

Info Security

PROFESSIONAL®

WINTER 2008

An (ISC)² Digital Publication

www.isc2.org



**LOOKING BACK,
LOOKING AHEAD**

CISOs DESCRIBE 2008-09 CHALLENGES

info war

John Soat investigates whether information warfare is a serious threat or over-hyped hysteria. Cybersecurity experts offer two words of advice: **BE PREPARED.**

The headlines last August sounded chillingly familiar, an arctic blast of

Cold War anxiety: “Russia Invades Georgia.” But while its politics seemed like déjà vu, the conflict offered an extensive look at an emerging—and unsettling—form of combat in an increasingly online and interconnected world: information warfare.

Georgia’s cyber infrastructure was under attack even before Russian tanks began rolling in. For several days, extensive denial-of-service (DoS) attacks rendered government Websites useless. Some observers downplayed the significance of the online attacks, ascribing them to “hacktivists”—savvy amateurs bent on inserting themselves into the fight. Russian officials have denied direct participation in the DoS attacks against Georgia, and no one is certain exactly where they originated or who was responsible.

Still, the U.S. government and its defense agencies are taking information warfare seriously. Several cyber warfare programs have been established, including the Air Force’s Cyber Command unit. In January 2008, President George W. Bush approved a new interagency cybersecurity effort to be run by the Department of Homeland Security, and a Silicon Valley-based entrepreneur was tapped to head it.

How seriously should information security professionals take the threat of information warfare? More seriously than they do now, according to many cybersecurity experts.

When, Not If

In their efforts to address the forest of security problems, information security professionals may be ignoring a few significant trees. In the (ISC)² 2008 Global Information Security Workforce Study, almost half (48 percent) of (ISC)² members say they are mildly or not at all concerned about the security threat posed by terrorists, and 38 percent say the same thing about organized crime.

“It really is a matter of semantics,” says Andre DiMino, co-founder and director of the Shad-owserver Foundation, a self-funded, non-profit

organization composed of security professionals who track and report on the progress of malware, botnet activity and electronic fraud. DiMino points out that one of the most important elements of information warfare is the botnet. Botnets are worldwide networks of compromised computers; those computers currently number in the millions—and that figure is growing (see “Battling Botnets,” *InfoSecurity Professional*, Autumn 2008). “The use of a computer in a targeted attack—that’s my definition of cyber warfare,” says DiMino.

Your organization may have already been the



victim of information warfare, or at least an intended victim. Phishing attacks are often used to obtain funds for terrorist organizations, according to watchdog groups. At the same time, certain nation states are interested in obtaining the intellectual property of companies to exploit the technical advances and competitive advantages represented by patented processes and copyrighted algorithms. Internet addresses in China, for example, have been linked to network intrusions in the U.S., including a well-publicized break-in last year into non-military networks at the Pentagon.

So, while most companies aren't likely to suffer coordinated, intense electronic bombardment, information security

professionals can expect to see a steady increase in the number and sophistication of those attacks with which they're already familiar: worms; Trojans; spam; phishing; network intrusions; and data theft.

Growing Capabilities

Ultimately, when it comes to security concerns, the "who" is less important than the "how."

"The information security professional can't be concerned with who it is that's attacking his or her network," says security consultant Winn Schwartau. "It's all about the capabilities, and capabilities keep going up." With the publication of *Information Warfare: Cyberterrorism: Protecting Your Personal Security in the Electronic Age*, he literally wrote the book on info warfare. According to Schwartau, it can be divided into three areas:

► **Class 1:** Personal Information Warfare, where the individual is the target. "We didn't call it identity theft back in the day," Schwartau says.

► **Class 2:** Corporate Information Warfare, or "the rough equivalent of what we used to call industrial espionage," he says.

► **Class 3:** Government Information Warfare. The Russia-Georgia conflict is an example of this. Another example is a similar situation that developed in Estonia last year, where that former Soviet satellite's cyber infrastructure was compromised by DoS attacks over several days after Estonian officials removed a Russian war memorial from the center of the capitol.

Businesses must be aware of all three areas of potential attack. "The information security professional has to understand the complete environment," Schwartau says. That's because, for example, Class 1 information warfare—identity theft—"may be coming from a Class 2 or Class 3 source," he says, making it more dangerous. Guarding against sophisticated phishing or malware attacks places greater emphasis on Web controls and PC security.

Class 2 information warfare involves "patents, copyrights, business deals—that is, the real value of companies," Schwartau says. It can be perpetrated by outsiders through network intrusions, but also by insiders. That's why it's important for information security professionals to work closely with their human resource departments to screen applicants for critical IT positions, including H-1B workers.

Schwartau says it has become increasingly important that all areas of security—HR, cyber security and physical security—are integrated as closely as possible. An example is a disgruntled ex-employee, "the insider that becomes an outsider," as he puts

it. To address that scenario, "part of the HR process should be irrecoverable revocation of all assets," Schwartau says—including, perhaps especially, electronic assets.

In the U.S., Class 3 info warfare will increasingly involve private companies because they own and operate most of the critical infrastructure used by government and military operations, such as the telecom network or the electric grid. Experts are divided on just how vulnerable that infrastructure is, and how aggressively it's being probed. There is still speculation that the 2002 power outage on the East Coast resulted from probing of the SCADA systems. While that speculation flirts with hysteria, the lesson is: Be prepared. "If you have a critical



"Is [info warfare] going to get nastier? Yes, it's going to get nastier."

Winn Schwartau, security consultant and author

system on the Internet, chances are it's going to be knocked," says Shadowserver's DiMino.

An important element to consider is the global supply chain. Andrew Colarik, an information security consultant and cybersecurity expert, says information security professionals must factor the possibility of regional information warfare conflicts, like those in Estonia and Georgia, into their business continuity plans. That means having alternatives ready, in terms of logistics and resources, if Internet access to supply chain partners is interrupted.

O. Sami Saydjari, president of the security consulting and research firm Cyber Defense Agency and a former cybersecurity expert with the National Security Agency, says most organizations aren't taking the cyber warfare threat seriously enough, and one area he points to is outsourcing. Because software coding and maintenance is often sent to other countries, information security professionals have to be aware of the possibility of "contamination in our corporate infrastructure," or applications that "come back with Trojan horses and back doors that can be exploited later on," he says.

It's a sensitive issue politically, but a risk that shouldn't be ignored. "In a global environment, they're going to have to put software quality assurance controls in place" to deal with that risk, Saydjari says.

Cyber Consequences

Cybersecurity experts say DoS attacks—or the threat of them—are used to try to blackmail organizations. They're also used by criminal organizations to demonstrate prowess. Shadowserver's DiMino recommends analyzing network infrastructure for the load balancing and redundancy needed to withstand a sustained DoS attack. "We see many sites that don't have that design built in," he says.

On a professional level, those involved in information

security, particularly those who work at critical infrastructure organizations, need "more training in the aspect of how to deal with a crisis," says John Bumgarner, CTO and research director for security technology for the U.S. Cyber Consequences Unit, a non-profit research organization funded by the Department of Homeland Security and other government agencies. This unit advises "the highest levels of government" on cybersecurity issues, Bumgarner says.

Information security professionals "usually respond to events that have already occurred," he says. The Georgian and Estonian incidents demonstrate that security professionals might benefit from training in how to respond while an attack is taking place. "A lot of agencies do not train that way, do not train for aggressive response," Bumgarner says.


Various types of info warfare resources are available. The Estonian Ministry of Defence recently posted a document titled "Cyber Security Strategy" on its Website (mod.gov.ee) that calls for, among other things, "the development and implementation of international cyber security policies."

The U.S. Cyber Consequences Unit offers a cybersecurity checklist intended to provide "a comprehensive survey of the steps that corporations and other organizations should take to reduce their vulnerability to cyber attacks." The checklist contains 478 questions grouped into six categories: hardware, software, networks, automation, humans and suppliers. It is "a baseline where we think organizations should be," Bumgarner says. He urges information security professionals to examine the checklist and offer their input. "It's not something created in a vacuum," he says. "We welcome any comments on it."

Schwartau says information security professionals must convince upper management that the threat of information warfare is real. That's because it's not just the security person's problem. "Too often the info sec guys get laden with things they shouldn't," he says. For instance, are the costs involved in implementing better power backup systems worth more than a potential data loss? "That's a business decision, not a technical decision," Schwartau says.

On the other hand, the threat of information warfare indicates how critical cybersecurity issues are in the Internet age. "There should be an info sec signoff on any major corporate decision," says Schwartau.

Finally, the most important lesson of the Georgian attacks may lie in how they compare to the Estonian attacks: While the Estonian attacks were simplistic and scatter shot, the Georgian attacks were targeted. The level of sophistication "jumped from ground zero to three," says Bumgarner. "An information security professional should worry about this."

Schwartau is more blunt. "Is it going to get nastier?" he asks. "Yes, it's going to get nastier." 

John Soat is a freelance business and technology journalist based in Cleveland, Ohio, USA.