The Corporate Cyberspace Menace You Don't Know

By Robert K. Ackerman
CIO Today, September 10, 2008

Spear phishing targets an individual for a phishing probe. For example, a malefactor accesses a specific person's e-mail contact list. That person then would receive an e-mail purporting to be from someone on that list, but instead it would contain some malware that downloads upon opening and exfiltrates valuable information such as passwords.

The business community may be both a backdoor and a front door to espionage activities that threaten U.S. national security. Hostile governments always have viewed companies that do business with their government as a possible conduit for valuable intelligence. But now that threat is extended to those companies' own activities in the global economy.

Much of the vital infrastructure is in the hands of the private sector, and national security experts have been working to reduce vulnerabilities there for years. What has changed now is that the commercial economic engine that powers the Free World is increasingly vulnerable to cyberspace marauders who are motivated more by profits than by ideology.

Dr. Joel F. Brenner, national counterintelligence executive in the Office of the Director of National Intelligence, offers that just a decade or two ago, most people might have considered counterintelligence a problem for the Federal Bureau of Investigation, the Central Intelligence Agency and the military. In that era, governments basically stole information from inside other governments.

But that trend has diminished over the years. In the West, as the relationship between the public and private sectors has grown, government increasingly has contracted for many activities that formerly were done by civil servants or a conscript military.

Today, many secrets that used to reside exclusively within government can be found throughout the economy in the hands of private contractors. Not only does the government outsource many traditional political-military functions that generate classified information, but a great deal of critical infrastructure information also is held by state and local governments and private companies. Commercial and non-governmental entities control a significant amount of the critical infrastructure.

This is not just an issue of contracting out services, Brenner emphasizes. That is a marginal issue. The real issue is that the relationship between the government and the private sector is fundamentally different than it was two decades ago. The two have grown into one another so thoroughly -- and the resulting dynamism is so great -- no one either can, or should want to, pull them apart, he states.

And one of the most important elements of national security is a healthy economy, and it is in this area where private-sector vulnerability may pose the greatest threat. Many key products that help drive the economy are targets for foreign governments that recognize the importance of competitiveness in a global economy. The quaint term of industrial espionage has given way to economic espionage-and instead of originating in a rival corporation, the espionage is organized and directed by foreign governments.

Brenner cites as an example how a pharmaceutical company can reap billions of dollars in short-term earnings from sales of a patented, valuable drug. Those earnings are a source of national wealth, and they generate more investment in research and development along with dividend returns to shareholders that also fuel the economy. If that drug formula is stolen, then an overseas company is competing in the global marketplace-and usually with the assistance of the parent government that stole it in the first place.

"We find ourselves developing technology, having it walk on airplanes on computer disks, and then get re-sold back into our own country," Brenner observes. "We are buying back our technology as finished goods. That is a security issue for the country.

"Counterintelligence now is a problem for everybody with secrets to keep who lives on the Internet," he declares.

Over the past 15 years, the United States has enjoyed a dramatic increase in productivity and profitability. Much of this growth is owed to the ability to create, transmit and store massive amounts of information easily, which is a direct result of the information revolution.

"If by taking one thing down you can take down lots of things -- which is what interconnectivity creates -- then you decrease robustness as you increase connectivity. This is a problem to be managed; this is not going to go away for us," he warns. "The degree of criminal behavior, of theft, of public and private espionage that are enabled by technical means through computers and networks has blossomed to a breathtaking degree.
"It's time we stopped and took a deep breath and began to come to grips with the vulnerabilities that these wonderful advances have brought to us," Brenner says. He continues that remote attacks through cyberspace can even remove the need for a human spy. But combining that type of attack with a spy inside the targeted organization can be much more effective.

Other ways of infiltration happen daily. Brenner cites how a businessman at a trade show may receive a jump drive that holds more than an exhibitor's promotional material. That jump drive may contain malware that downloads into the businessman's computer as soon as the drive is plugged in. The malware could perform any manner of roles from reporting the user's keystrokes to searching the hard drive for vital information. And, if that jump drive has a wireless capability, it may sniff around the company's wireless network for other devices through which it can infiltrate any number of computers.

Foreign governments are deep into cyberspace espionage on all types of devices wielded by all types of users. Brenner relates how one U.S. computer expert took a new personal digital assistant (PDA) on a trip to China knowing that it might be the target of an infiltration attempt. The new PDA was clean of any data files or other software appliques. But from the moment he landed at the airport in Beijing through the short cab ride to his hotel, his PDA was the target of Chinese cybernauts. In his hotel room, the American analyzed his PDA and discovered a handful of beacons that had been embedded in his device during that short trip. These beacons not only could tell Chinese police his location, they also could connect to his base computer when he synchronized his PDA.

Brenner warns that people now carry their whole lives in cell phones, PDAs or laptop computers. Any device with a wireless capability is vulnerable to penetration, and those lives are as good as public property. "If people travel in a hostile cyberenvironment -- and China and Russia are two -- I warn them not to take the same PDAs and phones they use when they are home," he allows. "If they have telephone numbers and information on those devices they wouldn't want competitors to have, they had better leave the phone at home.

"Now you can't tell a CEO not to communicate," Brenner continues, "but you can say, 'use a different phone or SIM card when you travel, and use a separate PDA-and when you get home with that PDA, give it to your IT people and let them examine it and clean it.'"

Another piece of advice that Brenner offers travelers is to remove the battery from any PDAs or cell phones when they are not in use -- "Especially don't turn it on between your plane and your hotel in downtown Beijing," he warns. Authorities have observed how foreign governments make microphones turn on even when they seem to be off.

This need for security extends beyond digital communications. One state-owned airline wiretapped the seats in the first-class cabins of its aircraft. It also placed cameras in the light fixtures above each passenger seat so that espionage analysts could read documents or laptops that a corporate official might be reviewing on a trans-Atlantic flight.

While China "has us under a full-court press" in cyberespionage, the Middle Kingdom is far from alone in those endeavors, Brenner emphasizes. Many countries have the capability and are doing it, he reports. Private organizations also can-and do-engage in cyberespionage. He cites one example of a "major U.S. household-word company" that was involved in negotiations with a large enterprise in a foreign country. Halfway through the negotiations, officials in the U.S. firm realized that their counterparts knew every one of their bottom-line positions-which they had lifted from company e-mails. "You can't communicate that way and think that you are maintaining secrets against a negotiating opponent," Brenner declares. "Instead, you put key terms on a piece of paper in your pocket-you leave them blank [in the electronic documents].

"You follow reasonable cyberhygiene practices."

In addition to government-sponsored cyberespionage, criminal organizations are using the Internet to fleece financial institutions. That criminal activity is growing at an accelerated rate, Brenner reports, and it now is producing losses for banks and credit card companies that might be unsustainable in the near future.

"Right now, the banks and credit card issuers have been eating these losses themselves and not passing them on to their customers," he relates. "I don't know that this is going to go on forever. Not only are the losses mounting absolutely, but the level of losses is escalating to a shocking degree."

He continues that these financial institutions monitor these cybertheft losses down to the basis point. They know exactly how much return on investment they are losing, and the rate of losses is escalating "in a very troubling way." And a convergence may be taking place among criminals, terrorists and rogue nations. Colombia's Marxist guerrilla movement FARC, which only recently has been knocked on the defensive, long has been active in narcoterrorism. It has acted as a quasi-governmental entity by taxing people and companies in territories it has controlled, and it has resorted to criminal fundraising to support its politico-military efforts. Brenner notes that the Russian government's toleration of organized crime, especially with regard to individuals, represents another convergence.

The skill of cybercriminals also is improving significantly. "We're now not only seeing denial of service and thefts of accounts, we're also seeing very specifically targeted phishing and spear phishing," he says.

Spear phishing targets an individual for a phishing probe. For example, a malefactor accesses a specific person's email contact list. That person then would receive an e-mail purporting to be from someone on that list, but instead it would contain some malware that downloads upon opening and exfiltrates valuable information such as passwords. "We're seeing lots of that now," Brenner states.

He points out that spear phishing is a technical attack that is preceded by a research effort into a particular person's way of doing business. It combines both human intelligence and technical intelligence.

That type of threat extends outside of the target of interest. Criminal elements increasingly are resorting to supply chain attacks. If a sophisticated cyberthief or foreign intelligence operative wants to penetrate a network with good cyberhygiene, that person might instead opt to subvert a product that the targeted organization is buying.

To illustrate how this is done, Brenner cites an actual case. A major credit card company uses swipe machines that are manufactured overseas. At some point before a shipment of these swipe machines left their overseas factory, someone took the machines apart and added extra circuitry that would transmit credit card information by radio frequency before it would be encrypted by the system. The device was re-sealed so that no one could detect the tampering. A user in the United States would swipe his or her card without knowing that vital information was being relayed to an unauthorized recipient.

Brenner adds that the swipe machine did not relay data on every card -- that would increase the chance of detection. Instead, it would betray only a small percentage of the transactions. However, with many machines in operation, this effort would generate huge amounts of stolen information. It would be relayed to another country, where it would be used to clean out certain accounts. The money would be wired to a fourth country, where it would disappear before the close of the business day.

Companies need to establish processes, not just technologies,that ensure their information security. Brenner decries companies that do not automate patching. "When Microsoft announces a vulnerability and distributes a patch, the hackers are on it in seconds," he says. "They are adapting their attacks in minutes. There are very few companies that within minutes -- within months in many cases-will apply these patches."

Brenner suggests that companies triage among issues that they can deal with alone; issues that companies cannot deal with alone, but can be addressed by the private sector as a whole; and cultural aspects that everyone must live with, such as the desire for constant and seamless communication. With this approach, the risks become manageable.

"Espionage and treachery are nothing new in the world," Brenner declares. "What is new is that they're enabled to an extraordinary degree by the devices we love that make our lives easier. People are not used to thinking about these devices we love being potential sources of treachery.

"We don't want people to stop communicating, but we want people to understand that there are certain environments in which they have to communicate a little differently if they want to protect themselves."