Five top cyber tips for risk managers

AIG

ASIA INSURANCE REVIEW

Five top cyber tips for risk managers

Cyber risk threats are increasing, and with more and more reports of cyber-attacks and organised crime moving into this arena, companies cannot take these threats lightly. **Mr Matthew Clarke** from **AIG** shares five tops tips on managing these cyber risks threats.

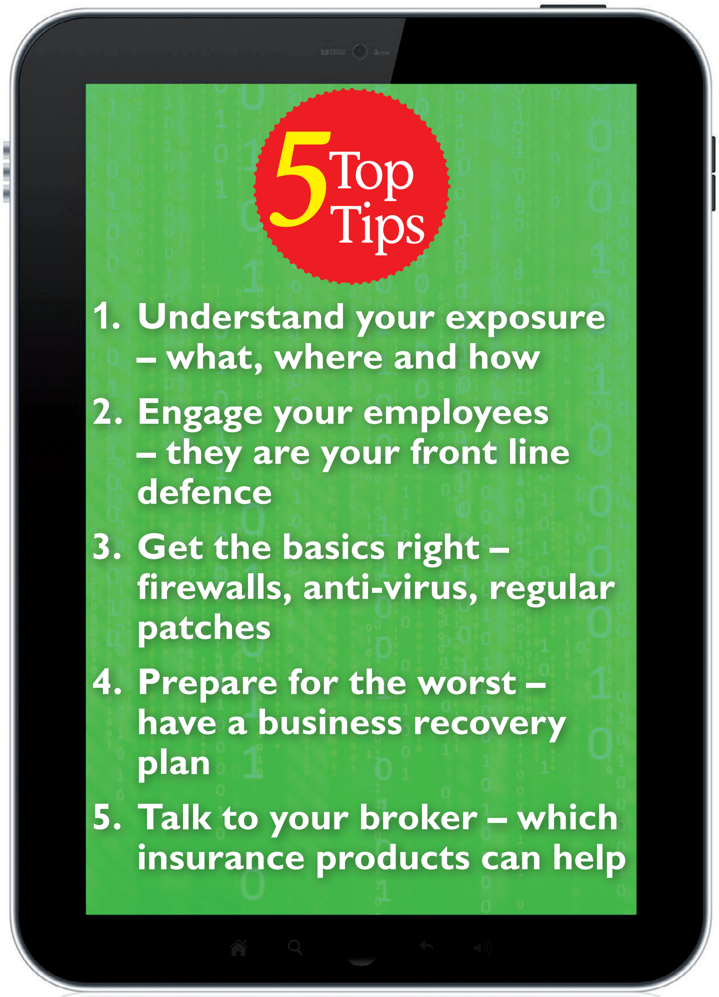
News reports from around the world are awash with stories of cyber-attacks and identity theft. Governments warn that the wars of the future will be fought online; some commentators argue the shift has already happened.

Organised crime has moved from the back streets of cities to the boulevards of cyberspace. Criminal gangs take advantage of the business advantages of the internet: economies of scale, global reach, and instantaneous access.

A brave new world

Add to these new realities the changes in privacy legislation being implemented around the world and you may be left wondering how businesses can possibly operate successfully.

So what can you do to stay ahead of the game? Here are my five top tips to help your company get ready to manage its cyber risks.



5 Top Tips

1. Understand your exposure – what, where and how
2. Engage your employees – they are your front line defence
3. Get the basics right – firewalls, anti-virus, regular patches
4. Prepare for the worst – have a business recovery plan
5. Talk to your broker – which insurance products can help

1. Exposure awareness

The most important action you can take is the simplest: understand your exposure.

Do you keep personal information about your clients or staff? Do you keep credit card or banking details of customers or suppliers? Do you have sensitive corporate information you would prefer to keep confidential?

This is the information that cyber-attackers seek to steal; if your company holds this information, it is a possible target.

Once you have identified what data may be targeted, you then need to consider how and where it is stored and maintained. Is it on a local server in the office? Is it stored in a company server in a remote location? Has it been outsourced and placed in the cloud? And if it is in the cloud, where is that cloud physically (and legally) located?

Your answers to these questions will allow you to understand the physical, technological and legal environment in which your data resides. For example, a Singaporean company using a cloud computing platform to drive marketing activity may actually have its data residing in Canada. You need to know the implications of such a situation.

2. Employee buy-in

Your employees are at the forefront of your operations and are often the first to identify an issue. By training them to use data and business systems responsibly you can create one of the most effective protections to cyber threats.

The ability of any business to manage its data is only effective if its employees understand and commit to their roles as responsible users and custodians.

A recent report by Verizon highlighted that employees are the second largest group responsible for data breaches and cyber-attacks. This includes malicious attacks from disgruntled employees as well as misuse, errors and accidents.

However it is not just the employees who need to engage with a culture of cyber risk management. As the now-infamous "mega breach" of US retailer Target highlighted, the financial impact of a cyber-attack can be significant and as such there is an obligation on directors and senior management to actively manage those exposures. Both the CEO and CIO of Target have left the business in the aftermath and the company faces a daunting array of law suits over the matter.

Cyber risk is no longer a problem for Risk Managers and IT Departments – if it ever was. It is an issue for your Board.

3. Getting the basics right

A recent report from IBM found that 49% of all attacks committed that year were opportunistic. By taking basic risk management steps, you can dramatically reduce the likelihood of falling victim to an opportunistic attack.

July 2014 www.asiainsurancereview.com

"Doing the basics right" means ensuring that as a minimum, your company deploys anti-virus software, installs firewalls and most importantly, encrypts your data whether mobile or "at rest". Furthermore, you need to ensure your software is kept up to date with patches, updates and the latest releases.

In some ways this is akin to locking the doors and windows of your house when you leave. You won't stop a determined burglar, but you will deter the opportunistic chancer looking for quick win. Sometimes, that's enough.

4. Business continuity planning

Most businesses have continuity plans in place to manage the consequences of physical threats such as flood or fire. It is equally important to consider how your business would operate if you could not access your computer systems, or your customers lost trust in the security of your credit card terminals.

Incorporating cyber risks into your business continuity plans, and updating them frequently, is a critical element of cyber-readiness. Much of the costs that are incurred with a breach come some time after the breach. By having a robust plan in place, you can minimise the consequences and accelerate your recovery.

5. Getting expert advice

Finally, talk to an expert to ensure you cover all aspects of cyber-risks. Be it your insurance broker, an IT security adviser or a specialist PR consultant, consider bringing in independent third parties to help you understand your risks.

Your risk management toolkit should include consideration of comprehensive cyber liability insurance to further minimise the impact of a cyber-attack on your business.

These policies are not designed as a replacement for good risk management; rather they provide an important safety net in the event that a breach occurs. You should also consider looking for a partner who can scan the environment on your behalf, providing updates, alerts and training where necessary.

The best defence…

Developments in cyber risk threats and protections are moving at breakneck speed. As you explore your options, you should ensure that you engage with advisers and risk carriers who can provide immediate incident response services, access to qualified IT security experts, advice on media relations post-breach, and a continuing flow of new covers and services.

Cyber threats are not going away any time soon; indeed they are likely only to increase. At AIG we are proud to be one of the leading innovators in the field of cyber insurance, offering an array of products, covers and services including our unique CyberEdge ™ app. With support like this behind them, we believe our clients can face the future with confidence. Bring on tomorrow.

Mr Matthew Clarke is AIG's Asia Pacific PI and Cyber Manager. For more information on AIG and its products and services, visit www.aig.com.

CyberEdge® insurance solutions keep you ahead of the curve.

Your company's information is at risk every day. And every day, that risk increases. Since 1999, AIG has been introducing advancements in cyber risk management. Today, our AIG CyberEdge app offers real time updates on data breaches, plus our proactive risk mitigation tools address network security, training and compliance to provide an additional layer of defense. Let us add our expertise to yours so you can stay ahead of the curve. Learn more at www.AIG.com/cyberedge

AIG

Bring on tomorrow

@AIGinsurance

Download on the App Store

All products and services are written or provided by subsidiaries or affiliates of AIG APAC Holdings Pte Ltd. Products or services may not be available in all countries, and coverage is subject to actual policy language. For additional information, please visit our website at www.AIG.com