

Audit committees' role in countering cybercrime

**Audit
Committee
Matters**

Summer 2011



pwc

How can you manage the risk?

Cybercrime in a connected world

While technological innovations continue to create new opportunities for growth through collaboration, they also give rise to new threats — especially the threat of cybercrime. In this rapidly changing environment, audit committees can play a key role in protecting organizations and their intellectual property from cybercriminals.

How great is the risk?

A successful cyber attack could see your systems compromised and key information assets stolen, with a considerable impact on your organization's reputation. Cybercrime is no longer simply the domain of young hackers. Instead, cybercrime is increasingly being committed by a multitude of offenders with diverse motives, including:

- insiders with authorized access to organizational systems;
- corrupt competitors seeking a commercial advantage;
- transnational criminal enterprises stealing data and extorting information to generate income; and
- foreign governments allegedly committing espionage for political or economic gain.

Recently, a number of companies have had sensitive intellectual property stolen, highlighting the risk to companies caused by cybercrime. Over the past eighteen months, there have been many publicly reported attacks against defence, technology and infrastructure organizations — among them companies like Sony, Google and Yahoo. Lesser-known attacks have involved entities such as DuPont, Walt Disney, General Electric and Johnson & Johnson.

In Canada, public and private networks come under attack from sophisticated threats everyday, with a number of cross sector incidents reported regularly. Also of concern is Canada's move from 13th to sixth most popular nation to host cybercrime, according to Websense.

In short, cybercriminals are usually organized, global, highly motivated, sometimes well-funded, and fully immersed in their tradecraft. They are typically patient and with determination can sometimes circumvent the existing control environment without detection. These factors make cybercrime a force to be reckoned with, which may in turn be a matter for the immediate attention of audit committees.

Why is the risk increasing?

The same collaboration tools that are currently helping to boost productivity and fuel business growth are increasingly being misused by cybercriminals to target vulnerable organizations. In particular, the wide adoption of social networking and media sites for both personal and professional purposes has resulted in a large amount of personal and private information being widely accessible. This information can be used to identify and target individuals within companies to circumvent existing information security controls.

Reports indicate that cybercriminals are also becoming more sophisticated and more patient. Transnational criminal enterprises have been known to maintain remote access to a target environment for six to eighteen months before being detected. Our experience suggests that many cyber intrusions result in lingering, unfettered access to systems and information, which in some cases is not detected. When intrusions are discovered, recognition does not typically come via in-house technology, processes, or people, but through third-party tipsters such as domestic law enforcement agencies, intelligence sources, customers or business partners.

When foreign governments, organized crime, or hackers target an organization, the techniques they use to compromise the network and enable sensitive data theft are usually well planned and methodical. Cybercrime and those who commit it are always evolving, with a focus on accessing sensitive information and maintaining persistent remote access for as long as they possibly can.

Recent large-scale data breaches have cost companies well into the hundreds of millions of dollars. Breaches also create the potential for litigation or regulatory investigations when customers' personal information is compromised. As a result, breaches can have a significant and potentially devastating impact on a company's reputation or financial position.

Are you ready to manage the risk?

1. Is the threat of cybercrime on your corporate risk register and discussed in your audit committee meetings?
 2. Do you know how many security incidents have occurred in the past year, and the nature of those incidents?
 3. Do you check computers, phones and other devices belonging to your board members or executives for tampering and malicious software both before and after they travel to high-risk countries?
 4. Do you have a security strategy and governance approach that is aligned with your business strategy?
 5. Do you have an incident response plan for cyber security issues and has it been tested?
-



What role should boards and audit committees play?

Traditionally, boards have tended to regard the security and integrity of their corporate data as a matter for the IT department. Now, however, the increasing threat and the rising impact of online security breaches mean that the prevention and detection of cybercrime should be a consideration for a board's agenda.

As well as the risk to the organization as a whole, board members and executives need to be educated about the risk to their own personal devices when travelling in and out of high-risk countries for business. There have been incidents where business executives have had their laptops removed from hotel safes and tampered with. There have also been examples of senior executives having malicious software installed onto their computers without detection.

While the risk is significant and growing, it is not unmanageable. With careful planning and the right advice, audit committees can play a crucial role in overseeing their organization's response to the risks of cybercrime.

How can audit committees help combat cybercrime?

- *Become informed about cyber issues. Ask for an introductory training session on cyber security.*
- *Understand the trends in your industry and your organization. Law enforcement agencies, security companies, and public-private sector information sharing organizations regularly publish information on cyber attacks.*
- *Establish an information security council that draws together the expertise of your information security, legal, risk and compliance teams. Foster an ongoing dialogue within your organization to discuss the threats facing your company and industry.*
- *Establish an incident response plan and test it periodically. Ensure that the company is able to act quickly if there is a security issue. The first 48 hours after an incident are critical.*
- *Establish clear guidance on what kinds of incidents need to be reported to the audit committee and the reporting timeframe.*
- *Cyber investigations require special skills and expertise. Ensure that a third-party specialist is available to be on-site within 48 hours of an incident to help determine whether your organization can prevent sensitive data from leaving your system and to minimize business disruptions.*

Additional thought leadership

You may find these other PwC publications helpful in your role as an audit committee member:



A Canadian perspective on the 2011 state of the internal audit profession study

With CEO confidence in growth returning in the wake of the global economic downturn, business executives are shifting their attention from crisis prevention and cost effectiveness to innovation, growth and bridging the skills gap.

www.pwc.com/ca/iastudy2011



2011 State of the internal audit profession study

Our 2011 study examines how internal audit is responding to a changing risk environment.

www.pwc.com/ca/iastudy2011



World Watch

Gain insight into the latest developments and trends in governance, financial reporting, broader reporting and assurance with our international publication, *World Watch*.

www.pwc.com/worldwatch



A Matter of primary importance: Making the most of audit committees in primary and secondary education institutions

This paper sets out a series of leading and emerging practices to assist school boards and other education institutions establish and implement effective audit committees.

www.pwc.com/ca/amatterofprimaryimportance

Who to call

Brenda Eprile
National Risk Leader
416 869 2349
brenda.j.eprile@ca.pwc.com

David Forster
Leader, DirectorConnect program
Managing Partner, GTA
416 869 8722
david.forster@ca.pwc.com

Salim Hasham
Associate Partner, Technology
Consulting, Security
416 365 8860
s.hasham@ca.pwc.com

Matthew Wetmore
National Internal Audit Leader
403 509 7483
matthew.b.wetmore@ca.pwc.com

Vancouver

Jane Butterfield
Partner
604 806 7519
jane.butterfield@ca.pwc.com

Karim Mahedi
Director
604 806 7233
karim.m.mahedi@ca.pwc.com

Calgary

Arun Gupta
Director
403 509 7597
gupta.arun@ca.pwc.com

Edmonton

Alexander Hilsbos
Director
780 441 6774
alexander.hilsbos@ca.pwc.com

Winnipeg

Gerry Valois
Director
204 926 2455
gerry.valois@ca.pwc.com

Toronto

Mike Harris
Partner
416 941 8256
mike.harris@ca.pwc.com

Dorothy Sanford
Partner
416 869 2353
dorothy.a.sanford@ca.pwc.com

Kseniya Babushkina
Director
416 941 8466
kseniya.babushkina@ca.pwc.com

Issa Habash
Director
416 365 8840
issa.g.habash@ca.pwc.com

Liane Kim
Director
416 815 5268
liane.kim@ca.pwc.com

Peter Koch
Director
416 814 5899
peter.koch@ca.pwc.com

Ottawa

Darren Budd
Director
613 755 5659
darren.b.budd@ca.pwc.com

Montreal

Josée St-Onge
Partner
514 205 5159
josee.st-onge@ca.pwc.com

Kelly Ohayon
Director
514 205 5146
kelly.ohayon@ca.pwc.com

Saint John

Janet Rieksts-Alderman
Director
506 653 9459
janet.a.rieksts-alderman@ca.pwc.com

Your PwC Ireland contacts...

Mike Sullivan
Partner
Phone: +353 (0)1 792 6450
Mail: michael.m.sullivan@ie.pwc.com

Bob Semple
Partner
Phone: +353 (0)1 792 6434
Mail: bob.semple@ie.pwc.com

Andy Banks
Director
Phone: +353 (0)1 792 6804
Mail: andy.j.banks@ie.pwc.com

Yvonne McBain
Senior Manager
Phone: +353 (0)1 792 8722
Mail: yvonne.mcbain@ie.pwc.com

www.pwc.com/ca/internalaudit
www.pwc.com/ca/directorconnect