Cyberwar: Sabotaging the System

Managing Network-Centric Risks and Regulations

Research 021-111609-03

Executive Overview

The computer systems that govern the operation of the world's electrical grids, oil and gas production and distribution facilities, nuclear power plants, water purification systems and financial systems are becoming increasingly vulnerable to cyber attack. This is because they are now being integrated with existing business information systems and deployed on common operating systems to more easily provide decision makers with better information. But these new connections and common systems have introduced a series of vulnerabilities that are opening the door to more viruses, worms and potential cyber-attackers.

The good news is that it is now possible for organizations to better secure their control systems without sacrificing performance. ArcSight provides the security and compliance management solutions that intelligently identify and mitigate business risk. Designed with the needs of highly complex, geographically dispersed and heterogeneous business and technology infrastructures in mind, ArcSight provides the industry's only vendor-neutral solution for intelligent identification, prioritization and network response to external security attacks, insider threats and compliance breaches.

This paper highlights these growing threats through a 60 Minutes interview, conducted with industry thought leaders. The segment aired on November 8, 2009. The paper concludes with ArcSight industry leading solutions that can enable organizations to effectively manage control system security and compliance.

Cyber Espionage and Cyber Warfare Statistics

360 million attempts to break into the Pentagon in 2008

+150% increase in unauthorized access to U.S. government computers in past 2 years

1,500 pentagon systems shutdown after the U.S. Defense Secretary's e-mail was breached

3 million+ cyber attacks a day experienced by Global Information Grid (GIG), the U.S. military network with 17 million computers

2 nuclear power plants shutdown due to cyber incidents since 2006

$1 million/day: cost to purchase power from other parts of the grid when a plant is shutdown

$700 billion+: possible cost of a single wave of cyber attacks on critical infrastructure

50 major hurricanes hitting the United States could cost the same as a single wave of cyber attacks on critical infrastructure

Cyberwar: Sabotaging the System

60 Minutes: Former Chief of National Intelligence Says U.S. Unprepared for Cyber Attacks

Nothing has ever changed the world as quickly as the Internet has. Less than a decade ago, "60 Minutes" went to the Pentagon to do a story on something called information warfare, or cyber war as some people called it. It involved using computers and the Internet as weapons.

Much of it was still theory, but we were told that before too long it might be possible for a hacker with a computer to disable critical infrastructure in a major city and disrupt essential services, to steal millions of dollars from banks all over the world, infiltrate defense systems, extort millions from public companies, and even sabotage our weapons systems.

Today it's not only possible, all of that has actually happened, plus a lot more we don't even know about.

It's why President Obama has made cyber war defense a top national priority and why some people are already saying that the next big war is less likely to begin with a bang than a blackout.

"Can you imagine your life without electric power?" Retired Admiral Mike McConnell asked correspondent Steve Kroft.

Until February of this year, McConnell was the nation's top spy. As chief of national intelligence, he oversaw the Central Intelligence Agency, the Defense Intelligence Agency and the National Security Agency. Few people know as much about cyber warfare, and our dependency on the power grid, and the computer networks that deliver our oil and gas, pump and purify our water, keep track of our money, and operate our transportation systems.

"If I were an attacker and I wanted to do strategic damage to the United States, I would either take the cold of winter or the heat of summer, I probably would sack electric power on the U.S. East Cost, maybe the West Coast, and attempt to cause a cascading effect. All of those things are in the art of the possible from a sophisticated attacker," McConnell explained.

"Do you believe our adversaries have the capability of bringing down a power grid?" Kroft asked.

"I do," McConnell replied.

Asked if the U.S. is prepared for such an attack, McConnell told Kroft, "No. The United States is not prepared for such an attack."

"It is now clear this cyber threat is one [of] the most serious economic and national security challenges we face as a nation," President Obama said during a speech.

Four months after taking office, Obama made those concerns part of our national defense policy, declaring the country's digital infrastructure a strategic asset, and confirming that cyber warfare had moved beyond theory.

"We know that cyber intruders have probed our electrical grid, and that in other countries cyber attacks have plunged entire cities into darkness," the president said.

But the people who do these sorts of things are no longer teenagers making mischief. They're now likely to be highly trained soldiers with the Chinese army or part of an organized crime group in Russia, Europe or the Americas.

"They can disrupt critical infrastructure, wipe databases. We know they can rob banks. So, it's a much bigger and more serious threat," explained Jim Lewis, director of the Center for Strategic and International Studies.

Lewis led a group that prepared a major report on cyber security for President Obama.

"What was it that made the government begin to take this seriously?" Kroft asked.

"In 2007 we probably had our electronic Pearl Harbor. It was an espionage Pearl Harbor," Lewis said. "Some unknown foreign power, and honestly, we don't know who it is, broke into the Department of Defense, to the Department of State, the Department of Commerce, probably the Department of Energy, probably NASA. They broke into all of the high tech agencies, all of the military agencies, and downloaded terabytes of information."

How much is a terabyte?

"The Library of Congress, which has millions of volumes, is about 12 terabytes. So, we probably lost the equivalent of a Library of Congress worth of government information in 2007," Lewis explained.

"All stolen by foreign countries?" Kroft asked.

"Yeah. This was a serious attack. And that's really what made people wake up and say, 'Hey, we've got to get a grip on this,'" Lewis said.

But since then, there has been an even more serious breach of computer security, which Lewis called the most significant incident ever publically acknowledged by the Pentagon.

Last November, someone was able to get past the firewalls and encryption devices of one of the most sensitive U.S. military computer systems and stay inside for several days.

"This was the CENTCOM network," Lewis explained. "The command that's fighting our two wars. And some foreign power was able to get into their networks. And sit there and see everything they did. That was a major problem. And that's really had a big effect on D.O.D."

Asked what he meant by "sit there," Lewis said, "They could see what the traffic was. They could read documents. They could interfere with things. It was like they were part of the American military command."

Lewis believes it was done by foreign spies who left corrupted thumbnail drives or memory sticks lying around in places where U.S. military personnel were likely to pick them up. As soon as someone inserted one into a CENTCOM computer, a malicious code opened a backdoor for the foreign power to get into the system.

Lewis said the Pentagon has now banned thumbnail drives.

"My impression is most people understand that there is a threat out there. I don't think most people understand that there are incidents that are happening," Kroft remarked.

"You know, I've been trying to figure out why that is. And some of it is the previous administration didn't want to admit that they had been rolled in 2007. There's a disincentive to tell people, 'Hey, things are going badly.' But it doesn't seem to be sinking in. And some of us call it 'the death of a thousand cuts.' Every day a little bit more of our intellectual property, our innovative skills, our military technology is stolen by somebody. And it's like little drops. Eventually we'll drown. But every day we don't notice," Lewis said.

Congress has noticed, allocating $17 billion for a top secret national cyber security initiative, and the Department of Defense has nominated Lieutenant General Keith Alexander, head of the NSA, to run a new military command devoted to offensive and defensive cyber war.

"How much of this are we doing? We, meaning the United States," Kroft asked Lewis.

"We're in the top of the league, you know? We're as good as any," Lewis said.

"So, whatever foreign countries are doing to the United States, the United States is doing to them?" Kroft asked.

"We're in the top of the league. We are really good. And if you talk to the Russians or the Chinese, they say, 'How can you complain about us, when you do exactly the same thing?' It's a fair point with one exception: we have more to steal. We have more to lose. We're the place that depends on the Internet. We've done the most to take advantage of it. We're the ones who've woven it into our economy, into our national security, in ways that they haven't. So, we are more vulnerable," Lewis said.

Even the country's most powerful weapons are targets. So technicians at the Sandia National Laboratories make their own microchips for nuclear weapons and other sophisticated systems. Jim Gosler - one of the fathers of cyber war - says most commercial chips are now made abroad and there are concerns that someone could tamper with them.

"So you're worried about somebody being able to get in and reprogram a nuclear weapon, or get inside and put something in there that would make it…," Kroft asked.

"Well, certainly alter its functionality," Gosler said.

Asked what he means by "alter its functionality," Gosler said, "Such that when the weapon needed to be to go operational, it wouldn't work."

"Have you found microchips that have been altered?" Kroft asked.

"We have found microelectronics and electronics embedded in applications that they shouldn't be there. And it's very clear that a foreign intelligence service put them there," Gosler said.

"There are thousands of attempted attacks every day, tens of thousands of attacks," Sean Henry, an assistant director of the FBI in charge of the bureau's cyber division, told Kroft.

Henry's job is to police potential targets all over the United States. He told "60 Minutes" that criminals have used the Internet to steal more than $100 million from U.S. banks so far this year and they did it without ever having to draw a gun or pass a note to a teller.

"The FBI became famous stopping bank robberies. Are there more bank robberies in terms of the amount of money stolen on the Internet than there are guys walking into branches with guns?" Kroft asked.

"Absolutely," Henry said. "I've seen attacks where there's been $10 million lost in one 24-hour period. If that had happened in a bank robbery where people walked in with guns blazing, that would've been headline news all over the world."

"And the bank probably didn't want it known," Kroft remarked.

"Certainly when there's a network breach, the owners of the network are not keen to have it known that their network was breached because of their concern that it might impact their business," Henry said.

The case Henry mentioned didn't involve just one bank - it involved 130, all of them victimized through an international network of ATMs, an international caper that required dozens of participants on three different continents.

Asked how they did it, Henry said, "It was a sophisticated operation. Clearly organized where adversaries accessed a computer network, were able to gain information from multiple accounts. They were able to decrypt PIN numbers and then taking that data, able to manufacture white plastic that enabled them access to get into ATM accounts."

Asked what white plastic is, Henry said, "Take a piece of plastic that's similar in size and shape and weight to an ATM card."

"They've got the card. They've got the PIN number and they just drained the accounts?" Kroft asked.

"Almost $10 million in 24-hour period," Henry said.

According to Henry, the cyber heist happened in 49 cities around the world, in Europe, North America, South America, and Asia.

Henry told Kroft they have an idea from which country the perpetrators were from, but he would not divulge that information during the interview.

Asked if they have caught any of the suspects yet, Henry said, "Workin' on it."

Another case you have probably not heard anything about involves an extortion plot against the state of Virginia. Earlier this year, a hacker got into a medical database and stole millions of patients' prescription records and then followed it up with a ransom note.

"The note said, 'I have your…' - I can't say that word on television - stuff, we'll call it 'in my possession right now,'" Kroft said.

The hacker went on to write, "I've made an encrypted backup and deleted the original. For $10 million, I will gladly send along the password."

The state of Virginia says it was eventually able to restore the system. But the stolen information, including names, Social Security numbers and prescriptions can be used, sold or exploited according to the FBI.

"Did the Virginia Prescription Monitoring Program pay the $10 million?" Kroft asked Henry.

"I can't discuss that," he replied.

"But you say this is an active investigation. I mean, this is a matter of public record. I mean, this actually happened," Kroft remarked.

"This is an active investigation that we're still involved in, and we are coordinating with the victim. They're cooperating with us, and we're actively involved with them and other state and local law enforcement agencies," Henry said.

Asked whoever did this is still at large, Henry told Kroft, "I imagine."

As serious as the electronic theft of hundreds of millions of dollars by computer thieves might seem, they pale in comparison to some of the other possible scenarios that are no longer outside the realm of possibility. They include an assault on the fiber optic networks that run the world's financial systems.

Admiral McConnell, the former director of national intelligence, worries about the integrity of America's money supply.

"I know that people in the audience watching this are going to say, 'Could somebody steal money out of my bank account or could somebody attack a bank that would wipe out my life savings?'" Kroft asked.

"And the answer is yes, that's possible, but that is not the major problem. The more insidious issue is, what happens when the attacker is not attempting to steal money, but to destroy the process that accounts for money? That's the real issue we have to worry about," McConnell said.

"It's all record keeping. It's accountability of the wealth and the movement of that money through the system that had to be reconciled at the speed of light. So if you impact or contaminate the data or destroy the data where you couldn't have reconciliation, you could have cascading impact in the banking system," he added.

Asked to describe the consequences, McConnell said, "If everybody goes down to take the money out, it's not there. So that's the issue. Since banking is based on confidence, what happens when you destroy confidence?"

One top U.S. intelligence official is on record saying that the Chinese have already aggressively infiltrated the computer networks of some U.S. banks and are operating inside U.S. electrical grids, mapping out our networks and presumably leaving behind malicious software that could be used to sabotage the systems.

"Can a penetrator or a perpetrator leave behind…things that will allow them to be there and watch and look…and listen?" Kroft asked.

"Any successful penetration has the potential for leaving behind a capability," McConnell said.

"Do we believe that there are, the governments have planted code in the power grid?" Kroft asked.

"Steve, I would be shocked if we were in a situation where tools and capabilities and techniques have not been left in U.S. computer and information systems," McConnell said.

Of all the critical components in the U.S. infrastructure, the power grid is one of the most vulnerable to cyber attack. The U.S. government has control of its own computers and those of the military. The power grid, which is run and regulated by private utilities, is unbeholden to government security decrees.

At the Sandia National Laboratories, Department of Energy security specialists like John Mulder try to hack into computer systems of power and water companies, and other sensitive targets in order to figure out the best way to sabotage them.

It's all done with the companies' permission in order to identify vulnerabilities.

In one test, they simulated how they could have destroyed an oil refinery by sending out code that caused a crucial component to overheat.

"The first thing you would do is turn it to manual controls so that your automatic controls aren't protecting you," Mulder explained.

Asked what the main target would be, Mulder said, "The heating element and the re-circulator pump. If we could malfunction both of those we could cause an explosion."

"How would you do that?" Kroft asked.

"The first thing we had to do was actually gain access to the network and that's, we just got that as launch attack. And then we turn up the BTUs, and then we're turning off the re-circulator pump. There we go," Mulder said.

Mulder said this type is simulation is "very" realistic.

But the companies are under no obligation to fix the vulnerabilities, which was graphically demonstrated in a much more realistic fashion at the Idaho National Labs two years ago in a project called "Aurora."

A group of scientists and engineers at the Department of Energy facility wanted to see if they could physically blow up and permanently disable a 27-ton power generator using the Internet.

"If you can hack into that control system, you can instruct the machine to tear itself apart. And that's what the Aurora test was. And if you've seen the video, it's kind of interesting, 'cause the machine starts to shudder. You know, it's clearly shaking. And smoke starts to come out. It destroys itself," Jim Lewis explained.

Asked what the real-world consequences of this would be, Lewis said, "The big generators that we depend on for electrical power are one, expensive, two, no longer made in the U.S., and three, require a lead time of three or four months to order them. So, it's not like if we break one, we can go down to the hardware store and get a replacement. If somebody really thought about this, they could knock a generator out, they could knock a power plant out for months. And that's the real consequence."

When Congressman Jim Langevin, who chaired a subcommittee on cyber security heard about it, he called representatives of the nation's electric utilities to Washington to find out what they were doing to fix the vulnerability.

The committee was told that the problem was being addressed. But that turned out not to be the case.

At a subsequent hearing seven months later, Langevin's committee members discovered that almost nothing had been done.

"Basically they lied to Congress, and I was outraged," Rep. Langevin told Kroft.

Asked if they admitted lying to Congress, Langevin told Kroft, "They admit that they misled Congress, that they did not give accurate testimony. And they subsequently had to retract the testimony."

"Have they made any progress since you caught them out in this lie?" Kroft asked.

"No, not sufficiently," Langevin said. "The private sector has different priorities than we do in providing security. Their, in a sense bottom line, is about profits. We need to change that. We need to change their motivation so that when we see a vulnerability like this we can require them to fix it."

Langevin and others have introduced legislation to that would do just that.

"I look at this as, like, a pre-9/11 moment. Where we identify a problem, we identify a threat, we know it exists, we know it's real, and we don't move quickly enough to fix the problem," he said.

"And what I'm worried about is, because of so many competing priorities, and so many issues that we have to deal with, we won't get we, will not get focused on this problem until we have some catastrophic event," Admiral McConnell said.

"If the power grid was taken off line in the middle of winter, and it caused people to suffer and die, that would galvanize the nation. I hope we don't get there. But it's possible that we will."

[End of 60 Minutes Interview.]

Video Link References:

http://www.cbs.com/primetime/60_minutes/video/?pid=n28ulEEUmYArYoieRGI_QLt8gJg19D1k&vs=Default&play=true

http://www.cbs.com/primetime/60_minutes/video/?pid=yOI9t_gYKzxWu18_UHUscHxvlbQ_y98J&vs=Clips&play=true

http://www.cbs.com/primetime/60_minutes/video/?pid=8QByFcMcFYkLrz0OC0ZNTti_MgaV34aJ&vs=Clips&play=true

Addressing Cyber-risk and Threat Monitoring

The ArcSight SIEM platform is designed to help organizations understand who is on the network, what information they are seeing, and which actions they are taking with the information. With this level of visibility, ArcSight customers can protect the business while reducing operating costs. The products are used today across the globe, preventing threats and securing information. ArcSight is unique in its ability to solve cyber-risk and threat monitoring. The ArcSight SIEM platform provides three primary benefits:

- **ArcSight Makes it Easier for Companies to Pass Audits:** Continuous compliance monitoring information, presented in auditor-friendly dashboards, increases the chance of passing audits. Automated collection and reporting cuts the burden on the staff and budget.

- **ArcSight Helps Companies Protect Processes and Data:** Real-time analysis and alerting notifies the department of threats early enough to prevent them and minimize loss.

- **ArcSight Increases Control Over an Organization's Networks as it Becomes Open to Partners and Customers:** Understand at all times who is on the systems, what data is being viewed, and which actions are being taken, whether the users are employees, contractors, customers, or anyone else.

Why ArcSight?

In conclusion to the concepts described in this paper, consider three reasons why ArcSight is best positioned to deliver enterprise threat and risk monitoring:

- **Market Leadership:** As the SIEM market share leader, ArcSight protects the IT infrastructure of the most demanding organizations in the world, including global banks, civilian and military government organizations, and many of the largest retailers in the world.

- **Future Proof:** The job of a CIO is to ensure that an organization's information strategy evolves with the business strategy. The unique ArcSight architecture ensures that as your technology changes, you will be able to continuously monitor the business for risk.

- **Platform Neutral:** Unlike large security enforcement vendors, ArcSight is well-suited to monitor technologies from a variety of providers. ArcSight focuses on risk and threat monitoring, across any third party platform.

About ArcSight:

ArcSight (NASDAQ: ARST) is a leading global provider of security and compliance management solutions that protect businesses and government agencies. ArcSight identifies, assesses, and mitigates both internal and external cyberthreats and risks across the organization for activities associated with critical assets and processes. With the market-leading ArcSight SIEM platform, organizations can proactively safeguard their assets, comply with corporate and regulatory policy and control the risks associated with cybertheft, cyberfraud, cyberwarfare and cyberespionage. For more information, visit www.arcsight.com.

ArcSight

To learn more, contact ArcSight at: info@arcsight.com or 1-888-415-ARST