Cyber Risk Management

Cyber security, securing the corporate balance sheet?

By: Andy Watkin-Child

Cyber, cyber security and cyber risk management are in the headlines almost daily. In the context of countries hacking countries, data breaches through data theft, States and companies being held to ransom or individuals having personal data stolen and published online. We are all living in what many now call the 4th industrial revolution, in a society which has become dependent upon the consumption of data and use of information and technology. In developed economies, governments, organisations and individuals rely upon technology platforms, data and information to manufacture and sell products and services, provide healthcare and manage financial transactions. To deliver basic services like gas, water or electricity, to access online banking, hail a taxi or to purchase the next film to watch on the mobile phone.

Data has become a commodity and if the flow of data and information are disrupted, trade flows slow or stop. What happens if power fails for 24 hours; no water, no cash, no fuel. What happens if you have power, but you disrupt the flow of information and data? With no data how do you distribute food if you cannot get the message to the distribution centre? How do you pay for shopping at the grocery store, how do you withdraw money from the ATM and how do banks transfer money between each other globally? Alongside the growth in data consumption and our reliance upon the use of technologies such as the internet, mobile communications and digital for the creation, transmission, usage and storage of data. The cyber threat has grown.

Cyber-attacks, a global problem everyone is talking about. The World Economic Forum (WEF) annual report of global risks places cyber-attack as one of the top 5 risks behind extreme weather events, failure of climate-change mitigation and adaptation, natural disasters and data fraud or theft. With the potential to have a significant global economic impact in the next 10 years. Cyber-attacks are a geopolitical weapon with countries targeting countries, countries targeting corporations and countries targeting individuals. The use of cyber as a weapon of warfare is gaining prominence, nation states are targeting power networks or using cyber to support conventional military campaigns.

Cyber-attacks are a well-run criminal activity. The global cost of cybercrime is estimated in the region of $600Bn, the global impact of cyber-attacks is estimated at 0.8% of global GDP and rising. Cybercrime is more profitable than drugs and people trafficking combined and with the source of cyber-attacks being difficult to detect, harder to prosecute. Cyber criminals can launch attacks with a high degree of certainty that they will not be caught. Cyber is a well-run criminal activity and if cybercrime were a country then it would have a GDP equivalent to the 13th largest globally. It is a well-managed economy with its own structures for the targeting of nation states, corporations and individuals. With an ecosystem for the trading of personal data, the buying and selling code to illicit cyber-attacks, the buying and selling of cyber-attacks (Cyber as a Service) and the trading of intellectual property (IP) and private information.

Cyber risk is a different risk to most. What makes cyber different from other non-financial risks? There is no one size fits all definition of a hacker. They range across governments, cyber criminals, hacktivists, script kiddies and insiders, they all have different motivations. Cyber-attacks can be global in their impact, whereas physical attacks are localised. The NotPetya attack in 2017 caused heavy losses to some company's impacting their global supply chains damaging technology platforms from the shop floor to the board room. Cyber-attacks can be run from just about any location in the world, there is no need to be physically present. Cyber-attacks can be generic in nature or they can be well planned, researched and targeted. The same tools can be used to attack individuals, companies or nation states, which can result in global collateral damage if an attack gets out of control. The speed of a cyber-attack is faster as a function of their impact than other forms of non-financial risk. Cyber-attacks are considered asymmetric in nature which means you must defend the entire surface of an organisation, whereas the attacker has only to be successful at one point of entry.

Cyber risks can significantly impact the balance sheet. All of this makes cyber a significant risk to understand and manage across a company. The global cost of Not Petya has been estimated between $4Bn and $8Bn. The companies it impacted suffered considerable damage, Maersk reported losses of around $300Mn and Merck of over $800Mn. Costs which impact both the top and bottom line. Such as the costs to fix the issues identified in the attack, communicating and compensating customers, lost revenues and sales, the associated brand and reputational damage and the on-going legal costs. The legal fallout of a cyber-attack can run for several years and the impact to corporate brand will never disappear. Target, a well-known US retailer has not lost the reputation it gained following its cyber-attack in 2013, where information relating to approximately 40 Million credit cards was stolen. The attack on Talk-Talk in 2015, still warranted column inches in the UK national press in June 2019. This does not include the costs to help protect the company from cyber-attacks in the first instance (work which needs to be carried out to improve the maturity of security across a organisation). There is growing evidence that the share price of companies is affected by a cyber-attack and credit rating agencies are running programmes to evaluate the impact of cyber security on credit scoring, which will have a direct impact on the cost of credit for companies in the financial markets.

Cyber risk management, firmly on the board table with the balance sheet. Cyber now sits on the board table and the long-term prognosis for cyber and the board is clear. Cyber as a risk is not going away, it will only become a more significant risk as the digital economy grows. The cost of regulatory compliance will increase, with regulators from many sectors focusing on cyber risk management. The EU GDPR regulation enforces fines of between 2% and 4% of global revenues, a cost British Airways will be negotiating following its data breach in 2018. The cost of a cyber-attack is rising, with the growth in dependency on digital and the impact that globalisation has had on supply chains. There is an additional issue with the lack of cyber skilled resources, there are not enough skilled people in the marketplace globally to help companies manage the risk.

Cyber places stress on the balance sheet. But what can boards do to get to grips with cyber security and how can they start to secure their balance sheet? By making a start.

1. Understand that cyber is here to stay. It's an enterprise wide business risk, not just a technology issue. A risk which drives significant cost pressures. Cyber-attacks impact brand, reputation, sales and profits.
2. Have clarity on what are the company's crown jewels. What are the critical data and key systems, what is the security posture?
3. Understand cyber risk. So that the board can challenge their teams on the effectiveness of cyber risk management. The regulatory environment is starting to address this, recommending cyber aware board members have a seat at the table.
4. Have clear governance and reporting in place to report cyber risk management upwards for discussion, on a regular basis.
5. Have a plan in place for managing a cyber incident. It is not possible to defend yourself against a nation state, an attack will happen. Be prepared for it.
6. If you are not sure about cyber then engage with independent professionals. Who can help you understand the risks and advise on the right questions to ask or provide a level of independent oversight.

There is plenty of evidence on the cost of a cyber-attack. There are many Chairmen and CEOs who now understand what cyber means to their business and what a well-run and targeted attack can deliver. There is also plenty of information which states that 'good Security hygiene' can help prevent 60% of cyber-attacks. The data to help quantify the risk will be available in the company. It needs the right governance and oversight at the board table, so that the board can place assurance that their teams are securing their balance sheet. Finally, don't be caught out in thinking that cyber insurance will allow you to transfer of all the risk, it won't. As the current court case with Mondelez, the manufacturer of Cadbury and Oreo, is proving.