CYBERSPACE

Cyber & Privacy Liability - You're Exposed, Now What

You can't read the paper or watch the news these days, without hearing about a new data breach or a cyber-attack. It was reported in the New York Times that in 2013 they ran fewer than 125 stories involving Data Breaches. In 2014 this number jumped to 700 articles on Data Breaches. From hackers trying to gain access to Canadian and U.S. governmental agencies and accessing the account information of un-suspecting users, to lost media including confidential client data at a financial institution, data breaches are all around us. And don't think that it is just large, high profile organizations that are at risk. According to industry experts and recently reported news stories, there has been a shift by cyber thieves away from targeting major banks and retailers like Sony, Target and Home Depot to attacking smaller based companies. A new version of malicious software was designed to steal credit and debit card data from hacked point-of-sale (POS) devices. In the recently released Verizon – 2015 Data Breach report **http://www.verizonenterprise.com/DBIR/2015** the study states that in previous years we saw phishing messages come and go with success in the 10% to 20% range. However, fast forward to the present and gone are the old gimmicky messages. These newer sophisticated messages have evolved to install malware as the 2nd stage of their attack campaigns. The 2014 phishing statistics are higher with somewhere around 23% of recipients now opening phishing messages and 11% clicking on the attachments; which is where the most dangerous threat comes from. This information proves once again that Cyber Risk is a constantly moving target. Only a small percentage of data breaches and cyber-activities are reported in the media.

How Losses Happen

Organizations must recognise the extent to which they are exposed and the various accidental as well as intentional way losses can occur:

- **Social Engineering; phishing** – this includes losses as a result of engineered attacks to trick individuals or organizations into divulging personal or confidential information, under the guise of legitimate business operations/activities or clicking on seemingly harmless attachments
- **Hacking** – loss due to someone gaining unauthorized access to your confidential information. This could be by an outside party or someone within your organization.
- **Physical Theft** – theft of a laptop, memory key, cd, blackberry/smartphone or other portable devices
- **Accidental Release** – insufficient online security, accidental posting of confidential data on a company website, accidental access granted to personal/confidential information
- **Lost Media** – loss or misplacement of a laptop, memory key, cd, blackberry/smartphone or other portable device
- **Employee Acts** – loss from accidental and unintentional acts of employees (human error) or physical theft or hacking by disgruntled or ex-employees.
- **Vendors/Third Party Custodians** – while an organization may transfer its data gathering and holding activities to a third party vendor or custodian, irrespective of this they are still responsible to individuals whose personal information is breached

Key Contacts:

Cyber & Privacy Liability Practice Group

Philomena Comerford
President & CEO
pcomerford@bairdmacgregor.com

Janie Osman
Vice President
janie@hargraft.com

Jesse Henkenhaf
Vice President
jhenkenhaf@bairdmacgregor.com

Head Office
825 Queen St East
Toronto, Ontario M5M 1H8
416-489-9600/1-800-387-0529
www.hargraft.com

HARGRAFT

Statistics on data breaches investigated in the Verizon Data Breach Investigations Report (DBIR):

- 31% involved companies with fewer than 100 employees
- 78% of cyber thieves employed techniques classified as "low" or "very low" difficulty
- 75% of attacks were untargeted and opportunistic
- 66% of breaches took months or longer to be discovered

The Victims represent a wide range of industries:

- Financial organizations (37%)
- Retailers and restaurants (24%)
- Manufacturing, transportation and utilities industries (20%)
- Professional services firms (20%)

What can you do:

In spite of all of this, however, there are some steps you can take to help prevent and/or reduce the costs in the event of a cyber-breach:

- Install a fire wall. This might limit the size of data you can receive, but can be invaluable in protecting your network.
- Outsource the gathering and protection of confidential information to a third party provider (ensure they have proper protection with a Cyber Network, Privacy liability policy in force or you may still be on the hook).
- Limit the use of remote access into your company systems.
- Back up all of your data daily and encrypt personal devices, laptops and computers. If they are stolen or misused by a disgruntled employee you can wipe them clean and use your back up data to start again.
- Adopt a social media policy. It can't be stressed enough to teach employees good protocols around securing networks such as not sharing passwords and not opening emails that can infect your system with a virus.
- Install Anti-virus software to ensure most phishing messages will be caught before reaching your employees.

In addition the following are some recommended best practices from the "Cost of a Data Breach Study – Executive Summary, Overview: Data Loss Prevention" by Symantec: **https://www4.symantec.com/mktginfo/datasheet/GL_NA_DS_053013_Ponemon-2013-Cost-of-a-Data-Breach-ExecSummary_dai258107_cta72383.pdf**

1. Educate employees and train them on how to handle confidential information.
2. Use data loss prevention technology to find sensitive data and protect it from leaving your organization.
3. Deploy encryption and strong authentication solutions.
4. Prepare an incident response plan including proper steps for customer notification.

For more details on the financial consequences of a data breach and how to best prevent, detect, and resolve one, please see the full global report by visiting: **go.symantec.com/DLP**. You can also estimate what a data breach could cost your company at **www.databreachcalculator.com**. This is a free online tool from Symantec that calculates your risk based on your organization's characteristics.

It goes without saying that today, organizations of any size can suffer **first party losses** and can be **liable to third parties** for a multitude of privacy and/or cyber related breaches or incidents.

First Party Exposures – Direct Damage Costs :

Potential first party exposures in the event of a data breach are varied and numerous. Failure to recognize and manage these exposures and the risk of loss to the organization can have a devastating effect. While strong internal procedures with respect to the handling and protection of sensitive and protected data is key and can help mitigate and manage risk to loss, simple human error can easily lead to an accidental release of data. Without a robust Privacy & Cyber liability policy in force, an organization may face loss for the following uninsured direct damage costs.

- **Fines and penalties levied as a result of a breach** – costs to cover insurable fines and penalties levied by privacy regulators and payment card charge backs
- **Business interruption and extra expense** – cost reimbursement for loss of business income and decline in revenue as a result of a data breach and/or the extra costs to continue business after a breach and mitigate loss
- **Forensic audit** – costs to investigate and identify the source of the breach. When a system is hacked into, the source of the hack is not always readily apparent
- **Costs to restore information assets** – costs to restore systems that are hacked and IT assets that are destroyed and/or damaged, including implementation of changes to internal process
- **Notification costs** – costs to notify individuals or entities that were affected by the breach – i.e. 1 800 numbers and call centre management, letters to individuals, advertisements in the paper to notify groups of potentially affected individuals in a certain geographic area
- **Crisis Management Costs** – costs to hire a lawyer or public relations firm to assist the organization in managing the messaging around the loss
- **Credit Monitoring** – costs to provide credit and fraud monitoring services to individuals whose personal information has been breached
- **Extortion threats** – costs to handle a cyber extortion threat, which can include fees of a negotiator or consultant to handle the extortion threat

Third Party Exposures – Legal Liability to Outside Parties

- **Downstream liability for viruses** – liability to third parties from introducing a virus into their system/computer, including contingent business interruption if the virus causes a full or partial shutdown of a third parties business/operations
- **Liability losses arising from a data breach** – liability to third parties whose data or personal information has been affected by a breach including liability where the data and/or personal information has been used to commit fraud against the breached individual (i.e. identity theft)
- **Liability from infringement of intellectual property** – liability to third parties for intellectual property infringement, including copyright and trademark infringement
- **Liability from defamation** – liability for allegations of libel, defamation of character or product disparagement from information posted on an organizations website
- **Third party subrogation costs** (i.e. credit card company charge backs) – liability for losses suffered by a third party that are a direct result of the actions or inactions of the organization

Conclusion

Business's need to prepare for "when they suffer a breach" rather than "if they suffer a breach". Our ever growing digital world, increased use of mobile and portable media devices and the true globalization of our economy, leave all of us vulnerable to cyber attacks, data breaches, and loss due to human error. Irrespective of how the loss occurs, organizations can find themselves facing jarring first and third party losses, under increased scrutiny by the regulators, and see consumer and stakeholder confidence in the organization take a sharp drop.

While a Cyber & Privacy Liability insurance policy will not stop a loss from happening, it can provide an organization with the funds to effectively and expeditiously handle a loss, hire crisis and public relations consultants where required to help mitigate the loss and the potential impairment of an organization's reputation, cover loss of business income as a result of a loss, including increased costs after a loss to mitigate further damage, and finally funds to deal with any third party lawsuits that arise from a breach or attack.

Traditional Insurance Policies – Mind the Gaps!

A traditional insurance program will not properly protect an organization from either first or third party losses. While limited liability coverage may be available in specific circumstances, organizations will find it difficult to trigger coverage under any of the following types of insurance policies traditionally purchased.

- **Property Insurance** – property policies usually require physical damage to a tangible asset to trigger coverage. Data is not considered tangible property in most policies
- **D&O Liability Insurance** – generally covers Directors & Officers and it is the entity that would be attracting liability for a cyber breach. Where the entity is covered, the policy will not provide any coverage for first party or direct damage costs
- **Commercial General Liability** – difficult to trigger coverage for a privacy breach, and limited coverage provided for advertising injury
- **Crime Insurance** – covers theft of money & securities, but does not cover the costs arising from theft of data
- **Professional Liability/Errors & Omissions** – provides coverage for wrongful acts related to insured professional services. Privacy and cyber related breaches would not fall under insured professional services

Mandatory Breach Notification – To Notify or Not to Notify?

Alberta

The Province of Alberta introduced mandatory breach notification on May 1, 2010, mandating breach notification to the Privacy Commission, who can then direct the organization to notify the affected individual(s). The legislation requires firms to notify affected individuals if there is "a real risk of significant harm". Notification must be given directly to affected individuals unless the Commissioner determines otherwise.

Federal Legislation Bill C 29, Safeguarding Canadians' Personal Information Act

While the proposed legislation died with the dissolution of Parliament on March 26, 2011, industry experts believe it is only a matter of time before Federal mandatory breach notification becomes law. The original proposed legislation would have required notification to the Privacy Commissioner of material privacy breaches and notification to individuals if the privacy breach created a real risk of significant harm.

While mandatory breach notification is not required in all jurisdictions for all breach scenarios, it is often in the best interest of the organization that has suffered a breach, to notify the affected individuals or organizations as well as the Privacy Commissioner that there has been a breach. Companies that act quickly, notify accordingly, take accountability and offer appropriate services (i.e. credit & fraud monitoring) and compensation where required, will often stave off large liability losses, protect their hard earned reputation, and secure goodwill with their customers and other organization and agencies they may do business with. Potential fines and penalties levied by the Privacy Commissioner may also be minimized by effectively managing the breach and proactively notifying affected individuals.

Cyber Network & Privacy Liability – Data Breaches in the News

CIBC lost a computer file which contained the confidential information of 470,000 of its customers. In another incident, **CIBC** sent hundreds of faxes containing confidential customer information to a scrapyard in West Virginia. The faxes included names, account numbers, social insurance numbers and detailed account information.

Passport Canada had a network security breach allowing unidentified persons access to passport applicant's personal information on line.

Canada Post recorded a security breach regarding its small business clients using its online complaints system.

Canada Post lost 26 packages from Cancer Care Ontario, which included the cancer screening results of 12,000 patients.

Canadian Bar Association disclosed a security breach allowing online access to orders and credit card information of its members.

Bell Canada had their personal information stolen. The data was contained on a hard drive, memory stick and CD.

Honda Canada Data Breach Triggers Lawsuit The class action suit accuses Honda of putting 283,000 customers at risk, in part by waiting two months to inform them of the data exposure. Lawyers for Honda customers filed a class action lawsuit on behalf of affected customers, seeking 200 million Canadian dollars ($206 million). The claim says that the breach exposed customers to "theft of their identity, theft from their bank accounts, and theft from their debit and credit cards.

Sony Erikson - Sony has admitted that hackers broke into its PlayStation Network making off with the personal information of more than 77 million members. The breach is being called the fifth largest data breach in history, according to Datalossdb.org (Identity Week.com)

The following pages are some data breach claims examples from 2 Insurers.

Private Company Loss Scenarios from Chubb

Hacker Steals ID and Victim Sues

COVERAGE	CyberSecurity by Chubb
Cause of action	Hacker
Type of organization	Resort

DESCRIPTION OF EVENT

Hackers installed a malicious software program into a high-end resort's credit card processing system from a remote source, hitting the resort's point-of-sale processing system where credit cards are swiped for purchases. One victim's credit history was damaged as a result of purchases made from the victim's stolen credit card, resulting in, among other things, being turned down for a mortgage he had applied for. After suffering the consequences for more than a year, the victim brought a lawsuit against the resort, seeking $750,000 in damages, including emotional distress.

RESOLUTION

In addition to paying overall costs of more than $4 million to recover from the security breach, the resort settled with the plaintiff for more than $300,000.

Manufacturer pays for invasion of privacy by intermediary firm

COVERAGE	CyberSecurity by Chubb
Cause of action	Negligence, Invasion of Privacy
Type of organization	Manufacturer
Number of employees	50
Annual revenue	App. $10 million

DESCRIPTION OF EVENT

A manufacturer leased a copy machine over a two-year period. During that timeframe, the company made copies of proprietary client information and its employees' personally identifiable information, including social security and driver's license numbers. After the lease expired, the manufacturer returned the machine to the leasing company through an intermediary company. Prior to making its way back to the leasing company, a rogue employee at the intermediary firm accessed the machine's data for nefarious purposes.

RESOLUTION

The manufacturer incurred $75,000 in expenses in connection with a forensic investigation, notification, identity monitoring, restoration services and independent counsel fees. It also incurred approximately $100,000 in legal defense costs and $275,000 in indemnity associated with the theft and sale of proprietary client information.

Private Company Loss Scenarios from Chubb

Criminal scheme skims customers' payment card info from retailer

COVERAGE	CyberSecurity by Chubb
Cause of action	Negligence, Invasion of Privacy
Type of organization	Retailer
Number of employees	35
Annual revenue	App. $5 million

DESCRIPTION OF EVENT

A criminal syndicate attached skimming devices to a local retail chain's payment card systems at a variety of locations. This permitted unauthorized access to the credit and debit card information of 15,000 customers over a three-year period.

RESOLUTION

The retail chain spent $850,000 performing forensics, engaging counsel for compliance assessment and providing notification and call center services to its customers. It also spent $900,000 reimbursing a variety of banks for costs associated with card cancellations and re-issuance charges. Lastly, it spent $75,000 in defense costs responding to a regulatory inquiry and $250,000 in fines.

Laptop Stolen from Exec's Car Results in Invasion of Privacy

COVERAGE	CyberSecurity by Chubb
Cause of action	Negligence, Invasion of Privacy
Type of organization	Energy Firm
Number of employees	100
Annual revenue	$20 million

DESCRIPTION OF EVENT

An energy company executive's laptop was stolen from a corporate vehicle. The laptop contained significant private customer and employee information. Although the file was encrypted, the overall password protection on the laptop was weak and the PIN for accessing the encrypted information was compromised.

RESOLUTION

After assessing the nature of the information on the laptop with a forensic expert and outside compliance counsel at a cost of $50,000, the energy company voluntarily notified relevant customers and employees and afforded call center, monitoring, and restoration services, as appropriate. While the additional first-party cost was $100,000, the energy company also incurred $75,000 in expenses responding to a multi-state regulatory investigation. Ultimately, the company was fined $100,000 for deviating from its publicly stated privacy policy.

Professional Services Loss Scenarios from Chubb

PII Theft Leads to Lawsuits, Business Interruption, Extra Expenses

COVERAGE	CyberSecurity by Chubb
Cause of action	Hacker, Breach of Contract, Negligence
Type of organization	Administrator
Number of employees	500
Annual revenue	$65 million

DESCRIPTION OF EVENT

An unknown organization hacked an administrator's network prior to a major holiday weekend and stole personally identifiable information (PII). In addition to obtaining names and credit card information of 25,000 customers, the organization stole employment data from 250 employees of the firm. Furthermore, the unknown organization disseminated a virus through the administrator's system and subsequently shut down the network altogether, rendering the firm unable to conduct business for 72 hours. The administrator's clients, who were unable to access the network for business purposes and sustained virus-related impacts to their own systems, sued the administrator for impaired access and conduit-related injuries.

RESOLUTION

The administrator incurred $250,000 in expenses associated with a forensic investigation, notification, monitoring and restoration, and independent counsel fees. It also sustained more than $2 million in lost business income and extra expenses associated with the system shutdown. Finally, it assumed an additional $300,000 in third-party defense costs and paid $5 million in damages to customers who were unable to obtain access to the network during a business critical timeframe.

Theft of Laptop

COVERAGE	CyberSecurity by Chubb
Cause of action	Breach of Contract, Negligence, Invasion of Privacy
Type of organization	Consulting Firm
Number of employees	1000
Annual revenue	$75 million

DESCRIPTION OF EVENT

An employee of a consulting firm had a business laptop stolen from his personal residence. The laptop, which was unencrypted and failed to contain password protection, included names and financial account numbers for more than 7,500 clients. It also included clients' business and proprietary information. After providing notice to the clients regarding the theft, a number of lawsuits were filed against the consulting firm for negligence, invasion of privacy and breach of contract.

RESOLUTION

The consulting firm incurred $1 million in expenses associated with notifying clients about the theft of personally identifiable information, changing account numbers, hiring a public relations firm, establishing a call center, and retaining independent counsel to assess notice and compliance obligations. The consulting firm also afforded clients with monitoring services for a year following the theft for an additional $150,000. Finally, after incurring approximately $250,000 in legal defense costs, the lawsuits against the consulting firm were resolved for an additional $2 million—the most significant aspects of which were driven by the theft of proprietary client data.

Health Care Organization Loss Scenarios from Chubb

Lost iPad

COVERAGE	CyberSecurity by Chubb
Cause of action	Unfair Trade Practices, Violations of HIPAA, Negligence, Invasion of Privacy
Type of organization	Hospital
Number of employees	2800
Annual revenue	$420 million

DESCRIPTION OF EVENT

A nurse lost an iPad containing names and protected health information for 25,000 patients vaccinated against the flu. A class action was filed against the nurse's employer, a hospital, alleging negligence and invasion of privacy. In addition, consistent with HITECH, an attorney general action was filed against the hospital for alleged violations of HIPAA, including failure to properly encrypt portable data and failure to provide timely notice to impacted individuals. Finally, the attorney general alleged violations of the state's unfair trade practice law.

RESOLUTION

The hospital incurred more than $750,000 in expenses associated with notifying patients regarding the lost iPad, hiring a public relations firm, establishing a call center, providing monitoring and restoration services, and retaining independent counsel to assess notice and compliance obligations. In addition, following class certification and defense costs in the amount of $500,000, the hospital resolved the litigation for approximately $1 million. The hospital also paid $500,000 in monetary fines and penalties as a result of the HIPAA and unfair trade practice violations and was required to implement new encryption and training protocols.

Rogue Employee Sells Electronic PII

COVERAGE	CyberSecurity by Chubb
Cause of action	Violation of State Notification Regulations, Breach of Contract, Negligence
Type of organization	Hotel
Number of employees	2500
Annual revenue	App. $250 million

DESCRIPTION OF EVENT

A former hotel executive gained unauthorized access to the hotel's confidential internal database that included names and credit/debit card information of 75,000 patrons. The database also included names and social security numbers for more than 2,500 hotel employees. The former executive ultimately sold the personally identifiable information (PII) to an organization allegedly affiliated with organized crime. After the unauthorized access was detected by the hotel's IT department and outside forensic investigators, the hotel notified the impacted patrons and employees about the breach. A regulatory action was subsequently initiated on behalf of impacted patrons and employees to establish a consumer redress fund.

RESOLUTION

The hotel incurred more than $2.5 million in expenses associated with forensic investigation, privacy notification, credit/identity monitoring and restoration, public relations, and regulatory defense fees. It also paid $2.5 million in fines and penalties as a result of the unauthorized access to its database and its failure to timely notify patrons and employees of the breach.

PII Theft Results in Extortion, Business Interruption, Extra Expense

COVERAGE	CyberSecurity by Chubb
Cause of action	Breach of Contract, Negligence
Type of organization	Law Firm
Number of employees	55
Annual revenue	$20 million

DESCRIPTION OF EVENT

An unknown organization hacked a law firm's network, and the intruder may have gained access to sensitive client information, including a public company's acquisition target, another public company's prospective patent technology, the draft prospectus of a venture capital client, and a significant number of class-action lists containing plaintiffs' personally identifiable information (PII). A forensic technician hired by the law firm determined that a bug had been planted in its network. Soon after, the firm received a call from the intruder seeking $10 million to not place the stolen information on-line.

RESOLUTION

The law firm incurred $2 million in expenses associated with a forensic investigation, extortion-related negotiations, a ransom payment, notification, credit and identity monitoring, restoration services and independent counsel fees. It also sustained more than $600,000 in lost business income and extra expenses associated with the system shutdown.

Hack of Third-Party Network Gets Media Company into Hot Water

COVERAGE	CyberSecurity by Chubb
Cause of action	Unfair Trade Practices, Negligence, Invasion of Privacy
Type of organization	Media and Entertainment Company
Number of employees	1000
Annual revenue	$30 million

DESCRIPTION OF EVENT

A media and entertainment company outsourced the storage and protection of its employment information to a third-party service provider. Subsequently, the service provider's network was breached, and outsiders were able to obtain unauthorized access to names, social security numbers and financial account details for 1,000 employees. A class action was ultimately filed against the employer, alleging failure to protect the personally identifiable information (PII), to adhere to the company's network security and privacy policy, to timely notify the employees about the breach, and to properly retain and oversee a viable third-party service provider.

RESOLUTION

The company incurred $200,000 in expenses associated with notifying employees about the theft of PII, changing account numbers, establishing a call center, and retaining independent counsel to assess notice and compliance obligations. In addition, the company afforded employees with monitoring and restoration services for two years following the breach at a total cost of $50,000. Further, after incurring approximately $100,000 in legal defense costs, the class-action lawsuit was resolved for $950,000. Lastly, while the company attempted to subrogate against the third-party service provider, the provider lacked sufficient assets and insurance to fully indemnify itself.

Could this happen to your organization? Contact your trusted Chubb agent or broker.

Chubb Group of Insurance Companies
Warren, NJ 07059
www.chubb.com

2/2012

ENCON Group Inc.
500-1400 Blair Place
Ottawa, Ontario K1J 9B8
Telephone 613-786-2000
Facsimile 613-786-2001
Toll Free 800-267-6684
www.encon.ca

Claims Examples - Cyber Security and Privacy Liability

The following claims examples have been developed to illustrate the types of cyber liability claims that clients may face.

Privacy Liability

1. Privacy Breach

An online mortgage company reported a breach after several former employees gave mortgage lenders access to confidential customer records. Over a two year period, lenders obtained access to private client information, such as social insurance numbers, income and employment data, and used it to market their own mortgages. The mortgage company incurred the cost of notifying their clients, and the cost to protect the privacy and identity of the firm's clients, restore their identity to pre-theft status if required and report any security breach to credit agencies. Total remediation costs were in excess of $75,000.

2. Privacy Breach

A mid-size accounting firm was broken into and laptop computers were stolen. Some of the information contained in these laptops was personal, including the social insurance numbers and bank account information of the firm's clients. Overall, a total of nearly 10,000 of the firm's clients were affected by this theft. Although the police investigating the case suspected that the theft was a simple "smash and grab," the firm had not encrypted the information found in these laptops, making it easily accessible. There was a one month lapse between the time of the theft and the time the firm notified their clients. The firm had to incur significant remediation costs, both to notify the clients and to retain a company to protect the privacy and identity of the firm's clients, and restore their identity to pre-theft status as required and report any security breach to credit agencies. Total remediation costs were $150,000.

Although this example involves an accounting firm, it could apply to professional practices of all kinds, including medical clinics, medical professionals, business consultants, brokerages or any other type of professional dealing with sensitive and confidential information.

3. Privacy Breach

A medical clinic employee accidentally emailed a file with client names, medical records and provincial health card numbers to an unauthorized individual. The medical clinic notified its clients of the breach immediately. Two months after the breach, one of the clinic's clients was a victim of identity theft and sued the clinic for damages. The final settlement was $50,000 and the cost to defend the clinic was $25,000.

Claims Examples - Cyber Security and Privacy Liability

Network Security Liability

1. Network Data Breach

A law firm faced a class action lawsuit filed by former employees. The lawsuit was filed after an employee database housed on the firm's network containing personal information and emails from 500,000 current, former and prospective employees was breached. Nearly 100,000 social insurance numbers were stored in the database. After the breach, the firm disclosed that some of the email information had been used to create fake emails to contact the individuals whose information had been compromised. The remediation costs incurred by the firm as a result of this breach included $25,000 in credit monitoring services for employees affected by the breach and $150,000 in public relations services. In addition, $60,000 was incurred in legal fees.

2. Network Data Breach

An association that offered educational webinars ran a promotion encouraging members to register and pay for an upcoming webinar on its online website. Shortly after running the promotion, the association's computer systems were improperly accessed by a third party. The members' names, postal address, phone number and credit card information were exposed. Remediation costs were in excess of $60,000 and included notification of the breach to the association's members, credit monitoring and public relations services.

Electronic Media Liability

1. Copyright Infringement

A health and safety consultant offered online courses such as first aid, human rights and leadership development. The consultant had previously purchased all copyrights from another health and safety training firm that had "allegedly" created the online courses. A lawsuit was launched against the consultant by a third party for copyright infringement. The lawsuit was also launched against the training firm who sold the material to the consultant. The plaintiff alleged that the material used online by the consultant was in fact authored by him and he had never authorized the consultant to use the material. The lawsuit went on for several years. A settlement was finally reached among all the parties. The final settlement was in excess of $300,000, with a contribution of $40,000 from the consultant. The cost of defending this claim was in excess of $100,000.

2. Defamation and Slander

The defendant, who ran an online newspaper, wrote an article about a medical clinic and its medical staff. The article referred to how doctors working at the clinic were involved in a conflict of interest regarding new software the medical clinic was about to purchase at a very high price. A libel notice was served on the defendant journalist and an online apology and retraction were requested. Shortly after the apology and retraction, a lawsuit was filed against the online newspaper for defamation in the amount of $4 million. The file settled for $400,000 and defence costs incurred were in excess of $200,000.computer systems were improperly accessed by a third party. The members' names, postal address, phone number and credit card information were exposed. Remediation costs were in excess of $60,000 and included notification of the breach to the association's members, credit monitoring and public relations services.