Laws and Cybersecurity

Instructor: Cyber or computer crime is a form of crime where the Internet and/or devices are used as a medium to commit a crime, serve as a target of crime, or are incidental to the crime. These types of crimes include fraud, sabotage, theft, and/or vandalism.

While there are regulations aimed at safeguarding information systems and their data from vulnerabilities of attack and intrusion, laws for criminal cyber activity can vary depending upon the state and the offense.

In the U.S. the federal Computer Fraud and Abuse Act, CFAA, is a mechanism for prosecuting cybercrime with penalties including civil and incarceration. The act prohibits a range of unauthorized access actions, such as intent to damage, defraud or obtain information to government or other protected systems. It also prohibits trafficking passwords and extortion.

Cyberattacks such as hacking, denial of service, phishing and malware infections fall under the CFAA. The CFAA is a federal law, but individual states also have laws that apply to specific areas of cybercrime.

There are laws protecting electronic communications that may also include penalties and imprisonment. The Electronic Communications

Protection Act, ECPA, relates to communications in storage and transit. Title 1 of the ECPA is the Wiretap Act which prohibits unauthorized interception of electronic communications. Title 2, the Stored Communications Act, makes unauthorized access to facilities that provide electronic communications, such as an email service provider, illegal.

Also related to email is the Controlling the Assault of Non-Solicited Pornography and Marketing Act, or CAN-SPAM. Marketing via email must strictly adhere to requirements such as honesty of emails' intent, their source, and that opting out of future emails is easily and quickly obliged.

Organizations who do not implement cybersecurity measures may also be subject to criminal violations. Regulated entities such as health and finance could suffer civil penalties in the event of a cyber breach if security controls and secure configuration guidance were not applied.

Many industry regulations protect privacy. The Privacy Act of 1974 is a federal law to govern information about individuals - personally identifiable information - that is collected, stored, used, or disseminated.

Some widely applicable regulations include:

The Health Insurance Portability and Accountability Act (HIPAA) establishes regulations for the use and disclosure of Protected Heath Information. Entities who work with customer health information are required to be HIPAA-compliant. Specifically, confidentiality of Protected Health Information (PHI) must be ensured in all its forms paper, electronic, or oral and be accessed or shared as minimally as possible.

The Gramm-Leach-Bliley Act, also known as the Financial Modernization Act of 1999, requires financial institutions to safeguard sensitive customer data and detail their information-sharing practices as well as give customers the right to opt out of sharing with third parties.

The Sarbanes-Oxley Act, sometimes also referred to by other accounting-related names, is a federal law meant to improve corporate governance and accountability. Companies must comply with SOX on both finance and technology as far as storage of records.

The Payment Card Industry Data Security Standard, PCI DSS, are security requirements that every company that works with or stores credit card information must follow. Compliance for the payment card ecosystem helps protect customers, retailers, and banks from data theft.

Besides industry regulations established to protect the privacy and integrity of consumer data, other

common protections also apply to cyberspace. For instance, there are intellectual property rights that protect creative and original works. The World Intellectual Property Organization is a global forum agency of the United Nations that leads the charge in intellectual property (IP) guidelines for:

Licensing and software licenses, which details the ability to transfer rights to use copyrighted work. All applications are going to include details for rights of use. Commercial software will include an End User License Agreement, EULA, detailing the cost and parameters for use. Shareware, trialware, or demoware is proprietary software that users may use for a set duration of time and usually with limited functionality. Freeware is available for use at no cost, but the manufacturer retains the rights to application and will still include an EULA.

Piracy, the copyright infringement of software, is punishable by legal actions. Piracy includes making a copy of a licensed product, abuse of agreement, and obtaining software fraudulently. As a software vendor, it's important to note that laws vary internationally and copyright protections may not be enforced in other countries. As an organization that licenses software for business use, maintaining a tracking management system is vital to stay within use guidelines and/or not lose productivity due to expiration.

This relates to due care and due diligence, generally accepted business and information security practices as well as regulatory requirements that must be followed to protect the company information and information assets. Negligence, on the other hand, could incur criminal and/or civil penalties, if for instance a data breach occurred and it was found a company did not reasonably follow security best practices.

Liability for negligence can also be passed through to an organization. If an attacker exploits a service through a vulnerability that a patch isn't available for yet, the company hosting the service could shoulder that liability. The same could hold true with downstream providers if for instance a third-party cloud provider didn't adequately protect the organizations data.

Laws and regulations are adapting as the types and varying circumstances of cybercrimes evolve. Protecting the confidentially, integrity, and availability of information and information systems is at the forefront. This data is very valuable to bad actors with ill intent of theft, fraud, or extortion. Laws and regulations ensure organizations prioritize security measures and are compliant with rules for safeguarding sensitive information.

Notices

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

DM18-0098