

President
Kris Matula

Vice President
Don Hutson

Secretary-Treasurer
Michael Drury

Executive Director
David M. Kemme

Executive Committee
Gene Huang
Kris Matula
Don Hutson
Michael Drury
David M. Kemme

Board of Directors

Class of 2012
Ralph Faudree
John Fowlkes
Ashley Mayfield
David Waddell

Class of 2013
Larry Cox
Rick Duerr
Carl Ring
Elizabeth Rouse

Class of 2014
Susan Scheidt Arney
Steve Bares
Beth Flanagan
Scott Fountain

Melissa Hathaway, President, Hathaway Global Strategies, LLC
By Jane Schneider

The scenarios cybersecurity expert Melissa Hathaway sketched during her talk before Economic Club members on October 27th, sounded like topics lifted from a sci-fi thriller: stolen identities, destructive worms, massive credit-card fraud. Yet, such threats are far more real today than many consumers and business owners realize. As global reliance on the Internet grows, so does the severity of security breaches which are increasingly placing consumer, corporation, and government information at risk. These threats, said Hathaway, are destined to become more frequent as global networks migrate to mobile technology.

Melissa Hathaway, an American University graduate who was the director of the Joint Interagency Cyber Task Force during George W. Bush's administration, and served on the National Security Council under Barack Obama's administration, used the forum to shed light on the variety of ways in which cyber espionage is taking place today and why it is of national concern.

The Internet, which Hathaway characterizes as America's largest export industry, is now home to a staggering 2.5 billion users. Users send 100 trillion emails annually (89 percent of which are spam, said Hathaway), conduct 34,000 Google searches per second, and download one video per second. (This figure will increase dramatically in the next decade, as business begins to transition from email communication to video). But as commerce hums on the Internet, so does the business of espionage, with an estimated 150,000 bots coming online every day, designed to take over computers and use them for malicious activities.

"The largest problem is awareness. People don't understand, as we adopt these technologies, where the vulnerabilities might be," she said. "And how porous our industries are to that exploitation by criminals."

In 2007, Hathaway led the comprehensive National Cyber Security Initiative for President George W. Bush. The initiative was created to address the federal government's increasing loss of intellectual property. During her six-month tenure with the Obama administration, President Obama pushed to make the federal government's Cyber Space Policy Review more national in scope, so as to beef up government and business computer systems and making them more resilient to attacks. Cybersecurity is considered one of the most serious economic and national security challenges being faced by the country today.

During the first part of her presentation, Hathaway described the various ways in which networks are being corrupted, from employees using thumb drives to export or import information, to infections being secretly encrypted onto large files and passed along to unsuspecting employees. Business executives traveling through foreign countries even run the risk of having malware coming into their computers when using public terminals in airports. Smart phones are also a huge problem, since they can be vulnerable via blue tooth when email is in use.

The example she cited was that of T.J. Maxx employees who were communicating transactions using a mobile device. The information was intercepted by criminals who were sitting in the parking lot using wireless networks to collect the data. From this and other incidents, the discount retailer lost the personal credit card data of some 45 million consumers. The information of millions of credit cards can be a potential gold mine to thieves. The T.J. Maxx incident (which took place over many months) is believed to be among the largest breaches of consumer information to date. The company was found to not have adequate security safeguards in place to protect customer information and paid restitution.

The loss of customer debit or credit card data by companies like TJMaxx, Citigroup, and others are leading to class action lawsuits, as consumers hold companies more responsible for the insecurity of their networks. Another issue raised by Hathaway is that companies like Google, one of the world's leaders in handling big data, are not held accountable when accounts are hacked and information stolen. A recent article in Atlantic Monthly by James Fallow reported that when his wife's Gmail account was hacked (with the potential loss of more than four years' worth of correspondence and images), the company's initial response was cut and dried: "Read our Security Checklist," followed by a terse reply which read, "Unfortunately, we will not be able to respond to any further emails on this case." Since Fallows had had professional dealings with Google executives over the years, he forwarded the details of his debacle and Google's response to Michael Jones, Google's "Chief Technology Advocate." A week later, his wife got her messages back. But in reporting the story, he learned that such security breaches are ongoing for many companies, and often accounts are vulnerable due to lax security practices on the part of both consumers and companies.

What's more, business and consumers aren't the only ones at risk for identity theft. In the past two years, children and teens have become the latest targets for hackers, entering through gaming devices like Xbox. Hathaway said several friends of hers had teens that had become of legal age, only to learn that they had already amassed huge debt from their social security numbers being stolen. What's more, parents often don't discover this until their child turns 18 and begins to apply for credit. (Her recommendation to parents is to contact allclearid.com, which will conduct identity scans for no charge.)

As security issues continue to mount, Hathaway said the country will need to shore up the supply of technicians currently educated in cybersecurity issues. One bright spot in her address was a nod to the University of Memphis' Fogelman College of Business and Economics, which offers a degree in information security. UM is only one of 125 schools nationally offering such a program.

Throughout her presentation, it was clear that knowing how to secure computer systems against hackers will provide long-term job security to those who do it well.