BNAC

B R I T I S H - N O R T H A M E R I C A N C O M M I T T E E

Draft report for review and comment

Cyber Attack — Risk Business Owners and Executives Must Manage

British-North American Committee

Sponsored by

Atlantic Council of the United States

British-North American Research Association (UK)

C.D. Howe Institute (Canada)

Abstract

Over the past 15 years, business owners and executives have come to rely increasingly on corporate networks, and their interconnection with the global Internet, as the backbone of their business sales, sourcing, operating and financial systems. Few situations, therefore, can be more embarrassing, or in many cases devastating, to these executives than the realisation that a corporate network, and its interdependence with the global Internet, may be the point of greatest vulnerability, and that success today depends in large part on the security and stability of that infrastructure. In many instances, an under-defended cyber attack could cripple even the largest corporations.

Business owners and executives can ill afford to expose the security and stability of their operating and financial systems, confidential information, intellectual property and business transactions to cyber predators through either lack of knowledge or lack of initiative. Corporate officers should also be aware that the nature of the Internet demands that their concern must extend to their business partners as well as their suppliers and vendors. The multi-layered, designed-in redundancies and protections that make the Internet so resilient are simply too costly to implement and maintain within an individual business network.

In addition, cyber criminals intent on harvesting corporate data, interrupting corporate business or compromising corporate computers and networks to launch attacks on other networks are immensely creative. Law enforcement can be effective, but only after the damage is done. Businesses are left with the escalating costs of recovery, including loss of trust on the part of their customers, a large percentage of whom move on to competitors that they perceive as better able to protect their personal information.

Chief executives and business owners must deploy a full suite of network, system and information security measures that encompass security policies and practices, technology solutions, and ongoing education and training.

There is also a complex legal situation surrounding the protection, release and storing of data, with Europe, the United States and Canada adopting different policies and laws. But many countries where corporate data services have been outsourced have no laws at all.

It follows that CEOs and their IT and security and legal staffs should deploy a complement of defenses that encompass network security policies and practices that demand supplier and Internet service provider management, technology solutions, and ongoing education and training. Moreover, maintaining and updating these measures on a regular schedule will ensure the continuity, stability, security and operability of their corporate networks, including their supply chains, and foster an information security corporate culture.

Further, while extremely resilient, the Internet's core infrastructure and operations also face increasing numbers of attacks. The multi-layered and private sector-led coordination of the Internet has effectively countered these threats. But CEOs must recognize that the Internet does not just happen, and that the private sector-led multi-stakeholder approach to its global security and stability requires their continuing recognition and support.

Why Should Chief Executives Act Now?

The business costs of cyber predation and cyber terrorism are already staggering. Indeed, the cost of virus or malware attacks in the U.S. alone between 2000 and 2005 amounted to $86.1 billion. In 2006, security incidents and breaches cost U.K. businesses up to £10 billion ($17.9 billion) annually, double the amount two years earlier.[1] Globally, malware and viruses cost businesses between $169 billion and $204 billion in 2004, and the trend is rising sharply. According to digital risk management firm mi2g, malware in 2003 did not account for even half of the economic damage sustained in 2004.[2] This works out to between $281 to $340 worth of damage per enterprise computer. The security of networks and the investment required to build that security has already been flagged by the U.S. Department of Homeland Security as a much-needed priority.

Moreover, the number of phishing attacks is rising exponentially, along with the costs of defense and recovery. Attackers' motivation is increasingly financial, with extortion, thefts of credit card details and abuse of private information proving more and more lucrative. In addition, spam now makes up 94 percent of all email traffic. This continued rise in spam levels is "threatening the viability of email for businesses and is sapping the productivity of hundreds of millions of workers around the world."[3] In terms of productivity alone, the losses are enormous. Just the time employees spend each day dealing with spam email can quickly add up to tens of billions of dollars worldwide.

Phishing and spam are just a part of the network and information security vulnerabilities facing CEOs. The recent examples given here are representative of a far larger problem.

- In one instance, a chief executive officer who built a multimillion-dollar software business found that the corporation's domain name address was no longer in the control of the corporation, but rather had been co-opted by domain name speculators. This domain name address was the only route through which hundreds of thousands of dollars of sales were made each day.

- In another instance, a multimillion-dollar infrastructure business was rendered unable to conduct business for more than 36 hours after a concerted and very sophisticated denial of service attack.

- Several European financial services institutions were the targets of extortion demands by criminal groups who had effectively launched denial of service attacks against their networks.

- Again, a major international corporation lost tens of millions of dollars of productivity after its principal computer systems and even its employees' individual computers were infected with a debilitating virus.

- A major international media company purchased a significant online business, but senior executives failed to ensure robust and redundant supplier and ISP support, leaving the acquisition vulnerable to attack at single points of failure.

- At least eight to ten Wall Street financial firms were unable to recover quickly from the effects of a terrorist attack owing to the poor data security policies and practices of one of their key suppliers.

- Dozens of Western corporations have seen vital business data lost or stolen owing to inadequate controls and lack of attention paid to security in outsourcing contracts to India, China and the Philippines.

- Finally, several banks had to pay millions of dollars in restoration fees and penalties because poor initial authentication protocols left their customers open to phishing attacks.

Businesses no longer operate as discrete entities. Their operating, financial and transactional network backbones are inextricably linked to Internet-based supply chains. Indeed, doing so is a key part of a company's business strategies because today's networked economy delivers millions of dollars worth of transaction cost savings to American, Canadian and British businesses every day.

While CEOs have reorganised their businesses to take advantage of these new efficiencies and business opportunities, they must also act to protect themselves against the increased risks inherent in doing business on the Internet. Managing risk is a key role for executives, and therefore they must foresee and understand what risks they face from the cyber world.

What Kinds of Risks Do CEOs Face?

The graphic below summarizes the risks that facing chief executives and business owners today. Each threat is discussed in greater detail together with preventive countermeasures corporations can deploy to combat them. Not all threats come from outside and not all stem from criminal intent. Nevertheless, the evidence is clear: corporations cannot afford to overlook or treat any of these threats lightly.

Threat	Risk	Solutions: Policy and Practice	Technology	Security	Education
Malicious Attacks					
Denial of Service (DOS) and Distributed Denial of Service (DDoS)	Disruption of network services and functions; network or server overload; shutdown	✓	✓	✓	
Phishing and Spam	Loss of productivity; corruption of operating systems, applications, programs, files		✓	✓	✓
Hijacking Corporate Domain Names	Risk to trusted corporate name; loss of intellectual property; huge recovery and restoration (including legal) costs for vandalized systems; threat of extortion	✓		✓	✓
Viruses and Malware	Loss of productivity; corruption of operating systems, applications, programs, files	✓	✓	✓	✓
Bugs and Security Holes	Disruption of network services and functions; network or server overload; system shutdown		✓	✓	✓
Non-malicious Threats					
Technical Outages	Disruption of network services and functions; network or server overload; system shutdown	✓	✓		
Supply Chain Risks	Risk to trusted corporate name; loss of intellectual property; huge recovery and restoration (including legal) costs; threat of extortion	✓	✓	✓	✓
Client and Server Negligence	Risk of penetration of networks, operating systems, and applications; corruption of operating systems; disappearance of intellectual property	✓	✓	✓	✓

Denial of Service (DOS) and Distributed Denial of Service (DDoS)

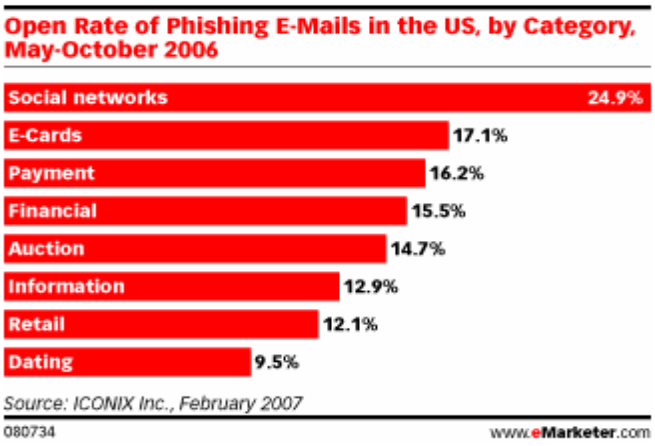
The distributed denial of service attack on the Internet's root servers in February 2007 showed that coordination and preparation are key to uninterrupted network stability and operability. The Internet Corporation for Assigned Names and Numbers recently prepared a fact sheet detailing that attack and its potential for disruption of all Internet-based functions[4]. That fact sheet makes clear that such attacks are not going to go away and, if anything, may increase in future. They are also increasingly being directed toward corporate networks, often as part of criminal extortion rackets. While the Internet's designed-in redundancies and protections are too costly to implement on a network level, there are solutions every chief executive should make it a policy to deploy and maintain.

Policy and practice solution – The most efficient management solution to such problems is the effective implementation of provisioning and filtering. Provisioning enough overhead and redundancy in bandwidth and systems to ensure that any increase the volume of attack traffic can be handled, and filtering to prevent unnecessary or illegitimate traffic from entering the network. Good working relationships with Internet service providers is critical in helping to push back attack traffic to the point where it is no longer a menace to corporate networks.

Security solution – Regular testing of access control lists, firewall software and other edge devices is also best business practice. Commercial products that detect abnormal traffic patterns and act accordingly to filter and protect the network edge are available, and both can be incorporated within routing equipment or can operate as stand-alone items.

Phishing

Phishing, one of today's most insidious attack mechanisms, can affect every aspect of a corporation's business. Not only can it redirect corporate staff to forged sites but it can also be used to redirect customers to a site imitating the corporate site. This is particularly common for corporations in the financial services business, where it undermines consumer confidence in online banking—a potentially expensive problem that must be handled well into the future. Phishing can also be a means of compromising entire computer networks that can then be used to launch attacks on other networks and individual computers linked to a corporation's supply and distribution chains.



Based on actual recorded email behaviour, the open rate of spoofed messages is highest when coming from social networking sites, followed by e-card, payment and financial sites.

Technology solutions – The current technology solution is the installation of an SSL certificate on corporate web servers. It is important to ensure that the certificate authority is supported by most browser applications. Newer browser applications and some stand-alone software solutions have the ability to detect sites that are suspicious and raise alarms.

Security solutions – Often, attackers enter by cracking simple passwords, a persistent weak point on many networks. Setting different levels of access to different staff members not only bolsters security but also underlines the seriousness with which security is taken in the organisation. Enforcing regular password changes and the use of complex passwords are critical to ensuring that comprises by this mechanism are controlled.

For organisations having a predefined clientele, it is possible to increase authentication strength. Distribution of one-time, or short-lived, password technologies—called tokens—can be an effective measure. Systems in which the customers use devices that

generate a new password every 30 seconds have been available on the market for many years. This same technology can be used for other places where clients or staff must access systems.

Education solutions – Chief executives must ensure that technology solutions are combined with user education around what to look for should an incorrect or unknown certificate warning occur in their browsers. On average, email users open one in six phishing messages. Based on industry estimates that 59 million phishing messages are sent each day, as many as 10 million fake messages may be opened each day, creating huge risk for people receiving the messages—and for the corporations that employ them.

CEOs would thus be wise to implement continuing training and educational programs on recognising and defending against fake messages. Such programs could start with new employee orientation, then go on to include web-based or intranet-based interactive refresher training. They certainly should include security alert messages delivered through push systems to all corporate employees and to all corporate partners.

Nevertheless, it would be a mistake to assume that the phishing we see today is what CEOs should have their security and IT staff design network infrastructures to combat. Major losses are never due a single point of failure but a combination of flaws whose relationship to one another is often not noticed until afterwards. Far more cunning attacks are already prevalent. Thus, infrastructures must be designed that are both reusable and adaptive and will take a corporation at least five years into the future.[5]

Hijacking Corporate Domain Names

Cyber criminals are finding the hijacking of corporate domain names—especially those that are so well known they have entered the lexicon or are associated with banking, finance, and related businesses—so lucrative in the past few years that corporate executives and business owners should dedicate special teams of security, legal and network experts to their prevention. Of course, once a domain name is hijacked or corrupted, the content of the domain is also open to predation. The effects of hijacking are often many-fold: the domain name owner can lose an established online identity, with all that implies, as well as valuable intellectual property, and can also have the corporate domain name held up for extortion. Further, these incidents often affect more parties than just the rightful name holders: customers, business partners, consumers of services provided by the name holder, and even parties wholly unrelated to the name holder often suffer collateral damage in hijacking incidents.

The High Price of No Protection

- **Productivity declines** as employees scramble to restore what's been lost or vandalised rather than doing their normal jobs.
- **Lost revenue** from disrupted transactions. Customers, suppliers, partners can be affected if, say, key databases have been made inoperable by a hacker or virus.
- **Vandalised systems** that take time and money to bring back to normal operation.

Unfortunately, most domain name hijacking scenarios arise through flaws in registration and related processes, failure to comply with domain name transfer policies, and poor administration of domain names and authentication information by registrars, resellers and registrants. This leaves a field ripe for picking by hijackers. The Security and Stability Advisory Committee of the Internet Corporation for Assigned Names and Numbers has

researched and reported extensively on this growing field of cyber crime and provided an array of solutions business owners and chief executives should take to protect their domain names from this particularly widespread form of predation.[6]

Because these attacks are so damaging and because they have the potential to disrupt business at all levels over the long term, the corporate focus must be on prevention rather than recovery and restoration.

Policy solutions – A system-wide multi-layered enterprise operating policy is the first line of defense against domain name hijackers. Corporate legal staff who are experts in domain name registration, transfer and protection must have free rein to build the most up-to-date, creative business and legal solutions to prevent exposing the corporate domain name and domain content to risk. The accuracy and integrity of all domain name records must be reviewed and updated regularly with registrars.

Security solutions – Although some technology solutions such as Register-Lock are available to deal with domain name hijacking, they should not be relied on as the sole source of protection. Domain holders would do well to have an emergency action plan in place and operating that will immediately intervene when a domain name is perceived to be at risk and will also immediately begin restoration of the domain name registration information and domain name system configuration. Emergency plans should clearly lay out practices covering protection of domains, including routine monitoring of domain name status and timely and accurate maintenance of contact and authentication information. Such emergency plans should be communicated to all the business partners and suppliers and should be updated and tested regularly.

Education solutions – Business executives must ensure that all their employees, contractors, business partners and suppliers are aware of the threats of domain name hijacking as well as impersonation and fraud. Clear practices should be in place for recognizing and reporting any suspicious behaviour. A false alarm is, after all, easier to deal with than an extortion threat.

The High Price of No Protection

- **Lost data** when backups don't work properly, or when a virus or Trojan horse infiltrates your system.
- **Competitive secrets stolen**, along with the potential business opportunity and product/service revenue streams they represented..
- **Compromised customer confidence** when security breaches result in late shipments, order errors, etc.
- **Legal liability** when sensitive information is stolen and contributes to theft of customer or employee identity and/or is otherwise misused.
- **A disconnect between security policy and security implementation.** Security systems and tools should be configured to enforce security policies. Any other choice leaves a business dangerously vulnerable.

Viruses and Malware

Viruses and malware account for a large percentage of the cost to businesses of data breaches, data loss and data corruption.[7] Other factors are lost or stolen laptops, records lost by third-party business partners and lost or stolen backup files. A 2006 survey[8] of 56 individual companies found that each company sacrificed roughly $2.5 million in lost business, with one particularly hard-hit company losing $22 million.

These figures combine costs from legal, investigative and administrative expenses with information related to affected companies' stock performance and customer defections, among other

indicators. The average financial losses and overhead expenses related to data leakage incidents increased in direct relation to the number of records lost, and the cost per lost record rose from $75 in 2005 to $98 in 2006, a $22 leap. This trend is more than likely to rise sharply over the next few years.

The unifying theme here is that all data today is digitised, making it in many ways more vulnerable than traditional paper records, especially since data loss can come from anywhere within a corporation's network of supplies, vendors, partners, customers and even employees.

Policy solution – CEOs must ensure that not just their companies' networks but also the networks encompassing their supply and distribution chains implement and maintain the same suite of solutions across the board. Like all other chains, a network supply chain is only as strong as its weakest link.

Technology solution – Chief executives should ask their IT staff to choose a tiered anti-virus solution. Many viruses can be detected by network devices and contained before they approach corporate servers and desktop computers. Anti-virus protections at the network, server, and desktop level will prevent corruption by most viruses. It is important that any solution chosen is always maintained with the latest updates.

Security solution – Security staff should have a policy of implementing and enforcing strict protocols for removing or distributing digital records from corporate premises and among corporate partners.

Education solution – Employees and corporate partners must be made aware of the risks and costs of data breaches and data loss. These costs are escalating in correspondence with the growth in the types and volume of attacks. Ongoing education and training in network, computer and information security will contribute significantly to keeping these costs to a minimum.

Bugs and Security Holes

There is no such thing as 100 percent secure software, and corporations must necessarily run dozens of software applications and programs as part of doing business, thus providing the potential loopholes cyber criminals are standing ready to exploit.

Technology/security solutions – Operating system and applications developers regularly release security patches for operating systems, applications and programs. It is critical that corporate IT departments keep abreast of these changes and upgrade to the latest stable version of the software they are using whenever feasible.

Education solution – Part of any corporation's ongoing education and training in network and information security should include the importance of installing these security patches at the time of release by the corporation IT organisation.

Technical Outages

Stuff happens, including non-malicious technical outages. And corporate executives must ensure that, to the extent possible, all contingencies have been foreseen and that

alternatives are available to ensure network security, stability and operability. Business systems should be designed to withstand the loss of individual parts or sections of the infrastructure.

Policy solutions – As with the Internet itself, redundancy is possibly one of the most effective solutions to limit damage caused by such outages. Corporations should examine their systems for single points of failure and eradicate these to the greatest extent possible. Some techniques, including multi-homing or providing more than one access route to the Internet, are important for critical services. It is also best to ensure that each of these paths to the Internet runs on separate router hardware in case of hardware failure.

Technology solutions – Critical services, such as customer portals and the data infrastructures that they access, can be built using mechanisms ranging from data backups (which take time to back up) to full blown off-site live mirrors that can become active in minutes or seconds.

For each of the parts that make up a corporation's infrastructure, it is important to understand the effect of temporary or permanent loss of that part and the cost of implementing the various options for redundancy. This understanding will enable corporate executives to make a cost/risk analysis and choose the best solution for their specific case.

Supply Chain Risks

In a networked economy no business is an island. Everything is connected. So even if a business ensures that its own network operations are reasonably secure, it can still be very vulnerable to the risks not addressed by its suppliers, partners, distribution channel or customers.

Policy solutions – Ensuring a due diligence program for existing or prospective partners should be a key part of business risk management. One CEO of a media company paid $400 million for an online business which was being leveraged to grow other business assets. This acquisition was part of an international investor road show. Neither the CEO nor his senior reports had checked on the acquisition's network supply. Investigation showed that it had little network redundancy and was particularly vulnerable to DDoS attack. Consider how badly the investor road show would have evolved if such an attack had been made. Shifting the acquisition to a more robust network supply situation required an investment of millions of dollars and took many months.

Technology/security solutions – Best practice requires continual oversight of a corporation's entire network structure, including any extensions. IT can implement regular testing along the network chain, and security staffs can investigate compliance with due diligence programs.

Education solutions – Education about all aspects of network and information security should be ongoing, should be updated along with infrastructure upgrades and should involve a corporation's employees, contractors and any entity having access to the corporate network systems.

Client and Server Negligence

Many malicious attackers take advantage of systems that are not kept up to date with the latest applications and operating systems. Negligence within the corporate IT structure can lead to severely outdated systems that may present exploitation points that are well known to predators. Corporate and network servers are at equal risk.

Exploits—penetration by predators—can disrupt websites, capture personal information and even lead to the complete compromise of a machine, turning it into a botnet zombie ready to participate in a larger-scale attack against other corporations. Should that happen, the corporation hosting the compromised machine may be at risk of legal action for not protecting its servers and client machines from predation by allowing operating systems and applications to become outdated.

Policy solutions – Corporate IT policy and practices should encompass regular updates to client and server systems. IT and security staff also should monitor these systems and applications at regular intervals to ensure they have not been compromised.

Technology solutions – Corporate policy and practices should also allow for regular replacement of hardware and software. IT staff should compile a database of all networked equipment, including wireless access devices, and should regularly verify that all such equipment is in place and properly maintained. Corporate IT staff should continually check with software vendors to ensure updates and patches are current. The return on investment in these preventive measures must be measured against the cost of unmanaged risk.

Security solutions – Regular interaction with CERT and other advisory companies, and subscription to their publications, security alerts and other preventive or cautionary services is a must.

Education solutions – Education about all aspects of network and client/server security should be ongoing, should be updated along with infrastructure upgrades and should involve a corporation's employees, contractors and any entity having access to the corporate network systems.

Does Your Company Have an Information Security Culture?

More and more companies are seeing the value in incorporating the concept of information security into their corporate culture. A strong security policy sets the security tone for the whole company and lets its employees know what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it.

In fact, a recent survey[9] published by *The Economist* reported that 45 percent of U.S. companies have appointed a Chief Risk Officer, with another 25 percent planning to recruit one within the next two years. Another survey reported that responsibility for IT security was represented at board level in 55 percent of companies.

With telecommuting and wireless devices, the workplace demographic is changing. Information security policies and practices must be able to adapt quickly to ensure that valuable networks, hardware, software and data remain secure.

Increasingly, budgets are being equally divided between staffing and external services such as vulnerability audits and risk assessments.

All this is in response to the changes in workplace demographics. The number of people working from home or otherwise remotely at some stage of their week has nearly doubled in the past six years to 28 percent of the workforce. Workers are more mobile and are using wireless communications, freeing them from the confines of the office but at the same time bringing fresh challenges for IT and security managers.

Common Mistakes Businesses Make

As businesses grow, information technology becomes increasingly more important to their operations, but ensuring that it is well-adapted to each corporation's needs is becoming tougher and tougher.

To keep businesses and processes functioning soundly, systems, networks and data all must be cost-effectively managed, even as business infrastructure becomes more complex. Malicious attackers are constantly on watch for small oversights in a corporate network infrastructure. Some of the loopholes attackers look for are:

- *Not keeping current on operating/application/antivirus software patches and updates.* Online hackers and criminals keep breaking their previous speed-of-defect exploitation records. Failing to patch and update software means they will penetrate corporate defenses sooner rather than later, so it is important for corporate IT staff to continually check with software vendors to ensure updates and patches are current.

- *Poor handling of sensitive data.* Is valuable intellectual property backed up? If it changes frequently, is there a process to back up those changes? Is it locked down? Can IT and security staff restore backups in a timely manner?

- *Not deploying encryption where available.* Today's businesses rely heavily on the Internet to transmit and transfer all kinds of data. However, the Internet is like a series of post boxes, the contents of which can be easily read and copied. If sensitive data must be private, then it must be encrypted.

- *Sacrificing security for convenience.* A strict security policy covering handling of corporate networked devices and intellectual property is a must. The installation of unauthorized software and applications from any source should be prohibited. The physical removal of data from corporate facilities should be strictly controlled and monitored. Employees should be made aware that while security may seem a hassle, lack of security bears far greater consequences. Chief executives must establish an information security policy and stick to it.

So how should implementing a stringent policy and infusing a solid security culture be undertaken?

1. *Make information security everyone's responsibility.* Everyone working for an organisation, including temporary staff and contract workers, must know exactly

what is expected of them. Further, the corporate security policy should be living and breathing—a resource relevant to the business and its risks—not just a checklist or a manual. Begin with a risk analysis to identify what is relevant and what is not.

2. *Rest responsibility for security with senior management.* Doing so gives information security the importance it deserves and means that decisions regarding policy are carried through. In larger or more extended businesses, a chain of command must exist so that all security issues are covered and taken responsibility for.

3. *Hold a security audit.* A company-wide research and analysis will expose vulnerabilities and strengths and give a complete picture of the organisation's security requirements. Consider contracting a third party organisation to perform that audit. Third-party agencies have the expertise and objectivity that ensure the audits goals are met.

4. *Underpin a robust security culture with frequent and rigorous testing.* This not only sends a strong message of compliance to employees and others, but it also means that any changes in the network, for example, can be included. Indeed, for some organisations network access points are in a constant state of flux. Regular testing will ensure that such changes are kept mapped and secure.

5. *Make education and training an ongoing exercise.* It is all very well to have a security policy in place, but unless staff members know how and why it operates, its points will be diminished. Security training should become a permanent function, with regular information updates offered, training given and alerts as required.

6. *Make keeping abreast of changes in security technology and best practices a priority.* It is important that resources are specifically designated for keeping track of any current and upcoming changes that are required to keep ahead of the game in the security of systems. New attacks and new solutions are continuously being developed. Those upcoming developments should be part of purchasing decisions. Ensuring that newly purchased hardware has the capability to either support or can be upgraded to support new technology both increases security options and saves long-term costs.

To stay abreast of the current state of Internet and network security threats and solutions, and to ensure that they can continue to rely on a secure and stable Internet for transacting business, senior executives and business owners must play an active role in developments surrounding the Internet. Since its inception, the Internet and its systems have been coordinated, not managed, through a private-sector led multi-stakeholder model that works collaboratively to coordinate the Internet's core functions of security, stability and operability. Those stakeholders come from the worlds of technology, science, industry, business, academia, government, the public and private sectors and civil society. Every stakeholder has an equal stake in the security, stability, and global interoperability of the Internet and its millions of linked enterprise networks, and every contribution or opinion is considered with equal weight and gravity.

To ensure that private-sector businesses around the world can use an Internet that enables rather than impedes their ability to transact business, chief executives should feel impelled to participate in their stakeholder community. Doing so will continue to contribute to the functionality and vitality of the global Internet and its core functions.

Conclusion

The costs of interruption to business are great and the risks are high. And the trend is rising. Forward-looking chief executives and business owners must make information security a continuing priority and give senior management the authority to implement network and system information security policies and practices.

Best practice in ensuring network security, stability and operability is defined by a corporation's ability to deploy an entire suite of coordinated tools and measures encompassing policies and practices, technology, security, and education and training. Only the full complement of solutions can support and secure a corporation's infrastructure and guard it against malicious attack and other potential outages. Making sure that all these measures are upgraded and updated regularly should be integral to the backbone of a corporation's business operating and financial systems.

Chief executives and business owners would do well to heed the words of Vint Cerf, chief Internet evangelist at Google and father of the Internet. He says the biggest threats not only to the Internet but to all networks linked to it are the proliferation of spam, botnets, malware and denial of service attacks. "Much work is needed to increase the security of the Internet and its connected computers," he says, "and to make the environment more reliable for everyone. Security is a mesh of actions and features and mechanisms. No one thing makes you secure."[10]

Glossary of Terms

botnet – Compromised computers, or "zombies", are combined to form "botnets" which can then be directed as required—typically to deliver distributed denial of service attacks or phishing attacks. Botnets are most commonly created by conning ordinary consumers into opening something on their computer that appears to do nothing but which installs hidden software to be used later for an attack.

Domain name hijacking – the practice of stealing the domain names of corporate registrants, especially those of well-know firms, in order to defraud the name holder's clients, steal intellectual property, and hold trusted names up for extortion.

Distributed denial of service attack, or DDoS – a denial of service attack in which an attacker uses malicious code installed on various computers to attack a single target. An attacker may use this method to have a greater effect on the target than is possible with a single attacking machine. On the Internet, a distributed denial-of-service (DDoS) attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users.

Malware (malicious software) – The uses of malicious software range from placing excessive demand on a computer's resources to destruction of data or even hardware. In some cases the user is made aware of the presence of the malware, for example, when it sends a message to the user or deletes the contents of a hard drive. Recent forms of malware may operate without the user's knowledge, steal financial information such as credit card details, or convert infected computers into an asset for the attacker. Common types of malware work as follows:

- Viruses infect computers or other electronic devices and are passed on by user activity, for example, by opening an email attachment.
- Worms self-propagate using an Internet connection to access vulnerabilities on other computers and to install copies of themselves. They are often used as a conduit to grant attackers access to the computer.
- Trojans are malware masquerading as something the user may want to download or install, that may then perform hidden or unexpected actions, such as allowing external access to the computer.
- Spyware transmits information gathered from a computer, such as bank details, back to an attacker. For example, "keylogging" software records anything entered using the keyboard, such as passwords.

Technological solutions – The following solutions can help block attacks on servers, networks and computers:

- Firewalls are hardware or software devices that block certain network traffic according to their security policy.
- Authentication involves determining that a particular user is authorised to use a particular computer. This can include simple mechanisms such as passwords, to more complex methods using biometric technology.
- Hardware cryptography uses computer chips with cryptographic capabilities intended to protect against a range of security threats.
- Patches are programs designed by software manufacturers to fix software security flaws. Patching is often installed automatically. This reduces end-user participation and increases ease of use.

Tokens – short-lived, one-time passwords used primarily by financial institutions that are randomly rotated or disposed of after one use. Tokens are also used effectively in blogs.

Endnotes

[1] Article titled *Analysts eye revamp of U.K. cybercrime law*, Networkworld.com, 7 June 2006. See http://www.networkworld.com/news/2006/060706-analysts-eye-revamp-uk-cybercrime.html?inform.
[2] Article titled *Cost of malware soars to $166bn in 2004*, Vnunet.com, 1 February 2005. See http://www.vnunet.com/vnunet/news/2126635/cost-malware-soars-166bn-2004.
[3] Daniel Druker, executive vice president of marketing, Postini, quoted in DarkReading, January 2007. See http://www.darkreading.com/document.asp?doc_id=114418.
[4] ICANN Fact Sheet titled *Root Server Attack on 6 February 2007*. See http://icann.org/announcements/announcement-08mar07.htm.
[5] "Authentication infrastructures cost money and ROI should be measured in terms of at least five years." Article titled *Phishing and forward looking financial institutions*, Financial Services Technology, US Edition. See http://www.USFST.com/pastissue/article.asp?art=268947&issue=183.
[6] Domain Name Hijacking: Incidents, Threats, Risks, and Remedial Actions, report by ICANN SSAC dated 12 July 2005. See http://icann.org/announcements/hijacking-report-12jul05.pdf.
[7] CA 2007 Internet Threat Outlook, January 2007. White paper published by CA, a New York State security consulting firm. See http://www3.ca.com/Files/SecurityAdvisorNews/ca_2007_internet_threat_outlook_final.pdf.
[8] Article titled *Cost of Data Breaches Rises Sharply*, by Matt Hines, eWeek.com, October 20, 2006. See http://www.eweek.com/article2/0,1895,2034667.00.asp.
[9] Article titled *Implementing an information security culture*, by John Redeyoff, Director of Information Security, NCC Group, Financial Services Technology, US Edition. See http://www.usfst.com/pastissue/article.asp?art=268975&issue=183.
[10] Vint Cerf, quoted in DarkReading, March 2, 2007, article titled *Father Knows Best*. See http://www.darkreading.com/document.asp?doc_id=118596.