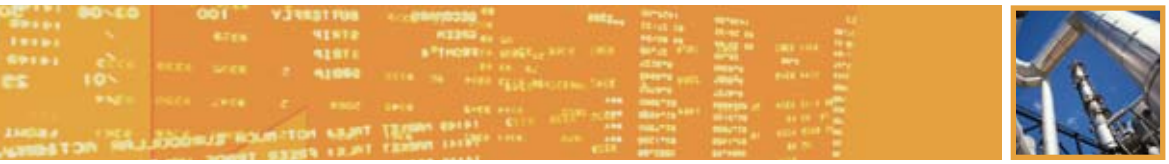


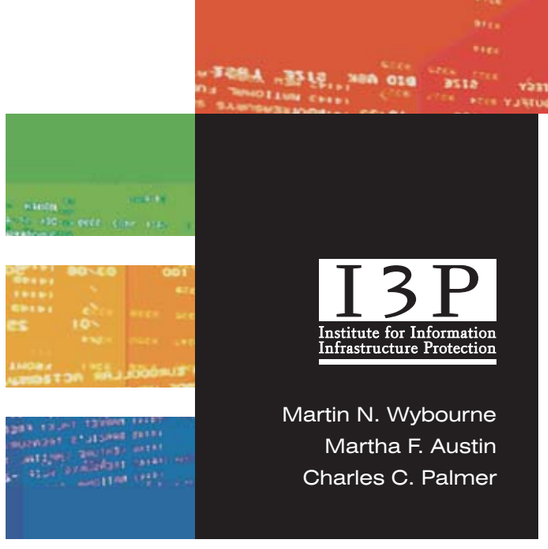
National Cyber Security
Research and Development Challenges
Related to Economics, Physical Infrastructure and Human Behavior

An Industry, Academic and Government Perspective

2009

I3P
Institute for Information Infrastructure Protection

A report to the Chairman and Ranking Member of the US Senate Committee on Homeland Security and Governmental Affairs.



Martin N. Wybourne
Martha F. Austin
Charles C. Palmer

2 Preface

4 Executive Summary

7 Economic Infrastructure Security

15 Physical Infrastructure Security

23 Human Infrastructure Security

29 Conclusion

31 Participants

The Institute for Information Infrastructure Protection (I3P) would like to thank US Senators Joseph Lieberman and Susan Collins, Chair and Ranking Member of the US Senate Committee on Homeland Security and Governmental Affairs, for serving as honorary co-chairs of the forums that led to this report. The Senators' recognition of the importance of making research and development in cyber security a national priority enabled us to bring together many experts in the field. We would also like to thank the Homeland Security Committee staff, notably Deborah Parkinson and Adam Sedgewick from Senator Lieberman's office, and John Grant, Counsel to Senator Susan Collins, for their help and guidance.

Our forum moderators were instrumental in shaping each topic area and guiding the discussions. Our thanks to Dr. M. Eric Johnson, Professor of Operations Management at the Tuck School of Business at Dartmouth for leading the economics forum, Dr. Robert K. Cunningham of MIT Lincoln Laboratory for leading the physical infrastructure forum, and Dr. Shari Lawrence Pfleeger of the RAND Corporation for her leadership of the human behavior forum.

Trudy E. Bell served as contract technical editor of this report, and we thank her for the time and effort spent on our behalf.

Finally, we would like to express our gratitude to the National Institute of Standards and Technology for the grant that allowed these forums to be held.

Preface

In 2002, the I3P was founded at Dartmouth College with a grant from the federal government and a mandate to coordinate and support multidisciplinary research and development in the area of cyber security.

Since that time, the world has witnessed a growing collection of cyber security threats, seen its dependency on the Internet grow, and struggled to keep emerging vulnerabilities in check. A recent report published by the Center for Strategic and International Studies (CSIS) identifies vulnerabilities in cyber space as an urgent national security challenge[1]. Corporate networks are increasingly at risk, malicious attacks are rising sharply, and organized crime and terrorists are improving their cyber capabilities.

No individual or organization, either in the private or public sector, is immune to the multifaceted threats of the digital era. Nor can any one research department or institution single-handedly address—or hope to stem the tide of—this continuously evolving problem. A concerted and collaborative research effort is needed to manage the situation and provide solutions to the pressing cyber security problems our nation faces.

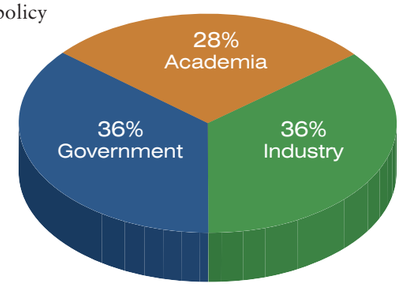
Recognizing this need, US Senators Joseph Lieberman and Susan Collins, Chair and Ranking Member of the Senate Committee on Homeland Security and Governmental Affairs, served as honorary co-chairs of a series of three forums in the Fall of 2008 focused on identifying cyber security research and development priorities for the new administration from the perspective of the public and private sectors. The forums were organized and moderated by I3P researchers in collaboration with US Senate staff.

The objective of the forums was to enlist the technical and scientific community's help in identifying government-supported research and development priorities for the next five to ten years. A total of 92 experts, representing industry, government and academia participated in one or more of the three forums. Asked to help set strategic objectives for moving the nation toward a more secure cyber infrastructure, the group wrestled with such hard questions as: What are the impediments to securing cyberspace? Can those impediments be overcome? What range of threats faces the nation's infrastructure? And how, once identified, can the vulnerabilities linked to those threats best be addressed in a timely, reliable, and sustainable way?

The forums focused specifically on the cyber security challenges facing the economic, physical, and human infrastructures within the US. At the end of each forum, the participants developed a list of research and development priorities. It is our opinion that if addressed by the government agencies overseeing the national agenda in cyber security, these priorities would lead to a more robust cyber security stance for the nation.

This summary report reflects the collective wisdom and expertise of the forum participants, who were evenly distributed across industry, government, and academia. This report is a distillation of the dialogue that took place within each forum and a summary of the opinions expressed by the participants. While no single best answer emerged from these discussions, barriers to progress were discussed and strategies for moving ahead in the short term were identified. The end results are specific recommendations for technology and policy research that reflect the primary concerns of both the public and private sectors.

The new administration has a major opportunity to direct and coordinate cyber security research and development efforts in ways that could provide protection from threats in the near term. This report is intended to provide informed suggestions as a path forward is determined.



I3P Forum Participation by Sector

Government, industry and academia were evenly represented at the I3P forums, where thought leaders from each sector engaged in discussion and information sharing.

[1] "Securing Cyberspace for the 44th Presidency", Center for Strategic and International Studies: http://www.csis.org/media/csis/pubs/081208_securingcyberspace_44.pdf

Executive Summary

An examination of the cyber security challenges facing the economic, physical, and human infrastructures underscores the need to make cyber security a national priority.

The scale of the challenges, as well as their significance to US security, demands nothing less than a concerted national effort. The set of recommendations produced as the result of the I3P forums will guide the research and development process by highlighting areas that will likely produce tangible results within the next five to ten years. Some of the recommendations that emerged from the forums are unique to an individual sector; others are common to all three.

The economics sector, that is, the businesses, supply chains and financial institutions that drive the US economy, depends heavily on Information Technology (IT) systems, which are neither entirely reliable nor fully secure. The lack of security is significant: economic losses attributed to IT attacks are reaching a magnitude that could affect US economic security. Globalization has also taken its toll on security, with multinational companies stymied by conflicting or non-existing regulations, cultural differences and varying degrees of technological maturity. Participants identified the need for a research and development agenda that would: (1) address market and regulatory impediments, (2) ensure that security is built into products and processes, and (3) develop national and international doctrines for information security.

Computer-based control systems run much of the nation's physical infrastructure, including such critical operations as telecommunications and power distribution, oil and gas production, and water purification and distribution. Such systems are increasingly connected to the Internet and therefore vulnerable to new and unforeseen types of cyber disruption. Participants identified three research and development strategies that should be supported by the government: (1) ensure the confidentiality, integrity and availability of real-time data generated by process control systems, (2) identify the origin and history of input data and of physical components so their trustworthiness in an untrustworthy environment can be assessed, and (3) develop metrics for security.

Human behavior is perhaps the most challenging and vulnerable of the three areas considered. Effective security depends not only on technology but also on the employees, business partners, customers and others using information systems and networks. As such, people are often the weakest link in the security chain. Security technologies and policies may be hard to use or understand and thus are seen as impediments. Moreover, workplaces are social environments, where people are often influenced by the social norms of their peers as well as by the way information technologies, such as online social networking, alter human interaction. Considering these and other factors, participants identified the following research and development priorities: (1) apply well known social-science protocols to the development of an effective security culture, (2) support the creation and implementation of motivation-based strategies for the prevention and remediation of human-induced error (including misuse and malicious use), (3) design security technologies based on the principles of good human-computer interaction so as to maximize user compliance, and (4) design curricula and outreach programs for K-16 education that will ensure the future workforce has an awareness of—and respect for—security.

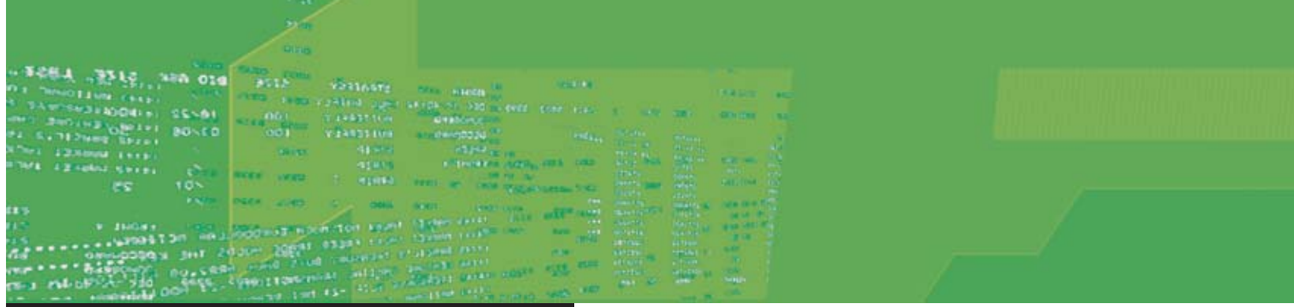
Four common themes emerged that form the core recommendations contained in this report:

- **A coordinated and collaborative approach is needed.**
  Cyber security research and development efforts in the US must be better coordinated; only through information sharing and collaboration can effective solutions emerge.

- **Metrics for security are a broad enabler and must be developed.**
  Metrics for assessing the security of a system, a process, or even a single component are key to many of the recommendations articulated in this report. Metrics are enablers, essential to helping companies, governments and suppliers make better security decisions; they also strengthen the legal and policy framework.

- **An effective legal and policy framework for security must be created.**
  A national strategy for cyber security requires a sound domestic legal and policy framework as well as an international doctrine, which the US should develop based on multilateral input and understanding. At present, rather than helping secure cyberspace, the US regulatory and legal environment indirectly encourages a "checkbox" mentality, which discourages innovation.

- **The human dimension of security must be addressed.**
  Technologists and policymakers must consider the human element carefully when developing security solutions. No culture can be made secure without understanding human behavior and motivation. Moreover, people—given the right level of understanding and awareness—can be engaged as a positive force in the quest for improved security.



Economic Infrastructure Security

"…there are three kinds of companies: one that has been broken into, one that is going to be, and one that is going to be again."

According to the Department of Homeland Security, an estimated 85 percent of the nation's critical infrastructures are owned and managed by the private sector. Corporations are critically dependent on the IT systems that handle the majority of their business processes and keep track of their corporate data, such as financial information, intellectual property, human resource records, and customer records. The loss or damage of these processes or data, or their unavailability due to an IT security incident, has caused damage ranging from supply disruptions or the loss of proprietary information, to the exposure of customers' private data, to the loss of millions of dollars for each hour of website downtime.

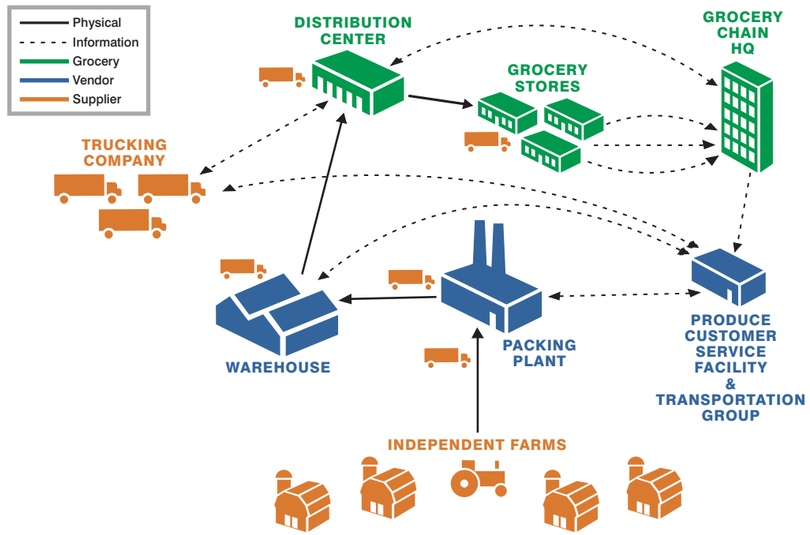
At the same time, globalization has created new concerns, with cyber security often at the mercy of conflicting regulations, no regulations, cultural differences, and varying degrees of national technological maturity. Thus, when IT security difficulties arise in the global marketplace, there are no clear paths to resolution.

While corporate dependence on IT systems is increasing worldwide, so are the risks associated with that dependence. Yet, the precise number and severity of IT security incidents is unknown. Companies have been quietly absorbing losses, unwilling to incur negative publicity or shareholder response by releasing information about any known penetration of their IT systems. Government intelligence and law enforcement organizations are hesitant to give statistics or warnings for fear of disclosing sources of intelligence.

IT professionals have invested so much time blocking cyber attacks that they are effectively shielding the fact that the attacks are occurring at all, so the seriousness of the problem is not clearly visible to the senior management of the company. The nation is increasingly at risk due to this invisibility and silence. Forum participants agreed that economic losses related to IT attacks are reaching a magnitude that could affect US economic security.

SPECIFIC RISKS

The fact that computers get hacked or infected with viruses is not new. What is new is the changing nature, sophistication, and subtlety of attacks. Far fewer attacks take down an organization's entire IT system; instead, attacks now penetrate IT systems without impairing them, specifically to siphon out sensitive information over time without detection.



Grocery stores, like most businesses, depend on complex networks of partners and suppliers, also known as supply chains. Although the chains are highly individualized, all depend on the information infrastructure. A cyber breach directed at any one link, for instance, a distribution center that manages inventory and shipments electronically, can affect the entire chain. Understanding critical interdependencies in this network and how they might be affected by a cyber disruption remains a significant challenge. *(Content provided by Scott Dynes.)*

Areas of growing concern include:

- **Insider threats:** This is perhaps the most difficult category of threats, since the perpetrators are already inside the organization leveraging their access to corporate information.
- **Persistent targeted threats:** These are sophisticated threats targeting proprietary or sensitive information, often through subtle means such as faked email messages or the exploitation of a series of individually innocuous vulnerabilities.
- **Supply chain threats:** In addition to the vulnerability of supply chains to direct IT security attacks, the danger of counterfeit or tampered computer hardware and software provided by vendors and suppliers, often based overseas, has already made headlines.
- **Attacks against data:** While great emphasis has been placed on securing data in transit, defending that data against unauthorized editing is often overlooked. (See figure p.19.)
- **IT security arms race:** The threat is asymmetrical, with the adversary able to focus time and money on attacks while the target has to prioritize spending on IT security among other budget items.
- **Unpunished attacks:** The non-US adversary is emboldened by the difficulty of prosecution across national boundaries.

"Every time I put a computer on the net, it gets shot at."

It is evident that research addressing the technological and policy challenges posed by the risks to the economic infrastructure of the nation is needed. Participants identified three key research strategies for the economic infrastructure: (1) address market and regulatory impediments, (2) ensure that security is built into products and processes, and (3) develop a national doctrine for information security.

1. MARKET AND REGULATORY IMPEDIMENTS

Corporations are continuously balancing response to market forces and maintaining shareholder value, while meeting their regulatory requirements. These regulatory frameworks protect the public as well as the corporations who must implement them. One challenge posed by

many regulatory frameworks is the prescriptive tone that can make compliance difficult and sometimes leads to conflicts with other regulations.

PARTIAL LIST OF COMPLIANCE REGULATIONS
SEC – Securities and Exchange Commission Regulations
FINRA - Financial Industry Regulatory Authority
SOX – Sarbanes Oxley
GLBA – Gramm Leach Bliley Act
HIPAA – Health Insurance Portability and Accountability Act
FISMA – Federal Information Security Management Act
FFIEC – Federal Financial Institutions Examination Council
CAN-SPAM Act (email spam laws)
FERPA - Family Educational Rights and Privacy Act
FACT – Fair and Accurate Credit Transactions Act (Id theft prevention)
US Patriot Act (money laundering deterrence section)
~46 state security-breach notification laws

Proliferation of regulatory requirements, some of them conflicting, creates compliance challenges.

Statistics regarding cyber security incidents, their causes, and impacts are difficult to obtain and are not comprehensive. Concerned that their shortcomings might be widely publicized or even lead to government intervention, corporations and governments are often reluctant to share information. This lack of reliable information may in turn inhibit executives and government leaders from taking action on cyber security. In addition, the limited availability and completeness of this kind of information adversely impacts the capability of technology providers to both understand the threats and investigate strategies to address them.

Research and development recommendations:

- **Development of outcome-based regulations.**

  Prescriptive regulation may negatively affect a business's security choices, making it hard to keep up with rapidly evolving technologies and vulnerabilities. Regulations also encourage a "checklist" attitude rather than a real focus on improving security. An outcome-based regulatory framework, such as exists for food safety or pollution controls, would encourage more meaningful action. Research is needed to develop new security assessment techniques that enable outcome-based regulations.

- **Better technologies to share restricted information.**

  Development of an accurate, up-to-date database from the private and public sectors on IT attacks, penetrations, causes, and consequences is needed. This would vastly improve the accuracy of threat modeling for building better systems. It would also enable new mechanisms for managing and transferring IT security risk, via insurance or other means. However, the research must also address the means of protecting the confidentiality of the organizations providing the information, while making the information widely available.

- **The measurement and communication of information risk.**

  Quantifying IT security risks is already recognized as an important research topic. While focus there must continue, it should be complemented with research toward the effective dissemination of that information to various levels of consumers, ranging from corporations and governments to the general public.

2. STRATEGY FOR BUILT-IN SECURITY

The forum participants agreed that security is often treated as an afterthought or as optional —downloadable antivirus software for example—rather than being integral to a system's hardware and software. As such, security add-ons are often poorly integrated with the rest of the system and are seen as an impediment rather than an enabler. Even when security is an integral feature of a product, it may be poorly implemented. One participant noted that even within the government, "very often cryptography for federal desktop computers is not implemented in the mode in which it was tested."

In addition to ensuring that security is a consideration throughout the software development lifecycle, seeing that the users of those computer systems have security built into their understanding and use of the systems is equally important. People trained to understand the importance of security are far more likely to follow security guidelines and to strive to improve

and streamline them. The cultural shift toward openness and free access to personal information that is the hallmark of the Web 2.0 generation was raised as a concern by the participants. One participant observed that we should train people to "treat information as if it were their own money."

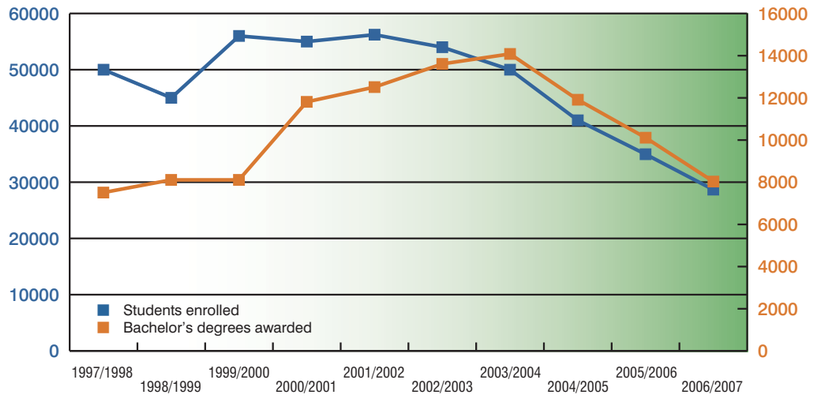
Research and development recommendations:

- **Better methodologies for assessing the security of complex systems.**
  Security must be considered for individual computers and software products; it must also be considered when these elements are combined. Companies are being driven to adopt new ideas like Web 2.0, but research into better ways to weigh the new functionality against any change in risk is needed.

- **Incentives in public/private partnership.**
  Producers of hardware and software currently have few, if any, motivations to provide secure solutions. Regulations too often encourage "checking the box" attitudes or fall behind the fast advance of technology. An exploration of incentives that would position security as a competitive advantage is needed. For example, innovation prizes and awards programs, like the Malcolm Baldrige National Quality Award[3] might be considered.

- **Develop a more holistic view of IT, including security, in K-16 education.**
  Several participants expressed concern that the number of US computer scientists continues to decline whereas in other nations the numbers are rising.

  As one participant observed, "[students] might find more excitement if they realized the field involves policy, legal, business, and economics, not just computer science." Investigation of the causes and potential remedies to this increasing shortage is needed, as well as how IT ethics and security can be incorporated into K-16 education.



Number of bachelor's degrees awarded in computer science from US Ph.D.-granting computer science departments fell 43 percent from 2004 to 2007; student enrollment in computer science programs also fell.[2]

[2] Chart based on statistics from the CRA Taulbee Survey; CRA Bulletin 3/1/2008: http://www.cra.org/CRN/articles/march08/jvegso_enrollments.html

3. NATIONAL/INTERNATIONAL DOCTRINE FOR INFORMATION SECURITY

The forum participants agreed that a US national information security strategy can only become a reality if the doctrine is based on multilateral international agreement. While there are US laws and regulations that address physical border concerns, the issues become far less clear in the borderless reality of cyberspace. One participant observed, "… a world protocol is needed. We have a world economy, a world legal system …. For information security, we need world conduct, ethics, monitoring, and response. The US cannot do it alone."

The object of the international doctrine should be to devise ways to eliminate threats, not just to identify ways to defend against them. Such a doctrine should specify clear roles and responsibilities regarding the security of IT components, from producers to customers. Moreover, the doctrine should codify normative behavior in cyberspace and should identify cyber attacks and abuse as crimes rather than national security issues.

"The US cannot do this alone. We may have the biggest stake. We were the originators of this technology, of these systems. But we can't do it alone."

[3] The US Commerce Department's National Institute of Standards and Technology manages the Baldrige National Quality Program. See http://www.quality.nist.gov/

The International Financial Reporting Standards (IFRS), which have already been adopted by dozens of nations, with many others moving toward adoption, represent a multinational agreement that has proven to be effective in world trade.

Research and development recommendations:

- **Tools for implementing, monitoring, and enforcing the international doctrine.**

  To be successful, the doctrine should include both policy and technology components. Policy tools include cross-border legal recourse and considerations of effective punitive measures. Technological responses needing investigation include advanced monitoring and forensic analysis at network speeds, and effective quarantining of network flows from specific origins.

- **Framework for defining normative behavior.**

  While fraught with subtlety and cultural differences, some basis for a definition of acceptable behavior in cyberspace is a component of this doctrine. This is a complex challenge, which is unlikely to have a single one-size-fits-all solution. Thus, a framework into which the various national concerns and standards can be introduced and harmonized should be pursued.

- **Protocol for the harmonization of security and privacy.**

  The doctrine will have to address the issue of achieving security without the elimination of privacy. The European Union's primary focus, for example, is on privacy rather than information security, whereas in the US, security concerns are paramount. Cultural differences and differing technological maturities throughout the world will also drive this research.

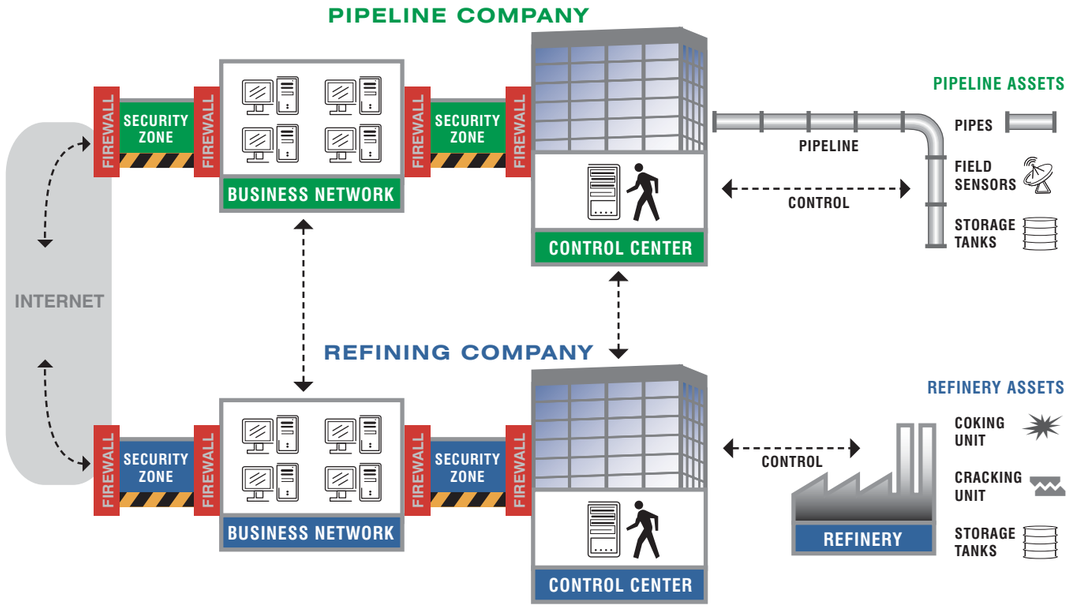
Physical Infrastructure Security

"In industry, one question often arises: How do I know that my system is secure?"

Process control systems efficiently manage large parts of the nation's physical infrastructure. For example, the oil and gas industry uses them to control flow in pipelines and refinery production; the electric power industry uses them to optimize power generation capacity and delivery; chemical plants depend on them for managing formulations and ensuring efficient production; water treatment systems rely on them for purification and delivery. Many other infrastructures could be added to this list, including air traffic control, transportation systems, nuclear power, as well as healthcare-related technologies such as embedded medical devices.

Process control systems comprise computers and the networks that interconnect them, as well as the sensors and actuators that physically monitor and control the process. When first introduced in the late 1960s, process control systems were a collection of special-purpose computers and sensors on closed, often proprietary, local networks. As such, these early systems were relatively easy to protect from electronic intrusion and sabotage.

As technology has evolved and process control systems have been developed to achieve better control, operational efficiency and audit capabilities, the security situation has changed. The forum participants agree that the Internet, a cost-effective and straightforward means to connect systems, was a significant contributing factor to this change. Another factor, although emphasized less at the forum, is the spread of wireless technology.



Process control networks are typically separated from the business network by a double-firewalled security zone. The control center monitors and manages a complex network of sensors, which provide real-time data on critical processes. Data may be transmitted to and from the control center via the Internet or other means. Despite security measures, vulnerabilities persist at each point in the communication chain. *(Content provided by A. McIntryre.)*

While such technological developments provide advantages, they also give rise to heightened security vulnerabilities and threats from hackers, terrorists, and nation states, as well as from insiders. The forum participants acknowledged that no single security strategy will work for all sectors, and that even within a sector the requirements may vary significantly. However, vendors indicated that they are interested in improving the security of products they develop and the networks their products support.

The security challenges associated with process control systems must be met within the framework of two key attributes: first, the systems must operate in real-time, which limits any latent time available for security related processing; second, the systems ideally should be uninterruptible but at least be able to recover rapidly and safely after a cyber disruption. An additional challenge is that process control systems often incorporate legacy components that have little built-in security.

Within this context, the forum participants discussed security principles and best practices for process control systems, and identified some important gaps that would benefit from focused research and development in the near future. They are: (1) the confidentiality, integrity, and availability of real-time process control system data, (2) the provenance of data, and (3) security metrics that specifically address the real-time environment.

While these are areas of active research for traditional IT systems, they are much less understood in the sector-specific, real-time environment of today's process control systems. The forum participants also stressed that evaluating the effectiveness of new security solutions for these systems will require the development of appropriate metrics, which will then have to be accepted and deployed.

1. CONFIDENTIALITY, INTEGRITY AND AVAILABILITY OF DATA

Confidentiality, integrity and availability of data are critical attributes for the correct operation of process control systems. Most process control systems are real-time systems, which means they must respond to inputs immediately, just as a conversation between two people proceeds without the delays imposed by written correspondence. Control systems must also respond correctly because some of the processes they control cannot be restarted or reversed.

Working in real-time hinders the adoption of the basic security attributes in process control systems. Traditional security solutions, such as anti-virus or intrusion detection and prevention schemes, are not appropriate for real-time environments as they can hinder a timely response. This situation can be problematic since it removes the protection from individual components of a process control system, thereby leaving vulnerabilities that can be exploited. The situation is further complicated by the difficulty of patching or reconfiguring an uninterruptible system.

Research and development recommendations:

- **Extremely large-scale, efficient authentication.**

  As the components of a process control system grow in number, type, ownership, capability, and interconnection, the trustworthiness of the entire system depends on the ability of the components to quickly authenticate themselves at system startup or following a local or system-wide disruptive event. Further, both the hardware and software systems should be able to be authenticated, and should be resistant to tampering attacks. Research toward an optimal means of handling these complex authentication processes is essential to improving the security of real-time process control systems.

- **Low overhead security protection for process control systems.**

  The exploration of low overhead (lightweight) tools for verifying the security of individual components operating from commodity platforms is a distinct need of the industry. Such tools cannot be limited to running against offline test systems; the security stance of the live systems must be available on demand.

- **Tools for secure process control system component development.**

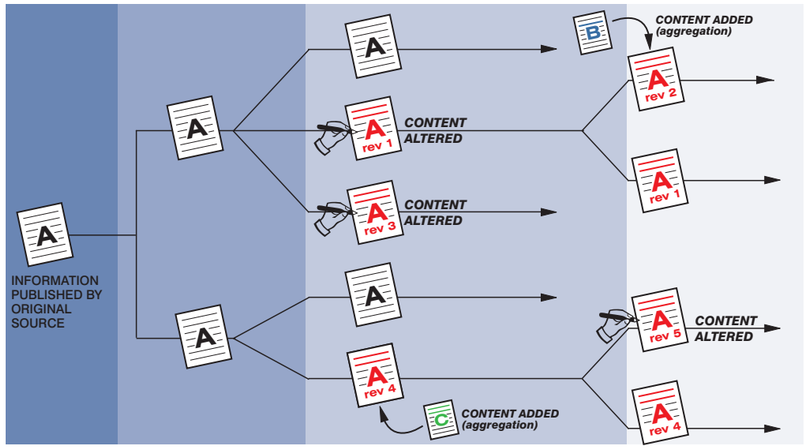
  While tools to enhance the security of software throughout its lifecycle have emerged for enterprise systems, few tools have appeared for process control system software development. The dual requirements of integrity and real-time availability bring new challenges to such tools. Research in secure software development for this environment is clearly needed.

2. DATA PROVENANCE

The origin, or history, of something is known as its provenance. The term comes from the art world, where knowing the provenance of a piece of art, such as its succession of owners, can help authenticate its origin. In the context of computer systems, data provenance immutably documents how data came to be in its current state—where it originated, how it was generated, and the manipulations it has undergone since its creation.

The data that drives process control systems is produced by a variety of sources, ranging from other process control systems down to individual sensors. The number of data sources within a system is growing rapidly and can include aggregations of data from distant sources. In some cases the data sources fall outside a single business and potentially come from an enterprise operating under a different jurisdiction or government. This diversity of data sources poses challenges in the areas of error handling and recovery, source attribution and proof of compliance and legal protection.

Understanding the provenance and, therefore, the trustworthiness of sensor information is vital for a process control system to operate predictably. For example, a control system may be managing a process affected by weather conditions. It would be inefficient for the owner of the control system to invest in technology that duplicates weather information that is readily available from others. Thus, once the dependence on an external data source is established, the provenance of the data provided is important to maintain the secure operation of the control system.



An electronic document can be modified and augmented at various stages, morphing into a product that bears little resemblance and has no direct ties to the original. The inability to trace or recreate this electronic pathway, known as provenance, remains a key problem in the field of information security.

Research and development recommendations:

- **Efficient implementation of provenance in real-time control systems.**

  The constraint of real-time operation makes data provenance for process control systems a hard problem. Further, when data from various sources is merged or processed, a loss of provenance can result. The dependence on the veracity, timeliness, and quality of data from external or vulnerable sources makes this a problem in urgent need of research.

- **Confidentiality and liability issues of provenance data.**

  Since provenance data may include supplier information, trade secrets, or other sensitive information, some industries have been reluctant to use it. Yet regulatory and competitive pressures are motivating its use. Both local and cross-jurisdictional procedures for protecting and regulating this information need to be investigated.

3. METRICS

The availability of a process control system is directly related to its overall security and its ability to recover from a security event. This translates into combinations of security statements about each of the system's components, local or remote, owned or vendor-supplied. Ideally, combining all of these security stances into a single, overarching security score is attractive, but may prove a longstanding problem.

THE CHALLENGES OF ASSESSING SECURITY

Challenging questions for the CIO	Challenging questions for the engineer
■ How much risk am I carrying?	■ Is design A or B more secure?
■ Am I better off now than this time last year?	■ Have I made the appropriate design tradeoff between timeliness, security, privacy, and cost?
■ Am I spending the right amount of money on the right things?	■ How will the system respond to a specific attack scenario?
■ How do I compare to my peers?	■ What is the most critical part of the system to test from a security point of view?
■ What risk transfer options do I have?	

Answers to basic questions, both on the cost-effectiveness side and on the security side, must be found.

In the absence of absolute security measures, an ability to quantify the security of a component or subsystem relative to another is desirable. Relative comparisons would inform choices regarding engineering tradeoffs among real-time response, data reliability, and integrity, and business tradeoffs such as system cost, past performance, and dynamic economic factors. Finally, the ability to perform such assessments would aid the government in evaluating its own progress in improving and maintaining the security of its systems.

Research and development recommendations:

- **Relative security metrics for process control systems.**

  While known to be a hard problem in general, developing techniques and tools to conduct assessments of the relative security of process control components and systems should be pursued.

- **Capabilities for measuring risk dynamically.**

  Most security risk assessment methodologies are lagging indicators that are neither predictive nor responsive to system changes. In order for complex, highly distributed process control systems to operate through security events, research is needed to identify how those systems can dynamically assess their security in the face of temporary outages or component failures.

- **Metrics for product specifications and vendor/operator liability.**

  Vendors have been reluctant to offer product metrics for quality or performance due to concern about potential product liability litigation. Progress in metrics for process control systems can only be leveraged if this concern is addressed. A policy covering process control system providers is needed, perhaps modeled after the *SAFETY Act of 2002*,[4] which provides liability protections to qualified anti-terrorism technology suppliers.

"Stop telling me to buy a secure operating system. Help us secure the ones we have."

[4] The official name of this act is the Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act of 2002.

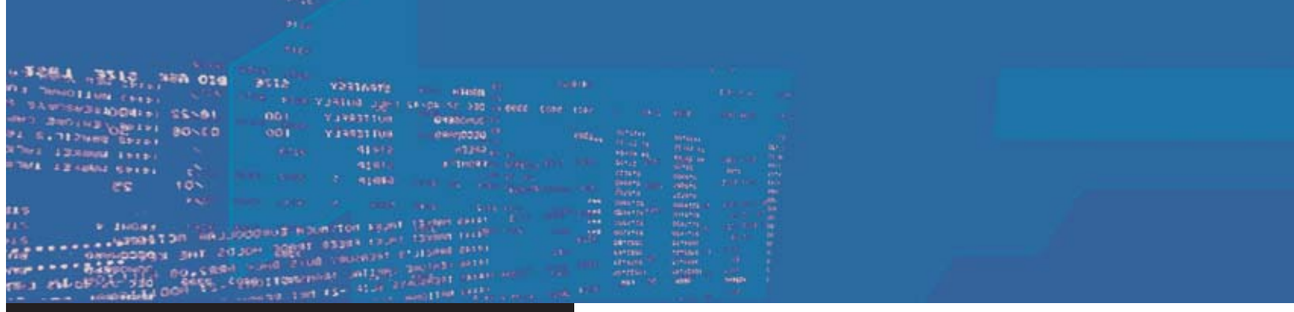
ADDITIONAL RECOMMENDATIONS

- **Security awareness for the process control industry.**

  An observation made several times during the forum was that the process control industry depends on legacy systems that predate modern computer- and network-enhanced control systems. Resistance to updating legacy systems is understandable, given that they are generally working well and the replacement cost is high. Without advocating their wholesale replacement, an educational campaign should be designed to inform system owners, operators, and vendors of the real threats they face, and how they can best determine where they should make security investments. In addition, some form of government acknowledgment should be considered for companies that make verifiable investments in their process control systems' security.

- **Physical provenance for components.**

  In some situations, supply chain vulnerabilities may result in counterfeiting and quality control issues. Counterfeiting poses both a security and an availability problem to the process control industry. Even without intentional malice, many critical control systems are built using components whose physical provenance is not fully known. While a variety of known technical approaches may be employed to verify the legitimacy of a device, component suppliers are currently not required to provide them. Similarly, there are no standards or policies directing owners and operators of critical physical infrastructure components to exercise such verifications even when available. Just as there are accepted standards for validating licensed software, similar schemes for validating process control system components should be investigated.



Human Infrastructure Security

> "Information security is more than an engineering challenge: people are an essential part of the critical infrastructure."

Information security depends not only on technology, but also on the awareness, knowledge, and intentions of the employees, customers, and others using information-based systems and networks.

IT is usually developed based on assumptions not only about need but also about how humans will use the systems and networks provided to them. But humans are prone to mistakes and misunderstandings, are subject to a wide variety of motivations (both good and bad), and experience internal and external stresses, all of which affect their actions. Indeed, humans are often an organization's weakest link for many aspects of security, from forgetting to lock doors to choosing a weak password to acting in counterintuitive or unanticipated ways. Any system's design and operation must address the people who use it or are affected by it. By understanding human aptitudes and attitudes, technologists and policymakers can complement and strengthen the design of an otherwise purely technological or procedural system. Thus, information security is more than an engineering challenge: people are an essential and integral part of the critical infrastructure.

IT is changing both individual and social behavior in ways that have serious implications for information security. The Internet is accessed not only from desktop and laptop computers, but also from personal digital assistants and cell phones. Cell phones are multifunctioned mobile computers, complete with web browsing, access to corporate intranets and email, instant messaging, social networking, cameras, and satellite global positioning

systems. Some applications can provide ground-level pictures of buildings and streets. "Situational awareness" software allows people to track each other's geographical whereabouts moment-by-moment, including taking and broadcasting photos. Such technologies may allow parents to feel more at ease when their children are away from home, but they also offer unsettling possibilities for predatory behavior, privacy breaches, or the orchestration of criminal or terrorist activities.

Online social networking sites can also alter behavior in both good and bad ways, allowing users to build trust and form communities of common interest and concern. For example, people who suffer from the same illness can use specialized medical websites to find emotional support and helpful tips from others in similar circumstances. Sociologists know that the more alike people are, the more they will attract others who are similar—so online social networking technologies can work equally well for support groups or hate groups. Moreover, unwelcome behavior is difficult to detect, track and mitigate; in many situations, online offenders can behave in blatantly illegal ways, with limited likelihood of discovery or punishment. Because criminals often exploit trust to deceive others for financial gain, fraudulent vendors are becoming an increasing problem at otherwise trusted shopping sites. Moreover, innocent people may unintentionally expose their personal information online, creating unexpected risks to themselves and their organizations.

This perception of trust and security can have unintended consequences. Not only are users likely to provide information at a site thought to be trusted or secure, users also may take greater risks, feeling that the system will protect them. For example, users may naively open attachments that harbor a virus or click on links that take them to unknown, potentially dangerous sites. Similarly, people have inherent biases that can lead them to make less-than-acceptable decisions about security.

These considerations—and more—suggest that technologists pay more careful attention to aspects of human behavior when considering solutions to security problems. Attendees of the forum concluded that understanding and addressing human behavior is essential to building a genuine security culture.

SPECIFIC CHALLENGES

Security approaches based only on training programs have proven to be inadequate. Even when employees want to comply with security policies and processes, sometimes they cannot. Cognitive psychologists who study how humans process information have demonstrated that well-intentioned users often ignore or misinterpret important information. For example, humans have an extraordinary ability to focus on what they believe is important; this characteristic enables people to home in quickly on essential elements of a problem, or to deal with emergencies in dangerous surroundings. But the ability to focus has its downside too; people may ignore seemingly irrelevant information and actions, thereby missing important things that should shape the nature of their response. Moreover, initial vigilance declines over time, even with periodic reminders. These human characteristics are not the result of intransigence or ignorance; they reflect inherent human flexibility and adaptiveness.

Information security in the workplace often presents employees with contradictory imperatives. Employees are paid to accomplish specific tasks, and they are evaluated based on their productivity. At the same time, corporate IT wants the organization to be secure. When a security procedure makes employees' jobs more cumbersome, difficult or stressful, they may find ways to work around it—perhaps in ways that make the organization less secure. For example, users who must change passwords frequently may write them on a note attached to the computer. Or, to be more productive, employees may take work home on an untrusted personal portable device. Contradictions may even arise between the corporate boardroom and company IT: the corporation may choose IT equipment based on lowest cost rather than on greatest security.

Workplaces are social environments, and humans are influenced by the social norms of their peers. In other engineering disciplines, operators of hazardous processes are encouraged to embrace a culture that promotes physical safety and security against accidental or intentional breaches. Information security can benefit from these lessons. Moreover, business has learned to harmonize disparate corporate cultures after mergers and acquisitions, suggesting useful principles for creating a security culture. In a culture of casual openness, sharing and helpfulness,

"An organization sensitive to employee motivation and values can use those characteristics in building a true security culture."

the imposition of security may be seen as excess. In a culture of tension and resentment, disgruntled employees may perceive status and fairness inequities. Resulting frustrations may be focused on IT targets, reflecting a mismatch between employee and organizational values and norms. An organization sensitive to employee motivation and values can use those characteristics in building a true security culture.

RESEARCH DIRECTIONS

Social science's findings offer many opportunities to enhance information security. The forum's recommendations for human behavior research and development fall into four major categories: understanding human behavior, incorporating knowledge about human-computer interaction, understanding motivation, and the development of effective educational materials. Each is discussed below:

1. DEVELOP AN EFFECTIVE SECURITY CULTURE THAT INCORPORATES INSIGHTS INTO HUMAN BEHAVIOR

Research and development recommendations:

- **Leveraging knowledge about human decision-making to improve the design and effectiveness of security processes, tools and training.**

  Cognitive psychologists have characterized many important biases that affect individual human decision-making. Security processes, tools and training should be designed to anticipate and accommodate an improved understanding of human behavior.

- **Using trust, empathy, and community to deter and mitigate the actions of predators and criminals and to improve security's effectiveness.**

  Trust, empathy and community have two sides. In certain circumstances, a bad actor is less likely to act against those with whom he/she feels a social bond. At the same time, some bad actors purposely build trust and community to enable their actions. Security processes and tools should take into account an understanding of these tactics.

- **Understanding organizational cultures to support building an effective security culture.**

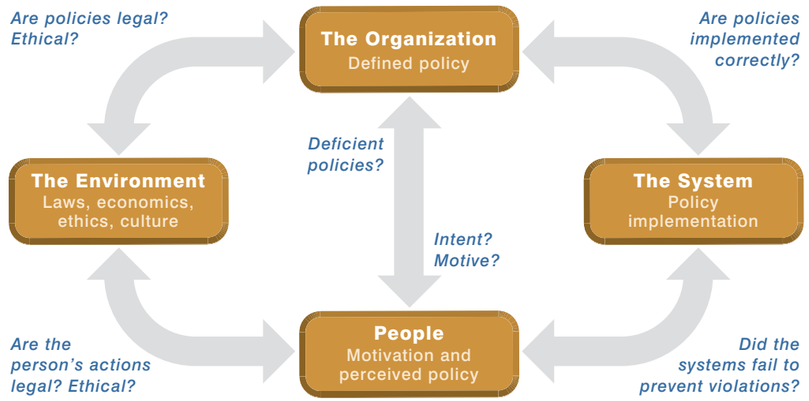
  Desirable norms and a security culture can be supported by technology as well as human processes.

2. UNDERSTAND DEVELOPER AND USER MOTIVATIONS

Research and development recommendations:

- **Understand the characteristics and context of past bad actors.**

  Studies of past bad actors can reveal the roles of four key contributors to a bad action: the organization, the information system, the motivation and intent of the actor, and the legal and ethical context in which the action was taken. A large body of this kind of information can suggest not only the circumstances that enable unwelcome actions but also the policies and technologies that might be effective in preventing or mitigating future bad actions.



Effective security strategies must address a range of non-technical issues, including the organizational environment, corporate policies and employee behavior.[5]

- **Understand the characteristics and context of past victims.**

  Similarly, studies of past victims can reveal the degree to which the organization, the information system, and the legal and ethical context enabled the bad action. A large body of evidence about victims can suggest policies and technologies that might be effective in preventing or mitigating future bad actions.

[5] J. Predd, S. Lawrence Pfleeger, J. Hunker, and C. Bulford, "Insiders Behaving Badly," *IEEE Security and Privacy,* vol. 6, no. 4, 2008, pp. 66-70.

3. UNDERSTAND THE PRINCIPLES OF GOOD HUMAN-COMPUTER INTERACTION TO DESIGN USEFUL SECURITY TECHNOLOGIES

Research and development recommendations:

- **Designing information security for ease of use.**

  Technology alters work flows: "People are not going to use something if it gets in the way of doing their job." Human-computer interaction research can suggest how information security can be made as easy and intuitive as locking a car door. As ease increases, so too should compliance: it should be easier to do the right thing than the wrong one.

- **Tailoring security solutions to users' actual context.**

  Security cannot be one-size-fits-all. Where possible, users should participate in the security-design process to give designers the benefit of user expertise in actual use. Security design must address not only the expected use but also failures and unexpected uses, when technology is compromised or does not work as intended. And user involvement in security technology and policy creation can lead to a bottom-up buy-in security culture.

4. DESIGN CURRICULA AND OUTREACH FOR K-16 EDUCATION

Research and development recommendations:

- **Provide the future workforce with an awareness of and respect for security.**

  Young people now in school are the workforce of tomorrow. Forum participants agreed that security awareness must begin in the earliest grades where youth begin working with computers and cell phones. Simply warning about potential future dangers of certain types of social networking, or getting a child or teen to sign a written contract for online rules of conduct, is virtually meaningless in terms of changing internal beliefs or external actions, especially when peers are engaged in appealing behaviors. Young people need vivid visual demonstrations. Research should be devoted to finding effective ways of educating youth how to protect themselves in cyberspace, empowering them to perform their own risk analyses about the consequences of loss of security and privacy.

Conclusion

Critical information systems drive virtually every aspect of modern life: they manage supply chains for basic consumer goods, control electrical power generation and water purification, provide data to government and law enforcement agencies, run hospital operations and banking transactions, and are essential to most businesses. Though efficient, these systems pose serious security risks that must be addressed as a matter of national security. The importance of doing so cannot be overstated.

Moving toward a more secure information infrastructure will require a concerted and committed effort on multiple fronts, with the government playing a major role in creating and managing an effective national research and development effort. To facilitate the process, participants in the I3P forums identified several research and development priorities for the next five to ten years.

- **A coordinated and collaborative approach is needed.**

  While some agencies strive to coordinate cyber security research and development efforts within their organization, when viewed across all the governmental agencies the chance of duplication, omission, and contradicting directions is all too likely. A national research agenda is urgently needed, with problems prioritized, innovative approaches encouraged and tracked, and a pipeline of short, medium, and long-term projects created.

- **Metrics for security must be developed.**

  Metrics are essential to both the development of new secure systems and to improve and maintain the security of existing systems. Organizations, including the government, cannot make fully informed purchasing and deployment decisions without metrics, which would also give vendors an incentive to make better-designed security tools. Similarly, metrics for security would enable policymakers to devise more effective regulations.

- **An effective legal and policy framework must be created.**

  The current regulatory and legal environment hinders cyber security by imposing overly prescriptive regulations while failing to fill troublesome gaps in the legal and policy framework. A more nimble framework must be created, one that encourages rather than discourages the adoption of secure practices and also incorporates metrics and other objective data.

- **The human dimension of security must be addressed.**

  With insider threat a growing concern, privacy issues increasing, and security features raising compliance challenges, an understanding of human behavior must be integrated into the design of secure computer systems. Ensuring that information security systems are easy to use by non-IT security professionals, for example, is one area needing attention. In addition, awareness raising and educational campaigns directed at the public and private sectors as well as the general public must be developed. At the same time, IT ethics and security training must be built into K-16 curricula to ensure that the next generation becomes a positive force in the quest for better security.

These are hard problems. While solutions to some will be found, other problems will persist and have to be managed on an ongoing basis. Either way, the nation must commit to a long-term collaborative research and development effort that is coordinated across government, industry, and academia.

Participants

Michael J. Ackerman
Assistant Director
National Library of Medicine

Christine Adams
IT Public Policy, The Dow Chemical Company
and Director, Chemical Sector Cyber Security Program

Susan Alexander
Chief Technology Officer
Office of the Deputy Assistant Secretary of Defense for Information and Identity Assurance

Martha F. Austin
Executive Director
The Institute for Information Infrastructure Protection
Dartmouth College

Stewart Baker
Assistant Secretary of Policy
Department of Homeland Security

Nabajyoti Barkakati
Chief Technologist
Government Accountability Office

William Barker
Chief, Computer Security Division
Chief Cyber Security Advisor
Information Technology Laboratory
National Institute of Standards and Technology

Patrick Beggs
Director, CIP Cyber Security Program
National Cyber Security Division
Department of Homeland Security

Deborah Bodeau
Senior Principal Security Engineer
The MITRE Corporation

Deborah A. Boehm-Davis
University Professor & Chair, Psychology Department
George Mason University

Randal Burns
Associate Professor
Whiting School of Engineering
Johns Hopkins University

Alenka Brown-VanHoozer
Senior Research Fellow
Department of Defense

Deanna D. Caputo
Lead Behavioral Psychologist
The MITRE Corporation

John Carlson
Senior Vice President
BITS/Financial Services Roundtable

Jeff Chumbley
Director of Global Information Security
Dell

Benjamin Cook
Principal Member of Technical Staff
Sandia National Laboratories

Eric Cowperthwaite
Chief Information Security Officer
Providence Health and Services

Robert K. Cunningham
Associate Leader
MIT Lincoln Laboratory

Robert C. Davis
Senior Social Research Analyst
RAND Corporation

James Dipasupil
Vice President and Chief Information Security Officer
Technology – Information Security and Compliance
Ameriprise Financial

Donna Dodson
Deputy Chief Cyber Security Advisor
National Institute of Standards and Technology

Thomas Donahue
Director, Cyber Policy
Homeland Security Council

Heather Drinan
Associate Director for Research
Institute for Information Infrastructure Protection
Dartmouth College

Christopher Dunning
Director, Information Security
Staples, Inc.

Mary Erlanger
Director, Global Information Technology Risk Management
Colgate-Palmolive Company

James Euchner
Vice President, Growth Strategy and Innovation
Pitney Bowes

Glenn Fiedelholtz
Network Security Deployment Division
Department of Homeland Security

Ronald Ford
National Cyber Security Division
Department of Homeland Security

Deborah Frincke
Cyber Security Chief Scientist
Pacific Northwest National Laboratory

Cita M. Furlani
Director, Information Technology Laboratory
National Institute of Standards and Technology

John Garing
Chief Information Officer and Director of Strategic Planning and Information
Defense Information Systems Agency

Richard George
Technical Director, Information Assurance Directorate
National Security Agency

Gene H. Gessert
General Manager, Principal
Business Focused Internet Systems

Judith Gordon
Assistant Inspector General for Audit and Evaluation
Department of Commerce

Lawrence A. Gordon
Ernst &Young Alumni Professor of Managerial Accounting and Information Assurance
Robert H. Smith School of Business
University of Maryland

John Grant
Counsel
Senator Susan Collins
Senate Homeland Security and Governmental Affairs Committee

David Alan Grier
Associate Professor of International Affairs
George Washington University

Richard Guida
Vice President, Worldwide Information Security
Johnson & Johnson

Minaxi Gupta
Assistant Professor, Computer Science Department
Indiana University at Bloomington

Rachelle Hollander
Director, Center for Engineering, Ethics, and Society
National Academy of Engineering

Barry Horowitz
Professor and Department Chair
Department of Systems and Information Engineering
University of Virginia

Bob Huba
Product Manager, DeltaV - System Security Architect
Emerson Process Management

Daniel Hurley
Director, Critical Infrastructure Protection
National Telecommunications and Information Administration
Department of Commerce

David J. Icove
Adjunct Assistant Professor
Min H. Kao Department of Electrical and Computer Engineering
The University of Tennessee

Somesh Jha
Associate Professor
Computer Sciences Department
University of Wisconsin

M. Eric Johnson
Professor of Operations Management and Director, Glassmeyer/McNamee Center for Digital Strategies
Tuck School of Business
Dartmouth College

Hank Kenchington
Program Manager
Office of Electricity Delivery and Energy Reliability
Department of Energy

Steven King
Associate Director for Information Assurance
Office of the Deputy Under Secretary of Defense (Science and Technology)

Mischel Kwon
Director of US Computer Emergency Readiness Team
Department of Homeland Security

Carl Landwehr
Program Manager
Intelligence Advanced Research Projects Activity

Robert Laughman
Director, Survivability Evaluation Directorate
US Army Test and Evaluation Command

Insup Lee
Cecilia Fitler Moore Professor, Department of Computer and Information Science
University of Pennsylvania

Richard Lippmann
Senior Staff
MIT Lincoln Laboratory

Martin Loeb
Professor of Accounting and Information Assurance
Robert H. Smith School of Business
University of Maryland

Jack Matejka
Director, IT Security & Compliance
Eaton Corporation

Douglas Maughan
Program Manager, Cyber Security R & D, Science and Technology Directorate
Department of Homeland Security

Patrick McDaniel
Associate Professor, Computer Science and Engineering Department
Pennsylvania State University

Miles McQueen
Principal Investigator
Idaho National Laboratory

Kevin Milliken
Vice President, Information Technology
Staples, Inc.

Ray Musser
Director, Security
General Dynamics Corporation

David Nicol
Professor, Department of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign

Sheldon Ort
Manager Information Technology Enterprise Process, Compliance and Monitoring
Eli Lilly and Company

Charles C. Palmer
Chair and Director for Research
The Institute for Information Infrastructure Protection
Dartmouth College

Mauricio Papa
Associate Professor of Computer Science
University of Tulsa

Deborah Parkinson
Professional Staff Member
Chairman Joseph Lieberman
Senate Homeland Security and Governmental Affairs Committee

Shari Lawrence Pfleeger
Senior Information Scientist
RAND Corporation

Walt Polansky
Supervisory Physicist
Office of Science
Department of Energy

Jennifer Preece
Professor and Dean
College of Information Studies
University of Maryland

Ernest A. Rakaczky
Principal Security Architect, Control System Cyber Security
Invensys Process Systems

Helga Rippen
President
Advisors in Health Information Technology

Charles Romine
Senior Policy Analyst
Office of Science and Technology Policy

David Ryan
Chief Architect, Federal Technology Solution Group
Hewlett Packard Company

Marcus Sachs
Executive Director, Government Affairs, National Security Policy
Verizon

William H. Sanders
Donald Biggar Willett Professor of Engineering
Acting Director, Coordinated Science Laboratory
Director, Information Trust Institute
University of Illinois at Urbana-Champaign

Adam Sedgewick
Professional Staff Member
Chairman Joseph Lieberman
Senate Homeland Security and Governmental Affairs Committee

Tomas P. Seivert
Office of the Director of National Intelligence
Joint Interagency Cyber Task Force

Jeff Sherwood
Manager, Office of the Chief Information Security Officer
H&R Block

Kang Shin
Kevin and Nancy O'Connor Professor of Computer Science
The University of Michigan

Anna Slomovic
Former Chief Privacy Officer
Revolution Health

Paul Smocer
BITS/Financial Services Roundtable

Eugene H. Spafford
Professor of Computer Science
Purdue University

Jeffrey Stanton
Associate Dean for Research and Doctoral Programs
School of Information Studies
Syracuse University

John N. Stewart
Vice President and Chief Security Officer
Cisco Systems, Inc.

Don Stokes
Director, Strategic Technology
Office of the Director of National Intelligence
Joint Interagency Cyber Task Force

Susan Straus
Behavioral Scientist
RAND Corporation

Keith Sturgill
Vice President and Chief Information Officer
Eastman Chemical Company

Rahul Telang
Associate Professor of Information Systems and Management
The Heinz College
Carnegie Mellon University

Roland Trope
Attorney
Trope and Schramm LLP

Zachary Tudor
Program Director, Computer Sciences Laboratory
SRI International

Peter Vold
Director, ACS Advanced Technology
Honeywell International

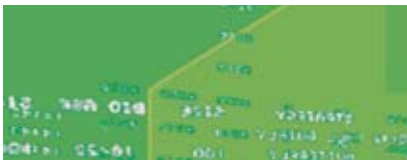
Lee Warren
Chief Information Security Officer
United Technologies Corporation

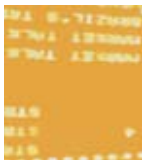
Martin N. Wybourne
Vice Provost for Research
Francis and Mildred Sears Professor of Physics
Dartmouth College

The Institute for Information Infrastructure Protection (I3P) is a national consortium of leading academic institutions, federally-funded labs and non-profit organizations dedicated to strengthening the cyber infrastructure of the United States.

In addition to guiding and supporting research, the I3P is committed to finding solutions to infrastructure vulnerabilities, facilitating technology transfer, and forging collaborative alliances with key stakeholders.

This material is based upon work supported by the U.S. Department of Commerce, National Institute of Standards and Technology, under grant award #60NANB1D0127, under the auspices of the Institute for Information Infrastructure Protection (I3P) research program. The I3P is managed by Dartmouth College. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Commerce, the I3P, or Dartmouth College.





I3P
Institute for Information
Infrastructure Protection

45 Lyme Road, Suite 300
Hanover, NH 03755
www.thei3p.org
603-646-0787