

#### CYBERSECURITY: A SPECIAL REPORT

#### Recent cyberattacks

Oct. 2

JPMorgan Chase says e-mails and personal information from 83 million households and businesses were

compromised when hackers infiltrated networks.

#### Sept. 18

Home Depot says hackers may have put 56 million cardholders in jeopardy.

#### Aug. 18

Hospital group Community Health Systems says a hacking group believed to be from China used advanced malware to steal the personal data, including Social Security numbers, of 4.5 million patients.

#### Aug. 4

Restaurant chain P.F. Chang's confirms a threat detected by the Secret Service involving stolen credit and debit card information at 33 of its locations.

#### July 23

Six people are indicted in connection with the hacking of more than 1,600 user accounts and fraudulent purchases worth more than \$1 million on the ticket-reselling site StubHub.

#### June 24

The Montana Health Department notifies 1.3 million people that their personal data was stored in a state computer hacked a year ago Compromised records include Social Security numbers, bank account numbers, health diagnoses and drug prescriptions.

#### May 21

EBay advises its 145 million users to change their passwords after attackers stole encrypted passwords and gained access to its corporate network.

#### Jan. 10

Retailer Neiman Marcus confirms that it is working with the Secret Service regarding a breach of customers' credit card information. The retailer later acknowledges that the hacking occurred for several months and involved 1.1 million credit and debit cards.

#### Dec. 19

Target confirms a data breach of credit and debit card information of up to 40 million customers. The company later says the thieves may have lifted information from up to 70 million more customers

- Compiled by

#### **EDITOR'S NOTE**

#### Cyber attackers have the upper hand



Mary Jordan

government are spending billions of dollars to try to lock down valuable information they store in computer networks, but thieves and spies continue to steal

U.S. companies and the

everything from credit card numbers to plans for nextgeneration military firepower.

Every week we hear of a new breach. The recent cyberattacks against JPMorgan Chase not only gave hackers access to tens of millions of e-mails and home addresses of its customers, but may have been aimed at trying to disrupt Wall Street, Home Depot, Target and other merchants recently have been hit and chief executives have moved

cybersecurity to the top of their agenda, according to speakers at The Washington Post's Cybersecurity Summit on Oct. 1. Excerpts from that forum are on pages 4 and 5 of this special report.

Arati Prabhakar, the director of the Defense Advanced Research Project Agency (DARPA), the government agency that brought the world computer networking, said a \$2 million prize awaits the winner of the Cyber Grand Challenge, a competition aimed at building an automated system that can secure software and detect harmful flaws

Today's attackers have the upper hand because they have the "inexpensive task of finding a single flaw to break a system," DARPA says. "Defenders, on the

other hand, are required to anticipate and deny any possible flaw - a goal both difficult to measure and expensive to achieve. Only automation can upend these economics."

As we await a better system to secure our networks, the current "patch and pray" approach is a gift to the bad guys. Hackers in Russia and China are behind many of the attacks on the U.S. government and companies, say cyber experts, including James Lewis, whose article in this report says the Wild West of cyberspace needs law and order and needs it now.

House Intelligence Committee Chairman Mike Rogers (R-Mich.) said there is a lot of debate about how aggressive the U.S. government should be in using its offensive cyber power.

"You don't want to reach overseas and flick somebody in the forehead if we're not exactly 100 percent sure that that was the perpetrator of that particular event," he said. "If you start this digital vigilantism about, Well, I got hacked. I'm going to go do something about it,' you could create a storm here, of which the rest of the network — that 85 percent [controlled by the private sector] — is not prepared to handle."

By the end of this year, the United Nations estimates that 3 billion people will be online and as each of us puts more and more of our lives in cyberspace — including bank information and health records everyone has a stake in the race to make the Internet more secure.

mary.jordan@washpost.com

## The ethics of Hacking 101

BY ELLEN NAKASHIMA AND ASHKAN SOLTANI

At the University of Tulsa, professor Suject Shenoi is teaching students how to hack into oil pipelines and electric power

At Carnegie Mellon University in Pittsburgh, professor David Brumley is instructing students on how to write software to break into computer networks.

And George Hotz, a largely self-taught hacker who became a millionaire in part by finding flaws in Apple and other computer systems, is now back in school, where he's one of the stars on Carnegie Mellon's competitive hacking team.

Shenoi, Brumley and Hotz are players in a controversial area of technology: the teaching and practice of what is loosely called "cyberoffense." In a world in which businesses, the military and governments rely on computer systems that are potentially vulnerable, having the ability to break into those systems provides a strategic advantage.

Unsurprisingly, ethics is a big issue in this field. Both professors say they build an ethics component into their curriculum; Shenoi won't even accept students who don't promise to work, if hired, for the National Security Agency, the Energy Department or another U.S. government

But some experts say the academic community is not taking ethics seriously enough, and professors are not accepting responsibility for the potentially dangerous skills they are teaching.

The very nature of hacking means that a lot of its skills and standards evolve outside academia. (Hotz, known in tech circles by the handle "geohot," says he learned most of what he knows on the Internet "and from playing with things.") This leads advocates of teaching cyberoffense to say that the "good guys" have to keep up — which in turn raises more questions about whether such education is morally right.

"There's a very large stigma around saying we do anything offense-related," said Tyler Nighswander, 23, a computer science graduate student at Carnegie Mellon. "It's certainly understandable that you don't want to say your school teaches offense - 'Oh, you mean you teach kids how to break into computers and steal stuff?'

Some academics note that it may be too late to stop the worldwide expansion of offensive cyber tools and techniques.

"There is an escalating arms race in cyberspace as governments, companies and malicious actors are all going on the offensive, most of it under a shroud of secrecy and absent any meaningful political oversight," said Ron Deibert, director of the University of Toronto's Citizen Lab.

#### Seeking 'vulnerabilities'

No more than a handful of professors have the knowledge and resources to teach cyberattack skills at the level of Brumley or Shenoi, whose students are heavily recruited for government and industry positions.

At Tulsa, Shenoi, 54, obtains permission from energy companies for his students to attempt to hack into them, infiltrating the systems that run gas pipelines or power grids and gaining access to critical U.S. infrastructure. They also do penetration testing for other companies, finding "vulnerabilities," or flaws, that enemy hackers could

"We have a class where we teach people how to write things like Stuxnet," Shenoi said, referring to a computer worm, reportedly developed by U.S. and Israeli scientists, that was found in 2010 and damaged about 1,000 centrifuges in an Iranian uranium-enrichment plant, delaying the country's nuclear program. Stuxnet, whose deployment is often considered the first true use of a cyberweapon, was built around an unprecedented four "zero-day exploits" — that is, attack tools based on previously unknown soft-

Shenoi began teaching courses on offensive computer techniques in 1999, he said, and by 2008, Tulsa was offering an entire program. Now, he said, there are "four courses in reverse engineering, two



Brian Pak, left, founder of a recreational hacker team called PPP, made up of current and former Carnegie Mellon students, participates in the DefCon 22 "Capture the Flag" competition in Las Vegas. His team won.

in cyber operations, two in offensive U.S. government. SCADA [supervisory control and data acquisition], and one on malware analysis and creation."

Shenoi said that the potential power of offensive cyber techniques is so great that he accepts only students who intend to work for the government and who have records that would qualify them for government security clearances. He interviews all the applicants as well as their parents. He sends 15 to 20 students a year, he said, to work at the NSA or the

"In order for me to teach these realworld attack skills, these students have to be trusted," he said. "They cannot go to work for the private sector.

"There's no reason to teach privatesector people how to use Stinger missiles," he continued. Similarly, he said, you don't teach them to use cyber weap-

Brumley, 39, has taught offensive cyber skills since 2009. A self-described "patriot," he says he discusses ethics in his classes at Carnegie Mellon — an introductory computer security course as well as more advanced vulnerability analysis. Some of Brumley's students work for the government, but most go to start-ups, big companies such as Google or defense contractors.

To develop their skills, Brumley encourages his students to compete in hacking contests. In August, a recreational team he advises called PPP, made up of about 20 current and former Carnegie Mellon students, won the ultimate U.S. showcase of hacking skills at the DefCon hacking conference in Las Vegas — a "capture-the-flag" competition in which 20 teams tried to break into one another's computers.

PPP's top gun is Hotz, who gained fame in 2007 for "jailbreaking" the previously impenetrable iPhone. He left Carnegie Mellon as a 23-year-old sophomore to work on his own, and is now back as a junior at 25. Hotz is so skilled that he has won some contests solo — as in July, when he beat nine teams to win \$30,000 at the SecuInside competition in Seoul. He earned \$200,000 in April for finding bugs in Google's Chromebook computer and the Firefox browser. Brumley calls him "a machine." Hotz boasts that he is "maybe the best hacker in the world."

#### A question of profit

Obviously, these students are developing valuable skills. Shenoi says his students never make money off the vulnerabilities they discover or exploits they develop. They give the information for free to the companies whose systems they are testing, or to the government. Intelligence agency officials fly every so often to Tulsa to be briefed on the flaws the students have found.

Brumley agrees that it is dangerous to share vulnerabilities or exploits with anyone but the software vendor or the

"If you're selling exploits in a free market," he said, "then you're potentially selling them to the adversary."

Nighswander, a former student of Brumley's, said that he has never sold a vulnerability to a software vendor, but that he thinks it's ethical to do so, saying, "When you think that finding a vulnerability can take weeks and months, you can understand that the person wants to get compensated."

Hotz declined to say whether he has sold an exploit (although he was caught last year on a surreptitiously recorded conversation appearing to broker a \$350,000 deal to sell exploits to jailbreak the iPhone to a Chinese company). "I have never worked with any country

aside from the U.S.," he said. He says he doesn't dwell on issues of morality, saying, "I'm not big on ethics."

Brian Pak, 25, who created the PPP hacking team while studying under Brumley and now works for a start-up he cofounded, said that sometimes. noodling around on his own, he finds

bugs in software and discloses them to the software vendor. He said he has never sold information about flaws, although some vendors offer "bounties" of up to several thousand dollars. He holds onto some vulnerabilities for use in research a practice common among security researchers, he said.

"I also don't think it's unethical to provide vulnerabilities or exploits to the U.S. government," Pak said. "I trust the U.S. government. The government protects me. As long as it's not used against our own people, I see less of an issue."

But some experts disapprove of providing previously unknown or "zero day" vulnerabilities to the government whether for free or for profit. They worry that, rather than disclosing these zero days to vendors, the government is stockpiling them for use against adversaries. Doing so would leave the software vendors ignorant of dangerous flaws in their products, making the Internet less secure, they say. They also charge that the government is using these tools with far too little public debate, for example, in the controversial area of domestic law enforcement.

Christopher Soghoian, chief technologist for the American Civil Liberties Union, said the government should have a policy of promptly disclosing any bugs it discovers so that software companies such as Microsoft can fix them before they cause damage. Not doing so can undermine network security, he said.

But Brumley said such a blanket policy would be unwise.

"The obvious example is Stuxnet," which destroyed Iranian centrifuges, he said. That, he said, was "an opportunity to use an exploit for good."

"Twenty years earlier, that would be the thing that we flew in bombers and bombed factories for, and people would die," he said.

#### **Dual-use tools**

Selling exploits and vulnerabilities is not illegal, per se, but selling them with the intent that they'll be used to hack someone else's computer is a crime. Software is a classic "dual use" product. It can be used to do something as innocuous as unlock an iPhone to allow consumers to switch providers or as destructive as causing an adversary's nuclear centrifuges to spin out of control.

Some academics say the teaching of hacking techniques should remain limited.

"I'm personally against the widespread or wholesale teaching of offensive cvber," said Arthur Conklin, associate professor of information and logistics technology at the University of Houston. For one thing, he said, vetting students for trustworthiness, as Shenoi does, would be impractical on a mass scale.

Giovanni Vigna, a computer science professor at the University of California at Santa Barbara, warned that not teaching offensive skills is "not a very smart option because the bad guys are going to develop them anyway." He added, "The key is to make the students understand what are the lines that cannot be crossed." So he integrates into his courses on offensive cyber "a very substantial chapter on ethical issues."

Some experts argue that the government should regulate the sale and use of offensive cyber technology — but others, including Shenoi, say regulation will only drive the market for such products deeper underground. At this point, the U.S. government is in the process of placing export controls on some hacking and surveillance tools. It already has forbidden the sale of such technologies to countries with particularly egregious human rights records, such as Sudan and

Meanwhile, interest in offensive cyber skills is growing. Experts estimate that several thousand personnel in private industry work at finding bugs and building exploits. More companies are training employees in offensive skills, and more people are competing in hacking competitions.

In this context, Soghoian of the ACLU fears that universities are teaching students high-end skills without a solid ethical foundation.

"The academic computer security community has not yet realized the role they are playing in cyberwar," he said.

Shenoi said that, above all, he wants to impress upon his students the responsibilities that come with their technological prowess.

"They have great power to do harm. They have power to intimidate. They have power to accrue money illegally," he said. "What I tell them is, 'You may be learning some potentially deadly skills. But use them gently and wisely, and use them for the good of society."

ellen.nakashima@washpost.comashkan.soltani@washpost.com

## Lassoing the Internet's Wild West

Taming lawlessness is tough amid worry that rules will harm 'free, open' Internet

BY JAMES ANDREW LEWIS

When Americans think about cybersecurity, they tend to focus on symptoms rather than causes — it's a symptom when almost every month a major company is hacked and millions of personal records are stolen. We pit weak defenses against skilled opponents. Changing this won't be easy, because there is no automatic fix, no new technology and no private action that can stop cybercrime and tame the Internet's Wild West.

First, we must recognize that most malicious actions in cyberspace directed against the United States come from hackers in two countries: China and Russia. These nations encourage their hackers to go after networks, data and money in the United States, and they protect them from prosecution. Russia allows criminal groups to steal from Western banks (Russian-speaking cybercriminal gangs can perform hacks as well as most intelligence agencies). The Chinese prefer to use military units to steal intellectual property for everything from the plans for the F-35 fighter jet to the formula for house paint.

That the United States' most active opponents in cyberspace are China and Russia (along with up-and-comers Iran and North Korea) is not a coincidence. These countries are our military rivals. Cyberspace creates opportunities to exercise national power, and these nations have seized those opportunities. Viewing the United States as their opponent, they skillfully exploit the Internet to gain advantage. This is not a cold war. In fact, it is not war at all. Our opponents have been careful not to use hacking for real attacks on the United States, as doing so would trigger a damaging response and get in the way of business.

In turn, these and other countries would say the National Security Agency is equally at fault. The problem is the same for everyone. All countries now depend on cyberspace, as it is built into every important part of the global economy. Better cybersecurity requires that nations agree on the norms and rules for responsible behavior in cyberspace, both for states and for powerful companies. Agreement is possible even among adversaries, as there is shared interest in making our digital economic backbone stable and more secure.

The idea of formal cooperation among governments is anathema to the old-school Internet community. The fear is that rules will harm the "free and open Internet" to which all kinds of miraculous economic powers are ascribed. It's true that the global network has brought us immense economic benefits and offers still more. However, the free and open Internet is long gone. Consumers are



MICHAEL S. WILLIAMSON/THE WASHINGTON POST

locked into vendors' "walled gardens" where choice is restricted, and privacy vanished well before former government contractor Edward Snowden leaked classified NSA information. Hacking remains far too easy and its costs are rising far too rapidly to stick with the laissez-faire approach.

To make cyberspace safe, we need something like Bretton Woods. After repeated financial crashes (the last of which, in 1929, led to global depression and war), the United States and its allies created the Bretton Woods system to establish transnational rules, norms and institutions to manage and reduce risk for global finance and trade. We can do the same for cyberspace. This does not mean creating a one-ring-to-rule-themall Internet body, nor does it mean an all-government approach. It means agreement on a collective approach to reduce risk and follow principles for stability. The Bretton Woods system was not perfect, but it was better than the chaotic national approaches that preceded it. Some countries will balk at following the rules - as they balked at rules against nuclear proliferation or moneylaundering — but the right blend of incentives and penalties (such as indictments in U.S. courts) will help change

Agreement on rules would ultimately reduce risk, and in a perfect world, international accord on cybersecurity would be enough to protect us. But reaching such an accord won't be easy or quick. The same way that banks rely on the police but still need vaults and guards, companies will need to do more to protect themselves and their customers. Most network breaches still require only simple hacking techniques.

The Obama administration favors a voluntary, standards-based approach (a time-honored American solution) to cybersecurity using the National Institute of Standards and Technology's new Cybersecurity Framework, but it has hinted at regulation if companies do not act. The framework sets minimum levels of cybersecurity, and companies can expect auditing firms to evaluate how secure their networks are and use that information in annual audits and shareholder reports.

Company liability also will create powerful incentives. A hacked company could face lawsuits from shareholders and customers if plaintiffs can show that it did not implement the framework. The framework has inspired other countries to set cybersecurity standards, and a single global approach to cybersecurity would be better than having each country design its own.

Like it or not, the pioneering days of the Internet are over. In the iconic American film "The Man Who Shot Liberty Valance," a mild-mannered lawyer supplants a larger-than-life cowboy who pioneered the West. There's an understandable reluctance in the movie to see heroic, self-reliant cowboys replaced by The FBI building in Clarksburg, W.Va., houses the National Instant Criminal Background Check System. These back-up tapes are part of the system, which can perform 8 million checks

3 billion

per day.

The number of people who will be online by the end of this year, according to the United Nations lawyers, but there also is a recognition that society has outgrown the pioneer phase and that it's time to move to a world ordered by the rule of law. And there is a similar reluctance to acknowledge that cyberspace has matured and that taming the cyber Wild West means extending the rule of law — internationally and domestically, existing laws and maybe some new ones — and creating institutions to enforce them. This means frameworks, international agreements, standards and formal oversight.

Getting the rule of law in cybersecurity requires collective action, nationally and internationally, and for now, that still requires U.S. leadership. Unfortunately, this may be impossible in Washington today. The political consensus that let this society build superhighways and the Internet is fractured. Until a new political consensus is forged, progress in cybersecurity will be slow. Cybersecurity is a good test of whether the United States has the resolve and the skills to maintain the world order it created decades ago. We may fail, in which case cybersecurity will be just another part of a larger unraveling of international peace. While Washington struggles to redefine its social contract, we should expect uncertain responses, half-measures and hacking.

JALewis@ csis.org

Lewis is senior fellow at the Center for Strategic and International Studies.

# With mobile devices, firms playing Russian roulette on security

BY AMRITA JAYAKUMAR

As head of a Michigan-based cybersecurity firm, Larry Ponemon has studied data breaches including the hacking of Target credit cards, and Chinese and other international cyber espionage. But his favorite incident, he says, was small, avoidable and probably victimless.

It involved a doctor and a tablet (tablet as in iPad, not medication). The physician's health-care network had just upgraded its data storage system, and he was given an iPad that he could carry from the hospital to his home in which he collected patient information that would go directly to a cloud-based bank of medical records.

Then, a few months ago, he lost the

Even more unfortunately, the device wasn't protected by a password. That gave anyone who found (or had stolen) it access to what Ponemon calls "a treasure trove" of personal data on as many as 1 million patients.

Why no password? "Doctors and clinicians have a history of not using passwords because they're busy people," Ponemon said. The health-care network's IT people had "jailbroken" the tablet's software to eliminate its password requirement, making it easier for the doctor to use. And easier for criminals to charge

That illustrates a conflict of interest not only in the health-care sector, but throughout the worlds of business and government. Management loves that it can get flexibility, mobility and efficiency out of new technology, and that tablets and smartphones mean employees can work from home — or anywhere.

But every mobile device is a potential chink in the armor of an entire organiza-

tion; any security lapse places at risk not just the device owner's private data, but potentially sensitive information about his or her company and other patients, customers or clients the company serves.

Employees often take shortcuts for the sake of convenience. And often companies, which benefit from increased productivity that mobile devices give their employees, don't effectively install or enforce security measures.

In 2013, Verizon analyzed more than 63,000 "security incidents" in 95 countries and found that the loss or theft of laptops, USB drives, phones and other devices, coupled with human errors — including sending sensitive e-mail to the wrong address or uploading private data to a public server — were responsible for 39 percent of the incidents. In its annual Data Breach Investigations Report, Verizon said that many of the rest of the incidents were malicious, but only 2 percent resulted in someone accessing the stolen data for criminal purposes.

The doctor who lost his tablet did have a "kill switch" that was activated when he reported it missing. That meant the hospital network would be alerted if the device was turned on.

Health-care records contain valuable information: the patient's name, Social Security number and date of birth. So anyone who got access to the records could, for instance, use that information to try to open a line of credit, submit fake claims for benefits, or sell the data to others for those purposes.

"So many of the breaches we study are so complicated," Ponemon said. "In the case of the doctor and the iPad, it was such a low-tech issue, but had potentially very significant ramifications."

The quality of the data may be one reason the health-care sector suffered



JUSTIN SULLIVAN/GETTY IMAGES

Verizon analyzed more than 63,000 "security incidents" in 95 countries and found that the loss or theft of laptops, USB drives, phones such as the Apple iPhone, pictured above, and other devices, coupled with human errors, were responsible for 39 percent of the

incidents

the largest share of cyberattacks in 2013, more than any other sector such as retail, education or finance, according to a report by the Identity Theft Resource Center, a nonprofit organization that tracks data theft.

Two laptops stolen from a New Jersey office of medical insurer Horizon Blue Cross Blue Shield last year contained unencrypted data on more than 800,000 patients. No incidents have been reported as fraud, but patients were offered free credit monitoring and identity theft protection services.

Last month, the Cedars-Sinai Medical Center in Los Angeles disclosed that the unencrypted records of 33,000 patients had been stored on an employee's laptop, which was stolen in a burglary over the summer. The unprotected information included names, driver's license numbers and Social Socurity numbers

bers and Social Security numbers.

Despite the increasing use of mobile devices outside the workplace, few organizations have clear policies for data security, a recent Ponemon Institute survey found. Of the 618 IT managers surveyed for the report, 29 percent said their organizations had no strategy to ensure mobile device security. Others

said their strategies covered only certain types of devices or operating systems.

One method that organizations use to secure mobile devices is known as "sandboxing." That means employees are allowed to work only within secure, walled-off sectors — or sandboxes — when using mobile devices.

Another approach is "virtualization," in which the mobile device doesn't store any information while performing a task. Virtualization software uses the mobile device the way a projector uses a screen: While an employee is logged on, information from the company's servers is "projected" onto the screen, but none of it is stored there. When the task is completed, it's as though the projector has been switched off — so if the device is hacked, there won't be any information to steal.

David Wennergren, senior vice president of technology policy at the Professional Services Council, a trade group, said the big question now is, "How do we allow people to share the information they need versus protecting privacy and security? The smart money is on finding the sweet spot between security provisions and convenience."

amrita.jayakumar@washpost.com

#### **CYBERSECURITY: A SPECIAL REPORT**



## Building the unhackable system

#### **Arati Prabhakar**

Director, Defense Advanced Research Projects Agency

he moon shot for cybersecurity in my view is to find techniques that scale faster than this explosion in information.... A combination of fundamental advances has the potential to get us to a place not where we never have a cybersecurity problem, but where it's manageable and we can get on with our lives.

Our mission today is still about breakthrough technologies for national security. What we're asking about

cybersecurity is, "What are the technology concepts that could fundamentally change the ground rules and give us a way to get out ahead?"

We're working on ways to build unhackable embedded systems. I hope you will see that rolling out into automobiles in the commercial sector and UAVs [unmanned aerial vehicles] in the national security context. I hope after our Cyber Grand Challenge that you start to see automated cyberdefense systems that become commercial products that people who are worried about their own cybersecurity can purchase and start using



PHOTOS BY KATE PATTERSON FOR THE WASHINGTON POST

Dana Priest, a national security reporter for The Washington Post, interviews, from left, government cyber experts Christopher Painter, John Carlin and Eric Rosenbach as part of The Post's Cybersecurity Summit.

#### **Sparking global interest**

#### **Christopher Painter**

Coordinator, cyber issues, State Department

The consequence of cyber being the new black [in the United States] where everyone cares about cyber and everyone wants to talk about cyber — is increasingly happening around the world. As you get countries doing national strategies around cyberspace, as you get them paying more attention to this, as you get them reaching out and saying, "How can we build these more cooperative frameworks against these threats?" I think that's helpful to us all.

Now people understand it's a major national security issue . . . an economic security issue, human rights issue and foreign policy issue. Getting other countries to get to that same level is one of the challenges. But more and more

#### Going after the money

Assistant attorney general for national security, Justice Department

I'd say the top threat are those who would not be deterred. If they had the capability, they would use it. To my mind, that's the terrorist organizations.

As a nation, and like many countries in the world, we have put almost everything we value into cyberspace. We put our personal information. We put our financial information. We put the way we operate our critical infrastructure. It's digitally stored, and most of it is connected to the Internet. The flip side of that means all the same bad guys and all the same activity that we've seen for years in the brick-andmortar world is going after where the money is, where the secrets are and where they can cause damage. As we put more of what we value, we're seeing the number of criminal groups that are trying to target it increase. We're seeing nation states develop it as part of their strategies.

#### **Taking diplomatic approach**

#### **Eric Rosenbach**

Assistant secretary of defense for homeland defense and global security, Defense Department

We'll work with other nations' militaries. There's a lot of demand in the world right now for people trying to figure out how to build their equivalent of a cyber command. And the reason we do that is we want them to do that in a responsible way. There's some things we've learned that we didn't do as well as we could have. How you balance that with respect for civil liberties within the law . . . executive oversight of military organizations.

Offensive operations are something that are always an option. But it's only one of many tools that you have available on the policy spectrum. Before you would ever take offensive action, you would want to work diplomatic channels first.

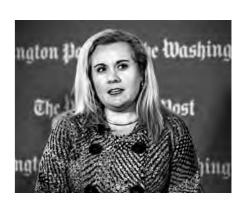


#### **Sharing information faster**

#### **Michael McKeown**

Supervisory special agent, Cyber Division, FBI headquarters

A couple of years ago [when a Russian crime ring was targeting banks], we had a threat against the financial sector. We brought in a lot of the largest financial entities and gave them essentially what we would call clearance for a day . . . to share information that would help them in real time. So we're getting better at getting that information out in a controlled structure to sectors, to partners. The key being real-time information.



#### Thinking like hackers

#### **Tiffany Rad**

Security researcher and lawyer

There's always a trade-off between security and convenience. When we have "bring your own device to work," there are vulnerabilities that can be exploited in someone's home and then be brought into the corporate network. When it comes to that type of trade-off, what I teach my students is to think like hackers. While that may sound scary to some, we're graduating students where they're writing code and they're considering the security implications of every line of code they write. It's not just "How fast does the algorithm run?" but "How secure is the stuff that you're producing?"

So when the students graduate and they go out into the workforce and work for all of you in private industry, they are designing things that are more secure. We like to think that this is going to be changing through the graduates that we have in the United States, taking jobs here in the U.S. Maybe they'll raise their hand in company meetings and say, "Hey, I think there's a different way that we could do this that would make it better and more secure."



#### **Protecting the electrical grid**

#### **Andy Bochman**

Senior cyber and energy security strategist, Idaho National Laboratory

The [electrical] grid is not all one thing. It's many different pieces, and it's designed to be resilient in the face of natural disasters and storm activity that happens all the time to it. It's not nearly as simple as saying]one very intelligent hacker can come in and start to take control of things. There are a lot of layers of protection, some of them vestigial from the way the grid was designed, even before computers came to the fore.

EE

#### **CYBERSECURITY: A SPECIAL REPORT**



### Issuing a call to action

#### Alejandro Mayorkas

Deputy secretary, Department of Homeland Security

I do not ascribe to a school of pessimism, and by that, I don't mean to belittle the magnitude of the threat, both in terms of its gravity and its frequency of occurrence. I think everyone understands that cybersecurity is a field of growth. With respect to the security of the government, and with respect to the security of the private sector, I would take the alarm not as necessarily a cause for concern, but rather as a call to action. While attackers are,

in fact, becoming more and more sophisticated, our prevention capabilities are growing in sophistication, our detection capabilities are growing in sophistication, our response and remediation capabilities are escalating as well.

The cyber threat is real and I think it will be a growth industry. We in the government, specifically in the Department of Homeland Security, have a number of tools and resources to deploy to protect a dot-gov environment.



#### Basic cyber hygiene

#### Jane Holl Lute

President and chief executive, Council on CyberSecurity

We know what to do for basic cyber hygiene. We're just not doing it. Basic hygiene will prevent 80 to 90 percent of all known attacks today. Do you know what's connected to your network? Do you know what's running or trying to run on your network? Do you know who has administrative permissions to change, bypass or override your configurations? And do you have an automated system in place like DHS's [Department of Homeland Security] continuous diagnostic and mitigation that allows you to be alert to vulnerabilities when they happen and patch them and take appropriate remediative action? Those top five of the 20 critical security controls constitute basic hygiene. We're broadly not doing it and there's no excuse now for why we're not. Let's use some common-sense things. Do you know who's getting on your networks at home? Pay attention.

We need to be smarter consumers, smarter citizens, smarter members of society when it comes to being online. But we also have a right to expect that companies and enterprises with whom we share our data are taking the basic measures. What expectation should we give to manufacturers? Why don't we get systems shipped with the security configuration switched on? Why do we all have to figure this out for ourselves? What will the role of government be as we distribute responsibility?

Let's prevent what we can at costs we can afford. That will reduce the noise level in the threat space and allow important, complex companies to focus precious resources on those advance persistent threats. But we're not even making it hard right now.



#### Disrupting terror recruiting Rep. Mike Rogers (R-Mich.)

Chairman, House Intelligence Committee

What we have seen in the past is that al-Qaeda, ISIS and other organizations have reached out and tried to find individuals who have the right capabilities to put together a cyberattack capability. We've never seen them actually put it together to where they could penetrate or do some cyberdisruption activities. But we know they have the aspiration to do it. I don't think that we're using all U.S. cyber capabilities to disrupt their ability to have these recruiting tools that we see are, candidly, very effective.

Part of the challenge is, the [U.S.] government has about 15 percent of the networks and the private sector holds about 85 percent of the networks. Contrary to popular belief, the NSA is not monitoring those networks. It's not on those networks. So, the only way that they see anything coming in is from the outside. You don't want to reach overseas and flick somebody in the forehead if we're not exactly 100 percent sure that that was the perpetrator of that [cyberattack]. If you start this digital vigilantism about, "Well, I got hacked. I'm going to go do something about it," you could create a storm here, of which the rest of the network — that 85 percent — is not prepared to handle.



#### **Protecting consumers**

#### Ellen Richey

Executive vice president and chief legal officer, Visa, Inc.

In terms of who pays and what happens when this breach might occur, wherever it might be, the first thing that everybody needs to be clear on: Here in the U.S., it is never the consumer — or only very rarely the consumer — who suffers any financial loss. That's because here in the U.S., we have a zero-liability policy that I'm sure you've heard all about, and your bank will take the charges off if they are unauthorized

Once [a breach] is identified, this huge machinery goes into place where the payment brands such as ourselves and our competitors get the information about the accounts that might have gone through that environment, and we get that information out to your banks. As consumers, you know that your bank has that information and can either monitor your account with special scoring because they know it's been exposed and protect you from the fraud, or reissue your account.

Consumers are protected financially to avoid the hassle. I would suggest one other thing you can do is sign up for real-time alerts from your bank. You can be in control of the use of your card the minute anybody is using it improperly. You'll see it yourself and you can be the one who notifies the bank, not the other way around.



#### **Businesses working together**

#### Brian Dodge

Retail Industry Leaders Association

There's enormous brand risk to the businesses that are hacked and the cost, ultimately, is something that's shared between all the players. It's shared between merchants, banks and the institutions across the payments ecosystem, which is why we have argued that the solution to these problems is one where all those players work together.



#### Attackers are getting better Phil Reitinger

Over a period of time, somebody devoting enough resources to get into your networks will.

VisionSpear

The defenders are getting better. But attackers are getting better, too. There are more of them, and there's more information available and valuable

A lot of our technologies don't scale well. That means that if you can't solve a problem completely with technology, you've got to have the right people.

......



#### Warning about social sharing

**Erin Jacobs**Urbane Security

Be careful what you share on social networks. I have a lot of friends in the security industry who are not on any social networks. But guess what? Their wives, their friends, their family, their kids — they are. And they're telling everything about them. And also our system in the U.S. doesn't help because we have so much public domain information. I think we need to do personal risk assessments of our own information and understand what's important to us and what we're willing to share and what we're not.



#### Informing responders

**Eric Friedberg** Stroz Friedberg

The main challenge for us as critical-incident responders is what corporations need from law enforcement not on day 20, not on day 40 or not on day 60, but what we need on day one or day two. There's a real strain going on right now in the speed at which private incident responders are able to get that information from the government.

It's a cat-and-mouse game where companies are often playing catch-up.

#### washingtonpost.com

The excerpts on these pages are from Washington Post Live's Cybersecurity Summit, which was sponsored by Lockheed Martin in partnership with the Cyber Security Policy and Research Institute at George Washington University. The Washington Post maintains full editorial control over the content of the conference and this special report. Video of the Oct. 1 event can be found on Washington PostLive.com.



## AND THE ABILITY TO SECURE IT.

#### AT LOCKHEED MARTIN, WE'RE ENGINEERING A BETTER TOMORROW.

Attacks against information systems are relentless, and they're not going away. But by taking an intelligence-driven approach to cyber security today, we're building resilient networks that can defend against threats that haven't been imagined yet. It's just one way we're creating solutions for a more secure future.

Learn more at lockheedmartin.com/cyber

© 2014 LOCKHEED MARTIN CORPORATION

LOCKHEED MARTIN