



European-American
Business Council



Fear Is an Option: Outcomes of the European-American Business Council and Wiley Rein Cybersecurity Conference

By [David A. Gross](#) and [Nova J. Daly](#)

October 2009 | *Privacy in Focus*

On Wednesday, September 30, 2009, the European-American Business Council (EABC) and Wiley Rein co-hosted a conference on "The Coming Cybersecurity Revolution: What Business Needs To Know." Representatives of more than 85 businesses and organizations attended, including executives from Adobe, AT&T, BAE, Dell, Deutsche Telekom, HP, ITT, Jellen Ventures, Lockheed Martin, Microsoft, Motorola, Nokia, Northrop Grumman, NTT, Opticon, SRA, Telefonica Internacional, UBS, Verizon and Yahoo.

The importance of the Internet to business and the global economy is growing rapidly. During the past eight years, the number of global Internet subscribers soared from about 400 million in 2001 to more than 1.7 billion. However, as expert panelists explained during the conference, the term "cybersecurity" is nearly an oxymoron. The fact that nearly \$1 trillion dollars was lost last year as a result of cybersecurity crimes, including the 45.7 million credit cards put at risk as a result of a cyber hack into TJMaxx, paints a stark picture. Nonetheless, there are important lessons learned and important public policies being discussed and developed, both in the U.S. and abroad, that businesses need to be aware of as they seek to secure their cyber infrastructure and information.

The Important Lessons for Business

The first conference panel, led by [Nova J. Daly](#) of Wiley Rein, included Department of Defense (DOD) Deputy Assistant Secretary for Cyber Identity and Information Assurance Robert Lentz; private industry executives from Oracle, Microsoft, BAE, VeriSign and UBS; and consultants from The Laconia Group and the Defense Group Inc. The panelists provided a detailed understanding of the most important cybersecurity issues that every business should consider and how cyber crime is best addressed. Conference participants learned that even though the DOD has thrown the most resources and money into cyber defense, it still has huge volumes of data stolen from its system, and will continue to be under constant attack. And cyber criminals not only try to disrupt business systems, but also seek to steal data over a period of years, and, in some cases, manipulate data to shake customer and business confidence. But government and businesses have learned important lessons, including:

- *Decrease your Access Points and Complexity.* Reduce the number of avenues through which information flows into your system, and, the complexity of your system architecture.
- *Invest in R&D.* Make sure your security system is constantly up to date.
- *Take a Risk-Based Approach.* Protect the most important information with the most resources; but make sure you address all vulnerabilities.
- *Build End-to-End Security.* This is accomplished by controlling identity access (beware of attacks through social networking), by employing secure procurement practices and by knowing your client's vulnerabilities, too.
- *Take Advantage of your Government Resources.* Use groups like [US-Cert](#), the Enduring Security Framework, and sector and government coordinating councils, such as www.it-isac.org/.
- *Stay Alert to Changes in U.S. Laws.* These will affect your costs and your relationships with both customers and others, as well as your privacy policies and responsibilities.

U.S. Cybersecurity Policy: Where It Is Going

The second conference panel, led by [Jim Slattery](#) of Wiley Rein, featured experts from the Federal Reserve Board, the private sector (Jim Lewis of the Center for Strategic and International Studies and HP) and Congress (House and Senate staff, including a keynote address from Rep. Bart Gordon (D-TN)). Congress is currently grappling with 18 new pieces of cybersecurity-related legislation, but none appears likely to pass this year. The Administration has yet to name a head of cybersecurity. However, the big developments that business should anticipate include:

- *Legislative Action.* Passage of a bill is not likely this year, but there will be action in the Committees. Expect action on bills to ramp up strongly for next year.
- *Senate Legislation.* The bills that will be at the forefront of Congressional consideration are S. 773 from Senators Jay Rockefeller (D-WV) and Olympia Snowe (R-ME) (which includes new Presidential powers), and a forthcoming bill from Senators Joe Lieberman (D-CT) and Susan Collins (R-ME) (which would put the Department of Homeland Security (DHS) at the center of cybersecurity policy and give it expanded powers). The two bills differ most in determining who will run cybersecurity policy, the White House or DHS.
- *House Legislation.* In the House, eyes should be focused on Congressmen Dutch Ruppersberger (D-MD) and James Langevin (D-RI), who will hold a series of strategy and budget meetings with officials from federal agencies and private companies. Also, legislation from Rep. Gordon, H.R.2020 (the only bill to pass either chamber this year), proposes a \$3.5 billion investment in R&D and information technology (and would coordinate R&D spending to stimulate collaborations among researchers in institutions of higher education and industry).
- *White House Action.* In May 2009, the White House issued its 60-day *Cyberspace Policy Review*. The report establishes the core policy principles for action and the position of cyber coordinator. However, a coordinator has not yet been named. Until a cyber point person is named, Administration progress will be slow but important.
- *Federal Government Action.* Federal agencies are building their cybersecurity abilities and defenses. DHS is in the process of reorganizing itself and building capacity. It just

announced its intention to hire 1,000 cybersecurity experts over the next three years. Businesses should also be aware that the government is reviewing its procurement practices, and this could affect government contracts.

- *Privacy Issues.* Privacy issues have plagued federal government efforts. While DOD has the best protections for its systems, those systems cannot be used by other agencies or the private sector. However, that issue is at the forefront of government policy discussions, and business should become engaged when outreach occurs through future public-private partnership initiatives.

International Cybersecurity Policy

The third conference panel, led by [Ambassador David A. Gross](#) of Wiley Rein, included experts from the U.S. State Department, the Embassy of Estonia and the private sector (Telefonica and Verizon). Given the global nature of the Internet, international criminals and rogue state actors potentially can gain access to any company's electronic information, both domestic or multinational. While efforts are being taken to secure U.S. networks, international efforts must find cooperation and convergence in order to attack the problem holistically. The U.S. is reaching out to its international partners, and so are U.S. businesses. Actions are being discussed and taken on the global stage that will have a direct impact on the costs that U.S. businesses incur, and the policies they should adopt. Some big considerations include:

- *International Consensus.* The international community is developing a consensus around five pillars of cybersecurity action, with each country building: 1) a national security response team, 2) informed legislation, 3) public-private sector awareness and public awareness, 4) strong enforcement and 5) capacity building.
- *Fragmentation.* Multiple international organizations and other groups are addressing the challenge of cybersecurity, including the Organization for Economic Co-operation and Development, Asian Pacific Economic Cooperation, the International Telecommunication Union and the Internet Governance Forum, but there is no movement on a single broad agreement. Encryption standards have caused particular fragmentation.
- *Congruence.* There is broad agreement to work on global issues regarding child protection, but it is often hard to reach consensus on other, more controversial issues. There is important work being done by various international standards bodies that is having a significant effect on technical cybersecurity issues. Panelists agreed that the efforts work best when they are primarily private sector driven.
- *U.S.-EU Cooperation.* Areas of cooperation include: 1) research, 2) identity management and 3) protection of Internet protocols. In March, the EU launched an initiative to enhance its networks.
- *Openness vs. Security.* Panelists agreed that the center of debate hinges on the balance between having an open system and having strong national security protections.

Conclusion

Finding the right balance between openness and security, as well as between privacy and protection is at the core of cybersecurity policy debates in the U.S. and globally. The issues surrounding cybersecurity must be addressed quickly but carefully. Every day, domestic and international businesses suffer countless intrusions and attacks on their networks, resulting in the loss of extremely sensitive data and high-value intellectual property. However, business and

government are finding areas of convergence and best practices, and companies benefit significantly from proactive measures.

Perhaps most importantly, there was complete consensus among all the panelists that because all companies are affected by cybersecurity, privacy and related issues, it is critically important that they take action—especially in the areas of legislation, regulation, industry best practices and self-regulation, as well as increase involvement in international decision-making forums, because the stakes are extraordinarily high, and those organizations that help make the rules will benefit.

For more information, please contact [David A. Gross](#) at 202.719.7414 or dgross@wileyrein.com and [Nova J. Daly](#) at 202.719.3282 or ndaly@wileyrein.com.