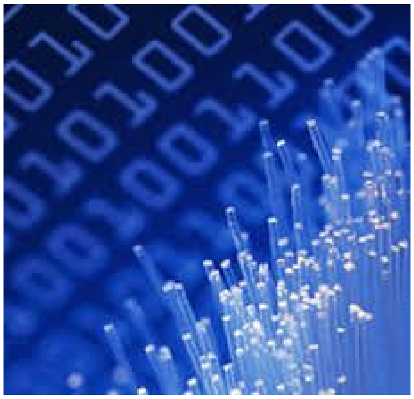
Cyber Liability

Some claims and risk management strategies to prevent losses from happening to you



The Claims

There has been an explosion of cyber liability claims in both the first party (a company's own system) and third party (allegations of a data breach) areas in the past few years.

First Party Claims

First party claims usually fall in 5 main categories: loss of computers, data, and digital assets; a security event; business interruption based on hardware or software failure; computer-based terrorism; and cyber extortion.

The most common loss scenarios fall into simple and expensive employee error. Given the amount of data that even the most junior of employees have access to, it is easy to see why this causes risk managers, human resource managers, and information technology professionals the most angst. The scenario is familiar - an employee loses a computer, phone, or PDA containing reams of data at a hotel, airport, or restaurant on business. The device is then compromised forcing the company to shut down data systems. If the information on the specific device is valuable enough or not saved on a shared drive, it must be rebuilt, new security measures implemented, and/or notifications must be sent to clients. There are thousands of these claims across the country each year generating millions of dollars in economic injuries.

Business interruption from a cyber-event is a new and budding trend. A typical circumstance is that an employee unknowingly opens an email containing a virus and it immediately goes to work shutting down a company's computer system. From there, systems become slower or shut down completely.

A recent event involving cyber terrorism and business interruption featured a high school student sending a worm to a consulting firm causing an 18 hour shutdown of the entity's computer system. Costs reached $875,000 as the firm had to repair and restore their systems and were unable to conduct business for 18 hours.

Cyber extortion is close on the heels of business interruption as an up-and-coming threat. 'Hackers for Hire' are a rising industry group roaming the internet promising to wreak havoc on a company for a price. A recent case involved a U.S. based company that contracted with an overseas software company. The overseas company deployed much less stringent computer defenses and a hacker gained access to millions of confidential records. A ransom of $2 million was paid to keep the information from being publicly disclosed.

Third Party Claims

In general terms, third party cyber claims revolve around three main torts: network and privacy liability; employee privacy; and personal/advertising injury.

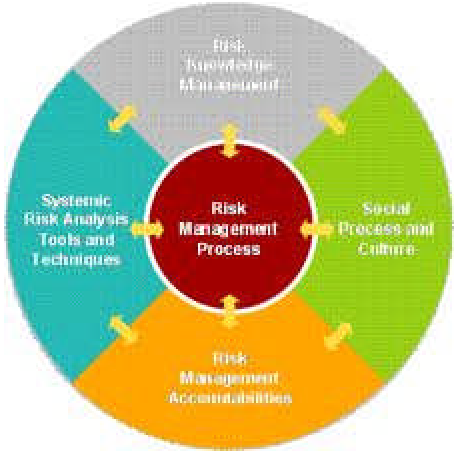
The largest claims we see, by far, involve compromising a company's network leading to the disclosure of confidential information. A recent case involved the theft of the records of 800,000 clients. Under notification laws, the company, not the ISP, was required to notify the affected individuals. Total expenses for disclosure requirements and crisis management exceeded $5 million.

Many government contractors are diversifying their business models by expanding into the medical world based on healthcare reform and the required digitizing of records by the HITECH Act (Health Information Technology for Economic and Clinical Health Act). While lucrative, the risk management issues surrounding the safekeeping of medical records are enormous. A recent claim involved a contractor that had backup tapes, laptops, and disks containing the social security numbers, clinical and demographic information, and in a small number of cases, patient financial data was stolen. Over 365,000 records were exposed. The company was sued by the state and by numerous individuals. The expected cost should top $10 million based on fines, lawsuits, the required revamping of security policies, implementing technical safeguards, and being subject to random compliance audits.

In the new world of social media, most companies are woefully under prepared for a tweet or blogs gone bad. Courts are still establishing case law, but it is clear that the cost of simply defending an action will reach six figures. A person or company can allege such torts as damage to reputation, unfair trade practices, libel, and financial injury.

Risk Management

So, to no one's surprise, it is a dangerous cyber world out there for federal government contractors. Digital assets and the protection of those assets become paramount to an effective cyber risk management strategy.


Risk Knowledge Management
Systemic Risk Analysis Tools and Techniques
Risk Management Process
Social Process and Culture
Risk Management Accountabilities

We see three basic parts to any solid risk management plan. You first have to identify and assess your risk. For example, what data are you storing, who has access to it, and how your administrative rights work are just a few simple questions to get you started. Second, once you have a basic understanding of your risk, what steps are you taking to minimize it? Do your employees have clear instructions what to back up on a thumb drive versus a hard drive? Do you have a data policy?

Finally, you need the proper insurance in place to ensure that if something does go wrong, you are fully covered. The defense alone for a cyber-case will exceed $100,000 and you want your insurance company to bear that expense and claim to allow you to focus on the business at hand.

Now What Do I Do?

You need to sit down with your risk management department and your broker and make sure you fully understand how your program would react to common loss scenarios. From there, a good broker will help you implement a loss mitigation program to ensure your business is protected in these unprecedented times.

For more information or for an initial consultation contact PIA at defense@palumboinsassoc.com or call 410.836.8591

Or to visit our website click on the link below.
PIA/Federal Government Contractors