Testimony of

Mark Shlanta

Chief Executive Officer

SDN Communications

on

"Confronting the Challenge of Cybersecurity"

before the

U.S. Senate Committee on Commerce, Science, and Transportation

September 3, 2015

Thank you, Senator Thune, for inviting SDN[1] to participate in today's field hearing. It is an honor to join this esteemed panel of experts to discuss the actions that should be taken to address the cyber threats facing our state and nation.

We applaud Senator Thune for his support of the voluntary framework that was developed by industry stakeholders and the National Institute of Standards and Technology (NIST). Our national and economic security depends upon the reliable functioning of critical infrastructure.[2] The communications industry represents one of the 16 critical infrastructure sectors.[3] The NIST Framework provides useful guidance and best practices to assist critical infrastructure operators in protecting their networks. In addition to codifying this successful process, Senator Thune's "Cybersecurity Enhancement Act" took important steps to increase our nation's commitment to cyber research, workforce development, and raising public awareness.[4]

The title of today's hearing, "Confronting the Challenge of Cybersecurity," gets to the heart of this pervasive and constantly evolving threat. Cybersecurity is not a problem limited to high-profile retailers, financial institutions, or the federal government. It is widespread. Any individual or organization using technology is a target. It can be daunting for individuals, businesses, and all levels of government to navigate how they can best reduce their risk.

[1] SDN Communications ("SDN") is the premier business-to-business broadband service provider in South Dakota and southern Minnesota with a fiber optic network connecting eight states with high-speed broadband Internet and Wide Area Network (WAN) connectivity. In 2014, SDN became an owner and the managing partner for Southern Minnesota Broadband, LLC, which extends SDN's fiber network across southern Minnesota. SDN also provides networking equipment, phone systems, and managed solutions, including security, routers, firewalls, remote network monitoring, and storage.

[2] "Framework for Improving Critical Infrastructure Cybersecurity," National Institute for Standards and Technology," page 1, February 12, 2014, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

[3] "Critical Infrastructure Sectors," Department of Homeland Security, June 12, 2014, http://www.dhs.gov/critical-infrastructure-sectors.

[4] "Rockefeller, Thune Statement on Passage of Commerce Cybersecurity Bill," Senator Thune Official Website, December 12, 2014, http://www.thune.senate.gov/public/index.cfm/2014/12/rockefeller-thune-statement-on-passage-of-commerce-cybersecurity-bill.

It was appropriate to host this discussion at Dakota State University (DSU), an academic institution that has distinguished itself as a national leader in cybersecurity education. The National Security Agency (NSA) and Department of Homeland Security designated DSU as one of the nation's first National Centers of Academic Excellence.[5] This summer, DSU, with support from the NSA and National Science Foundation, hosted a camp to get more young women interested in cybersecurity careers. When the 60 available spots quickly filled, SDN sponsored 40 additional participants. Like other operators of critical infrastructure, SDN relies upon a strong pipeline of skilled workers, and we are lucky to have many DSU graduates on our team. Prioritizing continued workforce development in the field of cybersecurity is an important national objective.

It feels like it has become nearly impossible to turn on the news without learning of yet *another* company or federal department that has been compromised. We hear about the high-profile attacks against companies like Sony, Target, Anthem, Home Depot, and JPMorgan Chase, and many small and regional businesses assume this is a problem targeting only large companies. Unfortunately, we here in South Dakota are not immune to this threat.

SDN sees a large number of threats against its own network and customers each day. SDN quarantines about half the emails directed toward its domain. Additionally, our company firewall blocks hundreds of unauthorized, malicious traffic attempts each day. We observed nearly 4,500 threats against SDN customers within a single year. Each of these threats ranged from one to several thousand separate attacks.

Bedford Industries is a small business, based in Worthington, MN, that subscribes to SDN's cybersecurity services. The company manufactures wire twist ties and other packaging equipment. Although an outside observer might question why Bedford would be a target, SDN's cybersecurity threat report tells a different story. In the past year, SDN successfully halted more than 100 types of cyberattacks against Bedford—ultimately mitigating over 5,300 separate incidents. In layman's terms, this means attackers tried to break into Bedford's network 5,300

[5] "Centers of Academic Excellence Institutions," National Security Agency, July 8, 2015, https://www.nsa.gov/ia/academic_outreach/nat_cae/institutions.shtml#sd.

times using 100 different attack methods. Some of the threats were launched by attackers in the United States, but others originated as far away as Brazil.

SDN offers a host of security services to counter cyber threats targeting businesses in South Dakota and the surrounding region. We provide secure data storage at our LaMesa Data Center that protects health care, financial, and other sensitive information. We also offer around-the-clock remote network monitoring that detects and responds to unusual, potentially malicious activity on customer equipment and networks. Our managed firewall service blocks harmful malware to prevent viruses from entering a customer's network, and SDN's managed router service closes security gaps by ensuring devices are properly configured. Currently, a limited number of business broadband customers subscribe to these managed services, and their networks subsequently face a heightened risk of cyberattack. Raising public awareness is key to strengthening our nation's preparedness.

SDN is in the process of deploying a managed Distributed Denial of Service ("DDoS") protection product. DDoS is a type of attack that can disable an online service by overwhelming it with massive data traffic. A DDoS attacker controls numerous infected machines—often termed "zombies" or "botnets"—to generate the data volumes required to perpetrate an attack. In some instances, a DDoS attack is designed to disrupt the delivery of services and impede private and public business operations. On other occasions, it may be a diversionary tactic timed to coincide with a coordinated effort to break through network defenses.

There has been a dramatic rise in the number of DDoS threats occurring across the United States, including in South Dakota.[6] During SDN's early deployment of this product, we have detected malicious DDoS traffic targeting the networks of South Dakota businesses and state government. Just last week during a single 24-hour period, SDN's technical team detected 105 possible malicious traffic patterns.[7] A 25-gigabit attack is the largest DDoS threat we have seen since launching the product.[8] To put this in perspective, a 25-gigabit attack would completely saturate a high-bandwidth business customer subscribing to a 10-gigabit Internet connection. A threat of this magnitude would take down or severely cripple the networks of most business customers in South Dakota.

Businesses are not the only organizations facing cybersecurity threats. South Dakota state and local governments, as well as our post-secondary education institutions, are regularly targeted by hacktivists and hackers. These attacks may involve DDoS threats. As previously described, a DDoS attack may be politically motivated, or it may represent a diversionary tactic working in concert with other efforts to infiltrate a network. Sometimes there is simply no clue as to why these attacks occur. On occasion, attackers warn their targets and are even boastful of their efforts. **Figure 1** and **Figure 2** include screenshots of Twitter posts from July 2015 warning of a forthcoming attack. **Figure 3** contains a "target list" of federal, state, and local government entities that the attacker has identified as targets. The domain names of the South Dakota state

[6] "Q1 2015 State of the Internet – Security Report," State of the Internet Akamai Report, 2015, https://www.stateoftheinternet.com/security-cybersecurity-ddos-mitigation.html

"Trustwave Global Security Report," Trustwave, 2015, https://www2.trustwave.com/rs/815-RFM-693/images/2015_TrustwaveGlobalSecurityReport.pdf

There has been a dramatic rise in the number of DDoS attacks, with the incidents of attacks doubling between Q1 2014 and Q1 2015. While hacktivists and other organized cyberattack groups, such as Anonymous or the earlier LulzSec, launch politically motivated attacks impacting large corporations or governments, individual hackers can now easily initiate a cyberattack by subscribing to a DDoS for hire service. According to Trustwave's 2015 Global Security Report, DDoS attacks can be purchased starting at $5.00 an hour, $40.00 for 24 hours, or $900 for one month of attacks. A recent Incapsula survey of IT professionals from companies with 250 to over 10,000 employees determined that even a small DDoS attack can have major financial impacts on the targeted organization. The DDoS attack profile is shifting; while the bandwidth required to execute an attack has decreased, there has been an alarming increase in attack frequency and duration. With low barriers to entry and large dollar amounts at stake, DDoS attacks are on the rise. DDoS cyberattack protection has become critical for organizations dependent upon the Internet for conducting business.

[7] "DDoS Cybersecurity Threat Report for August 24, 2015," SDN Communications.

[8] "DDoS Cybersecurity Threat Report for August 19, 2015," SDN Communications.

government and the city of Sioux Falls were included on the target list. These illustrative examples are attached as an appendix to this testimony.

Providers like SDN offer cybersecurity products that can reduce a company's cybersecurity risk. The story, however, does not end there. Businesses have a responsibility to establish and enforce internal security controls.[9] Employee error can create major vulnerabilities. According to IBM's "2014 Cyber Security Intelligence Index," 95 percent of all security incidents involve human error.[10] Businesses should therefore improve the cyber-literacy of their workforce and limit their employees' access and ability to distribute sensitive information. Businesses should also take the necessary steps to properly configure and maintain their equipment, software, and websites to prevent vulnerabilities that can be exploited.

[9] SDN has cybersecurity internal controls and policies in place to mitigate the company's risk of cyberattack. Businesses—both large and small—should adopt similar practices. While SDN has in-house expertise to operate its internal cybersecurity program, other businesses may opt to outsource this responsibility. For purpose of example, this footnote includes a general, non-comprehensive description of some internal cybersecurity procedures followed by SDN.

SDN protects its network with an enterprise firewall that enforces rules and only accepts traffic from approved external IP addresses. The company conducts daily and sometimes hourly antivirus definition updates to improve the detection of malicious software and prevent harmful downloads. Regular patches to SDN's operating system, PCs, and other devises close security gaps that could be exploited by an attacker. Any patch deemed critical to protecting our equipment and servers is performed immediately. The company enforces access policies that require passwords to be regularly changed and pin codes and badges in order to enter physical locations. Virtual and physical locations are limited to the employees that require access in order to perform their job responsibilities. Cameras and door access logs are equipped throughout the company premise, and fingerprint entry is required at SDN's most secure locations.

SDN requires employees working remotely to utilize an SSL Virtual Private Network (VPN) and perform two-factor authentication to access the company's network. This encryption service masks all traffic between SDN's network and the end user. The company's local administrator policy and account usage monitoring prevents unsanctioned software downloads onto company-issued equipment. Limiting an employee's ability to download malicious software helps reduce the risk of social engineering attacks. SDN also blocks foreign devices from accessing its network using a Network Access Control (NAC) appliance to prevent unauthorized devices from connecting to the network. Outside laptops and mobile devices cannot connect to the company's private wifi network and are segregated onto a guest wifi network.

This represents a limited sample of the security procedures SDN has adopted to protect its internal business network.

[10] "IBM Security Services 2014 Cyber Security Intelligence Index: Analysis of cyber attack and incident data from IBM's worldwide security operations," IBM, June 2014, http://www.slideshare.net/ibmsecurity/2014-cyber-security-intelligence-index.

SDN works to adhere to security standards and best practices to protect the integrity of our network. For decades, we have been researching and incorporating industry and regulatory cybersecurity standards. We completed a Statement on Standards for Attestation Engagement No. 16 (SSAE 16) SOC I compliance report and audit and are currently working through the SSAE 16 SOC II security module. SDN enforces its policies governing how the company operates its network and manages access to its facilities. The company also utilizes security guidance from the Payment Card Industry (PCI) Data Security Standards, Health Insurance Portability and Accountability Act (HIPPA), the Federal Trade Administration's Red Flags Rule, and Customer Proprietary Network Information (CPNI).

SDN has reviewed and continues to study the NIST Framework and the sector-specific guidance from the Federal Communications Commission's Communications Security, Reliability, and Interoperability Council (CSRIC).[11] The NIST Framework helps shift our national focus from a "check-the-box" mentality towards a risk-based approach tailored to addressing and mitigating unique organizational risk.[12] This is a preferred, more effective approach than strict and prescriptive regulation that would struggle to keep up with emerging and constantly evolving threats. The CSRIC guidance provides a useful tool to help communications providers evaluate and utilize the Framework, and it includes tailored recommendations for small operators. Although the Framework has been available since last year, the CSRIC guidance was only recently released this past March. It will take time for small and regional rural operators to fully digest and put these recommendations into practice.

While I applaud these efforts, it is important to remember that SDN—like many small and regional providers in the rural telecom industry—already endeavors to maintain a secure communications network. SDN's cybersecurity program seeks to protect its core network and meet the needs of its customers. That being said, only one thing is certain when it comes to cybersecurity: the job is never done. As such, my legal and technical teams continue with their

[11] "Cybersecurity Risk Management and Best Practices Working Group 4: Final Report, Communications Security, Reliability, and Interoperability Council, Federal Communications Commission, March 2015, https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_WG4_Report_Final_March_18_2015.pdf.

[12] "Cyber Solutions Handbook," Booz Allen Hamilton, page 4, 2014, http://www.boozallen.com/content/dam/boozallen/documents/Cyber-Solutions-Handbook.pdf.

review of the NIST Framework and the CSRIC "best practices" guidance, and SDN plans to utilize both of these tools to strengthen its existing cybersecurity program.

As the Senate Commerce Committee continues monitoring the utilization of the NIST Framework, I encourage you to maintain your support for a voluntary, flexible, and scalable approach to cybersecurity risk management. The federal government should encourage utilization of the Framework through outreach and education to assist critical infrastructure operators in understanding, digesting, and implementing these practices. It is important to note that some small operators may need additional assistance, such as one-on-one technical support, to help them apply the Framework to their unique operations.

In closing, I want to thank you again for inviting SDN to participate in today's field hearing. Cybersecurity is a responsibility that each of us has an obligation to uphold. As individuals, we should take steps to increase our cyber literacy. As businesses—both large and small, we have a responsibility to maintain strong safeguards to protect our network and the sensitive consumer information we have been entrusted. Finally, it is vital that our government and operators of critical infrastructure continue bolstering their defenses against growing and rapidly evolving cyber threats.

Thank you, Senator Thune, for your leadership in the United States Senate and for convening today's hearing to discuss this important topic. With that, I welcome your questions.

Appendix

Figure 1.

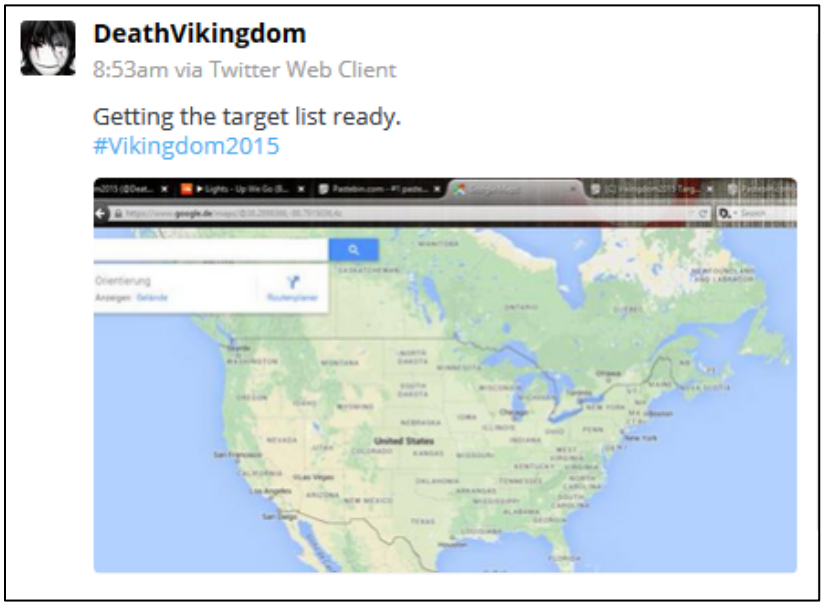


Figure 2.

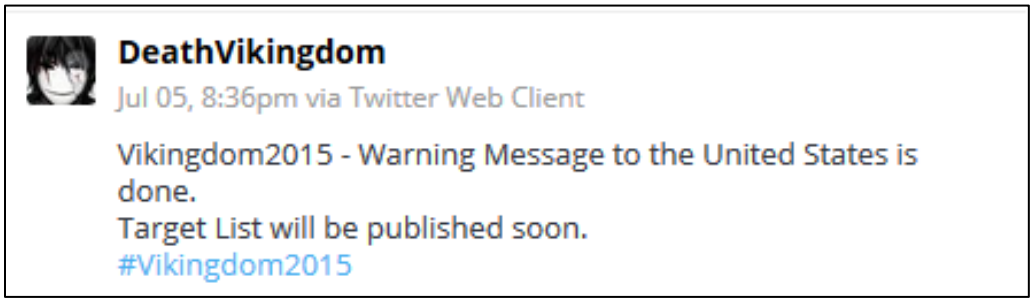
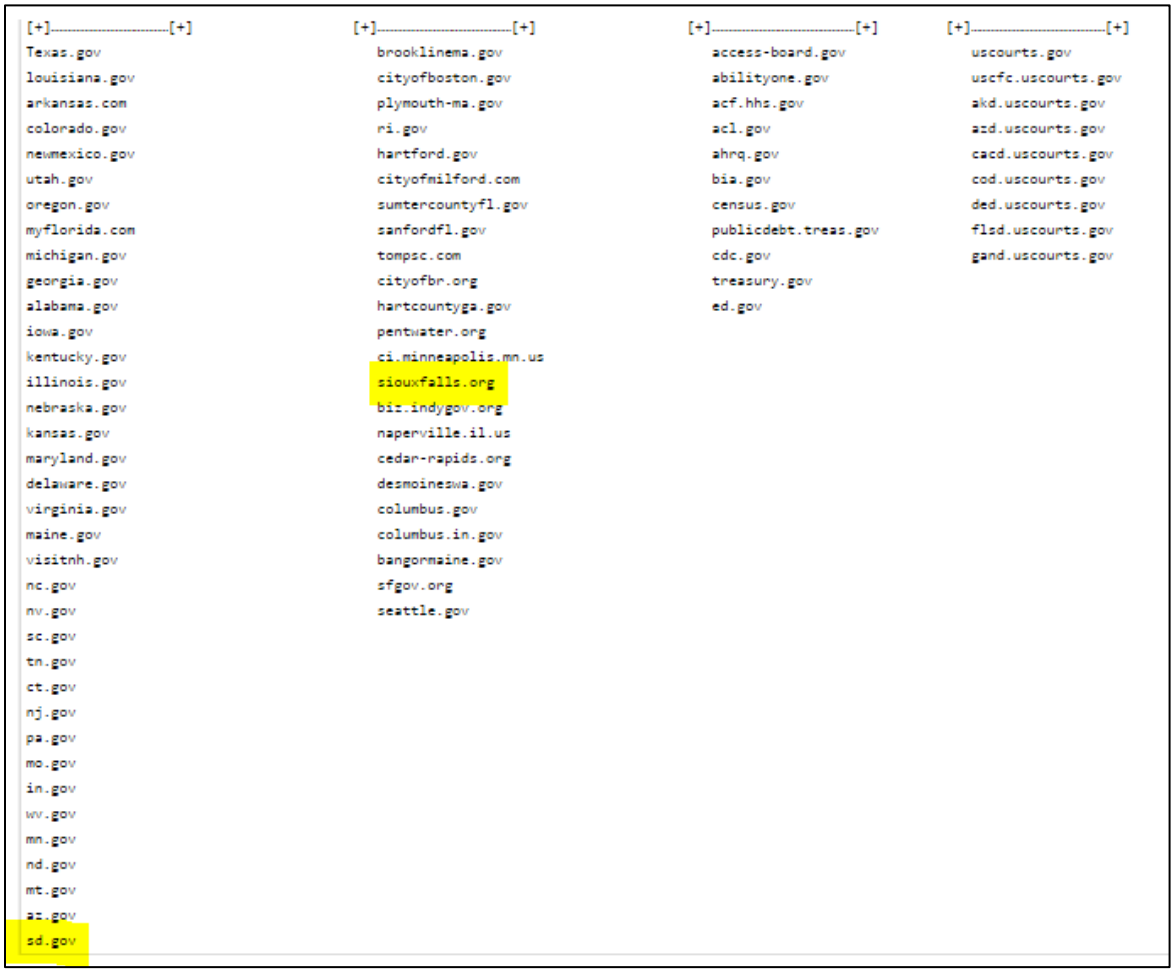


Figure 3.


[+]
Texas.gov
louisiana.gov
arkansas.com
colorado.gov
newmexico.gov
utah.gov
oregon.gov
myflorida.com
michigan.gov
georgia.gov
alabama.gov
iowa.gov
kentucky.gov
illinois.gov
nebraska.gov
kansas.gov
maryland.gov
delaware.gov
virginia.gov
maine.gov
visitnh.gov
nc.gov
nv.gov
sc.gov
tn.gov
ct.gov
nj.gov
pa.gov
mo.gov
in.gov
wv.gov
mn.gov
nd.gov
mt.gov
az.gov
sd.gov
[+]
brooklinema.gov
cityofboston.gov
plymouth-ma.gov
ri.gov
hartford.gov
cityofmilford.com
sumtercountyfl.gov
sanfordfl.gov
tompsc.com
cityofbr.org
hartcountyga.gov
pentwater.org
ci.minneapolis.mn.us
siouxfalls.org
biz.indygov.org
naperville.il.us
cedar-rapids.org
desmoineswa.gov
columbus.gov
columbus.in.gov
bangormaine.gov
sfgov.org
seattle.gov
[+]
access-board.gov
abilityone.gov
acf.hhs.gov
acl.gov
ahrq.gov
bia.gov
census.gov
publicdebt.treas.gov
cdc.gov
treasury.gov
ed.gov
[+]
uscourts.gov
uscfc.uscourts.gov
akd.uscourts.gov
azd.uscourts.gov
cacd.uscourts.gov
cod.uscourts.gov
ded.uscourts.gov
flsd.uscourts.gov
gand.uscourts.gov