

# A Real (Good) Hack Job

Cybersecurity professionals innovate and collaborate to combat the expanding threat posed by cybercriminals



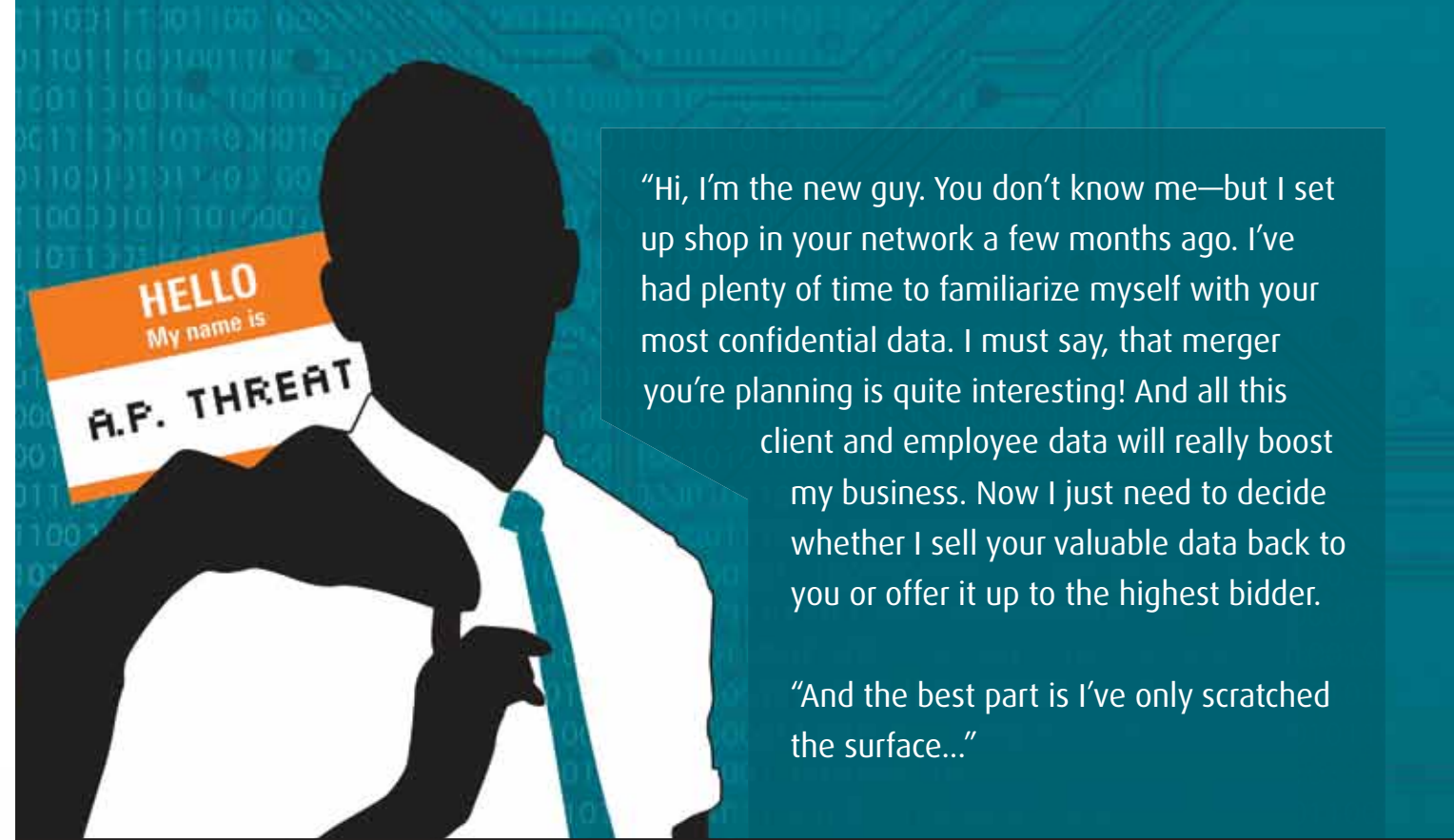
**F**or the past five years cybersecurity experts have posited that the U.S. is in the midst of a cyber war with China, which—experts claim—has launched a far-reaching hacking offensive. However, it wasn't until the Gmail accounts of senior U.S. officials were compromised in the spring that anyone in a position of power actually considered breaches of cybersecurity more than just a vague danger. The reality is that gargantuan amounts of intellectual property, the main asset of the modern economy, are compromised daily. "People often ask how much of a threat this is," says former Homeland Security Secretary Michael Chertoff, now Co-Founder of the Chertoff Group. "It's not a threat—it's actually happening. If your crucial business property and negotiating redlines are being sent to others who will use them against you, that's the same as someone walking into your bank and taking your money. We have to take this very seriously."

Naturally, risk is relative to the value and volume of stored data. "Collecting and sharing of consumers' personal information contributes to identity theft," says Susan Grant, Director of Consumer Protection for Consumer Federation of America. Large amounts of personal data are often gathered and housed by entities—think doctors' offices, government agencies, etc.—over which consumers have no control. "Judging by the nonstop news about security breaches, some of those entities don't seem to be doing a very good job," says Grant, whose organization also oversees IDTheftInfo.org.

Today's cybercriminals cause roughly \$100 billion worth of mayhem per year worldwide, and some believe it has exceeded drug trafficking in dollar value.



PETER DAZELEV/GETTY IMAGES



"Hi, I'm the new guy. You don't know me—but I set up shop in your network a few months ago. I've had plenty of time to familiarize myself with your most confidential data. I must say, that merger you're planning is quite interesting! And all this client and employee data will really boost my business. Now I just need to decide whether I sell your valuable data back to you or offer it up to the highest bidder.

"And the best part is I've only scratched the surface..."

Get to know your threats before they get to know your data.



- » Data Security & Privacy
- » Risk & Vulnerability Assessments
- » Data Analytics
- » Incident & Data Breach Response
- » Computer Forensics



Ask us about defense in depth or learn more:  
[KrollFraudSolutions.com/cyberrisk](http://KrollFraudSolutions.com/cyberrisk)



Certain Alteryx companies provide investigative services. State licensing information can be found at [www.alteryx.com/compliance](http://www.alteryx.com/compliance). © 2011 Kroll, Inc. All rights reserved. Item #ADV-002-2011-0929

An Alteryx Company

The newest wave of cyberattacks has assumed new forms. Medical devices offer a chilling example of devices easily susceptible to siege. In a 2008 study, researchers from the Medical Device Security Center in Amherst, Mass. were able to cause a pacemaker to beat erratically and ultimately crash, through a staged attack. Knowing the code used by the device wasn't even necessary—all the researchers had to do was throw gibberish at it, and the pacemaker was effectively “stunned” says Robert Vamosi, Senior Security Analyst for Mocana, a company that focuses on the digital securing of non-PC devices. “There’s ransom tied to shutting down a CEO’s pacemaker. Anyone with malicious intent could conceivably go after some of these devices, and it doesn’t take nation-state resources.”

The avalanche of mobile device usage over the last 10 years has vastly complicated the situation. “There’s no doubt that, with the proliferation of mobile, end-point security has become a huge problem,” says Jerry Archer, Chief Information Security Officer of Sallie Mae. Cybercriminals develop specific viral applications designed to intercept banking transactions. For example, since first being identified in 2007, the Zeus virus has been modified to infiltrate innumerable new devices as they’re created, causing a Trojan horse scenario that remains a substantial threat to financial institutions. “The latest FFIEC guidelines talk about how banks can defend against the end-point threat,” says Archer. “Complexity is the bane of security. The more complex the system is, the harder it is to defend.”

Regardless of their ultimate agenda, all cybercriminals share at least one key goal: to rapidly expand their victim pool.

**“It’s not a threat. It’s actually happening. It’s the same as someone walking into your bank and taking your money. We have to take this seriously.”**

**—Michael Chertoff**



Security Innovation Network (SINET) assumes the mission of defeating cyber threats through global collaboration between the public and private sectors. “To effectively combat cybercrime, we must bring new models that advance innovation and re-evaluate the way we view risk,” says Robert Rodriguez, SINET Chairman and Managing Principal. “There is a huge divide of awareness between the defense-industrial base and early-stage, emerging-growth cybersecurity companies. Our event programs, supported by the Department of Homeland Security Science and Technology Directorate, bring the investor, builder, buyer and researcher together, and connect the ecosystem of the entrepreneurs by giving them an opportunity to showcase their technologies.”

These budding companies gain access to SINET’s advisory services and community building, which helps guide their adoption into the cybersecurity marketplace. Advice on how to overcome entry barriers, where to focus limited budgets and matching the needs of government bodies (civilian or defense-based) is one of SINET’s strengths as a cybersecurity connector and builder of trust-based relationships. “Trust is the most critical element of relationship building,” continues Rodriguez. “You establish that incrementally. If you don’t have trust, public-private partnerships decline, and information that’s critical to both industry and government, specifically the intelligence community, isn’t shared.”

SINET also prioritizes strengthening the link between entrepreneurs and the academic, industry, government and research communities. New information on cyberse-

curity constantly springs from government-funded studies, with the ultimate goal of applying these gold nuggets of research to real-world problems. Academia can be even further leveraged by the sharing of data between cyber-expert universities, such as Stanford and MIT. Most importantly, SINET sculpts its services around the embrace of new cybercrime-fighting models. Rodriguez believes these game-changing technologies are more likely to come from small, independent businesses rather than established bodies that rely on old models. “It’s not the IBMs of the world that are constantly bringing about the most impactful change,” says Rodriguez. “It’s Hewlett-Packards raising \$536 of capital in 1936 to build product in their garage. It’s two Stanford students in their apartment, building the first servers for Google. It’s the little guys that push innovation. Where are they? When it comes to innovation, our nation can’t leave any stone unturned.”

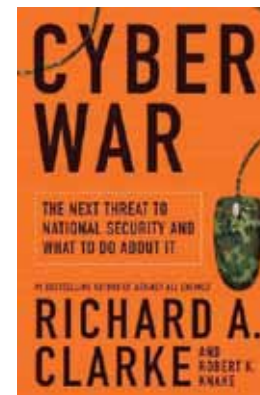
There are, naturally, contributors in the cybersecurity field that offer data protection as well as data loss prevention services. One such company is Kroll, where the Cyber Security and Information Assurance Practice assists organizations and consumers with data breach response, incident response, and fraud detection. Their client offerings include everything from turnkey data breach and identity theft solutions, electronic IP security consulting and recovery to data minimization strategies and litigation consulting. “When organizations understand that data breaches happen to everyone, the next step is to prepare for the inevitable,” says Karen A. Schuler, CFE,

# Software is the new cyber attack vector.

Do you understand the security posture of the software that runs your business?

Veracode helps secure business critical software — whether built in-house, purchased or developed by a third-party.

Build your application security knowledge. Register for your FREE copy of *Cyber War* today: [www.veracode.com/bloomberg](http://www.veracode.com/bloomberg)



Scan to register for your FREE copy of *Cyber War*. Quantities are limited. The first 500 registrants will receive a copy.

**VERACODE**



Kroll's Cyber Security & Information Assurance Practice Leader and Senior Managing Director. "While our focus is responding to events, the post-event assessment is critical to mitigating future risks."

Kroll often encourages clients to achieve this preparedness through vulnerability assessments, policy gap analyses and tabletop exercises. The tabletop exercise is when a hypothetical breach response is effectively staged. "This gives our clients the opportunity to vet their incident response plan, mitigate for documented gaps and augment their plans accordingly," says Schuler. "We've gone through exercises where we spend two to four days with clients, practicing the actual incident as if a breach had taken place. It helps—it gets people to think differently."

One of Kroll's most common client warnings regards reaction timing—but not in the way you'd think. According to a 2010 survey by the Ponemon Institute, the cost of reporting a breach and mobilizing data

recovery too quickly can cause indirect revenue hits. Hasty respondents risk regulatory fines, loss of business and damage to their reputation. This is just one area in which Kroll's advisors rescue clients. "Breach response is becoming more heavily regulated and complex, which means that poor execution will continue to cost companies more money when they are not compliant with state regulations," says Schuler.

A recent phenomenon that Schuler's team has observed and subsequently strategized to counteract is the hostage-taking of data. Says Schuler, "We have had clients come to us and say, 'We have data being held hostage.' Not only do our Cyber Security & Information Assurance professionals have the ability to respond, but we engage Kroll's kidnap and ransom team and investigators to provide an end-to-end solution from negotiations, investigations and analysis. All of a sudden it has become a hot topic and we will certainly continue to see a rise in attackers

taking data and holding it ransom."

From financial trading platforms to accounting systems, to customer support activity, individual companies manage innumerable software applications. The frameworks for these systems are often supplied by industry giants that write solid, secure software. However, some companies create these applications themselves, neglecting to generate sufficient protective coding, or any infiltration guard. At the very least, companies typically think of securing only their riskiest apps but ignore lower-risk apps that can be vulnerable to a breach. That's where Veracode Inc. comes in.

During the most recent five years, Veracode has assisted clients in two key areas: building security policies into the development life cycle of new applications; and, more significantly, securing the multitude of already deployed applications that represent essential cornerstones to their corporate functioning. "Customers

**A new technique in cybercrime is the taking hostage of data. "I think it's going to become a more common tactic for attackers," says Karen Schuler, Senior Managing Director of Kroll.**

want to understand which applications are most at risk and which they need to fix," says Veracode CEO Chris Wysopal. "Clients can have a huge backlog of 10-plus years of insecurely written code that they come to grips with only after a break-in."

Security-as-a-Service (SaaS), Veracode's cloud-based model for application risk management, allows it to search for security vulnerabilities across huge numbers of applications quickly, to service a global client base that ranges from software vendors to enterprises to government agencies. "The software, the hardware required to run it and the people administering the system are shared over many customers," continues Wysopal. "You get economies of scale. You also get continuous improvement because the creators of the software are also the operators, who can notice inefficiencies and correct them."

There's tremendous momentum across industry verticals behind the development and implementation of web and mobile applications. From health care to financial services, to government agencies, organizations are producing titanic volumes of code daily, and Veracode urges clients to security-test every last string. "We're in a transition period from ad-hoc security testing to more programmatic approaches to application security," says Wysopal. "But securing your most valuable software can't be an afterthought—it shouldn't only be done in special cases. The industry needs to move to an independently verified model to have a complete understanding of the software security posture of applications they build, buy or secure."

As severe as the bottom-line consequences are for loosely guarding sensitive corporate data, the protective need is even greater for the IP held by governments. ManTech International Corp. is a leading provider of technology services for the national security, intelligence and space exploration communities. It holds active contracts with all branches of the armed forces, the Justice and Defense departments, NASA and many additional federal agencies. Since its founding in 1968, ManTech's purpose has been to supply the federal government with technical aid, and it has grown into a \$3 billion worldwide

company with a presence in 40 countries.

"Both government and industry are equally at risk," says ManTech's Mission, Cyber and Technology Solutions Group President and COO, Bill Varner. "Much of our critical infrastructure relies on Internet transactions, and many of those transactions are over private networks."

Essentially, ManTech's mission is to enable trusted transactions over potentially untrustworthy networks. The U.S. government conducts business via long-established operational models; maintaining "business as usual" in the face of cyber threats requires an overall corporate culture within the government that brokers innovation, and this is precisely ManTech's role.

Not only does ManTech boast a robust internal R&D program that cultivates new tools and solutions, but the company also hosts security operations centers to evaluate these new tools in real-world environments. "In more than 10 labs for cybersecurity alone, we are developing new tools for malware detection, intrusion detection, penetration testing, reverse engineering and other technologies that will be needed by our clients in the years to come," says Varner.

2011 saw numerous assaults by cybercriminals and "hactivists" that resulted in the theft of national-security and other proprietary information, but Varner sees hope on the horizon. In July, the Department of Defense released a cybercrime strategy that's more comprehensive and aggressive than ever before, and numerous pieces of cyber legislation are currently pending in Congress. "We're getting a better definition of what the government may view as an act of war in the cyber world," says Varner. "And the marketplace is helping by providing incentives for companies to develop solutions to cybersecurity problems."

As a final point, Chertoff urges the consideration and enactment of multiple solutions. "There's no magic bullet or formula that cures the issue overall," he says. "You need to be fully aware of all data in your system, both in motion and at rest. You need to know how to vet the integrity of the hardware and software you're introducing. And you need to architect a system that reduces the impact of human error."

—Jamie Gerardi

## OUR HAPPIEST CUSTOMERS NEVER HEAR FROM US.



Every day, there are thousands of cyber attacks in this country. But our customers go about their business because they know they're protected. At ManTech International Corporation, it's our business to keep you in business with no interruptions. No compromised data. No customers harmed.

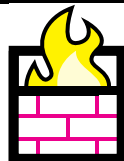
In cyber warfare, celebrate the quiet victories, and keep doing business as usual.

**ManTech**  
International Corporation®

www.mantech.com

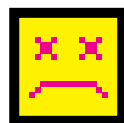
Leading the Convergence of  
National Security and Technology™

## How to Protect Your Computer



### Keep Your Firewall On:

Firewalls protect your computer from hackers who try to gain access to crash it or steal information. Software firewalls are widely recommended and come prepackaged.



### Install or Update Your Antivirus Software:

Antivirus software is designed to prevent malware from embedding on your computer. If it detects malicious code, like a virus or a worm, it works to disarm or remove it before it can do serious damage.



### Install or Update Your Antispyware Technology:

Spyware is surreptitiously installed on your computer to let others peer into your activities on the computer. Some spyware collects information about you without your consent or produces unwanted pop-up ads. Antispyware combats these intrusions.



### Keep Your Operating System Updated:

Computer operating systems are periodically updated to stay in tune with technology requirements and to fix security holes. Be sure to install the updates.



### Be Careful of What You Download:

Carelessly downloading email attachments can circumvent even the most vigilant antivirus software. Never open an email attachment from someone you don't know, and be wary of forwarded attachments even from people you do.



### Turn Off Your Computer:

Many of us leave our computers on 24/7, but a computer that is always turned on is more susceptible. Beyond firewall protection, which is designed to fend off unwanted attacks, turning the computer off effectively severs an attacker's connection—be it spyware or a botnet.