

City University of New York (CUNY)

CUNY Academic Works

Open Educational Resources

Hostos Community College

2020

Cybersecurity-Cybercrime-The Legal Environment

Amy J. Ramson

CUNY Hostos Community College

[How does access to this work benefit you? Let us know!](#)

More information about this work at: https://academicworks.cuny.edu/ho_oers/5

Discover additional works at: <https://academicworks.cuny.edu>

This work is made publicly available by the City University of New York (CUNY).

Contact: AcademicWorks@cuny.edu

Cybersecurity: Cybercrime-The Legal Environment

- 1-Challenge of cybercrime to criminal justice system
- 2-Industry and law enforcement dilemma
- 3-Cybersecurity Act of 2015-industry protected from liability for sharing cyber breach data
- 2-Federal government investigates and prosecutes-specific departments and agencies
- 3-Federal criminal statutes
- 4-NYS criminal statutes
- 5-Federal civil statute
- 6-State civil statute
- 7-Federal privacy statutes
- 8-NYS privacy statute

Professor Amy Ramson

This OER material was produced as a result of the PIT-UN network Challenge Grant – New America

Creative Commons License



This work is licensed under a

[Creative Commons Attribution-Noncommercial-Share Alike 4.0 License](https://creativecommons.org/licenses/by-nc-sa/4.0/)

Cybercrime-GROUPS OF CRIMES

- ◆ **DISTRIBUTION OF ILLEGAL GOODS**
- ◆ **THEFT, IDENTITY THEFT AND FRAUD**
- ◆ **CORPORATE ESPIONAGE**
- ◆ **Bullying and stalking**

Cybercrime presents a huge challenge to the criminal justice system

- ◆ There is a huge gap in the enforcement of cybercrimes;
- ◆ Most cyber criminals are not prosecuted;
- ◆ Cybercrime is a new category of crime which presents challenges for the justice system and the law enforcement community;
- ◆ It is growing tremendously quickly with new schemes being created daily;
- ◆ Traditional law enforcement methods can not detect it; and
- ◆ New technical skills must be developed to cope with the skills of the criminal

Catching the Cybercriminal: Reforming Global Law Enforcement-Video

Participants included high-level cyber experts, policymakers, and media speaking about the needs and capabilities of US and international law enforcement and diplomats to address cybercrime digital evidence

https://www.youtube.com/watch?v=Is11s4WhnNE&feature=youtu.be&list=PLJkLD_s9pYaby-ce9kwXeFeODoBae408t

Balancing Law Enforcement and Industry needs

- ◆ Due to the nature of technology and the difficulties of investigating and prosecuting cyber criminals, it had fallen to industry to police themselves
- ◆ Many manufacturers decline to reveal breaches and further decline to fix security risks they are aware of for fear of harming their profits and/or increasing the difficulties in the use of their products and continue to allow potential security breaches to remain even after being notified of hacking
- ◆ In response, President Obama, enacted the Cybersecurity Act of 2015 which creates a framework designed to facilitate and encourage confidential sharing of information concerning cyber-threats between the federal government and the private sector



Cybersecurity Act of 2015

- ◆ **In general:**
 - Encourages industry by granting them liability protection to provide cyber threat information to the government and authorizes DHS as the hub to share that information with other entities to investigate and prosecute cybercrime
- ◆ Creates a framework to facilitate and encourage confidential sharing of cyber-threats between the federal government and the private sector.
- ◆ Establishes a portal at the DHS and its National Cybersecurity & Communications Integration Center (NCCIC) to facilitate private-public cyber-threat information sharing
- ◆ Authorizes DHS to set up an automated system for real-time onward sharing to the rest of the government. Personal information must first be removed

Federal government investigates and prosecutes most cybercrime

There are a multitude of Federal departments, agencies and commissions involved with cybercrimes and cyber terrorism


This has led to overlapping responsibilities and no unified :plan for enforcement

The most significant are:

- Department of Justice. The FBI is the agency most involved with investigating cybercrime and terrorism
 - Department of Homeland Security
 - Federal Trade Commission
- Details about the above departments and agencies follow and some information about the other departments and agencies involved at a lesser level follow after



State enforcement barriers

- ◆ The global nature of cybercrime
 - ◆ Difficulty and lack of resources to track cybercrime
 - ◆ Jurisdiction-the power to administer justice over a controversy
 - ◆ Lack of unified set of laws addressing cybercrimes
- 

U.S. Department of Justice

Prosecutes cybercrime through:

Criminal Division, National Security Division, and Office of the United States Attorneys

Investigates through following agencies:

◆ **The FBI-AGENCY**

<https://www.fbi.gov/investigate/cyber>

- The FBI is the principal agency that investigates attacks by criminals, overseas adversaries, and terrorists.
- It has 60 cyber squads that work together with other federal, state, local, and private-sector agencies

U.S. Department of Justice

Has created special sections for cybercrime investigation and prosecution. Two such sections are:

- **The Computer Crime and Intellectual Property Section (CCIPS)** combats computer and intellectual property crimes worldwide. CCIPS prevents, investigates, and prosecutes computer crimes by working with other government agencies, the private sector, academic institutions, and foreign counterparts
- **The Child Exploitation and Obscenity Section (CEOS)** enforces federal child exploitation laws and works to prevent the exploitation of children, including online child pornography

Independent Agencies

- ◆ **Federal Trade Commission (FTC)**

Criminal Liaison Unit

- ◆ **Securities and Exchange Commission (SEC)**

Enforcement Division

Cyber Unit


Department of Homeland Security

- ◆ US Secret Service
- ◆ US Immigration and Customs Enforcement
- ◆ National Cybersecurity and Communications Integration Center (NCCIC)

CISA Cyber security and Infrastructure Agency **was created to address this issue in 2018**

- ◆ Is responsible for protecting the Nation's critical infrastructure from physical and cyber threats
- ◆ This mission requires effective coordination and collaboration among a broad spectrum of government and private sector organizations

CISA Cyber security and Infrastructure Agency

- ◆ Cybercrime threatens critical infrastructures, such as power grids or water supplies. Any object that uses electric power (street lights, banking systems, transportation) would be affected
 - ◆ **CISA was created to address this issue in 2018**
 - ◆ Is responsible for protecting the Nation's critical infrastructure from physical and cyber threats
 - ◆ This mission requires effective coordination and collaboration among a broad spectrum of government and private sector organizations
- 

Cyber security and Infrastructure Agency



Comprehensive Cyber Protection

CISA's National Cybersecurity and Communications Integration Center (NCCIC) provides 24x7 cyber situational awareness, analysis, incident response and cyber defense capabilities to the Federal government; state, local, tribal and territorial governments; the private sector and international partners.

CISA provides cybersecurity tools, incident response services, and assessment capabilities to safeguard the networks that support the essential operations of federal civilian departments and agencies.



Infrastructure Resilience

CISA coordinates security and resilience efforts using trusted partnerships across the private and public sectors, and delivers training, technical assistance, and assessments to federal stakeholders as well as to infrastructure owners and operators nationwide.

CISA provides consolidated all-hazards risk analysis for U.S. critical infrastructure through the National Risk Management Center.



Emergency Communications

CISA enhances public safety interoperable communications at all levels of government, providing training, coordination, tools and guidance to help partners across the country develop their emergency communications capabilities.

Working with stakeholders across the country, CISA conducts extensive, nationwide outreach to support and promote the ability of emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters.



National Risk Management Center

The NRMC is a planning, analysis, and collaboration center working to identify and address the most significant risks to our nation's critical infrastructure.

The NRMC works in close coordination with the private sector and other key stakeholders in the critical infrastructure community to: Identify; Analyze; Prioritize; and Manage the most strategic risks to our National Critical Functions.

Other Departments

Defense Department

THE NSA-AGENCY

- ◆ The National Security Agency (NSA) intercepts signals intelligence and decrypting physical and cyber threats

Department of State

- ◆ Bureau of International Narcotics and Law Enforcement (INL)
- ◆ United States Agency for International Development (USAID)

Treasury Department

- ◆ Office of Terrorism and Financial Intelligence
- ◆ Internal Revenue Services (IRS)
 - Criminal Investigation (CI)

The Commerce Department

- ◆ **The National Institutional Standards and Technology Act** gives the the Secretary of commerce power to develop new methods of cybersecurity that follow industry-led standards, guidelines, best practices, etc



Where to submit complaints: IC3

- ◆ The Internet Crime Complaint Center (IC3) is a partnership between the Federal Bureau of Investigation (FBI), the National White Collar Crime Center (NW3C), and the Bureau of Justice Assistance (BJA)
- ◆ Receives Internet-related criminal complaints and refers the complaints to federal, state, local, or international law enforcement and/or regulatory agencies

Reporting cybercrime-IC3

- ◆ The Internet Crime Complaint Center (IC3) is a partnership between the FBI, the National White Collar Crime Center (NW3C), and the Bureau of Justice Assistance (BJA)
- ◆ The mission of the IC3 is to provide the public with a reporting mechanism to submit information to the FBI concerning suspected Internet-facilitated criminal activity, and to develop alliances with industry
- ◆ Information is analyzed and distributed for investigative and intelligence purposes, for law enforcement, and for the public awareness
- ◆ This is the 2019 IC3 report

https://pdf.ic3.gov/2019_IC3Report.pdf

STATUTES

FEDERAL CRIMINAL LAWS

A stylized silhouette of a mountain range in a darker shade of teal, located in the bottom right corner of the slide.

Federal Wire Fraud Statute

- ◆ Prohibits the use of interstate wire communications to further a fraudulent scheme to obtain money or property
- ◆ Federal wire fraud statute applies to computer crimes

Appendix A

Unlawful Online Conduct and Applicable Federal Laws

The chart below details the type of unlawful online conduct, potentially applicable federal laws, and the section of the Department of Justice with subject-matter expertise. If the subject matter expert is not a component of the Department, but rather another agency, the entry will have an asterisk preceding its initials.

In many cases, prosecutors may also consider whether the conduct at issue is a violation of 18 U.S.C. § 2 (aiding and abetting) or 18 U.S.C. § 371 (conspiracy).

Unlawful Conduct	Applicable Federal Law	DOJ Section
Denial of Service Attacks	18 U.S.C. § 1030(a)(5)(A) (transmission of program, information, code, or command, resulting in damage)	CCIPS
	18 U.S.C. § 1362 (interfering with government communication systems)	CCIPS
Substitution or Redirection of a website	18 U.S.C. § 1030(a)(5)(A) (i) (transmission of program, information, code, or command, resulting in damage)	CCIPS
	18 U.S.C. § 1030(a)(5)(A)(ii)-(iii) (accessing a computer without authorization, resulting in damage)	CCIPS
Use of Misleading Domain Name	18 U.S.C. § 2252B (using misleading domain name with intent to deceive a person into viewing obscene material or with intent to deceive a minor into viewing harmful material)	CEOS

Unlawful Conduct	Applicable Federal Law	DOJ Section
Extortion	18 U.S.C. § 1030(a)(7) (transmitting, with intent to extort, communication containing threat to cause damage)	CCIPS
	18 U.S.C. § 875(b), (d) (transmitting, with intent to extort, threat to kidnap or harm a person, or threat to injure a person's property or harm a reputation) (Hobbs Act)	CTS
	18 U.S.C. § 1951 (interfering with commerce by robbery, extortion, threats or violence)	DSS
Internet Fraud (e.g., auction fraud or "phishing")	18 U.S.C. § 1030(a)(4) (accessing a computer to defraud and obtain something of value)	CCIPS
	18 U.S.C. § 1028 (fraud in connection with identification documents and authentication features)	Fraud
	18 U.S.C. § 1028A (aggravated identity theft)	Fraud
	18 U.S.C. § 1343 (wire fraud)	Fraud
	18 U.S.C. §§ 1956, 1957 (money laundering)	AFMLS
	18 U.S.C. § 1001 (making false statements in any matter within the jurisdiction of the government)	Fraud
	15 U.S.C. § 45 (unfair or deceptive trade practices)	*FTC
	15 U.S.C. § 52 (false advertising)	*FTC
15 U.S.C. § 6821 (fraudulent access to financial information)	*FTC/Fraud	

Unlawful Conduct	Applicable Federal Law	DOJ Section
Credit Card Fraud	18 U.S.C. § 1030(a)(2)(A) (accessing a computer and obtaining information from a financial institution, card issuer or consumer reporting agency)	CCIPS
	18 U.S.C. § 1029 (access device fraud)	Fraud/CCIPS
	15 U.S.C. § 1644 (credit card fraud aggregating at least \$1,000)	Fraud
	18 U.S.C. § 1343 (wire fraud)	Fraud
Password Fraud	18 U.S.C. § 1030(a)(6) (trafficking in computer passwords)	CCIPS
	18 U.S.C. § 1029 (access device fraud)	Fraud/CCIPS
	18 U.S.C. § 1343 (wire fraud)	Fraud
Child Pornography, Child Luring, and Related Activities	18 U.S.C. §§ 2251, 2252, 2252A (sexual exploitation of children)	CEOS
	18 U.S.C. § 2423 (transportation of minors or travel with intent to engage in illicit sexual conduct)	CEOS
	18 U.S.C. § 1466A (obscene visual representations of the sexual abuse of children)	CEOS
Obscenity	47 U.S.C. § 223(a)(1)(A) (using telecommunications device to make, create, or solicit, and transmit any obscene comment, request, suggestion, proposal, image, or other communication)	CEOS
	18 U.S.C. § 1465 (using interactive computer service for purpose of sale or distribution of obscene material)	CEOS

Unlawful Conduct	Applicable Federal Law	DOJ Section
Sale of Prescription Drugs and Controlled Substances	15 U.S.C. § 45 (unfair or deceptive trade practices)	*FTC
	15 U.S.C. § 52 (false advertising)	*FTC
	18 U.S.C. § 545 (smuggling goods into the United States)	Fraud/AFMLS
	18 U.S.C. § 1343 (wire fraud)	Fraud
	21 U.S.C. §§ 301 et seq. (Federal Food, Drug, and Cosmetic Act)	*FDA
	21 U.S.C. §§ 822, 829, 841, 863, 951-71 (Drug Abuse Prevention and Control)	Fraud/NDDS
	18 U.S.C. § 2320 (trafficking in counterfeit goods or services)	CCIPS
Sale of Firearms	18 U.S.C. § 922 (unlawful sale of firearms)	DSS
Gambling	15 U.S.C. §§ 3001 et seq. (Interstate Horseracing Act)	OCRS
	18 U.S.C. § 1084 (use of wire communication facility to transmit bets or wagering information)	OCRS
	18 U.S.C. § 1301 (importing or transporting lottery tickets)	OCRS/AFMLS
	18 U.S.C. § 1952 (use of facilities in interstate or foreign commerce to aid in racketeering enterprises)	OCRS
	18 U.S.C. § 1953 (interstate transportation of wagering paraphernalia)	OCRS
	18 U.S.C. § 1955 (conducting, financing, managing, supervising, directing, or owning an illegal gambling business)	OCRS/AFMLS
	28 U.S.C. § 3701 et seq. (Professional and Amateur Sports Protection Act)	OCRS/AFMLS

Unlawful Conduct	Applicable Federal Law	DOJ Section
Sale of Alcohol	18 U.S.C. §§ 1261 et seq. (transportation of liquor into state prohibiting sale; shipping liquor without required marks and labels on package)	OCRS/*Treasury
	27 U.S.C. §§ 122, 204 (interstate shipping of alcohol)	OCRS/*Treasury
Securities Fraud	15 U.S.C. §§ 77e, 77j, 77q, 77x, 78i, 78j, 78l, 78o, 78ff (securities fraud)	Fraud/*SEC
	18 U.S.C. § 1343 (wire fraud)	Fraud/CCIPS
Piracy and Intellectual Property Theft	17 U.S.C. §§ 1201-1205 (Digital Millennium Copyright Act)	CCIPS
	18 U.S.C. § 545 (smuggling goods into the United States)	AFMLS
	18 U.S.C. §§ 1831, 1832 (theft of trade secrets)	CES/CCIPS
	18 U.S.C. § 2318 (trafficking in counterfeit labels)	CCIPS
	17 U.S.C. § 506 and 18 U.S.C. § 2319 (criminal copyright infringement)	CCIPS
	18 U.S.C. § 2319A (trafficking in recordings of live musical performances)	CCIPS
	18 U.S.C. § 2320 (trafficking in counterfeit goods or services)	CCIPS
	47 U.S.C. § 553 (unauthorized reception of cable service)	Fraud
Trade Secrets/ Economic Espionage	18 U.S.C. § 1831 (theft of trade secrets for benefit of foreign government)	CES/CCIPS
	18 U.S.C. § 1832 (theft of trade secrets)	CCIPS
	18 U.S.C. § 1905 (disclosure of confidential information)	Public Integrity
	18 U.S.C. §§ 2314, 2315 (interstate transportation or receipt of stolen property)	OEO

Unlawful Conduct	Applicable Federal Law	DOJ Section
Electronic Threats	18 U.S.C. § 875 (transmitting communications containing threats of kidnap or bodily injury) (Hobbs Act)	CTS
	18 U.S.C. § 1951 (interfering with commerce by robbery, extortion, threats or violence) (Hobbs Act)	DSS
	47 U.S.C. § 223 (a)(1) (C) (anonymously using telecommunications device to threaten person who receives communication)	CCIPS
Electronic Harassment	47 U.S.C. § 223 (a)(1) (C) (anonymously using telecommunications device to harass person who receives communication)	CCIPS
	47 U.S.C. § 223(a)(1)(E) (repeatedly initiates communication with a telecommunication device solely to harass person who receives communication)	CCIPS
Interception of Electronic Communications	18 U.S.C. § 2511 (intercepting electronic communications)	CCIPS
	18 U.S.C. § 2701 (accessing stored communications)	CCIPS
	18 U.S.C. § 1030(a)(2) (accessing a computer and obtaining information)	CCIPS
Cyberstalking	18 U.S.C. § 2261A (using any facility of interstate or foreign commerce to engage in a course of conduct that places person in reasonable fear of death or serious bodily injury to person, person's spouse or immediate family) See also <i>Electronic Harassment</i>	DSS

Unlawful Conduct	Applicable Federal Law	DOJ Section
Espionage	18 U.S.C. § 1030(a)(1) (accessing a computer and obtaining national security information)	CES
	18 U.S.C. § 1030(a)(2) (accessing a computer and obtaining information from any department or agency of the United States)	CCIPS
	18 U.S.C. § 1030(a)(3) (accessing a nonpublic United States government computer)	CCIPS
	18 U.S.C. § 793 (gathering, transmitting or losing defense information)	CES
	18 U.S.C. § 798 (disclosing classified information)	CES
Hate Crimes	Look to civil rights laws and penalty enhancements	Civil Rights
Libel/Slander	Look to civil laws	
Posting Personal Information on a Website (e.g., phone numbers, addresses)	This is not a violation of law. May also be protected speech under First Amendment.	
Invasion of Privacy	See <i>Interception of Electronic Communications</i>	
Disclosure of Private Information	18 U.S.C. § 2511(1)(c) (disclosing intercepted communications)	CCIPS
Spam	18 U.S.C. § 1037 (CAN-SPAM Act)	CCIPS
Spoofing Email Address	18 U.S.C. § 1037 (CAN-SPAM Act)	CCIPS

Computer Fraud & Abuse Act

- ◆ Passed in 1986, the Computer Fraud and Abuse Act (CFAA) is designed to reduce cracking and hacking of computer systems and to address federal computer-related offenses

CFFA

Seven types of criminal activity :

- ◆ 1.obtaining national security information,
- ◆ 2.compromising confidentiality,
- ◆ 3.trespassing in a government computer,
- ◆ 4.accessing to defraud and obtain value,
- ◆ 5.damaging a computer or information,
- ◆ 6.trafficking in passwords,
- ◆ 7. threatening to damage a computer.
- ◆ A violation of the CFAA can be committed in two ways:
 - ◆ 1.By an outsider who trespasses into a computer or
 - ◆ 2.By an intruder who goes beyond the scope of his given authorization.

The Federal Economic Espionage Act of 1996

EEA, [18 U.S.C. §§ 1831-1839](#),

Economic espionage: Criminalizes the misappropriation of trade secrets (including conspiracy to misappropriate trade secrets and the subsequent acquisition of such misappropriated trade secrets) with the knowledge or intent that the theft will benefit a foreign power.

Foreign espionage performed to benefit a foreign government

- ◆ *Theft of trade secrets*: Criminalizes the misappropriation of trade secrets related to or included in a product that is produced for or placed in interstate (including international) commerce, with the knowledge or intent that the misappropriation will injure the owner of the trade secret

Commercial theft regardless of beneficiary

Federal Civil Remedy Defend Trade Secrets Act (“DTSA”)

- ◆ The DTSA (18 USC §§ 1836 et seq.) signed into law in 2016 creates a federal, private cause of action for trade-secret protection
- ◆ The DTSA provides a uniform statutory scheme to be applied in federal court; it does not pre-empt state law
- ◆ Before the DTSA trade secret owners seeking damages or injunctions for stealing a trade secret could only sue in state court.
- ◆ Emergency injunctions are necessary to halt the secret from being made public or being used for another’s benefit

State Civil Remedy (NY did not enact)

Uniform Trade Secret Act has been enacted into law by 48 states

STATUTES

NYS CRIMINAL STATUTES

A stylized silhouette of a mountain range in a darker shade of teal, located in the bottom right corner of the slide.

New York Criminal Laws- computer crimes

NY PENAL LAW s 190.77-83:

Offenses involving theft of identity

NY PENAL LAW Article 156

Computer Crimes

STATUTES

**FEDERAL PRIVACY
PROTECTION LAWS**

A stylized, layered mountain range graphic in shades of teal and blue, located in the bottom right corner of the slide.

Protection of Privacy

- ◆ Most important privacy legislation is on the federal level of government
- ◆ Some States have privacy laws
- ◆ The laws protect all consumers, medical information and the most vulnerable-children and the elderly

Federal: Electronic Communications Privacy Act

- ◆ The Electronic Communications Privacy Act and the Stored Wire Electronic Communications Act are commonly referred together as the Electronic Communications Privacy Act (ECPA) of 1986. The ECPA updated the Federal Wiretap Act of 1968, which addressed interception of conversations using "hard" telephone lines, but did not apply to interception of computer and other digital and electronic communications.
- ◆ The [USA PATRIOT Act](#), clarify and update the ECPA to keep pace with the evolution of new communications technologies and methods but have eased restrictions on law enforcement access to stored communications in some cases
- ◆ [Carpenter v. United States](#): Law enforcement needs a warrant to search and seizure cell phone records, which include the location and movements of cell phone users

ECPA

- ◆ Protects wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers.
- ◆ Applies to email, telephone conversations, and data stored electronically

Federal Privacy: The Health Insurance Portability and Accountability Act

- ◆ The United States has comprehensive federal health privacy legislation, with the key legislation being the Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- ◆ HIPAA mandates the creation and distribution of privacy policies that explain how all individually identifiable health information is collected, used, and shared, and establishes strict controls on how that information is used and disclosed

Federal Privacy: Children

The 1998 Children's Online Privacy Protection Act (COPPA)

Its goals are:

- ◆ to enhance parental involvement in order to protect the privacy of children in the online environment;
- ◆ to help protect the safety of children in online forums
- ◆ to limit the collection of personal information from children without parental consent

Federal Elder Abuse Prevention and Prosecution Act of 2017

Several federal agencies currently collect elder abuse data (including physical abuse, neglect, and financial exploitation) on an ongoing basis at different points in the process. This page provides snapshots of elder abuse through the lens of three distinct federal data sets:

- ◆ [National Adult Mistreatment Report System \(NAMRS\)](#) collects state-level adult protective services data
- ◆ [National Incident-Based Reporting System \(NIBRS\)](#) collects state-level law enforcement data
- ◆ [FTC Consumer Sentinel Network](#) collects consumer complaints from multiple sources
- ◆ [Financial Crimes Enforcement Network \(FinCEN\)](#) collects data on suspected elder financial exploitation submitted by financial institutions

STATUTES

NYS PRIVACY STATUTES

A stylized silhouette of a mountain range in shades of teal, located in the bottom right corner of the slide.

NYS Shield Act

- ◆ On March 21, 2020, the data security provisions of New York's Stop Hacks and Improve Electronic Data Security Act ("SHIELD Act") went into effect.
- ◆ The SHIELD Act requires any person or business owning or licensing computerized data that includes the private information of a resident of New York to implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information

NYS SHIELD Act

1-Tightens the requirements for providing data breach notifications

2-imposes a new requirement on entities possessing private information associated with New York residents to implement “reasonable” security measures to protect that information

3-Provides penalties for non-compliance

4- Requires that there be a designated employee for cybersecurity at entity

Penalties

- ◆ Enforcement of law is handled by the NY Attorney General's office
- ◆ Potential penalties for an entity that violates the SHIELD Act:
 - For data holders who fail to notify their employees or customers of a data breach, monetary relief may be awarded
 - If New York residents do not receive data breach disclosure notices, courts can award those residents monetary damages for actual costs or financial losses they incur as a result of the breach