Oral Statement To Congress

Posted on May 13, 2020

Oral Statement To Congress

Good morning, CEO, the congressional committee, and members of the subcommittee. I sincerely thank you for granting me this opportunity to enhance the discussion of cybercrime legislative proposals. The proposals will be helpful in combating cybercrime and protecting the security of the people of America. I would like to share some of the proposals that would be helpful in curbing cybercrimes. Congress has all the powers to focus on federal laws by enforcing resources on inter-jurisdictional threats. Congress can fix the problem of hacking by scaling the scope of CFAA's criminal liability. Particularly, I would like to thank the CEO for continued support and leadership on important issues like these.

CFAA Background

The Computer Fraud & Abuse Act (CFAA) initially aimed at protecting financial records, classified information as well as credit information on financial and government institution computers. The CFAA was amended in 1986. The intention of the Congress was to prohibit unauthorized access to government computers. However, it is good to note that as the Act was being implemented, the internet was just developing, and computer crimes were rare. All the same, the Act defined 12 key terms alongside the identification of seven criminal activities. In this case however we are only interested in few terms such as "Exceeds authorized access", "access without authorization" and "protected computer".

Developments In Computer Crime And Cyber Laws

Over the years, computer threats have increased due to the growth of computers and the availability of the Internet. Computer viruses were present in the 1990s, but nowadays, they are more familiar than ever before. Some of the attacks made by these viruses include web page defacement, DDOS, as well as ransomware. DDOS causes traffic to computers and may cause severe damage. Besides, DDOS makes online services unavailable by overwhelming them. Ransomware holds data hostage, leaving the victim with no option other than paying the ransom or restoring the data. Therefore, given the fact that technology is developing each day, there is a need to update the existing laws on matters concerning cyber threats. Employers should limit electronic access to their employees. In this case, employees, as well as contractors, should be given adequate access only to perform their duties but nothing more. CFAA should protect the employer from disabling the log-in rights of contractors or ex-employees.

Recommendations To Improve CFAA's

The purpose of CFAA is to protect computer users from hacking, unauthorized access or undesired attacks by cybercriminals. Countless people have been victims of cyber threats, and they have been left wondering which course of the law would help them. As such, CFAA needs an urgent revision. I will discuss three proposals, namely "must implement," "highly recommended," and "generally recommended."

Must Implement

One of the changes that should be made is establishing terms of service contracts since they are not CFAA automatic violations. The term of service is the legal agreement between the users and the service provider. The user is, therefore, expected to assent to the terms and conditions set by the service provider. This will be helpful, as it will define 'access without authorization' under the CFAA. Besides, it will bring balance back to CFAA through the elimination of redundant law provisions. The act defines the term as authorization in a computer as well as to use the information in accessing and obtaining information that the user is not allowed to alter or obtain. It will circumvent technological controls, such as encryptions or password requirements. Due to the broadness of the definition of the term, companies usually misinterpret it while seeking prosecution (Harrington, 2014). In this way, hacking, such as malware injection and phishing viruses, would lead to prosecution through provisions of the CFAA. This will eliminate redundant provisions by enabling individuals to be punished numerous times through duplication charges for the same violation. Through this elimination, the law will be streamlined.

Another thing that I would like to recommend is having greater proportionality to CFAA penalties. As for now, penalties for CFAA are tied to the definition of terms, giving prosecutors wide discretion. As a result, they ratchet up the severity of penalties, leaving no room for felony charges under CFAA (Harrington, 2014). Therefore, if the law is changed, prosecutors will not be able to inflate sentences through the stacking of multiple charges in CFAA. Recently, Lori Drew created a fake Facebook account. Through the account, he bullied a teenage girl, making her commit suicide. Under the CFAA, such a person should be prosecuted.

Federal resources should be prioritized toward international and national threats. It is notable that most cybercrime threats are organized internationally. Therefore, it is the work of Congress to push federal law enforcement to prioritize investigations of cyber threats. All the same, the prioritization enforcement is the duty of the Executive. However, Congress has the tools for enforcing resources toward serious risks. According to the Fourteenth and Thirteenth Amendments, congress has the power of enforcement through legislation.

Another step that can be taken is to direct investigators to deal with threats affecting businesses and consumers, such as malicious damage, fraud, and organized crimes. Despite the businesses being

aware of the cyber-crimes they are unaware of the scale of the problem. Cybercriminals use credential abuse and theft while doing their business. Since some criminals who commit crimes are in other countries, it is necessary to relocate the enforcement resources to international investigations. More so, the executive must have improvements on mutual legal assistance with other countries.

One should note that a conviction can be overturned on appeal through the Ninth Circuit's interpretation. In this case, the CFAA shows that access is not governed by written restrictions, and it only punishes hackers. To solve this Act, the terms "exceed authorized access" and "access without authorization" should be combined to mean "access without authorization."

Highly Recommended

One of the things that I would highly suggest is to change the definition of "exceeding authorized access." Currently, the definition has a chilling effect on security research. In most cases, the security researchers do violate CFAA since they routinely "exceed authorized access," terming it as part of their job. When called upon, the researchers seek out security networks in embedded devices, computers, networks, and applications. After completing their work, the researchers report the resolution to the manufacturer. For instance, there is a researcher who identified some problems associated with children's toys. However, after reporting the flaws to the manufacturer, they threatened him under CFAA. The researcher cannot do otherwise rather than drop the research. Such threats have discouraged researchers from working in the field. In such a case, the cybercriminals are continuing to exploit the security vulnerability. If the research is done responsibly, there can be a significant improvement in security. Therefore, it is good for CFAA amendment that will exempt security researchers.

There should be a strategy in such a way that everyone understands the big picture. In the industry of cybersecurity, there is fear, uncertainty, and doubt inspiring gadget-driven space. In such a way, there is anxiety while selling new services or products. As a result, this is the highest and latest solution to cyber security problems. The main problem here is that everyone is touting his or her solution. On the other hand, businesses are buying different answers from different companies; therefore, no one stands to see the big picture of whether security gaps get filled. Moreover, there is no one who checks whether anyone is working at all or how the solutions play with each other. In most organizations, there is no head coach, and it is essential to establish and understand the strategy in order to make sure it gets executed. Many businesses create infrastructures that are secure by design, forgetting to rely on bolt-on solutions like antivirus and firewalls.

Generally Recommended

The CFAA should provide a clause that prevents owners of computers from being exploited by their employees on matters concerning cybersecurity. It seems ironic, but the chances are high that

employees are the most prominent threat to a business. Although they are seldom directly involved in cybercrimes, they can be a door providing hackers with access to business information. For instance, workers may be using poor or weak passwords on their computers, allowing them to be easily accessed by hackers. In fact, a computer can be hacked within minutes if they have a weak password or network; therefore, it is good to train employees to prioritize security as their watchword. One way of achieving this is to use more complex and longer passwords (Smith, 2017). One rule to be applied in this case is including special characters, lower and uppercase letters, and extensions. This way, it is difficult for hackers to break the passwords. Similarly, passwords should not be reused on multiple accounts. In fact, organizations should hire experts to train staff on this issue.

If the above suggestions are implemented, then the business is safe and protected. All the same, it is good to be prepared for something to happen. If the hackers can detect a loophole, then there will be trouble. As a way of qualifying for an invasion, there must be an installation of intrusion detection. Such a tool will notify the user whenever there is a breach in the system. After it gets installed, every employee should monitor his or her system (Kshetri, 2015). Even if one may see himself as cyber-savvy, it is good to be on high alert for any new tricks that may be out there. It is also crucial to back up data regularly in order to ensure its safety. Moreover, one should credit reports and monitor accounts to ensure hackers are not able to access information.

If sensitive information is accessible to all employees, it is a recipe for vulnerability. It is useful to know the people who are accessing confidential information and when. According to Kerr (2016), it is difficult to know whether a business is vulnerable to attacks if there is no experience in accessing risks found in cyber security. An IT expert will cover the inappropriateness here. The work of the expert is to check potential threats and prevent them from manifesting. When a business expands, more loopholes are accessed, and an expert will use his or her expertise to mitigate damages in case there is an intrusion.

It is more comfortable for hackers to get access to data that gets transmitted to a wireless network that is not guaranteed. If a router has enabled firewalls, then it will be difficult for hackers to access the information. Moreover, it is good to change administrator passwords since cybercriminals are aware of the default passwords (Smith, 2017). Besides, it is good to have the router set up to ensure people's passwords are encrypted.

It is our wish to continue working with the committee to address the issues of cybercrimes. The evolvement of cybercrime laws is a must to enhance countering cyber threats.

Thank you for the opportunity to speak and I'm willing to take any questions.

References

Harrington, S. L. (n.d.) (2014). Cyber Security Active Defense: Playing with Fire or Sound Risk Management. Richmond Journal of Law & Technology, 20(4), 12.

Kerr, O. S. (2016). Trespass, Not Fraud: The Need for New Sentencing Guidelines in CFAA Cases. Geo. Wash. L. Rev., 84, 1544.

Kshetri, N. (2015). Recent US Cybersecurity Policy Initiatives: Challenges and Implications. Computer, 48(7), 64-69. doi:10.1109/mc.2015.188

Smith, M. (2017). *The Federal Cyber Role: How Federal Cybersecurity Policy has Affected the Public and Private Sector* (Doctoral dissertation, Utica College).