AXIS INSURANCE GROUP

Cyber Risks Insurance

Insurance for Network Security & Data Protection

Identity theft, hacking, anonymous cyber-attacks, phishing, spam. The list of technological threats is a long one. It seems no matter how sophisticated or useful the technology, there are unscrupulous people the world over who are willing to exploit it for nefarious purposes. But it isn't only deliberate exploitation which threatens companies. Sometimes mistakes happen. Laptops left in taxis, data files which should have been encrypted, or a harmful email opened by mistake– these can cause tremendous headaches for companies. Mistakes or deliberate harmful acts in the technological arena can be costly to a company and brand, both financially as well as to its reputation.

Axis Insurance Group
#400 - 555 Burrard St. Box 275, Vancouver, BC, V7X 1M8
Toll Free 800.684.1911 | Fax 604.331.0662 | axisgroup.insure

Cyber Risks Insurance

Insurance for Network Security and Data Protection

Executive Summary

This paper explains some of the risks in detail and provides pertinent information and solutions to help protect your business from cyber risks.

It's no secret that the world of information technology is changing rapidly. But It isn't just new technologies like social networking or cloud computing that are changing. Software, content and products are also developing, and their influence can be seen in the service sector along with processing, consulting and outsourcing. These charges have led both to a shifting legislative landscape as well as a much more sophisticated criminal underworld.

According to the national non-profit Identity Theft Resource Center (ITRC), in 2010 some 16 million confidential records were exposed through more than 662 reported security breaches. One of the most high profile cases was that of Sony Computer Entertainment America. The company reported a security breach of its PlayStation Network in which hackers obtained personal information on some 100+ million subscribers. The breach resulted in a security investigation so broad it suspended business operations, and faced multiple class action lawsuits costing up to an estimated $2 billion.

Honda Canada issued a warning that a data breach exposed the personal data of somewhere in the region of 280,000 customers. And a few years ago the confidential tax files of almost 2,700 Canadians went missing after a Canada Revenue Agency worker took them home and let a friend download them onto a laptop. And in the U.S., an employee of Fannie Mae was alleged to have been attempting to sell handwritten copies of the financial information of approximately 1,100 people.

The study by the ITRC showed that the most frequently breached sectors are healthcare and financial services and the average cost per breach was $2.4 million, with the majority devoted to legal services. It is can be daunting to imagine what kind of impact costs like that can have on a business.

Classification of Risk

Cyber risks, or risks related to technology fall into two broad categories – data protection and operational.

In the area of data protection, there are many risks. Some are familiar, such as the loss of data – either in error or for malicious purposes. But other risks include contractual liability, for example when a company has outsourced data or information technology and includes data protection in their contracts. However, other risks can be from regulatory enforcement – which changes rapidly, or damages and lawsuits following a breach. And the risks from a data breach can be costly too – not just in compensating individuals who have suffered identity theft. There can be a wide range of costs relating to forensics, notification and credit monitoring following a security breach. All of these risks can have a direct impact on your company's customer base – and your reputation. In the operational arena, there are risks related to first party protection for critical assets – such as your network, data, applications, software etc. Additional risk comes from the vital importance of network availability and the protection of your digital assets. If things go wrong, there is the very real risk that your business will lose both income and customers.

Axis Insurance Group
#400 - 555 Burrard St. Box 275
Vancouver, BC, V7X 1M8
Toll Free 800.684.1911
Fax 604.331.0662
axisgroup.insure

Cyber Risks Insurance

Insurance for Network Security and Data Protection

Data protection - Security and Privacy

When people think of data protection, they often think of how their data can be used inappropriately. However, there are two areas which are covered by data protection – security and privacy.

Security

Security encompasses data protection issues where someone (for example an employee, associate, vendor, or independent contractor) attacks or accesses your computer network in an unauthorised manner. It can also refer to stolen hardware, like a smartphone, laptop, USB stick, or paper records, to perpetrate data theft.

Privacy

Privacy, again part of the data protection arena, relates to the violation of privacy laws and regulations which permit individuals to control the collection, access, transmission, use and accuracy of their personally identifiable information (PII), personal health information (PHI) and/or personal financial information (PFI). Additionally, businesses should also consider voluntarily notifying individuals when their data is lost, not just when a privacy law or regulator mandates it, to reduce the negative impact the company's reputation.

Company directors also need to understand that they and their company are not only exposed to data protection regulation in their home jurisdiction, but also where the data subject resides and where the breach occurred as well – increasingly complicated in the new age of cloud computing.

The distinctions between security and privacy help when considering what kinds of technological or cyber risks your company might face – either now or in the future. Cyber risks encompass a multitude of requirements which aren't always consistent with each other. Therefore trying to find a one response fits all solution could trigger yet further liability. It is always wise to take legal advice on the appropriate response to a situation, as well as having the right insurance coverage in place.

Axis Insurance Group
#400 - 555 Burrard St. Box 275
Vancouver, BC, V7X 1M8
Toll Free 800.684.1911
Fax 604.331.0662
axisgroup.insure

Cyber Risks Insurance

Insurance for Network Security and Data Protection

Risks Related to Data Ownership

As owners of data it often helps companies to know what the kinds of risk they face are – and from whom or from what those risks arise. According to recent research, hackers caused 32% of breaches and were responsible for 75% of all exposed records. Malicious activity by rogue employees (usually caused by firing, downsizing, poor economic conditions and the relative ease of selling stolen information) accounted for 19% of breaches. Finally loss or theft was also found to be a leading cause of data breaches. Meredith Schnur, Vice President, Professional Risk Group, Wells Fargo Insurance Services, said: "In the last six months, we've had six to ten data breach claims reported from lost thumb drives, missing laptops and missing hard copy reports."

And the research also demonstrates that more than 60% of breaches occurred in financial services, healthcare and retail. In fact, 88 percent (122 million) of records exposed occurred in financial services alone. The kinds of data protection breaches usually involve financial espionage or financial crime as well as identity theft – particularly personally identifiable information (PII) and personal health information (PHI).

Data owners are also vulnerable to email hacking – and there have been some very high profile cases – Sarah Palin in Alaska, the Prime Minister of Australia and numerous celebrities. But often these breaches aren't made public and the lack of publicity can mask the scope of hacking operations, which is fast becoming a lucrative industry for the criminal underworld.

Another area of risk, and one that has been on the increase in recent years, is the transmission of malicious code (viruses). Although many computers and servers are protected with proprietary software, the creators of viruses are very creative and as soon as one door is closed, they write code which exploits other vulnerabilities within a system.

And the threats come from inside an organization too. For companies it is vital to have strong access controls, file retention and password protection as well as physical safeguards (for example storing files and/or servers in a locked room) as inappropriate access can trigger a breach of data protection regulations.

The final area which data owners have to be vigilant against is a denial-of-service attack (DOS). A DOS attack is, according to various definitions, the attempt to make a computer resource unavailable to its intended users. There are many ways this can happen, but most of them relate to a computer system being bombarded with requests or emails, which force it to run incredibly slowly or crash. There are legion examples of this happening – a recent high profile case being when the Metropolitan Police in London foiled a DOS attempt on the official Royal Wedding website for Prince William and Kate Middleton.

Handling a breach can be expensive. Research has shown that the average expenses per breach for crisis services were about $200,000 per service (forensics, notification, credit monitoring, and legal counsel), while legal damages ranged between $450,000 and $1,000,000.

Axis Insurance Group
#400 - 555 Burrard St. Box 275
Vancouver, BC, V7X 1M8
Toll Free 800.684.1911
Fax 604.331.0662
axisgroup.insure

Cyber Risks Insurance

Insurance for Network Security and Data Protection

Operational risks

So what are the kinds of risks that are related to data protection? And how can they affect your business? Without getting too deep into insurance jargon, one of the biggest areas of operational risk is known as non-physical business interruption. Non-physical business interruption is when your normal everyday business cannot continue because of an event which is out of your control and closes or curtails your business. It can be caused by a range of technological-related factors such as software failures or operational mistakes. And it doesn't take much to imagine your business being interrupted by events such as malicious code, denial of service attacks, eVandalism or similar malicious acts.

Coupled with non-physical business interruption is contingent business interruption. In simple terms, it means that if things go wrong for your company, they can also have an effect on others, such as suppliers or customers. In other words, your interruption of business may well cause others to lose profits and or create extra expenses for them. And that also relates to your co-dependency with another vendor's infrastructure. An example of this is if you have outsourced your business processing or information technology.

A final operational risk is one of extortion. How would you deal with hackers who stole your data and held it ransom? This is a frightening and potentially costly scenario.

Regulatory environment

The regulatory environment is constantly changing. It varies from country to country and sometimes jurisdiction to jurisdiction. However, in Canada privacy laws are enshrined in various acts including the 1983 Privacy Act. Data protection can be covered by several acts of law, depending on the relevant legislation. For example, Data Protection is covered by the Food and Drug regulations and protects drug manufacturers and pharmaceutical companies.

Canada does not have a privacy minister – however it does have an Office of the Privacy Commissioner. This office was created in 1977 under the Canadian Human Rights Act, Part IV. The Privacy Act currently governs the functions of the Privacy Commission.

As an Agent of Parliament, the Privacy Commissioner oversees compliance with both the Privacy Act, which covers the personal information-handling practices of federal government departments and agencies, and the Personal Information Protection and Electronic Documents Act, Canada's private sector privacy law. The mission of the Office of the Privacy Commissioner of Canada is to protect and promote the privacy rights of individuals.

Axis Insurance Group
#400 - 555 Burrard St. Box 275
Vancouver, BC, V7X 1M8
Toll Free 800.684.1911
Fax 604.331.0662
axisgroup.insure

Cyber Risks Insurance

Insurance for Network Security and Data Protection

Impact of risks

As we've seen, the impacts on a business from cyber risks can be enormous. There are four main areas to consider:

1. Financial Risks - This covers areas like the costs of notification, public relations and associated media costs and the costs of forensics. It doesn't include the cost to your business of lost revenue and lost customers.
2. Litigation and Regulatory Exposure - It's not just the financial costs which can hit your business. Imagine having to deal with lawsuits and legal fees. Then there are the costs of damages or settlement, working through any regulatory investigations and the costs of any fines or penalties. Damages can be considerable depending on the sensitivity of the data – for example, healthcare information is particularly sensitive, and can result in heavy litigation if lost.
3. Brand Equity - While this might be a difficult cost to quantify and might seem intangible, the damage to your business's reputation could be immense. Not only will you face a barrage of bad publicity, but your image, goodwill and customers' trust could be severely damaged.
4. Assets - The final area of your business which is impacted by cyber risks is that of your core assets – items like software, data, trade secrets and IP rights.

Taken in isolation, each area of risk impact is daunting enough. But when things go wrong, either through negligence or malicious acts, the impact on your business can be wide ranging and devastating. That's why it pays to consider all the issues and act before it is too late.

Axis Insurance Group
#400 - 555 Burrard St. Box 275
Vancouver, BC, V7X 1M8
Toll Free 800.684.1911
Fax 604.331.0662
axisgroup.insure

Cyber Risks Insurance

Insurance for Network Security and Data Protection

Traditional Insurance is not Enough

Many businesses believe that their traditional insurance policies will cover them. That just isn't the case. Take crime insurance as an example. It is limited to money, securities and "tangible assets" and there must be a "loss" and a "gain" to trigger cover. That's difficult to do when you're dealing with information technology and data protection. It also requires the identification of a perpetrator – nearly impossible in the online world. A hacker is adept at covering their tracks and part of their stock in trade is to hide their identities. Crime insurance also doesn't include any element of coverage against a business's lost income.

Then there's general liability insurance. That doesn't help either. There is no first party cover, it's strictly third party. And more often than not, the policy will have geographical limitations – again posing a problem for cyber crime. Also general liability insurance is triggered by negligence, and does not provide any contractual privacy cover. A cyber policy will cover an event where the privacy policy of the company is compromised.

Property insurance coverage won't help much either. It doesn't usually cover damages or losses caused by computer viruses and will only cover consequential business interruption – but that is only following a physical damage event. There is no cyber extortion coverage with property insurance and the perils covered will only include fire, wind or water.

Even if a case can be made for some cover under other types of insurance policies, it is important to question whether the coverage is intentionally there. In other words, has that particular coverage been underwritten? Unless it is specifically addressed, it is difficult to know how a particular event would be treated under a policy. For example, would a hacking event over several days that impacts multiple individuals be treated as one event and therefore only one retention apply, or would they be treated as multiple events? That's why you should never assume you have coverage under other insurance policies and protect yourself with appropriate cyber risks insurance.

Axis Insurance Group
#400 - 555 Burrard St. Box 275
Vancouver, BC, V7X 1M8
Toll Free 800.684.1911
Fax 604.331.0662
axisgroup.insure

Cyber Risks Insurance

Insurance for Network Security and Data Protection

As with every insurance policy there are different options, policy wordings, enhancements or amendments available. Your Axis Insurance manager will be able to help create a bespoke policy to suit your requirements exactly..

Axis Insurance Group
#400 - 555 Burrard St. Box 275
Vancouver, BC, V7X 1M8
Toll Free 800.684.1911
Fax 604.331.0662
axisgroup.insure

The Right Protection with the Right Insurance

The good news is that there are now solutions to cover all the aforementioned risks. There are two main types of coverage – data protection and non-physical business interruption insurance. A brief outline of each product follows, but the specialist and expert team at Axis Insurance will be able to give you much more detail and explain how the policies can be tailored specifically to your business.

Data protection cover

This specialist insurance product has four main areas of coverage. Each one is explained below:

- Network Security Liability - This covers the liability and defence costs for claims arising from computer attacks caused by failures of security including identity theft, negligence and so on. It also covers losses and damage from the transmission of computer viruses and denial of service attacks.
- Privacy Liability - This element of the policy covers the damages awarded as a result of a data breach.
- First Party Costs - This covers the costs associated with notification, forensics, public relations and media management as well as credit monitoring costs. It will also cover costs related to regulatory investigation, civil fines and/or penalties.
- Multimedia Liability - The final element in Data Protection Insurance covers advertising and intellectual property perils arising from content in electronic and non-electronic media.

Non-physical business interruption cover

This second insurance product which would assist with covering losses from a cyber peril would be non-physical business interruption insurance. This would cover three specific areas of loss:

- Data/Electronic Information Loss - The insurance policy would covers the cost of recollecting or retrieving data destroyed, as well as data which had been damaged or corrupted due to a computer attack
- Business Interruption or Network Failure Expenses - This part of the policy covers the cost of lost net revenue and extra expense arising from a computer attack and other human-related perils. This is particularly valuable for computer networks with high availability needs.
- Cyber-extortion - Finally, a Non-Physical Business Interruption insurance policy would cover both the cost of investigation and the extortion demand amount related a threat to commit a computer attack, implant a virus, etc.

To find out more about cyber risks insurance, or to discuss your existing insurance policies, please give one of Axis Insurance Group's professional and experienced team a call on 604.731.5328. We would also be pleased to outline the benefits of Cyber Risks Insurance with your management team or board members. If you would like to schedule a meeting or request an application form, please contact us.