Managing cyber & security risks

Liability trend emphasises need for cybersecurity risk management programmes

Cyber risk is at the top of the list of what keeps company directors up at night, according to the Association of Corporate Counsel's recent survey of chief legal officers worldwide. The trend for holding companies liable for cybersecurity incidents confirms and helps explain this concern. Unfortunately, how to address it is often misunderstood and focusses far too much on the technical issues related to cybersecurity rather than on the legal aspects.

Shawn Tuma
Partner in the Cybersecurity and Data Protection Law Group at Scheef & Stone, LLP

When company leaders hear the words 'cybersecurity incident' their natural inclination is to associate it with the information technology aspect of the company. The reality is, when a company has such an incident, it impacts several key aspects of the company: information technology, business operations and public relations – as well as legal. Responsibly addressing this risk requires a team effort that involves all these aspects – especially legal.

Many who have never encountered a significant cybersecurity event do not realise that legal is often the primary force driving cybersecurity compliance. Significant cybersecurity incidents are legal events. Given the choice, most companies would prefer to mitigate security incidents internally and then keep it quiet. Legal obligations – whether public laws and regulations, industry standards or private contracts – prevent this from happening. They not only mandate disclosure, but also require the company to dictate how it must respond, how quickly it must respond, what must be disclosed and to whom, and what remedial measures it must take for those affected.

Compliance with these obligations can be challenging in the best of times. Given the state of panic companies usually experience immediately post-breach and the extremely compressed timeframe within which they have to work, it is virtually impossible for a company to effectively comply with these obligations unless it has prepared to do so well before the incident.

With litigation trending toward finding companies liable, regulatory agencies becoming more aggressive and the heightened focus on holding officers and directors responsible for company breaches where the company had not adequately prepared, the only reasonable thing a company can do is anticipate that it will have a security incident, put measures in place to prevent it and then get prepared and stay prepared for how it will respond if one occurs.

Companies are evaluated on their reasonableness, after the fact. Those evaluating are usually legally trained administrative attorneys, state attorney generals, judges and plaintiffs' attorneys – all looking through the lens of their legal training and experience, with the benefit of 20/20 hindsight, to determine what was reasonable.

In preparing to manage this cybersecurity risk, it is critical for a company to try and figure out today what, at some point in the future, these people will expect the company to have done prior to the incident, to be considered as taking reasonable measures before the incident. In other words, the company must look into the future and imagine asking itself in such a situation, 'what would we wish we would have done today' and then do it.

CYBER IMPERATIVES
Putting in place written policies can mitigate loss in a controlled way

Given that its audience will be predominantly made up of attorneys, looking through the lens of their legal experience and training, it is important to have legal counsel on board to help determine what measures may be considered reasonable and appropriate.

Litigation and regulatory liability trends

The second half of 2015 saw a significant increase in the trend toward holding companies liable for cybersecurity incidents. There have been significant developments in this area by litigation in the courts as well as by enforcement actions by federal regulatory agencies in the US.

In 2015, a tectonic shift occurred in assessing liability against companies for data breaches. Before this shift, consumer data breach cases were often dismissed quickly. The courts were finding plaintiffs' fears of future harm were insufficient to support a lawsuit.

This trend changed in July 2015 with the United States Court of Appeals for the Seventh Circuit's ruling in the Neiman Marcus breach litigation. In this case, the court found that where hackers had deliberately broken into Neiman Marcus's database and stolen its customers' private information, it was reasonable to presume that they did so to commit fraud and such showing was sufficient to demonstrate a substantial risk of harm. This, the court found, was more than simply a fear of future harm and was sufficient to support a lawsuit.

The latter part of 2015 saw two cases that furthered the Federal Trade Commission (FTC) and the Securities and Exchange Commission's (SEC) respective roles in regulating cybersecurity.

In August 2015, the United States Court of Appeals for the Third Circuit, in FTC v. Wyndham Worldwide Corp, ruled that the FTC has the authority to regulate cybersecurity under the unfairness prong of section 45(a) of the Federal Trade Commission Act (FTC Act) and that companies have fair notice that their specific cybersecurity practices could fall short. The FTC brought this action against Wyndham following three data breaches that Wyndham had between 2008 and 2009 due to its rudimentary cybersecurity posture that the FTC alleged contravened the recommendations in its 2007 guidebook *Protecting Personal Information: A Guide for Business*. Wyndham argued that the FTC lacked the authority to regulate cybersecurity under the unfairness prong of the FTC Act and argued that it did not have fair notice that its specific cybersecurity practices could fall short of that provision. The ruling in August 2015 found both of these arguments to be without merit.

> *When company leaders hear the words 'cybersecurity incident', their natural inclination is to associate it with the information technology aspect of the company*

Even before having its authority confirmed, the FTC had taken an aggressive approach in pursuing one company, LabMD, for cybersecurity issues. In November 2015, the FTC's own chief administrative law judge ordered the FTC to dismiss its complaint in the case FTC v. LabMD because the FTC was unable to provide evidence that any consumer had suffered any injury from what it alleged were LabMD's unfair acts or practices. The FTC has since appealed this decision and continues its pursuit of LabMD.

The FTC originally opened its investigation into LabMD in 2010, based on information provided to it by a cybersecurity forensics firm that regularly provided information to the FTC. The incident arose when one of LabMD's employees was using LimeWire, a peer-to-peer file sharing program for sharing music and videos, on the company's computer network without authorisation. The security forensics firm was able to use LimeWire to gain access to one file from LabMD's network that contained protected information of its customers. Once it obtained this information, the firm contacted LabMD and offered to 'remediate' this issue for the sum of $40,000. When LabMD refused to pay, the firm sent the information to the FTC, which used it to pursue LabMD. Due to the disruption, expense, and negative publicity of the FTC's case against it, LabMD went out of business in 2014. Despite that, and despite the fact that the single file that the cybersecurity forensics firm obtained from LabMD, through LimeWire, was never exposed to anyone beyond that firm, an expert witness, and the FTC itself, the FTC continues to pursue LabMD.

In September 2015, the SEC established its role in regulating cybersecurity. In SEC v. R.T. Jones Capital Equities Management, the SEC brought an enforcement action against R.T. Jones for violating the 'safeguards rule' of Rule 30(a) of Regulation S-P of the Securities Act of 1933. During a four-year period when R.T. Jones did not have cybersecurity-focussed policies and procedures, hackers accessed more than 100,000 of its clients' records. No individuals reported financial harm, however, the SEC assessed a $75,000 penalty based on this standard: "Firms must adopt written policies to protect their clients' private information and they need to anticipate potential cybersecurity events and have clear procedures in place rather than waiting to react once a breach occurs."

Cybersecurity risk management

As the liability trend increases, so too does companies' need for an adequate cybersecurity risk management programme. They must realise, however, that cybersecurity preparation requires addressing more than information technology. In many cases, the technical aspects can be resolved rather early on in the process but the legal fallout can last for months or years. Because of the legal obligations, legal preparation is essential. »

The enforcement actions in Wyndham, R.T. Jones, and LabMD related to the companies' policies and procedures. An employee using an unauthorised computer program brought down LabMD, emphasising the need for appropriate policies, procedures and training.

What can a board do? It should ensure the company has an adequate cybersecurity risk management programme. Such a programme requires team effort from within and outside of the company and should consist of several phases.

The programme should begin with an initial risk assessment to identify each company's unique risks to determine its baseline security posture. It should be tailored to the company's business and examine how much and what type of data the company transmits or stores, the various ways that are available to access the company's network and how those entry and exit points are protected. It should examine who has access to what data and what internal safeguards are in place to protect it. It should examine what IT assets and security assets are in place, how they function and how often they are tested and upgraded. It should assess the company's internal and external policies and procedures as well as the existing, and existing training of the workforce. It should also examine the company's contracts and business relationships to see how data is handled and what obligations are in place. By looking at this, as well as other data, the assessment should determine the overall risk exposure of the company by measuring the magnitude of risks it faces multiplied by the likelihood of those risks.

Thinking strategically

The next step is to develop a strategic plan for improvement. Using the risk assessment and looking at the needs and security requirements of the company's industry, the strategic plan should focus on improving the company's security posture by creating specific action items that are prioritised, based on the severity of risk to the company.

If a cybersecurity incident ever occurs, the company has documented evidence to show that it recognised the cybersecurity risks

Either next or, if circumstances warrant it, simultaneous with developing the strategic plan, deploy necessary IT and security assets that are the first line of defence against attacks on the company network. The timing for this step will depend on what is learned during the risk assessment, especially in situations where penetration testing is performed as part of the risk assessment and reveals substantial weaknesses in network defenses.

Implementation of the action items developed in the strategic plan is the next step. A critical component is to prepare and adopt appropriate internal policies and procedures. Once adopted, they should provide the structure to use when training the company's workforce (and management) on how to protect the company's data.

Training is critical for several reasons: first, it's an opportunity to reinforce a culture of security within the company; second, it helps members of the workforce understand the policies and procedures; third, and perhaps most importantly, training should incorporate case studies to demonstrate key principles and help teach the trainees how to think about variations on the examples given as rarely are any two real-world situations identical.

One of the key policies that should be prepared is a cybersecurity incident response plan that will be the company's playbook should it experience a cybersecurity incident. This response plan should be given to appropriate personnel within the company and they should tabletop test the plan.

Next – and at regular intervals, as determined by the unique needs of the company – its cybersecurity posture should be reassessed and refined using the same process, from the beginning.

Finally, each of these steps should be well-documented so that if a cybersecurity incident ever occurs the company has documented evidence to show that it recognised the cybersecurity risks it faced and took reasonable steps to protect against the risks and respond, should they occur.

ESSENTIAL LEARNING
Training helps everyone understand the policies and procedures in place