EMPLOYMENT WEB SERIES

“Cybersecurity in the Workplace”

How to Strengthen and Protect Your Business in an Era of Easy Computer System Access

HINSHAW

Meet Today's Presenters

Ambrose McCall advises businesses on a range of employment issues, including regulatory, compliance and employee program matters; he also counsels employers on employee social media and digital workplace policies.

Ken Yeadon uses his experience as a former Assistant U.S. Attorney and SEC Enforcement Attorney to provide defense, representation, and advice to individuals and corporations on criminal, securities, health care, and civil regulatory matters.

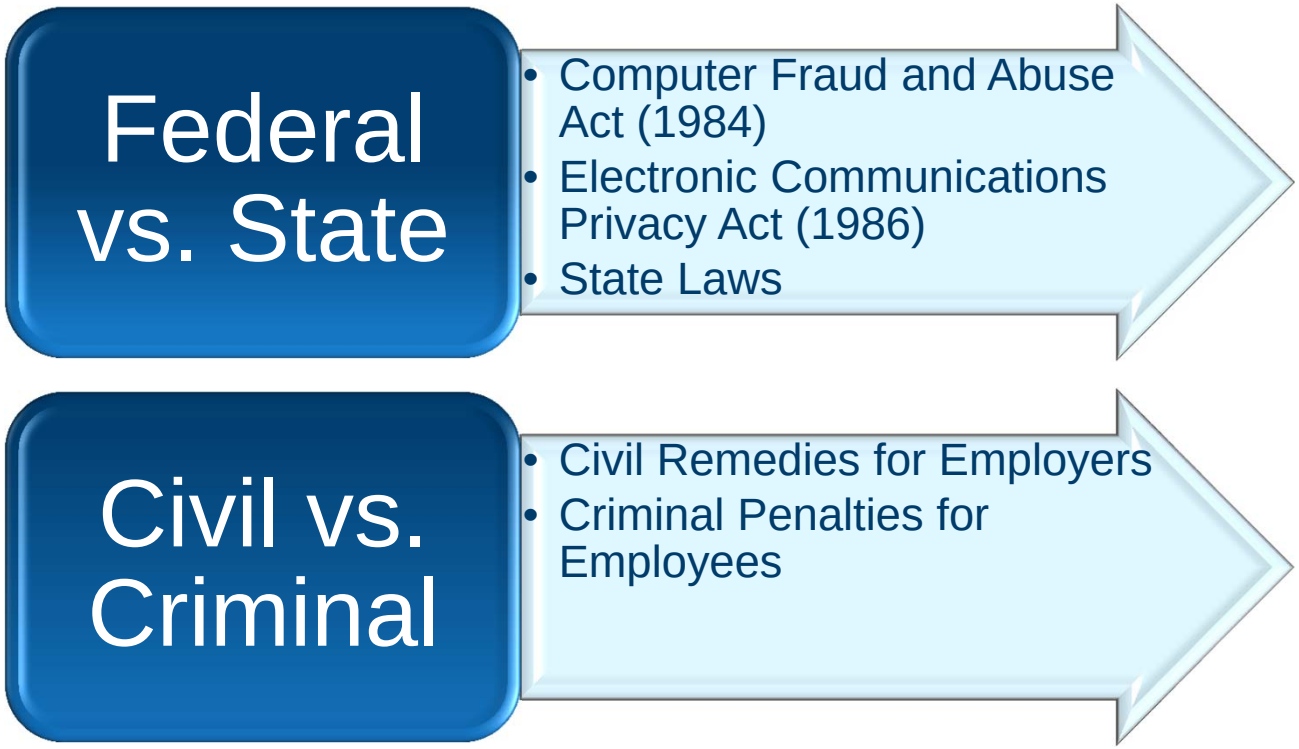
Cybersecurity in the Workplace: Learning Objectives

1. Review relevant law that promotes cybersecurity and protects businesses
2. Demonstrate cybercrime and potential recourses through case studies
3. Best practices that promote cybersecurity and protect your business

Recent Examples

- Andrew Auernheimer – exploited vulnerability in AT&T website to obtain email addresses of AT&T iPad users
- Matthew Keys – disgruntled employee gave log-on info to hacker, who used info to alter an LA Times news story
- David Nosal – talked former colleagues into accessing their company's database to give him trade secrets to launch a competing company

Cybersecurity Overview



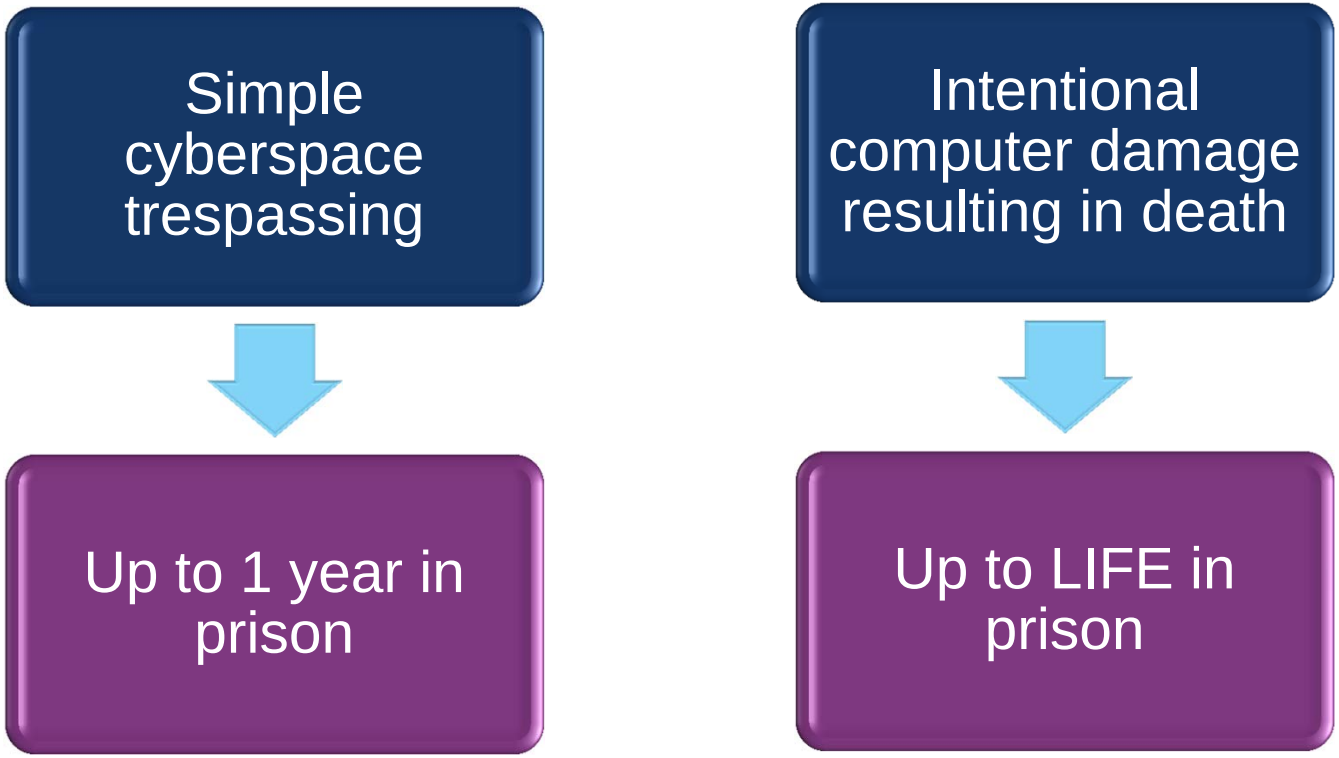
The Computer Fraud and Abuse Act: A Criminal Statute

- Fraud involving unauthorized access to a Gov't computer, a bank computer, or a computer used in, or affecting, interstate or foreign commerce, to further a fraud (must be >$5K & not just to access the computer)
- Threatening to damage a Gov't computer, a bank computer, or a computer used in, or affecting, interstate or foreign commerce
- Trafficking in passwords for a Gov't computer, or when the trafficking affects interstate or foreign commerce
- Computer trespassing (hacking) in a Gov't computer
- Computer trespassing (hacking) resulting in exposure to certain Gov't, credit, financial, or computer-housed information
- Damaging a Gov't computer, a bank computer, or a computer used in, or affecting, interstate or foreign commerce (a worm, computer virus, Trojan horse, time bomb, denial of service attack, and other forms of cyberattack, cybercrime, or cyber terrorism)
- Accessing a computer to commit espionage

Cybercrime and the CFAA

- The CFAA outlaws conduct that victimizes computer systems
  - Protects federal computers, financial institution computers, and computers connected to the Internet (interstate commerce)
  - Shields these types of computers from trespass, threats, damage, espionage, and use as corrupt instruments of fraud

Criminal Penalties under the CFAA

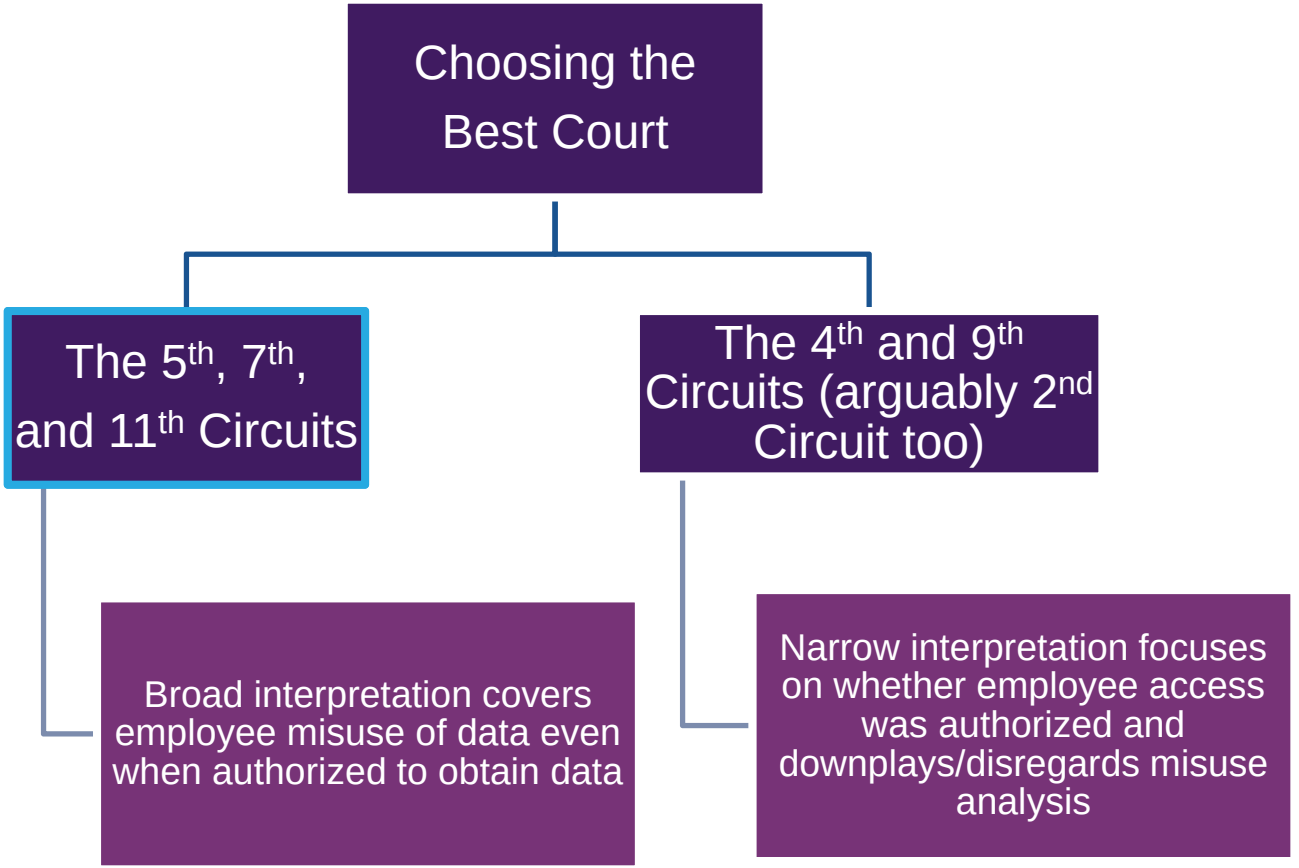


The Computer Fraud and Abuse Act: Key Terms

"Protected Computer"	"Exceeds Authorized Access"	"Without Authorization"
• Workplace computer • Used in/affects interstate or foreign commerce or communication of the U.S.	• Access without authorization • Using unauthorized access to obtain or alter information • (Supreme Court passes)	• Access of a "protected computer" without express permission

More on “Protected Computer”

The Divide over “Authorized Access”



Key Terms (Continued)

- "Damage" is harm to data and information and means "any impairment to the integrity or availability of data, a program, a system, or information"
- "Loss" is monetary harm and means "any reasonable cost" to an employer
  - Costs include: responding to an offense; conducting a damage assessment; restoring data, programs, systems, or information to their pre-offense condition; and the revenue lost, costs incurred, or other consequential damages incurred because of interruption of service
  - Plaintiffs need to plead and provide evidence of at least $5,000 loss within 1 year
- Without sufficient damage or loss, a CFAA claim falters
  - *Turner v. Hubbard Sys., Inc.* affirmed summary judgment against plaintiff where access to software was restored after a few hours and remained uninterrupted from point of restoration

CFAA Action Rules and Procedures

- CFAA limitations provision requires filing action "within 2 years of the date of the act complained of or the date of the discovery of the damage"
  - *Sewell v. Bernardin* – Accordingly, the statute of limitations under the CFAA ran from the date that Sewell discovered that someone had impaired the integrity of each of her relevant Internet accounts
- Plaintiff can seek compensatory damages, injunctive relief, and other equitable relief, which in certain circumstances, is limited to economic damages

Typical Civil Action Claims under CFAA

Current or Ex-Employee…

- Intentionally accesses a computer without authorization or exceeds authorization and thereby obtains information from a protected computer
- Accesses a protected computer without authorization or in a manner that exceeds authorization with intent to defraud and obtains value beyond use of computer and value of such use exceeds $5,000 in any 1-year period
- Intentionally accesses protected computer without authorization and by such conduct causes damage and loss
- Knowingly transmits harmful code and as a result of such conduct intentionally causes damage without authorization to a protected computer

Employee Scenarios

- The CFAA can apply to employees who exceed their authorized access to information stored on computers for non-business reasons in violation of the Employer's policy
- Application of *United States v. Rodriguez* and *Hamilton Grp. Funding, Inc. v. Basel*
  - Applying *Rodriguez* as binding authority in 11th Circuit and broadly interpreting what qualifies as exceeding "authorized access" for CFAA claim against employer's former assistant VP and Director of Information Systems

CFAA Covers Data Destroyers

- Employers who can show intentional damage to data and computer networks receive more leeway to proceed with CFAA claims
  - *United States v. Nosal* – Ex-employee with revoked computer access credentials violated CFAA by accessing employer's databases after revocation
  - *LVRC Holdings LLC v. Brekka* – Employee violated CFAA by logging into employer website after employment ended

CFAA Covers Indirect Hackers

- Recent court opinions signal CFAA coverage of persons who recruit current employees to obtain access to data on protected computers of Employer
  - *Space Sys./Loral, LLC v. Orbital ATK, Inc.* – allegation of "exceeds authorized access" under CFAA was sustained against contractor charged with accessing files on server beyond what employee was authorized to view
  - *Teva Pharm. USA, Inc. v. Sandhu* – Ex-employee with authorized access to misused information dismissed but outside individual and competitor who acted in concert with employee to access employer's protected computers for shared data with trade secrets maintained as defendants

Government Investigations

- Victim rights
- Cooperating with the government while knowing your rights
- Keep your tech people in the loop
- Don't let the government disrupt your operations
- Press releases
- Stay informed
- Government wants you to help proactively

For an “Employer’s Cybersecurity Checklist,”

Please contact Ambrose or Ken…

Thank You

We welcome your questions and feedback.

Ambrose McCall
Ken Yeadon

309-674-1025 – amccall@hinshawlaw.com
312-704-3524 – kyeadon@hinshawlaw.com

www.hinshawlaw.com