

Executive Summary:

The Cyber-Security Summit

Hosted by Booz Allen Hamilton & Lucent Technologies/Bell Labs

December 11, 2001



Booz | Allen | Hamilton

How would the U.S. population respond to a coordinated cyber-attack on the country's telecommunications and information infrastructure? What would the effect of an attack be on the public at large, and on American business specifically? How can companies assure their own business resilience and mission assurance – and how might the public and private sectors join together to limit the impact of cyber-war?

On December 11 – three months to the day after terrorist attacks in New York City, Washington, D.C., and Pennsylvania alerted Americans to a newly recognized sense of vulnerability – 350 corporate and government chief information officers and other senior executives came together to develop answers to these and other complex issues in information security. They came from such diverse companies and agencies as Amtrak, AT&T, Bell South, the Departments of the Army and Navy, the Department of Energy, the Department of the Interior, the Department of the Treasury, General Motors, Goodyear Tire & Rubber Co., Hewlett Packard, IBM, the Internal Revenue Service, Liberty Mutual, NASA, Northrup Grumman, Sun Microsystems, and Verizon. They represented a range of fields that included banking, telecommunications, high tech, heavy manufacturing, the armed services, and health care.

Sponsored jointly by the international strategy and technology firm Booz Allen Hamilton and Lucent Technologies/Bell Labs, the “Cyber-Security Summit,” held simultaneously in video-linked facilities in Washington, D.C., and Murray Hill, N.J., was the first major conference to draw together top information officials from business and government to discuss the ongoing security of the nation's information infrastructure.

The gravity of the challenge was underscored by keynote speaker **Richard Clarke**, Chair of the President's Critical Infrastructure Protection Board and

Special Advisor to the President for CyberSpace Security. “Our national defense is dependent on IT infrastructures,” Mr. Clarke told the audience. “Our national economy is dependent on IT networks and systems. There is no way to go back to the previous economy. This is like Cortez landing in the New World and burning his ships. We’ve burned our typewriters. We are all of us dependent for our existence – dependent for making money, and doing the work of the government – on IT networks.

During the course of a lively dialogue, the Fortune 1000 executives and senior government officials reached a remarkable degree of consensus around common themes:

- Adequate information network defenses are essential to business continuity and national security.
- Technology can strengthen cyber-security, but it must be accompanied by appropriate organizational policies and practices to be effective.
- Customers must demand greater security from software vendors and service providers.
- Infosec solutions must cut across functional silos within organizations.
- Cyber-security requires organizations to breach the walls and misunderstandings that often divide the public and private sectors.

The latter theme was emphasized time and again during the Summit. “We realize together that we have an immense challenge ahead of us,” said Bill O’Shea, Lucent executive vice president and president of Bell Labs, in opening the day-long meeting. “Day in and day out, we hear reports of denial-of-service attacks, and hacker intrusions. These are mounting evidence of the need for a unified response.”

Recalling President Franklin D. Roosevelt’s Depression-era reminder that we rise or fall as one people, Booz Allen Chairman and Chief Executive Officer Ralph W. Shrader told attendees, “One of the great differences between our world in 2001 – and FDR’s world when he said this in 1937 – is our information infrastructure. It is an awesome force for unity and progress – and as we all know, its very power and essence makes it vulnerable.”

Following is a summary of the proceedings of the Cyber-Security Summit.

Opening remarks by Messers. Shrader and O'Shea as well as by MC Mark Gerencser, Booz Allen Hamilton Vice President and Co-Leader of the firm's Global Strategic Security initiative, provided the broad framework for the session. Keynote speakers included:

- Jeff Jaffe, President, Bell Labs
- Bill Joy, Chief Scientist and Co-Founder, Sun Microsystems
- Mike McConnell, Vice President, Booz Allen Hamilton, and former director, the National Security Agency
- Richard Clarke, Chair of the President's Critical Infrastructure Protection Board and Special Advisor to the President for CyberSpace Security

Panel discussions on how technology can strengthen business security and Panelists included Martin M. (John) Atalla, chairman, TriStrata Inc.; Abel Ebeid, chief technology officer, state of New Jersey; Avi Freedman, vice president/network architect, Akamai Technologies; Sam Halim, chief information officer, ABN Amro North America; Bill Howard, chief information officer, Sun Microsystems; Chuck Lucier, senior vice president/chief growth officer, Booz Allen Hamilton; Elizabeth Primrose-Smith, vice-president for global security solutions, International Business Machines Corporation; John Reese, chief information officer, Internal Revenue Service; Lt. General Jack Woodward, chief information officer for the U.S. Air Force; and Larry Wolfe, Chief Information Officer, National Institutes of Allergy & Infectious Diseases.

Lunch featured roundtable discussions, with facilitators from Booz Allen Hamilton and Lucent. Topics included: Automated Access Management; Broadband Security; Common Exploits and Vulnerabilities; Cyber-Security Program Issues for the Enterprise; Disaster Recovery and Business Continuity; Disaster Recovery and Network Reliability; Emergency Management Planning; Internal Firewalls; Network Security; Personnel Issues Impact on Cyber-Security; Physical Security Issues; Privacy Issues in Government; Privacy Issues in the Private Sector; Risk Management; Security Architectures and Web Security; Transforming Security Policy to IT Infrastructure; VPNs and IPSEC; and Virus/malicious code/worms.

Keynote:

“Security Technology”

Jeff Jaffe

President

Bell Labs Research

The September 11 attacks and the anthrax-laden letters that followed have awakened America to its vulnerability and prompted a nation-wide review of common security practices. While cyber-attacks have grown exponentially in frequency, severity, and cost, they have until recently not received a commensurate degree of attention. Leaders in government and industry have now recognized this insidious threat and say it must be met before the kind of catastrophic event occurs that could claim lives or paralyze the economy.

As Mark Gerencser of Booz Allen observed, “this is exactly the right time to get the public and private sectors to dialog on the problem.”

In the first keynote of the day, Jeff Jaffe, president of Bell Labs Research, advised leaders to concentrate less on short-term security concerns, and more on the future of information networks and the different security issues new technologies will create. He suggested that the shift to optical networking will embed more security into information systems than currently exists.

Mr. Jaffe, who has led research teams at Bell Labs and IBM in developing networking and security software, criticized industry and government executives for what he said was a dilatory approach to cyber-security. “We find it difficult to stay focused on cyber-security,” he said. “We’ve talked about it for years, but a lot of what we do is talk. We have to get past the talk, past conversations and imperatives and get to action.”

Such action, he suggested, would yield real results, and rapidly. Industry’s mobilization to solve the “Y2K bug” showed the effectiveness inherent when organizations create a “culture” of cyber-security. “Once you have the culture, a lot of the technology is there already,” Mr. Jaffe said.

Although some years away from deployment, all-optical networks will eliminate some of the security weaknesses of today's copper-wire, switched infrastructure, Mr. Jaffe said. These networks will be installed first by major telecommunications service providers, and will then rapidly move to the enterprise. But the tremendous speed and bandwidth offered by optical data transmission also will create new challenges for firewall technology and require new types of cyber-security. In the question and answer period that followed, Mr. Jaffe was asked how to enhance security of the existing infrastructure. "The biggest weakness we have in securing networks is the lack of focus on it," he said. "The year 2000 problem was an incredible example of how when we focus on a problem, we solve it. We licked that problem and there were almost no negative consequences. We have nowhere near that level of attention on security. The question is how to create a culture of security. Once you have the culture, a lot of the technology is there already."

Panel Discussion:

“Using Technology to Strengthen Business Security”

Moderator:

Chuck Lucier, senior vice president/chief growth officer, Booz Allen Hamilton

Panelists:

Martin M. (John) Atalla, chairman, TriStrata Inc.; Avi Freedman, Vice President/Network Architect, Akamai Technologies; Bill Howard, Chief Information Officer, Sun Microsystems, Inc.; Larry Wolfe, Chief Information Officer, National Institutes of Allergy & Infectious Diseases.

The Cyber-Security Summit’s first panel of senior information executives and officials picked up on the theme of a security culture, and drove home the point that for many organizations, security can be vastly improved by taking simple practices and making them a standard part of the institution’s policies. Embedding information security in the fabric of the organization will render current measures, such as secure IDs, encryption and firewalls, far more effective, panelists said.

For many companies, a first step is creating a standard directory governing who within their organization can access what parts of their network, said Bill Howard, Sun Microsystems’ chief information officer. With databases and network points-of-entry proliferating, most companies have lagged in standardizing access privileges. As companies’ value webs grow more extended, an access directory is a core component of any organization’s information security program, he suggested.

“This is all about having access based on the role you have,” said Mr. Howard, whose company is the world’s leading provider of Unix-based workstations and servers. “Your privileges are based on that. Understand who the person is, and what privileges they have, so they can access things inside your network. At any given time, anyone from outside the network needs to get access inside, so getting this directory in place is key. The

challenge is to get a meta-directory so this role-based access policy can be implemented globally.”

Martin M. (John) Atalla, chairman of TriStrata, which produces secure systems for application service providers (ASPs), and the inventor of the technology that secures 80 percent of all ATMs worldwide, supported the recommendation for role-based access controls. “Very rarely do you find penetration of a network is due to a weakness in cryptography,” said Mr. Atalla, who is widely regarded as the father of the automatic teller machine. “It is not the fixes, it is the management.”

Maintaining security requires three simple components, Mr. Atalla said. Robust encryption must protect all information at all times; controls must determine how to access that information and who can access it; and an audit trail should be created to trace what happens and how. “If you have those three things, you have the problem solved,” he said.

Central policies and policies can only go so far, however. Attacks can occur anywhere on the network, several panelists noted, so the implementation of security must be distributed.

“Compartmentalization is a really vital way to handle the problems,” said Larry Wolfe, chief information officer for the National Institutes of Allergy & Infectious Diseases, a division of the National Institutes of Health. “Centralization is important, but when you get down to it, the people who need to respond are right on the front lines.” When the Nimda virus struck, “our people were able to respond because we had compartmentalization, and they were able to respond immediately,” he said.

Indeed, the organization’s people are at least as important as any policies or programs in implementing information assurance, panelists agreed. Akamai Technologies, a company specializing in speeding Internet content delivery, actually pits its researchers against each other to find – and solve – network vulnerabilities, offering bonuses to those who find security holes in vendors’ software products. “One of the things Akamai has seen as a constant is people really are key,” said Avi Freedman, vice president and network

architect for Akamai Technologies. “Designing architecture in saves a tremendous amount of time versus doing Band-Aids after the fact. We have smart people and put them in competitive situations.”

But this means that the people who come on board through acquisitions must be carefully scrutinized, Mr. Freedman added. “Bring your technologists in and try to have a general white-board conversation about things that should be of interest. If they just sit there staring, fire them.”

The question and answer session focused on matters of cost, how to define an acceptable level of security, and how to calculate a return on investment for security measures. How to get employees to support a security framework, and how to extend that framework to mobile users, were also topics of lively discussion.

Keynote:

Bill Joy
Chief Scientist and Co-Founder
Sun Microsystems

“I’ve spent most of my time in the last 25 years working on simple, reliable information technologies,” said Bill Joy, co-founder and chief scientist of Sun Microsystems, Inc. “Despite 25 years of work in this area, I think it’s not really news we don’t have very much security in our systems today. We’ve just had the nth teenage hacker attack. It’s just stupid. So I think it’s fair to ask how did we get here?”

A legendary technology guru – he was the principle designer of Berkeley Unix, which brought the concept of networking using TCP/IP to the Unix operating system originally created at Bell Labs – Mr. Joy in recent years also has played a public policy role. He has written and spoken extensively about the potential dangers and ethical issues inherent in the development of 21st century sciences and technologies. Throughout his career, he said, security has been among his major concerns.

Many vulnerabilities arise from common software industry practices, such as writing code in high-level programming languages with inadequate provision for testing and detecting bugs, Mr. Joy said. Although he singled out the Microsoft Corporation’s Windows operating systems – with its millions of lines of unpublished code – as particular repositories of bugs and security holes, he said the whole industry is guilty of shipping unfinished products and leaving customers vulnerable to their flaws. These cascading vulnerabilities create a defective virtual ecology, Mr. Joy said, in which software programs are not redundant or diverse enough to resist attacks.

Just as the Federal government sets fuel standards for automobiles, it could set security standards for software, at least for its own purchase, Mr. Joy recommended. He also supported government backing for the development of all-optical networks, which replace today’s switches and shared copper wires, with dedicated fiber optic cables, which provide an end to end

conduit. Only this technology can prevent denial of service attacks, a crude but effective hacker attack, which paralyzes a network simply by flooding the circuits with superfluous traffic, he said..

“With all these problems, I still believe there is opportunity,” Mr. Joy said. “The properties we want our systems to have will not occur by accident. We have to decide what we want and put our money where our mouths are. It’s going to be expensive and it’s not going to be easy, but it is important,” he said.

Keynote

“Business Resilience”

Mike McConnell

Vice President, Booz Allen Hamilton; former director, National Security Agency

Stepping back from the intimate, software-based perspective, Booz Allen Vice President Mike McConnell, the former director of the U.S. National Security Agency, viewed the dilemma of cyber-security from a geopolitical perspective. He reminded the meeting attendees that although the Cold War was a time of terrible threats, it also marked an era of peace, stability and prosperity. Security, in such an environment, was the province of the military, and companies could concentrate on doing business. “Now we live in a world where industry is the target, and the enemy lives among us,” Mr. McConnell said. “Because industry owns and operates the targets we need to think differently about security for the future. The business continuity baseline challenge has changed.”

This is not a new threat, although the temptation is to view it as one, Mr. McConnell said. “For those of us that were Cold War warriors, history did not end with the fall of the Soviet Union. A counterpoint to that is that history did not start on the 11th of September. The 11th of September, however, did get us focused and... galvanized [us] so that we’re going to look at, think about, and adapt to threats in the future.”

Massive networking has made the U.S. and its companies the world’s most vulnerable target for information attack – activities that could include outright theft of intelligence; exploitation of sensitive data; disruption of a firm’s network infrastructure; or destruction of valuable data, Mr. McConnell said.

“It really is a different world,” Mr. McConnell said. “There are new threats now that live among us, and I’m going to advocate a new way to think about security, internal and external. As much as 75 to 80 percent of the problems for business today, particularly in a cyber-context, are internal not external. I

also advocate a stronger partnership between industry and Government to solve these problems. I don't think either side can solve them alone." Because the United States has led the world in the creation and adoption of information technology, it has significantly more to lose to information attack than other countries.

"What's different today is the value of networked information has gone up significantly," Mr. McConnell said. Information "is us, it's what the country does and relies on. I like to use the example of banking. There isn't enough money in the bank for us to go take out what we have stored in the bank. It's not in gold, its not printed, so if we tried to withdraw we'd have a banking crisis. What's in the bank is an accounting system, electronic entry. The value of that has increased significantly and it would similarly be true across any industry today for the value of the information that's moved around the internet.

Cyber-vulnerability likewise has increased significantly, Mr. McConnell added. "The risk and the potential from cyber-attacks has increased dramatically." Because public and private infrastructure are increasingly one and the same, protecting the system from cyber-attacks is a shared responsibility between business and government.

"There is a new awareness that business security is critical to national security," Mr. McConnell said. "We are going to cooperate and integrate across boundaries that have not engaged in much cooperation in the past. Risk is stovepiped by nature, but security requires a cross-cutting solution. Business must adopt a strategic view of the operating, financial, and information issues," he said.

Adopting a strategic view means integrating security across all the managers in an organization. It also means integrating physical security with personnel security – both safeguarding the organization's people, vetting those people vigorously, and tying both together with cyber-security. It means that security must now clearly be on the CEO's agenda.

“Security is so important it can no longer be delegated,” Mr. McConnell said. “CEOs traditionally delegate things they don’t have expertise in or they don’t have the time to get to. This is one thing that has to be internalized at the CEO level. The private sector owns and operates what we all depend on. We rely on this global infrastructure and the private sector must assume a new role for risk control to maintain what makes us so strong: Openness on the one hand and economic growth on the other combined with the right level of security to be able to protect both.”

The payoff for taking a strategic approach to security is, “the business enterprise becomes better positioned for continuity and growth,” Mr. McConnell said. “I believe and I would hope that with this kind of approach you would achieve new levels of trust and collaboration.”

Mr. McConnell concluded, “Senior leadership is going to have to build security into the organization because the threats live among us. Security was effectively outsourced during the Cold War while the military held the threat at bay. With the threat among us, you can’t leave it to government to get it right. If you do, you won’t like the result.”

Panel Discussion:

“Placing Cyber-Security at the Top of the CEO Agenda”

Moderator: Chuck Lucier

Panelists:

Abel Ebeid, chief technology officer, state of New Jersey; Sam Halin, chief information officer, ABN Amro North America; Elizabeth Primrose-Smith, vice-president for global security solutions, International Business Machines Corporation; John Reese, chief information officer, Internal Revenue Service; Lt. General Jack Woodward, chief information officer for the U.S. Air Force.

CIOs from a variety of public- and private-sector backgrounds agreed with Mr. McConnell that cyber-security must become a CEO concern. When security meant little more than badges and gate guards, chief executives could (and did) delegate it to subordinates. Cyber-security was the responsibility of the IT staff. But in today’s networked world, with new threats manifest, security is a strategic issue. Decisions now must be made at the highest levels of an organization. The threat of devastating cyber-attacks means there is a greater need than ever for dialogue between CEOs and CIOs.

“For years and years I used to beat on the CEO and say, ‘We need security,’” said John Reese, chief information officer for the Internal Revenue Service and a former CIO for Time Warner Inc. Too often, security needs would conflict with budget priorities, he said. “The greatest antidote to that scenario is fear,” he said, adding that he believes chief executives will be increasingly called to account by board members and shareholders if their security processes are not adequate. “You have to start with an assessment. At the end of the day it’s a question of what does the business have to have to protect it. Awareness is often 90 percent of the battle.”

New Jersey’s chief technology officer raised security awareness by demonstrating its systems’ vulnerability to intrusion. “We went out and

secured a vendor to do ‘war dialing,’” said Abel Ebeid. “Hack in wherever you can and let us know where we’re vulnerable. We’ve used those reports to concentrate where we spend our dollars. It was a call to action, a way to get to the 16 managers who run the state of New Jersey and really educate them about how we’re vulnerable. We were able to educate the governor and treasury that it’s really okay to fund projects based on what-if scenarios. Due to 9/11, they’re more open to those ideas,” he said.

IBM has long offered what it calls “ethical hacking,” to test security systems, and has seen a spike in demand since September 11. “It was a call for action for many of our customers,” said Elizabeth Primrose-Smith, IBM’s vice-president for Global Security Solutions. “Data security and IT operations have always been on our customers’ list, but maybe third or fourth. Now, they have leapfrogged to number one,” she added. “You need to start out with an assessment of your abilities, really set up and understand what is going on in your enterprise. Security is not just something to pay attention to because there are threats on the horizon. It is really something a prudent enterprise must do to assess their readiness,” she said.

Banks are on the front lines of the cyber-wars every day, but banks have also been among the most proactive adopters of robust security and business continuity planning. As a result, even banks operating in the World Trade Center and surrounding area, were able to transfer employees and maintain operations relatively transparently.

“We’ve been able to move our people to Long Island. We’ve been able to operate despite what happened,” said Sam Halim, chief information officer for ABN Amro North America. “Security is a lot of common sense. We collected all the business units together, with IT, and we created a group to focus on what is the business vulnerability. What happens if one of the buildings goes down? What happens if one of the networks goes off? What is the worst-case scenario?” he said.

For the military, the worst-case scenario is an intrusion that compromises a mission or the safety of personnel, and some cyber-attacks have come very close. “We’ve been at cyberwar for a pretty good period of time now,” said

Lt. General Jack Woodward, chief information officer for the U.S. Air Force. “My lack of sleep and worst nightmare is a cyber-event that causes loss of life. Let’s go to the air war in Kosovo: individual’s names, rank and where they were located were placed on a report, associated with certain types of aircraft and certain types of bombs. They were attacked as families here in the U.S. from a cyber-standpoint because that information was available,” he said.

Keynote:

Richard Clarke

Chair of the President's Critical Infrastructure Protection Board and Special Advisor to the President for CyberSpace Security

President Bush's creation of a board to address infrastructure protection and appointment of a new advisor on cyber-security reflect the recognition of our nation's dependence on information technology systems – not to mention the rapidly multiplying threats to those systems. Richard Clarke, a career member of the Senior Executive Service, was appointed by National Security Advisor Condoleezza Rice and Director of Homeland Security Governor Tom Ridge.

Asked by President Bush to draft a National Cyber-Security Strategy, Mr. Clarke said he has turned to industry, academia and individuals for their input, and encouraged the members of the audience to share their own cyber-security ideas with him. He hopes to complete the strategy by the spring.

“Our future enemies will use our technology against us,” Mr. Clarke said. “Just as Al-Qaeda used 767s, transforming them into effective missiles, our future enemies will turn our technology against us. And they will understand it as well as we do. When they look for weakness they will find it. Our enemies will look for the cracks, the fissures, the weaknesses that we know are there. Some of the reconnaissance activities on our networks every day is by our future enemies,” he said.

The government will help, through research spending, new education initiatives and by sharing information about threats in a timely way, Mr. Clarke said. But industry has a responsibility as well: to create a culture of security by using the tools that are available; by demanding secure products and services from software vendors and Internet service providers; and by spending much more on cyber-security than it does now. He cited a Forrester Research report that the average company's expenditure on cyber-security is, “.0025 of revenue, a little bit less than most companies spend on coffee.

If that's what your priority is, don't come complaining to me when you get hacked. Freedom isn't free."

In closing, Mr. Clarke admonished leaders not to draw analogies from past experiences, because the future will be different and unexpected.

"Look at our risk not from the past but by looking at our vulnerabilities and imagining what would be the worst case," Mr. Clarke said. "That's the way to look at our IT vulnerabilities. Not by what Nimda and Code Red did in the past, but what could somebody do to your company, what somebody could do to our national defense by a smart coordinated attack on our IT infrastructure. Because, as September 11 proved, sometimes worst-case scenarios actually do happen."