NAVAL WAR COLLEGE FOUNDATION

CENTER FOR CYBER CONFLICT STUDIES

U.S. NAVAL WAR COLLEGE

PROCEEDINGS

Cyber-Insecurity: Privacy vs. Protection

Can Business, Academia and Government Be Partners in National Security?

Cybersecurity Roundtable Forum
The University Club, Chicago, IL
April 30, 2015

The Naval War College Foundation (NWCF) convened its third Cybersecurity Roundtable Forum on behalf of the Center for Cyber Conflict Studies at the U.S. Naval War College to address cyber threats to America's financial infrastructure and institutions. Specifically, the forum focused on what government, business, and academia needs to do to collaborate on ensuring systems are protected at a minimal cost to privacy. This forum is a continuation of roundtables held in Chicago and Washington, DC. in October and November 2014, respectively. Since then, the cyber threat has only escalated. The destructive attack on Sony is the most notable example of the increasing frequency and intensity of the efforts made to penetrate U.S. corporate, institutional, and government systems. Cybersecurity is now firmly at the top of the agenda for CEOs, boards of directors, and the White House. While awareness and a sense of urgency have increased and the Department of Defense has issued its specific strategy, there is still no coherent *national* strategy to address this threat to our national and economic security.

We were pleased to have join us a remarkable and well-established group of senior executives and Chief Information Security Officers (CISOs) from banking, investments, insurance, financial services, law firms, consulting firms, academia, and technology development. This meeting was representative of the Naval War College Foundation's ability to convene leading technologists and experts from the Naval War College on cybersecurity.

The forum was designed to examine the issues and to stimulate a discussion flagging the policy gaps that inhibit the development of a coordinated national policy. With the talent and perspective of those well-versed in governance, application security, access control management, risk assessment, compliance, and patents and trade secrets, the insights gathered and reflected in this document provide a unique perspective. The participants discussed common goals, critical elements for a successful framework, best and worst case scenarios, and "the deal breakers" in developing a strategy to implement and maintain a plan to safeguard our national security and commercial interests. The findings from this forum strike a balance between protection and privacy.

The forum was chaired by NWCF's Center for Cyber Conflict Studies Task Force member Mr. William Obenshain, and moderated by Dr. Peter W. Singer, Strategist and Senior Fellow, New America Foundation, and Dr. Lewis Duncan, Provost, U.S. Naval War College. Professors Peter Dombrowski and Derek Reveron from the Naval War College also participated.

More than forty distinguished attendees participated, including Superintendent of the U.S. Naval Academy, Vice Admiral Walter E. "Ted" Carter; senior executives and leaders in information security and risk, consultants to finance and military organizations, and leaders from banking, insurance, investment, cybersecurity, law, and academia.

The forum continues the national dialogue on cybersecurity under the convening authority of the Naval War College Foundation. Notwithstanding the time constraints of a four-hour format, many key issues and questions were raised and addressed with preliminary findings and recommendations offered. These are grouped below by the core themes considered by the forum, including:

- Key issues and questions
- An overview of the discourse
- Representative unattributed quotes, and
- Recommendations for further consideration by key stakeholders.

I. NIGHTMARES & CHALLENGES

KEY ISSUES AND QUESTIONS

- Definition of the problem set
- Nightmare scenarios: reputation risk and liability of release of personal information; data corruption
- Challenges: proper employee training, generational attitudes, keeping up with pace of issues and requisite responses

OVERVIEW OF THE DISCOURSE

Cyber threats show no signs of abating or diminishing. Some 97% of Fortune 500 companies report breaches to their networks or data. It is widely believed that the remaining 3% have also been hacked but refuse to admit it publicly. If anything, the threats are increasing and growing in complexity.

Recent polls indicate that individuals have a huge fear of others accessing their information or identity and thus gaining access to their funds, much more than they fear a violent terrorist attack. Studies also show that 72% of consumers are more likely to buy from those companies they view as “secure.”

One bank representative detailed how a gang of foreign cyber-criminals penetrated the bank’s process for conducting wire transfers. As a result of that incident, the bank has tightened its

process for verifying the authenticity of customer instructions. Another bank representative noted that his corporation was a victim of 1.7 million hacking attempts last year.

Cybersecurity has now infused all aspects of security, commerce, communication, and conflict. At least 100 nations have established cyber commands. Nation states are increasingly evaluating the weaponization of cyber technology. Organized crime is a multi-billion dollar funded adversary. Cybersecurity-related products and services generate at least $160 billion in annual revenue. The Pentagon is turning its attention to cybersecurity. In the 2012 Pentagon budget the term "cyber" was used only 12 times. In the 2014 Pentagon budget, the term "cyber" appeared 146 times. Finally, the fact that 98% of military communications travel over the civilian Internet proves the criticality of protecting its integrity.

While awareness and engagement increase, the issue remains that each sector perceives cyber threats differently. Believing that economic security is equivalent to national security, we sought to define the problem set among our participants. We sought insights on "nightmare" scenarios and identification of the most common "day-to-day" cybersecurity challenges.

The following "Nightmare Scenarios" were discussed by each of the industry participants:

- Undetected intrusion and penetration of the customer base
- Applications mixed with data corruption that undermine a company's reputation resulting in a pandemic effect
- Massive reputation risk if hacked and the liability associated with unauthorized release of personal information
- Specific sectors as targets; e.g., in the securities sector disruption of communications and denial of access are catastrophic because connectivity is essential to the functioning of capital markets
- The "weakest link" can be used as gateway to cause widespread destruction and disruption
- Sustained denial of service attack
- Rogue computers
- Major data breach. Fear of being "Sony'd" with the accompanying damage to brand and reputation which is embarrassing and disruptive
- Disclosure of private data; consequences of loss of trust; e.g., university student records
- Ransom of law firm data; the release of confidential or privileged information which could be catastrophic and threaten survival of the firm
- Loss of trade secrets and patents
- Impact of quantum computing on encryption
- Technological surprises

The participants noted the following "day-to-day" challenges with cybersecurity:

- Proper personnel training to detect and respond to unauthorized intrusions; differentiation between basic and advanced security training. This is analogous to learning how to drive a car. At the most basic level, the user's tendency is to learn how to drive it, not to learn how it works.

- Volume and rapidity of change in functions and new applications such as cloud migration; keeping up with systems integration and protection
- New connections and application rollout
- Retention of good people
- Gap between perception and reality of cyber threats among employees, consumers, students, and faculty
- Adjustment of risk tolerance levels to reflect costs vs. benefits
- For law firms, a significant day-to-day challenge is addressing the heightened data security required to protect market sensitive information (material, non-public information about companies with publicly traded securities) and the valuable intellectual property that comes into the custody of the law firm as deal counsel, as litigators engaged in discovery, or as patent counsel or in other intellectual property (IP) roles.
- Adoption of technological solutions that create potential vulnerabilities
- Changing norms on ethics of IP protection; younger people believe whatever can be accessed on the Internet is free.

REPRESENTATIVE UNATTRIBUTED QUOTES

- "317 million variants of malware discovered in 2014, or just under one million per day."
- "Tomorrow's problems are being addressed with yesterday's answers."
- "In the securities business, the disruption of communications and account denial are catastrophic."
- "Disruption of communication to capital markets would be devastating. They cannot be closed for more than 3 days without significant adverse impact."
- "Law firms don't have a consumer brand. They have their reputations. A serious hacking incident or security breach could destroy the firm entirely."
- "Cybersecurity is a board-level responsibility."

RECOMMENDATIONS

- Government leadership needs to work more closely with private industry to share national-level awareness of state-sponsored cyber terrorist threats and to provide a coordinated public-private sector response.

- All parties need to understand the difference between cybersecurity and national security. Private parties manage private space and need a protocol for reporting to the government breaches that have national security implications.
- Corporate governing boards need to recognize the importance of Information Security Officers and cyber threats to their business. Technical cyber experts should provide briefings to corporate leadership at every board meeting.

II. ACTORS & CYBER LEADERSHIP

KEY ISSUES AND QUESTIONS

- Motivations vary between actors: from state-on-state attacks to criminal, to generally accepted, to a generational perception that does not recognize private ownership or IP.
- Attribution in general is a significant challenge.
- Definition and baseline controls/parameters for cybersecurity vary from inconsistent to nonexistent.
- Threats and associated costs need to be tied clearly to business operations to get the attention and investment necessary to respond adequately to threats and to develop broader strategies.

OVERVIEW OF THE DISCOURSE

For precisely the same reasons the Internet is a success, it is also a virtually unprotectable system. In addition to legitimate users, it is gamed by actors, some of whom seek only to prove they can access networks and data, and others who have more sinister motivations of theft or disruption. One academic participant noted that a nightmare scenario is to have students leading a cyber attack on their own college. They do it for curiosity and peer recognition, not for profit.

Nation states have the resources to conduct nightmare attacks; some support criminal networks that seek to disrupt processes or exploit the vulnerabilities of non-favored countries or corporations. Insiders (e.g., disgruntled employees), competitors, and proxy actors may pose an even greater threat that is much harder to detect because they may be working from a position of privileged intelligence. Well-intended younger generations, who perceive everything on the Internet as "open source" and free to all, unwittingly compromise intellectual property, proprietary information, practices, and trade secrets. "Hacktivists" may promote social agendas tied to a host of government and industry policies and practices.

Attribution, the confirmed determination of those responsible for launching a cyber attack, remains a significant issue. One participant noted how gas pipelines have wireless access points; that while convenient and efficient, the tradeoff is increased risk to system integrity. Artificial Intelligence also raises issues of control. Institutions strive to design controls that do not encumber the ability to operate, yet still provide maximum system protection. The application of quantum computing rises as a threat to frustrate even the most sophisticated encryption protections.

Given the lack of consistency and continuity in perspective, it should come as no surprise there is not a baseline framework in place for industry-focused research leading to policy formulation and policy analysis. While solutions may differ by industry, there are common issues that can provide a basis for accountability among employees, management, vendors, and partners.

The issue of cyber insurance arose as an innovative way to force the issue of placing a cost/value on cyber threats and security. Contributors indicated that there were no consistent underwriting standards that could serve to drive consistency in cybersecure practices.

REPRESENTATIVE UNATTRIBUTED QUOTES

- "There's no equivalent to food safety in cybersecurity."
- "A threat is what you choose NOT to do; generational difference impacts what a threat is and why it is a threat."
- "There is no equivalent to a Centers for Disease Control in the cyber field."
- "A mature cybersecurity program is not about technology, it's about how to manage the solution."

RECOMMENDATIONS

- Make cybersecurity a board-level responsibility. Ensure the right people have proper resources to make the right decisions. Board and management must lead and demonstrate that security is an issue for the entire organization. CISOs and other technology operatives will not be the convenient scapegoats.
- Consider cyber insurance as one proxy for risk tolerance and security standards.
- Identify metrics that matter and enforce internal processes.
- Create a one-page dashboard for communicating the status of organizational security to the board and senior management.
- Require a strong relationship among the CISO, IT Director, and privacy personnel to ensure effective process integration and communication across the entire organization.
- Establish an effective working relationship with regulators who look to the private sector to educate them about threats and appropriate protection actions.
- NIST (National Institute of Standards and Technology) frameworks should be more widely used to compare standards across industries. Consistency of standards is a worthy goal but must be balanced by industry requirements. There must be government buy-in to these frameworks to ensure a requisite level of industry engagement and compliance in adhering to the standards, enforcing any violation of the standards, and benefiting from protections afforded by the government for participation.

III. POLICY IMPLICATIONS

KEY ISSUES AND QUESTIONS

- What is the role of the government in protecting against the cyber threat?
- What does normal look like?
- Who is involved and responsible for development of cyber policy and to what extent?

OVERVIEW OF THE DISCOURSE

Education: VADM Ted Carter described how cyber training is being incorporated into the curriculum at the U.S. Naval Academy. Recalling how a smart phone has more computing power than the planes he flew, VADM Carter elaborated on how critical cyber was in even the most basic concepts of the military. He spoke of the cyber domain merging with the electro-magnetic spectrum and the resulting impact, as one cannot execute Command & Control without cyber.

As it relates to networks and electronic systems, cyber is not its own unique domain, but a thread through land, sea, air and space. Since cyber is totally integrated into our warfare systems, basic concepts must be mastered as backup in cases of system failure. The return of celestial navigation to the U.S. Naval Academy curriculum was cited as an example. As evidenced by the creation of the Information Dominance Corps, education must be an integral part of any centralized effort. The integration of cyber hygiene and security in general should be part of all science and tech education. Cyber is multidisciplinary and promoting good internal education will serve as an effective monitor of potential external risks.

Cooperation & Collaboration: The banking industry is credited with having one of the more robust sharing agreements in terms of cyber strategy and tactics. CISOs have an informal peer-to-peer mechanism that facilitates information exchange. For some groups, it is a fee-based information exchange. Companies are individually responsible for protecting their own data and "red team" their systems to identify vulnerabilities. Cooperation among industries does not necessarily translate into a desire to partner with the federal government. The Financial Services Information Sharing and Analysis Center (FS/ISAC) is one organization that provides early warning about security threats to its member institutions.

Liability: There are no "rules of the road" or public infrastructure to improve cybersecurity. All participating corporations, industry groups, and others who seek to benefit from a coordinated strategy and the protections afforded by it must be held accountable for cyber hygiene and correction of vulnerabilities.

Role of Government: The government's role is to respond to hostile state actors. It was noted that China often appears to take the position that they are beyond the law, and an effort must be made to bring China into the fold. Data theft can be addressed through lawsuits and needs no government intervention.

It is unwise to assume all companies want government involvement. Many want attorney-client privilege wrapped around any possible breach in order to protect company liability and enterprise value. The loss of trust and damage to intellectual property and reputation has a more significant impact/use than retaliation. Victims often want to keep the fact they have been attacked quiet in order to avoid image damage unless the breach can remain anonymous. It was pointed out that Sony had been breached multiple times since 2007 but did nothing to improve its security; however, it could not hide the most recent, catastrophic intrusion.

Within these overarching findings, key determinations can be made regarding the following areas to ensure the successful execution of any effective policy and action.

Timing: Even with some areas of engagement defined, a clear timeline must be developed that indicates what would trigger a government response.

Terms of Engagement: Today's focus is on recovery, but we need better front-end products. How can industry and vendors-to-industry more effectively deliver and manage solutions? We need to respond and recover quickly.

The government has offensive cyber weapons. What "war" policy governs their use? Since industry does not have offensive weapons, the threat of government response on its behalf should be touted as a deterrent.

Level of response: What level of response is acceptable? Is the mere threat of an overwhelming and decimating response more effective than sanctions/or more punitive reactions?

What is the impact of a private-public partnership on multi-national companies' global inter-operative level of engagement and cross-border businesses?

REPRESENTATIVE UNATTRIBUTED QUOTES

- "Can we conceive of an immune system for the Internet?"
- "Ultimately, there should be established a system for governing the Internet similar to the ideals of the International Rules of the Road or the Law of the Sea: The Internet must remain interoperable, secure, and accessible to all legitimate users."
- "We talk about 'public-private partnerships.' Make it 'private-public' instead. Ninety percent of government information goes over the commercial network. There's a preference for limited government and private solutions."

RECOMMENDATIONS

The Forum concluded its policy discourse with a summary of the ways business, government, and academia can cooperate to create a more coherent, secure cyber landscape. The recommendations are noted below:

Education:

- Foster the development of talent beginning with cyber security training in lower, middle and high school levels and extend to STEM programs at the university level, MBA programs, and vocational schools.
- Encourage talent retention principally by reforming the visa program for foreign students with relevant education and training.

Cooperation & Collaboration:

- Align government and private sector with common vocabulary and framework.
- Allow industry to conduct baseline threat management while government conducts offensive cyber work (covert/other).
- Develop models that reflect best practices for cyber defense and cyber hygiene.
- Recognize cyber challenges and collaborate on standards for reporting breaches and strengthening response, recovery, and resiliency.
- Promote development of centers of excellence for cyber research, training, and policy formulation. Research is needed on topics such as developing an immune system for the Internet, e.g., automatic patch of vulnerabilities.
- Promote industry organizations such as FS/ISAC and NIST that encourage information sharing and standards development. Create infrastructure for companies to report breaches and intrusions on an anonymous basis.
- Develop an incident management culture so a response to a cyber attack is understood by all industry and government entities that are affected. Ultimately, the goal is to develop a better process between private sector and government that results in reducing threats.

Liability:

- Consider establishing a grading/reporting system like the ISO quantifications. This requires equal commitment by vendors to establish cyber hygiene protocols and standards. Many of these entities may develop software and other platforms used by companies specifically to protect information systems and customer data, which will be compromised from the onset if they do not conform to the requirements for basic cyber hygiene.
- Encourage the insurance industry to develop underwriting standards and create insurance products for a wide range of organizations and situations.
- The judiciary can also play a key role to enhance the cybersecurity landscape:

    - Consumer data breach class actions do little to enhance data protection and impose disproportionate litigation expense. Although the federal courts have, generally, been quite skeptical of the theories of liability advanced by the plaintiff's bar, the class action firms continue to bring new suits. Clear, decisive, precedent barring these claims would allow both the business community and the courts to focus on more critical data security issues.

- It is widely accepted that data security is an essential part of protecting the critical assets of most public companies in which shareholders invest, yet shareholders still lack even basic information about the data security of those companies. More vigorous enforcement by the SEC and perhaps even a few high-profile shareholder class action suits based on failure to disclose material risks could do much to increase the information available to shareholders and to enhance the incentives for public companies to invest in data security.
- "Security by design" is a concept that is much talked about but still falls short in practice. Data security should be part of the basic functionality of both hardware and software, and not an afterthought to be addressed in the final stages of product development. Imposing meaningful liability for products that have inherent data security design flaws would greatly enhance the incentives for developers to take seriously the concept of "security by design."

Role of Government:

- The universal baseline in this area stipulates upfront that the government role should be minimal in the private sector.
- Consider creation of an agency on the model of the Center for Disease Control and Prevention with the mission of protecting the nation's cyber health and security.
- Promote legislation that addresses issues such as anti-trust and liability that inhibit industry collaboration.
- Promote the development of centers of excellence for cyber research, training, and policy formulation. Research is needed on topics such as developing an immune system for the Internet, e.g., automatic patch of vulnerabilities.
- Create an infrastructure for companies to report breaches and intrusions on an anonymous basis.
- As outlined above under Liability, encourage the judiciary to play an instrumental role enhancing the cybersecurity landscape.

IV. CONCLUDING REMARKS

The Forum concluded the proceedings by expressing gratitude to Dr. Peter Singer and Dr. Lewis Duncan for leading the Roundtable participants through an exploration and analysis of the "Nightmares and Challenges" facing business, government and academia. The Chairman also expressed appreciation to the assembled leaders for their time and talent and for their recommendations for establishing a more coherent set of cybersecurity policies, practices and initiatives The Chairman noted that findings and recommendations would be circulated to all attendees for use in their respective organization in the form of Forum Proceedings. The Chairman encouraged all participants to continue an ongoing dialog with the Naval War College Foundation and the Center for Cyber Conflict Studies in addressing cybersecurity solutions and policy for their organizations, industry groups and the Nation.

Naval War College Foundation
686 Cushing Road, Newport, Rhode Island 02841-1213
www.nwcfoundation.org