Why directors must get on board and address cyber threats, risks and security

by Rois Ni Thuama

Recent history

In the first half of 2021, we watched as large organisations around the globe ground to a standstill following significant cyber-attacks. The impact moved beyond the boundaries of the targeted businesses and spilled into patient care and the consumer world.

Almost immediately into the second half of the year in a single week in July, Google[1] announced four zero-day security vulnerabilities (vulns). i.e. unknown software flaws which if left undetected can be exploited by attackers. Google researchers also noted that 2021 has been a particularly active year for in-the-wild zero-day attacks. The following week, the governments of Norway and the United States accused China of interfering with their email and of gaining access to intelligence critical to the safety of those nations.

It is impossible to know what the situation will look like by the end of this year. What is already entirely predictable is that 2021 will surpass previous years in terms of volume and severity of attacks, merely continuing the known trajectory. There is no good reason to believe otherwise reviewing the data at the time of writing.

All hands to the pump

Cybersecurity and risk management professionals have long called for an all-hands to the pump approach to deal with the pressing and expanding cyber threat landscape.

It is becoming increasingly clear that informed and decisive leadership by way of active board members assuming a role at the helm is critical. Not only so that board members address their legal obligations to their business and its stakeholders, but that they look beyond the legal issues. It is a well-established principle of good governance that boards consider their civic responsibility as good corporate citizens.

Good corporate citizenship prompts the board to consider their community and how to make a positive local impact or avoid negative outcomes.

For years, firms have considered their impact on the environment. Boards have worked with local and national authorities to inform their decision-making process to protect the ecosystems that they operate in.

Cyber governance offers progressive boards a similar opportunity to think beyond the maturity of their own IT estate and their digital ecosystem and to consider the potential harm of their oversights and omissions to their clients, consumers, patients, supply chains, and the wider community.

In the same way that boards access outside expertise to consider the environment, the same could be done in the digital world. A good starting point is to access the vast literature compiled by the intelligence communities. In particular, the world leading institution the National Cyber Security Centre (NCSC), in the United Kingdom (UK) provides keen insight as well as critical toolkits for boards.

If directors are unsure of whether their obligations run to this type of exercise, they would do well to review the directors' duties set out in the Companies Act.

The 'L' word

In the United Kingdom and in Ireland, legislation already exists in the form of directors' duties.

These duties are codified and contained in the Companies Act (CA) in 2006 and 2014 respectively. The list is non-exhaustive. When considering cyber threats, risks and solutions, the duties that directors should pay special attention to are:

1. Duty to promote the success of the company (CA 2006, UK) or to act in good faith in the interest of the company (CA 2014, Ireland).

   To promote the success of any company, directors must consider digital marketing, online retail, customer acquisition and client databases containing potentially sensitive data, social media and the potential for reputational damage.

   To drive efficiency, cloud computing and Software as a Service (SaaS) must also be at the forefront of the board's thinking. SaaS means that small businesses can access enterprise class technology at a fraction of the price. This levels the playing field for small and medium enterprises meaning that they can pitch for larger contracts as they are able to compete to meet the digital standards expected by larger, more sophisticated clients.

   There is simply no way that a director can act in the interest of the company or promote the success and simultaneously overlook or ignore their digital operational resilience.

2.

1 https://blog.google/threat-analysis-group/how-we-protect-users-0-day-attacks/

3. Duty to 'exercise reasonable care, skill and diligence' (s174 CA 2006, s228 CA 2014).

In the US, a similar duty arises, although not codified it is well established:

Directors must... use that amount of care which ordinarily careful and prudent men would use in similar circumstances... [and] consider all material information reasonably available' in making business decisions.

To what extent directors exercised reasonable care, skill and diligence would be considered on a case-by-case basis and is a matter of fact, not law. However, it is still possible and practicable to consider strict adherence to basic principles and to deal with the most significant known cyber threats as a priority. Indeed, a US case in 2018 proved instructive.

The reasoning was clear. The court considered the following questions:

1. Was the threat well known and understood?
2. Was the solution well known and understood?
3. Was it reasonable, affordable and practicable to deploy it?
4. Would a reasonable IT director have known to deploy it?

Side bar: *The IT director(s) had recommended the solution to the board, but the board denied their team the budget. The failure to deploy a well-known solution led to a data breach and the court issued a record fine.*

The cost of the fine plus the fees for their legal defence considerably outweighs the cost of the solution. Professional investors who may find themselves with a smaller dividend payment as a result of losses arising from the board's failure 'to exercise reasonable care, skill and diligence' may find this provision useful to redress the harm they have suffered.

The appetite for legislating board responsibility for cyber matters is certainly gaining ground.

Most recently in Europe, the Digital Operational Resilience Act (DORA) puts the matter clearly and succinctly. *'[T}he management body shall...bear the final responsibility for managing'* the firm's cyber risks. I have written about DORA in the last edition of Accountancy Plus, it is not unduly burdensome and merely requires that firms within the scope of the Act address reasonably identifiable cyber risks.

Similarly, the US has indicated its unwillingness to continue to permit sloppy and haphazard approaches to cyber security by mandating a cybersecurity maturity model for suppliers to the US Department of Defense. The only sensible question at this point is - what's taken them so long?

Cyber catastrophes - under review

It is inevitable that we will see public inquiries for cyber catastrophes similar to reviews prepared in other sectors. Our entire professional world is working online, it is imperative that we assess

where the responsibility lies for any failures and what lessons are to be learned.

In all likelihood, we will also start to see the rise of cyber litigation. Large global law firms looking to protect their clients are already building out their cyber law and tech law departments. The primary purpose will be to protect their client's position by providing robust advice to help them avoid harm. However, the secondary position would be to seek to recover damages for clients who have suffered losses (direct or indirect) or suffered some other harm.

It will be a Herculean but ultimately hopeless task to try to defend directors who have failed to adequately address known threats. Oversights of this nature will lead to hefty fines and punitive damages. Failing to strictly adhere to basics has never worked in the defendant's favour and such failures in the cyber space should be the subject of harsh criticism. Particularly as the harm of cyber-attacks can be so extensive. I look forward to reading the judgements in these matters.

As board members ultimately bear responsibility for their firm's strategy, the boards must take a more active interest. A simple and effective starting point is to address known significant cyber threats to protect their firm and then to mandate appropriate action for their supply chain. Whatever scrutiny boards come under; this will be more so where health care providers have been targeted. The impact caused by delays to life saving measures or the corruption of essential intel could (it is no exaggeration to write) be life threatening.

Health & Safety Executive

Take for example, Ireland's Health & Safety Executive (HSE) which was hit by the Conti ransomware. Since Conti first appeared in 2020 it has undergone rapid development, moves quickly and encrypts the data using state-of-the-art encryption methods. It is a 'double extortion' ransomware that (i) encrypts and (ii) steals data. This is followed by a demand which if paid will (a) unlock and (b) withhold that data (rather than release it into the wild).

Aside from (i) the reputational damage, and (ii) the cost of disaster recovery; the implications for patient safety may take some time to surface. The harm is no less real and no less painful if that harm is only realised months after the initial attack.

It is entirely likely that law firms who have previously operated in the 'slip & trip' claim world and already have the infrastructure to deal with similar claims will turn their attention to these types of data breaches.

The relatively formulaic approach for considering the merits of a matter in the tort of negligence means that the initial inquiry and intelligence gathering can be achieved at low cost through call handlers or a simple web survey.

In the matter of health care, the duty of care to patients is well established. We know from the facts that data was exfiltrated and released into the wild. Damage is more difficult to assess at this early point. We do know that ransomware is well known and understood, which makes it foreseeable. It is also well known that ransomware is also avoidable. This is going to make it very difficult to defend the board's lack of preparation and protection especially if the attack vector was via email.

The same reasoning would apply for investors in commercial ventures. While there is no indication yet that we will see litigation in the following matter, it certainly remains open to the investors to consider their position.

Colonial pipeline

Colonial pipeline is the operator of the US's largest fuel pipeline serving 260 delivery points across 13 states and Washington DC. The ransomware attack which paralysed the operating system created considerable business disruption leading to panic buying and shortages across the country.

Despite the US Intelligence Community discouraging ransomware payments, leadership in the firm opted to pay the demand, reports put the figure

in the region of US$5 million. It was widely reported that the decipher keys provided by the criminal gangs had limited efficacy and the return to normal business was slow and challenging.

While neither instance (HSE nor Colonial) is good news, it significantly raised the profile of the importance of digital operational resilience and the importance of a strict adherence to basics. Moreover, these attacks have led to higher levels of engagement from the governments in Ireland and the US.

The bounty hunters are here...

Colonial pipeline was not an isolated incident. The United States (US) has been so frequently hit with ransomware attacks (estimated to be 1,500 so far) that in July this year the US Government offered a reward of US$10 million. This reward is in return for information leading to the arrest of crime gangs behind the attacks.

The bounty is a significant step to encourage ethical computer hackers to track down and pass on crucial evidence; but it is not without its potential pitfalls. Prosecutions based on stolen information risk running afoul of the doctrine enshrined in the legal metaphor 'fruit of the poisonous tree'. Evidence that is gathered illegally is usually inadmissible. So, we find ourselves in another wait and see to learn how this plays out.

Alternatively, a different set of actions which are not legal minefields could protect firms, the country and the economy.

Boards - where the buck stops

It is no exaggeration to write that the ability of corporate leaders to confidently navigate the multi-layered cybersecurity and cyber threat landscape is essential to a firm's prosperity and even to its survival, (see directors' duties above).

To what extent a company adapts to the cyber challenges that lie ahead will depend on the effectiveness of its board.

Boards must embrace the criticality of identifying the fundamental organisational causes of cyber instances as opposed to considering any single underlying fault.

Without sufficient insight, it is not possible to accurately attribute where the fault lies in either the HSE or the Colonial pipeline ransomware attack or call out individuals. However, we do know that culture, strategy, budget and leadership are all essential for good risk management.

To drive boards to consider their role at a strategic level, I reached out to two leading experts who work with boards.

Basics are critical (not optional)

Mark Evans, Managing Partner with Define: Athene who works almost exclusively with FTSE 100 boards explained:

'[t]he purpose of risk assessment is to assess known significant risks in order that you can take appropriate steps to manage, eliminate or minimise those risks.

Without a proper comprehension of the cyber threat landscape, cyber security measures, directors duties and board obligations, boards are simply not equipped to give proper and clear directions.

Boards frequently misunderstand the importance of critical deployments which they dismiss as trivial, whereas basic factors are never trivial. This is precisely why they've made it onto the basic list. Fundamental oversights are leading to a lot of corporate pain. This is pain which can be avoided'

Culture and leadership

Sean Lyons is globally recognised as a corporate defence thought leader and strategist and author of the critically acclaimed book, 'Corporate Defense & the Value Preservation Imperative'.

Lyons explained:

'[t]he firm's culture will determine the extent to which the organisation adopts a proactive or reactive approach to its security component.

The promise of value is an integral part of any corporate strategy. We're all familiar with value generation however cyber-attacks bring value preservation into sharp focus.

For value preservation to operate the firm must have a sensible corporate defense strategy. It is too much to leave corporate defense to the IT teams alone and hope for the best.

Conclusion

Since Covid-19, businesses that quickly adapted to the 'new normal' world have thrived, those that did not may not survive. The same ability to recognise the opportunities and challenges that lie ahead for all businesses operating in the digital world will mean the difference between long term success and failure.

The Cyber Security Toolkit for Boards is a must read, and a sensible starting point for boards at all levels. Depending on the size and complexity of the firm, it may be all that is required. But for multi-office operations across different locations, in different jurisdictions, outside expert assistance will help directors to identify well known pitfalls and avoid them.

Leaders create culture. It is the board's responsibility to change it. Cultural traits and organisational practices which are detrimental to the firm sit with the board.

Critical deployments are often dismissed as trivial and basic. Boards frequently misunderstand the importance of basics assuming sophisticated tech is more valuable. Basics are never trivial. They are basic because they are considered essential to the best outcome.

Rois Ni Thuama

A Doctor of Law and subject matter expert in cyber governance and risk mitigation, Rois is Head of Cyber Security governance for Red Sift one of Europe's fastest-growing cybersecurity companies. Working with key clients across a wide market spectrum including legal, finance, banking, and oil & gas Rois writes and presents on significant cyber threats, trends, addressing and managing risks.