CYBERSECURITY FOR TELECOS

BACKGROUND

Cybersecurity has always been an important issue for telcos, and is becoming more so as a result of an increasing number of threats and increasingly more complex and serious threats. An Executive Order is also around the corner, and legislation is continually on the plate in Congress.

CHALLENGES

Washington, D.C.-based USTelecom, previously known as the United States Telephone Association, is a national trade association representing service providers and suppliers for the telecom industry. Membership ranges from large publicly-traded communications corporations to small private cooperatives, all providing advanced communications services to urban and rural markets.

USTelecom notes that, "A single cyber-attack on an unsuspecting carrier could disable thousands of consumers' communications services if delivered effectively. For a cyber-terrorist, this potential for mass destruction makes carriers and their affiliated industry members very appealing targets." It goes on to note that: "Cyber-attacks are here to stay and will only grow more dangerous and sophisticated as the Internet ecosystem evolves. The efforts by carriers to deploy effective measures will remain a vital component of our national security posture."

In terms of cybersecurity threats for telcos, according to Steven Senne, P.E., chief technology officer for Finley Engineering Company, there may be people trying to penetrate their networks, finding weaknesses and exploiting holes in their firewalls and internal networks. "Telcos may be also subject to attacks on their websites or VoIP systems," said Senne. He points out that a number of telcos already have relatively stringent security programs in place and do a good job maintaining their own security. Unfortunately, though, security may be somewhat of an afterthought for other telcos. "It may be something they thought about a few years ago when they upgraded their networks or did some rework on their networks," he said. "Since that time, though, it may have ended up on a back burner."

There are also some social engineering concerns, where hackers try to get around some security measures by exploiting the workers in the company. An example of this is phishing e-mails with forged links to try to install backdoor software. "Your system should be able to filter out the vast majority of phishing attacks," said Senne. "However, every now and then, one will get through, and someone will click on the link."

Of even greater concern, according to Senne, is that a lot of attacks these days are silent. In these cases, the hackers don't want to let themselves be known. "This can be scary," he said. "In this situation, someone gets access to the network but doesn't do anything immediately."

Certainly, most hackers who want to mount these attacks are going to target large utilities or large telcos. So why should rural telcos be concerned? "Some hackers may focus on smaller rural telcos as an alternate route or a back-door entry into a power company network or a military installation," said Senne.

According to Senne, virtually all telcos had a good network design when they set things up. However, over the years, they may have let their anti-virus software go out of date, and/or they may be running a firewall but may not have had the software or firmware on it patched in recent times. As a result, they are not protected against any of the known exploits that have been developed in recent years.

According to Michael Goins, general manager, Midwest Data Center, a division of Rock Port Telephone Company (Rock Port, Missouri), his company typically isn't a target by a foreign government or by corporate espionage. "Our biggest threat is to our ISP customers," he said. "When you provide Internet services to subscribers, you tend to get some overzealous people who like to experiment with computers in a destructive manner. There can also be problems with disgruntled employees." The sophistication of the attacks can vary, according to Goins. "In our company, though, we are fortunate, in that we haven't seen any very sophisticated threats."

In the meantime, the industry has been working tirelessly to address the issue of cybersecurity. "This industry has done a lot of work over the years on its own, especially because it has so many enterprise clients, where cybersecurity is an absolute necessity," said Anne Veigle, vice president, media affairs, for USTelecom.

FINLEY ENGINEERING
INTEGRITY INTO EVERYTHING

GOVERNMENT INVOLVEMENT

While the industry is taking steps to address cybersecurity concerns, the government has also been getting involved.

An October 2012 Bloomberg Government Study, "Companies Face Expanded Federal Role in Cybersecurity," by Afzai Bari, a Bloomberg Government technology analyst, and Jason Wilson, a federal business intelligence analyst, looked at possible cybersecurity standards, existing regulatory authority, and federal spending on cybersecurity.

The study concluded that electric utilities, telecommunications companies, banks, and other businesses operating the nation's infrastructure may be pressed to improve cybersecurity as a result of an update that the White House is drafting to a homeland security directive. This directive may tell government agencies that regulate electric utilities, telecommunications companies, banks, and other infrastructure-related businesses to use their (the agencies') regulatory authority to draft new rules and/or issue cybersecurity standards for these businesses. The rules may be voluntary or expand existing requirements. Currently, according to the study, the Obama administration is most concerned with telecommunications companies and electric utilities.

One part of the draft directive calls for a near real-time system to monitor cyber threats to critical infrastructure. The system may require companies to deploy systems that monitor Internet traffic and share information on cyber attacks. A potential model for such a system is an existing program that links telecommunications networks to defense contractors' computer systems to monitor Internet traffic for malicious activity. Another possibility is a system that receives feeds from companies to monitor traffic and share information on cyber attacks.

What is still unclear is what type of standards or rules the agencies may issue. As a result, costs cannot be determined. However, companies that operate the nation's critical infrastructure said in a January 2012 Bloomberg survey that they would have to pay, on average, nearly twice as much each year to improve network security in the next 12 to 18 months.

In November 2012, the Senate failed to pass cybersecurity legislation, originally introduced by U.S. Rep. Michael Rogers (R-Michigan) in November 2011, called the Cyber Intelligence Sharing and Protection Act (CISPA). The bill would have allowed the government to share all of its classified cyber-security knowledge with private companies, forming knowledge-sharing agreements that would be designed to keep foreign and domestic hackers out of the U.S. computer networks. In addition, companies would also be allowed to share private data with the federal government, provided there was a reasonable cyber-threat.

The Senate killed the legislation in part due to the U.S. Chamber of Commerce's opposition to the "voluntary standards" nature of the legislation, seeing the approach as a "back door" to regulation, as well as an approach that would quickly become out of date as cyberthreats continued to evolve.

Another challenge to the legislation was that, since it encouraged government and companies to share information about cyber threats, the Obama administration threatened to veto any legislation that did not safeguard the privacy of that shared consumer data.

In response, the White House released a draft executive order in late 2012, which was limited, in that it would only be able to ask for voluntary participation among most targeted power plants, water systems and other utilities, since these utilities are privately-held.

The draft executive order contained a Cyberspace Policy Review, which identified ten near-term actions to improve cybersecurity:

1 - Appoint a cybersecurity policy official responsible for coordinating the nation's cybersecurity policies and activities.

2 - Prepare for the president's approval an updated national strategy to secure the information and communications infrastructure.

3 - Designate cybersecurity as one of the president's key management priorities and establish performance metrics.

4 - Designate a privacy and civil liberties official to the NSC cybersecurity directorate.

5 - Conduct interagency-cleared legal analyses of priority cybersecurity-related issues.

6 - Initiate a national awareness and education campaign to promote cybersecurity.

7 - Develop an international cybersecurity policy framework and strengthen our international partnerships.

8 - Prepare a cybersecurity incident response plan, and initiate a dialogue to enhance public-private partnersh partnerships.

9 - Develop a framework for research and development strategies that focus on game-changing technologies that have the potential to enhance the security, reliability, resilience and trustworthiness of digital infrastructure.

10 - Build a cybersecurity-based identity management vision and strategy, leveraging privacy-enhancing

technologies for the nation.

The draft executive order would direct certain government agencies to look into taking action. For example:

- NIST would be responsible for developing a cyber security framework.

- DHS would be responsible for producing unclassified reports on specific targeted threats.

- Multiple agencies would also work together to create a system for tracking and reporting cybersecurity incidents.

"We are expecting the final executive order in the near future," said USTelecom's Veigle. "We think there will be some positive things in that executive order."

Meanwhile, Rep. Rogers plans to reintroduce CISPA in the current session of Congress, and will push hard to make sure the revised bill will be acceptable to the Senate. "We don't know if it will encounter opposition as it did last year," said Veigle.

Regardless of what does or doesn't happen with legislation, the executive order would continue to exist on its own. "Legislation wouldn't replace it," said Veigle. "However, an executive order can only do so much. The executive order would allow government agencies to clarify certain roles, but wouldn't actually change the law. For example, legislation would be necessary to allow information sharing. The law, as it exists, prohibits certain communications between private industry and government."

REACTION TO GOVERNMENT INVOLVEMENT

Currently, according to Veigle, USTelecom is working out the advocacy positions that it will take in tandem with other communications providers, such as the cable industry and wireless industry.

"What the telecoms really need is legislation that will enable information sharing between private industry and government, so that, if networks get a threat, they can share that information," said Veigle. "Right now, they are not allowed to do so, which is currently a big downside for all of us, because there is very potent and dangerous stuff happening to the networks that are taken care of, but that we never know anything about. It would be useful to be able to share that, so everyone is on the same page. This is only possible with legislation."

One thing the industry doesn't want, according to Veigle, is the government coming in heavy-handed, telling companies how to operate their networks. "This would be very counterproductive," she said. "Companies want the ability to respond very quickly to attacks. Having to notify multiple government agencies and file a lot of reports would be detrimental to that."

According to Finley Engineering's Senne, if legislation or an executive order does come to pass, not only will telcos have to make sure their cybersecurity systems are effective, but they will also likely need to follow a much more formalized audit process.

"In order for any cybersecurity measures to truly be effective, there needs to be a paper trail when any threat is detected," said Midwest Data Center's Goins. "One concern with legislation is that there will likely be an exorbitant amount of recordkeeping. It is difficult enough in the competitive environment we are in to cover our costs and turn a profit. However, if we have a central government impose strict regulations on monitoring and recordkeeping, the sheer volume of records would eat up terabytes of disk space." Then, he added, telcos would also have to be able to manage and search the data so they could provide information to law enforcement upon request. "There doesn't seem to be a moderate approach to this," he said. "I think that any cybersecurity legislation needs to have some sort of unified mechanism for maintaining these logs and records across the industry."

,

RECOMMENDATIONS

In the meantime, what can telcos do to improve their cybersecurity measures?

According to Goins, it is important to have a multi-tiered security infrastructure, including access control

list on the perimeter, deep packet inspection, and threat management in the form of firewalls. "These firewalls need to be updated on a regular basis," he said.

, Finley Engineering' Senne offered some additional recommendations:

1 - First, and at a minimum, update existing security technology (antivirus software, firewall patches, etc.).

2 - Engage in employee education. Make sure your employees know how to recognize a phishing link. "For example, you can hold your mouse over it and look at the URL that pops up to see if it looks like it is supposed to," he said.

3 - Create an internal audit system. A good audit should cover the firewalls and internal security. If someone gets through the firewall and into the network, are they using default passwords and user names on servers and telecom equipment? Are they running the appropriate and updated anti-virus programs in-house? Do they have an intrusion detection system in place?

USTelecom also offers some resources of interest to telcos. In October 2012, it unveiled its Cybersecurity Toolkit, a one-stop on-line source of information designed for a broad set of stakeholders involved in cybersecurity policy, research and planning. The Toolkit is a linkable resource that organizes the cyber policy world into the various arms of government, academia, industry and partnership groups that are working together on cybersecurity issues. The Toolkit provides links to the latest key congressional, academic and military reports, as well as up-to-date information from groups tracking real-time cyber threats. Links provide access to the multitude of laws and regulations on the books now that address computer security, as well as information about common attack methods and security protective exercises. Links are also provided to ongoing legislative efforts in Congress, recent Congressional Research Service and Government Accountability Office reports on various aspects of cybersecurity, and efforts by multiple government agencies to track and protect against cyber-attacks. "The Toolkit also provides a lot of 'best practices,' by providing links to individual companies on some of the measures they have taken related to cybersecurity," said Veigle.

The Toolkit is available at: www.ustelecom.org/issues/cybersecurity/ustelecom-cybersecurity-toolkit.

Steven Senne, P.E.
Chief Technology Officer
Finley Engineering Company
Johnston, Iowa

Michael Goins
General Manager
Midwest Data Center
a division of Rock Port Telephone Company
107 Opp St.
Rock Port MO 64482
Office: 660-744-5900 x0
Cell: 660-744-4411

Anne Veigle
Vice President, Media Affairs
USTelecom
Washington DC
202-326-7344
aveigle@ustelecom.org