SESSION 3 | 2004 REAL & VIRTUAL WAR: CIIP & THE PUBLIC / PRIVATE COLLABORATION

Tuesday, June 8, 2004 – 12:30 – 17:30
Geneva – FLUX Laboratory

Attending this session as leaders so far ->>

Click on the link above to get the participants list

"Efforts to enhance the security of information systems and networks should be consistent with the values of democratic society, particularly the need for an open and free flow of information and basic concerns for personal privacy"

OECD. 2002. ***Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security***

Protecting the global information infrastructure ("critical information infrastructure protection" or "CIIP") is essential to the national security of every country, and of the business security of every company.

All critical infrastructures (transportation, finance, electric power, water, etc.) are increasingly dependent on the evolving information infrastructure—the public telephone network, the Internet, and terrestrial and satellite wireless networks—for a variety of information management, communications, and control functions. September 11 and more recent terrorist activities significantly increased awareness of the interdependencies of critical infrastructures, and it heightened governments' sense of urgency regarding the need for increased private sector and public sector information sharing with respect to cyber and physical threats. While threats to public infrastructure have always been realities of organized society (protecting water reserves or crops), the convergence of real and virtual war on a planetary level has given new meaning to the word "protection". It is not surprising that security experts all over the world, from every field of business, are using a vocabulary closer to that of warriors than civilians.

According to InfoSurance Foundations, which sits at the center of the CIIP discussion in Switzerland, a clear systematic definition of the responsibilities is still missing, as well as a co-ordination between the different sectors, which actually deal with partial aspects of this problem. Up to now, only the starting phase of coordinated actions concerning possible defense strategies (prevention, early recognition of risks, crisis management, resolution, judicial prosecution, etc.) has taken place. The unco-ordinated development of separate work teams in various industrial countries (i.e. USA, Germany) is a sign of the difficulties with which the classic crisis prevention systems are confronted as they work to find solutions to these new perils.

Questions that will be discussed:

- The Internet as Critical Infrastructure
- Protecting Information Infrastructure, Protecting Personal Information and Expression
- Criminal Law and Critical Information Infrastructure Protection
- Public-Private Partnership: Keys to Success
- Regulating Government Intervention in the Information Age
- Building the Case for Economically Sound Investments in Security
- Cyber Insurance: Improving Security Through Risk Management
- Protection Efforts and Business Pressures

Definitions

Critical Infrastructure Protection (CIP)

Protecting critical infrastructures (CI), such as communications, transportation, and energy, against disruption of any kind is increasingly crucial in maintaining both domestic stability and national security. The Critical Infrastructure Protection (CIP) approach is broader that the information security approach. CIP includes both, cyber and physical, measures to secure systems and assets whose incapacities or destruction would have a debilitating impact on the national security and the economic and social well being of a national (and its neighbors in physical and cyber space).

CIP and CIIP

Critical Information Infrastructure Protection (CIIP) is a subset of CIP. CIIP focuses on the protection of information technology systems and assets including components such as telecommunications, computer/software, Internet, satellites, etc.. and on interconnected computers and networks, and the services they provide (from CIIP Handbook 2002). CIP is a challenge within each nation's responsibility that can be supported by bilateral and transnational activities.

Source: Prof. Dr. B. M. Hämmerli presentation – R&D Challenges for Resilience in Ambient Intelligence (RAmI) – March 19, 2004

Key Points

Creating an environment of trust to encourage the flow of information

- Information Sharing Framework – creating the channels to share
- Real and perceived barriers to Information Sharing
    - Freedom of Information Act (US)
    - Antitrust laws and "culture"
    - No incentives

Deterrents for those who have unsecured systems

- Criminal Law
- Domestic and International Jurisdiction
- Civil Liability
- Contract Law
- Standards and Best Practices
- Regulation and Directives

Involving the Private Sector through motivation

- Insurance: better premiums for good "secure" behavior
- Financial Institutions: better credit ratings for good behavior
- Tax authorities: tax benefits
- Give private business a leadership role :Privately funded R&D to alter the costs of security
- Rewarding awareness on the board level
- Creating a public / private Trust Network

Imperatives

- Delivering secure, trustworthy banking, financial and investment services
- Since Switzerland is not an island … fostering a co-operative, international, inter-governmental approach of setting standards, policies and strategies for protection of global communications and information infrastructure
- Securing the delivery of trusted trade, transport and logistics infrastructure and services

Overview

The increasing dependence on common technology and interconnected systems, suggests that many of the technical vulnerabilities can be overcome only through collective, concerted action.

Prior to September 11, the security of information systems and the protection of personal data and privacy were considered to be mutually reinforcing and compatible goals. Many experts suggest that the crisis-management mentality in the aftermath of September 11 has pushed aside issues of privacy and civil liberties. Technical mechanisms proposed to aid government efforts in the war on terrorism appear, to some, to sacrifice privacy and civil liberties for only the illusion of an increased ability to protect the nation's infrastructures.

Phil Reitinger, former deputy chief of the Computer Crime and Intellectual Property Section of the U.S. Department of Justice, has made the following recommendations:

- Vendors have to produce more secure products, and systems and customers have to demand and implement better security.

- We need management solutions. Companies must adopt and share best practices.

- We need to to develop public education efforts to help all users better understand computer ethics (just as throwing a stone through a neighbor's window is wrong, so is breaking into someone else's computer system). Reducing nuisance attacks will allow government to focus resources on the greater threat.

- We need knowledge solutions. The private sector and law enforcement must gather and share information about threats, vulnerabilities, and remedies.

Source: Critical Information Infrastructure Protection and the Law - Stewart D. Personick and Cynthia A. Patterson, Editors Copyright 2003 by the National Academy of Sciences. All rights reserved.

Some principles that may or may not apply…

1. CIIP is best accomplished through private sector solutions that are market driven and industry led. The private sector owns, operates, and has developed the networks and services that constitute the information infrastructure.

2. Governments and industry must work cooperatively on a voluntary basis towards achieving CIIP. This should include an institutionalized and thoughtful dialogue between key government officials and industry.

3. Government must not mandate the private sector use of particular technologies or processes, dictate standards, or prevent companies from using tools to test products because this would stifle innovation and harm the very infrastructure that needs protection.

4. Governments must not violate personal and corporate privacy in the quest for CIIP. The primary threat to the privacy of Americans at home and at work in today's electronic world is unwarranted by the increased government monitoring and surveillance. Such privacy protection is best preserved by careful public scrutiny of new governmental CIIP authorities.

5. Government should get its own house in order and improve information security within the government and should strengthen the government's personnel and technological capabilities to address cybercrime.

6. Barriers to strong CIIP should be removed, including barriers to the widespread use of strong encryption. Encryption promotes national security, prevents crime, and protects privacy. The U.S. government must fully implement the recent relaxation in U.S. encryption export controls and make additional changes as necessary to ensure the ability of American companies to lead globally. Governments must not impose foreign import barriers or domestic controls. What about Europe? What about Switzerland?

Source: ACP (Americans for computer privacy) 2001 Statement of Principles

The Players – Who's in charge?

Because legal liability often depends on which actors are best positioned to prevent the harmful activities (in this case, computer attacks), some experts suggest that the diverse entities in the Internet community should not all be held to the same standard of care with respect to computer network security.

- Given that certain Internet Service Providers (ISPs) may know (or should know) about risks and have the capability to mitigate attacks, many experts suggest that ISPs should face significant liability if their systems are insecure.

- Financial institutions with regard to protecting consumer privacy.

- Insurance can play a role in motivating the private sector by transferring the risk of computer security losses from a company to the insurance carrier.

- The fact that vendors can be held liable for negligence may change the cost-benefit calculation, encouraging the development and delivery of more secure computer products.

- Home users represent an important source of potential security hazards.

- Other important players include International Organizations, Federal Authorities of the Swiss Confederation, Parties, Pressure groups and NGOs, Universities / Institutes and the media.

Security vs. Privacy?

The OECD's Guidelines for Security of Information Systems states:

[]"Security of information systems may assist in the protection of personal data and privacy. . . . Similarly, protection of personal data and privacy . . . may serve to enhance the security of information systems. The use of information systems to collect, store and cross-reference personal data has increased the need to protect such systems from unauthorized access and use. . . . It is possible that certain measures adopted for the security of information systems might be misused so as to violate the privacy of individuals. For example, an individual using the system might be monitored for a non-security-related purpose or information about the user made available through the user verification process might permit computerised linking of the user's financial, employment, medical and other personal data".

Private and public trust

Why have past efforts failed to build trust between partners? One argument is that the government's message to the private sector has varied, ranging from national security to the economic delivery of vital services to mixed messages in between. The transition from a focus on CIP to the larger concept of homeland security compounds the challenge of communicating what is wanted and why. Although CIP presents a bigger picture, which can be a good thing, it may also make the objective so big and unfocused that it causes confusion.

The second problem is that the government interface with the private sector on CIP issues is quite confusing and not necessarily user friendly. The private sector, for example, often does not know which government entity it should be dealing with on CIP matters, whom it should be sharing information with, or whom it can depend on within the government for up-to-date information.

Antitrust concerns in the private sector further challenge national security efforts.

Information Sharing

Although the sharing of information has been the centerpiece of both the government's and the private sector's efforts over the past several years to protect critical information systems, most information sharing still occurs through informal channels.

Fundamental questions persist about who should share what information, when, how, why, and with whom. One reason for the lack of progress, according to private industry representatives, has been the lack of clarity regarding the benefits and associated liabilities in sharing information within and between industry sectors and with the government.

For example, information sharing could lead to allegations of price fixing, restraint of trade, or systematic discrimination against certain customers. Further, it could raise privacy concerns, expose proprietary corporate secrets, or reveal weaknesses and vulnerabilities that erode consumer confidence and invite hackers. Overcoming these concerns requires an informed position on the existing legal framework—an imperfect understanding of the law is both excuse and explanation for some observed limits to sharing.

Legal perspective

The legal framework for CIIP a moving target. There is a wide range of legal issues associated with information infrastructure protection, particularly those that affect the willingness of private sector companies and organizations to co-operate with the government to prevent, detect, and mitigate cyberattacks.

Information sharing and liability — there must be a recognition of the tension between these often conflicting approaches, and that strategies for critical information infrastructure protection must ultimately resolve these conflicts.

Laws and Standards

- US Freedom of Information Act
- Global Antitrust Law and private collaboration
- Europe vs. US ?
- What about Asia? Africa?

Liability and litigation – the debate continues in the private sector on whether there is a legal duty on the part of the company to secure its critical information infrastructure. How much liability should be on the part of Government? The patchwork of regulations relevant to CIIP complicates efforts to develop a regulatory framework for critical infrastructure protection.

In the US, the Gramm-Leach-Bliley Act (GLB), resulted in regulations promulgated by several government agencies (including the banking agencies, the Securities and Exchange Commission, and the Federal Trade Commission), which outline the responsibilities of financial institutions with regard to protecting consumer privacy.

Standards, Best Practices, and Audits

Establishment of operational best practices for network administrators and users, combined with ongoing training and enforcement of the practices through random tests, is one possible way of increasing computer security.

An obvious option is for firms to begin immediately to share best practices, including attack scenarios and practices to protect against these attacks. Best practices should focus on policies that improve computer network security rather than on procedures and rituals, which only create a perception of protection. In addition to playing a role in tort liability determinations, best practices can also serve as a benchmark against which firms can be audited. Routine audits based on well-accepted principles of testing and analysis, principles that need to be developed for computer security, can help firms avoid litigation or reduce liability.

Motivating the private sector: What are the real incentives?

Successful corporations focus on activities that contribute to increased profits, increased opportunities for profit, reduced constraints, and/or reduced risk.

Part of the difficulty with cost-benefit analysis applied to these issues, is that the cost of security breaches is not widely available or known—this is part of the data problem noted above. Companies are hesitant to disclose costs because of the effect it might have on shareholder value and/or confidence, and the attendant risks of litigation. A related problem is that the large numbers associated with the cost of publicized national incidents, such as distributed denial-of-service attacks, are considered suspect because they depend on simple assumptions about the behavior of large numbers of parties and on a simple aggregation of resulting cost projections.

A lingering challenge is how to achieve a greater understanding of the problem and possible solutions in smaller companies, particularly those that cannot afford a dedicated information technology support staff. Small businesses often are not aware that they need better computer security than what they have—if they have any at all.

Another proven method of incentives, is driven by the the standards and requirements of the insurance industry. To qualify for certain types of insurance coverage, companies must prove they are an acceptable risk. The three components to managing risk from this view are typically : people, policies, and technology.

Is Government a helping hand?

Is there any real reason for industry to be concerned about all this government activity? The administration has said that it will work cooperatively with the private sector. But where "encouragement" fails to yield desired results, forced compliance may follow. In meetings and at conferences, officials from the NSC, DOD, DOC, and FBI all say that regulation remains an option. The private owners and operators of the information infrastructure could someday be required to meet federal standards, use federal technologies, and follow federal policies and practices. There are several very good reasons why that kind of government intervention would be a bad idea:

- *The government does not have the expertise.* It's the private sector that has the knowledge necessary to protect the information infrastructure. The government has hardly done an exemplary job of protecting even its own systems.
- *Regulation would be counterproductive.*
- *Government standards would raise costs.*
- *Government intervention could violate privacy rights.*
- *Government action could compromise business secrets*

Mandatory compliance in this area would not be unprecedented.

So what would be the best way to protect our critical information infrastructure? Both the private sector and the government have essential roles to play. But a *voluntary* partnership is the only approach that can succeed.

The private sector needs to:

- *Continue improving protection in product lines and networks. Practicing good "security hygiene."*
- *Do a better job of sharing information among industry members and with the government about threats and vulnerabilitie,s as well as best practices.*

At the same time, the government must:

- *Share information with the private sector.*
- *Get its own house in order.*
- *Improve law enforcement's ability to detect and prosecute cybercrime.*

information technology has made many national essential services more robust and reliable. Yet the same interconnectedness that allowed increased efficiency and opens new frontiers of commerce and government, also makes them more vulnerable. Better protection of computer networks is essential to the public and private sectors.

Source: ACP - At Risk: A Secure Net Federal Oversight of the Internet May Lead to Interference by Bruce J. Heiman

Appendix

Tax incentives key to improving national security
22 April 2002
By: Leif Gamertsfelder

"Tax incentives are one tool that Australia could use to ensure the private sector allocates adequate resources to Critical Information Infrastructure Protection", said Leif Gamertsfelder, head of the e-security group at the law firm, Deacons.

Speaking at the inaugural Critical Information Infrastructure Protection Conference in Sydney (Tuesday 22 April), Mr Gamertsfelder said that there was unanimous consensus that Critical Information Infrastructure Protection (CIIP) was a matter of national security. However, he also noted that CIIP security concerns would persist if corporate goals and national security were not better aligned.

"When the private sector controls 90% of highly internetworked critical infrastructure, including telecommunications, finance, transport and electricity, the big question is how do you incentivise the private sector to invest in matters of national security?

"National security is a social good for which governments are usually responsible for delivering. On the other hand, the primary goal of private sector organisations is to increase benefits and wealth for their shareholders, not national security. This makes it difficult for private sector organisations to include or increase CIIP expenditure in already tight IT budgets, especially where the goal of increasing returns for shareholders does not coincide with CIIP objectives.

"In order to address this problem, Government should consider implementing a tax concession scheme similar to the R&D tax concession scheme. A tax concession scheme that allowed private sector organisations to claim CIIP expenditure at a concessional rate of around 175%, would go a long way to providing a solution to the private sector CIIP issue.

"Under the CIIP tax concession scheme, an agency such as NOIE could perhaps take the lead in determining what was legitimate spending on CIIP for the purposes of the scheme. By introducing this scheme and allowing NOIE to approve applications, the government would provide a light-handed means for increasing CIIP and benchmarking security.

A CIIP geared tax concession regime would generate a win-win outcome. Government would be discharging its national security obligations by indirectly providing funding for CIIP, and private sector organisations would be sufficiently incentivised to increase investment in CIIP.

"Humble tax concessions rather than mandatory legislative impositions may well be the key to securing Australia's CIIP moving forward," said Mr Gamertsfelder.

Attending this session as leaders so far...

Castellani	Laurent	Reed Midem, IT Director (France)
Fischer	Peter	Bakom, Deputy General Director
d’Heureuse	Charles	Bluewin AG, CTO
Lubich	Hannes	Computer Associates, Information Security Strategist
Haering	Kurt	EFSI, President
Hämmerli	Bernhard	ETH Zürich – FGSec, Abteilung Informatik HTA, Vice President FG Sec, Board member, InfoSurance
Hunt	Steve	Forrester Research Inc, Vice President Research (USA)
Schmid	André	Infosurance, Director
Koch	Stéphane	Intelligentzia, Membre du comité scientifique et enseignant (TBC)
Adar	Eyal	ITcon - Information Technology Consultants, Managing Director (Israel)
Rieder	Carlos	IWI Hochschule für Wirtschaft / Competence Center IT Security, Lieter Competence Center IT Security
Trenta	Giampaolo	Julius Baer & Co. Ltd, Chief Security Officer
Stuger	Alexander	Microsoft Schweiz GmbH, General Manager
Arnold	Roger	SUVA, IT Security
Vogt	Lilia	WIPO, IT Security
Blackman	Kevin	Wisekey, CTO
Braun	Thomas	WTO, IT Security
Bombardieri	Giancarlo	Zurich Financial Services, Head of Information Security / chief Risk officer
Stadler	Robert	Zürich Kantonal Bank , Chief Security Officers
Reich	Peter	Winterthur Insurance, WGR Group IT, Information Security