BRITISH-NORTH AMERICAN COMMITTEE

CYBER ATTACK:

A RISK MANAGEMENT PRIMER FOR CEOs AND DIRECTORS

SPONSORED BY

The Atlantic Council of the United States
British-North American Research Association
Internet Corporation for Assigned Names and Numbers

The British-North American Committee is a group of leaders from business, labor, and academia in the United Kingdom, the United States, and Canada committed to harmonious, constructive relations among the three countries and their citizens. It meets regularly to discuss common concerns with invited experts and senior policymakers in an off-the-record setting, and its regular research and publishing program seeks to discover and disseminate potential solutions. While nonpartisan and supportive of closer economic and political relations on a broad international basis, the BNAC believes that close personal ties and cooperation among leaders from various spheres in the three countries will in the future, as in the past, play a special role in promoting global security and prosperity.

Implicit in the Committee's existence is recognition that the three countries share ties that go beyond economic and security questions, extending to issues of culture and habits of mind. Although the Committee has never sought to be a policy institute, its regular commissioning and publishing of research testifies to its members' desire to disseminate useful analysis of issues of common concern.

The British-North American Committee is sponsored by three nonprofit research organizations - the British-North American Research Association in London, the Atlantic Council in Washington, and The Massey College of University of Toronto in Canada. Alan R. Griffith, formerly of the Bank of New York, and Sir Paul Judge, chairman of Teachers TV, are, respectively, the North American and British co-chairmen. Professor Thomas H.B. Symons, C.C., is chairman of the Executive Committee.

Disclaimer

The views expressed in this publication are those of the BNAC members who have endorsed it (see page 9). They do not necessarily reflect the views of the BNAC membership as a whole, nor of the Atlantic Council of the United States or the British-North American Research Association and its Council and Members, or the Internet Corporation for Assigned Names and Numbers.

BNAC
BRITISH-NORTH AMERICAN COMMITTEE

Revised and reprinted April 2008

Executive Summary

Today's businesses rely increasingly on corporate IT networks and their connection with the global Internet as the backbone of their sales, sourcing, operating, and financial systems. However, the convenience of global connectivity comes at a cost—the vulnerability of network infrastructures and systems to the malicious actions of cyber criminals and espionage agencies. Yet few CEOs or managing directors are prepared to lead their companies against these dangers. Too often CEOs and directors fail to understand the level of potential risk and liability, and cede responsibility for dealing with cyber attacks to their IT department. Instead, leaders of corporations, nongovernmental and not-for-profit organizations, and public sector agencies in the 21st century must know enough to at least ask the right questions of their chief information officer.

No business, government, nongovernmental, or other organization of whatever size is invulnerable to cyber attacks. Business owners and executives, including managing directors, cannot afford to put at risk the security and stability of their operating and financial systems, confidential information, intellectual property, and business transactions to cyber predators through lack of knowledge or initiative. Just as CEOs and directors are responsible for ensuring that their chief financial officer has managed their funds appropriately, so they must be convinced that the CIO has taken all reasonable and prudent steps to safeguard the company's digital resources. Moreover, the nature of the Internet demands that corporate officers extend these concerns to their business partners, suppliers, and vendors, by insisting that they also take precautions against electronic aggression that could put both parties at risk.

"Much work is needed to increase the security of the Internet and its connected computers 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."

– Vint Cerf
Chief Internet evangelist at Google and father of the Internet.

Successful cyber attacks are rarely made public, but the following have all happened in the past few years.

The Cyber War Lines Have Been Drawn

• In April 2007, the small northern European country of Estonia was nearly brought to its knees after three weeks of attacks on key websites—including government, banking, and business.

• These attacks, originating from multiple sources, were unsophisticated but effective, often saturating links that connected towns and counties to the Internet.

• Although small, Estonia relies heavily on the Internet. This attack cost the country, its institutions, and its citizens much trouble and money.

• Together with earlier, similar attacks targeting governments in the Middle East and the Balkans, these show that as societies become more reliant on Internet technologies, these same technologies become a conduit for protest and attack by the disaffected.

What Risks Do CEOs Face?

• One CEO built a multimillion-dollar software business but found that the corporation's domain name address had been co-opted by speculators. This domain name address was the only route through which hundreds of thousands of dollars of sales were made each day.

• A multimillion-dollar infrastructure enterprise was unable to conduct business for more than 36 hours after a concerted, very sophisticated denial of service attack.

• Several European financial services institutions were targeted by criminal groups who launched denial of service attacks against their networks and then issued extortion demands.

• A major international media company purchased a significant online business, but the acquisition was vulnerable to attack after senior executives failed to ensure robust and redundant supplier and Internet service provider support.

• Dozens of western corporations have seen vital business data lost or stolen because of inadequate controls and neglect of security in outsourcing contracts to India, China, and the Philippines.

• 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.

Criminal attacks on the Internet's systems and cyber espionage are on the rise, and, in the case of domain and address theft, are increasing exponentially. Cyber criminal gangs are increasingly motivated by the potential gains from extortion, theft of credit card details, and abuse of private information. Sophisticated, persistent groups—particularly organized criminal gangs and state or corporate espionage agencies—are targeting specific enterprises to steal intellectual property and conduct fraud or other money-making activities. Moreover, according to the most recent Symantec Internet Security Threat Report[1], attackers are now creating global networks that support coordinated criminal activity. All this sophisticated criminal activity has driven up the costs of defense and recovery.

The business costs of cyber crime and cyber terrorism are already staggering. Globally, malware and viruses cost businesses between US$169 billion and US$204 billion in 2004, and the trend is rising sharply. According to digital risk management firm mi2g, the economic damage caused by malware in 2004 was more than twice that sustained in 2003.[2] Even the cost of spam is significant: costs associated with spam in the United States, United Kingdom, and Canada in 2005 amounted to US$17 billion, US$2.5 billion, and US$1.6 billion, respectively.[3]

What Mistakes Do CEOs Make?

Few CEOs or business and government leaders are IT professionals. For many, their primary interaction with their IT department happens when their own computer or email malfunctions. Given the speed of change in the digital world, it is easy to become overwhelmed. As a consequence, too often CEOs fail to pay adequate attention to whether their own corporation has a sufficient strategy against cyber attacks. In particular, they:

Underestimate the scale of the problem.

The U.S. Computer Emergency Readiness Team (CERT) has been tracking an upswing in targets among the entire online economy, including the financial, aerospace, defense, and computing industries, and reported 80,000 instances in March 2007 alone. Even spam by itself can be enormously costly. It is estimated that spam now makes up 94 percent of all email traffic. This continued rise in spam levels threatens the "viability of email for businesses and is sapping the productivity of hundreds of millions of workers around the world."[4] In terms of productivity and business continuity 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. In addition, cyber criminals and corporate espionage agencies intent on harvesting corporate data, interrupting corporate business, or compromising corporate computers and networks to launch attacks on other networks are immensely creative and readily adapt to defensive measures. Even without malicious external actors, risks can also arise simply because of negligence. It is surprising how many corporations fail to keep their domain names and Internet Protocol addresses—their online real-estate—registered and updated.

Fail to recognize the consequences for business.

Too often, law enforcement is effective 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. A corporation may also simply fail to meet its target business objectives through disruption to business continuity. There is also a complex legal situation surrounding the protection, release, and storage of data, with Europe, the United States, and Canada adopting different policies and laws. But many companies have outsourced corporate data services to countries that have no laws at all, making the loss of data more likely and possibly opening themselves up to liability claims.

Assume that because their company is protected, their business is safe.

Businesses no longer operate as discrete entities. Their operating, financial, and transactional networks—the backbones of a company—are inextricably linked to Internet-based supply chains. Such links are often a key part of a company's business strategy. Today's networked economy delivers millions of dollars worth of transaction cost savings to businesses in the United States, Canada, and the United Kingdom every day. While CEOs have reorganized their businesses to take advantage of these networks and their efficiencies, they must also act to protect their companies against the increased risks those networks bring. The breakdown of a key supplier's computer system, for example, could delay the delivery of essential parts or data, and thus have devastating consequences on a company's ability to conduct its own business.

The Language of Cyber Crime

***Botnets** – compromised computers combined into networks that can be directed to deliver distributed denial of service or phishing attacks.*

***Spam** – any unsolicited email. Usually considered a costly nuisance, spam now often contains malware. Malware is a class of malicious software—viruses, worms, trojans, and spyware—that is designed to infect computers and systems and steal critical information, delete applications, drives and files, or convert computers into an asset for an outsider or attacker.*

***Phishing** – a form of Internet fraud that aims to steal valuable information such as credit cards, social security numbers, user IDS and passwords by creating a website similar to that of a legitimate organization, then directing email traffic to the fraudulent site to harvest what should be private information for financial or political gain.*

***Denial of service attack** – Malicious code that blocks service for users of a targeted system. The flood of incoming messages essentially forces the targeted system to shut down, thereby denying use by legitimate users.*

***Virus** – a form of malware that infects computers or other electronic devices, making them unusable.*

***Patches** – programs designed to fix software security flaws, often installed automatically to reduce end-user participation and increase ease of use.*

What Mistakes Might Your Business Be Making?

For a business or other entity to function smoothly, its leaders must ensure that its computer systems, including networks and data, are managed cost-effectively, even as the business infrastructure and its operating environment become more complex. Cyber criminals and espionage agencies are constantly watching for small oversights in a corporate network infrastructure that will give them the opportunity they need. Some of the most common mistakes include:

Failure to maintain the corporation's online identifiers. Companies and other organizations can spend very significant resources in developing an online presence, but then fail to maintain the leases on the corporate domain names or associated Internet Protocol addresses that keep them connected to the Internet. The negligent failure to renew those addresses—or the criminal hijacking of a domain name—can have a devastating effect. Once a domain name or IP address is hijacked or corrupted, the content of the domain is also open to predation. Corporate executives and business owners should only feel secure if they have special teams of security, legal, and network experts working to prevent such instances.

Neglect of security-related software patches and updates. Online criminals continue to stay ahead of their victims in designing and deploying creative technologies. 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 that the latest updates and patches are installed.

Poor handling of sensitive data, including the failure to deploy encryption when necessary. Today's businesses and other organizations rely heavily on the Internet to transmit and transfer all kinds of data, including valuable intellectual property. That information may include data required to run the organization or even information or processes that are central to the generation of business income. Too often, that information may not be backed up frequently enough to include regular changes. Backups may also be difficult for IT staff to restore if something happens. And, when information is transmitted, it is well to remember that the Internet is like a series of post boxes, the contents of which can be easily read and copied. If sensitive data is to remain private, it must be encrypted.

Sacrificing security for convenience. Businesses and other organizations must have a strict information security policy that is in place at all levels of the corporate structure, and that covers intellectual property and corporate networked devices, including BlackBerries and laptops. 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 more than 28 percent of the workforce. Workers are more mobile and wireless communications free them from the confines of the office. At the same time, this mobility brings fresh challenges for IT and information security managers. Employees should be prohibited from installing unauthorized software and applications from any source. 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.

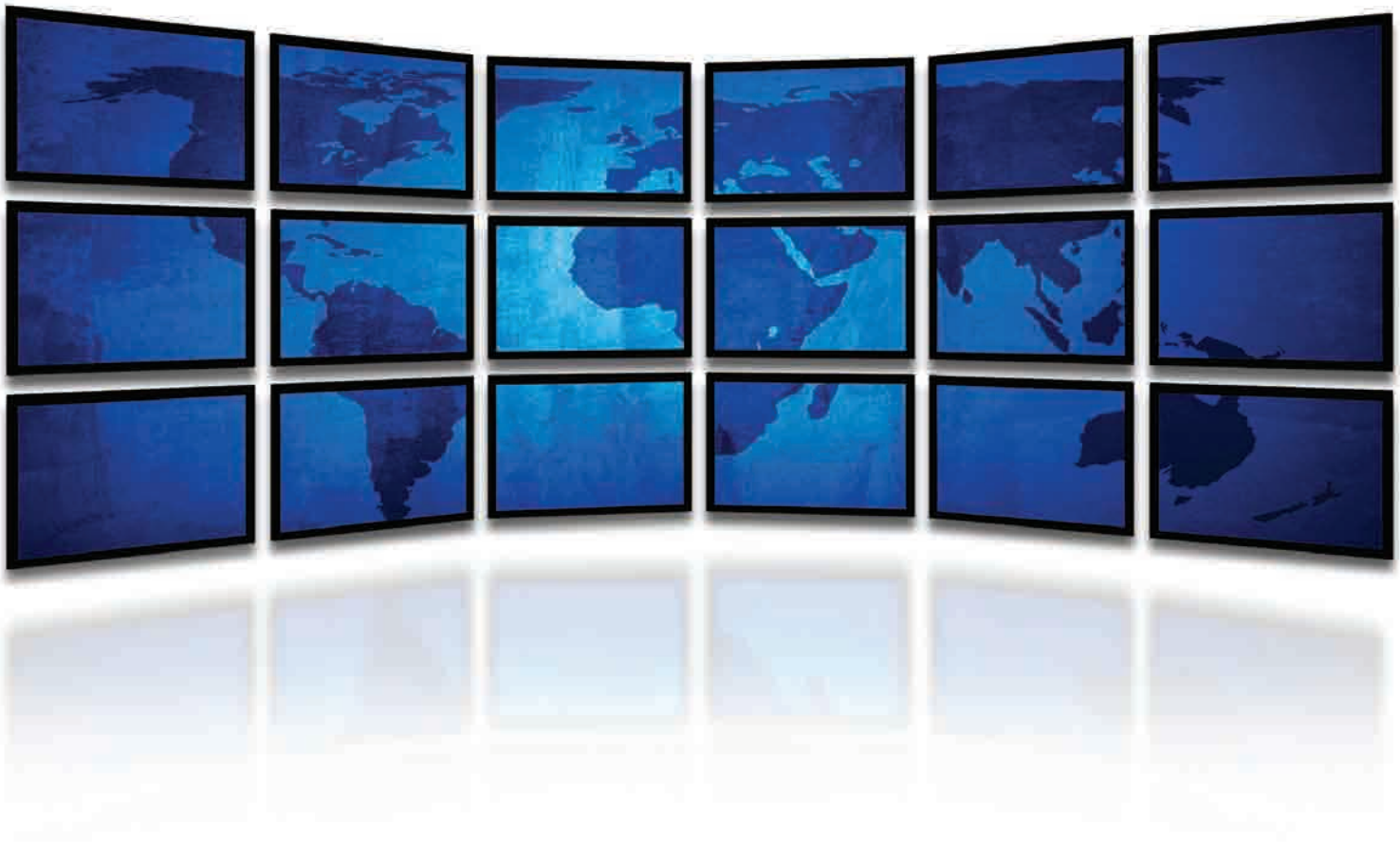
How Should a CEO Respond?

It is easy to place the responsibility for fighting cyber attacks on others, including the government. In fact, 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. In addition, the U.S. Congress is considering no fewer than five bills in the information security space. As with the Sarbanes-Oxley Act, any new legislation is likely to mandate new requirements and affect corporate bottom lines.

Since its inception, the Internet and its systems have been coordinated through a private-sector led effort that works to coordinate the Internet's core functions of security, stability, and operability. Participants come from the science and technology community, industry and business, academia, government, and civil society. Although no single group can be in charge of the Internet's security, the Internet Corporation for Assigned Names and Numbers (ICANN) runs several committees that, along with other expert stakeholders such as the Internet Engineering Task Force (IETF), provide advice and recommendations about its operational requirements and security. In addition, the International Organization for Standardization has proposed two international standards for information security: ISO 27001 of 2005, titled *Information technology – Security techniques – Information security management systems – Requirements,* and ISO 17799, *Information technology – Security techniques – Code of practice for information security management*, which was updated in April of 2007. These will also require businesses to take specific steps to ensure security of their networks.

But CEOs, corporate directors, and leaders of organizations cannot abdicate their responsibilities to either the government or the international community. Managing risk is essential, and is thus a vital part of their responsibilities in safeguarding their business. They must foresee and respond to risks they face from the world of cyber crime and cyber espionage. To succeed, they must elevate information security to become an integral and essential part of their corporate culture.

		Responses			
Threat	**Effect**	Corporate Policy/Practice	Technology Fixes	Security Measures	Employee Education
Malicious Attacks					
Hijacking Corporate Domain Names	Risk to trusted corporate name and reputation; loss of intellectual property; huge recovery and restoration (including legal) costs for vandalised systems; threat of extortion	▼	▼	▼	▼
Denial of Service (DOS) / Distributed Denial of Service (DDoS)	Disruption of network services and functions; network or server overload; shutdown	▼	▼	▼	
Phishing and Spam	Loss of productivity; risk to business continuity; corruption of operating systems, applications, programs, files	▼	▼	▼	▼
Viruses and Malware	Loss of productivity; risk to business continuity; 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	▼	▼	▼	▼



CEOs must work with their information and legal experts to deploy a full complement of safeguards, including revised corporate policies and practices, technology fixes, security measures, and employee training. As the chart on page 5 shows, most threats require more than one approach, and these, to be effective, must be coordinated. Unfortunately, even in the best of circumstances, they will not provide a solution in the sense that a problem, once solved, remains solved. Sadly, that thinking has no place in the world of cyber security. CEOs can only ensure that they have an ongoing awareness of emerging threats, along with the capacity to assess risks and then build effective response capabilities. Only a full complement of approaches can secure a corporation's infrastructure and protect it from malicious attack and other potential outages. These measures must be upgraded on a regular basis in order to secure a corporation's essential operating and financial systems.

As a corporation undertakes this journey, the April 2007 report by the President's Identify Theft Task Force[5] offers an instructive guide. That document adopts a two-part preventive approach—keeping data out of the hands of criminals, and making it harder to misuse data—and combines physical plant security with information system security measures. But perhaps the most important element of any corporate strategy will be to create an information security culture.

Creating an Information Security Culture

A strong information security policy on the part of the CEO, agency head, and senior management sets the security tone for the whole organization 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. A recent survey[6] 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 in the near future. A similar survey reported that responsibility for IT security was represented at board level in 55 percent of companies. As a sign of the growing importance of information security, budgets are now often equally divided between staffing and external services such as vulnerability audits and risk assessments. To create an effective information security culture:

• ***Make information security everyone's responsibility.*** Everyone working for an organization, including temporary staff and contract workers, is more effective when they know exactly what is expected of them. The best corporate security policy is not just a checklist or a manual, but a living and breathing resource—an information security professional—who can guide employees away from the risks most likely for a particular business. Begin with a risk analysis or risk mapping to identify what is relevant and what is not.

• ***Rest final responsibility for information security with senior management.*** This gives information security the importance it deserves and means that policy decisions will be implemented. In larger or more extended businesses, a clear chain of command ensures that all security issues are addressed and lines of responsibility are clear.

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

• ***Underpin a robust security culture with frequent and rigorous testing.*** This will send a strong message of compliance to employees and others, and will also include any changes in the network. For some companies, network access points are in a constant state of flux. Regular testing will ensure that such changes are kept mapped and secure.

• ***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 strengths will be diminished. Security training should become a permanent function, with regular information updates offered, additional training given, and alerts sounded as required.

• ***Make keeping abreast of changes in security technology and best practices a priority.*** Specific corporate resources should be specially designated to keep track of current and pending changes related to the security of corporate servers, networks, and systems. New attacks and new responses are continually developed, and this should be kept in mind when purchasing new hardware or software. Ensuring that hardware can support or be upgraded to support new technology both increases security options and saves long-term costs.

Organizations can reinforce their own information security culture by drawing on the efforts of the international community. For example, the two international standards for information security mentioned earlier—ISO 27001 of 2005 and ISO 17799 of 2007—can serve as excellent sources of best practices. The Security and Stability Advisory Committee of ICANN has reported extensively on domain name hijacking scenarios and identified an array of measures business owners and chief executives can take to protect their domain names from this particularly widespread form of predation.[7]

To make the most of these resources and stay abreast of the newest information on Internet and network security threats and solutions, CEOs and agency leaders should consider whether their company should play an active external role. Senior corporate officers might participate in ICANN, while appropriate technical staff could attend the security meetings of IETF. These institutions can not only provide the latest information on potential attacks and responses, but also provide contacts with other executives dealing with the same challenges.

Leading an Information Security Revolution

It is in the nature of the Internet that no one—even an IT expert—can anticipate future threats and challenges. A CEO, especially one who does not come from an IT background, cannot be expected to master every detail of this often technical subject. But CEOs, directors, and agency heads should push and support those with the expertise to ensure that their organizations are taking the right steps. Only when cyber attacks are regularly discussed in board rooms will an information security revolution be truly under way.

To lead that revolution, CEOs and directors must know the questions to ask their information and legal professionals. By asking the following key questions, business and agency leaders can begin to ensure that their network and system security approaches are effective, comprehensive, and in line with best practices. Only then will they see their corporations securely into the future.

- Does your organization dedicate specific resources to security work? Budget? Staffing? Time?
- Is final responsibility for implementation of both physical plant and information security placed at the executive level? Do you discuss information security issues at your board meetings? Is that responsibility and ownership/accountability clearly defined?
- Is there a user security policy or acceptable use manual? Does every staff member receive the manual? Is it updated on a regular schedule? Are those policies implemented enterprise-wide, even along your supply and partner chains?
- Is there a clearly documented policy for keeping networks, servers, and systems up to date? Is this policy also implemented enterprise-wide, even along your supply and partner chains?
- Is valuable intellectual property backed up? If it changes frequently, is there a process to back up those changes? Is it stored securely? Can IT and information security staff restore backups in a timely manner?
- How often is this system tested? Are any lessons learned incorporated into training sessions and manuals?
- Does your organization make use of an external auditor to provide objective security audits? How often does this occur? Are security audits regularly scheduled? Are security audits included in your recovery and contingency plans?
- Are risks assessed and mapped on a regular schedule? Once mapped, is there a plan to manage or mitigate these risks?
- Does your organization have an ongoing security training program? Does it cover best practices and acceptable use? Does it emphasize the responsibility of the user? How often are training sessions scheduled? Does training include your partners, contractors, and suppliers?

The costs of cyber attacks to business and business continuity are great and the risks are high. As organized criminals and corporate espionage agencies see a growing return on investment, threats are increasing in boldness and creativity. Chief executives and directors must make information security integral to their corporate cultures and give senior management the authority to implement and maintain network and system information security policies and practices. CEOs, business owners, and organization heads should mind the words of Vint Cerf, chief Internet evangelist at Google and father of the Internet, who says, "Much work is needed to increase the security of the Internet and its connected computers 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."[8]

"Presence of mind . . . is nothing but an increased capacity of dealing with the unexpected."

– Baron Carl von Clausewitz, On War

Information Security Checklist

CEOs and directors must know the questions to ask their information and legal professionals. By asking the following key questions, business and agency leaders can begin to ensure that their network and system security approaches are effective, comprehensive, and in line with best practices. Only then will they see their corporations securely into the future.

- ☑ Does your organization dedicate specific resources to security work? Budget? Staffing? Time?
- ☑ Is final responsibility for implementation of both physical plant and information security placed at the executive level? Do you discuss information security issues at your board meetings? Is that responsibility and ownership/accountability clearly defined?
- ☑ Is there a user security policy or acceptable use manual? Does every staff member receive the manual? Is it updated on a regular schedule? Are those policies implemented enterprise-wide, even along your supply and partner chains?
- ☑ Is there a clearly documented policy for keeping networks, servers, and systems up to date? Is this policy also implemented enterprise-wide, even along your supply and partner chains?
- ☑ Is valuable intellectual property backed up? If it changes frequently, is there a process to back up those changes? Is it stored securely? Can IT and information security staff restore backups in a timely manner?
- ☑ How often is this system tested? Are any lessons learned incorporated into training sessions and manuals?
- ☑ Does your organization make use of an external auditor to provide objective security audits? How often does this occur? Are security audits regularly scheduled? Are security audits included in your recovery and contingency plans?
- ☑ Are risks assessed and mapped on a regular schedule? Once mapped, is there a plan to manage or mitigate these risks?
- ☑ Does your organization have an ongoing security training program? Does it cover best practices and acceptable use? Does it emphasize the responsibility of the user? How often are training sessions scheduled? Does training include your partners, contractors, and suppliers?

Notes

BNAC Members Endorsing the Report

CO-CHAIRMEN:

ALAN R. GRIFFITH
Former Vice-Chairman (Retired)
The Bank of New York

SIR PAUL JUDGE
Chairman
Teachers TV

CHAIRMAN, EXECUTIVE COMMITTEE

PROF. THOMAS H.B. SYMONS, C.C.
Founding President and
Vanier Professor Emeritus
Trent University

MEMBERS:

NANCY AOSSEY
President and CEO
International Medical Corps

PAUL R. BAAY
Chairman and CEO
True Energy Inc.

DARYL BENNETT
President
Liftlock Group

ROBERT A. BURGOYNE
Partner
Fulbright & Jaworski

SIR ANTHONY CLEAVER
Chairman
The Engineering and Technology Board

SIR FREDERICK CRAWFORD
Chairman
Haruspex Consulting

PHILIP C. DECK
Managing Partner
MKS Inc.

PHILIP EVANS
Senior Vice President
Boston Consulting Group

MAUREEN FARROW
President
Economap Inc.

SIR BRIAN FENDER
Chairman
BTG PLC

BROOKS FIRESTONE
Founder
Firestone Vineyard

LAWRENCE P. FISHER, II
Managing Director
Bessemer Trust Company

JOHN A. FRASER
Master of the Massey College
University of Toronto

PETER GODDARD, Ph.D.
Director
Institute for Advanced Studies

KERRY L. HAWKINS
Former President (Retired)
Cargill Ltd, Canada

NIGEL HORNE, Ph.D.
Director
Foresight VCT PLC

BRIAN A. HUNTER
Managing Director and CEO
Strategic Capital Allocation Group

HON. ROBERT L. HUTCHINGS
Diplomat in Residence
Woodrow Wilson School
Princeton University

FREDERICK KEMPE
President and CEO
Atlantic Council of the United States

PROF. J.A. KENNERLEY
CTRL Complaints Commission

SIR JOHN KINGMAN
Former Vice-Chancellor
University of Bristol

GEORGE KITCHING
Chairman and CEO
Idelia Advisers Inc.

MICHAEL M. KOERNER
President
Canada Overseas Investments Ltd

CLAUDE LAMOUREUX
President & CEO
Ontario Teachers' Pension Plan Board

W. A. FITZHUGH LEE
Chief Executive Officer
Vivum

DAVID LEVY, M.D.
Partner
PricewaterhouseCoopers LLP

GEORGE W. MALLINCKRODT, K.B.E.

CLIVE MATHER
Former President and CEO
Shell Canada Limited

WILLIAM MAYER
Founder
Park Avenue Equity Partners

DEAN MENEGAS
General Counsel
Spinnaker Capital Group

JON MOULTON

DEREK OLAND
Chairman and CEO
Moosehead Breweries Ltd.

GEORGE D. O'NEILL
Chairman
Meriwether Capital LLC

GORDON F. PAGE CBE MA FRAeS
Chairman
Cobham PLC

NEIL RECORD
Chairman & CEO
Record Currency Management Limited

SIR BOB REID

WILLIAM B.P. ROBSON
President and CEO
C. D. Howe Institute

RICHARD D. SIMMONS
Founder
R.D. Simmons & Sons

HON. JAMES R. SCHLESINGER
Senior Advisor
Lehman Brothers, Inc.

W. IAIN SCOTT
Chairman & CEO
McCarthy Tétrault Barristers & Solicitors

HON. BARBARA THOMAS JUDGE
Chairman
UK Atomic Energy Authority

GERALD H. TURNER
Partner
FOCUS LLC

WILLIAM I.M. TURNER, JR.
Chairman and CEO
Exsultate, Inc.

PAUL TWOMEY, Ph.D.
President and CEO
ICANN

SIMON WEBLEY
Research Director
Institute of Business Ethics

VISCOUNT WEIR
Former Chairman
Balfour Beatty Plc

FREDERICK B. WHITTEMORE
Advisory Director
Morgan Stanley & Co., Inc

DAVID A. WILSON, Ph.D.
President and CEO
Graduate Management Admission Council

SIMON WOOLLER
Managing Director
Corporate Real Estate Group
Land Securities Trillium

LORD (ANTHONY) YOUNG
OF NORWOOD GREEN
Vice Chairman
The Ethical Trading Initiative

Acknowledgments

Like all BNAC publications, this report grew upon the insights and comments of BNAC members, who met in three separate working group sessions between October 2005 and May 2007. We would like to thank Dr. Paul Twomey of ICANN, for offering the working group members stimulating and thoughtful insights on the information security challenges facing business and nonprofit organizations. We are very grateful to William Mayer of Park Avenue Equity Partners, the working group chairman, for his superb guidance throughout the preparation of this report and especially during the working group meetings themselves. Finally, we want to thank the BNAC members and staff of the Committee and ICANN for their contributions to developing what we believe are practical and helpful guidelines for business and public leaders and all those connected with the World Wide Web.

Alan R. Griffith
Sir Paul Judge
Thomas H.B. Symons, C.C.

Joint Chairs of the British-North American Committee

Members of the Cyber Security and Business Working Group

William Mayer, Chairman	Founder, Park Avenue Equity Partners
Paul Twomey, Principal Advisor	President & CEO, ICANN
Amanda Bowman	Sloatsburg, New York
Fred Crawford	Chairman, Haruspex Consulting
Philip Deck	Managing Partner, MKS Inc.
Philip Evans	Senior Partner and Managing Director, Boston Consulting Group
Maureen Farrow	President, Economap Inc.
Brian Fender	Chairman, BTG plc
Peter Goddard	Director, Institute for Advanced Studies
Kerry Hawkins	Former President (Ret.), Cargill Ltd, Canada
Brian Hunter	Managing Director and CEO, Strategic Capital Allocation Group
Fred Kempe	President & CEO, The Atlantic Council of the United States
Sir John Kingman	Former Vice-Chancellor, University of Bristol
Claude Lamoureux	President & CEO, Ontario Teachers' Pension Plan Board
George Mallinckrodt	President, Schroders plc
Katherine Mayer	New York, NY
Neil Record	Chairman & CEO, Record Currency Management Limited
William Robson	President & CEO, The C.D. Howe Institute
Helen Robson	Toronto, Canada
Richard Simmons	Founder, Simmons & Sons
William Turner, Jr.	Chairman & CEO, Exsultate Inc.
Simon Webley	Research Director, Institute of Business Ethics
David Wilson	President & CEO, Graduate Management Admission Council
Lord Anthony Young of Norwood Green	Vice Chairman The Ethical Trading Initiative

BNAC would like to acknowledge the support of Sara Stohl at ICANN, Marina del Rey, CA; Fran Burwell and Elena Pak at the Atlantic Council of the United States, Washington, DC; and David Robertson and Melanie Jones at the British-North American Research Association, London, UK.

Footnotes

1 Symantec Internet Security Threat Report, Trends for July–December 06, Volume XI; published March 2007. See ***http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf***.

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 Ferris Research report titled Spam and Other Email Threats, 26 March 2007. See ***http://www.ferris.com/2007/03/26/spam-and-other-email-threats/***.

4 Daniel Druker, executive vice president of marketing, Postini, quoted in DarkReading, January 2007. See ***http://www.darkreading.com/document.asp?doc_id=114418***.

5 Combating Identity Theft: A Strategic Plan, April 2007. Issued by the President's Identify Theft Task Force. See ***http://www.idtheft.gov***.

6 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***.

7 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***.

8 Vint Cerf, quoted in DarkReading, 2 March 2007, article titled Father Knows Best. See ***http://www.darkreading.com/document.asp?doc_id=118596***.

BRITISH-NORTH AMERICAN COMMITTEE

North American Office
The Atlantic Council of the United States
1101 15th Street NW, 11th Floor
Washington, DC 20005
Tel: +1 (202) 778 4967
Fax: +1 (202) 463 7241
bnac@acus.org
www.acus.org

UK Office
British-North American Research Association
Warnford Court, 29 Throgmorton Street
London EC2N 2AT
Tel: +44 (0)20 7382 4596
Fax: +44 (0)20 7374 6220
bnac@underlinegroup.com
www.bnac.org