SENG 460

Practice of Information Security and Privacy

Legal, Regulations, Investigations, and Compliance

Overview

- Computer Crime Related Concepts
- Complexity of Computer Crimes & Laws
- Intellectual Property
- Privacy
- Liability
- Information Security Laws, Directives, and Regulations
- Computer Crime Investigations
- Security Professional Ethics

Computer Crime Related Concepts

- **Computer-assisted crime**: a computer is used as a tool to help carry out a crime.
- **Computer-targeted crime:** a computer is the victim of an attack crafted to harm it (and its owners) specifically.
- **Incidental computer crime:** a computer is involved in a computer crime without being the victim of the attack.
- **Computer prevalence crime:** a crime which relies on computer's prevalence.
- **Hackers versus crackers:** hackers break systems for malicious intent; crackers break systems for fun.
- **Zombies, Bot, Botnet:** zombies refer to computers controlled by hacker's computer; bots are malicious software installed on zombie machine; botnets refer to a system that consists of a set of zombie machines with bots installed.
- **White Hat, Black Hat, Grey Hat:** A white hat does not have any malicious intent; A black hat has malicious intent; A gray hat is considered somewhere in the middle of the previous two.

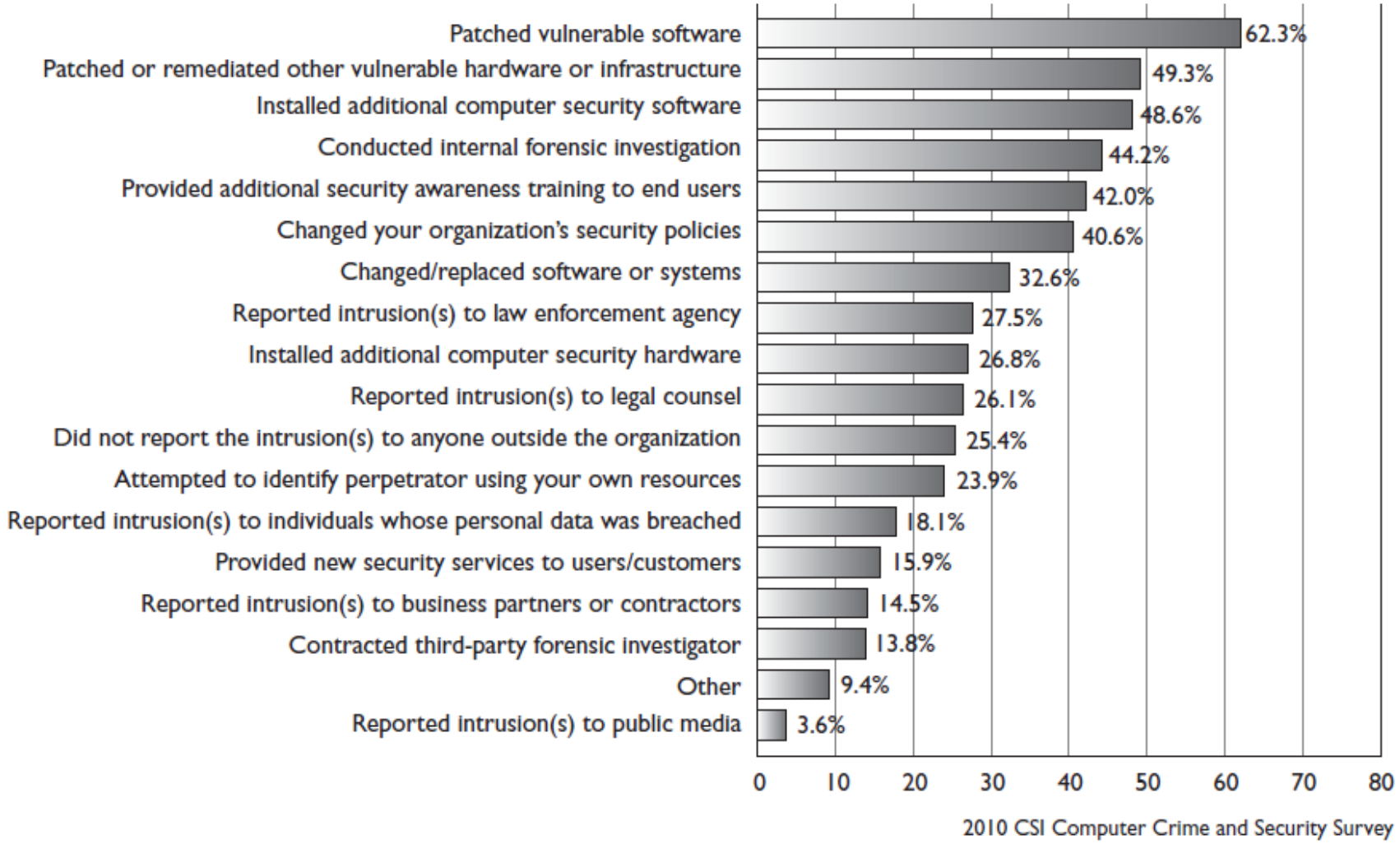
Complexity of Computer Crimes & Laws

- Computer hacking activities can take place really quickly without being noticed.
- Obtaining a trail of evidence of activities performed on a computer is hard because evidence is mostly *intangible*.
- Prosecuting computer crimes is hard due to the difficulties of tracking criminals and the diversity of cyber laws in different regions.
- Some regulated organizations—for instance, financial institutions—by law, must report breaches. However, most organizations do not have to report breaches or computer crimes.

The legal system and law enforcement are behind in their efforts to track down cybercriminals and successfully prosecute them.

Actions Taken After Incident

By Percent of Respondents



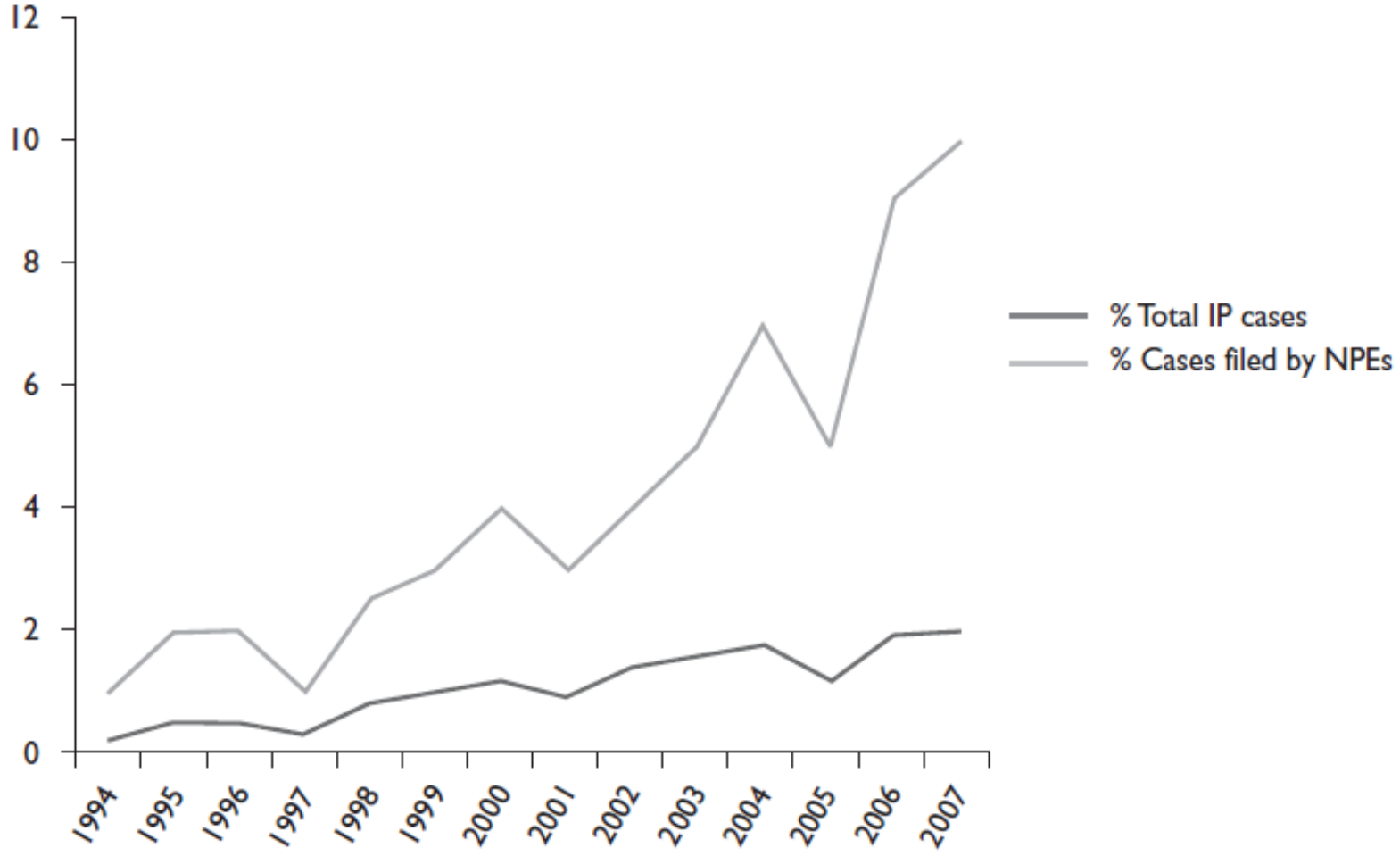
2010 CSI Computer Crime and Security Survey

Intellectual Property (IP)

- **Intellectual Property** law is a group of laws that protects exclusive rights for creations of the mind.
  - **Patent:** Legal ownership of an invention, which enable patent owners to exclude others from using or copying the invention covered by the patent.
  - **Copyright:** The expression of the idea of the resource instead of the resource itself.
  - **Trade Secret:** Something that is proprietary to a company and important for its survival and profitability.
  - **Trademarks:** A word, name, symbol, sound, shape, color, or combination of these, which represents their company (brand identity) to a group of people or to the world.

Lawsuits by Patent Trolls on the Rise

Percentage of intellectual property-related lawsuits by nonpracticing entities to total IP-related lawsuits



Intellectual Property (IP)

- Internal Protection of Intellectual Property

- Employees are the greatest threat for any organization.
  - Organizations should take measures to protect confidential resources from unauthorized internal access.
  - Any information that is part of a patent, trade secret, trademark, or copyright should be marked and given the appropriate classification.
  - Access controls should be customized for this information, and audit controls should be implemented that alert personnel should any access occur.
  - Procedures and policies must be in place to ensure that any laws that protect these assets can be used to prosecute an offender.

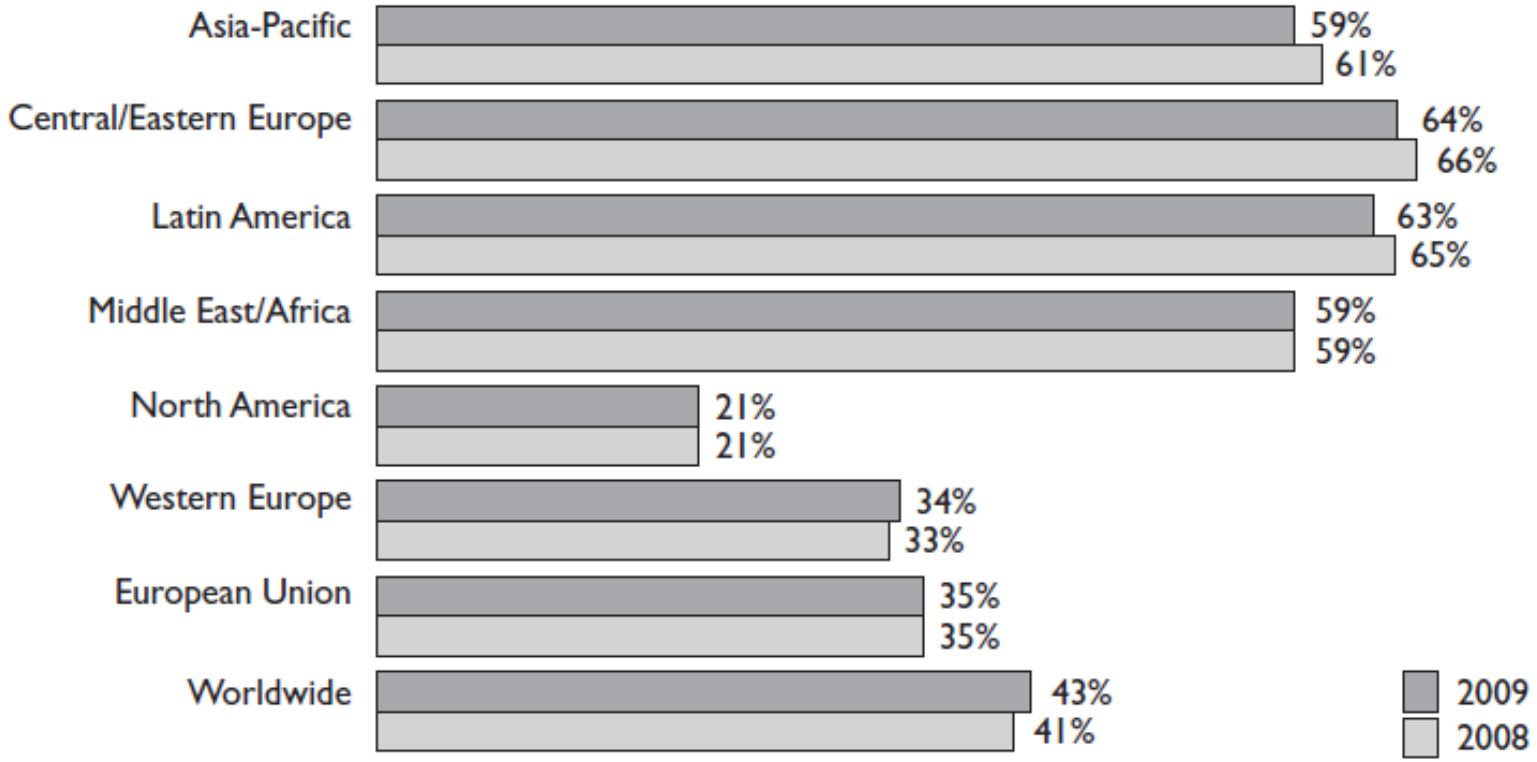
Intellectual Property (IP)

- Software Piracy

- Software piracy is an act of infringement on ownership rights, which can result in being sued civilly for damages, being criminally prosecuted, or both.
  - There are four categories of software licensing:
    - **Freeware**
    - **Shareware (Trialware)**
    - **Commercial Software**
    - **Academic Software**
  - Not every country recognizes software piracy as a crime, but several international organizations have made strides in curbing the practice:
    - ***Software Protection Association (SPA)***
    - ***Federation Against Software Theft (FAST)***
    - ***Business Software Alliance (BSA)***

Digital Millennium Copyright Act (DMCA) *is a U.S. copyright law that criminalizes the production and dissemination of technology, devices, or services that circumvent access control measures that are put into place to protect copyright material.*

Software Piracy Rates by Region



Source: Seventh Annual BSA/DC Global Software Piracy Study, May 2010

Privacy

- What and Why

- Privacy is the ability of an individual or group to control who has certain types of information about them, which usually covers three areas:
  - Which personal information can be shared with others
  - Which people are permitted to know that data
  - when those people can access it
- Privacy Laws are needed increasingly because:
  - Data aggregation and retrieval technologies advancement
  - Loss of borders (globalization)
  - Convergent technologies advancements

Privacy *is different with* ***Security****. Privacy defines the personal data access rights, Security is used to enforce these privacy rights.*

Privacy

- Personally Identifiable Information (PII)

- **Personally Identifiable Information (PII)** is a set of data that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.

PII components defined by The U.S. Office of Budget and Management:

- *Full name (if not common)*
- *National identification number*
- *IP address (in some cases)*
- *Vehicle registration plate number*
- *Driver's license number*
- *Face, fingerprints, or handwriting*
- *Credit card numbers*
- *Digital identity*
- *Birthday*
- *Birthplace*
- *Genetic information*

Less often used PII Items:

- First or last name, if common
- Country, state, or city of residence
- Age, especially if nonspecific
- Gender or race
- Name of the school they attend or workplace
- Grades, salary, or job position
- Criminal record

Privacy

- Privacy Protection

- Employee privacy issues must be addressed by all organizations to ensure that the organization is protected.
- Give employees the proper notice of any monitoring that might be used.
- Ensure that the monitoring of employees is applied in a consistent manner and compliant with laws andregulations.
  - e.g. European Union Principles on Privacy include strict laws to protect private data.

Liability

- Primary Concerns

- Liability is the status of being legally responsible to another entity because of your actions or negligence. Recent laws hold senior management responsible for organizational liability.

  - **Due diligence** means that the company properly investigated all of its possible weaknesses and vulnerabilities.
    - Due diligence is all about gathering information
    - When due diligence occurs, organizations will recognize areas of risk.

  - **Due care** means that an organization takes all the actions it can reasonably take to prevent security issues or to mitigate damage if security breaches occur.
    - Due care is all about action
    - When due care occurs, organizations take the areas of identified risk and implement plans to protect against the risks.

Liability

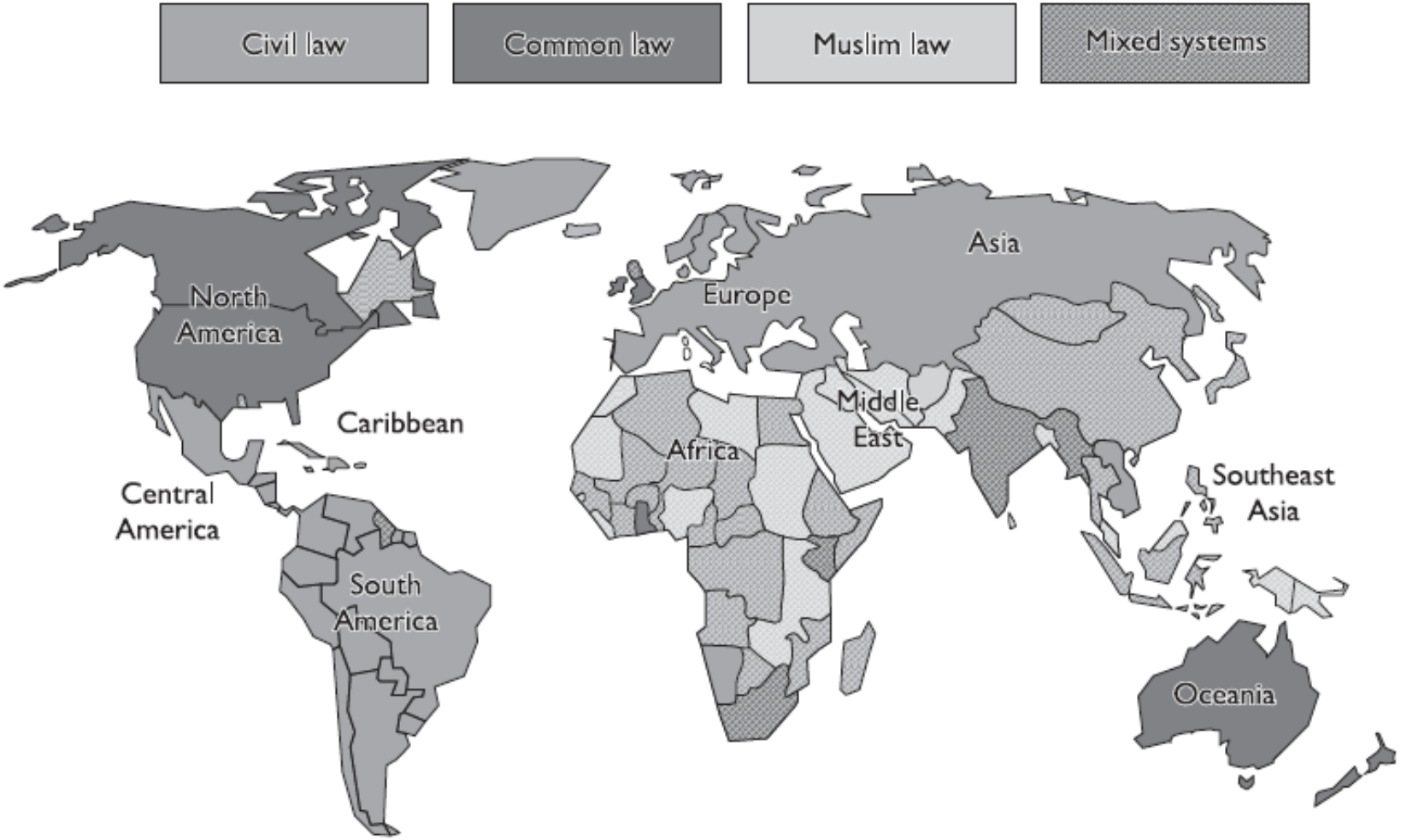
- Other Concerns

- ***Negligence*** means that an organization was careless and as a result of being careless, some person or organization was injured.
- ***Downstream Liability*** refers to liability that an organization accrues due to partnerships with other organizations and customers.
- **Contractual Agreements:** Contractual agreements need to cover regulatory, legal, and security requirements.
- **Procurement Process:** Procurement is not just purchasing something, but includes the activities and processes involved with defining requirements, evaluating vendors, contract negotiation, purchasing, and receiving the needed solution.
- **Compliance:** Auditors can be internal or external to the organization, who will determine if an organization is compliant with the specifics of regulations and laws.

Information Security Laws, Directives, and Regulations

- Brief Introduction to Legal Systems

- **Civil (Code) Law System**
  - Focused on codified law—or written laws.
  - The most widespread legal system in the world and the most common legal system in Europe.
- **Common Law System**
  - Uses judges and juries of peers. If the jury trial is waived, the judge decides the facts.
- **Customary Law System**
  - Based on traditions and customs of the region.
- **Religious Law System**
  - Based on religious beliefs of the region.
- **Mixed law**
  - Two or more legal systems are used together and apply cumulatively or interactively.


Civil law
Common law
Muslim law
Mixed systems
North America
Caribbean
Central America
South America
Europe
Asia
Africa
Middle East
Southeast Asia
Oceania

Information Security Laws, Directives, and Regulations

- Common Law Legal System

- Developed in England. Typical systems consist of a higher court, several intermediate appellate courts, and many local trial courts. Precedent flows down through this system. Led to the creation of barristers, or lawyers, who actively participate in the litigation process through the presentation of evidence and arguments.

  - **Criminal Law:** deals with an individual's conduct violates the government laws, which have been developed to protect the public. Jail sentences are commonly the punishment for criminal law cases.
  - **Civil Law (*tort law)*:** deals with wrongs against individuals or companies that result in financial restitution and/or community service instead of a jail sentence.
  - **Administrative/regulatory Law:** deals with regulatory standards that regulate performance and conduct. Government agencies create these standards, which are usually applied to companies and individuals within those specific industries.

Information Security Laws, Directives, and Regulations - What needs to know as a security professional

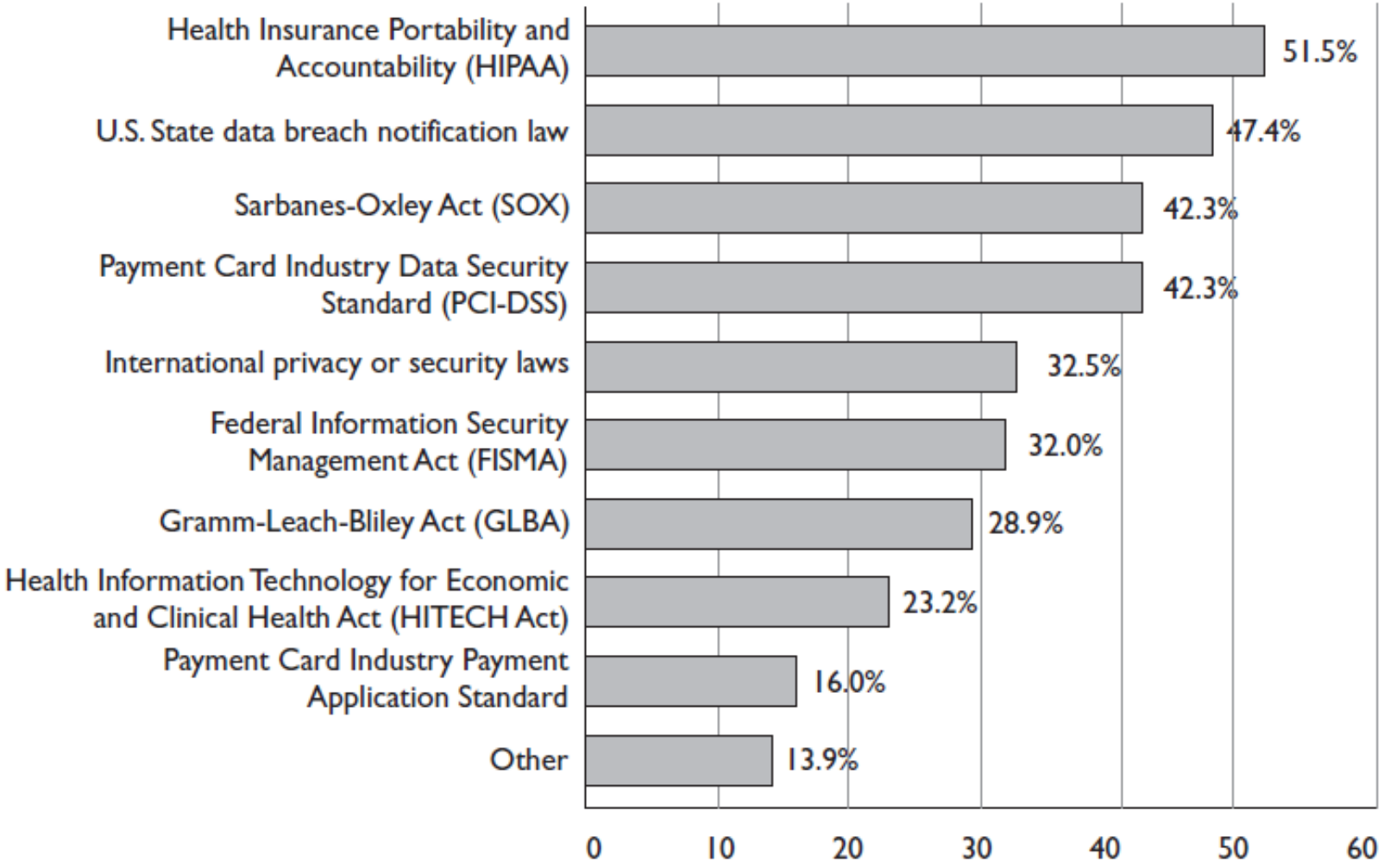
- Regulation in computer and information security covers many areas for many different reasons
  - data privacy
  - computer misuse
  - Software copyright
  - data protection
  - controls on cryptography
- Security professionals must be aware of the laws and at a minimum understand how those laws affect the operations of their organization.
  - The name of the law
  - The purpose of the law
  - The industry affected by the law

Information Security Laws, Directives, and Regulations - Some Information Security Regulations good to know

- **Sarbanes-Oxley (SOX) Act:** provides requirements for how companies must track, manage, and report on financial information, applies to any company that is publicly traded on U.S. markets
- **Health Insurance Portability and Accountability Act (HIPAA):** a U.S. federal regulation, has been mandated to provide national standards and procedures for the storage, use, and transmission of personal medical information and healthcare data.
- **Gramm-Leach-Bliley Act (GLBA) of 1999:**requires financial institutions to develop privacy notices and give their customers the option to prohibit financial institutions from sharing their information with nonaffiliated third parties.
- **Computer Fraud and Abuse Act (CFAA) of 1986:** the primary U.S. federal antihacking statute, the most widely used law pertaining to computer crime and hacking.
- **Personal Information Protection and Electronic Documents Act (*PIPEDA)*:** a Canadian law that deals with the protection of personal information.
- **Payment Card Industry Data Security Standard (PCI DSS):** applies to any entity that processes, transmits, stores, or accepts credit card data.
- **Federal Information Security Management Act (FISMA) of 2002:** a U.S. law that requires every federal agency to create, document, and implement an agency-wide security program for information protection.

Which Law and Industry Regulations Apply to Your Organization?

By Percent of Respondents



2010 CSI Computer Crime and Security Survey

Computer Crime Investigations

- Incident Response

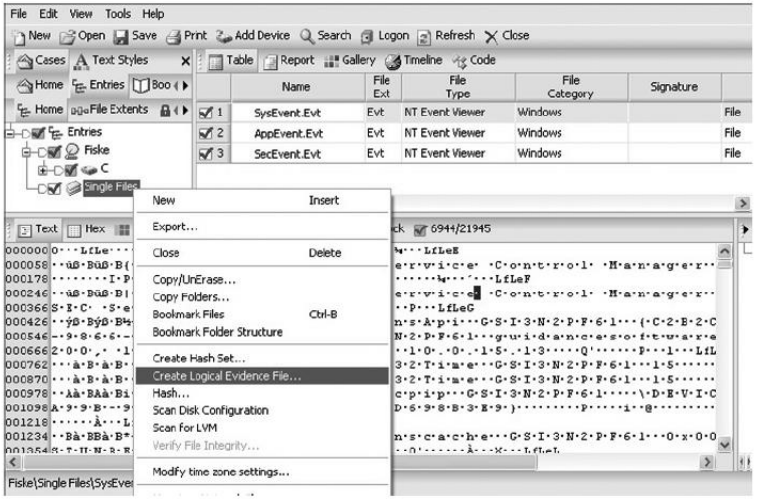
- **Triage:** take in the information available, investigate its severity, and set priorities on how to deal with the incident.
- **Investigation:** actions for the proper collection of relevant data, which will be used in the analysis and following stages
- **Containment:** actions for minimizing the damage, e.g. an infected server is taken off the network, firewall configurations are changed to stop an attacker, or the system that is under attack is disconnected from the Internet.
- **Analysis:** Computer forensics take place, more data are gathered (audit logs, video captures, human accounts of activities, system activities) to try and figure out the root cause of the incident.
- **Tracking:** determine whether the source of the incident was internal or external and how the offender penetrated and gained access to the asset
- **Follow up:** implement the necessary fix to ensure this type of incident cannot happen again.

Computer Crime Investigations

- Forensic

- **Computer forensics** is a set of specific processes relating to reconstruction of computer usage, examination of residual data, authentication of data by technical analysis in order for evidence to be admissible in a court of law.

Identification	Preservation	Collection	Examination	Analysis	Presentation
Event/crime detection	Case management	Preservation	Preservation	Preservation	Documentation
Resolve signature	Imaging technologies	Approved methods	Traceability	Traceability	Expert testimony
Profile detection	Chain of custody	Approved software	Validation techniques	Statistical	Clarification
Anomalous detection	Time synchronization	Approved hardware	Filtering techniques	Protocols	Mission impact statement
Complaints		Legal authority	Pattern matching	Data mining	Recommended countermeasure
System monitoring		Lossless compression	Hidden data discovery	Timeline	Statistical interpretation
Audit analysis		Sampling	Hidden data extraction	Link	
Etc.		Data reduction		Spatial	
		Recovery techniques			



EVIDENCE

Station/Section/Unit/Dept_____

Case number_____ Item#_____

Type of offense_____

Description of evidence_____

_____

_____

Suspect_____

Victim_____

Date and time of recovery_____

Location of recovery_____

Recovered by_____

CHAIN OF CUSTODY

Received from_____ By_____

Date_____ Time_____ A.M./P.M.

Received from_____ By_____

Date_____ Time_____ A.M./P.M.

Received from_____ By_____

Date_____ Time_____ A.M./P.M.

Received from_____ By_____

Date_____ Time_____ A.M./P.M.

WARNING: THIS IS A TAMPER EVIDENT SECURITY PACKAGE. ONCE SEALED, ANY ATTEMPT TO OPEN WILL RESULT IN OBVIOUS SIGNS OF TAMPERING.

Forensics Field Kits

When forensics teams are deployed, they should be properly equipped with all of the tools and supplies needed. The following are some of the common items in the forensics field kits:

- Documentation tools Tags, labels, and timelined forms
- Disassembly and removal tools Antistatic bands, pliers, tweezers, screwdrivers, wire cutters, and so on
- Package and transport supplies Antistatic bags, evidence bags and tape, cable ties, and others

Chain of Custody is a history that shows how evidence was collected, analyzed, transported, and preserved in order to be presented in court. Because electronic evidence can be easily modified, a clearly defined chain of custody demonstrates that the evidence is trustworthy.

Computer Crime Investigations

- Evidence Concerns

- Evidence must be ***Relevant, Legally permissible, Reliable, Properly Identified, and Properly Preserved***.
- When gathering evidence, an investigator must ensure that the evidence meets the five rules that govern it, which are ***Be authentic, Be accurate, Be complete, Be convincing, Be admissible***.
- The types of evidence Includes:
  - Best evidence
  - Secondary evidence
  - Direct evidence
  - Conclusive evidence
  - Circumstantial evidence
  - Corroborative evidence
  - Opinion evidence
  - Hearsay evidence

Security Professional Ethics

- Ethics for any profession are the right and wrong actions that are the moral principle of that occupation.
- Security professionals, particularly those who hold the CISSP certification, should understand the ethics that are published by
  - the International Information Systems Security Certification Consortium $(ISC)^2$,
  - the Computer Ethics Institute,
  - the Internet Architecture Board (IAB)

Security Professional Ethics

- (ISC)² Code of Ethics

- The four mandatory canons for the Code of Ethics are as follows:
  - Protect society, the common good, necessary public trust and confidence, and the infrastructure.
  - Act honorably, honestly, justly, responsibly, and legally.
  - Provide diligent and competent service to principals.
  - Advance and protect the profession.

Security Professional Ethics

- Computer Ethics Institute

- The Computer Ethics Institute created the Ten Commandments of Computer Ethics:
  - Do not use a computer for harm.
  - Do not interfere with the computer work of other people.
  - Do not snoop around in the computer files of other people.
  - Do not use a computer to steal.
  - Do not use a computer to lie.
  - Do not install and use licensed software unless you have paid for it.
  - Do not use another person's computer unless you have permission or have paid the appropriate compensation for said usage.
  - Do not appropriate another person's intellectual output.
  - Consider the consequences of the program you are writing or the system you are designing.
  - Always use a computer in ways that ensure consideration and respect of other people and their property.