# 1

# *Homeland Security: A Convenient Invention*

*A friend was listening to a baseball game on the radio a few weeks ago. As the fans were going into the stadium, the announcers explained that "for security reasons" they could no longer bring bottles and cans through the checkpoints. Was this an attempt to prevent a terrorist disguised as a fan from hijacking a stadium with the jagged end of a broken bottle, or was it an obvious and insultingly stupid attempt to increase the revenues of in-stadium drink sellers?*

Homeland security is not a game for amateurs or the impatient. This is a scenario that involves complex challenges, from finding ways to stop terrorists from hacking into secret databases, to developing new procedures for airline security, communicating with the public about threats, and tightening immigration policies.

In this chapter I take a look at how we got where we are today. Jump on board the scare and hype bandwagon and get a taste for where we might all be headed.

## INFORMATION WARFARE: THE INTANGIBLE THREAT THAT KEEPS ON GIVING

To understand how we got where we are today, take a step back in time. It's the early 1990s; the Cold War is ending and suddenly a lot of

people are talking about the "peace dividend." Of course, politicians, bureaucrats, and Beltway bandits are busy positioning themselves to grab a chunk of any windfall that might come. Nobody is quite sure what is going to happen, and many folks in the information security and computer security fields are wondering if their research grant money is going to dry up and blow away.

What's a warrior to do when the enemy packs up and closes operations? Simple: *Generate worry about an intangible threat*.

## All Aboard the Scare and Hype Bandwagon

When it came to casting the part of Intangible Threat, information and technology, two linchpins of the 1990s, seemed to be likely candidates.

In 1994, Winn Schwartau, a charming rogue, wrote a blockbuster book called *Information Warfare: Chaos on the Electronic Superhighway*. It hit a nerve. This was during the height of the early dot-com boom, and the book filled readers' eyes and minds with visions of stealthy international cyber ninjas and countries brought to their knees by teenaged hackers working for ideological extremists.

There were visions of aircraft falling out of the sky because their command systems had been wiped with pulses of directed radiation and government agencies collapsing when a pimply-faced subculture hacked into their information resources.

The spooks who were looking at budget cuts had found their foe. Best of all, because it was a nebulous foe — a threat that didn't really exist — it had advantages: It could not be beaten, could not surrender, and could be ascribed awesome, superhuman powers.

## Hacker, Cracker . . . Whatever

Immediately after Schwartau's book came out, conferences devoted to information warfare began to crop up and more books were published on the topic. Eventually, congressional hearings were held on the threat, featuring suit-wearing, longhaired hackers who announced that they could "take down the entire Internet in minutes," assuming they wanted to.

Otherwise sensible people made comments such as "If an info war attack took down the AMTRAK train scheduling systems, the U.S. economy would grind to a halt in three days." Of course, these comments completely ignored the fact that AMTRAK strikes and track

outages lasting weeks had already failed to have a noticeable effect on our economy.

> *"You could feel the bandwagon rocking from the sudden weight of all the bodies climbing onto it."*

Researchers having anything to do with computer security rushed to change the titles of their grant proposals to contain the words "Information Warfare." You could feel the bandwagon rocking from the sudden weight of all the bodies climbing onto it.

## you should know

Today, strategic think tanks write scholarly tomes on information warfare, and the term is in widespread use. A search on Amazon.com's site returns over 70 pages of book titles matching the search term "information warfare." This shows a tremendous amount of interest in a form of war that doesn't have a whole lot of substance.

There are a few interesting aspects of the information warfare scare that are worth noting:

- The term information warfare is used so broadly that it can cover everything from crank calls and email spam to destructive attacks against physical components of online systems.
- The antagonists are so vague and ill-defined that anyone, ranging from a nine-year-old hacker to a government-sponsored researcher, can be an information warrior.
- None of the world-class scarifying events that have been projected has ever really happened. When minor information faux pas have occurred — for example, pieces of the Internet went down or Web sites were deliberately crashed — most of the victims reacted with bland indifference rather than panic.

### Information Warfare in the Trenches

Here's an interesting paradigm: As soon as someone conceives of a possible weapon that could threaten our security, the military creates defenses against that weapon. Once there's a defense in place, someone almost inevitably feels compelled to build the weapon itself. In other words, conceiving of a defense against a possible threat will automatically encourage someone to make that threat a reality.

So, the information warfare scare-hype gave birth to any number of organizations that build defensive information warfare capabilities — as well as stimulating shadowy efforts to build offensive information weapons. Thus, information warfare may become a self-fulfilling prophecy as some clever hacker comes up with an offensive to match our defense.

What would an offensive information weapon look like? Probably a lot like the kind of stuff we're already dealing with. Right now the Internet is rife with worms, viruses, and Trojan horses. While we may not be dealing with it 100 percent effectively, these kinds of threats haven't exactly crippled our information economy, yet, or even slowed it down.

A huge amount of money has been spent on ameliorating the threat of information warfare. In general, that money has been spent on a mix of initiatives that are either (1) a complete waste of time, (2) useful basic research, or (3) improvements to infrastructure.

*"Perhaps the best description of the information warfare defense process is a kind of Chicken Little make-work program for Beltway bandits and high-tech firms."*

Taxpayers can take refuge in the hope that the information warfare fad, so far, has simply been a very inefficient vehicle for funding research in computer security and systems and network management, as well as an excuse for buying lots of new PCs for government workers. Perhaps the best description of the information warfare defense process is a kind of Chicken Little make-work program for Beltway bandits and high-tech firms.

## Bandwagon on a Roll

The information warfare movement is a good example of how scare and hype bandwagons get rolling and take on a life of their own. In a lot of ways, the information warfare scare-hype bandwagon is like the terrorism scare-hype bandwagon, except that, so far, the former has just been a waste of money.

Unfortunately, unlike cyber ninjas, terrorists are a real threat. Most people don't immediately withdraw from the economy and head for the hills when their email is inaccessible.

## THE EMPTY PROMISE OF EMERGENCY RESPONSE

Once you've got the public good and scared about a threat, the first thing they'll ask is "Well? Isn't someone going to *do* something about it?" (The other common American refrain is "There ought to be a law.") Once everyone was good and scared about information warfare, organizations quickly flocked to embrace the new cash cow.

### THE BEGINNING: CERT

Early adopters included the various Computer Emergency Response Teams. The granddaddy of such teams was the original CERT, from Carnegie-Mellon University. CERT was founded in 1988 with funding from Defense Advanced Research Project Agency (DARPA). Its stated goal was to act as a coordination center in the event of future Internet attacks and outbreaks, such as the 1988 Morris Internet worm.

CERT was hugely successful in drawing attention to itself. While it never accomplished a whole lot, it had a highly visible team of experts that gave lots of good talks at conferences and became expert media-handlers and an excellent source of quotes for journalists. The level of attention the first CERT received spawned a raft of imitators, both at home and abroad. Many government agencies founded their own CERTs — not because they needed them, but because being part of a CERT was a virtual ticket to all the conferences you wanted to attend.

Pretty soon, there were meetings where CERT organizers could go to learn how to run CERTs. Meanwhile, networks kept getting hacked, and the state of network security remained pathetic. Eventually, a lot of the early CERT founders made their reputations and went to startups during the mid-1990s. If all the CERTs ever accomplished anything, I'm damned if I know what it is — but a lot of beer was consumed in the process.

### STAYING ALERT?

During its early days, the CERT's charter was primarily to educate organizations about the need for computer security and to work with vendors to fix glaring bugs in their software. The CERT's main vehicle for getting the message out was security alerts.

Alerts are a critical aspect of the whole emergency response scenario, as well as a hugely important aspect of this particular scare and hype

bandwagon. In 1998, the year it was founded, CERT released only one alert — about the Morris worm — adhering to a long-standing tradition among alerting agencies of only issuing alerts after it is too late to do anything about them.

## you should know

During the course of this book, you will run into countless cases where alerts are issued and they're either ignored or are simply too late. They are useful, but only within a very narrow window of time, and only if you're in a situation where you can actually do something about the threat.

The CERT was supposed to act as a sort of Internet Center for Disease Control (CDC), but that doesn't really make sense in an environment where a problem (such as a computer virus) can transmit without you getting near another person who is infected. In fact, in this case, the means of transmitting the alert is one of the carriers for the disease. It would be like getting a letter in the mail from the CDC saying, "Be alert. There is anthrax in the mail. Do not open any envelopes." Most online security alerts are sent via email — a popular avenue for hacking attacks and a transmission medium for many viruses.

Emergency response is not something that works through warnings; it is something that works through preparedness. This is especially true when the threat is terrorism or another form of sneak attack. By definition, the attack is a surprise, and any warning that is issued will simply serve to confuse the people who are trying to deal with the problem.

> *"Emergency response is not something that works through warnings; it is something that works through preparedness."*

The military has always understood this, and that's why emergency drills are a way of life on naval vessels. Sailors understand that "general quarters" means "get to your assigned post and deal with problems you see there, be prepared to do other stuff if told to, and stay out of the way if not."

When you're driving down a road and see a sign that reads "Falling Rock," you're receiving a useful warning to help you practice preparedness: Presumably you're going to be more ready to dodge large moving objects, and unmoving objects that are sitting in the road. Generalized

warnings, such as the FBI's antiterrorist warnings, are like seeing a sign by the side of the road that reads "LOOK OUT." Look out for what? Should I speed up, or slow down? Should I call someone on my cell phone? Or get out of my car and run for cover? In fact, I'm more likely to ignore the sign and turn up my radio a notch; at least if danger is present, I can hum along.

## Prepared for Anything . . . or Nothing

Preparedness is critical for dealing effectively with virtually any kind of surprise. As societies are repeatedly forced to deal with many new types of nasty surprises, they quickly evolve responses and people become prepared to use them.

In the United Kingdom the Provisional IRA planted a car bomb at Bishopsgate in 1993. An observant local police officer identified the vehicle as suspicious and began a response within two minutes of the terrorists leaving the vehicle. The police began taping off a cordoned area within minutes, and the IRA actually called in a warning *after* the police had already begun to respond to the weapon. Existing evacuation plans prepared by local businesses were invoked, and the police were able to almost completely evacuate the buildings in the area before the bomb exploded. Preparedness showed in the fact that the police were thinking about car bombs rather than parking tickets, the police had bullhorns, the businesses had plans, and the civilians reacted rapidly and in a disciplined manner.

Imagine a similar incident in a U.S. city. Some employees would remain at their desks and not take the situation seriously. Other people, inspired by curiosity, would stand in the middle of the evacuation path trying to get a look at the bomb. And, of course, a camera crew from a local TV station would get itself blown up while asking people on the scene, "Do you think the terrorists were *serious* about a bomb being in that car?" Such attitudes change rapidly with experience. Compare the Israeli and British popular media attitudes to terrorism if you want a perspective on the difference between us and countries that have truly internalized the terrorist experience. In the United States we simply haven't had enough time and contact with terrorism for it to sink in. I'm not saying 9/11 was unimportant, but there is a major difference in the cultural attitude of a society that lives with a constant threat of terrorism at home and one that is still surprised by it.

### Fighting the Last War

There's an adage in military theory that says "armies always prepare to refight the last war." It's generally spoken as a criticism of stodginess in military thinking. But unless you're able to anticipate new methods of warfare on a regular basis, there is no alternative.

Being prepared to fight the last war is certainly better than being prepared to run around flapping your arms and shouting "The sky is falling!" In fact, preparing to fight the last war at least shows an awareness that you may need to fight. On a more practical level it shows an awareness you'll need somewhat up-to-date equipment, well-trained troops, and a familiarity with the latest tactics. The drilled-in reactions to a car-bomb threat will not serve effectively against a biological weapons attack, but the discipline required to respond to the threat, and perhaps some of the tools available, might.

### Hey, What About Us?

As the United States prepares to deal with homeland security, there will be any number of organizations attempting to boost their budgets and importance by preparing to lead responses to incidents as they occur. Oddly enough, to date, the most fundamental component of response — disciplined and thoughtful civilians — has been left out of the equation.

Those who grew up in the late 1950s and early 1960s recall how we mindlessly performed air-raid drills against possible nuclear attack. We performed fire drills in schools at various grade levels. The time it took for us to evacuate the building was always too long, but it was always shorter than it would have been if we had never performed a single readiness drill.

This preparedness is the point of incident response organizations. The poor ones exist to increase their funding by issuing alerts to exaggerate their importance. The good ones teach people response procedures for categories of problems within their purview.

These organizations are prepared to act as the coordinating locus in their area of expertise. They are also prepared with appropriate lines of communication that work during the duration of the emergency.

## you should know

The CDC has the necessary contacts within the media to be able to issue necessary instructions in the event of a plague. But do they waste people's time with weekly plague-level alerts as the FBI has done post-9/11? No. For one thing, the folks at the CDC have a pretty good sense of the damage a pointless panic can cause.

## The Nicheless National Infrastructure Protection Center (NIPC)

The National Infrastructure Protection Center (NIPC) is an example of an organization that has had problems finding an effective niche. It was established by the FBI — basically it *is* the FBI — with a broad charter but no actual ability to execute. Its mission: "To serve as the U.S. government's focal point for threat assessment, warning, investigation, and response for threats or attacks against our critical infrastructures. These infrastructures, which include telecommunications, energy, banking and finance, water systems, government operations, and emergency services, are the foundation upon which our industrialized society is based."

But if you look closely at what NIPC can actually do, its authority extends to releasing alerts, "coordinating," and "sharing information." In other words, it relies on other people to tell it what's going on, and then it hopes to turn that information around quickly enough to issue an alert to those who have not already succumbed to the threat.

One audit performed by the Government Accounting Office (GAO) found that NIPC issued many of its incident warnings after the incidents — especially the spread of computer viruses and worms — had occurred. Lots of organizations already knew they had massive-scale worm attacks under way because their network connections were clogged with worm traffic in the form of millions of email messages generated by self-propagating attack programs. NIPC's alert was drowned out by the flood of emails that crashed servers worldwide. (Unfortunately, there is no Internet equivalent of a bullhorn, such as the British Police used in the Bishopsgate bomb incident.)

*"One audit performed by the Government Accounting Office (GAO) found that NIPC issued many of its incident warnings after the incidents had occurred."*

NIPC typifies a number of other problems that exist with incident response organizations throughout the government. NIPC has

- A lack of staffing and expertise.
- A confused position within governmental structures, especially with regard to relationships between the FBI and the National Security Council (NSC).
- A lack of credibility with the private sector.

*Somebody Forgot to Train the Staff…*

There's a saying in the military: "You fight the way you train." Well, what does that say about how well you fight if you're basically untrained? Lack of staffing is usually synonymous with lack of expertise. In fact, if your staff members don't know what they're doing, it doesn't matter how many of them you have (clueless × 1,000 still equals clueless).

The NIPC was originally funded in 2000 with $27 million and 200 FBI agents. In the private sector, substantial, successful companies have been founded with far less. Indeed, that level of staffing is comparable to the funding and head count of many software security companies, such as those that produce Internet firewalls and antivirus software. Two hundred employees is only "lack of staffing" if the lack of expertise is severe.

The NIPC was initially forced to train its staff by inviting outside Internet security experts in as unpaid guest speakers and instructors. This resulted primarily in NIPC's educational input coming from the marketing departments of vendors who were hoping to influence federal security procurement efforts.

*Being Left Out of the Pecking Order*

Organizational confusion is another major problem bedeviling many government organizations. It most acutely strikes those groups that are chartered to "coordinate" but have no actual management authority over the things they are supposed to be coordinating.

"How is the NIPC supposed to make a positive impact when the only way they can bring about change is by asking nicely?"

How is the NIPC supposed to make a positive impact when the only way they can bring about change is by asking nicely? Further, because NIPC is supposed to work with the private sector, there is a huge problem because private-sector organizations are often technologically ahead of NIPC. But even within the federal government, nobody knows if they have to listen to NIPC — or, more precisely, they're sure they *don't* have to listen to NIPC, which makes NIPC into a vestigial organization that can't do much more than issue bulletins.

*NIPC — Who??*

Last, but far from least, is the lack of credibility many federal agencies have with their private-sector counterparts.

While many commercial firms had problems with some of the outbreaks of Internet worms such as CodeRed and Nimda, a large number of them had adequate protections in place, and many even had antivirus response procedures. Many commercial antivirus products had released signatures to detect and block the worm before the NIPC's alert was issued. So, for a large number of private-sector organizations, the entire alert was a nonevent.

Many of NIPC's alerts are essentially derived from the alerts issued by commercial product manufacturers, which makes private-sector organizations wonder if NIPC exists to do much more than to paraphrase and summarize alerts that have already been issued by commercial antivirus or security companies.

How does this lack of credibility come about? Why is NIPC recognized as a failure even by the government, when the CDC is a highly respected organization? It's simple:

- Government can only dominate an agenda when they clearly monopolize expertise.
- An organization can lead only when it is ahead; in this case, the government would have to be ahead of the private sector, and it's not.

The CDC operates in an area where there *are* no private-sector competitors. In areas where "to provide for the common defense" obviously holds, the private sector has a history of letting the government lead. National-level response to disease outbreaks and biological warfare are closely related topics that most people clearly expect our government to take the lead in. Information technology, and use of near-cutting-edge information technology, is not something most people expect the government to be good at.

Indeed, the government's entry into cyberspace has been slow and fraught with embarrassing faux pas. During the early 1990s, when many Americans were jumping onto the Internet with both feet, most federal employees' email addresses ended in "@aol.com." Many senior and motivated law enforcement personnel purchased their own computers so that they could begin to learn cyber forensics because the desktop systems available to them were barely powerful enough to run word processors.

### WHERE DID ALL THE COMPETENT PEOPLE GO?

These observations about government efforts at mastering technology are not intended to belittle the incredible efforts of the small but diligent number of federal workers who struggled and overcame the technological backwardness of the government. Long, hard hours of self-training brought many FBI and Department of Defense computer experts to skill levels meeting or exceeding those of their private-sector peers.

In fact, many of those federal experts were unable to resist the lure of healthy raises and stock equity offered by Internet security startups during the late 1990s. After years of working on a shoestring in a management structure that was stifling, a lot of motivated people left government employment and earned healthy fortunes by doing so.

Many federal agencies are using hopelessly obsolete computers and software — yet somehow the federal government still spends massive amounts on information technology. My guess is it's not being spent well.

## 9/11 AND THE BANDWAGON TAKES OFF

The homeland security bandwagon lurched into gear after 9/11. In many respects, it was a perfectly natural reaction to the fear and confusion caused by the terrorist attacks. Practically the first thing out of everyone's mouth was "How could this have happened?" The second was "How can we keep it from happening again?"

The media only added to the hysteria, and it was clear that *something* was going to have to be done, whether it made sense to do it or not. So the bandwagon began to roll, accelerating through 2002 to become a bureaucratic and financial juggernaut of epic proportions.

Three different segments were fueling the bandwagon:

- The media asking "What is going to be done about this?"
- The government looking for an answer to the media's question
- Vendors of security solutions looking for an opportunity to make money off the whole thing

Each of these groups' concerns is *perfectly valid*, but because of the vested interest each has in the outcome, it's nearly impossible to get a sensible answer.

**you should know**

See Chapter 10 for more about security vendors and their role in homeland security and Chapter 8 for a closer look at the media.

## The Media's Question

The media, of course, doesn't really want definitive answers to the problem of homeland security. In fact, the media is probably happier with unanswered or unanswerable questions, since those make for better stories and provide a good forum for endless pundits to discuss endless questions endlessly.

You've doubtless heard the theory about the infinite number of monkeys typing at random and how they'd eventually re-create *Hamlet*. Media pundits probably couldn't accomplish that much; remember, their role is to clarify divisions and present opposing views. A cynic might call that "sowing discord."

The media's role in getting the bandwagon rolling was primarily that of acting as Monday morning quarterback — searching for the "could have dones" and "might have beens" that would have prevented the act of terrorism in the first place. The media sells 20/20 hindsight; after all, when was the last time you heard CNN say "Today, a potentially disastrous situation was staved off years in advance because of some sensible decisions that were made by a federal agency"?

> *"The media sells 20/20 hindsight."*

In fact, the media was in a perfect position to get the bandwagon rolling by simultaneously asking "How could this have happened?" and "What is the government going to do about it?" casting the onus of response clearly on the administration. After all, the pundits were the ones who implied something was wrong when President Bush didn't immediately drop everything (he was visiting a children's school when notified of the attack) and rush to do something. The very same pundits would have implied something was wrong about how President Bush "panicked and fled" if he had immediately run from the school children, jumped on Air Force One, and headed to Washington.

One person's panic is another person's resolute action; one person's disinterest is another person's deliberate action in the face of a crisis.

### MEDIA VERSUS BUSH

I think the Bush administration did about as good a job as could be done handling the 9/11 crisis. President Bush basically said: We are going to learn what happened, we are going to study matters, we are going to decide on an appropriate response, and we are going to enact that response. That's actually what leaders are supposed to do in time of crisis.

But we had a media that wanted dramatic, drastic action; they wanted to stampede into doing something — *anything* — but at the same time they were standing by to enthusiastically second-guess anything anyone did. The media even second-guessed itself — anything to fill the vast, uncertain, nervous emptiness between advertisements.

> *"The media even second-guessed itself — anything to fill the vast, uncertain, nervous emptiness between advertisements."*

I recall one TV show where an expert was talking about horrible scenarios and how easily terrorists could do tremendous amounts of damage. One listener sent a feedback email asking if it was a good idea to discuss such things — whereupon the talking head who fielded the question proceeded to describe, "Oh, there's lots worse things I could have said! For example . . . blah blah blah." Another talking head was quick to take up the baton by asking, "Does the media sometimes err in what we divulge?" That's sort of like asking the town gossip to tell you which person in town talks too much. It was a relief to see that CNN at least implemented a policy of not reporting on operational details during the most recent Gulf War, when Geraldo Rivera revealing troop locations on live TV was more the kind of grandstanding I'd come to expect of the media.

## IN A PERFECT WORLD

Poor government technology infrastructure, emergency response systems that don't extend to the general populace, and at-risk public buildings don't bode well for effective homeland security. What could make a difference?

### Ensuring Cyber Security

Cyber warfare, if it happens at all, is going to mostly damage systems that are insecure, poorly designed, and badly managed. The *single best* security technology for improving the attack resistance of a system or network is a good system administrator who understands security and is motivated to keep his or her systems safe. Unfortunately, we've come to accept poorly secured systems as a matter of course.

### Taking Emergency Response Seriously

To me, emergency response is the one ray of hope in the whole homeland security mess. If you practice reacting sensibly to one kind of emergency, the discipline of the drill will stand you in good stead even in a completely different kind of emergency. Practiced responses go a tremendous way toward reducing the hand-flapping and hair-pulling that takes place during the first few minutes of a disaster. Indeed, if there's one expenditure in the entire homeland security budget that I support absolutely, it's the money set aside for more training opportunities and drills for first responders.

I'd even go so far as to say that we should consider establishing civilian emergency drills and procedures so that civilians learn the basics of their evacuation procedures and the basics of how to respond to the current threat models. Fire drills really *do* save lives. The same applies to computer security incident response: Teach people useful things to do in the event of a fast-spreading worm or virus, and suddenly it's a lot less of a panic and media circus. Of course, such drills and procedures must be well designed and presented to the public in a disciplined and thoughtful manner. And I'm not talking about having some idiot go on CNN to tell everyone to stock up on bottled water, tape, and plastic sheeting.

Another tremendously valuable side effect of performing response drills is that it teaches people *whom to listen to* in the event of a problem. Right now, most Americans wouldn't have a clue what to do if their local police told them one thing, CNN said a different thing, and the Department of Homeland Security told them another. One of the first things I remember from my grade-school fire drills was learning that "when there's a fire alarm going off, listen to the fireman." I'm terrified that if there is a severe national level incident, we'll get nothing but

*"'We're from the government and we're here to help' is only comforting if it's not accompanied by contradicting messages from 15 different sources at once."*

conflicted messages and turf wars as various government entities try to stake their claim to being the ones best suited to help. "We're from the government and we're here to help" is only comforting if it's not accompanied by contradicting messages from 15 different sources at once.