How cyber savvy is your organization?

Harry Raduege
United States
hraduege@deloitte.com
Contact me on LinkedIn

Tse Gan Thio
Singapore
tgthio@deloitte.com
Contact me on LinkedIn

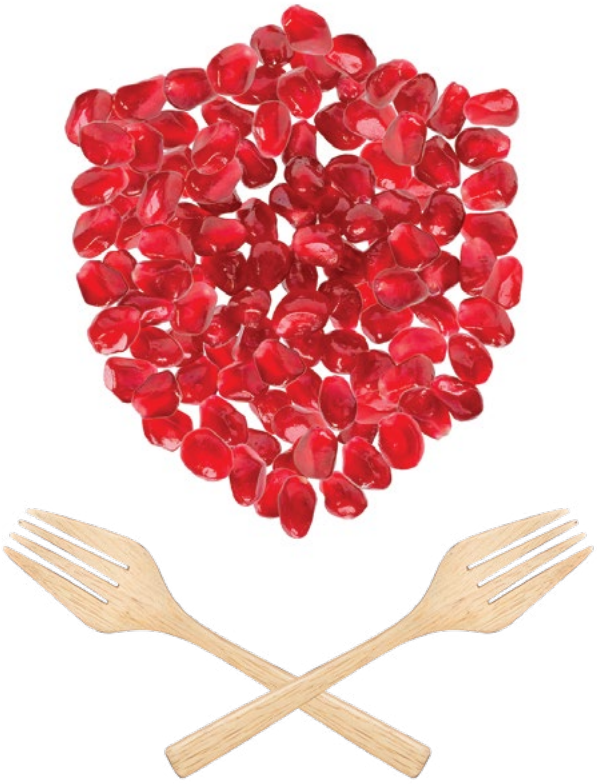
It's no longer a matter of whether a cyber breach will occur; it's when it will occur if it hasn't already. Globally, in the first half of 2015, more than 245 million data records were stolen by cyber hackers every single day—or 16 records per second.[18]

Cyber attacks are becoming more sophisticated and harder to investigate and contain. Advanced Persistent Threats (APT), for example, are low-key attacks that slowly siphon off critical data and are difficult to detect using traditional methods.

Cyber attacks come in various forms:

- **Data breaches**—stealing an organization's data or manipulating it so the organization can no longer trust it.
- **Cyber crimes**—the theft of data, such as credit card information, that hackers use for their own financial benefit.
- **Acts of sabotage**—denial of service or other attacks that literally shut down the organization.
- **Espionage**—attacks on the industrial or economic security of the organization.

Cyber attacks are inevitable, and often the attackers are already inside the organization's network.



In addition to the immediate disruption created by a cyber crisis, a cyber attack often leads to drawn-out litigation, regulatory actions, ongoing operational disruptions, an impaired ability to execute strategy, and increased insurance liability—all of which diminish corporate value. It's not surprising, then, that cyber security is an increasingly important oversight responsibility for directors, and one with personal implications for members of the board. Following some cyber breaches, shareholders have called for the removal of directors or have filed derivative lawsuits against them. Class action lawsuits are also becoming more common following a cyber breach.

The bad news is that the problem is likely to become worse because every organization has a growing number of cyber risks. For example:

- Organizations are linked with others in their ecosystem through their supply chains that, to function effectively, require sharing of information among the ecosystem partners. Each of these links introduces vulnerabilities.
- Cyber espionage and data theft are becoming commonplace in mergers and acquisitions where hackers attempt to gain financial or operational intelligence to use as leverage in the negotiations or to devalue one of the organizations in the transaction.
- Employees often utilize their own personal digital devices to access an organization's data—an entry point whose security depends largely on the cyber awareness and care employees take with their devices both in and out of the workplace.
- A growing number of companies and individuals are taking advantage of the cost-effective and convenient alternative of cloud technologies—something that is equally convenient for cyber criminals and malicious actors.

Building a cyber secure organization

It has been said that an organization's cyber security is only as strong as its weakest employee, since cyber hackers look for naïve, uneducated, or untrained employees to provide them with an entry point into their employer's network.

> Boards need to assume that their organization's information network either has been, or soon will be compromised and they need to realize that cyber security isn't a zero tolerance issue—in other words, attacks will happen despite the organization's best efforts. The key is how quickly and effectively the organization responds to cyber threats and attacks. The board has a key role to play in ensuring that management is building a cyber savvy organization.
>
> –Harry Raduege

In today's environment, with the widespread use of technologies, you can't be a responsible board member and not be concerned about cyber security. Boards need to inquire about the organization's cyber strategy, what information the organization exposes to third partners, and the security of the organization's ecosystem.

–Tse Gan Thio

Hackers will use bogus email accounts designed to look as if they were sent by a friend or co-worker, which, when opened, will upload malicious software (malware) to the organization's networks. Free gifts, such as thumb drives that are generously handed out at trade shows and other events, could also contain malware. Employees who use their digital devices to access unsecure WIFI could unknowingly be giving access to hackers.

In this environment, organizations need to build a culture of data security—a process that should be led by the board and management and needs to involve more than just the IT department. Today, organizations need their entire workforce to be cyber savvy to ensure that they continuously operate in a secure, vigilant, and resilient environment.

Secure—Many organizations have spent significant amounts of time and money on traditional security controls and preventative measures, and most likely that investment will need to be increased in the future. Despite this, it is impossible to protect everything equally.

Organizations need to focus on their "crown jewels"—the mission critical data that they absolutely must protect. Organizations must also know the cyber hygiene of their partners and authorized connections—contractors, vendors, and suppliers—who may be security allies or liabilities. It's important to think in terms of the information supply chain, and decide who will or will not be allowed to access the information network.

Vigilant—Being vigilant means being cyber savvy. Awareness of cyber risks needs to be a priority for everyone within the organization, and for every one of its external partners. Cyber vigilant organizations build, maintain, proactively monitor, and test their cyber defense. When hackers attempt to gain entry or other suspicious events occur, the organization needs to respond appropriately to fend off the intrusion, and also learn from it so it can adjust its business and technology environment accordingly.

Resilient—Inevitably, some cyber intrusions will succeed so organizations need a crisis management strategy and cyber risk management plan that enables them to respond and recover quickly. (See the article on crisis management on page 32.)

Cyber security and the board
Boards of directors need to challenge management's assessment of the organization's cyber posture and critically review the cyber crisis management capabilities that management has put in place.

The board may also want to review its own processes for providing oversight of cyber security. For example, the board may want to expand the charter of the board-level committee responsible for overseeing cyber risk to include how the organization allocates resources in managing cyber risk. Another consideration may be to create a board cyber chair to oversee management's activities and ensure that senior management is appropriately focused on cyber security.

Boards may also want to establish a cyber risk process that defines cyber risk management priorities for the organization and outlines mechanisms of accountability. The board may also want to have access to its own cyber security experts.

Questions for directors to ask

1. What is our organization's cyber footprint? What information do we deliver? What channels do we use to deliver that information? What information do we share with third parties? Are we confident that our supply/information ecosystem is robust enough to protect information and data throughout the chain?

2. How well does the board understand cyber risk? Should the board engage outside experts to educate directors on cyber risk, how to mitigate it, and the signs that might signal a breach? How often does the board receive reports or updates from the people responsible for monitoring cyber risk?

3. What are our "crown jewels"—the critical information that, if compromised, would undermine our organization's ability to continue operations? How do we protect this information?

4. Does our organization have an overall enterprise cyber strategy and cyber risk management plan? Do they have both proactive and reactive components? Has management established working relationships with local law enforcement? Does our management team conduct regular cyber assessments and cyber security scenario planning exercises?

5. Is our organization able to detect a compromise early? What controls have been put in place? How do we know those controls are operating effectively? Have they been validated recently? How many actual breaches have we had, how well did we respond to them, and what did we learn from them?

6. In mitigating our risk, do we have cyber insurance? If so, what is the extent of our coverage?