States Confront the Cyber Challenge

A Review of State Computer Crime Law
November 1st, 2016

Introduction

The term "cyber crime" is often used in reference to a wide array of criminal acts that use computers, such as child pornography, online stalking, and copyright infringement. However, cybersecurity is first and foremost concerned with computer hacking and computer fraud, which this memo refers to collectively as "computer crime." These acts involve the use of computer software to disguise one's identity, steal personal information or other data, control a computer without permission, install unauthorized software, falsify digital credentials, deface web pages, or disable electronic services.[1]

States first tackled computer crime in the late 1970s and early 1980s. The federal government followed suit in the mid-1980s with the Computer Fraud and Abuse Act (CFAA), which Congress has since amended on several occasions.[2] Today, virtually all computer crime statutes regulate one or a combination of three types of behavior: (1) using, accessing, or damaging a computer with criminal intent or for a criminal purpose; (2) using, accessing, or damaging a computer without permission; or (3) using, accessing, or damaging computerized data without permission.

Broad Statutes

Some state computer crime statutes are quite short, and use vague language that allows prosecutors to target a broad range of criminal acts. For example, prior to 1992, **Massachusetts** law only prohibited individuals from removing data from a computer; it was technically legal to corrupt or destroy computer data as long as it was not stolen.[3] In response, Massachusetts adopted the following provision:

> Whoever, without authorization, knowingly accesses a computer system by any means, or . . . knows that such access is not authorized and fails to terminate such access, shall be punished [by imprisonment or fine] . . . .[4]

Under this formulation, mere access of a computer without permission can establish criminal liability. The method of compromise and the extent of damage caused by the suspect is irrelevant to any finding of guilt. Moreover, the suspect may violate the statute even if they do not intend any harm. This provides law enforcement with flexibility to investigate and prosecute creative criminals that try to exploit gaps in the criminal code. This also reduces pressure on legislatures to revisit and amend their respective computer crime laws to keep pace with innovations by criminals. States with similarly or equally broad provisions include **West Virginia**[5] and **Wyoming**.[6]

Targeted Statutes

By contrast, other legislatures have adapted their criminal code by prohibiting specific acts. **Virginia** has conducted two comprehensive reviews of its computer crime statutes, one in 2005 and one in 2015. These studies resulted in series of changes to Virginia law:

- Creating a new felony for phishing attacks by criminalizing the use of a computer to attempt to access, steal, or create identifying information with fraudulent intent;
- Criminalizing fraudulent attempts to guess passcodes or passwords;
- Targeting botnets by criminalizing the installation of software without authorization;

Notably, in 2005 Virginia narrowed its prohibition on computer trespass (i.e., hacking) to require a showing of malicious intent—a standard that is difficult to prove. The 2015 Virginia Cyber Security Commission recommended substituting this strict formulation for the broad approach taken by states such as Massachusetts, West Virginia, and Wyoming.[7] The Virginia legislature has yet to act on this suggestion.

Other states have also amended their criminal code to reflect developments in the world of computer crime. In 2008, **Colorado** criminalized the use of a computer to interfere with online ticket sale operations. In 2011, **Texas** imposed a harsher penalty on anyone who hacks into critical infrastructure systems or government computers.[8] In 2014, **Wyoming** created the crime of computer trespass,[9] explicitly defining malware to include "viruses, worms, trojan horses, rootkits, keyloggers, backdoors, dialers, ransomware, spyware, adware, [and] malicious browser helper objects . . . ." In 2015, **New York** created a new criminal prohibition focused on denial-of-service attacks.[10] In 2016, **California** plugged a hole in its laws targeting extortion by explicitly and clearly prohibiting the use of ransomware.[11]

Washington recently has overhauled its computer crime statute, creating a new chapter of crimes based on the STRIDE threat model.[12] Like other recent updates, Washington intended to create space for security researchers and whistleblowers. The reform repealed the existing computer trespass law and created two new offenses: unauthorized access in the first degree (intending to commit another crime or access a government computer) and unauthorized access in the second degree (any other intentional, unauthorized access). In addition, the legislature enumerated four computer crimes: electronic data service interference (DDOS), spoofing, electronic data tampering, and electronic data theft.[13]

Immunity for Researchers and Third Parties

Another recent trend involves providing safe harbors for innocent entities who might accidentally run afoul of the law. In 2011, **Nevada** exempted from criminal liability persons conducting "any testing," including penetration testing, of state agency computers or networks.[14] When **Florida** created a new offense for committing computer crimes against public utilities in 2014, it immunized unwitting telecommunication companies or Internet Service Providers (ISPs) that served as a conduit for any perpetrators.[15] **Wyoming** also protects common carriers and ISPs under its computer trespass statute.[16]

In 2011, **Texas** supplied a statutory defense for any individual who obtains unauthorized access to a computer for the purpose of facilitating a legitimate law enforcement purpose. Four years later, Texas sought to strengthen the deterrent against "insider threats" by explicitly criminalizing any access of a government- or business-owned computer in violation of an express contractual prohibition. In doing so, Texas also created a new statutory defense for any individual who contracts to probe security vulnerabilities.[17]

Other Considerations

In addition to the matters described above, state officials should consider the following questions when reviewing and proposing amendments to computer crime statutes:

(1) *Definitions*: Those states that do not use broad language should carefully consider whether the definitions that govern the interpretation of their criminal statutes properly capture the range of activity that legislators want to prohibit. For example, if a state's definition of "computer" does not reflect recent innovations in digital technology, criminals might escape liability. As noted above, Wyoming has explicitly defined "malware" to include a long list of computer tools. Officials and legislators might choose to exclude simple computers, such as pocket calculators, from their computer crime statutes.

(2) *Venue*: States generally allow courts to try computer criminals in the jurisdiction where the defendant was located when they committed a computer crime, or in the jurisdiction where the victim computer resided. Some states may wish to restrict or expand the venue.

(3) *Measuring cost*: For purposes of determining criminal and civil liability, states should decide how the law values damages inflicted by computer crime. For example, **Utah** passed a 2010 clarifying that measuring the cost of computer crime should include the value of any item or service lost, the value of the use of those items or services, and the cost of replacing or restoring such items or services. [18]

(4) *Inchoate offenses* (e.g., solicitation, conspiracy, etc.): States should review whether their criminal code presently allows prosecutors to charge suspects with computer crimes that have not yet been committed. **California** recently prohibited any person from offering to commit a computer crime or soliciting another person to commit a computer crime.[19]

(5) *Predicate offenses*: A predicate offense is conduct that forms a component of a more serious crime. For example, many states have passed their own analogue to the federal Racketeer Influenced and Corrupt Organizations (RICO) Act. RICO characterizes "racketeering" as a pattern of separate, enumerated offenses. Certain states may choose to review whether their criminal code includes computer crime as an underlying component of RICO or any other similar statute.

Future Outlook

State law enforcement bodies should be aware of pending changes to procedures regulating how federal investigators search computers over the Internet. Rule 41 of the Federal Rules of Criminal Procedure currently prohibits federal officials from gaining remote access to a computer whose geographic location is unknown. Many computer criminals use special techniques to hide their geographic location, thereby making it difficult for law enforcement to obtain the search warrant they need to gather electronic evidence. As a result, federal officials want changes to Rule 41 that would permit them to search computers even if their location is unknown.[20] This reform has drawn criticism from advocates who claim it allows investigators to hack "into thousands or hundreds of thousands of computers that belong to innocent third parties and even crime victims."[21] Whether or not the federal proposal becomes law, states should carefully consider whether they wish to emulate it.

[1] COMMONWEALTH OF VIRGINIA, REPORT OF THE JOINT COMMISSION ON TECHNOLOGY AND SCIENCE 14 (2005), http://leg2.state.va.us/dls/h&sdocs.nsf/fc86c2b17a1cf388852570f9006f1299/4b6422d449faa6ec85256ec500553bbe/$FILE/RD11.pdf.

[2] S. Rep. No. 99-432, 99th Cong, 2d Sess., 1986 WL 31918, https://assets.documentcloud.org/documents/715257/ae-134-legislative-history-def-motion-dismiss.txt.

[3] Tufts Computing and Communications Services, *Computer Crime: New Massachusetts Computer Crime Law* (2001), http://emerald.tufts.edu/admin/data-warehouse/.

[4] Mass Gen. Laws ch. 266, §120F.

[5] "Any person who knowingly, willfully and without authorization, directly or indirectly, accesses or causes to be accessed a computer or computer network with the intent to obtain computer services shall be guilty of a misdemeanor, and, upon conviction thereof, shall be fined not less than two hundred dollars nor more than one thousand dollars or confined in the county jail not more than one year, or both." The law defines "computer services" as "computer access time, computer data processing or computer data storage and the computer data processed or stored in connection therewith." *Id.*

[6] "A person commits a crime against computer users if he knowingly and without authorization: (i) Accesses a computer, computer system or computer network; [or] (ii) Denies computer system services to an authorized user of the computer system services which, in whole or part, are owned by, under contract to, or operated for, on behalf of, or in conjunction with another." Wyo. Stat. Ann. § 3.6-3-504.

[7] *See* COMMONWEALTH OF VIRGINIA CYBER SECURITY COMMISSION, FIRST REPORT (2015), http://technology.virginia.gov/media/4396/cyber-commission-report-final.pdf.

[8] Tex. Pen. Code § 33.01.

[9] Wyo. Stat. Ann. § 6-3-506.

[10] N.Y. Penal Law § 156.28.

[11] Cal. Pen. Code § 523.

[12] The STRIDE system categorizes threats into five categories: (1) spoofing identity; (2) tampering with data; (3) repudiation and nonrepudiation; (4) information disclosure; (5) denial of service; and (6) elevation of privilege.

[13] Washington, Laws of 2016, Chapter 164, 64th Legislature, 2016 Regular Session, http://lawfilesext.leg.wa.gov/biennium/2015-16/Pdf/Bills/Session%20Laws/House/2375-S2.SL.pdf.

[14] Nev. Rev. Stat. § 205.4765.

[15] Fla. Stat. § 815.06(9).

[16] Wyo. Stat. Ann. § 6-3-506(c).

[17] Tex. Pen. Code § 33.01, 33.02.

[18] Utah Code § 76-6-106(4).

[19] Cal. Pen. Code § 653f.

[20] *See generally* RICHARD M. THOMPSON II, DIGITAL SEARCHES AND SEIZURES: OVERVIEW OF PROPOSED AMENDMENTS TO RULE 41 OF THE RULES OF CRIMINAL PROCEDURE (2016), https://www.fas.org/sgp/crs/misc/R44547.pdf.

[21] *See, e.g.*, Ron Wyden, Matt Blaze, & Susan Landau, "The Feds Will Soon Be Able to Legally Hack Almost Anyone," WIRED, September 14, 2016, https://www.wired.com/2016/09/government-will-soon-able-legally-hack-anyone/.