Demystify Cyber Risks at Board Level

We live in a hidden cyber war for quite some time. The past 2 years have shown us at Board Level that we have to be increasingly prepared for extraordinary, parallel risk situations that not only suddenly affect the global economy and geopolitical stability but can also put upside down the everyday life of each and every one of us.
There are many lessons we can learn from the ‘real virus’ and apply to cyber security. One of the most important preventive measures to spread pandemics has been social distancing for months. Fortunately, in this increasingly highly networked, interconnected and interdependent world, we often can virtually continue our professional and private lives. Given the huge increase in the number of people working remotely from home, though, it is critical that we proactively continuously take care of our cyber hygiene and the remaining cyber risk. This approach requires a broader understanding of risk, potential targets (‘intangible assets’), some in-depth knowledge of cyber security and, in particular, the insight that anyone can become a victim of a cyber attack at any time.

Risk similarities

Cyber risks (including cyber warfare) and pandemics have a lot in common, but also major differences. Both of these risks are global, broadly contagious, possibly disastrous, and particularly human caused (‘man-made’). However, the possible response time for cyber risks is much shorter and the incident frequency is higher. Cyber risks mutate like real viruses, but much faster between continents. Both risks affect SMEs and large corporations, as well as board members and private individuals. It is therefore not surprising that boards globally were confronted with an exponential frequency of incidents (extortion, phishing and malware) over the last two years. An unsettled situation and fear attract new attackers like bees to honey, who then work with pressure to get credentials released from their target persons.

Lessons from recent attacks

In order to protect themselves effectively, many boards have decided that their data must be divided and segmented into certain areas, using selective access authorization to certain specific files (‘network zoning’). In most cases, this methodology can prevent some infections from entering new segments. However, it gets much more complicated when, for instance a complex ’ransomware attack’ spreads horizontally across the infected network, instead of spreading to other networks. The attacker then often gains administrator rights and login information and controls ultimately infected computers in order to gain control over other computers in the same network. Whether by chance or consciously, the 'real viruses'(Covid-19), allow companies and risk teams to learn important lessons for their cyber security strategy. Attacks can also affect companies whose systems run current, regularly updated and properly patched software. Certain malware shows how important it is to restrict administrator privileges. A simple way is ‘leasing’ privileges so that employees who need them only have access to admin rights for a certain period of time. Attacks often show that companies also need to consider other forms of security, such as endpoint monitoring, network zoning and access to enhanced security information platforms (‘threat intelligence’) to ensure that systems, processes and people are in place to respond to the inevitable attacks. Ultimately, this approach, if stress-tested across all levels (including boards), will make a big difference to what harm attackers can do.

Simple, but often, an underestimated, deadly attacking strategy

The easiest way for attackers on the net is to first identify and break through low-value targets and then to reach outside for better and more valuable targets. No company can effectively protect its networks to every end point efficiently with limited resources. A Hacker often begins to find a basic vulnerability. If he finds this flaw, there are unfortunately often many opportunities to move sideways from one place to another in the large network. Popular destinations are, for instance, social networks of senior employees, followed by targeted phishing attacks or even CEO whaling (fake president news) examples. Sophisticated attacks are prepared and executed with a high degree of detail.

Remaining on the front foot is essential, but requires broad and continuous basic cyber hygiene

The first, often basic, but efficient line of defence of every company's board or their individual directors always remains their own network hygiene, risk awareness and knowledge transfer. Knowing what is on the network, and who has access, that the devices are configured securely, the network is set up as intended, and that changes do not compromise security are fundamentals. Sounds entirely logical, but it is not always implemented. Equally, it quickly becomes apparent that this strategy is not always easy transformed and consistent to do. Hence, boards and individual directors should stress test and simulate their level of readiness. Desktop exercises won't help you feel the consequences of your decisions recognizing it in real time and under stress.
Broad experience let us conclude that in many cyber security networks there is an unintentional failure of hygiene. Even at 95% compliance level with basic hygiene standards is often not enough, in particular, if the board was targeted and cyber security is not represented amongst directors. Unfortunately, such situations remain frequently the case. For security teams, and their leaders (CISO/CIO), it is vital to perform basic controls in-depth anytime, anywhere, to involve top management consistently. Demystifying cyber risk at board level represents a significant task and challenge, but often makes the difference between failure and success under an attack.

It is and remains a material investment prior and during crisis, but absolutely worthwhile undertaking it.

Experience shows that companies that invested materially and proactively in adequate IT resources, capabilities, skills and cyber security at board level remained on the front foot. In the past Covid-19 crisis, these successful companies were quickly out of their box. They provided quickly a large number of simultaneous connections from the start of the crisis, efficiently scaled via Virtual Private Network (VPN) and secured Video Conference Solutions to meet exponential Working from Home ('WFH') demands. In a next step, they often worked along a pre-agreed and stress-tested Business Continuity Management approach, including but not limited to

- provide employees (plus board members) with devices, regularly checked patch levels and access to basic threat intelligence knowledge
- allow access to the Internet only via secure networks (no open WiFi) despite higher operational expenses
- prevent external access to company applications except via encrypted communication channels
- enforce multi-factor authentication mechanisms and preventing remote system access interfaces
- permit ‘Bringing your own device’ (‘BYOD’) only under strictly limited aspects (configuration checks and patches)

Despite such precautions an incident could still occur. In many cases the companies could then rely on an already checked incident scheme ('Incident Response Plan') with clear guidelines and tested partners (forensics, investigation, disclosure, public relations, hotlines), that allowed employees and clients to be adequately informed and that regulatory data protection requirements and any potential insurance solution were taken broadly into account.

Knowledge transfer and risk recognition at board level must accelerate

Demystify ‘cyber’ at board level with priority. Cyber risk can hardly be diversified globally because it occurs too often simultaneously and is becoming increasingly complex. In the event of an attack, fundamental questions arise, such as: "How did the attackers get into our network, where did this infection come from, where does it go next, what does it mean for us internally and externally, where is the weakest link?" To find this answer, security teams must map a network well before an attack and understand all access paths and normal information flows for the company and demystify cyber security at board level. A designated director at board level must become an active and knowledgeable sponsor of the CISO/CIO if no board representation is feasible. This approach has to be planned in detail and is not easy to implement.
We all need to be better at risk identification, attack detection, automation and defense algorithms to analyze situations and issues like these that defy human thinking. At the same time, slowing down a cyber attack can make the difference and provide defense advantages.
We know that not every determined attacker can be stopped, but if we slow them down, our defense mechanisms (e.g. sensors) have time to detect digital intruders so that they can respond to blockages or quarantine, or communicate efficiently internally with employees and externally with regulators, clients, suppliers and partners. Cyber Risks are global and so operating internationally does not diversify your enterprise risk. And they are manmade. They are driven by criminal minds, stealing knowledge, IP and money or destroying and disrupting lives. The attackers have become even more sophisticated, and their targets are increasingly intangible assets that often represent 80% - 90% of the market value of a company or the board of directors. Without any doubt, cybercrime remains a fundamental issue for management. Every company can be a victim of cyber crime at any time. It's just a matter of time, means and type of attack. If you want to survive in today's world, with an ever-increasing complexity of attacks, you have to ask yourself:

- Are we prepared for an attack at all levels and especially at board level?
- Where do I stand in liability as a board member? Am I aware of it?
- Where are our targets? How do we constantly train our employees and equip them with the right devices?
- Who could be potential intruders? Does our Business Continuity Management Program match them in respect of Crisis Management, Forensic, Incident Management and Risk Transfer?
- How do we selectively protect our data, systems, employees, customers and intangible goods (IP, brand, reputation)?
- How do we communicate from the inside out in a crisis (strategic public relations)?
- Have we already simulated an attack in real terms and stress--tested our incident management(s) teams top-down? If so, how are we filling potential gaps (means, capabilities, investments, partners)?
- Are there external risk transfer options (cyber insurance)? What added value do these approaches bring and what do they cost?

Conclusions: A risk unlike any other in your portfolio

Cyber risks have an unparalleled and unique risk nature and challenges. Your Risk Profile is global and man-made and operating internationally does not diversify your risks. The size of company does also not matter much. The stakes are certainly high for any board of directors.
At this moment cyber risk is still the most underestimated risk and it is no longer a black swan because too much is already known. Without a managed risk approach to cyber exposures at board level, any company is severely exposed and could suffer from outlier losses, eventually causing reputational harm, unforeseen financial losses and even class actions.
Attackers are driven by criminal minds, stealing knowledge, IP and money or destroying and disrupting lives. State-sponsored attacks are much worse as they seek to infiltrate or damage entire sectors or economies. These attacks focus on materially important companies, critical infrastructure including healthcare, telecommunications, financial services and utilities, provoking contagious effects, creating a chain reaction through a large number of damaged entities intended to destabilize a sector or even a nation.
Cyber exposures will most certainly further grow due to the increasing vulnerability of our social and economic life. The driver behind this trend is the massive growth in number of interconnected devices and upcoming new technologies (5G) that are all capable of being compromised.

Peter Hacker, Cyber Security Expert, Entrepreneur and Author – www.peterhacker.io

Over the past 15 years, Peter Hacker has worked with Top Managements from (re)insurance, banking, pharmaceutical, critical infrastructure, retail, telecommunications, media and technology companies across more than 90 countries. Being a global Cyber Expert and Risk Thought Leader in Financial Services, his global expertise is sought after by International and Regional Organizations, Regulators and Rating Agencies. His dynamic and insightful keynotes aims at Cyber Intelligence, Threat Developments and Digitalization mainly reiterating the risks and opportunities.