Enterprise Risk Management & Governance

Vol. 8, No. 2

Corporate Cyber Attacks, Threats, and Security

by Arun K. Majumdar, Senior Consultant, Cutter Consortium

This *Executive Report* provides executives, government workers, and security professionals a fast track to gaining insight into cyber security. It covers executive liabilities and accountabilities, the top eight cyber security cases, situational awareness, and a multitude of need-to-know issues for immediate practical use. Is your company at risk? Why? How? When? What damage has already been done? The report is based on facts, evidence, and real-world cases through a fictionalized account of names and situations to protect privacy and legality. In addition, some real company names and individuals of recent public cases have been provided.

Access to the Experts

Cutter Consortium is a truly unique IT advisory firm, comprising a group of more than 100 internationally recognized experts who have come together to offer content, consulting, and training to our clients. These experts are committed to delivering top-level, critical, and objective advice. They have done, and are doing, groundbreaking work in organizations worldwide, helping companies deal with issues in the core areas of software development and agile project management, enterprise architecture, business technology trends and strategies, innovation, enterprise risk management, metrics, and sourcing.

Cutter offers a different value proposition than other IT research firms: We give you *Access to the Experts*. You get practitioners' points of view, derived from hands-on experience with the same critical issues you are facing, not the perspective of a desk-bound analyst who can only make predictions and observations on what's happening in the marketplace. With Cutter Consortium, you get the best practices and lessons learned from the world's leading experts — experts who are implementing these techniques at companies like yours right now.

Cutter's clients are able to tap into its expertise in a variety of formats, including print and online advisory services and journals, mentoring, workshops, training, and consulting. And by customizing our information products, training, and consulting services, you get the solutions you need while staying within your budget.

Cutter Consortium's philosophy is that there is no single right solution for all enterprises, or all departments within one enterprise, or even all projects within a department. Cutter believes that the complexity of the business technology issues confronting corporations today demands multiple detailed perspectives from which a company can view its opportunities and risks in order to make the right strategic and tactical decisions. The simplistic pronouncements other analyst firms make do not take into account the unique situation of each organization. This is another reason to present the several sides to each issue: to enable clients to determine the course of action that best fits their unique situation.

Expert Consultants

Cutter Consortium products and services are provided by the top thinkers in IT today — a distinguished group of internationally recognized experts committed to providing top-level, critical, objective advice. They create all the written deliverables and perform all the consulting. That's why we say Cutter Consortium gives you *Access to the Experts*.

For more information, contact Cutter Consortium at +1 781 648 8700 or sales@cutter.com.

The Enterprise Risk Management & Governance Advisory Service Executive Report *is published by the Cutter Consortium, 37 Broadway, Suite 1, Arlington, MA 02474-5552, USA. Client Services: Tel: +1 781 641 9876; Fax: +1 781 648 8707; Email: service@cutter.com; Website: www.cutter.com. Group Publisher: Chris Generali, Email: cgenerali@cutter.com. Managing Editor: Cindy Swain, Email: cswain@cutter.com. Print ISSN: 1554-7035 (*Executive Report, Executive Summary, *and* Executive Update*); online/electronic ISSN: 1554-7043.*

Rob Austin | Ron Blitstein | Christine Davis | Tom DeMarco | Lynne Ellyn | Tim Lister | Lou Mazzucchelli | Ken Orr | Robert Scott

Cutter Business Technology Council

Corporate Cyber Attacks, Threats, and Security

THIS ISSUE'S AUTHOR

Arun K. Majumdar
Senior Consultant, Cutter Consortium

IN THIS ISSUE

2 Types of Cyber Crime

3 Executive-Level Situational Awareness

4 Cyberspace and Hackers

6 Yuri's Hacker Tradecraft

8 Pentagex Vulnerability: Yuri's Attack Begins

11 Ready to Launch Botnet Attacks

12 The Executive Checklist for Cyber Threat Risk Mitigation

16 Executive Social Engineering Countermeasures Strategy

17 The Executive Top 15 Countermeasures Checklist

18 Conclusion

18 Endnotes

19 About the Author

The hour is late, the offices at Pentagex,[1] a financial services company, are closed, and the streets outside are empty. Yet within the IT department, the lights are still on, the racks of blades are humming, and the world is connected.

Yuri is sitting at his desk in his apartment in the city of Sofia, Bulgaria. He is running the latest version of the US National Security Agency (NSA) Security-Enhanced Linux (SELinux), which he got from his buddy's last visit to *ShmooCon*, a hacker's convention in Washington, DC. You see, Yuri is on the FBI wanted list of elite black hat hackers and thus cannot visit the US. However, his buddy Boris is not on any list and got him what he needed: the coveted SELinux kernel code.

Armed with the best in US technology, Yuri has spent the night cautiously, stealthily, and determinedly probing the Pentagex security systems. His work has not been in vain; he has identified a useful vulnerability in one of the servers. But it won't be long until Pentagex opens its doors to its employees and customers. Yuri must work quickly before his window of opportunity closes. So he calls up a client account list at Pentagex and harvests the lists of credit card numbers and other key identifying information. At the end of the hour, Yuri has a list of 50,000 names, numbers, and IDs. Yuri then closes the link to the Pentagex servers.

Next, Yuri calls his other buddy Mustafa and offers the list for sale. They negotiate vigorously. Yuri wants 2 euros per credit card number while Mustafa offers 50 cents. After an intense exchange, the two finally come to an arrangement. Mustafa pays 1 euro per card and also gives Yuri access to a quarter-kilo of narcotics; he knows Yuri likes to party and can sell the contraband for profit at local nightclubs.

A day later, Pentagex is flooded with calls from angry customers who have tracked charges that have depleted their credit levels; the news and media report harshly on Pentagex, its stock begins to fall, and executives scramble to find out what went wrong. Simply put, the executives were blind, and the IT department took

things for granted. The questions the Pentagex executives were blind about come down to the following:

1. Do you know you are at risk?
2. Do you know why you are at risk?
3. Do you know when you are at risk?
4. Do you know how much damage has already been done?
5. Do you know what you need to know to be aware and take action?

If you have answered no to any of these questions, then what you need to know is in this *Executive Report*. For those that answered yes, I suggest adding: "Do you know *everything* you need to know?" This report will add to what you already know and perhaps more.

Security boils down to human behavior, vigilance, and a resolve to mitigate threats before they can cause damage beyond a certain level.

TYPES OF CYBER CRIME

Unless you bury your computer in the backyard and grow roses on top, the answers to the questions above will not change no matter how many security devices you put in place around your computer. The issue boils down to human behavior, vigilance, and a resolve to mitigate threats before they can cause damage beyond a certain level. In other words, you will always take a hit of some kind unless you mitigate both human and machine factors. Let's look at some recent real-world accounts of cyber crime:

1. Insider threat:[2]

> A federal jury in Baton Rouge, LA, today convicted a former research scientist of stealing trade secrets from Dow Chemical Company and selling them to companies in the People's Republic of China, as well as committing perjury…. In one instance, [Wen Chyu Liu aka David W.] Liou bribed a then-employee at the Plaquemine facility with [US] $50,000 in cash to provide Dow's process manual and other CPE-related information.
>
> "Today a federal jury found Mr. Liou guilty of stealing protected trade secrets from Dow Chemical Company, including by bribing fellow employees for this valuable information," said Assistant Attorney General Breuer. "American industries thrive on innovation and they invest substantial resources in developing new products and technology. We will not allow individuals to steal the technology and products that US companies have invested years of time and considerable money to create.…" Companies within the US lose millions of dollars to the theft of trade secrets such as this," said Special Agent-in-Charge David Welker of the FBI's New Orleans Division."

2. Identity theft:[3]

> The Account Slurper attacked AT&T's servers for several days in early June 2010, and was designed to harvest as many ICC-ID/email address pairings as possible. It worked by mimicking the behavior of an iPad 3G so that AT&T's servers would be fooled into granting the Account Slurper access. Once deployed, the Account Slurper used a process known as a "brute force" attack — an iterative process used to obtain information from a computer system — against the servers, randomly guessing at ranges of ICC-IDs. An incorrect guess was met with no additional information, while a correct guess was rewarded with an ICC-ID/email pairing for a specific, identifiable iPad 3G user. From June 5 through June 9, 2010, the Account Slurper stole for its hacker-authors approximately 120,000 ICC-ID/email address pairings for iPad 3G customers.

3. Cyber warfare:[4]

> In mid-December, we detected a highly sophisticated and targeted attack on our corporate infrastructure originating from China that resulted in the theft of intellectual property from Google. However, it soon became clear that what at first appeared to be solely a security incident … was something quite different.
>
> First, this attack was not just on Google. As part of our investigation we have discovered that at least twenty other large companies from a wide range of businesses … have been similarly targeted. We are currently in the process of notifying those companies, and we are also working with the relevant US authorities.

4. Cyber credit fraud:[5]

> On October 18, 2005, a federal grand jury in Cleveland, Ohio, returned an indictment charging [Kenneth J.] Flury with one count of bank fraud, arising from a Flury's scheme to defraud Citibank which occurred between April 15, 2011, and May 4, 2011, and involved Flury obtaining stolen Citibank debit card account numbers, PINs and personal identifier information of the true account holders which Flury fraudulently encoded onto blank ATM cards. After encoding blank cards with the stolen account information, Flury used the counterfeit ATM to obtain cash advances to withdraw cash and obtain cash advances totaling over $384,000 from ATM machines located in the Greater Cleveland area over a 3 week period. After Flury fraudulently obtained the funds, he transferred approximately $167,000 of the fraud proceeds via Western Union money transfers to the individuals supplying the stolen Citibank account information located in Europe and Asia.

5. Darknet services:[6]

> [Jeanson James] Ancheta admitted using computer servers he controlled to transmit malicious code over the Internet to scan for and exploit vulnerable computers. Ancheta caused thousands of compromised computers to be directed to an Internet Relay Chat (IRC) channel, where they were instructed to scan for other computers vulnerable to similar infection, and to remain "zombies" vulnerable to further unauthorized accesses.

6. Kids for fun:[7]

> On August 14, 2003, the juvenile directed the infected computers to launch a distributed denial of service attack against Microsoft's main Web site causing the site to shutdown and thus became inaccessible to the public for approximately four hours. The juvenile was 14 years old when the activity occurred. …The juvenile told Judge [Robert S.] Lasnik, "Seventeen months ago, I made the worst mistake I ever made in my life. I did it out of curiosity and did not think I would cause any damage. I am sorry I created problems for people I did not even know."

7. Cyber fraud:[8]

> [Alexey] Ivanov had previously pleaded guilty … and admitted to numerous charges of conspiracy, computer intrusion (i.e., "hacking"), computer fraud, credit card fraud, wire fraud, and extortion. Those charges stemmed from the activities of Ivanov and others who operated from Russia and hacked into dozens of computers throughout the US, stealing usernames, passwords, credit card information, and other financial data, and then extorting those victims with the threat of deleting their data and destroying their computer systems. In sentencing Ivanov, the district judge described his participation as a "manager or supervisor" in an "unprecedented, wide-ranging, organized criminal enterprise" that "engaged in numerous acts of fraud, extortion, and intentional damage to the property of others, involving the sophisticated manipulation of computer data, financial information, and credit card numbers." The district judge found that Ivanov was responsible for an aggregate loss of approximately $25 million.

8. Disgruntled employee:[9]

> A disgruntled computer systems administrator for UBS PaineWebber was charged today with using a "logic bomb" to cause more than $3 million in damage to the company's computer network, and with securities fraud for his failed plan to drive down the company's stock with activation of the logic bomb.

Hackers are only one part of the problem. If your focus on security efforts is in preventing hackers, then there may be several ongoing, undetected cyber attacks. For example, under the umbrella of insider threats, consider the exfiltration of corporate information for sale by a hard-up employee, or an employee's child playing around at the office on "Dad's" computer and inadvertently downloading malicious code, or the unwary office worker who throws out a number of sensitive documents, without shredding them, into an outside trash bin, and so forth. All this distills down to executive-level situational awareness and its corollary aspects, as we shall see next.

EXECUTIVE-LEVEL SITUATIONAL AWARENESS

Executives have many responsibilities to stockholders, employees, clients, and the public. On multiple levels, today's executive challenge is *situational awareness*:

> Situation awareness involves being aware of what is happening around you to understand how information, events, and your own actions will impact your goals and objectives, both now and in the near future.[10]

Marketers understand one form of situational awareness: awareness of new competitors, applicability of new research to the product sphere, market movements, and sentiment. This is conveyed to executives through briefings and reports. Executives understand another form of situational awareness: the awareness of their bottom line. And they receive briefings and reports from the financial department. Given that several departments (e.g., R&D, production, A/R, marketing) write briefs and the executive gets a fair overview of the company from these reports, he or she can use this insight to steer the company toward success — and away from failure. However, by the time an executive receives a briefing on a cyber issue, it is usually after the fact of an attack rather than as an awareness briefing prior to an attack.

This *Executive Report* focuses on situational awareness toward cyber threats and draws attention to the toxic corporate cultures that enable such threats. To be effective on this topic, we must first provide the distinctions that illuminate a broad understanding of the landscape of cyberspace, cyber culture, and cyber threats with respect to corporate culture in a way that will enable the senior executive to ask questions and then determine if the IT department is aligned with the processes and procedures that mitigate the risk of corporate theft and information loss or whether the HR department is aligned with the processes that mitigate threats before they emerge.

All companies are targets for hackers, and all are vulnerable. No one is immune: even Google got hacked. Every company will have some disgruntled employees. And most organizations are largely defenseless. Sooner or later, every company is someone's target. Sometimes this is due to a strategic need of a competitor to gain advantage via information espionage or from hackers

stealing salable information or direct dollars from company coffers; others times, it's simply some kid wanting to prove a point.

Although many companies have been exposed — or have been vulnerable — to such threats, many have survived and have managed to identify the right structures and processes to diminish the threat of cyber intrusions, data theft, and insider threats. So what can you do? The first steps are to (1) become attuned to the distinctions, (2) become present to the concepts of hacking, and (3) develop situational awareness. By knowing how hackers think, how they operate, and what tools they use, you can become a better decision maker overall and provide more beneficial support to the IT department (and their counterpart of corporate security). The next section on cyberspace will very rapidly get you up to speed regarding hacking to a level where you will have a deeper understanding and an improved vocabulary about hacking and hackers as well as their tools, culture, and operations. It will equip you to learn a lot more about this area.

P2P technologies are operating within the fabric of about 360 million PCs, and the increasing daily numbers online provide a new context for short-lived but massively influential communications.

CYBERSPACE AND HACKERS

In 1984, William Gibson, a visionary science fiction writer invented the word "cyberspace" and described it the following way in his book *Neuromancer*:

> Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts.... A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data.[11]

Since then, we have seen revised definitions, including this one from the US Department of Defense (DoD):

> A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[12]

There's also one from the US Department of Homeland Security (DHS):

> Our Nation's critical infrastructures are composed of public and private institutions in the sectors of agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping. Cyberspace is their nervous system — the control system of our country. Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work. Thus, the healthy functioning of cyberspace is essential to our economy and our national security.[13]

The Internet is not only growing but also transforming on a daily and hourly basis; new computers are rapidly being connected online, and, concurrently, individuals are creating multiple identities, multiple evolving neological language communities are surfacing, and participation is growing in a multiplicity of globally proliferating distributed electronic services. In fact, peer-to-peer (P2P) technologies are operating within the fabric of about 360 million[14] PCs, and the increasing daily numbers online provide a new context for short-lived but massively influential communications. Our hacker Yuri is very content with the money he made from his attack on Pentagex, but he also knows that the Pentagex executives are scrambling hard to obtain the right security experts to help its IT department plug any security holes and possibly attempt to trace Yuri back to his home. Yet despite the remote possibilities that Pentagex may find a path back to him, Yuri plans yet another — even more devastating — plan on Pentagex. Yuri is comfortable and confident that by using the tools at his disposal to mask out his true identity, he will remain immune from the security consultants at Pentagex.

Yuri has access to several powerful and compelling new technologies that enable anytime/anywhere communications with his network of colleagues who are vested in robbing Pentagex and others for their own ends. Such technologies include:

- P2P, such as torrents
- Anonymous overlays, such as Freenet and Darknet
- Online chat rooms
- Online gaming environments
- Viral communications systems, such as botnets, email, and flux servers
- Second Life and other virtual environments
- Twitter

- SMS
- Blogs
- Wireless (Wi-Fi and others)

Of course, Yuri is no fool. He ensures that when he and his colleagues log on to use these technologies, they don't give away their true identities. Consequently, they adopt several patterns of behavior within these networks, picked up as tradecraft, namely:

- **Identity obfuscation.** Yuri changes his online name to "6y83Punk."
- **Identity aliasing.** Yuri creates several aliases such as "Cybe7Punk37."
- **Multiple identities.** Yuri himself creates identities for himself such as "Paul Stanwyck"
- **Mobility.** Yuri uses his home setup carefully but often hangs out at cyber cafes.
- **Dynamism (never repeating patterns).** Yuri calls on his friends to trade log-ons.
- **Encrypted ciphertext messaging.** These include messages such as "Blue sky," which really means "Call me now."
- **Nontraditional information-hiding techniques.** Yuri's favorites are porn sites.
- **Code language invention.** Yuri loves to make up new words such as "figrendow."
- **Anonymous or anonymizing communications systems.** Yuri loves Freenet!

Yuri's patterns of behavior explicitly hide malcontent or adversarial intent and enable him to conduct clandestine criminal operations at will and with impunity. For example, Yuri's transnational criminal logistical operations include stealing corporate trade secrets, monitoring critical executive communications (e.g., boardroom discussions), capturing critical data via insertion of rogue wireless devices into the corporate wired or wireless networks, and even having his buddies scouring corporate trash bins after hours for information and data and relaying it all back to him over Freenet.

Systems such as Freenet were originally conceived to support the high ideals in goodwill and privacy protection but could just as easily be used for malicious purposes. Consider this quote from Freenet's website:

> Freenet is software designed to allow the free exchange of information over the Internet without fear of censorship, or reprisal. To achieve this Freenet makes it very difficult for adversaries to reveal the identity, either of the person publishing, or downloading content. The Freenet project started in 1999, released Freenet 0.1 in March 2000, and has been under active development ever since.[15]

Yuri and his friends have already leveraged these systems in combination with other methods in operations to deliver significant offensive value; the most notable and recent case was the cyber attack on the nation of Georgia by malicious Russian hackers, friends in Yuri's network, which had combined these communications capabilities with software "bots" to deliver a crippling blow to their target, Georgia.

Yuri is a deep part of this cyber culture and knows where to get the information to learn new techniques or to improve his trade. In Yuri's small IKEA-furnished bedroom, he has several shelves laden with books by Colonel Colin Gubbins of the Royal Artillery, such as *The Art of Guerrilla Warfare*, *Partisan Leader's Guide*, and *The Housewife's ABC of Home-Made Explosives*.[16] One of Yuri's favorites is *The CIA Insider's Dictionary of US and Foreign Intelligence, Counterintelligence & Tradecraft* by Leo D. Carl.[17] Through Carl's book, he found several searchable keywords he could apply in Webcrawler, then Yahoo!, and finally Google, which, over the years, had provided access to information about agencies, such as the NSA, in documents once classified as "secret" (only a few years ago), including the "NSA Transition 2001" document, now available on the Web.[18] It is easy to see how Yuri could use these sources to acculturate his friends toward dark hacking, create communities, and provide ideas on how to camouflage, deceive, disrupt, degrade, destroy, or deny access to the true intent of his communications with Mustafa and his other procurers or sources of money.

But Yuri is cautious and understands that some political savvy is critical to gaining friends and influencing others. He knows that while the US is a vast source of free information, stemming from its culture of being a free society, China, in contrast to the US, has developed a significantly different policy: the Internet and even roadmaps are censored by the government.[19] So Yuri has been forging a network of friends from Hong Kong to mainland China who might be willing to help him hack into Pentagex again, or any other US target, because the state might just turn the other cheek for political reasons. North Korea, another highly reclusive nation with little or no publicly accessible information, appears to have similar policies, so Yuri scours the IRC chat lines in search of friends he can make there, too.

In short, Yuri has learned good tradecraft directly or indirectly from government and publicly originated sources in the US simply because open publication is

a cultural quality of a free nation. Unfortunately, this same type of publication is also open to creative adaptation by those who would bring about the collapse of the system or use the system for their own ends, such as our hacker, Yuri. Yuri is optimistic that globalization and global communications will continue to increase in pace, rate, flow, and density, thus shielding him from sight in the vast oceans of growing data traffic.

Before we get to Yuri's next attack on Pentagex, let us take a detour from his story to delve into the environments that support Yuri's activities. We need to do this because an awareness of those environments produces the mindset to understand how to thwart hackers like Yuri — and Yuri's newest attack is completely unobvious and not anything Pentagex has ever prepared itself to handle. Yuri will gain access to Pentagex's plans for its newest and most secretive product launch. Pentagex has worked for years developing the product, and Yuri's old friend Mustafa has made an offer that Yuri just could not refuse: $1 million dollars spread over multiple accounts with a new identity and passport so that Yuri could once again gain entry into the US.

Hackers embedded in the culture of dark cyber communities understand their own strengths and weaknesses.

Mustafa can sell the information to a consortium that is trading Pentagex stocks, and, armed with this "insider" information, can make a killing — not to mention selling off the Pentagex secrets to competitors for even more return on their investment. In fact, the knowledge of what, when, and how Pentagex will launch its new product will provide a window in advance of the launch for the consortium to buy up Pentagex stock and then sell it; after which, the secrets will be sold to the highest bidder. The net result: Pentagex stocks will balloon and then come tumbling down as cheaper cloned alternatives are presented to the hungry markets.

Of course, this time around, Yuri will need a team. Thus, his immediate goals are to get a new team: a team inside the US and outside the doors to the Pentagex building in New York's Wall Street district. Yuri understands that this will require special communications protocols, specific preparations, and a unique approach. So Yuri makes his preparations and begins the recruitment process.

YURI'S HACKER TRADECRAFT

Yuri does not keep his most precious records at home; if he were ever accused, raided, or captured, people would find nothing there. Yuri's favorite filing system is the vast troves of pornographic sites and the millions of free upload and download areas for obscene pictures that nobody would really care to look at (unless, of course, they knew what was buried in the bits and bytes of those photos). Yuri stores his virtual Rolodex, posting various pictures onto "The Pirate Bay," the largest BitTorrent tracker, and other download archives. He uses a technique known as steganography[20] to hide his most precious information regarding the whereabouts of the latest Darknets, their communications protocols, and access procedures. Yuri knows that by hiding his data in the vast oceans of Internet data, there is little chance of discovery.

But what are Darknets? And what does a Darknet provide to Yuri? How can this help Yuri gain access to Pentagex's most critical secrets? "Dark" networks are inaccessible to traditional Internet browsers such as Google Chrome, Safari, Internet Explorer, and others, yet can be used at a moment's notice to disrupt social order and deny economic transactions or to conduct secretive communications (in support of criminal logistics or even terrorist operations). Although such networks are hidden from the more common tools, they are a part of the Internet and use special tools for access.

Criminal or terrorist-funded hackers, arms smugglers, trade secret or intellectual property thieves, transnational criminal corporate espionage groups, child pornographers, international gangs, drug traffickers, and many other covert networks exist as dark networks using various uniquely "cyber" techniques (such as servers that change their hardware identities every few seconds or Tor or Freenet networks). Hackers embedded in the culture of dark cyber communities understand their own strengths and weaknesses; they know how to create communications systems where traditional cryptographic attacks are useless. Their tradecraft principally involves: (1) *identity masking* (hackers seldom meet in person), (2) *infrastructure hijacking* (a well-known but now obsolete example is phone phreaking), (3) *vulnerabilities development*, (4) *botnets*, and (5) *dark networks*.

Dark network techniques have developed because hackers understand how important it is to their tradecraft to maintain multiple active countermeasures to being tracked by competitors, law enforcement, or other hackers. There are several critical elements that highly paid hackers (i.e., those paid in millions of Euros), like our

hacker Yuri, use to escape identification and tracking, including the following:

- **Data fragmentation transports.** These systems, such as BitTorrent or uTorrent, mix up the data into a jigsaw puzzle. Systems like torrent networks rely on the use of P2P technology to rapidly disseminate information from decentralized sources. One of Yuri's techniques is to post a file (e.g., a picture file that contains malicious code destined for a transnational criminal network) by posting the picture (e.g., "HotGirl345.jpeg") onto the Pirate Bay. Yuri then sends a message over an IRC channel to Mustafa about the picture. Once Mustafa acknowledges that the message has been delivered, Yuri simply releases another picture file, also called HotGirl345.jpeg, onto the Pirate Bay, but this time without the malicious code, effectively erasing the first. Or, if not erasing, at least diluting out and corrupting its content, since torrent clients will inevitably mix up one HotGirl345.jpeg with the other via piecemeal downloading of multiple files before reassembly. The net effect is that since downloads will occur from multiple sources and files, the malicious code will simply be "diluted" out of existence during reassembly. In other words, Yuri will have succeeded in erasing his tracks as well as any evidence of malware through global information deletion by exploiting the nature of the fragmented downloads used in torrent-like P2P file distribution systems.
- **Overlay networks.** These systems, including Freenet and Darknet, create new topologies and use fragmentation as well as data and temporal encryption methods. Overlay networks use the Internet as a base network to create a virtual overlay using special clients and servers. Well-known techniques such as frequency-hopping spread spectrum encryption, wherein a message is encrypted by dividing it up over different frequency bands, hopping from one frequency spectrum to another so that the listener can never get the whole message, has its digital analogy in using multiple "spread hosts" as multiple messaging services on the Internet for equivalent encryption by dividing up message pieces onto many different hosts. It becomes easy to send out files and confound the information by sending out junk files. This is done by posting multiple files with the same name and similar, but not identical, content; only the hacker knows which one is the real file after the real and intended files have been acknowledged as delivered by their receivers. In this way, it is difficult for others to trace a piece of information from the sea of message files. The newest overlay is VoIP, and bots can immediately interchange information using VoIP protocols and cause SPIT (SPAM over Internet Telephony),[21] which may be used for real-time communication.
- **"Hidden in plain view" methods.** These systems bury information in broadcast email spam or as individuals hiding in chat rooms, using, for example, multiple languages, alias changes, identity shifting, and semantic encryption. Yuri, like many other hackers, speaks several languages and can carry on multiple communications concurrently in multiple languages via multiple chat rooms. Yuri does this because he knows that traditional techniques to identify, translate, or analyze the hidden networks forged by these communications over multiple chat services simply fail. One of Yuri's other favorite tools is to use the NiceText cipher system to generate messages while rotating a lexicon through either a temporary Web page (where his update is posted) or through another chat line. For example, if Yuri wanted to send a message such as "I own the Pentagex trade secrets," then the ciphertext might read "My blue roses are of sky in their skies." Sending "I will send you the Pentagex documents today" may then read "A clear lagoon holiday likes sea pearls of lagoons." Clearly, communications networks like this become impossible to identify, even by humans, and Yuri knows that while the US may own leadership in traditional cryptography, his semantic cipher can easily withstand any decryption attempt as long as his lexicon rotations are maintained and undiscovered.
- **Skill barriers.** Getting into a secured game room takes a considerable level of skill, including skill transactioning, media steganography, and situational encryption, or privy access. Yuri, from time to time, likes to use his preferred online games as communications environments to coordinate his criminal and other activities. Yuri is one of those game players who is extremely good; he can get to "hidden" areas in vast multiuser online worlds. As a master gamer, Yuri can make extra money by selling his game positions to others who can use them as temporarily secure, compartmentalized communications environments simply because the skill level needed to penetrate the game's hidden treasure areas are too high for most folks.
- **Hijacking.** This is merely getting possession of someone's computer or data using vulnerabilities and viruses, wireless and RFID identity theft methods, and physical methods. Here is where Yuri will recruit some help: he will need his onsite recruits to go through trash, sit at airports with wireless devices

and pick up information, or maybe even pickpocket or use other known field methods to acquire critical pieces of information. This information will then be sold to Yuri, who pays well. Yuri himself had been successful in using cell phones (i.e., stealing, modifying, and replacing) to target other cell phones for use in direct spying. In one instance, Yuri had hacked the telephone company's switching boxes (anyone can see these telephone service boxes near any neighborhood), most of which have no camera surveillance, so criminal methods cannot be traced (since Yuri can drive by, use service lines directly, and leave).

- **Non-obvious protocols.** These include use of Alternate Data Streams (ADS), Multi-User Dungeon (MUDS), Bulletin Board System (BBS), and X.25. While most of the world may use HTTP (or TCP/IP) standard Internet protocols, because Yuri lives in Eastern Europe, he has the advantage of being able to use a vast network of older protocols (e.g., Telnet, X25, and others). In fact, the use of acoustic modems is still done via pay-as-you-go or disposable cell phones. He can also use VoIP for secured and hard-to-intercept transmissions. Additionally, BBS and MUDS, as well as chat systems, can use alternate protocols where many open source intelligence efforts are thwarted due to the close-knit communities of users that set them up, use them, and then take them down.
- **Marketplace and public systems.** These include emails, websites, and ATMs. It is quite easy to hack email and to use email servers for communications for logistics and to control dark hidden networks. Yuri uses the technique of inserting Web pages into public corporate websites, usually buried deep into site maps, so his related hackers or their botnets can use, for example, semantic ciphertext-written sites, which can form a temporary hub of communications between botnets or hacker groups for coordinating activities. Yuri prefers to use ATM cards for cash transfers since he can mail them to anyone; many gamers and hackers like to be paid by being provided ATM cards that they can use anywhere/anytime through foreign sources of funding or through proxies set up with multiple smaller accounts. This leveraging of marketplace systems forms just one part of the financial network that Yuri, as an integral part of the dark networks, can utilize — as well as direct credit card and ATM fraud.

Yuri has found that not everything can be done in cyberspace alone, so he judiciously chooses to trade with those hackers that can physically steal trash, computers, wallets, or whole identities by plowing though and harvesting US government building sites for information such as Social Security numbers, addresses, and automobile registrations from local and state legal sites. The most dangerous hackers may travel and use their computers in hotels, lobbies, cafes, and rest areas, which are often proximate to airports or large complexes. These hackers know that they can "ride" the airwaves and scan for RFID identity information (hidden in passports) or intercept wireless computer communications by generating fake router information. For example, a portable router can be used as an access point; a hacker can use his or her computer in a public space, such as an airport, to capture packet traffic from nearby users and steal their credit card information. All this can be done with the use of free software, downloadable from the Internet, a laptop, and about $100.

Yuri is not your typical hacker because he is seasoned and well versed in all patterns of multimodal vulnerabilities development as well as multisource operations based on botnets and communications using dark networks. He vigilantly develops his tradecraft through continuous and rigorous study of freely available publications via Google searches and IRC trades. However, much of the core information is usually found in out-of-date sources on the Internet, since critical methods are preserved and propagated only within dark networks. Yuri's own hacker groups are highly secretive and their secrecy levels challenge the security that any US intelligence agency has in place today.

PENTAGEX VULNERABILITY: YURI'S ATTACK BEGINS

Yuri calls on his friend theRixter, a hacker living in the Bronx, New York, and through the Darknet, explains that he needs the personal account materials of one or more of the top Pentagex executives. Yuri sends theRixter the executives' addresses, which he purchased using an online "people finder" service. Armed with this information, theRixter, a lad of only 19 years of age, launches the attack.

theRixter is a master wireless protocol hacker. He carries with him his own portable USB-powered router and trolls the upper-class neighborhoods for target signals. Many homes have wireless routers present. theRixter understands that a common choice in most routers is WEP (Wired Equivalent Privacy), which typically means creating some complex passphrase the router will need to see before it allows a computer to log on. The problem is that these passphrases, no matter how convoluted, can be hacked in under a minute; theRixter has developed the tools and techniques to crack WEP in under 15 seconds.

After a few hours of trolling the various addresses Yuri provided, theRixter strikes gold! People are habituated to older methods such as WEP because they use them at home, taking for granted that they are secure. Unfortunately, this also means that new, more secure methods, such as WPA2, which are far superior, do not get used, simply because people are habituated into a status quo. theRixter knows that most people, sooner or later, will bring some of their work home with them, and, sooner or later, an email will be sent. So theRixter spends his next few days waiting, knowing that the weekend is usually when work is brought home in preparation for that big Monday morning board meeting. Once again, theRixter strikes gold and captures the log-on passwords that a certain Alex Richner, the CFO of Pentagex, has used from his home computer — thanks to one of theRixter's socially engineered utilities, a handy little file shredder that also reports and intercepts a user's keystrokes for passwords relaying them whenever connected to theRixter's own database. theRixter immediately relays all his findings to Yuri who rewards him generously with a thousand-dollar bonus and a connection to some online free gaming.

There has been a steady increase in the number of vulnerabilities developed to exploit computers for use in cyber criminal operations or to steal valuable information. While it's difficult to acquire techniques, the one common element is that most hackers, like Yuri, use team-based brute-force cooperative probing: they work in teams, exchanging as they go, to probe an operating system, an application, or a database for defects. Others use reverse decompilation and reverse engineering techniques on the OS binaries (i.e., the ROM code). Yuri's personal favorite is the use of an in-circuit emulator (ICE). The pattern is the following: simply load an operating system onto a Pentium class machine, which has the Pentium ICE inserted. ICE is typically used in development for debugging programs, but, in this case, Yuri uses it to capture *everything* that running an application, for example, does on startup. From this point, he can look at seldom-used functions and write code to take advantage of the presence of a target application on a system, or even on the OS itself (i.e., to develop Trojans and backdoors). Complementary to ICE are software emulators, disassemblers, and other tools.

Yuri has tapped into much vulnerability over the course of his criminal career by a simple understanding of the source codes of open source products, such as MySQL, that many of his corporate targets utilize for various data stores. For example, SQL injection attacks utilize the Web forms interface to enter executable code commands to instrument and probe the database behind a Web page; Yuri often uses this technique to post his cryptic messages so that his community of interest can get the information anonymously. The technique is so easy; anybody can do it by simply downloading hacking how-tos from Google searches (which are a favorite tool of Yuri's). One particularly nasty technique for vulnerability development is cross-site scripting and executable strings. Yuri learned about this method through YouTube, where full details on how to achieve cross-site scripting are provided.[22] Of course, Yuri understands that he needs to combine other methods (e.g., SQL injection attacks to get usernames and passwords to gain access); hence, these tutorials are for advanced users.

It is much, much harder to catch a sparsely spread group that seamlessly operates through the dark networks than a lone-ranger type.

Yuri's Botnets

Yuri cannot do it all alone, all by himself, although he has been known to achieve certain hacks single-handedly; these days, that style is rare for one as experienced as Yuri. He prefers to let others try the single-handed approach knowing that they will most likely get caught. It is much, much harder to catch a sparsely spread group that seamlessly operates through the dark networks than a lone-ranger type. Yuri is, therefore, collegiate with several other master hackers, a few of whom own and operate one or more botnets. For example, one botnet can be used to generate email spam that can serve the dual purpose of coordinating messaging and logistical operations online, while another botnet can be connected to online chat rooms communicating to a botnet that collects information elsewhere, which can relay this to yet another botnet managing temporary distributed phishing sites. Yet another botnet can provide a dynamically changing dark network by shifting Internet packets to alternative protocols to conceal information flow, especially in high-value targets such as Pentagex. Another can use proxying to reroute and hide the surfing of Yuri and his hackers on sensitive sites when and as needed (e.g., government, military, and other sites, such as Social Security site servers).

Yuri calls on his old school buddy and fellow hacker Frederic in order to maintain a technology watch so that none of Yuri's mission-critical systems is taken down, exposed, or compromised in any way. Frederic reports that there are some new and advanced systems such as

Phalanx,[23] but these could be targeted by Yuri's smart and adaptive botnets, which can sense when there is a system like Phalanx in operation (i.e., the bots can know when they are being thwarted rather than simply being insect-like bits of software blindly committing attacks). Frederic's conclusion is that it's unlikely that Phalanx could defeat a multimodal, multilateral attack of several coordinated botnets, run by smart-thinking humans, because Phalanx makes the assumption that the botnets are simple and static with a fixed strategy of operation, and are essentially rules-based. None of which is true, since the humans in the loop change everything all the time. Yuri is content.

There are myriad ways to insert and operationalize botnets. The latest trend has been seen in the Storm system.

Yuri receives the files and the data from theRixter by downloading the movie *Deep Throat*, which theRixter has manipulated by inserting information into the digital picture encoding. Because theRixter has a few megabytes of information, he uses a movie to hide it. Yuri watches a few of the opening scenes and then stops. Next, he loads up his decoder having shared the encoder with theRixter. Once he runs the movie through the encoder, instead of the now familiar opening scenes, he sees regimented rows and columns of a key Pentagex Microsoft Excel spreadsheet with information about key product members, milestones, costs, and release dates. He also finds out that a new product Pentagex is planning to release has some funding codes that he knows only the DoD would use, codes such as "BAAxxxx" (numbers have been hidden to not reveal possible BAA codes). This innocent-looking piece of information means that Pentagex is obtaining funding to develop some kind of new antifraud, antimoney-laundering process into its newest technology. Yuri now realizes that penetrating Pentagex may have far more risk than he had previously thought. He needs to decide to go or no-go. This is a critical decision.

So Yuri calls up Mustafa and renegotiates. He tells him that things have gotten more complicated due to the US military and law enforcement relationships with Pentagex. Mustafa argues that Yuri is trying to back out of the deal. Yuri explains that more money is needed because both Yuri and Mustafa could be exposed. The two reach an agreement: Mustafa will raise an additional $250,000 for Yuri to acquire resources and another additional and equal amount as a delivery bonus. The total of half a million more dollars in cost has been approved. Mustafa's clients feel the risk and commensurate cost is worthwhile to procure a key piece of US technology — not to mention the run on the stocks they have already planned. Yuri is back on.

Yuri plans to swamp the NY regional Internet exchange, which includes Pentagex, with bogus threat traffic in order to hide his access to the real information he intends to procure. There are myriad ways to insert and operationalize botnets. The latest trend has been seen in the Storm system and the newer socially engineered malware systems.[24] These systems utilize applications to load or inject Storm bots into the host computer and then mimic and hijack the look and feel of bona fide companies and websites. Thus, Yuri looks through his set of cracked and hacked websites and plans his strategy of cyber warfare as a decoy against his true target.

Some of Yuri's university friends had developed botnets for purely financial reasons, such as market analysis, advertising analysis, and customer value propositions (e.g., peer-based search techniques). These types of botnets were intended to serve the needs of business intelligence and competitive intelligence. Yuri decided to mix things up by hijacking these botnets, though not designed as malware, and repurposing them to become significant and powerful weapons in his hands. His goal was to add traffic to the mix of his own malicious viral botnets to degrade, deceive, confuse, and confound detection systems that he knew regional ISPs would have. Finally, Yuri called on another New York buddy, manixMask666, a master of voices, disguises, and hypnosis, through his IRC alias UR33 and his NiceText cipher. The encrypted communication is illustrated in the sidebar (with decrypted translations in bold).

manixMask666 knew exactly when CFO Alex Richner would be out of town, so he set up studying Pentagex and memorizing the patterns of Alex's voice. He dug through the unshredded corporate trash and found several useful documents, including one with a printed memo for employees to change security passwords regularly. manixMask666 had indeed studied the CFO's voice well. When Alex left for the airport, manixMask666 phoned in, pretending to be the CFO, hurriedly and desperately seeking his network password, citing the memo. The help desk was happy to help. In the few weeks that manixMask666 had available, he spent regular times every other day developing a friendship with the janitor, Sammy Birch, gently bringing him into a more trusting state using suggestive hypnosis. That evening, Sammy let manixMask666, his new best friend, enter Alex's office. Once in the CFO's

ENCRYPTED COMMUNICATION SAMPLE

2011-06-01 15:20:00.0 : *** _ UR39 changes topic to ` * @Pick looking for _UR39's 8k bots.. <@_UR39> i gave em to dark <@_UR39> ask him <@ddark0> ya <@ ddark0> i have only 2k of em 2011-06-01 15:20:00.0 : * +hotrockettes bends over backwards.
2011-06-01 15:20:00.0 : <+hotrockettes> LOL
2011-06-01 15:20:00.0 : <@manixMask666_> damn
2011-06-01 15:20:00.0 : <@manixMask666_> Whaddya need?
2011-06-01 15:20:00.0 : <@_UR33> days of wine and roses ha ha ha!
2011-06-01 15:20:00.0 : <@_UR33> I need you do to a physical onsite target.
2011-06-01 15:20:00.0 : * +hotrockettes giggles.
2011-06-01 15:20:00.0 : <@ manixMask666_> o_0
2011-06-01 15:20:00.0 : <@ manixMask666_> Tell me about the target.
2011-06-01 15:20:00.0 : *** _UR33 sets mode +o hotrockettes
2011-06-01 15:20:00.0 : <@hotrockettes> thx babe.
2011-06-01 15:20:00.0 : <@_UR33> there's no pet xaneg better way to say I love you :
2011-06-01 15:20:00.0 : <@_UR33> Target is Pentagex, need you to study CFO's voice and call in.
2011-06-01 15:20:00.0 : <@_UR33> np dude
2011-06-01 15:20:00.0 : <@ manixMask666> lol
2011-06-01 15:20:00.0 : <@hotrockettes> manixMask666, i restored his faith in women.
2011-06-01 15:21:00.0 : <@hotrockettes> haha
2011-06-01 15:20:00.0 : <@ manixMask666_> ha ha back at you today we're all flowers aren't we?
2011-06-01 15:20:00.0 : <@ manixMask666_> Send me a phone recording of the CFO and what you want.
2011-06-01 15:21:00.0 : <@ manixMask666> :p
2011-06-01 15:21:00.0 : <@hotrockettes> it was funny.
2011-06-01 15:20:00.0 : <@_UR33> Goodbye baby blue eyes, no one's gonna make fool of u
2011-06-01 15:20:00.0 : <@_UR33> CFO is out of town this Thursday, call in for internal net password.
2011-06-01 15:21:00.0 : <@hotrockettes> =P
2011-06-01 15:21:00.0 : *** Joined SA7ORA ^_^ i (vincent@h-68-167-85-162.nycmny83.covad.net)
2011-06-01 15:20:00.0 : <@ manixMask666_> make my day baby and will you gimme some sugar?
2011-06-01 15:20:00.0 : <@ manixMask666_> consider it done, upload notes CFO voice to usual place?
2011-06-01 15:20:00.0 : <@_UR39> U're way to cute
2011-06-01 15:20:00.0 : <@_UR39> OK, it's on its way, bye!
2011-06-01 15:21:00.0 : <@hotrockettes> i had a good time, tho.

office, manixMask666 logged onto the computer for Yuri to hack into. Meanwhile, an oblivious Sammy continued his janitorial duties.

READY TO LAUNCH BOTNET ATTACKS

Yuri got a message on Twitter and knew then that manixMask666 had succeeded in his mission and now Pentagex was wide open. Moving on to the next step, Yuri called on his friends kidcid and drone5 to launch their botnet attacks.

Yuri had already shopped around for bots and servers to hide information sources, as the following relatively recent advertisement, one of which Yuri considered, illustrates:[25]

> *Botnet Hosting Servers*
>
> 5 Ips that changes every 10 minutes (with different ISP)
>
> Excellent ping and uptime.
>
> 100 percent uptime guarantee. Easy Control Panel to add or delete your domains thru webinterface.
>
> Redhat/Debian LINUX OS. SSH Root Access.

The advertisement helped Yuri gain access to a very large-scale botnet market with the key point being that the network identity keeps changing every 10 minutes, making legal tracking extremely difficult. The most damaging kind of technology in use by Yuri is, without any doubt, botnets, because they:

- **Leverage the Internet architecture itself to convey extremely sensitive information.** For example, certain servers become active and come "online" for short durations, during which encrypted data can be transacted. Then the servers are taken "offline" (i.e., their IP addresses appear and disappear very quickly); this makes it difficult for others to act against or intercept such "fleeting" data. Corporations can use this same technique to avoid getting hacked by interception attacks.
- **Are used to coordinate with in-the-field criminal operators and provide location-aware intelligence collection capabilities,** which are situationally relevant at short time scales (e.g., interception of credit cards and other privacy-related information). In the future, corporations might fight back using intelligent software agent technologies to thwart these types of activities by injecting deception information into the botnet traffic to the point where botmasters will not know that the logistical or operational data they are getting is fake and has been spoofed by corporate security. This will make it difficult for transnational criminals to continue to work with impunity in corporate bodies.
- **Are able to scale beyond international, social, and cultural boundaries in both offensive and defensive tasks by providing immediate, precise action against a target.** Consider the use of botnets to shut down a significant level of important traffic to Georgia. Larger corporations need to work with ISPs to help support router networks that can reroute at a moment's notice for their and other's traffic; we are all connected and the idea that the larger corporation is a standalone organization is no longer accurate (not that this was ever the case).

Yuri asked kidcid and drone5 to begin a gradual attack on the Wall Street hub. Within minutes, the Internet began to spike and load the systems. Yuri immediately began searching Alex's computer, looking up his full travel schedule, downloading his agendas, and opening up his email accounts, knowing that the attack was soon going to overwhelm even his connection. There, within the corporate intranet's emails, were the documents he had been looking for. Next, he opened the email attachments, uploaded his encryption code to Alex's computer, created the information packet, and then posted them, using Alex's own Web browser, onto one of Yuri's remote data sites. Yuri then immediately launched his defConVirus on Alex's office machine, and the virus began a DoD-level cleanup of Alex's computer, cleansing the hard drive of all of Yuri's code — and logs of activities — so that no trace of what had happened was left. Finally, the virus erased itself in memory and shut down Alex's computer; the operation was clean and complete. Pentagex networks continued to struggle with the increasing traffic from kidcid's botnets, while, for a few moments, the region was overwhelmed with packets until, just as suddenly, it all stopped. Yuri instrumented his remote server, changing its Internet address and rebuilding the information into a new set of pictures (with his favorite steganography tool), then posting them onto the pirate site. Finally, after the transmission was completed, Yuri launched his cleaner virus on his own server, erasing all traces. He paid kidcid and drone5 for their great work.

Mustafa was delighted to hear back from Yuri. Meanwhile, Alex was still out of town and unaware of what had occurred. Eventually, network security began analyzing the attack, but so much of it was packet noise recorded from the botnets that the security team was simply overwhelmed. It could not see the real information; it was like searching for the proverbial needle in a haystack amongst all the noise.

THE EXECUTIVE CHECKLIST FOR CYBER THREAT RISK MITIGATION

A week later on a cold, rainy Monday, an ashen-faced group of the Pentagex board of directors sat around its plush meeting room table with an acoustic void. Finally, Chairman and CEO Adrian Stanford rose and asked five questions that landed like hammer-handed blows to the table of senior executives:

1. Who is responsible and accountable?
2. What are the requirements to meet accountability with respect to the law, to the public with whom the company deals, and to the shareholders?
3. What business processes are needed to meet the requirements of providing security for the company?
4. What kinds of technologies does the company need if it is to defeat or thwart attackers?
5. What might a picture of cyber operations and cyber warfare look like in the near future for the corporation?

Adrian quickly learned that nobody knew the answers. Baines, head of business development, blamed the IT department; Gordon, from IT, forcefully pushed back, claiming that HR had failed in its screening protocols, while Evans, chief of HR, blamed Alex Richner himself. Adrian knew that no single person was to blame.

Adrian commanded the answer to be found within 48 hours, in time for the next board meeting on Wednesday morning. With that goal, Adrian called in a consulting group (CG) from a boutique firm; he had heard that this group was vendor-agnostic with access to the best people that could help him in a personalized and caring way. The consultants were brought on call for Wednesday's meeting and Adrian began by asking for help, "Please tell me what we need to know so that we can prevent another cyber attack and figure out if there are any attacks still occurring. We need five questions answered." The call then went as follows:

Adrian Stanford (AS): Who is responsible and accountable?

CG: The board of directors is ultimately accountable when anything in a corporate body goes wrong. It is a misconception to think that corporate information protection is in the hands of IT. On the contrary, members of the board and the senior management team are responsible for being aware, for being compliant to laws, for planning, for monitoring, for testing, and for validating that the implementation of an IT risk management system works.

An audit of the security of a corporation usually means hiring hackers to break in and expose all flaws, holes, blind spots, and business process failures. This is typically an unsavory step to consider, but necessary. Senior management must understand the risks in failing to go beyond sole sourcing or any single vendor's recommendations (or security consultants' egos) when it comes to safeguarding and maintaining a secure environment. In short, no person and no system is perfect and that is why diversity is needed when systems need to be penetration tested.

AS: What are the requirements to meet accountability?

CG: The Gramm-Leach-Bliley Act of 2001 specifies requirements, while more specifically the Interagency Guidelines Establishing Information Security Standards[26] characterize administrative, technical, and physical safeguards for financial institutions, but these really apply to any corporation.

Identity integrity (authentication, preservation of true identity, notification, and protection) has recently become a requirement in the Red Flags Rule.[27] If a corporate employee's identity is stolen, to what extent is the corporation connected (via credit cards and other material) to the compromised employee? A compromised employee means a compromised corporation. The two are not separate because corporations are "people."

AS: What business processes do we need to have in place?

CG: A company must have a security awareness training program for both employees and trusted partners in order to inform and educate personnel about information security risks as well as the responsibilities required of each individual or partner in complying with security policies and procedures designed to reduce risks.

Therefore, a company must put in place an education program that complies with workplace requirements that are compliant to regulatory requirements. To do this, a corporation should turn to the available expertise in those consulting firms that offer the highest diversity of security specialists in order to provide meaningful analyses and recommendations.

An audit of the security of a corporation means hiring hackers to break in and expose all flaws, holes, blind spots, and business process failures.

AS: "OK, I get all this, but it's too vague. We need a specific, concrete, tangible checklist. We don't want to contract someone else; we've already hired you. Can you provide a short list?"

CG: Absolutely, here's a checklist of 10 questions:

1. What kind of information security business process does the company have in place? Does the company even have one?
2. What goal does the company have with respect to its public posture, its internal posture to its employees, and its trusted partner posture? Does the company even have any media content that supports its posture and image?
3. Does the company have a security awareness practice? For the board and senior management team? For employees? For trusted partners?
4. Does the board have a solid understanding of the information security business processes? Does the senior management team understand what are the required policies?
5. What methods will the board and senior managers use to assess how well they themselves, the company, and the employees have mitigated risks?

Whom do they call on for outside security help to get them out of any blind spots?

6. Does management understand and have a schema as to what levels of security breaches cause what levels of corporate damage? At what levels are business operations interrupted? At what levels do corporate security failures lead to damaged or lost trust? What are the levels at which substantial financial loss and lost revenues occur? What levels add to the damage in high forensics and remediation costs?
7. Does the company have an inhouse security officer, and does that officer manage a comprehensive security strategy to mitigate both insider and outsider threats? Is there a proactive culture of security awareness and practices that identify, prevent, and respond to potential threats?
8. What safeguards are in place to protect internal, in-transit, and trusted partner information or data? Does anyone in IT have access to everything and anything, or is there a limited, need-to-know access policy? Who gets access to corporate networks and applications, and are there policies and protocols in place to mitigate the risk of unauthorized access? What is the password policy across all users? Who monitors and has visibility into all user access activities across disparate systems? Who is responsible for locking down all user network and application access in the event of an attack? What is in place at the company that protects physical access with software IT and data access?
9. Does the corporate security business processes integrate individual, group, and corporate-wide security policies with sign on and identity management? Does the corporation know who accesses its networks, when they are accessed, and by whom? Does the security and audit posture enhance user access productivity (or degrade it), and is it convenient or difficult to use?
10. Does the corporation have an internal forensics business process in place? Does it have business processes and cultures for proactive monitoring and analysis? Is the company aware of how many attack attempts are made on its systems, to what extent, and by whom? Does it have the appropriate technologies to support security-oriented business processes (e.g., separate key-based encryption for email and attachments)?

AS: "Thank you. We appreciate this checklist. Can you send someone down to help and do this … um … cyber inventory gathering process?"

CG: "Sure. But before we do, let's continue on in answering your five questions. You do want those answered, right?"

AS: "Yes, please go on. What kinds of technologies do we need?"

CG: Any mid-sized to large corporation is a target. The FBI estimates that losses at $100 billion each year due to "industrial espionage" through insecure email, first, and insecure data stores (e.g., USB sticks, hard drives), second. Consider the following requirements:

- PGP (pretty good protection) key encryption should be the minimum security requirement for email. Has this been implemented?
- Logging technologies are needed in order to have a manageable process for dealing with the high volumes of raw data from disparate systems, services, devices, applications, and databases. Is this in place?
- Infrastructure-monitoring technologies are required to examine data for anomalies, red flag them for review, and escalate the issue quickly to mobilize a response through downstream analytics. Do you use any?
- Analysis technologies are needed to get the intelligence that is required to enable sound risk management and/or to meet compliance requirements. What are you using right now?
- Personnel security technologies (e.g., sign-in cards, authenticated badges/cards, and identification devices) are needed to manage access. What protocols are in place?
- Penetration-testing technologies to regularly probe systems for weaknesses are required to maintain vigilance in security measures. Is anyone doing this work for you?

AS: What might corporate cyber operations look like in the near future?

CG: The future involves human-oriented, security-oriented, privacy-preserving business processes coupled with insider/outsider threat-monitoring business processes and technologies to support those processes. The chief security officer (CSO) will increasingly become a key player in boardroom discussions. The communications infrastructures as well as the social, cultural, and individual security policies will be made explicit by the CSO.

We have sketched five broad areas that we believe your chief/cyber security officer (CCSO) will need to set up as a baseline to govern total corporate security operations. Remember, these are top-level guidelines, and

we would need to work with you to fill these in with the details:

1. Physical Security Operations

- Physical access, buildings, locations of hardware servers containing critical data
- Access keys, identity cards
- Wired LANs

2. Wireless Security Operations

- **Wi-Fi coverage management.** How far outside the building does it go?
- **Wi-Fi signal operations.** Many devices actively engage in automated association when an unauthorized Wi-Fi network with a stronger signal than that of the corporate Wi-Fi network becomes available.
- **Wi-Fi cultural social engineering.** Corporations that restrict use of the Internet to its employees, as well as to prevent malware from entering the corporate network by enforcement via a corporate firewall, often tempt employees to deliberately connect to unauthorized Wi-Fi networks in order to gain full-blown Internet access. There are solutions that accommodate access, security, and productivity.

3. Human Security Operations

- **Security awareness.** Consider this for senior management, trusted partner, and employee training programs.
- **Intracorporate human intelligence operatives.** Professional hackers should be hired by the company to find ways to compromise security, identify potential insider threats, and to report findings of compromise to senior management for effective action.
- **Security hygiene training.** Make sure your browser caches are cleared after sessions, ensuring you do not keep materials on USB sticks that can fall out of your pockets; authenticate whom you intend to answer security-related questions, and so forth.

4. Application Security Operations

- **Application provenance.** Potentially untrustworthy sources of software, for example, are within the US; this includes Russian, Chinese, and other Asian sources.
- **Auditing outsourced code.** Outsourcing operations for developing custom inhouse applications or tools are targets for hidden holes or even malicious intent.
- **Ensuring mission-critical systems are on hard-to-hack systems.** This includes customized versions of Linux or Unix and security-modified open source products with trusted security partners for assessment (boutique consulting firms and inhouse security personnel can do this type of job).

While many well-established processes and products exist for tracking external attacks, less oversight and protection is made for identifying the human dimension.

5. Security Vigilance Operations

- Membership in security organizations such as Information Sharing and Analysis Center (IT-ISAC)
- Continual monitoring, testing, and training
- Working with and proactively developing liaisons and links with law enforcement and national security agencies such as the FBI; this is particularly important because targeting by hackers today includes:
  - Hackers that masquerade as security consultants but in reality breach the business environment.
  - Hackers that take advantage of social engineering schemes.
  - Hackers that work for organized crime but engage as trusted partners.
  - Hackers that enable insider threat — in most cases, the insider threat is inadvertent, while in other cases authorized access to data is being taken advantage of for malicious purposes that may, to the target employee, appear innocent. Organizations must comprehend the impact of these threats, both in terms of regulatory compliance as well as overall business risk. While many well-established processes and products exist for tracking external attacks on information, or software-only focused attacks, less oversight and protection is made for identifying the human dimension (authorized users inadvertently handling information in unauthorized ways or being manipulated into doing so).
- Analysis of user activity inside/outside corporate body (i.e., collaboration with law enforcement) — reports on all user activity including, but not limited to, email, Internet, and Intranet files accessed, files created and deleted, and user access times.

AS: This has been a very valuable phone call, and I am at a total loss about what to say other than thank you. But what I still don't get is how they managed to open the door to my office?

CG: There are many ways ranging from direct break-in to advanced social engineering using hypnosis, hypnotic-enhancing drugs, false friendships, women, bribes, and other means. Let's coordinate a visit to ensure we get our folks over to help you so we can learn how the entry was specifically made. Our team includes professional hackers as well as top security personnel. Several hold current US security clearances and will do more for your company than anyone else because they are committed, not only to the safety of the infrastructure at Pentagex, but to everyone's.

Social engineering is here to stay so we all need to take a step back and be reflective of ourselves; without reflection, therein lies our own blind spots that are visible to the observant hackers.

EXECUTIVE SOCIAL ENGINEERING COUNTERMEASURES STRATEGY

For the purposes of this report, I have told you a story, a fictionalized account hiding the facts of real cases, but one that nonetheless reflects reality. At this point, I am going to leave behind the tale of Pentagex and switch to my role as a Cutter Senior Consultant, writing to you as a technology journalist and as a professional, bringing you the facts as they have developed in today's context of cyberspace, cyber awareness, and cyber security.

In the remainder of this report, we will focus on two aspects: sociological and technological. Social engineering is here to stay so we all need to take a step back and be reflective of ourselves; without reflection, therein lies our own blind spots that are visible to the observant hackers. Basic technical countermeasures can be implemented by understanding a few simple things:

- The role of the executive has changed.
- Executive management and its information assets are direct targets.
- A dark network, information-trading economy drives hackers to target executives.

Hackers will always work hard to invent new ways of infiltration into organizations with commensurate exfiltration of high-value information. More damaging and hard to predict or protect are medium-to-long-range operations, where moles penetrate the critical infrastructure of a company. What can senior management do transform a mole?

A corporate climate of anti-patterns,[28] "cults of personality," "charismatic authority," "hero worship," betrayal and deceit, one-upmanship, destructive internal office politics, and morally questionable competition for advancement will engender and support the hacker's ability to compromise and damage the corporate body. Do you love to go to work? Why? Why not? Do you trust the person in the office next door to catch you if you fall (that's an oldie but goodie and was once part of corporate cultural training offered by some consulting firms)? Do you care if the third person down the rung of the ladder from you gets fired? Do you know the third person down? Do you know his or her spouse's name? Kid's name? Do you the name of the grandchild of the chairman of the board (if he or she is of age to be a grandparent)? Where are you having difficulties in your workplace? Do you blame anyone for any difficulties? Is there someone that is always causing trouble? Who do you dislike? Why?

By considering these and other questions, your role in company life, your position, and your communicative network becomes visible to you. It is in the blind spots of these networks of conversations and relatedness (e.g., being related is knowing the spouse's name of a coworker and having had them over for dinner) in which hackers adept at psychosocial engineering can operate with impunity.

So what is the overall answer in how to thwart the social and cultural cyber threat? The answer is very simple: provide a caring, aware, and positive work environment.

Developing a sense of community; building teamwork; developing strong, mutually supportive ties and relatedness amongst coworkers (e.g., office picnics); and developing the concept of "play" as integral and as important to the concept of "work" produces a climate in which any mole working in a long-range operation will have issues of allegiance to his or her original goals and may even "switch sides" — confiding to executives about an impending attack, or, in the other extreme, leaving the company and advising the FBI of the situation via anonymous messaging. Humans are not robots and do not follow rigid rules, remaining within rigid commands or goals. If the incentives to perpetrate an act are removed, the act will no longer be perpetrated.

One of the primary incentives behind successful cyber attacks today is that of disgruntled employees. When firing an employee, consider your company as a route to help the employee find another job; consider an office ombudsman whose one job responsibility is that of helping a fired employee get a new job elsewhere.

In the end, it is all about how you, the senior executive, leave people feeling after you have had a conversation with them, especially if the conversation is about firing someone. The concept of how you leave someone feeling after you have interacted with them also applies to trusted partner relationships. If you leave your trusted partners feeling a certain way, perhaps negatively, after a conversation, will that partner continue to be trusted or to trust you? These are the kinds of very difficult issues that executives face.

Therefore, one of my strongest recommendations is to hire a consulting firm that specializes in corporate cultural development, integration, and training in leadership through positive incentivization. Positive incentivization includes assessing and taking care of employee fulfillment, greatness, and success-oriented thinking. People are the strongest and weakest asset of a corporate body; they must be cared for as well as protected against social engineering, the most powerful and devastating weapon that exists.

Enterprise dynamics involve computers and people, other corporations, buyers, and sellers. Senior management is responsible and accountable for all corporate dynamics, good or bad. Its role — in the new economy of cyber threats — is to understand, acknowledge, and deal with the environment that creates or supports those threats, to mitigate the risks of threats, and to create spaces in which the likelihood of threats are extremely small.

Individuals who telecommute do a lot of work for corporations. Telecommuting is a wonderful way to reduce costs and increase market presence as well as a way to provide services and call center support. However, telecommuters must also be brought into the space of the corporate community, which includes security as well as social and community relatedness. Today's hacking enterprise is in the hundreds of billions of dollars, with attacks in the hundreds each and every day. Do you screen your potential hires, and does HR follow up with adequate due diligence (checking references)? We, as humans, are all trusting by nature; therefore, attacks that involve manipulating people and end users and even yourself are the greatest vulnerabilities. Social engineering of your own environment is the key to thwarting the engineering of that environment by others for malicious purposes. Sometimes, advanced techniques such as hypnosis, drugs, sexual partnerships (that may be scandalous), and other approaches may be used individually or in combination to break a target individual into giving up corporate secrets.

THE EXECUTIVE TOP 15 COUNTERMEASURES CHECKLIST

Know the enemy and the multitudinous guises it wears. Know your weaknesses or inadequacies and those around you. Do not trust vendor security solutions at face value; ask a third-party vendor-neutral consultancy firm to validate the performance or audit security. Do not believe marketing propaganda; check the facts. Analyze the workplace community, sentiments, and opinions. Don't just put these items on a "to do" pile for later; act on them now.

Here is my 15-point checklist of the condensed hacker's most popular styles of attack:

1. Applying for a job such as janitor, or other worker, to gain access.
2. Identifying and targeting disgruntled employees or ex-employees.
3. Web and personal social engineering.
4. Exploiting specific protocol implementations.
5. Attacking built-in authentication systems.
6. Attacking through HTTP and SMTP applications; these are frequently attacked because most firewalls and other security mechanisms are configured to allow full access to these programs from the Internet.
7. Attacking through malicious software (malware); these includes viruses, worms, Trojan horses, and spyware. Malware clogs networks and takes down systems.
8. Wreaking havoc on system availability and storage space through spam; this can carry malware.
9. Breaking file-system security.
10. Cracking passwords and encryption mechanisms.
11. Connecting into a network through a rogue modem attached to a computer behind a firewall.
12. Exploiting weaknesses in network-transport mechanisms, such as TCP/IP and NetBIOS.
13. Flooding a network with too many requests, creating a denial of service (DoS) for legitimate requests.

14. Installing a network analyzer on a network and capturing every packet that travels across it, revealing confidential information in clear text.
15. Piggybacking onto a network through an insecure 802.11b wireless configuration.

Hackers prefer attacking Windows systems because they are widely used and better known for their vulnerabilities. Operating systems that are more secure out of the box, such as Mac OS X, Novell NetWare, and other types of Unix, are harder to attack. Hackers use software, such as NetStumbler and Kismet, and other commercial scanners to survey the airwaves for rogue access points and some network vulnerabilities. When was the last time your network administrator physically walked through the wireless LAN coverage area with a scanner to pick up data to identify all access points and wireless LAN traffic zones for security? How secure is the cloud environment you plan to use? How do you know that the cloud is secure? Who is telling you it's secure? The vendor or a third-party security auditor? What measures are in place? Who put them there? How do you know that they work? What data access policies are in place in the cloud? How are they managed? Who has access? Can the data be tampered with and changed?

How secure is the cloud environment you plan to use? How do you know that the cloud is secure? Who is telling you it's secure?

CONCLUSION

Professional, highly skilled hackers do not usually dress in business suits, advertise themselves in trade journals, or adhere to the normative standards we expect in the traditional workplace. Hacking is not a traditional enterprise and attracts nontraditional out-of-the box thinkers. They would have to be so or else they would not be hackers. Appearances can be very deceptive. Spotting a hacker is about considering competence levels and track records, which are often only through word of mouth and trusted references; indicators include past activities with security and other business intelligence organizations and relevant efforts as well as other credentials.

Security consultants, while many do wear suits, often partner with deep-skilled hackers (who don't necessarily don the dapper executive attire) and can provide synergies with seasoned consulting professionals. Together, a team like this can understand and communicate the highly technical and sometimes obscure findings of the penetration-testing teams and other technical groups that may be called into a security audit or support effort. This clear path of communications is critical to senior management, which is often the target of the hacking enterprise.

As we move toward cloud computing and into more extended corporate structures that are often more loosely coupled, there is the question of how such systems can handle data tamper-proofing, data integrity, and the chain of custody through various systems and services that, today, are loosely knit, far from tamper-resistant (in fact, downright easy to hack), and highly vulnerable.

Tamper-evident devices are as commonplace as the aluminum seals on most off-the-shelf medications. Integrated circuits used in cryptography may be tamper-evident as well as tamper-resistant. They can fry their internal information if tampered with, but even in these cases, tamper-resistance can be hacked effectively (e.g., smartcard and payment system hacks).[29] The closest thing to true tamper-resistance data today are digital rights management (DRM) systems. For example, tamper-proofing email (before it gets to the recipient) would be a significant value. At present, there is little available in the form of tamper-resistant data interchange other than cryptography for service-oriented architectures. This is a key area for growth as the battle against cyber intrusion is fought.

It is my hope that we all find ways to work with the diversity needed to deal with cyber threats because it is these same kinds of people — like the hackers we hire — who sit on the other side. Remember, you cannot step into a fight in a boxing ring unless you have practiced at that level.

ENDNOTES

[1]Pentagex is a fictitious corporation used here to illustrate the situation for corporations in general; any similarities in names in this report to persons living or dead is purely coincidental.

[2]"Former DOW Research Scientist Convicted of Stealing Trade Secrets and Perjury." Press release, US Department of Justice, 7 February 2011 (www.justice.gov/criminal/cybercrime/LiuConvict.pdf).

[3]"Two Men Charged in New Jersey with Hacking AT&T's Servers." Press release, US Attorney District of New Jersey, 18 January 2011 (www.justice.gov/criminal/cybercrime/auernheimerArrest.pdf).

[4]"A New Approach to China." *The Official Google Blog*, 12 January 2010 (http://googleblog.blogspot.com/2010/01/new-approach-to-china.html).

[5]"Cleveland, Ohio Man Sentenced to Prison for Bank Fraud and Conspiracy." Press release, US Department of Justice, 28 February 2006 (www.justice.gov/criminal/cybercrime/flurySent.htm).

[6]"Botherder Dealt Record Prison Sentence for Selling and Spreading Malicious Computer Code." Press release, US Department of Justice, 8 May 2006 (www.justice.gov/criminal/cybercrime/anchetaSent.htm).

[7]"Juvenile Sentenced for Releasing Worm that Attacked Microsoft Web Site." Press release, US Department of Justice, 11 February 2005 (www.justice.gov/criminal/cybercrime/juvenileSent.htm).

[8]"Russian Man Sentenced for Hacking into Computers in the United States." Press release, US Department of Justice, 25 July 2003 (www.justice.gov/criminal/cybercrime/ivanovSent.htm).

[9]"Disgruntled UBS PaineWebber Employee Charged with Allegedly Unleashing 'Logic Bomb' on Company Computers." Press release, US Department of Justice, 17 December 2002 (www.justice.gov/criminal/cybercrime/duronioIndict.htm).

[10]See http://en.wikipedia.org/wiki/Situational_awareness.

[11]Gibson, William. *Neuromancer*. Ace Book, 1984.

[12]See www.dtic.mil/doctrine/dod_dictionary/data/c/10160.html.

[13]"National Strategy to Secure Cyberspace." The US White House, February 2003 (www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf).

[14]See www.internetworldstats.com/stats.htm.

[15]See http://freenetproject.org.

[16]This book listing was taken from: Stevenson, William. *A Man Called Intrepid*. Ballentine Books, 1978.

[17]Carl, Leo D. *The CIA Insider's Dictionary of US and Foreign Intelligence, Counterintelligence & Tradecraft.* NIBC Press, 1996.

[18]See www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB24/nsa25.pdf.

[19]"China Cracks Down on Illegal Online Map Services to Protect State Security." *People's Daily Online*, Xinhua, 26 March 2008 (http://english.people.com.cn/90001/90782/6380703.html).

[20]Steganography is a way to hide in plain sight by encrypting information into pictures or photos.

[21]Schmidt, Andreas U. "SPAM over Internet Telephony and How to Deal With It." Proceedings from the *7th Annual Conference on Information Security*, Johannesburg, South Africa, 7-9 July 2008 (http://arxiv.org/abs/0806.1610).

[22]See www.youtube.com/user/Gregorpm and www.youtube.com/watch?v=WZCXIrW0xZ0.

[23]Dixon, Colin, and Thomas Anderson. "Phalanx: Withstanding Multimillion-Node Botnets" (www.usenix.org/event/nsdi08/tech/full_papers/dixon/dixon_html/index.html).

[24]"2008 Internet Malware Trends: Storm and the Future of Social Engineering." Cisco/IronPort, 2008 (www.ironport.com/pdf/Malware_Trends_Report_IronPort_2008.pdf).

[25]See blog.spywareguide.com/2006/05/interview_with_a_botnet_host_1.html.

[26]"Interagency Guidelines Establishing Information Security Standards." Board of Governors in the Federal Reserve System (www.federalreserve.gov/bankinforeg/interagencyguidelines.htm).

[27]"New 'Red Flag' Requirements for Financial Institutions and Creditors Will Help Fight Identity Theft." Federal Trade Commission, Bureau of Consumer Protection, June 2008 (http://business.ftc.gov/documents/alt050-new-red-flag-requirements-financial-institutions-and-creditors-will-help-fight-identity).

[28]Brown, William J. *AntiPatterns: Refactoring Software, Architectures, and Projects in Crisis*. Wiley, 1998. Anti-patterns clarify the negative patterns that cause development roadblocks due to poor management, lack of architectural control, or personality clashes. This book shows how to detect and defuse 40 of the most common anti-patterns.

[29]Anderson, Ross, and Markus Kuhn. "Tamper Resistance — A Cautionary Note." *Proceedings of the Second USENIX Workshop on Electronic Commerce*, USENIX Association, 1996 (www.cl.cam.ac.uk/~rja14/tamper.html).

ABOUT THE AUTHOR

Arun K. Majumdar is a Senior Consultant with Cutter Consortium's Enterprise Architecture practice. He is currently at the cutting edge in the industry, working with various companies and providing next-generation data to information and information to knowledge systems using various intelligent agent platforms. Mr. Majumdar has experience in the areas of software engineering, cyber analytics, hacking, object-oriented methods, agent programming, and Web technologies. He is a world-renowned expert in distributed knowledgebased computing. Mr. Majumdar is currently working on various systems for VivoMind Research LLC. He can be reached at amajumdar@cutter.com.