Chapter 7

Constant Vigilance

- Ten years ago, the biggest threat to your company's information came from your own employees.

  Not anymore.

- Ten years ago, an external hacker actually had to sneak onto your property to steal something valuable.

  Not anymore.

- Ten years ago companies bought firewalls and felt safe from hackers.

  Not anymore.

- Ten years ago, to prosecute a perpetrator you had to nab him or her on misuse of a telephone or some tangential law.

  Not anymore.

- Ten years ago most of your data was in one place.

  Not anymore.

- Ten years ago your corporate officers were willing to accept technology risk because it wasn't "their job."

  Not anymore.

- Ten years ago, I had just finished bringing out the top-selling PC security device—Centel's Net/Assure—and was moving to help launch secure eCommerce on the newly public Information Superhighway. I too thought that security products were the answer.

  Not anymore.

Ten years ago, the most important commercial asset on the Internet was reputation. Early Web sites were just electronic copies of annual reports or product spec sheets. The biggest damage came from someone hacking in and defacing one of two pictures on a home page. (Sometimes companies did this to themselves. When IBM launched its first Web page, they put up a "large" picture of then-CEO Lou Gerstner. However, the image was so large that most people couldn't even load the page, and if they did, their browsers could only display a feature or two—an ear or a nose or a chin.)

Constant-Vigilance Key Questions: CEO Focus

1. How has your infrastructure matched the changes in your business these past 10 years?
2. Who (besides you) is responsible for managing your corporate risk?
3. What changes do you track proactively that could be affecting your business?
4. What security-related changes are you tracking, and what do you do with the results?
5. Who on your board understands and cares about your risk governance?

Even though this may seem like a pointless exercise in nostalgia, I do have a method to my madness: We are not through the cycle of change brought about 10 years ago. Rather, we are right in the middle of it. Without maintaining constant vigilance, no security is safe. And now that operations, threats, and countermeasures quite often cross borders, you suddenly need to be vigilant on a lot more information in a lot more places. To do that, you need a system.

Not Anymore, Continued

Constant change is relentless in global corporate security; overtime regulations, threats, countermeasures, and the technology facilitating all of it morph to higher levels of magnitude and complexity. This inexorable progression needs to be figured into your company's global corporate security strategy. Five years ago you might have been more willing to take risks. Why? Risks were less significant than today. In 1988, there were roughly 100 reported security incidents via the Internet, and by 1996 there were nearly 350 in just the third quarter. Today incidents per year are in the millions, and these intrusions do not even begin to touch the issue of piracy. Nearly 40 percent of all the world's software is pirated, and in countries such as Pakistan and China those rates eclipse the 80 and 90 percent marks, respectively.

A typical organization with 100 servers and 3,000 PCs behind a firewall will generate 10 million security events a month. Of these, 500 to 600 require human intervention, only 50 will involve some malicious intent, and just 2 will have caused a problem.

—John Schwarz, President, Symantec, San Jose

Every element of charting a course—regulations, personal liability, corporate governance, greater awareness of the damage caused by threats, and greater reliance on computer networks to function as a business—have significantly evolved. In the past year, you might have asked your CFO about a potential violation of Zimbabwe's data privacy act, and he or she said not to sweat hiring a lawyer to descend upon Harare, but check this year and see what she says. Regulations are in constant flux.

To outpace change and to realize ultimate ROSI from your global corporate security strategy, remaining constantly vigilant on the following four fronts is critical:

- Threats
- Countermeasures
- Regulations and legal frameworks
- Technology

Threats are evolving fast, but by the time you read about them in your morning paper or news brief, you are already behind the curve. You need to have some insight into what is around the next corner (and the one after that). And given the very nature of the threats, it is mandatory to call your security package complete.

Luckily for you, countermeasures are quickly evolving. Not only do the biggest names in security products and services develop new tools, but there are also numerous smaller companies scattered around your world that will save you time, money, and significant headaches (or worse). Regulations and their various legal frameworks are written in sand at best right now. Not only are the "regs" different in every country you do business in, they also differ in the same countries, from day to day. Compound that with the evolving legal frameworks that you are relying on to protect you, which change from court case to court case, and from political leader to political leader. I know of one company that relied on one-year-old business intelligence for some operations in Bolivia, only to arrive to a changed government and legal system that disallowed everything they had planned to do there. The biggest mistake is assuming that *your* laws will work where *your* data goes–an assumption that could cost you significantly.

Finally, your COO will say that the only thing remaining constant from your technology providers over the years is the brand. Software is rewritten, acquisitions and mergers are common, and suddenly you are running a completely new information system after an upgrade. This can and does offer real challenges to your organization, and the best way to turn these changes into positives is to gear up with advance warning, advance copies, and advance planning. Do not be fooled by the sticker on the box or the logo on the startup screen; your technology is changing as you read this.

Constant Vigilantes: Where to Find Them

- **Technology**–Your tech group
- **Threats**–A trusted third party
- **Countermeasures**–Your security group
- **Regulations**–Your legal group

Even as you consider the people you will need, it is also critical to remember that the four fronts of constant vigilance, which are changing today, tomorrow, and forever, are out of your sphere of effective control, but they are within your sphere of adaptive control. However, you must know what is happening in each of these areas, and ROSI within constant vigilance is gauged by how cost efficiently you acquire this knowledge.

Deputize to Realize ROSI

You should be aware that in many cultures it is not appropriate to question authority. Doing what you are told and following orders is still the preferred management style in some countries in Europe, the Middle East, Africa, Central and South America, and the Asia Pacific areas. People are more used to questioning orders from a security perspective in places such as the United States and Canada. This questioning of the status quo is critical after your corporation

continues...

Deputize to Realize ROSI Continued

and your global security strategy are distributed throughout the world. There are too many nuances at work for you to maintain a handle on them all, and you need people who will come to you and say, “This won’t work because of this.” You need to go the extra mile when training and managing and find ways to specifically solicit the input you are going to need based on this cultural difference.

Ideally, these sectors are delegated, with specific reporting reaching up through the CSO. I have enjoyed success delegating each of the four to different members of my staff. For instance, in nearly any company, there are staffers who scour the chat rooms, list serves, and Web sites of technology companies. I would just create a process whereby I alerted them of information I wanted or needed and information that could be discarded. Although it takes some back-and-forth dialogue at first, soon you will have initiated a reliable, free-flowing channel of information.

Identify someone in your technology group, deputize that person as your information asset, train him or her as you want, and then let that person do what he or she loves to do. Each month, hold a pizza party in the evening to debrief and share information. It is fun, everybody learns something, and those you have deputized have a vested interest and role in helping the company adapt.

Tracking threats necessitates a more exhaustive route, and this cost is best shared with others—lots of others. Imagine trying to staff a team tasked with watching the development and deployment of every threat around the world. The bill for pizza and Coke would raise the eyebrows of your CFO. Luckily, there are a precious few companies that do this on behalf of hundreds and thousands of clients around the world, and this allows them to employ a large enough staff, vast enough technology, and deep enough experience to provide the right information at the right time and in the right manner. After you have deputized your information asset infrastructure, these considerations must be correlated with your business requirements. It demands a routine loop back to department heads and business owners to let them know what has changed. In turn, they should report on what has altered for them and, in light of the latest global security intelligence, what level of risk they are now willing to live with. Ultimately, they are the ones who stand to gain or lose from the process. This virtuous circle, comprised of trend spotting, reporting, adapting, and correlating is what I call *constant vigilance*.

Threats

In a global corporate security stance, keeping an eye on threats correlative to which ones are relevant to you is extremely important, and here's what you need to know. Threats come in two varieties:

- General attacks
- Targeted attacks

Both demand awareness. This does not mean that you need to become a regular at Black Hat or Def Con conventions or read *2600* magazine. In fact, you do not even need to know that the *lingua franca* of the hacking underground is Portuguese—the most active hacking collectives are located in Brazil. However, your global security team does need to stay current. If you run UNIX BSD and there exists a new UNIX BSD threat posted by rya (Rooting Your Admin), you will need to act.

Newest Hacking Threats in Business Terms

- **DoS attacks**
  Hackers are now using "standard" viruses to launch *denial-of-service* (DoS) attacks on specific companies or industries. Computers by the thousands are being turned into unwitting zombie machines, ready to launch coordinated attacks against anyone who is targeted by the latest hacker. Examples include MyDoom and Slammer (the latter of which targeted banks).
- **Black holing**
  Another type of hacker attack is black holing, which I call *corporate identity theft*. Someone completely out of your control can issue a command to many of the routers that make up the backbone of the Internet. Anyone who tries to link to your site through one of these routers will be *redirected* to the hacker's site—either a black hole of empty space or a fake site that looks just like yours that was designed to entice customers into typing their ID and password.
- **Mail spoofing**
  Mail spoofing is the forgery of an e-mail *header* so that the message appears to have originated from someone or somewhere other than the actual source. Distributors of *spam* often use spoofing in an attempt to get recipients to open, and possibly even respond to, their solicitations.

continues...

Newest Hacking Threats in Business Terms Continued

- **War driving**
  The use of wireless technology is a great timesaver, and easy for companies to use. A lot of companies have it without even realizing it. War driving enables people to drive down the street with a $100 antenna and tap right into your organizational lifeblood, tap right into your intranet and your internal networks. It is like dropping a wire outside your office window down to the street with a big sign that says "Plug In Here."

Known Vulnerabilities and Known Exploits

If you knew that your company's warehouse door was often left unguarded for three minutes during a daily shift change, would you do something about it? A better lock? Change the shift schedule? Maybe add a video camera at the door? Perhaps. Or you might think, "It is only three minutes, and cameras are expensive"—no one will know that you are supremely vulnerable for those 180 seconds. Then, after the inevitable happens, and you have lost your property, you would overspend to make sure that the specific door would never be compromised again. That is the real world.

When you factor in the Internet, the question begins to look even more ridiculous to the uninitiated. I'm talking gaps of milliseconds on one open, internal password-protected port among thousands. Yet to a hacker, these types of commonplace vulnerabilities represent more than a three-minute open gate, and hackers capitalize on them every minute of every day, in every country in the world. Even though crime fighting is growing—among EU member nations, groups such as the UK's National High Tech Crime Unit sniff out and investigate cybercrime—hacking is still a favored pastime for the 12- to 20-year-old set.

Known vulnerabilities are weaknesses inherent within existing technology of all types. Exploits are hacker attacks on those known vulnerabilities.[1] Keeping tabs on what vulnerabilities exist in your hardware and software and discovering what new (or previously undiscovered) ones apply in both legacy and upgraded systems is absolutely vital to the ongoing security of your company. Keeping up with these threats is paramount.

[1] *Definition of "exploit," n.d., searchsecurity.techtarget.com/sDefinition.*

As your global security team prepares for new hazards, it should also master the technology hardware and software you run, knowing what its strengths and weaknesses are. All team members should have a card by their desk that literally lists this exhaustive roster so that it is easily referenced when threats are anticipated and dispatched.

One of the best, least-expensive ways to maintain constant vigilance on threats is by joining your country's *Computer Emergency Response Team* (CERT). CERTs were born in the aftermath of the world's first virus–the Morris worm–which infected fewer than 100 computers worldwide, when it was found that the world's collective of Web administrators knew only e-mail addresses. (What was needed was a list of phone numbers. With no computers working, they had no way to contact each other!) Its founders understood the long-term ramifications of threats and developed the very first CERT on Carnegie-Mellon University's campus in Pittsburgh. These individuals knew that a clearinghouse of confidential, yet available contact information must be readied and shared for the next-generation Web.

CERT Alerts Require Translation

Always translate CERT alerts for your CxO of choice. Tell me, how could they understand it if you quickly IM them this recent CERT high alert?

A Cross-Site Scripting vulnerability exists in the 'index.php' script in both the 'admincp' and 'modcp' application directories due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code.

The original CERT was a simple phone tree, and it evolved into the safe place to report threats, bugs, break-ins, and thefts so that information could be analyzed and redirected. CERTs have since grown, country by country, into independently run, cosmopolitan organizations. If you do business in Singapore, you would access SingCERT through the country's Information Development Authority (www.ida.gov.sg). Thailand runs a ThaiCERT, and Malaysia boasts a MyCert. You get the idea. If you are a legal, certified business, it is generally free to subscribe. CERT will help you put your own process in place for vetting exploits by delivering ongoing alerts and offering insight on how to create a threat-readiness posture.

CERTS are so successful, an international umbrella organization was created called FIRST (www.first.org). FIRST stands for the *Forum of Incident Response and Security Teams*, and it coalesces security-incident response teams that work in government, commercial, and academic organizations throughout the world. It "aims to foster cooperation and coordination in incident prevention to prompt rapid reaction to incidents and to promote information sharing among members and the community at large."

One indicator that new information-sharing links with federal governments are strategically important to top corporate executives can be found in the 13 *Information Sharing and Analysis Centers* (ISACs)—one for virtually every key vertical sector of private critical infrastructure. The companies participating in these ISACs constitute a who's who in their corporate world. For example, those looking for the Information Technology ISAC will find it at IT-ISAC.org. ISAC's are built around trust. It started with the financial services industry, and most major industries in major countries followed suit. You must be invited to join by another, trusted ISAC member. There are almost no vendor members—just security personnel who are trying to do their job well.

Targeted Threats

Although known exploits target known vulnerabilities, there are also threats that act against software in perfect working order. It is not a mistake or a bug that will victimize you. Instead, a targeted attack is launched using an exploit that only requires a way into your systems. Hackers are using well-known exploits that target specific businesses.

During the summer of 2003, a targeted threat materialized aimed at financial institutions. BugBear.B, discovered on June 5, 2003, was the first instance wherein a known virus proved increasingly harmful depending upon the specificity of the target. If you had updated your patches, BugBear.B would be detected by antivirus scanning and removed from your system. If it attacked you and you were not prepared, however, you simply lost all your data. If it attacked you and you happened to be connected to one of about 1,200 financial institutions that were hard-coded into the virus, it would deploy in your system and wait for your employees' keystrokes to reveal usernames and passwords. After the sensitive information was collected, it would forward it on to 1 of 10 e-mail addresses written within the virus.

Share and Share Alike

Wherever you do business, ISACs can be your friend. Join as many as apply to you.

This trend is worsening at this writing and will continue to on an array of fronts. A targeted threat could be industry specific. It could arrive via a dissatisfied customer or a disgruntled ex-employee. You need to be on top of targeted threats. Threats that are either well known, or that piggyback themselves on well-known attacks, are easy to stop with the proper foresight and planning.

Critical Systems and Threats

Solid, big-picture data from your local CERT will assist in combating known exploits and targeted threats. At a granular level, you can enlist customized products to forewarn you. One such service is Symantec's Deep Site, which gives clients raw data and customized security alerts about all threats. Before deploying either mechanism, you must prioritize your technology, mapping it to critical systems at critical times. Note that labeling a system as critical takes discernment. If you use Linux to print the company newsletter, it would not be categorized as a critical system. If Linux processes payroll every month, that's a different matter (especially at month's end—if payroll goes down for a day on the last week of the month, it is a crisis).

Make sure to give your global security team ample time to stay current. Threats have changed since you last worked on your security plans, and they will continue to change. You cannot stop it, but you can track it and adapt accordingly, and honestly; to do less would be shirking your fiduciary responsibilities.

Countermeasures

Usually, for every threat there is a pretty effective countermeasure. Some countermeasures are built in to your regular software and its patch regime. There are multiple third-party countermeasures that save you time and agony, and security technology is evolving on the hardware, software, systems, and managed services sides. It pays to have a policy in place that is designed to stay fresh on all fronts in an organized way. Moreover, you should consider how countermeasures can boost ROSI.

Instant messaging provides a handy object lesson in how countermeasures can provide ROSI. It also exposes a problem symptomatic of companies that do not yet practice constant vigilance. In any work environment, instant messaging can offer a handy mechanism for employee theft of intellectual property, enabling the attachment and sending of it wherever the employee wants. Moreover, it can be a huge time waster.

I have seen instant messaging at its worst, and I have worked with companies where it was used to make fun of management in real time during corporate conference calls. I have also seen employees send company-sensitive data to their home or to their friends because they knew that even though the corporate e-mail was monitored, there was no system in place to track instant messages.

On the flip side of such flagrant abuse, I have also run a global business where instant messaging was a critical time- and money-saving tool. With the time zones around the world, instant messaging is a cheap and easy way to get real-time information passed around the world. I had all my leadership teams use instant messaging at the office and at home so that they could be reached as needed. It was a lot cheaper than provisioning global Blackberrys to everyone, there was no training required, and it was deployable around the world within an hour of our decision to use it. People who say instant messages do not have a place in the office are probably the same ones (or their children) who told us that desktop PCs were just toys and would never become a workplace solution.

It is tough for a company's existing, global security system to track instant messaging, and because of this internal threat, an instant messaging backlash has persisted in many corporations. In many organizations, the technology group might see someone using instant messaging on a network port (say port 64) and think, "Ha! Shut it down." This is generally considered to be a solid practice. However, instant messaging has figured this out, and in response, it has installed a clickable option that asks users whether they would like to hunt down another available port in a network through which to get access. A user clicks, and instant messaging zooms up and down the company firewall, looking for a way in. When it finds one, previously closed "port 64" is dumped in favor of wide open "port 2048."

Taking it a step further, when the technology group discovers instant messaging operating on its new port, it might decide it is time to take an extreme countermeasure—it shuts down IM throughout the entire organization. Seems logical. However, in the current global business environment, this action could prove Draconian. Remember, technology is supposed to enable productivity and enhance communication. In this instance, wouldn't it be great to let the right people use IM for the right reasons and stop the wrong people from using it for the wrong reasons?

Countermeasure constant vigilance ensures that you understand what innovations exist that can map back to your business requirements while delivering fiscally responsible solutions that reduce risk. In the case of our instant messaging dilemma, a countermeasure does exist. Developed by British-based HyperScape

Security, netREPLAY is a tiny appliance that you attach to your network that enables you to track every system that is unscanned by your existing, major security systems. If netREPLAY finds anybody using instant messaging, it will lock on it and look for sensitive information being transmitted through it, automatically shutting off access should it detect suspicious activity. This small appliance will cost you a few thousand dollars. Over time, however, it could you save you millions by allowing your organization to re-enable instant messaging and communicate in real time, increasing productivity and the bottom line.

External threats—those that originate outside the company—require another form of countermeasure vigilance. In February 2004, one such menace—the *distributed denial-of-service attack* (DDoS)—afforded an effective contrast in constant vigilance related to external threats and their countermeasures. MyDoom was a targeted virus that carried a DDoS aimed at international software provider SCO Group, Inc. A variant known as MyDoom.b—bug-plagued but no less serious—carried the same attack to Microsoft. In late January, both companies braced for the storm and commented on their respective countermeasures in veiled, yet revealing terms.

SCO spokesperson Blake Stowell spoke to the technology tabloid eWeek: "Every security expert talking about this and the ones we are talking to say this is really real and needs to be taken seriously. This will probably be the biggest test our company has seen from the Web site standpoint ever."[2]

In the same article, a Microsoft spokesperson commented, "While [we are] unable to discuss the specific remedies [we] are taking to prevent the reported DDoS attack, we are doing everything we can to ensure that Microsoft properties remain fully available to our customers."[3]

On February 1, MyDoom slammed into SCO, and, according to *eWeek*, "The SCO Group Inc. confirmed that by midnight EST, a large-scale, DDoS (distributed denial-of-service) attack had rendered its Web site completely inaccessible."[4] SCO.com was useless, and service interruptions began. The article continued, "SCO will not be defending itself against the attack though until Monday.

[2] *Matt Hicks, "SCO, Microsoft Prepare for MyDoom Battle," 30 January 2004, www.eweek.com/article2.*

[3] *ibid.*

[4] *Steven J. Vaughan-Nichols, "SCO's MyDoom DDoS Hammering Begins," 1 February 2004. www.eweek.com/article2.*

Spokesperson Stowell explained, 'We don't expect many real site visitors on not only Sunday, but Super Bowl Sunday.' Stowell goes on, 'We have seen this coming and do have plans in place to address it on Monday morning. If Plan A doesn't work, we're ready with Plan B, and then with Plan C.'" It is important that plans not be created in real time or days before the threat, and SCO seemed to have been caught with its guard down.

Two days later, MyDoom.b careened into Microsoft. *eWeek*'s lead read, "Microsoft Corp.'s main Web site showed no ill effects from the scheduled denial-of-service attack generated by computers infected with the MyDoom.b virus."[5] The company would not reveal its countermeasure in the article, but its message? Microsoft hadn't sweated the attack. Somehow, it thoroughly understood the level to which they needed to be prepared for attacks of this nature. It had deployed the correct countermeasure to address MyDoom.b.

The suspense is killing you at this point. You want to know what I think the killer "anti-Doom" was. I will say that Microsoft, as a part of its global corporate security strategy, is a customer of—you guessed it—Akamai. When Microsoft chose Akamai to host some of its Web presence, it had done its homework. It knew that Akamai gets more than 30 billion hits a day and controls more than 10 percent of the Internet's traffic.

The SCO and Microsoft contrast underscores how your global security team must identify, evaluate, and apply new countermeasures that can keep you running smoothly and securely.

Regulatory Issues

The global environment necessitates an acute awareness of regulations in any country in which you do business. Just like your technology, you should map your organization's literal geography and all the geographic regulations—countries and locations—that apply. If you are a Swiss company, you might not know the whole of German law. If you are headquartered in Brazil, you cannot be expected to have a working knowledge of Dubai regulations.

[5] *Dennis Fisher, "Microsoft Unfazed by MyDoom's DDoS Attack," 3 February 2004, www.eweek.com/article2.*

Regulations represent terrain on which your global security team, your technology team, and your legal department must have a strong and close working relationship. This team will expand as your business expands. That way, if you move into the United States, you can figure out that each state has its own regulation profile: California has more regulations, for example, and Oregon has fewer. Having a legal team in place on the ground or at home that has a strong working knowledge of the laws that apply to you both geographically and vertically is critical to any constant-vigilance plan.

The World Economic Forum's Little Black Book

At the 2002 World Economic Forum in Davos, Switzerland, HP wanted to introduce attendees to its latest palmtop device that was replete with Windows CE and a wireless card. The Forum outfitted these new beauties with all the attendee information and personalized codes for finding places to eat and, when loaded with your credit card number, you could use it to scan and purchase books.

That year's Forum was met with antiglobalization demonstrators who showed up in person and virtually. One of them war drove the conference and was able to hop onto the wireless network provided by the Forum's host. There was no security, and soon the demonstrator had the information of every attendee in his or her computer. This included the addresses, private cell phones, credit card numbers, and exclusive e-mail addresses of the world's power brokers, including the likes of Bill Gates, Al Gore, and a host of others. This experience quickly illustrates how constant vigilance can even be missed at the highest levels.

Note that war driving is illegal in some spots around the globe, and hackers can be cited in interesting ways. In the United States, a man was arrested because he tried to access a corporate WiFi net while standing in the company's parking lot. He was found guilty, because he did it from their property—had he sat across the street, there would have been no law with which to prosecute him. In most countries, there are still no laws covering this new technology, so each case is handled differently. Look for these laws to evolve quickly, matching the rise to prominence that wireless is making around the world. Understanding what rules are in place will help you lay out the distribution of your WiFi repeaters and help you plan your WiFi policies accordingly.

Technology

Your and every company's technology—the bread and butter that has enabled you to go global—shifts throughout its lifecycle before it is retired and replaced. These movements range from subtle to seismic, and they occur in phases. Once a quarter, patches pop up and are added. Every year your Oracle databases are upgraded from X.1 to X.2. Every handful of years you have to consider major upgrades as Oracle moves to 9.0 and you decide to outfit the entire company with WiFi-enabled laptops. Okay, so what do you do when WiFi becomes WiMAX?

You must maintain constant vigilance regarding technology. At the writing of this book, a bevy of legacy systems are giving way to newer, faster, and potentially more *secure* technology. Your global security strategy must account for what technology you need as it relates to the risk and business requirements of each business owner.

Suppose, for example, that data is important and it travels on myriad laptops out the door of your company. If your concern is losing that data through theft, perhaps you want to consider the new IBM Thinkpad that carries a built-in encryption chip inside. If your concern is damaged or potentially lost data, you might want to consider the Thinkpad that devotes 20 percent of its disc space to making a mirror image of all your data. Even if you get hit by a virus and your data becomes toast, you can bring the Thinkpad to the office, boot it up, and boom!—you have your data back. These new machines, which cost about $500 more than a typical notebook, might prove more expensive in the short term, but the total cost of ownership could prove dramatically less if your investment properly accounted for the risks your people face outside the office. However, if your business owners do not even know they have the option, then that is a correctable fault.

A Word About the Long Term: IPv6

If I had a nickel for every time a business executive told me that he didn't need to buy my security stuff now because the next generation of the Internet protocol, called IPv6, would be available "next year" and have built-in security... Back in 2000, when I was at IBM, I briefed the U.S. secretary of commerce on IPv6, and what it would be able to do. Although we spent more time trying to convince him that broadband would become commonplace and that wireless was a reality, we did focus on the additional security that would be available when there was full adoption of IPv6. (Today we run under IPv4. No one knows what happened to version 5. It is like that weird uncle who just disappeared and is never talked about at dinner.)

IPv6 is here now. Can you feel it? Do you use it? Does it matter? If you use Microsoft XP or newer, you can select version 6 as your protocol. But the key to my message to the secretary was that it needed to be "fully adopted." It is not today, and it will be a while until it is. Also, like much new technology, it won't live up to its hype. Just like Dean Kaman's Segue did not "revolutionize human transportation around the world, changing the way cities of the future are designed," IPv6 will not automatically make the Internet a safe place to work. Just as Segue turned out to be the adult bicycle of the scooter set, IPv6 will be just the next protocol. It will not be the answer to all your prayers, and waiting for it is no excuse for poor security today. That's not to say IPv6 isn't necessary and won't help. Today only 10 percent (600 million out of 6 billion) of the world's humans are online (and the world is adding 79 million new people a year—and IPv4 is already running out of address space). Compound that with the coming "always on" broadband evolution, wherein each human will require dozens of individual network addresses. IPv6 will give us an almost limitless supply of these addresses, and this is the key driver. Also, IPv6 has security built in, whereas IPv4 needs to add security on top. IPv6 also has built-in privacy capabilities.

Some countries are betting big time on this next generation. Japan has invested in IPv6 more than any other country, and its companies are best positioned to enjoy the future fruits. Companies such as Sony have met an "All IPv6 Compatible" pledge, and these companies stand to be a prime supplier to European countries such as France and Sweden. Although the United States has many IPv6 product companies, look for them to export more than is used domestically for a while, despite a strong Department of Defense mandate to purchase. High-population countries that came late to the Internet, such as China and India, will benefit most from IPv6, because their address space allocation under version 4 is highly fragmented and prone to breakdowns and workarounds. And countries trying to leverage mobile communications such as Sweden, Japan, and Germany will see early rewards.

What does all this greatness-to-come mean for cross-border companies today? One piece of advice, from a trustee of the Internet Society and the president of the IPv6 Forum Latif Ladid, is to "look for 'IPv6 aware' on all the communications products that you purchase today, and expect to be buying new security technology from new security vendors over the next five years, to leverage the different security capabilities that will be available to you. Although it will have many new security capabilities available to us, it will still be up to the companies that use the Internet to ensure their own safety."

Internet Protocol (IP) has become a cross-border natural resource. It's up to all of us to increase its capabilities.

–Latif Ladid, President, IPv6 Forum, Luxembourg

IPv6 Security Benefits to Come

- Greater address space provides for greater granularity.
- Built-in header authentication, which will stop current spoofing.
- No need for *Network Address Translation* (NAT) boxes, which have raised risks.
- Built-in end-to-end security functionality.
- Slower spread of viruses because of longer address lengths. (IPv4 = 10 hours and IPv6 = 2 billion years to scan address space.)
- Built-in privacy protocols.

The Organizational Security Posture

Within this chapter, you have seen how keeping tabs on threats, countermeasures, regulations, and technology creates an effective virtuous circle of awareness. To maintain this posture, your IT team must stay current and aware by having a keen grasp on what's out there, and communicating it to business owners in a clear, business-relevant manner.

Having your IT and global security teams scour the Internet for online tradeshows and conferences represents an easy-to-cull intelligence. They should also join key professional organizations such as the *Information Assurance Advisory Council* (IAAC.Org.UK) and begin immersing themselves in the constant-vigilance circle in person and virtually.

At times, it will be wise to send your teams to tradeshows in your country or region to see the latest innovations first hand. These gatherings showcase relevant tools for counteracting threats. Teams should approach them with a critical eye, looking past "brochureware" and custom testimonials and asking for the contact information of at least three CSO or CIO customers with whom they can talk who support the product. If they get the "If I told you, I would have to kill you" treatment, it is time to move on. The CSO and CIO community *will* talk and share with peers—just not in public.

As they become steeped in knowledge, create opportunities for raising constant-vigilance issues within your business owners' units. Host an after-work pizza gathering where everyone has a chance to share—and listen—to new threats, countermeasures, regulations, and technology that might affect each unit. This should roll into a formal audit process that occurs yearly and is figured into the following year's cycle of security planning.

What Parts of Constant Vigilance Should I Outsource?

As constant vigilance begins to seep into a corporate culture, it, too, is evolving. In a recent conversation with Marco Plas, security chief at Netherlands-based broadband provider nlTree, we talked about this evolution and where it is headed.

Marco illuminated three stages of global security constant vigilance that companies tend to work through, and in each stage, more control is given to third-party providers. This change has been catalyzed by (you guessed it) the growth and complexity of threats, countermeasures, regulations, and technology.

- Basic Monitoring Packages
- Adding Infrastructure-specific traps and traces
- Allowing Remote Control

Stage one—general information security—is usually outsourced to monitoring companies such as Symantec. Specialists in below-ground bunkers in London or Berlin spend their lives tracking viruses throughout the world and providing patch-level updates. By outsourcing this portion of constant vigilance, you will receive updates such as "MyDoom is headed your way; update your patch."

In the second stage of constant-vigilance outsourcing, a company moves to handing the blueprint of its technology to a third party. In turn, that third party examines what levels of threats, countermeasures, regulations, and technology you should pay attention to based on the customized needs of your organization, sending you alerts and updates accordingly. Still, the company takes the action to secure itself from harm or legal action while executing disaster recovery. This second stage is where most companies in Europe are today.

Moving beyond the blueprint and giving a level of control is the third stage of constant-vigilance outsourcing. At this stage, the company hands over the blueprint and select scripts that enable a third part to take control of your systems when you are not there, so if a patch is needed or a portion of your system requires shutdown, it can be done remotely. This effectively ensures a more thorough form of constant vigilance. This is happening more and more throughout Europe because the need is increasing.

Marco Plas on the Consequences of Intermittent Vigilance

In the recent past, I worked to put together a constant-vigilance program for a bank in the Netherlands. After deployment, and on a Friday afternoon, we alerted the bank that a patch was needed for an incoming virus. We saw it, and we said, "It is coming to you; we need you to take your firewalls down for the patch install." We sent it to them, and they began to install it.

By that evening, the patch was in place, and we called the bank to bring the firewalls back up, but no one was there to do so. Now this was a pretty big bank with many ATM machines. With their firewalls down and their system vulnerable, they lost 2 million euros over that one weekend.

Scenarios such as Marco's are propelling many European companies to take the next step in the outsourcing evolution curve—providing a third party with full access to a company's firewalls so that the third party can leverage even more control over serious threats. This final stage will ultimately evolve into the full outsourcing of constant vigilance at a network level.

What to Keep

When outsourcing, it is important to remember that you are mainly offloading fault—not risk. Although you have someone to blame should something go wrong, you must also arm yourself with unparalleled constant-vigilance resources and keep some elements of the process. When giving your constant vigilance over to a third party, remember to maintain control of the security policy that you created, which maps regulations and business requirements to threats and delivers a process whereby your organization reviews its constant vigilance in the virtual circle discussed earlier. In addition, you should routinely audit your third-party provider for response times and other key factors that figure into your program.

Who to Seek

Constant vigilance is best undertaken by a party that has significant scale and that maintains a client base that spans your industry and the parts of the world in which your extended enterprise does business. On the technology side, there are some good local shops, but I recommend the strength in numbers and working with a Symantec, Redhat, or ISS. On the consulting side, going with a big four such as Deloitte, PWC, KPMG, or Ernst and Young, or one of the global consulting firms that has a strong security area (not just a pretty brochure, but lots of people and lots of R&D) is advisable, because they all have very structured approaches to security. In both cases, again, make sure that policies remain in your control and conduct an internal audit of your business requirements and an external audit of your third party at least annually.

You Have Just Charted a Course: Let's Set Sail

In Part 1, "Charting A Course," I spelled out the six global (and universal) security keys to success that cross all borders:

- You need to design a clear policy—or **global security strategy**—that is embraced by the global organization by listening to and working with business owners, who are ultimately responsible for the amount of risk they do or do not mitigate.
- Understanding that a **security base** tied to the concept of ROSI as it relates to what components are base-worthy or best executed independently can prove potent to your organization as threats increase in magnitude and intensity. Although base-relevant ROSI varies from maximum to minimum, understanding and applying my Rule of 3 will help you determine what kind of a return any one of the components I discussed could be realized within your organization. By using this rule of three, you can also drive greater adoption of security services throughout the organization.
- **Business systems enhancement** (finance, HR, CRM, supply chain) presupposes that the deployment of security can and will deliver money savings and time/productivity efficiencies. Similarly, **functional process enablement** (operations, networks, call centers, development) posits that security, if prudently applied, can drive profitability and prove the worth of a strategy.

- **Developing radar** that effectively integrates monitoring into the flow of corporate vital signs when reported in business terms to the business owners can ensure that a strategy deployed remains strong, successful, and legal.
- **Constant vigilance**, that step you take to deputize key people within your organization to stay current on the changes to technology, threats, countermeasures, regulations that will at once vest them with a sense of responsibility and accountability when it comes to security, will ultimately prepare your organization and keep it in a potent security posture.

Now that we have addressed some universal truths in global corporate security, it is time to set sail and begin visiting local security environments in *Europe, the Middle East, and Africa* (EMEA), the Americas, and the Asia Pacific regions. Here we step off our boat and walk the streets that might already comprise your map, examining local rules, regulations, customs, best practices, and conventions. I do so in Part 2, "Reality, Illusion, and the Souk," with an eye toward helping you succeed in countries beyond your own.