Implementing Information Security and Its Technology: A Line Management Perspective

William A. Barletta
Lawrence Berkeley National Laboratory, Berkeley CA
August 19, 2005

Abstract: Assuring the security and privacy of institutional information assets is a complex task for the line manager responsible for international and multi-national transactions. In the face of an unsure and often conflicting international legal framework, the line manager must employ all available tools in an Integrated Security and Privacy Management framework that ranges from legal obligations, to policy, to procedure, to cutting edge technology to counter the rapidly evolving cyber threat to information assets and the physical systems that information systems control.

Motivations

The efficient and effective operation of both public and private enterprises requires the generation, collection, retention, use, and exchange of ever expanding quantities of information[1]. Similarly the configurations of those information systems and their connexions with and even controls over embedded physical systems are becoming more complex[2]. The access to much of that information and, a fortiori, to information networks and to embedded physical systems must be strictly controlled and limited to comply with laws, to assure business confidentiality, or to prevent direct financial loss. Managing the risks associated with the use of information and an organization's information network is the goal of an integrated information security and privacy program. At the operational level cyber security and cyber privacy are two sides of a unified management task; without security there can be no privacy.

Moving beyond the individual enterprise and across national borders, the situation becomes even more complex for the line manager. One must recognize that distributed science, finance, business operations, police and intelligence activities are a reality. Increasing numbers of international enterprises rely upon information megasystems to handle enormous quantities of data and vast network traffic with an exploding assortment of connected wireless devices and sensors. The operational requirements of multi-national commercial enterprises and partnerships, multinational scientific research projects that rely on peer-to-peer distributed computing[3] and collaboratory tools[4], and

---

[1] "OECD Guidelines for the Security of Information Systems and Networks," at p.7, OECD, June, 2002

[2] An example of an attempt to control a vast physical scientific research complex with an extensive computer network is described in Deborah Agarwal, Gary Olson, Judy Olson, "Collaboration Tools for the Global Accelerator Network," Final Report of the Collaboration Tools for the Global Accelerator Network Workshop, Berkeley, CA, August 26, 2002. LBNL-532, http://dsd.lbl.gov/Collaboratories/GANMtg/GAN-Berkeley-workshop-report.pdf

[3] For a research community perspective on the promise of GRID computing, see www.gridcomputing.com and www.gridforum.org. Security architectures for the GRID are discussed in Mary R. Thompson, Abdelilah Essiari, Keith Beattie, "Distributed Security Architectures – 'Providing security services for Grids,'" www.itg.lbl.gov/security/DistSecArch.html

international counterterrorism efforts (even those restricted solely to the European Union) all require interconnections among complex autonomous information systems. These interconnections demand rigorous, multi-level authorization and access procedures that fulfill both operational and fiduciary responsibilities defined in a complex variety of judicial frameworks of uncertain scope[5].

The threats that confront line management include 1) security breaches, 2) compromise of privacy (personal and proprietary information), 3) unauthorized activities by insiders, 4) theft, sabotage and destruction of information, 5) damage to employee morale, 6) attendant public relations consequences. Each of these items can be assigned an economic value for the purpose of managing risk to the organization. This set of items, however, does not exhaust the range of threats[6] to an institution. Prudent risk management also aims at *avoiding* loss to total economic value and legal standing; for example, 1) civil and criminal penalties, 2) liabilities, 3) loss of market share, 4) drop in stock price, and 5) direct financial loss. Except for items 3) and 4), public sector employees and the governmental units for which they work face analogous risks. In addition, the public sector manager charged overseeing critical infrastructure resources faces the potential of human loss in the failure of computer controlled physical infrastructure. The most effective approach to managing this complex of risks is the enterprise-wide information assurance program.

Legal obligations

An institution's information security program forms the foundation for the soundness and integrity of its business operations. Top management[7] has a primary fiduciary responsibility to protect corporate assets; these assets include information assets and infrastructure. In *Caremark International Inc. Derivative Litigation*,[8] a Delaware court

---

[4] "The access to a remote collaborative environment, whether it is for monitoring or for control of experiments, requires that security and access limitation mechanisms be in place, so that safeguards against unauthorized access and privacy of proprietary data exist. …. Collaboratories will provide network based access to very expensive equipment and must be designed to avoid several potential security and safety problems. They must also be designed to have automated equipment failure modes with sanity checks on all incoming data and be resistant to network-based tampering." From "A Use-Condition Centered Approach to Authenticated Global Capabilities: Security Architectures for Large-Scale Distributed Collaboratory Environments", William Johnston and Case Larsen, Lawrence Berkeley Laboratory report LBNL-38850, http://www-itg.lbl.gov/~johnston

[5] See for example the discussion of conflicting access statutes in "Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes", Orin Kerr, NYU Law Review, Vol. 78, No. 5, pp. 1596-1668, November 2003 at p. 1600

[6] With respect to threats to governmental information assets, cyber criminal acts can also damage capabilities of first responders, undermine international security and development efforts, and destroy trust in modern society. For a further discussion see E. Gelbstein and A. Kamal, *Information Insecurity: A survival guide to the uncharted territories of cyber-threats and cyber-security*, United Nations ICT Task Force and United Nations Institute of Training and Research, 2nd ed., Nov. 2002, http://www.un.int/kamal/information_insecurity.

[7] By top management we refer to the Chief Executive Officer, Board of Directors and other corporate officers reporting directly to the CEO.

[8] *Caremark International Inc. Derivative Litigation*, 698 A.2d 959 (Del. Ch. 1996). This case could provide a basis for derivative shareholder suits against corporate officers and directors.

held that, "a director's obligation includes a duty to attempt in good faith to assure that a corporate information and reporting system, which the board concludes is adequate, exists, and that failure to do so under certain circumstances may, in theory at least, render a director liable for losses caused by non-compliance with applicable legal standards."

As the action of the U. S. Federal Trade Commission (FTC) in its cases against Eli Lilly & Co.[9], Guess?[10], and Microsoft Passport[11] illustrate, the implementation of an enterprise-wide information assurance program cannot be left as an afterthought. The FTC has made clear[12] that it will examine corporate security procedures where personal data has been or may be *disclosed inadvertently* because of a lack of implementation of *commonly accepted security practices*. Even the possibility of inadvertent disclosure and the mere potential for injury involving sensitive information can trigger an FTC investigation.

The FTC consent orders in these cases offer important guidance[13] to a wide range of stakeholders from regulators and judges to line managers, chief information officers and corporate counsels. What is required for sufficient care and due diligence is an enterprise-wide, integrated, 360 degree approach to protect the security of information. In cyberspace privacy of information is achieved through security.

In the world of multi-national enterprises whether they be private or governmental, the responsibilities of top managers can be exceedingly complex. A thorny legal compliance issue concerns the sharing of or potential access to data in multi-national operations. For example, the European Union (EU) has addressed meeting the standard for due diligence with respect to safeguarding confidential data through model privacy contracts[14] developed by the European Commission (EC). The second, revised model privacy contract that has taken effect in April 2005 seeks to fully address the EU Directive on Data Protection[15] while remedying the shortcomings perceived by the business community in the EC 2001 model contract. Unfortunately, US and EU practice[16] are not

---

[9] *In re Eli Lilly and Co.*, Agreement Containing Consent Order, FTC No. 0123214, Jan 18, 2002, http://www.ftc.gov/os/2002/01/lillyagree.pdf. (Hereinafter *Lily*)

[10] *In the Matter of Guess?, Inc. and Guess.com*, File No. 022 3260, Docket No. 0223260, http://www.ftc.gov/os/2003/06/guesscmp.pdf.

[11] *In the Matter of Microsoft Corporation*, File No. 012 3240, Docket No. C-4069, http://www.ftc.gov/os/2002/12/microsoftcomplaint.pdf and; *In the Matter of Microsoft Corporation*, File No. 012 3240, Agreement Containing Consent Order,

[12] Id. *Lily*

[13] See the discussion in "International Strategy for Cyberspace Security," J. Westby, ed. American Bar Association, August 2003, pp.178 – 182. (Hereinafter ISCS).

[14] These EU model contracts followed proposed clauses offered by the International Chamber of Commerce in February, 1998. The present European Commission decisions and standard contractual clauses can be found at "Model Contracts for the transfer of personal data to third countries ," http://europa.eu.int/comm/justice_home/fsj/privacy/modelcontracts/index_en.htm

[15] "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," Official Journal of the European Communities of 23 November 1995 No L. 281 p. 31, http://www.cdt.org/privacy/eudirective/EU_Directive_.html

[16] A detailed presentation of this issue can be found in Chapter 2 of the *International Guide to Privacy*, J. Westby, ed. May, 2004, American Bar Association

fully consistent with the EU requiring greater privacy protection than mandated under US law.

Bringing policy into action

Flawlessly designed security and privacy policies and procedures afford little protection of institutional information assets if they are embodied only in management edicts, documentation, and software. In fact, "organizations that adopt policies but never implement nor enforce them may find these same policies to be a liability."[17] Corporate directors and officers must bring the security program to life through the people in an organization; security like safety is the responsibility of all personnel. In particular, all levels of line management bear an essential responsibility[18] that transcends sets of technical requirements that emanate from the chief information security officer, chief security officer, or legal counsel.

This paper recommends an approach of Integrated Privacy and Security Management[19] of information that embodies several components in a cycle of continual vigilance and improvement:

i. Assessments of risks[20] and liabilities[21] in the context of business function,
ii. Top management review of risks and formulation of policy objectives
iii. Design of policy[22], procedural and technological tools and evaluation of the associated costs,
iv. Top management review and endorsement of mitigation tools and costs,
v. Training[23] / commitment[24] at all levels within the organization,

---

[17] Michael Rasmussen, "Adopted But Not Implemented Security Policies May Be Your Liability," *Ideabyte,* Apr. 9, 2002.

[18] ICSC, at 151 - 161

[19] This set of activities closely parallels the Integrated Safety Management (ISM) and Integrated Safety and Security Management (ISSM) presently promoted by the U. S. Department of Energy.

[20] Typical risks include but are not limited to a) inappropriate use, b) denial of service attacks, c) file damage or destruction, d) physical attack, e) unauthorized control access, f) unauthorized user access, g) non-directed attacks such as viruses, worms. and other malware, g) spam and spam relaying.

[21] In high-risk situations – for example, acquisitions, takeover attempts, shareholder suits, etc. – top management is required to obtain professional assistance or perform adequate analyses to mitigate the risks. See S. G. Schulman and U. S. Ottensoser, "Duties and Liabilities of Outside Directors to Ensure That Adequate Information and Control Systems are in Place – A Study in Delaware Law and The Private Securities Litigation Reform Act of 1995," Professional Liability Underwriting Society, 2002 D&O Symposium, Feb. 6-7, 2002

[22] The development of a security policy in consonance with institutional governance is discussed in ISCS, Ch. 5, Sec. B.

[23] Employees and managers cannot be expected to carry out a security policy if they are not made aware of what is expected of them. " In an "optimized" organization, training and awareness efforts ... are fully integrated into employee career paths and sufficient budgets, resources, facilities, and instructors are provided for training and education programs. There is continuous improvement in business processes taking advantage of best external practices and maturity modeling with other organizations. Problems are resolved based on root-cause analysis and organization response is efficient and fast ... Automated tools and other education technology are used extensively and integrated into training and education programs. External trainers are used as needed." ISCS, at 186.

[24] Due to the rapidly evolving nature of the information security threat, some experts recommend training and testing three times per year. Dale McNulty, "Management's Role in Information Security - The 7 Top

vi. Implementation of tools including test and evaluation of tools
vii. Monitoring[25] of compliance and enforcement,
viii. Annual reviews and audits,
ix. Adjustments to the security program.

This "enterprise program" of change management in the organization functions through a culture of acceptance of standards, policy and ethics by all employees and managers rather than through a regime of complex rules.

Unlike modern worker safety programs the most successful of which are based on the assumption that all accidents can be avoided, a prudent Integrated Privacy and Security Management System recognizes that some attacks on the information system have minimal negative impact and that some of these attacks will succeed. Consequently, for large enterprises that amass extensive data on cyber-attack incidents, a system based on a detailed return on investment (ROI) model[26] is both practical and consistent with the "due care" standard of liability. In the ROI approach the enterprise assesses the severity and frequency of each type of threat, the probability of its occurrence, the impact and costs (probable, nominal and maximum) incurred in a successful attack, the type of protection to mitigate the threat, and its enterprise-specific costs. One can then compare the costs of protection with the most probable value of cyber-damage avoided to determine the ROI, the cost effectiveness of individual protective measures. Not deploying countermeasures with a cost greater than the probable value of damage is both prudent and non-negligent.

Employees must comply with security policies and procedures, and management must take enforcement action taken in instances of violations. Both employee monitoring and audits are important compliance tools. Monitoring and screening, however, are fraught with legal considerations[27] and vastly differing legal frameworks around the globe. The

---

Mistakes," Nov. 4, 2002, www.surrex.com/changing_it_landscape/2002_11_04.html.

[25] " Employee monitoring of ICT [Information and Communications Technology] usage is one of the easiest ways to monitor compliance with security policies and procedures, but it is an area increasingly fraught with legal liability. At the outset, there are wide inconsistencies in the global legal framework in this area. Under U.S. law (and in most third world countries), private sector employees are afforded virtually no expectation of privacy in the workplace698 and are not protected by the [US] Constitutional right to privacy." ISCS, at 187.

[26] " A framework can help evaluate the costs and benefits of IT security solutions using a company's risk profile. Using an unconventional concept, this framework bases benefit on avoided risk rather than increased productivity. Lawrence Berkeley National Laboratory (LBNL) uses this framework to help demonstrate to management and auditors that it is significantly less expensive to accept some damage from cyberattacks than to attempt to prevent all possible damages. This pragmatic approach continues to enable LBNL's cybersecurity staff to optimize security countermeasure investments and reduce spending without sacrificing protection." Ashish Arora, Dennis Hall, C. Ariel Pinto, Dwayne Ramsey, Rahul Telang. "Measuring the Risk-Based Value of IT Security Solutions," IT Professional, vol. 6, no. 6, pp. 35-42, November/December 2004.

[27] "Under U.S. law (and in most developing countries), private sector employees are afforded virtually no expectation of privacy in the workplace and are not protected by a constitutional right to privacy. A few states have laws protecting privacy in the workplace; however, a notice to employees that there is no expectation of privacy often removes their effect. According to a review of case law by the U.S. General Accounting Office (GAO), 'Courts have consistently held, however, that privacy rights in such communications do not extend to employees using company-owned computer systems, even in situations where employees have password-protected accounts.' Public sector employees are, however, afforded the Constitutional right to privacy. U.S. common law tort theories also provide employees with remedies for

laws of the European Union afford the employee a higher expectation of privacy in the workplace than the U.S. Consequently multinational institutions and international enterprises, in particular, need to ensure that employee monitoring is legal within every jurisdiction where they conduct operations and conversely that sufficient monitoring is performed to meet liability standards.

Internal and external audits[28] that follow industry standards and best practices can validate compliance and due diligence. They can also measure the overall effectiveness of a security program. A strong, distributed audit system[29] should embody the following design principles:

1) Everyone is subject to audit.
2) Audits are cross-organizational.
3) Audit accuracy is measured by cross-validation.
4) Usage records are tamper-evident.
5) Audits are fully documented to include methods, findings, and recommendations and conclusions

Ideally, external audits are conducted through counsel, with the intention they be privileged as an attorney work product[30].

Technological approaches

While cyber security is not just a technological issue, it cannot be managed without up-to-date cognizance of technological trends and without continual improvement of technical tools to meet the evolving security challenge. In this sense the technological face of information security must be anticipatory, not with respect to who and how malicious parties may attack, but with respect to technological developments that enable or facilitate entire new approaches to cybercrime or cyber terrorism. As hackers and authors of malicious software develop new methods to circumvent and undermine security controls, security experts must counter with more sophisticated means of detecting intrusions in institutional networks and quarantining the compromised areas. Consequently, robust cyber-security in the most challenging of international assignments for information technology must presuppose vigorous supporting R&D in the development of technological tools.

---

invasion of privacy. The European Union, however, affords much greater privacy to both information and employees in the workplace due to its comprehensive data protection laws, and the EU approach is starting to be followed globally. *Thus, companies should take care to ensure that their employee monitoring policy is in compliance with all jurisdictions where they have employees.*" The ABA "International Corporate Privacy Handbook," J. Westby, ed., August 2003 at 146 – 147. (Hereinafter ICHP)
Management's failure to monitor traffic on its computer systems for illegal activities such as copyright infringement by employees can likewise lead to liability for the enterprise.

[28] ICHP at 149 – 157 presents a detailed discussion of the many factors that should be included in an internal audit program See also Deborah Radcliff, "The Annual Checkup," *ComputerWorld*, Sept. 9, 2002, http://www.computerworld.com/printthis/2002/0,4814,73993,00.html.

[29] The Information Systems Audit and Control Association, Inc.'s (ISACA's) has the goals to advance globally applicable standards for auditors with the skills necessary to perform information system auditing.

[30] With respect to audit reports, work product and attorney-client privilege may not provide blanket protection from disclosure. Limitations on these privileges are discussed in ICHP at 156 – 158.

The development of such a generally accepted approach to and set of technological tools for information assurance has been the goal of the Information Assurance and Survivability (IA&S) programs[31] at US Defense Advanced Projects Research Agency (DARPA). The strategy of DARPA IA&S program has been based on a layered set of defenses developed in evolving generations of technology. The foundational research for the development of defenses is creating an ever-increasing understanding of the evolution of information networks. At this most fundamental level researchers[32] have been investigating how packet traffic will move as one increases the complexity of the Internet.

The aim of first generation of defensive technology has been to *prevent intrusions* via a) trusted computing base, b) robust access control and physical security, c) multi-level security, and d) cryptography (AES[33]). As intrusions do and will occur, the second generation of security tools is designed to *detect intrusions and limit damage* via firewalls[34], boundary conditions[35], Intrusion Detection Systems (IDS)[36], monitoring and screening anomalous and unallowed activity, Virtual Private Networks, and Public Key

---

[31] S. Sastry, "Testimony and Statement for the Record," Hearing on "Cybersecurity: Getting it Right" Before the Subcommittee on Cybersecurity, Science, Research and Development, Committee on Homeland Security, United States House of Representatives, July 22nd, 2003, (hereinafter Sastry), http://hsc.house.gov/files/testimony%20Sastry.doc. The IA&S program is specifically aimed at developing architectures and network sub-systems that will make mission-critical networks highly survivable in the face of large-scale cyber attacks.

[32] Traffic models include geometric and topological characteristics of networks, statistical properties of traffic (stochastic and Markov models), and analyses of contagion and virility of malware. One goal is to understand the traffic well enough that simulators of the Internet can be built with ~10,000 nodes for the testing of survivability strategies and technical security components.

[33] "Announcing the Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf. See also "The Next Generation of Cryptography: Public Key Sizes for AES," *Code & Cipher*, http://www.certicom.com/resources/codeandcipher/volume1/issue1/template.php?article=1-nextgen ("AES succeeds DES and Triple-DES…. To date, AES remains the only symmetric encryption algorithm providing at least 128 bits of security that is approved for use by U.S. government organizations to protect sensitive, unclassified information.").

[34] *Security of the Internet*, "Firewalls," CERT Coordinating Center, Carnegie Mellon University, Software Engineering Institute, http://www.cert.org/encyc_article/tocencyc.html#BasicSec. For a description of the basic technical functioning of firewalls, *see* Gary Smith, "A Brief Taxonomy of Firewalls – Great Walls of Fire," May 18, 2001, SANS Institute, www.sans.org/rr/firewall/taxonomy.php.

[35] "Propagation of false routing information in the Internet can deny service to small or large portions of the Internet. For example, false routes can create "black holes" that absorb traffic destined for a particular block of address space. They can also lead to cascade failures that have occurred in other types of large routing/switching systems in the past, where the failure of one switch or mechanism results in the failure of those connected to it, resulting in additional waves of failures expanding outward from the initial fault." U.S. National Cyberspace Strategy at p. 30.

[36] Intrusions are "attempts to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer or network." R. Bace and P. Mell, "NIST Special Publication on Intrusion Detection Systems," www.dougmoran.com/tatzlwyrm/CACHE/nist_special_pub_on_ids.pdf. Bro, developed at the Lawrence Berkeley National Laboratory by Vern Paxson, is an example of an open source IDS which works well under very heavy loads in an open computing environment. Bro has now been adopted as the IDS software used by the US Department of Energy, sectors of the Department of Defense, and the Department of Homeland Security. ftp://ftp.ee.lbl.gov/papers/bro-CN99.ps.gz.

Infrastructure[37].

Even the most vigilant of institutions have learned that some attacks will succeed. The response to this realization is research to develop a third generation of security technology that will *operate through attacks*. Such information systems are being designed to have properties modeled on biological systems[38]; they are characterized by intrusion tolerance, graceful degradation, self-repairing capabilities[39], and real-time situation awareness of and response to attacks.

Gradually the message is getting out that firewalls are no protection[40] against insider threats, carelessness, and incompetence. In contrast powerful network IDS tools such as Bro, developed at Berkeley, are vigilant against all anomalous activity whether initiated from outside the LAN or from within. Unlike a firewall, an IDS does not assume that any activity initiated inside the firewall is innocuous. For maximal protection an IDS system should be combined with software that monitors the host computer to detect anomalous activity, especially that which leads to root compromise or the installation of software without the express instruction or consent of the system administrator. The simplest form of anomaly detection software is anti-spyware[41] software such as Spybot.

---

[37] Whitfield Diffie and M.E. Hellman, "New Directions in Cryptography," IEEE, *Transactions on Information Theory*, Vol. IT-22, Nov. 1976 at 644-54. The best known (though not the strongest) public key system is the RSA algorithm based on factorization of large integers. R.L. Rivest, A. Shamir, and L.M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, Vol 21, Feb. 1978 at 120-126.

[38] Proponents of this approach advocate modifying information systems to mimic the response of living beings which are subject to infectious diseases (viruses and worms), genetic defects (replicated architectural flaws), and attacks from other beings. From that perspective one looks to the methods that persons and other living beings use for self-protection: 1) No one expects that a person to be one hundred percent healthy all the time. The bio-system has built-in strategies for functioning at a reduced level until the system self-repairs. 2) An immune system that detects (an IDS) and adapts to new threats as they are encountered and, in many cases, can ward off infection without external assistance. The immune response may, however, cause the biological system to operate at a reduced capacity especially when it is overloaded. 3) A person being can describe its condition to external experts speeding diagnosis and recovery. 4) Health protection (cyber-security) can be administered using a cost vs. benefit approach that weighs the cost of prevention against the cost of doing nothing and come up with a cost effective policy for health care (cyber-security). 5) A person can incur liability. He can infect other beings; he can be taken over and used to attack and damage other beings. This type of behavior is clearly a danger in networks.

[39] For a discussion of the utility of and the approach to self-healing systems see R. J. Ellison, N. R. Mead, T A. Longstaff, R. C. Linger, "The Survivability Imperative: Protecting Critical Systems," http://www.stsc.hill.af.mil/crosstalk/2000/10/linger.html; *see also* H. F. Lipson and D. A. Fisher, "Survivability—A New Technical and Business Perspective on Security," CERT Coordination Center; Carnegie Mellon University, Software Engineering Institute, http://www.cert.org/archive/pdf/busperspec.pdf. A substantial bibliography can also be found at http://www.cert.org/nav/allpubs.html.

[40] As firewalls neither stop traffic on allowed ports nor prevent the movement of what is already allowed through the system, they are useless against insider attacks and the far more prevalent mistakes and follies of inside users Relying primarily on the firewall is one of the seven top management errors that lead to computer security vulnerabilities. See "The 7 Top Management Errors that Lead to Computer Security Vulnerabilities," The SANS Institute, http://www.sans.org/resources/errors.php. This is not to imply that firewalls are not valuable, only that they must be combined with other countermeasures in a layered defense.

[41] Executable applications, deployed without adequate notice, consent, or control of a computer owner (spyware) represent an increasingly malicious threat to personal computer systems: CoolWebSearch

Wireless communications offer enhanced flexibility and convenience at the cost of a wide range of potential security vulnerabilities including compromise of an organization's security boundaries.

The past two years have witnessed malicious codes[42] with an unprecedented level of infectiousness and virulence. As the time constant of contagion decreases, so also must the response time of network cyber defenses. To make security defenses more responsive, network architects will need to develop a deeper understanding of just how infection traverses and expands across networks. That understanding is a goal of two large-scale test-bed projects[43] in the US being conducted under joint NSF-HSARPA sponsorship.

Contemporaneous with the appearance of cyber attacks having a worldwide effects in a matter of less than 24 hours, the expanding demand and need for ultra-high speed information networks is presenting the largest institutional users with the opportunity to insist on new "rules of the road" unencumbered by the unattractive economics of retrofitting existing equipment. One may expect the users of next generation internets not only to accept but also to demand the use of Internet Protocols (such as IPv6[44]) and logging procedures that will allow rapid packet tracking for reliable attribution (and

---

renders browsers useless by changing Internet Explorer settings and installing malicious applications; KeenValue collects information about users and sends advertisements to their systems; Perfect Keylogger logs keystrokes users enter, putting users' personal information and passwords at risk; Marketscore redirects traffic from a host system to another that collects data before traffic reaches its final destination. Moreover, the data gathered by spyware can easily be used to convert the host computer to be used as a "zombie" (unwitting accomplice) computer in large-scale denial of service attacks. Surprisingly, an industry-wide definition of spyware is lacking to guide anti-spyware development.
With respect to anti-spyware statutes, the legal framework is in the early stages of development. At the Federal level in the US, five bills were introduced in the Congress in 2005; none have yet been signed into law. At the state level the legal framework is more advanced. "…State lawmakers are rushing to pass legislation. New antispyware laws have been enacted in the past three months in Arizona, Arkansas, Georgia, Iowa, Virginia and Washington. Utah, which led the state rush with its initial antispyware statute last year, recently strengthened its law to restrict pop-up ads and clarify penalties for violations. Spyware legislation is pending in 20 more states. Facing a hodgepodge of state laws and regulations, business and consumer groups are throwing their weight behind federal legislation that would stiffen penalties and give the FTC specific enforcement authority over spyware interlopers." J. Ostroff, Kiplinger Business Forecasts, Vol 6, May 27, 2005. http://www.compassweb.com/cob/kiplinger/200506/fighting_spyware.html
In the European Union, Directive 2002/58/EC (July 12, 2002), "Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector" targets specific technical means that provide access to information, store hidden information or trace the activities of users without their knowledge. Article 5(3) of this Directive requires Member States to ensure that electronic communications networks store information or gain access to information stored in the terminal equipment of users only if they have clear and comprehensive information in accordance with Directive 95/46/EC of October 24, 1995 "Protection of Individuals with Regards to the Processing of Personal Data and on the Free Movement of Such Data."

[42] The web site of the CERT Coordination Center, Carnegie Mellon University, Software Engineering Institute, publishes incident notices concerning malicious codes. www.cert.org/incident_notes/index.html.

[43] Two university collaborations including U. C. Berkeley and Carnegie-Mellon University will set up closed networks of approximately 10,000 nodes on which they will launch malicious code of varying degrees of virulence in presence of simulated network traffic. See Sastry, sec. 4

[44] See Lipson at p.55, footnote 52 ("For example, a shortage of IP addresses has led to the increased use of dynamic IP addresses instead fixed IP addresses, and the use of network address translation (NAT) allowing multiple machines to share a single globally routable IP address.").

retribution). Thus we may eventually see the debate over the values and dangers of anonymity relegated to the back roads of cyberspace as institutional users "vote with their feet."

The convergence of affordable, high quality audio-visual technology with extremely high bandwidth information networks and with global collaborative enterprises is being embodied in GRID computing[45] and extensive peer-to-peer, multi-access level environments. This trend will extend the challenges of operating within and across multiple legal frameworks from being the province of large multi-national corporations to the realm of small businesses and university researchers.

Line management must be aware of the varied and numerous technological tools[46] that can impact privacy and security programs both with respect to benefits and to costs. Strong encryption[47] can protect sensitive data and privacy at the cost of administrative and performance overheads. Authorization and access controls (such as passwords, biometric technologies[48], and common access cards) are evolving rapidly to enhance security, but often at the cost of less privacy within an organization. Digital signatures[49], authentication technologies, and digital time stamps are useful for evidentiary, audit, and

---

[45] The GRID implements one the characteristics of extensive computation envisioned in the earliest days of the ARPAnet, i.e., making the network the computer. This vision was largely postponed by the advent of the microprocessor combined with the relatively low bandwidth and high latency of networks at the time. The result has been the present infrastructure of and extremely large number of powerful localized computers. Ian Foster, Carl Kesselman, Steven Tuecke, "The Anatomy of the Grid: Enabling Scalable Virtual Organizations," Int'l Journal Supercomputer Applications, Vol. 15, No. 3, 2001 at 200-222, www.globus.org/research/papers/anatomy.pdf. For a description of a large number of functioning scientific grids, *see* Ron Oldfield, "Summary of Existing and Developing Data Grids," Sept. 11, 2001, www.ggf1.nl/abstracts/DATA/datagrids3.pdf.

[46] See ICSC, Sec. VI.C.2.a at 208 - 222

[47] The theoretical strength of an encryption system is measured by the amount of time required by a computer to break the coding algorithm. Governmental policies in many countries have evolved over the past decade to favor the expanded use and dissemination of strong encryption tools, especially public key infrastructure systems. A discussion of relevant governmental policies and responsibilities worldwide can be found in "Cryptography and Liberty 2000," Electronic Privacy Information Center, http://www2.epic.org/reports/crypto2000/overview.html#Heading7

[48] Biometric identifiers are rapidly becoming a widely required element in transportation security. For example "In the United States, the Enhanced Border Security Act calls for the Immigration and Naturalization Service (INS) to take a unique biometric identifier, like a fingerprint or a face scan, from every alien entering and exiting the United States with a visa by 26 October 2004 (US House of Representatives, 2002). The United States is also extending the requirement for biometrics to be incorporated into tamper-resistant travel documents of other countries in its visa waiver programme as a condition of continued participation (Fonseca, 2002; US Department of State, 2002)." Working Party on Information Security and Privacy, "Biometric-Based Technologies." OECD report DSTI/ICCP/REG(2003)2/FINAL 30 June 2004 at 10.
As biometric data that characterize an individual are increasingly being considered by many states to be the property of said individual, the use of and transfer of biometric identifiers raises particular concerns with respect to the compromise of privacy of the individual. Reflecting this point of view the OECD Directorate For Science, Technology And Industry recommends that "…the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* and the *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* be embodied in any biometric system design and project." Id at 5.

[49] A thorough review of international statutes concerning digital signatures and certification is given in Simone van der Hof, "Digital Signature Law Survey," http://rechten.kub.nl/simone/ds-lawsu.htm

security purposes; the cost of these measures, however, may be decreased interoperability among an organization's information systems. System logs are crucial to tracking and tracing attacks and audits, but they also constitute another large, sensitive database to protect[50]. Anonymizing and sanitization technologies can also be useful in protecting privacy, but may also protect malicious agents. In the end it is the responsibility to weigh the benefits against the costs.

Conclusions

The Internet is intrinsically a transnational entity. Every day from every portion of the globe new forms of cyber-threats emerge with increasing virulence. The cyber-vandal and cyber thief may launch their hidden by distances of thousands of miles from their targets. While being an indispensable staring point, local action within the enterprise cannot alone safeguard information assets. The private sector must continue to work with governments to create a suitable legal framework including new, transnational evidentiary standards[51] for the protection of those assets in an international operating environment. Securing information assets will in the end require continuing vigilance and cooperation among the business, research, technical and service provider communities in the framework of a robust and consistent international legal framework in which law enforcement has appropriate and sufficient forensic tools.[52]

Integrated privacy and security management of information depends upon the effective implementation of policy, procedural, and technological tools utilized to help automate the privacy plan and monitor the effectiveness of and compliance with policies and procedures. The problem for the top management in consultation with counsel is to decide where to operate its information systems in the three dimensional space of security, performance and functionality, to decide what costs of security and privacy are consistent with sufficient care, due diligence, and information system functionality. The result should be a regime of cost-effective risk management that is balanced with respect to potential harm.

If all organizations establish enterprise security programs (on a scale commensurate with their operations), if they train personnel and management at all levels throughout the

---

[50] In fact, logs are frequently among the files that attackers destroy. Moreover, as noted in the United States Department of Justice manual, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Ch. 3, Pt G. (2002)

> Some providers retain records for months, others for hours, and others not at all. As a practical matter, this means that evidence may be destroyed or lost before law enforcement can obtain the appropriate legal order compelling disclosure.

[51] "… existing rules of criminal procedure are poorly equipped to regulate the collection of digital evidence … new rules of criminal procedure will evolve to regulate digital evidence investigations… Rules that balance privacy and public safety when applied to the facts of physical crime investigations often lead to astonishing results when applied to the facts of computer crime investigations. They permit extraordinarily invasive government powers to go unregulated in some contexts, and yet allow phantom privacy threats to shut down legitimate investigations in others. " Orin Kerr, "Digital Evidence and the New Criminal Procedure," Columbia Law Review (Jan. 2005)

[52] For a recent survey of current computer forensics practices see Bill Nelson, et. al., "Guide To Computer Forensics And Investigations," (Thompson 2004)

organization, if they take technological considerations into account and counter vulnerabilities and risks with appropriate technologies, and if they work with governments to promote a responsive legal framework, a global strategy for information security will emerge.

Recommendations for the World Federation of Scientists

Cost-effective cybersecurity and privacy in nascent information societies: The integrated privacy and security of information for enterprise users of the internet in nascent information societies will depend upon their implementing effective procedural and technological tools to bring to life privacy and security plans and to monitor the effectiveness of and compliance with privacy and security procedures that meet at least minimal standards established and tested by expert developers of information system for small and medium sized enterprises.

This paper recommends that

A) the development of risk management tools specifically tailored for enterprise managers in nascent information societies that include
    1) model information security plans scaled to the size and nature of the enterprise,
    2) templates for assessing their vulnerabilities and returns on investment for employing cybersecurity tools,
    3) training modules to promote awareness in employees in secure computing practices and procedures.
    4) self-help modules for conducting periodic cybersecurity audits.

B) the use of network security tools including strong forensic capabilities at the early installation phases of networking hardware in nascent information societies.

C) the articulation of a uniform, transnational legal guidelines for enterprise managers that can be embodied in the laws of nascent information societies.

Toward an effective anti-spyware strategy: Executable applications and monitoring hardware deployed without adequate notice, consent, or control of a computer owner and outside judicial control represent an increasingly malicious threat to the operability of personal computer systems and to the privacy of information on these systems. Moreover, the data gathered by spyware can easily be used to convert the host computer to be used as an unwitting accomplice computer in large-scale denial of service attacks. With respect to anti-spyware statutes, the legal framework is in the early stages of development.

This paper recommends that

A) adopting industry wide definitions of spyware in both hardware and software forms to guide anti-spyware development.

B) developing guidelines that provide a uniform legal framework to stiffen penalties for the use of spyware and give relevant national entities specific enforcement authority over spyware interlopers.

Acknowledgment

I wish to thank the editor, Jody Westby, and all my fellow authors of the "Science & Technology and Implementation" chapters of the ABA books, *International Strategy for Cyberspace Security* and *International Guide to Privacy* for many hours of illuminating discussions concerning the configuration of institutional security policies and procedures. I am grateful to Dr. D. Agarwal, D. Hall, and A. X. Merola of the Lawrence Berkeley National Laboratory for their deep insights concerning multi-level access systems, return-on-investments models, and bio-mimicry in cyber protection strategies.

This work was partially supported by the U.S. Department of Energy under Contracts No. DEAC03-76SF00098 and DE-FG02-04CH11231.