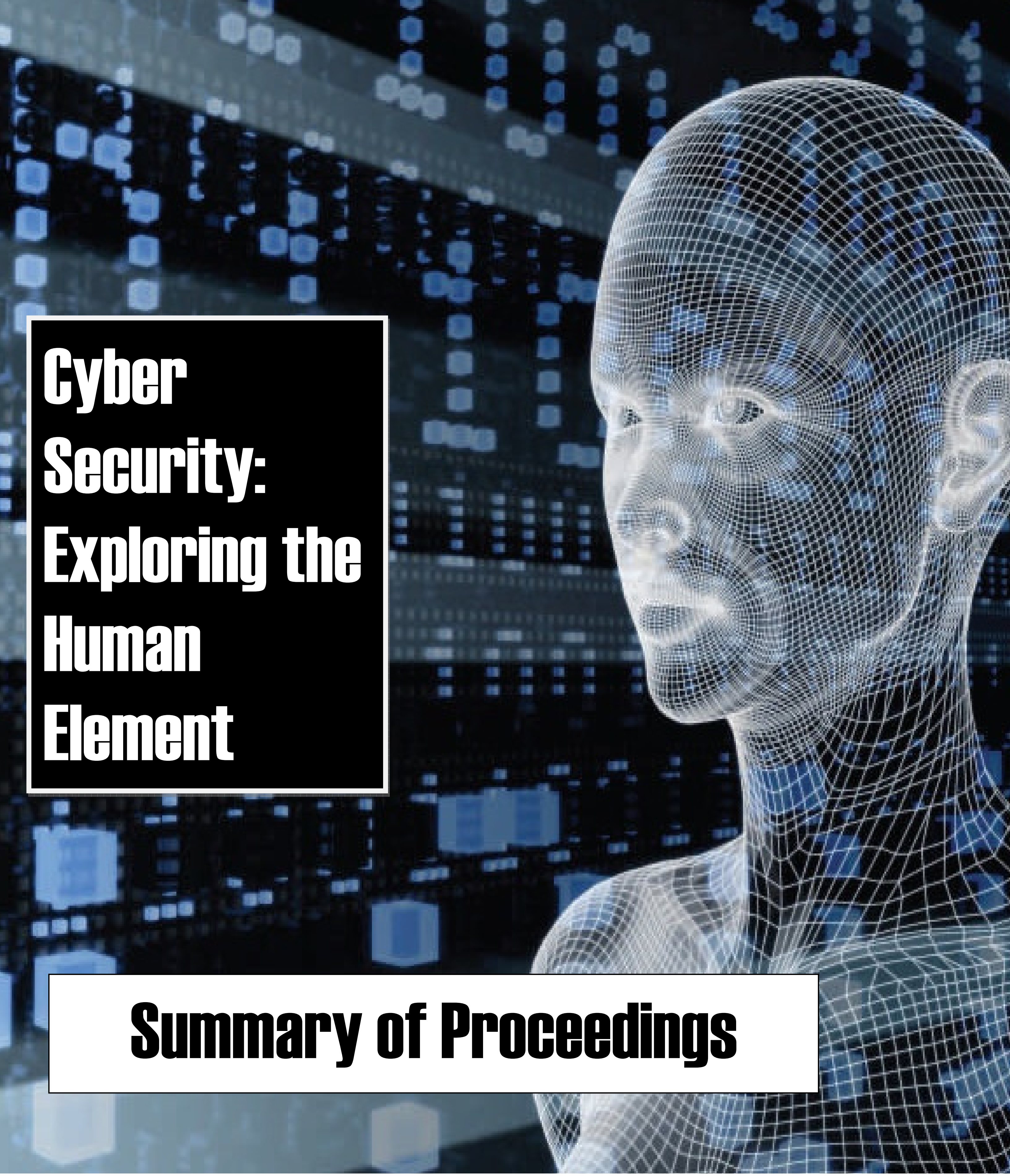
Cyber Security: Exploring the Human Element

Summary of Proceedings



RTI INTERNATIONAL

Institute for Homeland Security Solutions
Applied research • Focused results

Triangle Center on Terrorism and Homeland Security
DUKE - UNC - RTI

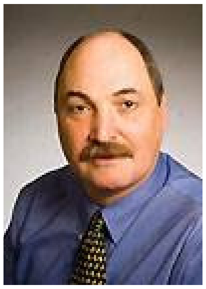
START
NATIONAL CONSORTIUM FOR THE STUDY OF TERRORISM AND RESPONSES TO TERRORISM
A CENTER OF EXCELLENCE OF THE U.S. DEPARTMENT OF HOMELAND SECURITY BASED AT THE UNIVERSITY OF MARYLAND

Cyber Security: Exploring the Human Element
Institute of Homeland Security Solutions
March 8, 2011—National Press Club

Introduction

A secure cyber environment is essential to public, corporate, and private aspects of our modern society. Government and industry are aggressively developing technical solutions to improve this key dimension of our national security. *This policy forum supplemented these efforts by exploring the central role that understanding human behavior plays in creating a more secure cyber environment*. How individuals and organizations behave—from the tools they purchase to reduce their vulnerability to the activities they engage in on the Internet—dramatically affects the overall security of the entire cyber infrastructure. The experts convened for this forum discussed the importance of the human element, current research in the field, and the policy implications of these important issues.

Keynote Speaker—James A. Lewis, Center for Strategic and International Affairs



Lewis opened the forum by explaining the gravity of the threat and the legislative debate taking place in Congress over the proper framework for addressing cyber security. Lewis emphasized that there "is no such thing as a safe system" and that even with advances in technology, absolute security cannot be ensured. Cyber warfare, intelligence exploitation through cyber space, and cyber espionage are all now part of the background landscape that must be taken into consideration when developing policy.

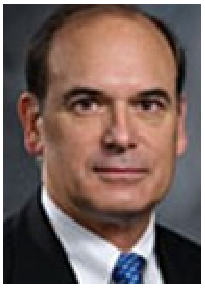
The international community no longer accepts the old model of the Internet as a transparent, communal forum to be governed by consensus-based organizations; nation states will act to impose new controls to promote their interests. In the United States, we are dissatisfied with the vulnerability of our critical infrastructure to cyber attack and are debating whether it can best be secured through incentives or a regulatory model. Lewis expressed his opinion that the voluntary model we have depended on for the past decade will not deliver the added protection we want in a timely fashion.

This debate will also be affected by the evolution from PCs/laptops to tablets and mobile devices. "Most consumers want their computers to work like their refrigerators," Lewis noted, “they want it to do what it needs to do without having to be patched, updated, and installed.” The move to the cloud is inevitable, so responsibility for security is going to shift from users to service providers.

For all these reasons, we need to reassess how we are approaching cyber security. Many of our assumptions about how users would address security have been wrong. First, we were wrong to assume that people and businesses would change their behavior if they understood the magnitude of the threat. It takes a great deal of knowledge for people to understand the threat, and, even if they do, considerations such as business competitiveness, antitrust, and liability all factor into decision making. Second, we underestimated skepticism—most businesses and users simply will not react to a potential threat they cannot see. Third, businesses and individuals do not default to the view that they are responsible for security. Most other security threats are viewed as a governmental responsibility. When individuals do not have the level of information necessary to assess the threat, we cannot expect them to take responsibility for addressing it. Finally, Internet technology changes how people treat information. We have overestimated the value that people attach to protecting information.

In sum, the voluntary, nonregulatory model assumed an incentive link between knowledge and behavior that does not necessarily exist. We need to better understand the linkages between incentives and behavior. To make progress in this area, we are going to have to step back and reassess the assumptions that have driven policy to date.

Corporate Perspective—Steven P. Bucci, Associate Partner, Cyber Security Lead, Global Leadership Initiative, IBM Global Business Services



Bucci agreed that cyber security is not a technology problem, because the system includes people. To improve security, we must deal with both the technological and the human side of the equation.

For example, Bucci explained, although better anomaly detection could have prevented the Wikileaks, there were many more human problems that led to this event. Too many State Department cables were being routed through U.S. Central Command when they were not needed, employees were allowed to play music CDs on secure systems that held classified information, and supervisors were not properly overseeing PFC Manning’s work.

Bucci argued that leadership and training are key elements of cyber security. Right now, 90 percent of supervisors do not do the security training that is mandated for their employees. This is a problem and sends the wrong signal to their workforces.

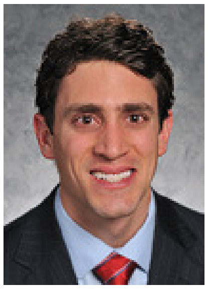
We need to understand how the public perceives the threat. Instead of large-scale public information campaigns, Bucci preferred smaller meetings where government officials could explain to small businesses and civic organizations how to lower their threat profile.

“The biggest vulnerability in our cyber system is the place between our two ears.” Fixing the human part will not solve the problem any more than if we could completely fix the technology part, but we have to do both if we are going to address the big vulnerabilities.

Panel Discussion

A panel of scholars and practitioners addressed the current role of the human element in cyber security policy and implementation and identified areas that should be addressed by the social and behavioral sciences to advance our national security.

Brent Rowe, Senior Economist, RTI International



Rowe summarized the state of social science research relating to cyber security. First, he noted that it is important to understand the interests and motivations of the different stakeholders in cyber security: Large businesses (focused, possibly too much, on regulatory compliance), small businesses (worried about business costs other than security), home Internet users (uneducated about the threat), Internet service providers (do not see a demand for security services, but do see significant costs), software makers (want to be first to the market with their product, regardless of security), and insurance companies (lack data to develop a market for cyber insurance).

Social science concepts have been applied to the study of cyber security. In economic terms, cyber security is an externality—the cost of poor security behavior is borne by everyone, not just the bad actor. There are information asymmetries that affect behavior—some players (e.g., software makers) know more about the security of products than others (e.g., customers). And framing effects affect how individuals and organizations perceive the threats and the effectiveness of countermeasures.

Rowe explained that although usability and economic and psychology research has contributed to our understanding of behavior in cyber space in recent years, there is virtually no social demographic research, and only a few strong case studies exploring how companies respond to cyber threats. Rowe claimed that there is very little rigorous social science analysis.

Rowe argued for companies and the government to push more data into the public domain so research could be conducted on pricing, insurance, and information security education. He advocated for more rigorous cost-benefit analysis to guide policy and educational initiatives and to inform business investment judgments. Interdisciplinary teams of social scientists could contribute to our understanding of the problem and the development of solutions.

L. Jean Camp, Associate Professor of Information Science, Indiana University

Camp argued that technology could assist in promoting more appropriate human behavior through strong communication tools. Warnings generated by operating systems are often incomprehensible and frequently do not appear until after an individual is already at risk. Camp also noted that we need different mental models for conceptualizing and communicating about cyber security—for example, there are differences in the threat presented by worms and viruses on the one hand and state-sponsored cyber warfare on the other. Lumping them together makes risk communication more difficult. The irony is that a computer knows a lot more information about where it is and where it has been than the human being operating it. It would be much easier to comply with the maxim of "use who you know and remember where you have been" if computers were designed to share critical security-related knowledge with the human controlling the keyboard. "You may think you are in a bank, but you could be in a shack in Nigeria. Your computer knows, but you don't."

Robert Mayer, Vice President for Industry and State Affairs, U.S. Telecom Association

Mayer disagreed with James Lewis that the market model of self-regulation is not working. The pace of change in this field is too great, Mayer argued, for regulation to be used as the primary tool for advancing security. Threats are evolving rapidly. Operating systems used to be the key vulnerability; now it is the thousands of applications and updates that are flowing onto mobile devices at an astounding pace.

One key policy issue concerns tradeoffs between privacy and security. Barriers to sharing information about online conduct inhibit security. Organizations cannot disclose information about their members, even though the issues one member is facing could harm others.

Cultural issues and competition between federal agencies is another barrier to cyber security. These problems are even more severe when you consider the conduct of other nations that do not share our values or legal culture. Ultimately we need to face the fact that we deal with nations who do not share our values.

We need a large-scale cost-benefit analysis of proposed efforts to promote security, especially before spending millions of dollars.

Angela McKay, Senior Security Strategist, Global Security Strategy and Diplomacy, Microsoft

McKay stated that more attention needs to be paid to the threat and risk that individuals present to government and critical infrastructures. The "human element" is important because individuals have different frames of reference for dealing with computing devices. Improving security cannot be achieved simply by improving user interfaces—we need to manage the cognitive and memory limitations of the everyday user. We need to have a security system that ensures that the user can do what he or she needs to do on the computer, but also signals vulnerability to a security threat.

McKay listed a number of topics that could benefit from research:

- How do people perceive security?
- How do you help users recognize a "spoof" from a "real" warning?

- What are the differences in the ways demographic groups use computers and perceive security based on age, gender, backgrounds, and ethnicity?

Social science research into these areas needs input and engagement from engineers to be effective.