MEDIA CHALLENGED BY CHANGING NATURE OF CYBERCRIME

The global proliferation of cybercrime and how to better protect confidential, digital information were top of mind at the 2008 Workshop on the Economics of Information Security (WEIS) hosted by the Center for Digital Strategies (CDS) at Dartmouth's Tuck School of Business.

More than 100 information security experts, academics, researchers, reporters, corporate executives and government officials attended the lively three-day conference. Participants from China, Italy, Germany, Canada, Australia, Denmark, Japan, Sweden, Switzerland, the United Kingdom and the United States attended the annual meeting.

Academic and corporate researchers presented 22 papers and made informal presentations throughout the meeting which was sponsored by CDS, the Institute for Information Infrastructure Protection (I3P), Dartmouth's Institute for Security Technology Studies and Microsoft.

Reporters from USA Today, BusinessWeek, CIO Magazine, ZDNet Magazine and Tech Target took part in a provocative panel discussion, providing a fresh perspective on key issues relating to the economics of information security.

"Much of our work and the work of security colleagues wasn't front page news five or 10 years ago, but now there is a steady drumbeat of stories of breaches and identity thefts," said Prof. M. Eric Johnson, director of the Center for Digital Strategies and the media panel moderator. "This (reporting) has a huge effect on public perception around security, on public policy making and around funding the kinds of research we might undertake."

Stories detailing identity theft and personal computers being infected by 'bots' and malware are making headlines every day. Cyber criminals based in Eastern Europe, Russia and China are busy stealing and selling sensitive information, according to panelists. Massive data breaches, ranging from the theft of thousands of credit card account numbers from retailer T.J. Maxx, to the French trader who misdirected funds at Societe Generale, are keeping reporters busy.

"From my perspective, the next great business story is the business of cybercrime," said Brian Grow, who covers cybercrime for BusinessWeek magazine. "It's the fastest growing crime in America and in the world. The numbers have exploded….so, from a media perspective that makes it relevant because it affects millions of people."

Reporters said their challenge is twofold; selling the cybercrime story to their editors and trying to persuade corporations and law enforcement officials to help them expose the alleged scams. They said many corporations are reluctant to discuss embarrassing data breaches, despite new laws requiring them to report problems to law enforcement agencies and the public.

"It's easier to get sources in the criminal underground (to talk to us) than it is to get the law enforcement, the government and the business sources to talk about it," said Scott Berinato, formerly a reporter for CIO/CISO magazines. He is now with Harvard Business Publications.

The panelist said companies often choose to keep the data breach a secret rather than risking a negative reaction from investors or a public relations nightmare.

"It's only through public awareness that the public will put pressure on the bottom line of corporations to make that change," said Byron Acohido, of USA Today. "Otherwise, they'll just do an accounting trick and assign it as an acceptable loss and spread it out. They (corporations) are assigning a very low premium to the ongoing threat of my Social Security number being out there with 300 million people in a stored database that the bad guys are just doing low level stuff on now and can figure out what else to do in the future."

"The credit bureaus in particular are wide open for reform," continued Acohido. However, the industry is resisting change and the public seems to be apathetic when it comes to demanding more security. He said consumers are also "addicted to convenience" and often release personal information and conduct business online without adequate security precautions in place.

Dennis Fisher, a reporter for Tech Target, said he realized that companies need to focus on security in general, not just protecting information. Fraud is committed in many ways, not just by hacking into computer systems.

"Once I understood the fraud triangle; opportunity, motivation, rationalization, that started to bring to light that all of these cybercrimes were just fraud," said Fisher. "Somebody wants to make money, and so my physical security reporting really helped me write stores which I think the general public understood better because I was just talking about fraud."

However, he said it's tough to get people who have been defrauded to discuss what happened.

"They have a hard time dealing with it and they don't want to talk about it," he said. "But every once in a while, you come across a person whose method of dealing with it is to open up and talk about it. They feel like they are helping to solve the problem by making others aware."

Even when a so-called victim of a computer fraud is willing to be interviewed, Fischer said most corporations are reluctance to publicize a data breach because they don't want bad publicity. "Businesses have this beautiful thing called accepted loss budgets, so they just kind of bury their shame in the acceptable loss budget."

Despite the fact that many computer fraud stories still go unreported, BusinessWeek's Grow said "it's an endless story because it's going to take on new forms and going to shift and we're going to continue to say,' here's how they tricked you."

Apart from fouling up computer systems with Trojans, 'bots' and malware, computer crime is now a national security issue, according to BusinessWeek's Brian Grow. He shared a recent story he covered about an email with a malicious attachment that was made to appear as if it came from the Secretary of the Air Force.

"It was aimed at a military procurement guy at a consulting firm and it contained a request for proposal from the Indian government for 126 fighter jets…the real bid that Boeing and others were bidding on."

Clicking on random email is the quickest way to infect your computer system, according to Ryan Naraine, a reporter for ZDNet Magazine.

"It's fascinating to me that people still just click and install stuff," he said. "They'll install a Trojan for you…you can tell someone, 'here's Britney, she's half naked, click here and people just click."

TechTarget's Fisher said a friend recently sent out two emails to test response rate.

"In one, he said, 'this is a bad email with an attachment,' and the other he said, 'this is a bad email with an attachment, click here.' Naraine said the click rate for the bad email that ordered people to 'click here" had a response rate about 80 percent higher than the other one.

One strategy to protect digital information is to require several types of authentication before allowing access to any sort of sensitive information.

"The Europeans and the Asians to some extent are already several steps ahead of us," said Byron Acohido. "We're still locked at this level, essentially by and large, single factor, username and password. That's really all you need to open all the doors and windows you want on U.S. accounts."

Jane Applegate

PR & Marketing Manager
Center for Digital Strategies