

Protect Your Enterprise with Secure and Resilient Information Flow

Keynote Presentation

Robert F. Brammer, Ph.D.

Vice President and Chief Technology Officer

Northrop Grumman Information Systems



Aerospace and Defense Cybersecurity Forum

March 31-April 1, 2010

Hyatt Regency Washington Capitol Hill

Washington, D.C.

Protect Your Enterprise with Secure and Resilient Information Flow

Introduction

Good morning,

I want to thank Aviation Week for organizing this event. The theme of this Forum is “Protect Your Enterprise with Secure and Resilient Information Flow.” This is certainly a timely and important subject. I know a number of the outstanding people on the program today, and I am sure that this will be a very successful forum for the exchange of information about protecting your enterprises from cyber threats.

Any keynote speaker wonders how to start his presentation. I give talks all over the world, and I have always been impressed with the cultural differences in giving speeches. For example, in the US it is customary to begin a speech with a joke. In Japan, it is customary to begin a speech with an apology. Cybersecurity is not a subject for which I have been successful in thinking of jokes. However, since cybersecurity is a global issue, it is reasonable to combine these perspectives. Therefore, I am going to begin this speech by apologizing for not telling a joke.

There are a few key points that I would like you to get from this presentation. First, enterprise systems and services are increasing very rapidly in size, geographic distribution, functionality, and most notably in value. In this presentation, I will use the term “enterprise” broadly to include corporations, government agencies, universities, and any other significant information-intensive organization. I will also include both IT networks as well as infrastructure networks like power grids and oil pipelines in talking about these examples. There are very significant differences between IT networks and infrastructure networks, but they have in common both significant value and vulnerability to cyber attacks. The designs of many of these newer enterprise systems contain new architectures, standards, and products for good business reasons – increasing business value, improved service, functionality, reliability, etc. However, those new developments also make them increasingly valuable targets.

Second, these cybersecurity threats are increasing rapidly in sophistication, breadth, and speed. Those of us who have been in this business for a large number of years have seen the incidents go from defaced websites to theft of large volumes of intellectual property and money, military actions, and so forth. Notable among these threats is the “Advanced Persistent Threat.” In the cybersecurity context, this phrase refers to the systematic cyber targeting of significant government and industry organizations in order to obtain sensitive information in many areas such as advanced R&D, financial services, critical infrastructure, national security, and others. I will discuss these threats further in this presentation.

Third, cybersecurity is a very difficult subject for several reasons. We will discuss some of the important reasons for this and the implications that lead to the conclusion that the cyber protection of a large enterprise requires a multidimensional strategy. At Northrop Grumman, our approach includes a multi-layer architecture, including documented policies and processes, a well-trained cybersecurity staff, integrated technology suites, specialized facilities, advanced research, education and training, and

professional activity leadership. I will discuss our approach to cybersecurity operations further later in this presentation.

Finally, protecting the large enterprise cannot be accomplished simply with short-term fixes like changing passwords and patching systems more quickly, although those steps do help somewhat. Today's cyber threats are far too sophisticated. Moreover, they are increasing rapidly in number and in capability. Cybersecurity is a long-term issue and requires a strategic approach for the enterprise.

The Growth of Enterprise Information Systems and Services

The growth of the Internet has been astounding. In a period of about 15 years, the Internet has grown from essentially zero users to nearly two billion users around the world¹. E-commerce on the Internet is growing also. Forrester Research estimates that e-commerce grew 11% last year in the United States in a period of recession. Forrester forecasts online retail sales in the U.S. will be nearly \$250 billion by 2014, up from \$155 billion in 2009. Last year, online retail sales were up 11%, compared to 2.5% growth for all retail sales². EMC estimates that the world's information systems have created more than 223 exabytes of digital information since January³. Americans continue to consume larger volumes of information. "Consumption totaled 3.6 zettabytes and 10,845 trillion words, corresponding to 100,500 words and 34 gigabytes for an average person on an average day."⁴ These numbers indicate the growth and value of information in large-scale information systems. (An exabyte is 10^{18} bytes (i.e., a billion gigabytes) and a zettabyte is 10^{21} bytes, (i.e., a thousand exabytes).)

The mobility of this information is also increasing rapidly. Cisco Systems does a very good job of calculating what they call their Visual Networking Index⁵. The data presented on this website show the rapid growth of Internet traffic. Global IP traffic will increase by a factor of three from 2010 to 2013, approaching 56 exabytes per month in 2013, compared to approximately nine exabytes per month in 2008. By 2013, annual global IP traffic will reach two-thirds of a zettabyte. By 2013, the various forms of video (TV, Video on Demand, Internet Video, and peer-to-peer video) will exceed 90% of global consumer traffic. By 2013, global online video will be 60% of consumer Internet traffic (up from 35% in 2010). Mobile data traffic will roughly double each year from 2010 through 2013. The importance of mobile computing brings a new dimension to the field of cybersecurity. The growth of networking is also indicative of the value of information and presents many additional cybersecurity challenges.

New information architectures are also significant in the development of large-scale information systems and services. Web 2.0, cloud computing, green IT, mobile computing, optical networking, and unified computing are all quickly developing and present many capabilities for new functionality, higher performance, and lower costs. Many large-scale enterprises have significant developments that adapt

¹ <http://www.internetworldstats.com/>

² Forrester Research Web-Influenced Retail Sales Forecast 12/09

³ www.emc.com/digitaluniverse

⁴ How Much Information? 2009 Report on American Consumers, Global Information Industry Center University of California, San Diego, January 2010

⁵ <http://www.ciscovni.com/index.htm>

or plan to adapt these new architectures to major operational systems. However, these new architectures also have various cybersecurity vulnerabilities that we will discuss.

Infrastructure networks such as electric power grids, oil and natural gas pipelines, and transportation networks are major parts of our national critical infrastructure and key resources, as discussed in the National Infrastructure Protection Plan⁶. These networks differ in many essential ways from IT networks. For example, the nodes of these networks may be objects like power generators and subway terminals and not just servers and routers. The traffic that they carry includes electric power and natural gas and not just digital bit streams. The differences between infrastructure and IT networks lead to significantly different approaches for securing them. We will discuss some of these differences later in this presentation. However, Weiss⁷ summarizes the difference in design priorities well.

“There is a significant difference between the security philosophies of enterprise IT and ICS (infrastructure control systems). The purpose of enterprise security is to protect the data residing in the servers from attack. The purpose of ICS security is to protect the ability of the facility to safely and securely operate, regardless of what may befall the rest of the network.”

In decades past, these infrastructure networks were physically and logically separate from enterprise IT networks. During that time, these infrastructure networks were not designed to protect against cyber threats. However, in the past several years, there has been a significant convergence or integration of these networks. There are many good business reasons for this convergence, including the integration of operational data from the infrastructure networks with customer and financial information from the IT networks. However, this convergence can also create some new types of security vulnerabilities.^{7 8}

A particularly important example of this type of convergence is the Smart Grid. The Smart Grid concept includes significant integration of Internet technologies with electric power generation, transmission, distribution, and end-user applications⁹. Potential Smart Grid benefits include lower costs, higher efficiency, and positive environmental impacts. However, there are many potential security and privacy issues to be resolved. The National Institute for Standards and Technology is leading a significant effort to define Smart Grid standards, including cybersecurity standards¹⁰.

So far, we have discussed the significant and continuing growth of enterprise systems and services in terms of functionality and value. We have also described some aspects of new cybersecurity

⁶ National Infrastructure Protection Plan, US Department of Homeland Security, 2009

⁷ Weiss, J., “Control Systems Cyber Security—The Current Status of Cyber Security of Critical Infrastructures”, Testimony before the Committee on Commerce, Science, and Transportation, U.S. Senate, March 19, 2009

⁸ Pires, P. and Oliveira, L., “Security Aspects of SCADA and Corporate Network Interconnection: An Overview”, Proceedings of the International Conference on Dependability of Computer Systems, Institute of Electrical and Electronics Engineers, 2006

⁹ The Smart Grid: An Introduction, US Department of Energy, 2008

¹⁰ www.nist.gov/smartgrid

risks resulting from the introduction of immature technologies and protocols as well as the lack of traditional emphasis on cybersecurity. Now we will describe some major cybersecurity threats.

Threats to the enterprise

In the past two years, there has been an increasing recognition at the highest levels of the US government about the seriousness of the cybersecurity threats.

In May of last year, President Obama, in announcing the results of the White House Cyberspace Review¹¹, said¹²

“... it's now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation.

It's also clear that we're not as prepared as we should be, as a government or as a country. In recent years, some progress has been made at the federal level. But just as we failed in the past to invest in our physical infrastructure -- our roads, our bridges and rails -- we've failed to invest in the security of our digital infrastructure.”

In February, Dennis Blair, Director of National Intelligence, in testimony¹³ before the Senate said

“The national security of the United States, our economic prosperity, and the daily functioning of our government are dependent on a dynamic public and private information infrastructure, which includes telecommunications, computer networks and systems, and the information residing within. This critical infrastructure is severely threatened.”

What are the primary threats? I will discuss three major categories. They have some important differences in terms of the intentions and methods of the “bad guys.” However, they also have some overlap and have a common characteristic of becoming much more specifically targeted than were many threats like worms and viruses of previous years.

I think that the most significant threat is that of cyberespionage and the theft of intellectual property. This encompasses much of the Advanced Persistent Threat mentioned earlier. There have been several reports of such incidents in the news media that show that such incidents occur in many industries, including aerospace and defense, financial services, manufacturing, and others. The White House Cyberspace Policy Review noted, “Industry estimates of losses from intellectual property to data theft in 2008 range as high as \$1 trillion.”

¹¹ The White House, “Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure,” May 29, 2009

¹² The White House, “Remarks By The President On Securing Our Nation's Cyber Infrastructure”, May 29, 2009

¹³ Blair, D. “Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence,” February 2, 2010

The Christian Science Monitor reported in January one example of an incident that affected three major oil companies. The article described the cyber theft of one of the crown jewels of the industry: valuable “bid data” detailing the quantity, value, and location of oil discoveries worldwide.¹⁴ The Wall Street Journal reported another example in February. In this case, “Hackers in Europe and China successfully broke into computers at nearly 2,500 companies and government agencies over the last 18 months in a coordinated global attack that exposed vast amounts of personal and corporate secrets to theft.”¹⁵

In a very widely reported incident, cyber intruders stole software and other intellectual property, including information about human rights activists, from Google in China. Named “Operation Aurora,” this very serious breach has led to Google’s reconsidering its approach to China. The analysis of this incident has also led to, among many other things, an analysis of the vulnerabilities of software configuration management processes and tools¹⁶.

Vulnerabilities in software management are particularly serious. In addition to the intellectual property value of the software, there is also the risk of malware (i.e., malicious software) implants that could be very difficult to detect and that could lead to continuing information breaches, financial losses, and system and service malfunctions.

A second serious threat is that of other types of Internet crime. These include non-delivered merchandise and/or payment, identity theft, credit card fraud, auction fraud, and computer fraud (destruction/damage/vandalism of property). The Internet Crime Complaint Center, led by the Justice Department, reported in March that the monetary losses from incidents reported to the center in 2009 were \$560M. This level was more than a 100% increase from the reported 2008 value of \$260M.¹⁷

A third type of threat is cyberwarfare. In these cases, attackers use cyber technologies to cause significant damage or destruction to national operations. In addition to government facilities and systems, significant cyberwarfare would have significant effects on US critical infrastructure systems and operations. Cyber attacks can be coordinated with physical or kinetic attacks to achieve military objectives. Cyber pre-attacks could provide information for targeting through espionage and disseminate disinformation. Real-time cyber attacks combined with physical attacks can suppress communications and emergency response capabilities. Cyber post-attacks can target backup and recovery processes and systems.

¹⁴ Christian Science Monitor, “US Oil Industry Hit by Cyberattacks: Was China Involved?”, January 25, 2010

¹⁵ Wall Street Journal, “Broad New Hacking Attack Detected Global Offensive Snagged Corporate, Personal Data at Nearly 2,500 Companies,” February 18, 2010

¹⁶ McAfee Corporation, “Protecting Your Critical Assets: Lessons Learned from “Operation Aurora”, March 3, 2010

¹⁷ Internet Crime Complaint Center, “2009 Internet Crime Report,” March 2010

These are no longer just theoretical possibilities. The Russian-Georgian conflict in 2008 demonstrated many of these characteristics. A recent report¹⁸ from the Cooperative Cyber Defence Center of Excellence in Tallinn, Estonia said

“Before the Russian invasion into Georgia commenced, cyber attacks were already being launched against a large number of Georgian governmental websites, making it among the first cases in which an international political and military conflict was accompanied – or even preceded – by a coordinated cyber offensive.”

It seems very likely that cyber attacks coordinated with physical attacks will become a very common concept of operations for many future military conflicts. Earlier this month, a senior NATO official said, “Future hostilities will begin with cyberattacks¹⁹.”

Many new developments in information technology have the potential for significant positive impacts on the functionality, performance, and costs of enterprise systems. Developments like Web 2.0, cloud computing, virtualization, green IT, and mobile computing all offer the potential for very significant benefits to enterprise system operations, but they all have important security and privacy issues associated with their concept of operations and their underlying technologies. In particular, Web 2.0 social networking sites like Face Book and Twitter are also becoming platforms for many enterprise applications for some new businesses. Their cybersecurity vulnerabilities have already led to some disrupted operations and losses of information privacy²⁰. Because of the potential business value from resolving these security and privacy issues, there are many groups addressing security and privacy issues in these new architectures. These include, for example, the Cloud Security Alliance, the Web Consortium, and the Open Group^{21 22 23}.

The combination of the value of the enterprise systems and services and the growing threats has led to the development of a growing market for cybersecurity systems and services. Gartner estimates that the worldwide market for enterprise security infrastructure market was \$44B in 2009, including software, hardware, and services²⁴.

Within the US, there have been various estimates of the Federal Government market for cybersecurity products and services. This market will grow, in part, because of the Comprehensive National Cybersecurity Initiative. The White House made an unclassified announcement about this initiative earlier this month.²⁵ Also earlier this month, Market Research Media estimated that the U.S.

¹⁸ Cooperative Cyber Defence Center Of Excellence, “Cyber Attacks Against Georgia: Legal Lessons Identified”, November 2008

¹⁹ Welsh, W., “Future hostilities to begin with cyber attacks, NATO official says,” www.securitysystems.com, March 25, 2010

²⁰ The Guardian, “Twitter phishing hack hits BBC, PCC ... and Guardian ... and cabinet minister ... and bank,” February 26, 2010

²¹ Cloud Security Alliance, “Security Guidance for Critical Areas of Focus in Cloud Computing, V2.1,” Dec. 2009

²² www.w3c.org

²³ www.opengroup.org/security

²⁴ The Gartner Group, “Key Issues for Technology Providers: Security Markets, 2010,” March 9, 2010

²⁵ The White House, “The Comprehensive National Cybersecurity Initiative,” March 2010

Federal Cybersecurity market during 2010 through 2015 will grow at about 6.2% CAGR over the next six years with a cumulative market valued at \$55B.²⁶

There will be growth in the private sector markets, as well. For example, as discussed earlier, security for the power grid has become a significant concern. Accordingly, there is a growing effort to address Smart Grid security issues. In February, the Wall Street Journal reported, "Pike Research, a clean-tech market research firm, expects the global smart grid cyber security market to grow to \$4.1 billion in 2013 at a compound annual growth rate of 35%."²⁷

Why is Cybersecurity So Difficult?

Now that we have discussed the growth of enterprise systems and services, the cyber threats to them, and the consequent markets that are developing quickly, let us consider the following question. Why is cybersecurity so difficult? Because it is difficult and the cybersecurity of our enterprise systems and services are so valuable, we are seeing large expenditures and developing markets. Answering this question correctly will allow an enterprise to focus its resources properly to improve the situation.

There are several causes of the difficulty of cybersecurity. This morning, I will discuss five of them. This will lead to some conclusions about the theme of this Forum, how to "protect your enterprise with secure and resilient information flow."

First, cyberspace is a new frontier as compared to other domains in which the US is also devoting significant resources to securing. The first airplane flight happened more than 100 years ago. The first satellites launched more than 50 years ago. The World Wide Web began only 20 years ago. Aviation and space security concepts were virtually unknown 20 years after their initial events, and even now, we have much to learn about securing aviation and space. We are still at the beginning of our understanding of cyberspace and cybersecurity. Cyberspace is a very different domain from the physical world, and we have much to learn about the sciences of networks and cybersecurity. However, we are seeing how quickly events occur in cyberspace, so there is a special urgency for cybersecurity. Because cyberspace and cybersecurity are both new and very significant, Northrop Grumman has an extensive related research program that I will summarize briefly later in this presentation.

Second, there are many parts of the technology and technology management of enterprise systems and services that are immature. Competitive pressures and needs for more cost-effective industry and government operations lead to continual introduction of new enterprise system architectures and technology. I described some important examples earlier in this presentation, including cloud computing, virtualization, Web 2.0, mobile computing, etc. As said earlier, these new developments can have significant business value and potential for major new developments. However, these introductions are too often made without sufficient enterprise-level management processes and tools as well as adequate cybersecurity design validation and testing. As a result, we all see frequent news reports of "security holes" and patches to correct previous errors. Despite a voluminous literature

²⁶ www.marketresearchmedia.com

²⁷ Wall Street Journal, "Power Up on Smart Grid Cyber Security," February 25, 2010

on secure system architecture, management, and software techniques, there are daily instances of cybersecurity shortcomings due to immature management processes, architectures, and technology. Because of these technology issues, Northrop Grumman has an extensive cybersecurity testing and integration team that is part of our cybersecurity operation.

Third, neither government nor industry yet has a broad understanding of cybersecurity economics. This is a relatively new subject, but it does have a growing community of researchers, who participate, for example, in the annual Workshops on the Economics of Information Security.²⁸ There has been some research, for example, in this community on an economic perspective on the difficulty of information security resulting from conflicting economic incentives.^{29 30}

There is another economic issue affecting cybersecurity. That is the difficulty of placing economic value on cybersecurity and cybersecurity investments. There has been good research done in this area^{31 32}, but it has not yet been widely implemented in major enterprises. This type of valuation is essential for making cybersecurity business cases, and I hope that there will be much progress made soon in the economics of cybersecurity. Economic valuation is one aspect of a more general challenge of determining appropriate metrics for security. However, I have focused on economic measures here, because the lack of credible valuation measures has been a limiting factor in stimulating sufficient investment in cybersecurity. Northrop Grumman continues to develop both research and budget strategies for cybersecurity and has active collaborations with others in this field. In particular, our Northrop Grumman staff members have worked closely with our Department of State customers on risk-based strategies for improving cost effectiveness in cybersecurity to develop our iPost system.³³ That system received recognition last year by winning the NSA Rowlett Award for Organizational achievement. The Department of State has been a leader in implementing risk-based strategies in their global network.³⁴

Fourth, the legal environment is complex and changing rapidly. There is much legislation in development in the House and Senate created in response to the judgment by many that the US does not have an adequate legal framework to address important cybersecurity issues. For example, last year a Congressional Research Service report³⁵ stated,

²⁸ <http://weis2010.econinfosec.org/>

²⁹ Anderson, R. "Why Information Security is Hard - An Economic Perspective," 17th Annual Computer Security Applications Conference, New Orleans, December 2001

³⁰ Anderson, R. and Moore, T., "The Economics of Information Security," Science vol. 314, 27 October 2006, p.610-613

³¹ Bodin, L., Gordon, L., and Loeb, M., "Information Security and Risk Management," Communications of the ACM, vol.51, No. 4, April 2008, pp 64-68

³² Pfleeger, S. and Rue, R., "Cybersecurity Economic Issues: Clearing the Path to Good Practice," IEEE Software, January/February 2008 pp 35-42

³³ Rudman, R., "Choosing the Right Tools for Automating and Measuring the Critical Controls," The National Summit on Planning and Implementing the 20 Critical Security Controls, Washington DC, November 2009

³⁴ Streufert, J., "More Security, Less Waste: What Makes Sense for our Federal Cyber Defense" Testimony before the Senate Committee on Homeland Security and Governmental Affairs, October 29, 2009

³⁵ Rollins, J., "Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations," Congressional Research Service, March 10, 2009

“In response to calls for executive action, questions have arisen regarding the adequacy of legal authorities justifying executive responses to cyber threats.”

Additionally, the legal framework limits cybersecurity research in certain ways. As concluded in a report³⁶ last year by the Institute for Information Infrastructure Protection

“At present, rather than helping secure cyberspace, the US regulatory and legal environment indirectly encourages a “checkbox” mentality, which discourages innovation.”

Addressing these limitations and others is the subject of the several legislative initiatives now under consideration by the Congress and the Administration. Northrop Grumman has continual communications on all legal aspects of cybersecurity from legislative development to law enforcement. These aspects are an important part of our business planning and cybersecurity operations.

Fifth, we all need to understand the human dimensions of cybersecurity. This may ultimately be more important than the other three factors, but this is a very new field of study. A new workshop series, Workshop on Security and Human Behaviour³⁷, has formed to include issues like trust, social phishing, human performance with computer interaction, privacy, and other related topics like training. In particular, Northrop Grumman is addressing the problem of creating greater cybersecurity awareness and defensive skills in all of our staff members – not just the IT Staff. We believe that this awareness is particularly important with respect to the Advanced Persistent Threat. We have recently published some of our work in the Proceedings of the 13th Colloquium for Information Systems Security Education.³⁸

An analysis of these five factors has led us to the cybersecurity approach that we use at Northrop Grumman, both in our current operations and in our R&D program. We have responded to the challenges of new concepts, technology, economic, legal, and human aspects with a significant multi-layered security policies, architecture, processes, integrated technologies, and operations staff, as well as with a vital research program.

Current Northrop Grumman Cybersecurity Operations

Next, I will discuss our current Northrop Grumman cybersecurity operations and follow this discussion by a summary of advanced cybersecurity research. Although I believe that Northrop Grumman has an outstanding cybersecurity posture, we work continually to improve it. Like other organizations whose businesses are in global security, we face growing cybersecurity threats.

We have a dedicated cybersecurity staff that works in close collaboration with our internal IT staff to protect Northrop Grumman’s information and network operations. The Northrop Grumman

³⁶ Institute for Information Infrastructure Protection (I3P), “National Cyber Security Research and Development Challenges, Dartmouth University, 2009

³⁷ Workshop on Security and Human Behaviour (SHB 2010), <http://www.cl.cam.ac.uk/~rja14/shb10/>

³⁸ Smith, A. and Toppel, N., “Case Study: Using Security Awareness to Combat the Advanced Persistent Threat” Proceedings of the 13th Colloquium for Information Systems Security Education, June 2009

Global Network (NGGN) serves more than 120,000 employees operating in all US states as well as in 25+ countries around the world. Moreover, the NGGN connects in certain limited ways with some of our customers, partners, and major suppliers. Consequently, we need a significant cybersecurity operation.

Our cybersecurity staff is responsible for monitoring the network for any signs of malicious activity and for responding to incidents, as required. This staff assesses security risks and works in collaboration with our internal IT staff on the testing and integration of new products for implementation on the NGGN. We also have a Cyber Threat and Intelligence Analysis unit that works in close collaboration with law enforcement and counterintelligence organizations for information sharing to ensure that we have the latest available information for potential threats to our network.

Our security architecture begins with our identity management policies and system. We make significant investments in identity management, and we collaborate internationally on these issues. For example, we are strategic members Transglobal Secure Collaboration Project (TSCP). TSCP is an international consortium of members in aerospace and defense. The project focuses on solving problems related to the security of information in collaborative activities among companies, governments, and individuals. Participants in TSCP have common requirements for secure, identity-based information sharing. Since there is a presentation on TSCP later in this Forum, I will not say much about TSCP here beyond that our participation in it is an important part of our overall identity management strategy and that the TSCP Chairman, Keith Ward, is a Northrop Grumman employee. We also focus efforts in improving identity security in other industries, e.g., financial services³⁹, and we apply all of this experience in various domains to securing our own enterprise operations.

Our security architecture is multi-layered and is a result of our corporate security policies. Our operational identity management system we call OneBadge. This integrated identity management system provides both building access and network access for our employees. At the first layer, we combine strong authentication and credential management used to authenticate users into our facilities and onto our network. In the second layer, we manage their privileges and access rights to various network services. Additionally, we have a variety of network controls for intrusion detection and prevention as well as data-loss-prevention systems that monitor data flowing out of the network. We have integrated technology from third parties with our own developments to provide broad cyber situational awareness for our information systems and networks. The evaluation and integration of this leading technology is critical to our cybersecurity operations and to the success of Northrop Grumman.

Addressing the human dimension is also an important part of our overall cybersecurity strategy. We have an extensive cybersecurity awareness and training effort throughout the corporation. This includes frequent messages about new cybersecurity issues, mandatory training for all employees, and specialized training for our network operations personnel. Additionally we have an annual presentation on the Advanced Persistent Threat for our management team in order to maintain their awareness of developments in that area. As noted in some earlier examples, we participate regularly in professional

³⁹ Brammer, R., "Identity Security in UK Banking and Other Financial Services," Symposium on Identity Security, University of Cambridge, 19 September 2008

conferences with various publications talking about our ideas and exchanging information with other organizations to improve the overall profession.^{40 41 42}

We are also active in a number of industry organizations in addition to TSCP. A few examples from a longer list include the Defense Industrial Base⁴³, the Internet Security Alliance⁴⁴, the National Security Telecommunications Advisory Committee⁴⁵, the National Infrastructure Advisory Council⁴⁶, and many others. Our participation in these organizations promotes the information sharing that is vital to protecting our enterprise from cybersecurity threats.

In summary, Northrop Grumman is continuing to develop our leading cybersecurity operations organization with a multi-disciplinary approach. This approach includes an integration of policies, technology, economics, legal, Information sharing, and human factors to address the major threats discussed earlier. However, we complement our current operations with a strong cybersecurity research program.

Advanced Cybersecurity Research

As discussed earlier there has been in the past couple of years a growing recognition in the US that both government and industry have not invested sufficiently in cybersecurity. That has led to the creation of the Comprehensive National Cybersecurity Initiative⁴⁷ as well as other government and industry investment programs⁴⁸. Many organizations have evaluated R&D agendas for cybersecurity, including the President's Information Technology Advisory Council⁴⁹, the National Science and Technology Council⁵⁰, the National Research Council⁵¹, the White House Office of Science and Technology Policy (OSTP)⁵², the Department of Homeland Security⁵³, and many others. Northrop Grumman has participated in many of these studies and we analyze their results in determining the structure of our own research program. In particular, Northrop Grumman has been very active in the OSTP-sponsored National Cyber Leap Year Summit⁵² and the follow-on activities. The National Cyber

⁴⁰ Brammer, R., "Significant Trends in Information Technology Security Threats and Defensive Technology," Keynote Presentation, FAA Information Technology and Security Conference, Dallas, TX, 15 March 2007

⁴¹ Brammer, R., "The Future of Broadband Mobile Networks," MIT Lecture Series on Advanced Communications, 19 March 2007

⁴² Brammer, R. "Broadband Wireless Comes of Age in Secure Mobile Government Services," Keynote, Wireless Communications Association International, 2007 Symposium -- Celebrating 20 Years, Washington DC, June 2007

⁴³ <http://defenseindustrialbase.blogspot.com/>

⁴⁴ <http://www.isalliance.org/>

⁴⁵ <http://www.ncs.gov/index.html>

⁴⁶ [Http://www.dhs.gov/niac](http://www.dhs.gov/niac)

⁴⁷ The White House, "The Comprehensive National Cybersecurity Initiative," March 2, 2010

⁴⁸ Wall Street Journal, "Power Up on Smart Grid Cyber Security," February 25, 2010

⁴⁹ President's Information Technology Advisory Council, "Cyber Security: A Crisis of Prioritization," February 2005

⁵⁰ National Science and Technology Council, "Federal Plan for Cyber Security and Information Assurance Research and Development," April 2006

⁵¹ National Research Council, "Toward a Safer and More Secure Cyberspace," 2007

⁵² White House OSTP, "National Cyber Leap Year Summit," September 2009

⁵³ Department of Homeland Security, "A Road Map for Cybersecurity Research," November 2009

Leap Year event in August 2009 was designed to address point #9 in the President's remarks¹¹ focusing on the need for stimulating activities to develop "leap ahead technologies" to solve our cybersecurity challenges. Northrop Grumman has made significant research investments to address these challenges.

In December, we announced another of our cybersecurity investments, the creation of our Northrop Grumman Cybersecurity Research Consortium^{54 55}. This is a partnership with three world-class universities – Carnegie Mellon, MIT, and Purdue. This research partnership will extend our own significant cybersecurity research program with a unique multi-university consortium. We are working in close collaboration with faculty and students at each of these universities on a wide variety of research projects to extend our interactions with the cybersecurity research community and to produce some important innovations that we can implement in large-scale cyberspace operations.

We have an extensive laboratory network across the US for cybersecurity modeling, simulation and testing. Our staff members use these labs to serve both our customers and our own operations. Our laboratory network includes our cyber test range, the Northrop Grumman Cyberspace Solutions Center. This is a robust Internet environment for emulating, attacking, and evaluating information technology, IT and infrastructure network operations, and cybersecurity defense. We have continued to develop this facility since its inception in 1999, staying on the leading edge with state-of-the-art technology and operations. Our research projects use our laboratory network, including the cyber test range, in realistic environments to test the viability and scalability of new cybersecurity concepts and products. We are now extending our laboratory network and cyber range to the UK in order to address some international cybersecurity issues.⁵⁶ We will be collaborating with the UK Technology Strategy Board, the Ministry of Defence, British Telecom, and leading UK universities in this development.

We design our research projects primarily to help build our external business. However, because the needs of our customers to defend their enterprises are very similar to ours, there are many close connections between our research program and our needs to protect our enterprise.

Concluding Remarks

In conclusion, protecting the enterprise is an increasingly difficult challenge. We have noted earlier the growth in value and distribution of enterprise systems in the face of a very dynamic and growing threat environment. As we have discussed, protection requires a multi faceted approach, including policies, processes, architecture, technology, economics, and human factors.

The growth of the security breaches continues at a rapid pace so we need to continue to increase our efforts. For example, the BankInfoSecurity web site has reported 173 significant breaches

⁵⁴ Brammer, R., "The Northrop Grumman Cybersecurity Research Consortium," National Press Club, Washington D.C., December 2009

⁵⁵ Wall Street Journal, "Northrop Joins With Academics For Cybersecurity Work," December 1, 2009

⁵⁶ www.northropgrumman.com, "Northrop Grumman to Develop UK Cyber Security Test Range for Evaluation of Threats on Large Scale Networks," December 16, 2009

so far this year (as of March 23, 2010); including 22 involving financial services companies⁵⁷. These numbers exceed last year's pace by about 30%.

I believe overall cybersecurity problems will become worse before the situation improves. Substantial incidents in the banking system, the electric power grid, or other critical infrastructure system will only exacerbate the situation and public concerns. These are very credible threats. We have already seen significant problems, and, if the situation worsens, then the cybersecurity, reliability, and credibility of a number of organizations will degrade significantly. The impacts of these degradations will adversely affect the reputations, share price, and other significant metrics for these enterprises.

However, some near-term progress is certainly possible. It is well known that 90+% of security problems arise from situations for which there are known solutions. Better implementation of system configurations and timely patches would reduce the impact of many of these incidents. The cybersecurity industry and end-user enterprises need to work more effectively in making these implementations easier and more reliable. There have been some good news cases showing the success of such increased efforts so the situation is not necessarily all-bad. For example, the Gartner Group reported last week that a bank had recently had considerable success against significant Zeus malware attacks⁵⁸. Gartner had observed, "Zeus and other malware authors continue to morph their malware into new, unpredictable attacks, requiring proactive fraud management to keep up with these evolving threats." However, in this case, this bank had "proved that pinpointed rules applied to comprehensive fraud monitoring can defeat Zeus and other malware-based attacks attempting to raid customer accounts." Last fall, Information Security Magazine reported⁵⁹ that Zeus was "the nastiest, most sophisticated Trojan I've ever seen. It's a money-stealing machine.... About 1.6 million infected machines make up hundreds of Zeus botnets..." However, a mid-size bank had considerable success from "... the alignment of IT and business staff processes as a key contributor to its effective attack mitigation and response strategy." This is one example of how an enterprise developed effective processes and technology to mitigate a major cybersecurity challenge.

However, we should all recognize that cybersecurity will be a long-term strategic issue for major enterprises for many years. The current widespread approach of patching poorly designed systems is clearly not sufficient to defend the enterprise. Solutions will require sustained and multi-disciplinary research and development as well as a very broad large-scale process and system implementations. I am optimistic that the American people can respond to this threat and that ultimately we will resolve these cybersecurity threats to a manageable level. This will require an extensive collaboration among government, industry, and academia. However, if we can do that then I believe that we will ultimately be successful.

⁵⁷ www.bankinfosecurity.com, "22 Banking Breaches So Far in 2010 Report: Hacking, Insider Theft Continue to be Top Trends," March 23, 2010

⁵⁸ The Gartner Group, "Case Study: Bank Defeats Attempted Zeus Malware Raids of Business Accounts," March 23, 2010

⁵⁹ Information Security magazine, "Zeus Trojan hitting banking customers hard," September 8, 2009