Cyber risk takes centre stage

A string of high-profile cybersecurity breaches has focused attention on an emerging challenge in the boardroom: are directors doing enough to ensure their companies are adequately protecting sensitive data and technology?

BY JIM MIDDLEMISS

When Doug Hayhurst traveled on company business in the 1980s, the former IBM and PwC executive used a briefcase with no corporate logo when visiting certain jurisdictions so as not to attract attention. Fast-forward to today. Hayhurst, an independent director who sits on a number of boards, including Canexus Corp. (TSX:CUS), says the rule for executives visiting certain high-risk jurisdictions is to travel with a clean computer and a burned cell phone. "Every business has some information. You don't want to be the weak link that opens it up."

Welcome to the new world order—one where organizations of all sizes must increase security measures and lock down the precious data stored in their information vaults to protect it from prying eyes and sloppy employees.

The problem, however, is that data is not a tangible gold brick and IT systems aren't capable of being isolated like a Fort Knox.

The result is that public companies are increasingly subject to revelations about embarrassing and damaging data breaches—and their boards are being held to account for the adequacy of their oversight.

Home Depot breach

The latest to make headlines is Home Depot. On Sept. 8th, America's largest home improvement retailer confirmed that its payment data systems for the U.S. and Canada had been breached, dating back to April.

Interestingly, it wasn't the retailer that first made the information public. A week before official confirmation, cybersecurity expert Brian Krebs, of Krebs on Security, blogged that banks were seeing evidence Home Depot was the source of a batch of new stolen credit and debit card data that was for sale on the Internet.

A short time later, Home Depot confirmed that the attack involved a record 56 million accounts, carried out with custom-built malware that had "not been seen previously in other attacks. The company now estimates costs of $62 million to fix the problem, offset by $27 million in insurance.

More ripples and repercussions are sure to follow, if the experience at Target Corp., which saw 40 million credit and debit cards stolen over a three-week period in 2013, is any indication.

Target's intrusion was traced back to password credentials stolen from a heating, ventilation and air conditioning (HVAC) firm that worked for Target and had access to its systems. And the news rocked Target's board—with calls from proxy adviser Institutional Shareholder Services for director resignations (which never happened)—pummeled its share price, and led to the resignation of its CEO and CIO. So far Target has spent more than $148 million to recover (still short of the $256 million that retailer The TJX Companies, Inc. spent after 45 million of its customer debit and credit cards were stolen in 2007).

The scenarios currently playing out at Target and Home Depot are a director's worse nightmare.

"Cybercrime is very sophisticated," says Deborah Rosati, who chairs the audit committee on Sears Canada Inc.'s board (TSX:SCC) and sits on a number of other boards. "You are always on guard."

Rosati, an accountant and management consultant, says her biggest fear is waking up in the morning to a news-alert about the company that "I wasn't aware of."

Adds Rosati: "At the end of the day you want to ensure that you've got the systems, the processes and the people in place to manage your business and…that you've got monitoring to ensure you are mitigating high-risk areas."

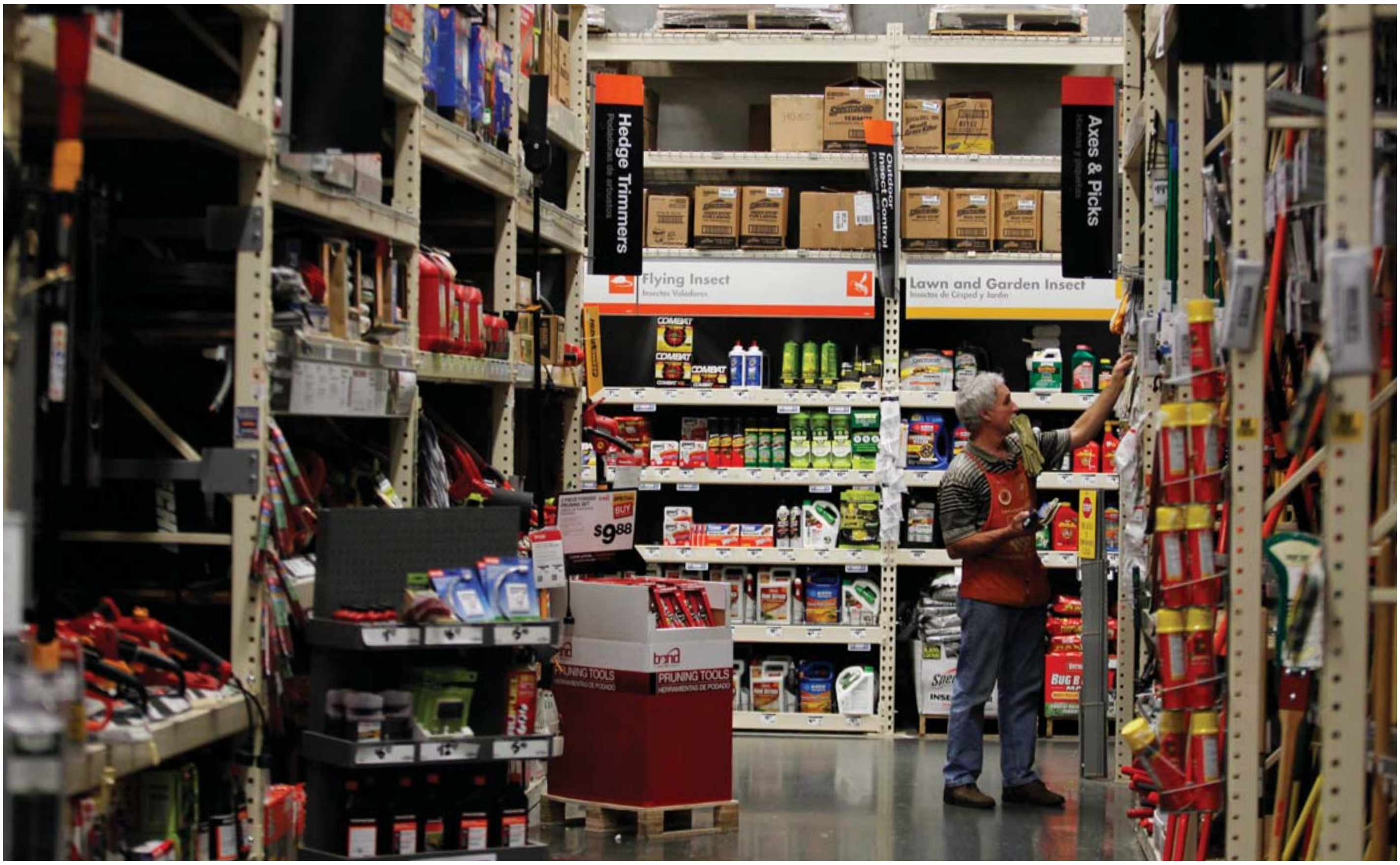
Stakes are high

The cybersecurity stakes are high. Consulting firm McKinsey estimates that "over the next five to seven years, US$9 trillion to US$21 trillion of economic-value creation, worldwide, depends on the robustness of the cybersecurity environment."

The worrisome part is that many boards seem ill prepared for the

Biggest fear: "Cybercrime is very sophisticated," says Deborah Rosati, audit chair at Sears Canada. "You are always on guard."

Photograph: Jeff Kirk



Customers exposed: The recent data breach at Home Depot involved a record 56 million customer accounts

Photograph: Beck Diefenbach/Reuters

challenge. A 2012 CyLab report from Carnegie Mellon University found "boards are not actively addressing cyber risk management." It comes at a time when the report says "corporate data is at a higher risk of theft or misuse than ever before." While boards are focusing on risk management, the study found that "there is still a gap in understanding the linkage between information technology risks and enterprise risk management."

The cost of a breach can be staggering. A 2014 study by the research firm Ponemon Institute of 314 companies in 10 countries found that a data breach costs an average of US$3.5 million per incident, up 15% over last year. The U.S. leads with an average of $US5.85 million per incident (the study did not examine Canada). The probability of having a breach involving a minimum of 10,000 records was 22%.

Ponemon also found brand and reputation declined between 31% and 17% and that it can take more than a year for an organization to recover its corporate image. As well, a breach damages consumer confidence in the company, can lower share price and expose a company to regulatory hearings and class-action lawsuits.

Interestingly, system glitches and careless employees and contractors accounted for 59% of breaches, according to Ponemon, while malicious and criminal attacks made up the remainder. However, criminal and malicious breaches are also the most costly.

Attacks are economic

Larry Clinton, president and CEO of the Internet Security Alliance, which promotes thought leadership and education around cybersecurity, says boards need to rethink the way they approach data breaches.

"People tend to think of it as an IT issue," he says, but "95% of attacks are economic" and the "economic incentives favour the bad guys."

"They are cheap to launch, incredibly profitable, and easy to do."

Moreover, he says, they are increasingly difficult to detect. Advance persistent threats, an effective form of cyberattack usually carried out by nation states, has "moved down the chain and criminals are now doing these things," notes Clinton, who worked with the National Association of Corporate Directors (NACD) in the U.S. to create a cyber risk manual for directors that has been endorsed by the U.S. Department of Homeland Security.

"It's a huge problem and its getting worse," Clinton says of malicious and criminal attacks.

It's not just financial data that is at risk, but everything from intellectual property to business processes are under siege. Part of the problem, he says, is the increasing connectivity of the global economy.

Policies like bring-your-own-device to work, voice-over-internet-protocol phone systems, a digitally connected supply chain all bring efficiencies and lower costs to organizations, but at the same time, they increase the number of doors into an organization that need to be locked down. "It's really hard to secure all this stuff."

And it's going to get worse, he says, as society enters the next stage of the Internet evolution, known as the Internet of Things. That's the creation of a smart grid, where more and more devices, such as fridges or microwaves, will be interconnected and interact with other systems, such as a smartphone.

"It is going to massively increase the number of access points and therefore the number of vulnerabilities."

Even now, director Hayhurst is surprised at the amount of snooping that goes on. “People are trying to go into systems all the time. It happens daily,” regardless of whether a company has customer lists or valuable credit card information, he says.

So what should directors do? Mark Fernandes, cybersecurity leader at Deloitte in Toronto, says there are five key messages directors need to keep in mind when it comes to cybersecurity risk: define it, address it, measure it, execute on a plan to combat it and communicate that plan. “The risk landscape is changing on an hourly, if not daily basis,” he notes.

Manage cyber risk across the enterprise

Directors say the first thing boards need to understand is cybersecurity risk needs to be managed on an enterprise basis and not simply viewed through the IT lens.

“Cybersecurity is just another one of the risks an organization needs to manage,” says Gary Baker, who sits on the board of financial company Libro Credit Union. “The board should be continuously challenging management to make sure what they are doing is appropriate and reasonable in circumstance.”

Rosati notes “not everything is foolproof. It’s about risk mitigation and reputational risk.”

Hayhurst adds: “I don’t put it as a new risk.” Rather, he runs a multi-year calendar for the board’s audit committee that addresses various risks facing the company, including cybersecurity. It usually comes up under IT security and controls or tech advancement.

Regular briefings are also key, says Clinton, since cyber threats can change quickly. But how much is enough? The NACD guide suggests quarterly committee briefings, while the full board should be briefed at least semi-annually.

Where responsibility should lie at the board for overseeing cybersecurity risk remains a bone of contention and it is all over the map.

In some companies, it falls to the audit committee, which is already overseeing financial controls. In others it falls to a full board committee, while at others a risk committee may be assigned the task.

The ISA’s Clinton suggests that a full committee of the board should be in charge because it’s too important to isolate to one committee.

Hayhurst, however, feels that the audit committee is appropriate because it can give the topic a “deep dive and report back intelligently to the whole board. A board can delegate, but it can’t abdicate.”

Challenge the IT assumptions

Mike Strople, president of telecom services provider Allstream, who also sits on the board of the Liquor Control Board of Ontario, warns boards not to be complacent when it comes to cybersecurity risk.

For example, he says, “Firewalls can give a false sense of security.”

“A firewall is not a big stone concrete wall, it has all sorts of holes punched in; it is only if you get all the holes lined up the right way that it does what it is supposed to do.”

He warns: “If the CIO or whoever advises the board says it’s a green check mark or a red X, it doesn’t come in those flavours. It is much more shades of grey.”

Adds Deloitte’s Fernandes: “What often gets overlooked is that insiders are being used as launch pads.” Those looking to gain access will target individuals in a company who might have specific knowledge about new products, or IT systems and security. For ex-

Cyber risk oversight 101

Before directors can provide proper oversight on cyber risk, they must ask management the right questions. Here’s a good list

When it comes to managing cybersecurity risk, there is no shortage of information out there for directors to tap.

“The last three years we’ve seen a lot of investment in cybersecurity,” says Mark Fernandes, cybersecurity leader at Deloitte in Toronto. “Boards are starting to educate themselves.”

One essential theme in the material is the matter of whether or not directors are asking management the right questions about their firm’s exposure to a cybersecurity breach.

Here is a compendium of the top questions directors should ask management, drawn from the National Association of Corporate Directors’ handbook for *Cyber-Risk Oversight*.

Situational awareness

- What are the company’s cybersecurity risks and how is the company managing these risks?
- How will we know if we’ve been hacked or breached and what makes certain we will find out?
- Who are our likely adversaries?
- What is the biggest vulnerability in our IT systems?
- Has the company assessed the inside threat?
- Have we had a penetration test or external assessment? What were the key findings and how are we addressing them? What is our maturity level?
- Does our external auditor indicate we have deficiencies in IT? If so, where?

Corporate strategy and operations

- What are leading practices for cybersecurity and where do our practices differ?
- Where do management and our IT team disagree on cybersecurity?
- Do we have an enterprise-wide, independently budgeted cyber risk management team? Is the budget adequate?
- Do the company’s outsource providers and contractors have cyber controls and policies in place and clearly monitored? Do these policies align with the company’s expectations?
- Is there an ongoing company-wide awareness and training program established around cybersecurity?
- Does the company have adequate cyber insurance?

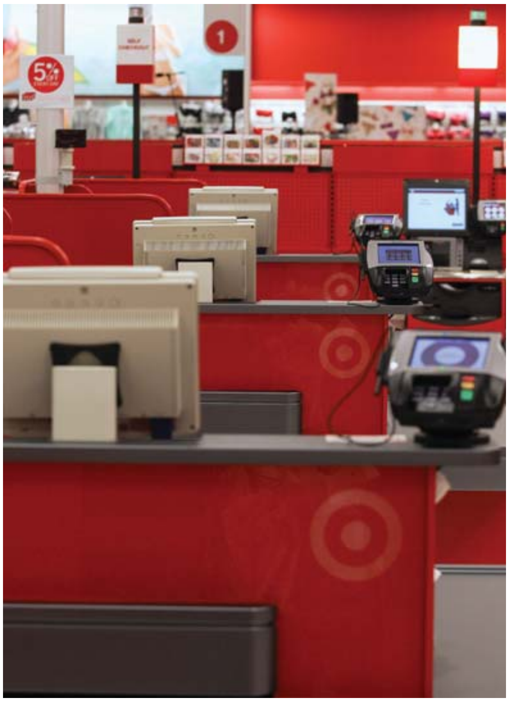
Incident response

- How will managers respond to a cyberattack? Is there a valid corporate incident response plan? Under what circumstances will law enforcement and other relevant government entities be notified?
- What constitutes a material cybersecurity breach and will those events be disclosed to investors?

ample, the advent of social media such as LinkedIn—where people post their business credentials—makes it easy for criminals to target key employees.

Also beware of third parties. One oil company was breached when hackers put malware on a downloadable menu from the local Chinese restaurant that staff often used.

As well, vendors and suppliers pose real challenges. Simply imposing your own security policy onto a vendor won’t work, since they may have 10,000 clients doing the same thing, each of which has different standards. As well, the sophistication levels of a vendor’s IT system may be suspect compared with your own organization. “You have to be real diligent in how you sign up third-party providers,” says Rosati. Understand what your company policies are, she says.



Repercussions: Target’s 2013 breach rocked the board and cost the CEO and CIO their jobs

Photograph: Geoff Robins/Reuters

Make sure you are benchmarking and monitoring

Hayhurst says it is also important to have benchmarking in place so the company knows where it stands in relation to its industry and competitors, which includes examining costs and making sure that the IT department is delivering value. “It may not be the mindset they (IT) bring to everything.”

Rosati adds it is important for directors to understand what basic systems are in place to monitor and protect their companies. So things like policies governing internal password protections and what happens when someone leaves a company to make sure they are not walking off with the passwords and how often a company changes them. “What technologies and what security tools does a company need?” is another area that needs to be examined, she says.

Adam Kardash, a privacy lawyer with Osler Hoskin & Harcourt, urges boards to put in place an incident response protocol as part of an overall “robust network governance framework” that addresses cybersecurity risk.

“The response plan is critical when the cybersecurity incident occurs and you are in a crisis event. The plan outlines the core steps, at a very general level, that the enterprise will take to address the crisis and investigate it to contain whatever has occurred and establish immediate and long-term remediation.”

He says a cross-disciplinary team needs to be established comprising senior management, information technology, legal, human resources, public relations, insurance, key vendors, forensic and people from core areas of the business. Law enforcement officials also need to be contacted.

He adds that the plan needs to be tested in advance of a real event. Little things can stymie it, such as the inability to reach a key person because of lack of contact information. “Once you’re in a crisis, all bets are off. You have to have information at your fingertips.”

Understand legal ramifications

Ross McKee, a corporate lawyer at Blake, Cassels & Graydon in Toronto, says directors also need to understand the legal ramifications of cybersecurity risk.

Regulators in Canada and the U.S. are approaching cyber disclosures differently. The U.S. has been much more prescriptive and in 2011, the SEC issued guidelines on disclosure of cyber risk. For example, companies “should disclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky.”

In Canada, the Canadian Securities Administrators issued notice 11-326 in September 2013 warning companies about cybercrime and advising them to “take the appropriate protective and security hygiene measures necessary to safeguard themselves.”

“Issuers should consider whether the cybercrime risks to them, any cybercrime incidents they may experience, and any controls they have in place to address these risks, are matters they need to disclose in a prospectus or a continuous disclosure filing.”

Ross McKee says while the SEC guidance is “helpful,” the reality is that “people don’t like to talk about security measures very much.”

“The SEC recognizes the challenge public companies face describing risk factors with respect to cybersecurity disclosure without giving away the keys to hackers at the same time.”

Kardash, however, warns that more disclosure is on the Canadian horizon. The next round of amendments to Canada’s *Personal Information Protection and Electronic Documents Act* will include a security breach notice provision, requiring companies to advise the public if their personal information has been compromised. “There will be more reporting,” he says.

Get the right expertise on board

As cyber risk issues become higher priorities for boards, directors say it’s increasingly important that boards have adequate IT expertise. Unfortunately, it’s a subject that can glaze over the eyes of the most adept director.

What constitutes the right skill set is still a matter of some debate. “You need diversity around the board,” Rosati says, and given the profile that IT issues are taking, “there might be an emerging trend to see more competence around that.”

Baker, however, believes that “you need people on boards that understand the business issues associated with IT. They have to understand the business implications of technology and the business risk of the technology. It’s an important distinction.”

Boards would also be wise to seek third-party advice about the vulnerability of their systems, says Hayhurst.

Above and beyond any specific action, however, Hayhurst stresses that the time for boards to act is now. “The hackers are going everywhere. It’s doesn’t matter what business you are in, you are going to be attacked and may be a through point. You cannot afford to be the weak link.”