Contents

➢IT Security Incidents: A Major Concern

◇ Why Computer Incidents are so Prevalent?

◇ Types of Exploits

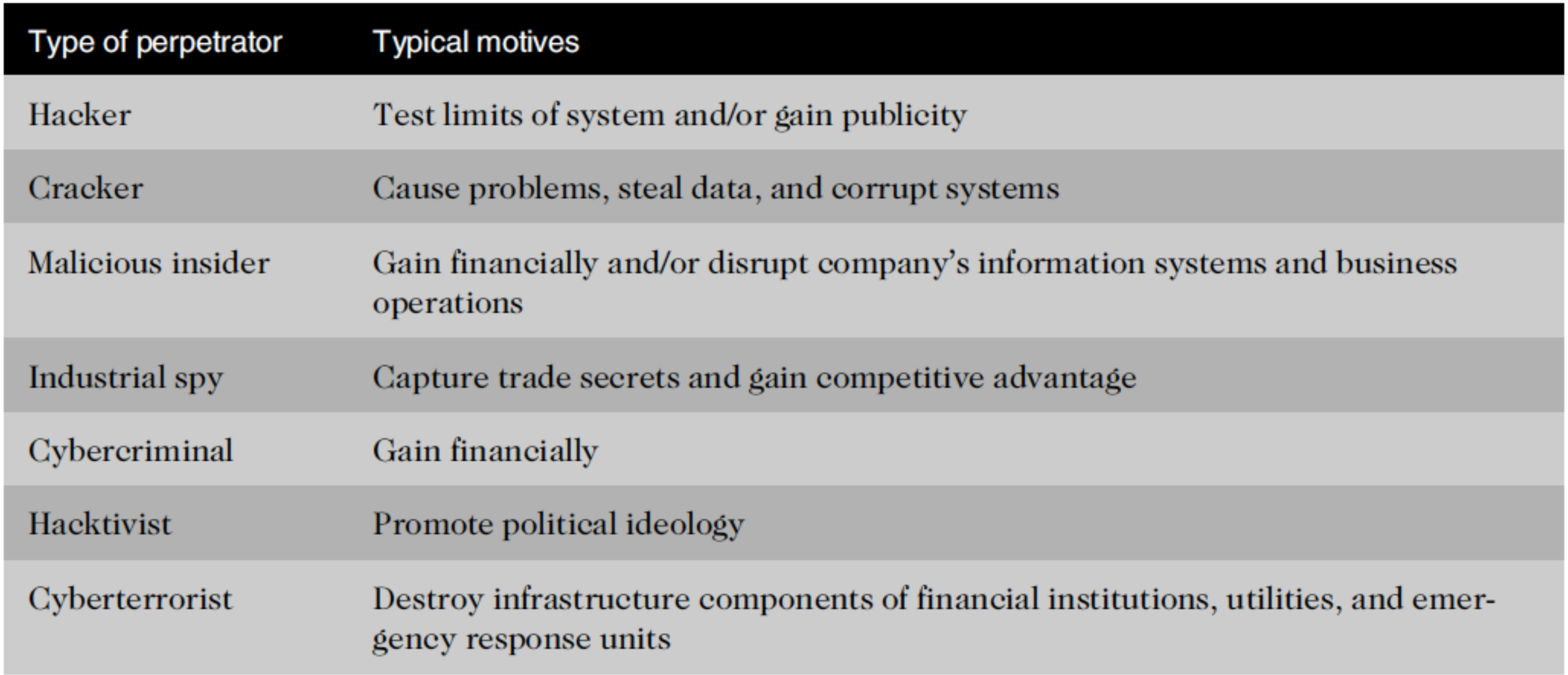
◇ Types of Perpetrators

◇ Federal Laws for Prosecuting Computer Attacks

Perpetrators

- Motives are the same as other criminals
- Different objectives and access to varying resources
- Different levels of risk to accomplish an objective

Classifying Perpetrators of Computer Crime



Type of perpetrator	Typical motives
Hacker	Test limits of system and/or gain publicity
Cracker	Cause problems, steal data, and corrupt systems
Malicious insider	Gain financially and/or disrupt company's information systems and business operations
Industrial spy	Capture trade secrets and gain competitive advantage
Cybercriminal	Gain financially
Hacktivist	Promote political ideology
Cyberterrorist	Destroy infrastructure components of financial institutions, utilities, and emergency response units

1. Hackers

– Test limitations of systems out of intellectual curiosity

– Their motivation comes from a desire to learn even more

Hackers: Case Studies

- **Twitter** has been hacked numerous times.
- One hacker force victims to join his Twitter follow list automatically.
- Created a Twitter account under the name of Vint Cerf (the person most often called the father of the Internet) and used it for spamming.
- Hackers gained access to several high-profile accounts (Barack Obama, Britney Spears, and CNN's Rick Sanchez) and sent out fake updates in their names.
- Chinese hackers have repeatedly hacked into systems to intercept e-mails between U.S. and UK government officials.

2. Cracker

- Cracking is a form of hacking
- Clearly criminal activity

Crackers: Case Study

- Defaced a CERN (the European Organization for Nuclear Research) Web page, disparaging CERN's IT security staff as a "bunch of school kids"
- Simply wanted to highlight the lab's security problems
- The crackers came very close to gaining access to a computer that controlled one of the 12,500 magnets that control the Large Hadron Collider built to perform particle physics experiments

3. Malicious Insiders

- **Top security** concern for companies
- **Estimated 85% of all fraud is committed by employees**
- **Due to weaknesses in internal control procedures**
- **Collusion** is cooperation between an employee and an outsider
- Insiders are not necessarily employees
  - Can also be **consultants** and **contractors**
- Extremely difficult to detect or stop
  - Authorized to access the systems they abuse

3. Malicious Insiders (Countermeasure)

1. Perform a thorough background check as well as psychological and drug testing of candidates for sensitive positions.
2. Establish an expectation of regular and ongoing psychological and drug testing for people in sensitive positions.
3. Limit the number of people who can perform sensitive operations (Minimum rights and privileges)

3. Malicious Insiders (Countermeasure)

4. Define job roles and procedures ➔ it is not possible for the same person to both initiate and approve an action.
5. Periodically rotate employees in sensitive positions ➔ unusual procedures can be detected by the replacement.
6. Immediately revoke all rights and privileges required to perform old job responsibilities when someone in a sensitive position moves to a new position.
7. Implement an ongoing audit process to review key actions and procedures

Case Study: Société Générale

Internal fraud carried out by an employee, **Jérôme Kerviel**
SocGen bank lost €4.9 billion (euros) as an immediate result of the fraud

Société Générale

- Kerviel knew that while the Risk-Control Department monitored the bank's overall positions very closely, it did not verify the data that individual traders entered into the system.

- Kerviel also knew the timing of the nightly reconciliation of the day's trades, so he was able to delete and then reenter unauthorized transactions without getting caught.

Société Générale and Eurex

- On November 7, 2007:
  - **Eurex** said that Kerviel had engaged in several transactions that had set off alarms at the exchange over the past seven months.
  - **SocGen**: Nothing is irregular
- **Eurex** was not satisfied with **SocGen's** explanation and demanding more details.
  - **SocGen** provided further details, and both **Eurex and SocGen let the matter drop**.
- Following the **Eurex** warnings, Kerviel took additional steps to cover his tracks by manipulating portions of the internal risk-control system with which he was unfamiliar.
- This ultimately led to the discovery of his alleged fraud!

Société Générale: How detected!

- On January 18, 2008, Kerviel executed a set of trades that set off another alarm
- **Another Alarm!**
  - They discovered that the trades had resulted in a market exposure for the firm of €50 billion (obviously far beyond Kerviel's trading limit), which, when finally cleared, resulted in a loss of more than €4.9 billion.

Kerviel Confesses!

- “The techniques I used aren’t at all sophisticated and any control that’s properly carried out should have caught it.”
- “My superiors tacitly approved his activities—as long as they were generating a profit.”
- Kerviel had earned a profit for the bank of nearly €1.5 billion in 2007 by exceeding his trade limit and executing similar, but successful, trades.

- Kerviel faces up to five years in jail and fines totaling as much as €300,000

4. Industrial Spies

- Illegally obtain trade secrets from competitors
- Trade secrets are protected by the Economic Espionage Act of 1996
- **Competitive intelligence**
  - Uses legal techniques
  - Gathers information available to the public
- **Industrial espionage**
  - Uses illegal means
  - Obtains information not available to the public

Industrial Spies: Case Study

- **Who:** Shekhar Verma
- **Where:** India, Geometric Software Solutions Ltd. (GSSL)
- **Why:** GSSL was awarded a contract to debug the source code of SolidWorks 2001 Plus, a popular computer-aided design software package.
- **Espionage:** Allegedly stole the source code and offered it to several of SolidWorks' U.S. competitors for $200,000. (The value of the source code has been estimated to exceed $50 million.)
- **Result:** Arrested, but Indian law at the time did not recognize misappropriation of trade secrets, so technically Verma did not steal from his employer, as the source code belonged to SolidWorks.

5. Cybercriminals

1. Hack into corporate computers and steal and engage in all forms of **computer fraud**

2. Chargebacks on disputed transactions

- Note that Loss of customer trust has more impact than fraud
- **To reduce the potential for online credit card fraud sites:**
  - Use encryption technology
  - Verify the address submitted online against the issuing bank
  - Request a card verification value (CVV)
  - Use transaction-risk scoring software

5. Cybercriminals (continued)

- **Smart cards**
  - Contain a memory chip
  - Are updated with encrypted data every time the card is used
  - Used widely in Europe
  - Not widely used in the U.S.

6. Hacktivist and Cyberterrorists

- Hacking to achieve a **political or social goal** intimidate or coerce governments to advance political or social objectives
- Launch computer-based attacks
- **Seek to cause harm**
  - Rather than gather information
- Many experts believe terrorist groups pose only a limited threat to information systems

Hactivist: Case Study

- 2009: Israeli hacktivists made available malware dubbed Patriot
- The malware converts computers into zombies, which launch a distributed denial-of-service attack intended to silence Hamas Web sites.
- Meanwhile, anti-Israeli hacktivists were also on the offensive

Bruce Jenkins

Our observations suggest that a large number of Web sites
have been defaced by a variety of hacker groups
from **Iran**, **Lebanon**, **Morocco** and **Turkey**
and the trend is accelerating.

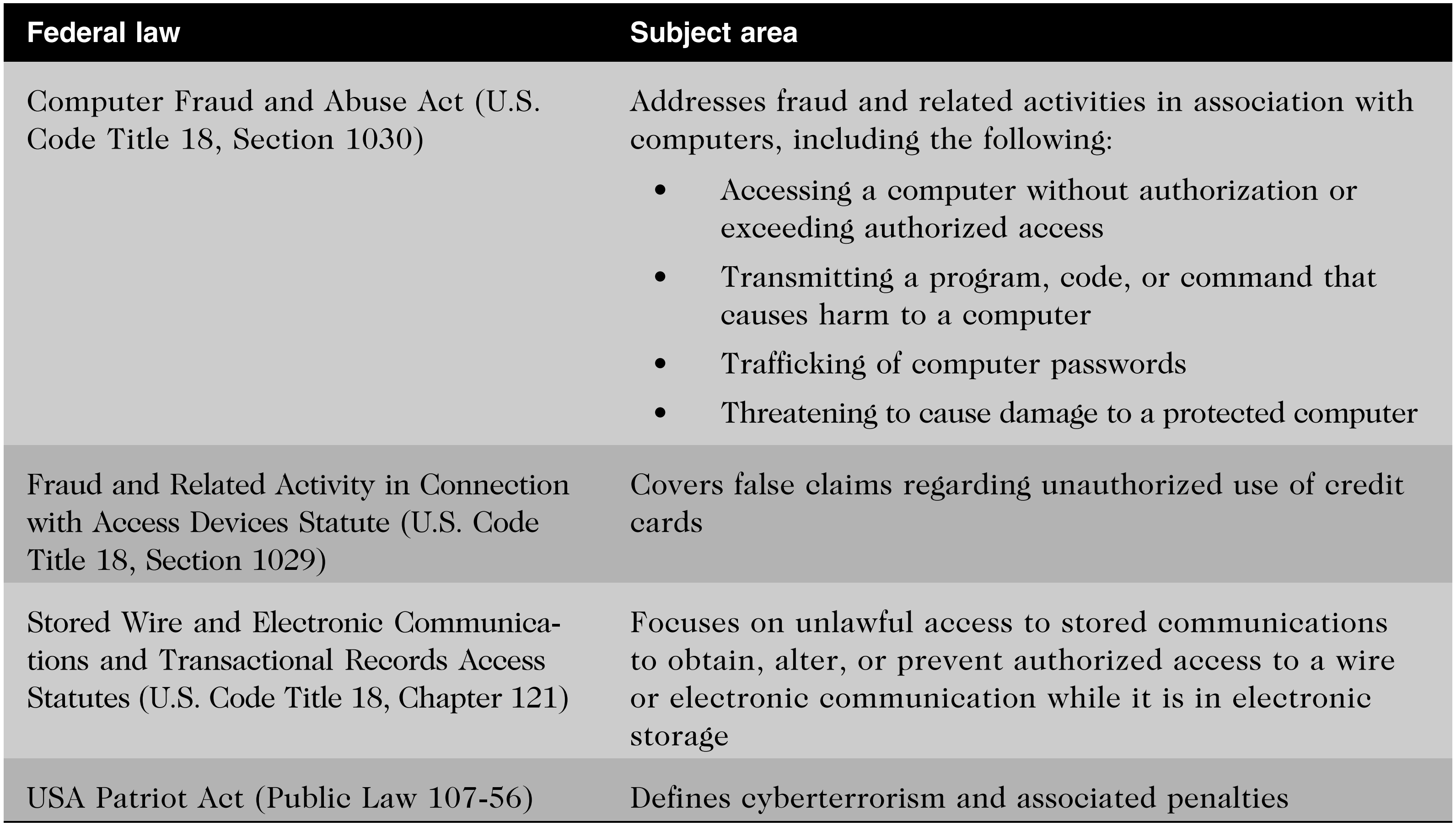
FORTIFY An HP Company

Contents

➢IT Security Incidents: A Major Concern

- ◇ Why Computer Incidents are so Prevalent?
- ◇ Types of Exploits
- ◇ Types of Perpetrators
- ◇ Federal Laws for Prosecuting Computer Attacks

Federal Laws
Apply to Computer Attacks



Federal law	Subject area
Computer Fraud and Abuse Act (U.S. Code Title 18, Section 1030)	Addresses fraud and related activities in association with computers, including the following: • Accessing a computer without authorization or exceeding authorized access • Transmitting a program, code, or command that causes harm to a computer • Trafficking of computer passwords • Threatening to cause damage to a protected computer
Fraud and Related Activity in Connection with Access Devices Statute (U.S. Code Title 18, Section 1029)	Covers false claims regarding unauthorized use of credit cards
Stored Wire and Electronic Communications and Transactional Records Access Statutes (U.S. Code Title 18, Chapter 121)	Focuses on unlawful access to stored communications to obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage
USA Patriot Act (Public Law 107-56)	Defines cyberterrorism and associated penalties