VANDALS AT THE GATES

Comments on Internet and Network Security and the Law in Canada

By James Swanson, BASc, LLB, MBA
Parlee McLaws
Barristers & Solicitors
Edmonton, Alberta, Canada
Tel. 780-423-8500
jswanson@parlee.com

I have been bankrupt but twice in my life:
once when I lost a lawsuit, and once when I won one - Voltaire

1. INTRODUCTION AND SCOPE OF THIS PAPER

Eliminating the barriers of distance and time, decreasing costs while increasing productivity, and reaping the benefits of connectivity and advances in technology are all good things, but there is a dark side. Businesses and their directors, officers and management, while understandably rushing to capitalize on those benefits, need to remember a fundamental basic: the networks and systems they use can be a tempting target to individuals with knowledge allowing them to exploit weaknesses in those networks and systems. Security is therefore increasingly a major area of concern as technology increasingly becomes the lifeblood of business.

We all know from reports in the press and possibly even personal experience that incidents of computer viruses, hacking, cracking, denial of service or "DoS" attacks, penetration of networks and other breaches of security are on the increase and the amount of financial and other losses continues to rise as time passes.

For example, in the 2001 CSI/FBI Computer Crime and Security Survey[1], released in 2002, the Computer Security Institute presents some alarming statistics. Ninety percent of the entities surveyed reported having detected security breaches and eighty percent reported resulting financial losses. Of the businesses surveyed, forty four percent were able or willing to quantify those losses, which totaled more than $450,000,000 (U.S. currency). However, only 34% reported their incidents and losses to law enforcement, which was up from only 16% the year before. The most serious losses were due to financial fraud and theft of confidential or proprietary material.

Many networks, companies and individuals may not even know of breaches of security or, if they do know, they do not report it for a variety of reasons. They may be embarrassed, or feel that there is nothing that can be done, particularly after the fact.

This paper will not delve into the intricacies of network and computer security from a technical point of view as such discussions are beyond its scope. However, it will discuss, in a general fashion, a few of the more significant legal issues arising out of Internet, network and system security and the consequences of breaches of that security, as well as relevant issues surrounding management's dealing with security issues.

2. DEFINING SECURITY

Security, in this context, could be described as the ability to allow free and easy access to the systems and resources in question to those who are desired to have such access, while eliminating access to those who are not. Key issues are freedom from danger or risk and confidence and trust in the systems and resources used.

In the context of a business, there are numerous ways in which network security can be breached, ranging from hacking and cracking to inside jobs to simple sloppiness in practices and procedures. Prevention of penetration from the outside requires implementation of technological solutions to harden networks and prevent such breaches of security. Adequate steps need to be taken to enforce proper procedures, limit access to what is required, as well as to watch for and guard against potential employee or other insider misconduct (whether such conduct is malicious or simply arises from ignorance).

In a more general sense, security may be physical (locks and restricted access), administrative or organizational (access restricted to appropriate personnel) or network and computer based. Of course, these three areas of concern will overlap.

3. CONSEQUENCES OF BREACHES OF SECURITY

Why do we want to have security? Because we want to be able to use our computers and systems to store, process and communicate our private and confidential information in the manner we wish, and only in that manner. There is a great deal of value to be derived

[1] Copies of the report may be accessed at http://www.gocsi.com/. There are also many reported summaries appearing in the press, both online and off. The limited information in this paper is derived from such third party sources and readers are advised to consult the complete report.

from using the systems in the desired manner and from everyone concerned having trust that such will be the case.

The other side of the coin is that there is a great deal of harm to be suffered if the security of a network or system is breached. In any such case, the value of the system is compromised. The system may become unavailable or may suffer a lack of performance. Information may be destroyed and therefore not be available to those we wish to have it. Such information may be irreplaceable. Information may be altered and we may not even know it, and therefore rely on it to our detriment. Information may be made available to those we do not wish to have it. Information may be misused, stolen or disseminated against our wishes.

In addition to loss of information, other unpleasant consequences may follow. For example, physical plants or processes run by computers may fail or operate improperly, causing failure of machinery or such things as discharge of toxic materials or the distribution of improperly manufactured products.

4. THE *WEB* OF BUSINESS AND LEGAL RELATIONSHIPS

Any business exists and carries out its functions and activities within a complex web of transactions and legal and contractual duties and obligations.

Very few top managers of organizations could even draw a complete flow chart of all such relationships. At best, they could list their major contracts, but might give little thought to things such as potential legal liability should failure of their own organization's systems (or of an organization on which they depend) lead to damages to third parties or the public in general. Management might also not fully consider their potential liability for breach of fiduciary duties or duties of due diligence (more about this below) to the corporate entity comprising the business.

Business has become increasingly dependent on technology to the point where the web of business relationships and the computer networks that support and enhance that web have reached almost biological complexity[2]. Because of that complexity, problems or failures at one point on the supply chain or web of relationships can create a domino effect triggering further failures or problems at other points.

5. POTENTIAL LEGAL CONSEQUENCES

Following are some of the key legal issues to consider in terms of both practices and procedures to deal with security issues and the consequences of security being compromised or breached.

---

[2] When you consider the manner in which computer viruses spread, this biological metaphor becomes even more real.

5.1 Breach of Contract

Loss of network function or integrity may lead to inability of the business to fulfill its contractual obligations. Where the business is in breach of contract, customers or clients, or others affected by the breach and sustaining losses, may sue the business for damages for such losses.

It is possible that this can lead to a sort of domino effect[3], with customers of the business being sued by others further down the supply chain, at which point other parties, (*including the business itself, if not sued at first instance*), may be brought in to the litigation by means of third party notices, notices of contribution and indemnity, or similar measures.

5.2 Tort Liability

It is also possible that breaches of security may lead to the business being exposed to liability in tort[4] as well as in contract. This is significant as it broadens the types of conduct, errors or omissions that may result in liability. It also allows parties not in a direct contractual relationship[5] with the business to be able to sue the business for damages.

If failure of a network caused by inadequate security leads to loss or damage to other parties, the initial question will be whether such loss was reasonably foreseeable, and therefore resulted in a duty of care being owed by the business to such parties. If there is such a duty, and it was not fulfilled by taking adequate steps to avoid damage and loss, legal liability may follow.

Certainly, failure of computer systems is reasonably foreseeable, particularly if the result of failure can cause damage to third parties, so such a duty of care is likely in most circumstances. That then leads to consideration of the required standard of care, which must be found to be have been complied with on a reasonable basis. If a court considering such a case finds that adequate steps were not taken to maintain security and avoid losses or damage, then the business may be found liable for any such losses caused by its negligence. Of course, such deliberations are after the fact and subject to 20/20 hindsight.

Sufficiently significant breaches of contract or tortious conduct and the resulting claims can adversely affect the bottom line, and can even end the existence of a business[6].

---

[3] For example, a computer failure in a German plant manufacturing door locks for a automobile manufacturing plant in England is reported to have caused the assembly line to shut down for three days, leading to losses estimated at £18,000,000. Due to just in time (JIT) production practices, there was insufficient inventory of the locks to allow manufacturing to continue.

[4] Civil wrongs giving rise to a right to sue for damages and other remedies. Examples, using the term "tort" in its broadest sense, can include negligence, product liability, infringement of intellectual property rights, etc.

[5] Privity of contract generally provides that non-parties to a contract have no rights under the contract.

[6] While not specifically a parallel situation, Enron illustrates how quickly things can unravel.

5.3 Loss of Trade Secrets

There is no specific Canadian legislation dealing with Trade Secrets. However, the Alberta Law Commission has authored a report in the area, including a draft Trade Secrets Act, which has not been enacted, but which included the following definition:

> "Trade Secret" means information including but not limited to a formula, pattern, compilation, programme, method, technique, or process, or information contained or embodied in a product, device or mechanism which:
>
> i) is, or may be used in a business,
> ii) is not generally known in that trade or business,
> iii) has economic value from not being generally known, and
> iv) is the subject of efforts that are reasonable in the circumstances to maintain its secrecy.

In addition to trade secrets, there may be other information that, once disclosed, can harm a business. Examples include customer or supplier lists, business or financial plans or even documents disclosing tortious acts.

Publication or disclosure destroys the value of a trade secret or indeed any other secret or confidential information. If a breach of security occurs, and a trade secret or other confidential material is disclosed or destroyed, competitive advantage may be lost. In some cases, this may even be the end of the business.

Lawsuits for infringement or disclosure may not lead to a satisfactory result, particularly where the defendant can't be found, or the defendant may be judgment proof, having no assets to pay or being in a jurisdiction where they cannot be attacked.[7] Even where damages can be collected, they can be a very inadequate remedy. Of course, once the secret is out, an injunction forbidding the disclosure is often neither possible nor, if granted, effective.

In order to succeed in any litigation, the business will need to show that it took reasonable steps to maintain secrecy and, where the trade secret is in the form of information accessible via a network, this will mean proving that adequate security was maintained. Inadequate security is not likely to be rewarded by the courts.

5.4 Privacy

Canada now has legislation regulating the obtaining, retention, use and disclosure of personal information in the private sector. The Personal Information and Protection of Electronic Documents Act ("PIPEDA") was proclaimed in effect as of January 1, 2001.

---

[7] The Internet is, after all, global. Hackers often cannot be tracked. Even if located, they may be in jurisdictions where the legal system does not adequately deal with the issues.

PIPEDA currently establishes a right to the protection of personal information collected, used or disclosed in the course of commercial activities, in connection with the operation of a federal work, undertaking or business or inter-provincially or internationally (meaning it will apply to many Internet based exchanges or transfers of information).

As of January 1, 2004, PIPEDA will extend its application to every Canadian business or organization that collects, obtains, uses or discloses personal information in the course of a commercial activity, including within a province.

PIPEDA specifically requires adequate security as one of its principles. Further, lack of security may lead directly or indirectly to a breach of privacy and therefore of the legislation.

PIPEDA provides for the Privacy Commissioner to receive complaints concerning contraventions of the principles of privacy protection required by PIPEDA, to conduct investigations, to conduct audits and to attempt to resolve complaints. An audit or investigation may follow a complaint, or the Commissioner may conduct an audit or investigation on his own accord.

The audit and investigation provision is significant – an audit can include entering a place of business, compelling production of documents and requiring witnesses to testify under oath. Unresolved disputes relating to certain matters can be taken to the Federal Court of Canada for resolution, at which point the Court may make appropriate orders, including awarding judgment for damages, which may be punitive in nature if appropriate. There are also penalties for failure to comply with the requirements of PIPEDA, the maximum fine being $100,000.00.

5.5 Acceptable Use Policies and Monitoring of Employees

One major area of concern with respect to maintaining security is to ensure that employees are following correct procedures.[8] Employees should be educated in appropriate security practices and acceptable use of the network resources of the business. Businesses may find themselves vicariously liable for the conduct of their employees in their use of the Internet and email[9]. As many compromises of network security are inside jobs, it is likely in the best interests of management and the business to conduct monitoring of employees.

---

[8] There are many other issues around employee use of the Internet and email, such as pornography, gambling, creation of toxic workplaces, harassment, stalking, etc., but those are beyond the scope of this paper.

[9] Vicarious liability means that the employer may be held responsible for the actions of its employees, particularly where those actions involve use of the employer's resources or the appearance of employer approval, e.g., by use of the employer's stationery or domain name in email addresses. For example, there have been cases where employees have used the network of the employer for illegal uses, and the employer has been held liable. An Arizona company recently paid $1 million to the Recording Industry Association of America to settle a claim for employee use of its systems to exchange large number of MP3 music files, which infringed copyrights. The principle of vicarious liability may even apply to students, as educational institutions are in fact some of the largest Internet Service Providers around and provide students with the resources to use the Internet and engage in various activities, appropriate or otherwise.

Management may therefore decide to monitor employees' use of the business's systems and computers, thinking that they have the right to do so. In the United States, the courts have tended to uphold this right. While there is little case law in Canada as yet, it is likely that Canadian law will prove different, so management must proceed with caution.

The *Criminal Code of Canada* generally makes it an offense to intercept electronic communications without at least one party to such communication having granted consent. If the employee does not know of and consent to the monitoring, such monitoring may be essentially an illegal wiretap.

In addition, PIPEDA may forbid collection of employee information contained in emails, visits to Web sites or chat rooms, and so on, without a free and informed consent from the employee. PIPEDA will likely require at the very least that employees know at or before the time of monitoring or other collection of information that such activities are occurring so that employees do not disclose personal or private information in the mistaken belief that such disclosure is made in confidence.

Third parties in communication with employees may also have such rights under PIPEDA. Of course, obtaining consent from such third parties is practically impossible. The best possible solution is likely to be a clearly published privacy policy, giving notice of potential monitoring of any and all communications with the business or its employees. This policy should be posted on the business Web site and, in appropriate cases, could be included in the signature files in outgoing email in order to be sure third parties have notice of such practices.

The Canadian courts have also demonstrated a willingness to uphold and enforce the tort of invasion of privacy and to apply to private disputes in civil cases the values contained in the *Charter of Rights and Freedoms*, even though the *Charter* is stated to apply only to government conduct. Those values do not generally agree with surreptitious monitoring or other invasions of privacy.

All of this means that employers trying to maintain security and avoid vicarious liability for the actions of employees need to enter into contractual provisions with their employees in order to ensure they have consent to monitor and maintain adequate security and employee compliance with appropriate practices. Otherwise, the business and its management may be acting illegally in monitoring but will be subject to potential liability if they don't. Those contractual provisions should be in writing and should observe all the rules of forming valid contracts, including adequate consideration.[10]

6. LIABILITY OF DIRECTORS, OFFICERS AND MANAGEMENT

It is well settled in Canadian law that directors and officers of corporations owe certain duties to the corporation carrying on a business. Where such duties are breached, directors and officers may be held to be personally liable for damages sustained.

[10] The fact that the employee is employed may not be adequate consideration. It is in the past and it is often stated that "past consideration is no consideration." Foisting an agreement on the employees without adequately addressing this issue may prove ineffective.

It should also be noted that which specific individuals are officers can be a question of fact, so that the courts can hold that a senior employee in appropriate circumstances has been acting as an officer and may therefore be held liable. Upper management may therefore well find themselves being held to be in fact officers of a corporation.

6.1 Duty of Due Diligence

Essentially, due diligence requires that every director and officer of a corporation in exercising his powers and discharging his duties shall exercise the care, diligence and skill that a reasonably prudent person would exercise in comparable circumstances.[11] This is similar to the common law duty of care discussed under tort liability above.

There may also be other duties of care with respect to directors and officers, but whether or not those exist in any particular situation, the duty of due diligence is likely sufficient to create director or officer liability if reasonable standards of conduct are breached. If due diligence is not demonstrated, then the director or officer in question may become liable personally for damages sustained by shareholders, investors, lenders, etc. as a result of failure of the director or officer to fulfill his or her duty.

6.2 Fiduciary Duties

Directors and officers also owe the corporation a fiduciary duty, which is in essence a duty of trust and good faith, to always act in the best interests of the corporation and not their own interests, or the interests of a third party. This duty may also arguably be breached where directors and officers do not deal adequately with issues of security.

6.3 Director and Officer Liability

In addition to the above, there are many ways in which directors and officers can be found liable for failure to adequately perform their duties, both to the corporation and to others such as employees, investors, shareholders, etc. The list is long and the trend in the case law has been for it to grow longer. It does not have to be a large corporation nor does it have to be a public company for these to be real concerns.

7. ADEQUATE SECURITY AND LIABILITY

Clearly, directors and officers owe the corporate entity carrying on a business duties with respect to protecting the assets of the business from harm. They also owe the business a duty to protect it from liability to third parties, however that liability may arise.

Lawsuits against the business or prosecutions for breach of the law are not in the best interest of the business and may lead to loss of assets or indeed of the business itself. In the case of such losses, directors and officers may find themselves held personally liable

[11] See, for example, section 117(1)(b) of the Alberta Business Corporations Act.

to the corporation, and potentially to shareholders, employees, investors and others in close relationships with the corporation carrying on the business.

As in the expression, "the buck stops here", duties of due diligence and the like make adequate security not just a technical or legal problem, but above all a management problem. Therefore, security is not something that can just be left to the IT department. Doing so abdicates the responsibilities and duties of top management and fails in the proper performance of their duties. It will be no defence for directors and officers to claim they had "assumed" that the IT department had taken all steps necessary to ensure adequate security.

Indeed, the typical IT department, with all due respect, are probably not the right people for the job. They are trained in such matters as network administration or user support, and may have minimal knowledge of security. They have a vested interest in not reporting or admitting to breaches of security and in assuring management that all is well with the network and systems. They do not have the authority to institute and enforce proper procedures with all employees and users of the network and systems, which is required in order to ensure security. Indeed, in some cases it is an employee in the IT department who is the source of the problem.

Due diligence in many cases may therefore require setting up a security group separate from the IT department, or at least semi-autonomous. This group can act as a watchdog and, with appropriate management backing, may significantly increase security[12]. Of course, the group will require adequate training (which would be quite specialized and distinct from the day to day requirements of more typical IT managers or network administrators), funding and management support, as well as appropriate technological solutions to security issues. In many cases, it will be necessary to augment the security group with advice and solutions from outside (and therefore independent and, hopefully, trusted) consultants and advisors.

8. CONCLUSION

Management, directors and officers need to take security seriously. They need to face the fact that it may be they who will be held responsible for adequate (or inadequate) security. They need to obtain the right advice and follow it.

Proper practices and procedures need to be implemented throughout the business in order to avoid such things as easy to crack passwords or passwords written down in visible places (yellow *Post-It* note on the computer monitor, for example). The budget needs to provide for sufficient spending on training, technology, independent consultants and advisors, procedures and personnel.

[12] The writer has been involved in cases where such a watchdog might have prevented significant losses perpetrated by members of the IT department. In one case, a company's CIO was involved in transferring valuable source code to an offshore server around the time of tendering his resignation and preparing to leave the country.

Ultimately, unless management *walks the walk*, talking about security will not be enough. Unless they are lucky, directors, officers and management may at some point find themselves held liable should they fail to give security adequate attention and consideration.

As technology advances, adequate steps need to be taken to remain current with technologies and other practices available to maintain an adequate level of security. It will likely not suffice to have the adequate security of last year or the year before.

It is hoped that this brief overview will have assisted the reader in understanding the business and legal issues surrounding Internet and Network security. There is a great deal of further information on the topic on the Internet, and the technological solutions available continue to advance. For further information, readers are invited to contact the writer.

James Swanson, April, 2002

About the Author:

James Swanson practices law with the TechCounsel group of the Parlee McLaws law firm, a full service firm of over 100 lawyers based in Edmonton and Calgary. His practice focuses on Intellectual Property and Technology Law, with a particular emphasis on Information, Internet, Web and Computer Technologies, E-Commerce, Cyberlaw, and Intellectual Property, dealing with matters such as Copyright, Trademark, Trade Secrets, Licensing, Computer Law, Business Law and the protection and commercialization of new technologies.

James is a former professional musician (keyboards) who became a computer buff in the late 1970's. He received a B.A.Sc. from the University of Lethbridge and graduated from the University of Alberta Law School with an LL.B. in 1983 (*Dean's Honor List*) and was called to the Alberta Bar in 1984. He is also one of the first graduates (*1997, with distinction*) of the innovative Athabasca University MBA program, focusing on Information Technology and Globalization, and delivered almost entirely over the Internet. In his career, he has worked both as corporate counsel and in private practice.

He has written papers and other works and spoken, presented and consulted extensively on issues related to his practice on many occasions to a wide variety of recipients, organizations and audiences throughout western Canada, including government, business, educational and not for profit entities.

James is a past president of the Alberta Civil Trial Lawyers Association (ACTLA). He spent five years as editor of ACTLA's newsletter, the *Barrister*, and in 1996, he coordinated the design and implementation of the Association's Web site (www.actla.com) as part of his MBA dissertation.

James is a Bar Admissions Course Instructor in Intellectual Property and Internet Law for the Legal Education Society of Alberta and the Law Society of Alberta and has recently revised the Intellectual Property section of the Bar Admission course. He is a member of the academic faculty of Athabasca University with regard to the Business Law elective for MBA students. He is also a columnist with the *Edmontonians*, writing a regular section on Cyberlaw and e-Commerce.