Business Roundtable

SECURING CYBERSPACE:

BUSINESS ROUNDTABLE'S FRAMEWORK FOR THE FUTURE

Introduction

Information technology (IT) and networks increasingly link economies, governments and societies into an ever-expanding global digital nervous system called cyberspace. The critical information infrastructures comprising cyberspace provide the backbone for many activities essential to the transaction of domestic and international business, the operation of government and the security of a nation.

Cyberspace is under increasing assault by malicious attackers capable of identifying and exploiting IT vulnerabilities. These attacks – through worms, viruses, hacking, identity theft, fraud, extortion and industrial espionage – are rising at unacceptable rates of frequency, speed, severity and financial cost. The ramifications of these attacks extend well beyond any one company or organization. Due to the interdependent and interconnected nature of cyberspace, attacks on a company in one infrastructure or industry sector can significantly impact suppliers, partners and customers in a variety of other businesses and industry sectors. This has the potential to disrupt the flow of goods and services on a regional, national, or even international scale.

The critical information infrastructures that make up cyberspace are largely owned and operated by the private sector, not the government. Therefore, securing cyberspace is mainly a private sector responsibility to be shared by suppliers and end-users of IT products and services and handled through market solutions and risk management strategies rather than government regulation.

As an association of 150 chief executive officers of leading U.S. corporations, the Business Roundtable has a unique perspective on cyberspace security that encompasses all major industrial sectors, including leading suppliers and end users of IT products and services. The chief executives of the Business Roundtable acknowledge their responsibilities to strengthen the security of cyberspace, both in their capacities as leaders of their individual companies and as catalysts for change in the marketplace and in public policy.

The Roundtable supports the following principles which it believes should guide the continual improvement of corporate IT security and the advancement of cyberspace security public policy:

1. **Information security requires CEO attention in their individual companies and as business leaders seeking collectively to promote the development of standards for secure technology.**

The threat to information security and the need to reduce risks of cyber attacks present significant business challenges that require the chief executive's attention and involvement – both individually within their companies and as business leaders seeking collectively to promote the development of

standards for secure technology. Chief executives should integrate information security into all relevant organizational policies, processes and controls to ensure that significant cyber related risks and vulnerabilities are identified and managed. Risk Management is an operational discipline that includes risk assessment, risk prevention, risk mitigation, risk transfer and risk retention. Chief executives should also ensure that key businesses in their value chain are also observing sound information security practices. Senior management should be aware of and informed by existing IT security standards, guidelines and "best practices," when developing and implementing IT security programs for their companies. Senior management should also undertake measures to ensure the security of all proprietary software developed and used within their organization.

2. **Boards of directors should consider information security an essential element of corporate governance and a top priority for board review.**

Boards of directors are urged to designate management responsibility for information security and business resiliency, and to periodically review management's plans as part of their oversight and governance functions. This should include reviewing existing information security policies, internal controls for information security, assessments of the most significant risks to corporate information assets and security resources, financial management, and business continuity and crisis plans and procedures for managing significant cyber disruptions.

3. **IT suppliers and end-users of these products and services have a shared responsibility for improving cyberspace security.**

Securing cyberspace is principally a private sector responsibility that must be shared between suppliers and end-users of information technology products and services. Business end-users must use and maintain information technology securely – recognizing and managing the risks that threaten business continuity, public safety, critical infrastructure operations, or homeland security. At the same time, suppliers and service providers of information technology have a responsibility to develop and maintain secure products and services that place minimal burden on the end user, to responsibly alert users when new vulnerabilities are detected, and to provide substantive security recommendations, best practices and other related guidance to assist end-users in the secure implementation of their products. IT suppliers should integrate security throughout the designing, manufacturing and upgrading cycles for software and firmware. Suppliers should adopt quality assurance standards that ensure compliance with security requirements before software and firmware products are released. Suppliers should also develop patch-management processes that are more secure and efficient, and less costly to end-users.

4. **The Federal government plays an important collaborative role in information security and can assist the private sector response by sharing information about threats and vulnerabilities, helping companies overcome legal barriers and encouraging appropriate corporate actions.**

While recognizing the lead role played by the private sector in securing cyberspace, the Business Roundtable also believes the government plays an important collaborative role in this undertaking. Specifically, the Roundtable believes the government should: share information on threats and vulnerabilities so that companies can set priorities and allocate resources to address such threats; together with business, define and mitigate legal obstacles that hinder private sector homeland security efforts; lead by example in the adoption and procurement of secure software and firmware;

and consider incentives to encourage appropriate corporate actions where market forces are insufficient. The Federal government should continue to collaborate with the private sector in the open, voluntary and consensus-driven security standards arena, and in the development of checklists and similar means for coordinating and making easily accessible important security recommendations.

The government should also work with the private sector to raise awareness and educate the public on the importance of practicing sound IT security in their communities, homes, schools, and small businesses. Finally, the U.S. government should work globally to promote a culture of cyber security, safeguard intellectual property rights of software and hardware, protect the privacy of individuals, and ensure effective and comprehensive laws against cybercrime.

5. Public policy initiatives on cyber security should take a balanced and comprehensive approach that reflects the shared responsibility of end-users and IT suppliers.

Public policies intended to strengthen cyberspace security must, to be effective, reflect the shared responsibility of business end-users and IT suppliers. Policies that focus only on the responsibilities of business end-users (or more narrowly, publicly traded companies) offer an incomplete and potentially counterproductive approach to securing cyberspace, because they fail to address the considerable problems arising from the lack of quality assurance in software security. Indeed, most of the significant cyber incidents that have harmed American business and consumers over the past several years have had at their root cause defective and readily exploitable software code. Most software development processes used today do not incorporate effective tests, checks or safeguards to detect those software coding defects that result in product vulnerabilities. Accordingly, the Roundtable believes that these problems, as well as those arising from poor security practices by business end-users, including failure to apply patches when doing so is appropriate, must be addressed together as a matter of sound and responsible public policy.

6. Market solutions to cyber security are to be preferred over statutory and regulatory mandates.

Traditional regulations directing how companies should configure their information systems and networks could discourage more effective and successful efforts by driving cyber security practices to the lowest-common-denominator, which evolving technology would quickly marginalize. Such an approach also could result in more homogeneous security architectures that are less secure than those currently deployed. Given the complexity and dynamism of cyberspace, the marketplace will provide in most cases the necessary impetus for improving IT security. In those instances where existing market forces fail to provide such impetus, incentive programs that rectify market shortfalls by encouraging proactive private sector solutions should be considered and adopted as appropriate.

7. Public disclosure of corporate information security practices should be voluntary, not mandatory.

Public disclosure of corporate information security practices should be made at the discretion of senior management. Mandating such disclosures could have a leveling effect on corporate IT security, as companies are forced to be more concerned about complying with disclosure standards than in optimizing their security practices to meet their unique industry and corporate needs.

Mandatory disclosures could inadvertently encourage cyber attacks by drawing attention to company security practices and approaches. Mandatory disclosures could also expose companies to greater liability in the event they are attacked and harmed despite having implemented solid cyber security programs. In such instances, companies will bear a difficult and costly burden of proving that they did not misrepresent the level and quality of their cyber security in their public disclosure statements.

Conclusion

The Business Roundtable recognizes the long-term, complex challenges entailed in securing cyberspace. The Roundtable is committed to advancing the above principles and to undertaking measures that (i) inform and guide its CEOs on appropriate risk management processes and procedures for ensuring that their companies' IT systems and networks are adequately secure and the potential consequences of disruptions adequately managed; (ii) urge the marketplace to improve the overall quality and reliability of security in IT products and services; and (iii) engage and partner with leaders in the Executive Branch and Congress to develop effective, common-sense public policies that strengthen the security of cyberspace. The Roundtable is also committed to working with other industry organizations, as appropriate, to promote and achieve these objectives.

FINAL
May 19, 2004