

Getting serious about cybercrime

Awareness of cybercrime has never been higher but unfortunately the bad guys still appear to be winning. Organisations need to rethink the way they deal with digital threats to protect their data, make them a more difficult target and ensure they are safe to do business online.

May 2014

Cybercrime is pervasive, expensive and on the rise. The total cost of cybercrime to the global economy is \$110 billion a year, and climbing.

The latest findings from PwC's Global Economic Crime survey show that more than one in four organisations have reported a cybercrime in the last 24 months. But experts suggest the real numbers are much higher and that virtually every major organisation has been attacked.

There are two types of organisations in the world – the ones that know they have been breached and the ones that do not.

So what are businesses doing – or not doing – in response to this growing issue? And why do they appear to be losing?

The biggest hurdle to effectively tackling cybercrime is that executives still largely see it as a technology problem.

Cybercrime is not primarily about technology. It is actually a business problem because it involves systems, processes and people. And people are the weakest link in the chain.

Most CEOs will rely on the assertions from their CIO about the strength of the organisation's firewall. But it does not matter how strong your wall is if the people in the business are vulnerable.

A historical example can be used to illustrate this point.

The Great Wall of China was strong too. But it was breached by enemy soldiers bribing lazy or corrupt guards to leave doors open. The enemy was simply allowed to walk through. The same applies today—a firewall is useless if someone within the organisation lets outsiders in.

There are a number of techniques that cyber criminals use to walk through an organisation's 'digital front door'. Sometimes people knowingly let them in but in many cases they are tricked or coerced.

One popular method currently is 'spear phishing'. This is similar to the email scams of old, but is much more sophisticated and targeted.

Cyber criminals will specifically single out a high profile individual and send them an email that appears to be from someone within the business. Or it may be from a contact they have identified through your LinkedIn or Facebook profiles. But the email carries with it a malignant payload that can scan your laptop for passwords, credit card details and sensitive business information.

In other words, this type of cybercrime relies not just on technology, but on familiarity and people's natural tendency to trust those they know.

OSHI: Know your cyber crooks

An easy way to remember the different types of people likely to commit cybercrime.



Organised crime groups: looking for cash or information to sell. Bribe, scam or extort their way in.



State-sponsored groups: looking for business or security information. They gather company data for months before it is detected.



Hacker: varied motives, but often social or environmental in nature. Disruption is generally their aim.



Internal: one of the biggest risks. Might be disgruntled or dishonest employees, or working under threat from criminals.

Who's attacking us?

Effectively dealing with cyber risk means firstly, understanding the different types of cyber criminals as well as their particular motives and preferred methods.

We have identified four main types of cyber criminals: organised crime gangs, state-sponsored groups, hackers and insiders. We have coined the term OSHI for this group of cyber criminals.

Organised crime groups typically look for cash or information to sell and go after credit card details or personal information. They will often target and blackmail high-level executives using spear phishing techniques. They have also been known to steal company IP and sell it to competitors.

State-sponsored groups are quite different. They are looking for business or security information – passwords, strategic plans, pricing, M&A activity – that might advantage businesses in their country. They might install software that sits in the background monitoring your activity or gathering data for months before it is detected.

The term **hacker** refers to activists that use computer hacking to further their aims. This group is particularly difficult to deal with as their motivations are varied. They might have a specific social, environmental or political agenda, or they may just be trying to be a nuisance. Typically their goal is to disrupt or disable your organisation's digital network.

Internal threats are one of the most dangerous as your own people hold 'the keys to the gate'. And it's not just the disgruntled or dishonest that pose a threat: crime gangs often target vulnerable employees then bribe or extort them to carry out cybercrimes from within an organisation.

Rethinking your approach

While there are specific tactical ways to deal with each of these threats, the real challenge for executives is to take a holistic, business-based approach to cybercrime.

This means firstly elevating cybercrime above the IT division and incorporating it into your whole-of-organisation risk management framework.

One of the most important questions a CEO can ask is: who's in charge of cyber security? If the answer is only the CIO, then you may have a problem.

Cyber security is a fundamental part of risk management. It should operate across the breadth of the organisation and report directly to the top

The other critical element of cyber security is thorough planning and preparedness.

Plan ahead, plan thoroughly and review your plan regularly because you will come under cyber attack.

Importantly, the plan should consider a range of scenarios and questions that go beyond technical responses to a cyber attack.

For example, have you thought about your fiduciary duties to shareholders? Do you need to inform the regulators or issue a trading halt? What do you need to tell customers? Will the media be interested? If you are in an M&A situation, when do you need to inform the target board? What is your escalation plan? It is critical that you think about these things before a cybercrime occurs.

What you need to know

Cybercrime is  pervasive, **expensive** and on the rise 


 **1 in 4** organisations globally reported that they have experienced cybercrime in the last 24 months

\$110bn is the annual cost of cybercrime to the global economy

243 is the average number of days that malicious monitoring software can be on your system before it is

 **Detected**

Cybercrime is not just about technology, it is a **business problem** and involves **systems, processes and people.**



Where to from here?

Cybercrime, unfortunately, is a price we pay for the tremendous benefits and opportunities presented by the exploding digital economy. And just as organisations have adjusted to risks in the past, so too can they adapt to the new and growing risk of cybercrime.

But it will require a revision of our current thinking. Business leaders need to:

- lift cyber security out of the technology department and into the executive team and boardroom
- know your cyber criminals – OSHI
- set the tone from the top and determine how cyber security fits with strategy and culture
- plan ahead, plan thoroughly and review plans regularly
- ensure plans are aligned across the organisation
- share information about what incidents are occurring and how they are responding.

Cyber security is everyone's business.

Contact us

Greg Unsworth
greg.unsworth@sg.pwc.com
+65 6236 3738

Chan Hiang Tiak
hiang.tiak.chan@sg.pwc.com
+65 6236 3338

Yong Jiunn Siong
jiunn.siong.yong@sg.pwc.com
+65 6236 7238

Mark Jansen
mark.jansen@sg.pwc.com
+66 6236 7388

Tan Shong Ye
shong.ye.tan@sg.pwc.com
+65 6236 3262

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PwC does not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.