure.

**Failure to Plan Is Planning to Fail**

The military knows that failure to plan is planning to fail. Companies should take the same approach when it comes to cyber.

First, companies should survey the regulatory landscape across all jurisdictions in which they do business or maintain consumer data. A cyberattack in New York is likely also to be felt in London and Singapore, for example, and each jurisdiction will have its own requirements, including rules for the timing of regulatory notifications. The plan should call for a coordinated response across jurisdictions and it should...
account for a “best fit line” or “high water mark” approach. No regulator wants to read about a breach affecting their citizens in the papers.

Similarly, jurisdictions will be subject to different rules of legal privilege and how that privilege could be waived if the breach response is not handled in a certain manner. If a breach originates in Paris, for example, lawyers involved have to understand the privilege implications for, say, calling in a cyber forensics company through the IT department rather than outside counsel.

Second, while planning is critical, companies need to know what military planners also know: no plan survives contact with the enemy. Cyber-incident response plans involve facing off against a live enemy, one who will adjust to your every move and may even know your plan (or make a pretty good guess) before they launch the attack. What is therefore important in planning is that everyone knows who will manage the response, what role each member or department will play, what third parties will need to be involved, etc. Because of the worst-case scenario involving litigation and regulatory enforcement actions, the plans should involve a central role for the lawyer. Without legal involvement — especially before a notification or public statement goes out the door—a bad day can become a tragic year.

Third, when it comes to a cyber-attack, planning for the worst should incorporate the low tech. Companies that maintain their incident response plan solely on a share drive are tempting fate and savvy adversaries, and also risk falling below “reasonableness” standards. Similarly, if your plan assumes that all response team members will be at their desks when the incident happens, your plan is inevitably flawed. Instead, wallet cards with key desk, mobile and even landline numbers are critical. Similarly, printing the plan out and keeping copies securely in offices and at the homes of those who will be responding is another low-tech, low-cost, and high-value precaution.

**Beware of the Apology**

External communications cannot be the sole province of marketing, or even of external communication companies. Any external statements — including to Boards or third parties — need a legal review to ensure that what may work in the moment doesn’t haunt the company for years in litigation. There is an inherent tension between the imperatives to disclose the basic facts quickly to control the narrative and maintain disciplined, informed communications. However, early reports are rarely accurate, and a rushed, overconfident response risks accusations of misstatements as well as loss of control over the narrative. Further, apologizing can be seen as an admission. It is a delicate balance, and sometimes a decision to prioritize the short term over the long term is wise, but the plan should ensure that those choices are deliberate.

Communications and other reputational considerations are especially important for larger companies that could be subject to shareholder derivative suits to recover for any losses in stock value. In recent years, Boards have faced shareholder litigation following cyber incidents based on alleged insufficient precautions to guard against attacks and inadequate management during the incident. Beyond any statements made by a company, it is crucial to also manage how employees publicly communicate about the incident, especially on social media. A carefully crafted response can be upended by a stray tweet by an employee that suggests a narrative contradictory to the company’s. Being proactive...
and having clear public statement policies in advance is important.

**Hold Your Fire**

In the heat of battle, strategic patience is critical. However, passions will get enflamed, and fatigue will play a role. It is important to recognize when these tendencies are likely to happen and to make sure a plan is in place to control them. For example, there may be an impulse to hack the hackers. A CEO may instruct his response team to “hack back,” but under many laws, that is illegal. It also is likely ineffective, since hackers tend to hack after taking over an innocent person’s computers. Hacking back against a highly sophisticated hacker may also make your hack even worse.

Another impulse is to pay the hackers during a ransomware attack. In 2019 alone, thousands of businesses were subject to a ransomware attack in which their data was encrypted and held hostage. In many cases, businesses are unable to access any of their data unless a ransom is paid to the attackers. A company may calculate that paying a ransom will result in less injury than an ongoing interruption, but ransom payment is fraught with difficulty and risk. First, there are no guarantees that paying the ransom will “unlock” your data. There are tax implications that must be accounted for regarding the payment. Further, payments may put a company at risk of both civil and criminal liability. Depending on the location and nationality of the hackers, there may be US sanctions that are implicated in making any payment. Similarly, ransom payments may violate anti-money laundering legislation. In advance of the prospect of making a ransom payment, it is important to consider these risks and have a plan in place to address them.

**After Action Reviews**

After a cyberattack, conducting an after action review or internal investigation of the circumstances is an important step to understand the incident, report to stakeholders, and identify gaps to fill in the organization’s cybersecurity that may have led to the incident. However, companies should be aware that an internal investigation not properly focused and managed can risk litigation and regulatory enforcement exposure. It is critical to define the scope of the investigation — as an investigation that reaches beyond its scope unnecessarily puts a company under the microscope.

When conducting an internal investigation with outside and in-house counsel, companies should be aware of issues regarding lawyer-client privilege. Communications with counsel as a part of the investigation should not be assumed to be privileged — and a false reliance on privilege could expose unflattering facts or communications down the line during litigation. In most jurisdictions, for an internal investigation to be legally privileged, one of the primary purposes of the investigation must be to provide legal advice to the organization. Relatedly, all witness employees must be given a clear and full Upjohn warning.

Following an internal investigation, companies should be careful in reporting their findings. Conclusions about the incident should not be made prematurely. Assigning fault or success before all facts are known can lead to contradictory drafts of the report. Narrowing the scope also applies to recommendations that may result from an investigation. Recommendations that are tangential or unnecessary, risk not being implemented in the aftermath, and recommendations that are not acted upon create targets for future liability.

**Conclusion**

At the end of the day, hope is not a plan. It can be fatal to hope that an attack won’t happen, or to hope that if it does happen, the right people will be available and everyone will remain calm.

Instead, companies should plan for the worst and hope for the best. Planning with an eye toward litigation, regulatory enforcement and reputational damage — rather than just planning around various types of specific attacks — can make all the difference.