Cybersecurity: The Role of the Board

A three-step process for board directors to start improving cyber-oversight.

In 2016, cybercrime cost U.S. firms more than US$17 million on average, based on a benchmark **study** of 237 global companies. According to a think-tank **report**, the global economic losses caused by cyberattacks total an estimated US$445 billion per year. The reason behind it is very simple. Various studies have estimated that between 70 and 90 percent of organisations and companies around the world just don't have sufficient cybersecurity.

It is the board's problem

The most common misconception is that cyberattacks are solely the IT department's responsibility. Whereas IT staff is indeed equipped with appropriate tools and experience to deter or mitigate an attack, it's up to the CEO to make the right decisions and take adequate actions. And for that to happen, cybersecurity has to be seen as a board responsibility, and discussions about this topic have to originate from the board.

One major problem with boards, however, is that they often don't have sufficient knowledge, tools and expertise. This is what is often referred to as one of the board's information gaps, prohibiting effective oversight. But directors' lack of knowledge doesn't absolve them of their fiduciary responsibility. In the face of board inaction, the CEO is confronted with a catch-22: In case of a successful cyberattack, the CEO will take the blame, whereas if the cyberattack is unsuccessful, the board will take credit for the proper decentralisation of responsibility.

A three-step starting point

Boards can begin taking ownership of organisational cybersecurity with a three-step process. The steps outlined below will work for nearly all organisations, but their difficulty will vary by sector. Though they may seem basic, very few boards I've come across have done all three.

1) Understand your organisation's biggest risks.
2) Conduct a "fire drill".
3) Know what you own.

Understanding cyber risk

Board members usually have not discussed cyber risk with the management team. It is extremely important to have a dedicated discussion that ends with consensus and commitment. The conversation should go beyond the obvious. For example, leaders at manufacturing firms should consider all possible ramifications of supply chain interruptions and communication lapses. After the initial conversation, reassessments should take place on a semi-regular basis.

Here are some general points about cyber risks that may aid exploration:

Risks can stem from an organisation's public profile. If a company's operations seem unethical—for example, the firm appears to unjustly fire people or act improperly—the probability of an attack increases.

Intellectual property is also often a reason for a hack. When a business is rich in R&D, unscrupulous actors—competitors, hackers, etc.—may mount a cyberattack to get at its secrets.

The **top three** industries targeted for cyberattacks are healthcare, manufacturing and financial services. **Sony Pictures**, **Anthem** (an insurance giant) and **Target** are only three of the better known companies that have been the victim of a cyberattack in recent years.

Fire drills

One can compare testing a company's cybersecurity functionality to conducting fire drills. In-depth, live testing gives an accurate sense of the organisation's vulnerability to, and ability to recover from, cyberattacks.

Phishing emails are **still the most common starting point** for data breaches. Most people are aware of phishing, but don't realise how easy it is to be taken in by these scams. A good way to signal commitment to cybersecurity is to test board members as a group to see how many of them fall victim to a simulated and targeted phishing attack. Sharing the results with management and employees spreads awareness and reduces embarrassment around the issue. It also makes everyone aware that cybersecurity is a top-level priority.

Over time, organisations can get tougher in enforcing vigilance. For example, Exxon Mobil frequently sends simulated phishing emails to employees. Those who take the bait can have their internet privileges revoked.

Knowing what you own

Often, board directors will unfairly blame IT for cybersecurity failures that actually originate from external sources (vendors, etc.). Boards that perform a cyber-exposure audit for the first time are usually shocked by how much risk resides outside the organisation itself.

Exposure in cyberspace is defined by how connected your organisation is and what its dependencies are. The more a company relies on third-party software, services, clouds and so on, the more vulnerable it becomes. Visible extranet solutions or integrations between companies are risk factors, too.

Essentially, cyber-exposure means that assets, services and processes are somehow accessible through public (and not-so-trusted) networks. It is measured by an organisation's attack surface. Examples of exposure points:

• Technical assets (networks, systems, online applications)
• People (email, social media, mobile)
• Information flows between systems
• Processes (maintenance, software development, banking transactions)
• Current security measures for each technical asset

Comprehending the sheer scale and dispersal of the risks should help banish the illusion that IT can manage cybersecurity entirely on its own. Directors should then realise that the final responsibility for an all-pervasive and potentially damaging issue rightly belongs with them.

Focusing on the most critical systems and most obvious findings gives you a jump-start. But remember, the only time a change in security happens is when a point of exposure is assessed and action taken to address the risk. Writing Excel spreadsheets listing the problems is not going to change anything, security-wise.

Final points to remember

The consequences of cybercrime are not limited to a one-time financial hit. The fallout can include reputational damage, in-depth regulatory investigations, long and costly litigations, and of course theft of intellectual property, just to name a few. Each of these entails damage to the company that may take years to undo, if the company is indeed able to fully recover.

To underline our point: No organisation is ever fully protected from cyberattacks, even those with the best possible safety measures. In 2016, hackers published **private information on 20,000 FBI employees**. Earlier this year, popular education platform Edmodo fell victim to hackers who obtained access to over 77 million user records. The list of such high-profile breaches is growing at a rate never seen before—a trend which is likely to continue.

*Mikko S. Niemelä is president and CEO of Kinkayo, a Singapore-based cyber intelligence agency. He is also chairman of **Silverskin** and author of **Anatomy of a Cyberattack**.*

*Follow INSEAD Knowledge on **Twitter** and **Facebook***

Find article at
https://knowledge.insead.edu/blog/insead-blog/cybersecurity-the-role-of-the-board-6776

Download the Knowledge app for free

Visit INSEAD Knowledge
http://knowledge.insead.edu