Compliance and Legal Issues

IN 2016, according to the Breach Level Index, 1,792 breach incidents occurred, resulting in 1,378,509,261 records being breached. In other words, 3,776,738 data records were lost or stolen per day, 157,364 per hour, 2,623 per minute, and 44 per second. Obviously, digital security laws and compliance regulations are tested every second of every day. Securing private information from outside threats is a critical need and responsibility. This E-unit introduces the cyber security terminology, resources, regulations, and laws that currently protect our data.

Objective:

Analyze security incidents and data breaches, regulatory compliance standards, and chain-of-custody procedures.

Key Terms:

AlienVault
APT (advanced persistent threat)
attestation
chain of custody
compliance
copyright
cyber attack
data breach
disaster recovery plan
evidence
forensics
heuristic software program
image
incident
logging
negligence
Open Threat Exchange (OTX)
open-source forensic software
patent
recovery
regulation
regulatory compliance
rules of evidence
security
threat
We trust but verify

Cyber Compliance and Regulations

Security is the protection of data from threats by controlling how the data is used, consumed, and provided. Security programs are designed to keep an organization secure daily, whereas compliance regulations change slowly and rarely catch up with the constantly changing security environment.

To be clear, **compliance**, according to the Armor Defense website, is "a demonstration—a reporting function—about how [the] security program meets specific security standards as laid out by regulatory organizations," such as those dealing with the payment card industry (PCI), HIPAA, and the Sarbanes-Oxley Act (SOX). Although compliance is a critical component of any security program, it is only a snapshot "that reflects how an organization's security program meets a specific set of security requirements at a given moment in time." (Source: Armor Defense website.)

The basic rule of cyber security compliance is, "We trust but verify." **We trust but verify** is the "concept of obtaining evidence of compliance with stated policies, standards, laws, regulations, etc. in order to issue the proper attestations as required." (Source: SSH Communications Security website.) An **attestation** is a formal statement, often written, or evidence that something is true, correct, or real.

Data breach compliance differs from state to state and country to country. In short, organizations are often not required to report many types of security incidents but are required by law to follow particular procedures in the case of data breaches.

SECURITY INCIDENTS VERSUS DATA BREACHES

Attacks and Threats

A **cyber attack** is an assault that targets an "enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information." [Source: "Glossary of Key Information Security Terms," NIST (National Institute of Standards and Technology), http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf.] Recovery from such an attack requires restoration of essential services and operation in the short and medium term and full restoration of all capabilities in the longer term.

A **threat** is "a circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society." [Source: "Glossary," NICCS (National Initiative for Cybersecurity Careers and Studies), https://niccs.us-cert.gov/glossary#R.] An **APT (advanced persistent threat)** is "a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time." The intent of an APT is to steal data rather than to cause damage. (Source: WhatIs website.)

AlienVault is a developer of commercial and open-source solutions to manage cyber attacks, including the Open Threat Exchange (OTX).

The **Open Threat Exchange (OTX)** is the world's largest crowd-sourced computer-security platform, with more than 26,000 participants in 140 countries who share more than 1 million potential threats daily. It is free to use and cloud based.

Incidents

An **incident** is a "violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices." (Source: NIST glossary.) Its actual or potential result is an adverse consequence to an information system or the information that the system processes, stores, or transmits. A response action may be required to mitigate the consequences. Incidents that do not "involve the theft of sensitive personal data…are viewed very different in the eyes of the law and for purposes of regulatory compliance." (Source: AlienVault website.) An incident is anything that happens to a network that is unexpected. Incidents are not necessarily damaging.

Damaging incidents include the release or collection of sensitive data.

Nondamaging incidents include:

- Denial of service
- Unauthorized user
- Website altering
- Impersonation

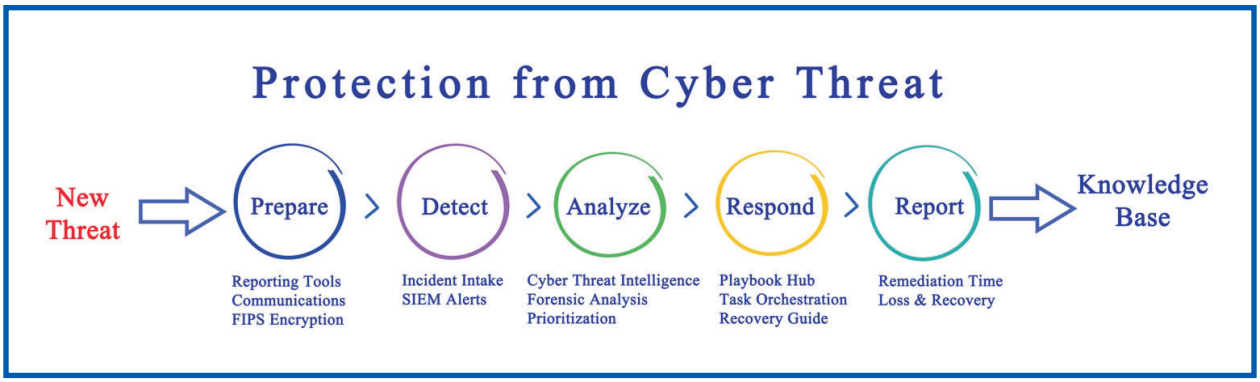

FIGURE 1. An incident's actual or potential result is an adverse consequence to an information system or the information that the system processes, stores, or transmits. A data breach is the intentional or unintentional release of personally sensitive, protected, and/or confidential data.

Data Breaches

A **data breach** (a.k.a. data leak, data spill) is the intentional or unintentional release of personally sensitive, protected, and/or confidential data, such as social security numbers and personal health records: a break in an organization's technology defenses that compromises sensitive data. If a security incident is damaging and/or committed with malicious intent and

results in sensitive data being lost, then that event is classified as a higher threat category: data breach. Breaches could influence the integrity or confidentiality of the organization. All breaches are incidents, but not all incidents are breaches. An incident can be a malware attack, a denial of service, or a hijacked webpage. As long as sensitive data is not compromised, the cyber event is considered an incident. Examples of data breaches include the Target hack and movie and miniseries attacks.

The Target Hack

In the Target department store hack of 2014, hackers captured the banking information of 40 million Target customers. It was much more than an incident; it was an epic breach. Hackers were able to gain access to the network and deploy a program that captured screenshots, keystrokes, and login credentials (usernames and passwords) for various account sites. This hack qualifies as a data breach because customers' personal financial information was stolen; both debit and credit card information was compromised. Target was found negligent in this case. **Negligence** is failure to take proper care in doing something. Investigators determined that Target ignored early warning signals from its cyber security systems about harmful traffic on the network: negligence. "Enabling the security notifications" would have prevented the breach.

FURTHER EXPLORATION...

ONLINE CONNECTION: Credit-Reporting Agency Breach

Credit-reporting agencies monitor and collect the data created by consumers spending money borrowed from banks and other financial lending institutions via credit cards, etc. Naturally, banks are not going to provide money to consumers based solely on name and address. Consumers fill out applications that contain education history, employment history, social security number, and sensitive information about relatives (spouse, parents, etc.).

Equifax, one of the three major credit-reporting agencies in the United States, experienced a massive breach in July 2017. Equifax began investigating and attempted to protect its "clients" from malicious intent—a virtually impossible task considering the extent of the breach. Then, the company responded by providing identity theft protection to consumers in case those responsible for the breach attempted to use the consumers' information inappropriately.

Read the *USA Today* article, "Equifax Data Breach: Feds Start Investigation," at https://www.usatoday.com/story/money/2017/09/14/ftc-investigating-equifax-over-data-breach/665550001/.

As you read the *USA Today* article about the Equifax breach, note of the role the Federal Trade Commission played in the investigation, and then note the point at which cyber security professionals alerted Equifax to the vulnerability that precipitated the breach.

Movie and Miniseries Hacks

The entertainment industry has also reported security breaches. The movie series "Pirates of the Caribbean" and the TV miniseries "Game of Thrones" were breached and distributed online. In each case, property was stolen, and copyright was infringed. **Copyright** is the exclusive legal right given to an originator to print, publish, perform, film, or record literary, artistic, or musical material and to authorize others to do the same. These works were stored digitally after production, and unauthorized users gained access, stole the files, and distributed them to the public. [NOTE: There is a difference between copyright and a patent. A **patent** is a set of exclusive rights granted by a government or other entity to an inventor or assignee for a limited time in exchange for detailed public disclosure of an invention. A patent to the creator of authentic material is used as protection against others imitating and profiting from the original invention. If the design is stored digitally and a hacker gains access, massive distribution can wreak havoc on the inventor. Although the patent protects the original design, modifications can be created, and competition can occur with the inventor.]

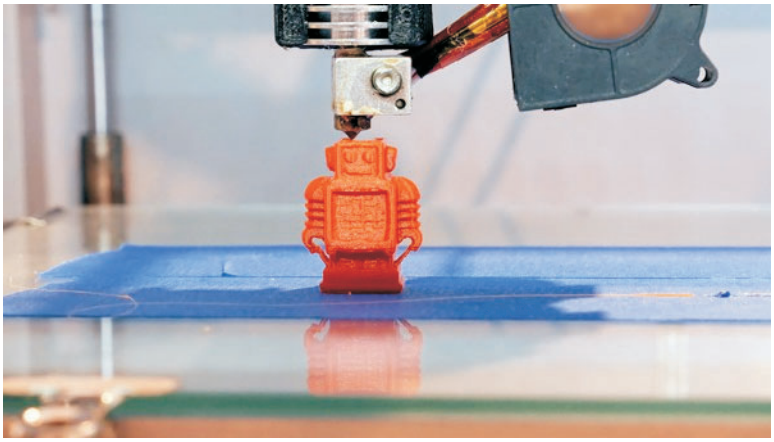

FIGURE 2. The file used to create this robot on a 3D printer is stored digitally. The file design belongs to an individual or to a company. The copyright for the 3D robot design is what network security works to protect.

REGULATORY COMPLIANCE

A **regulation** is a rule made and maintained by an authority. **Regulatory compliance** is an organization's adherence to laws and guidelines relevant to its business. Organizations governed by an authoritative body comply with that body's current legislation. Businesses and organizations that practice the rules of the authoritative body are said to be "in compliance." Regulatory compliance examples include the following entities.

ASPCA

The ASPCA (American Society for the Prevention of Cruelty to Animals) protects the rights of animals. Animal shelters, animal attractions, horse-and-buggy owners, etc., all comply with current ASPCA legislation.

FDA

Food manufacturers comply with the FDA (Food and Drug Administration) rulings. In some cases, manufacturers have two years to reformulate recipes to meet new guidelines. A manufacturer spends its own funds to investigate all its recipes and alter them if it wishes to

continue selling products in the United States. This type of regulatory compliance happens frequently, and the public may or may not know about the manufacturer's efforts.

HIPAA

The HIPAA (Health Insurance Portability and Accountability Act) was created in 1996 to protect the medical information of consumers. Access to electronic Protected Health Information (ePHI) must be controlled and authorized while data is at rest, in use, and in transmission. HIPAA allows patients more control over their medical data and dictates how organizations transmit and store that data. It provides consumer protection against sharing private information. Medical professionals are held to a strict code of confidentiality regarding patient records. For example, under HIPAA:

- Hospitals may not release the names of new mothers to baby formula companies. Physicians may not release the names of their allergy patients to allergy drug companies, which may then attempt to market directly to those patients. In either situation, release of patient names is at once an invasion of privacy and a conflict of interest.
- Patient information may not be sold to pharmaceutical companies, medical equipment manufacturers, or virtually any other manufacturer that produces a healthcare-related product. To do so would be considered an invasion of privacy.

FIGURE 3. A regulation is a rule made and maintained by an authority. Regulatory compliance is an organization's adherence to laws and guidelines relevant to its business. Organizations governed by an authoritative body comply with that body's current legislation. Businesses and organizations that practice the rules of the authoritative body are said to be "in compliance."

FERPA

The FERPA (Family Educational Rights and Protection Act) allows parents increased access to their students' records. Parents have the right to inspect school records in regard to their students. Should information be inaccurate, parents have the right to a hearing in an effort to correct the information. In general, parental consent is needed for any student records to be shared with other organizations or schools. For example, FERPA regulations:

- Prevent school officials from "selling" the educational interest of their students to publishing companies that would allow the companies to market directly to the students' homes.

- Prevent school officials from sharing information about students who have behavior problems with private schools that provide specialized curriculum for behavior issues. Such sharing could result in direct marketing to parents. The optimal outcome for a private school would be that families would send children to the new school.
- Prevent information from counseling sessions taking place within school walls from being shared with private companies. That information is sensitive and protected and must be stored on secure school networks.

SOX

The Sarbanes-Oxley Act of 2002 (SOX) is a federal law designed "to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes." (Source: The Act.) It establishes new regulations and expands existing ones for corporate boards and management and for the accounting firms with which they do business.

CHAIN-OF-CUSTODY PROCEDURES

Evidence

Evidence is anything presented in support of an assertion (statement, claim, allegation). The strongest evidence provides direct proof of the truth of an assertion. The **rules of evidence** are the laws and legal principles that govern the proof of facts in a legal proceeding. These rules determine what evidence must or must not be considered by the trier of fact in reaching its decision.

Recovery

Once a security event, incident, or data breach is realized/confirmed, the disaster recovery plan is activated. Investigations of incidents and breaches require several sequential events to occur, beginning with recovery.

Recovery is "the activities after an incident or event to restore essential services and operation in the short and medium term and fully restore all capabilities in the longer term." (Source: NICCS glossary.)

A **disaster recovery plan** is a documented process or set of procedures to regain lost control and protect an organization's IT infrastructure in the event of an unforeseen, damaging event: a plan to recuperate from the incident. It is part of the incident response plan but also maintains unique characteristics of its own. There are three types of disaster recovery plans: detective, preventive, and corrective.

Chain of Custody

Chain of custody is the "process of validating how any kind of evidence has been gathered, tracked, and protected on its way to a court of law." (Source: Sarah D. Scalet, "How to

Keep a Digital Chain of Custody," at http://www.csoonline.com/article/2118807/investigations-forensics/how-to-keep-a-digital-chain-of-custody.html.) It documents each person who handled the evidence, the date/time it was collected or transferred, and the purpose of the transfer. Proof of chain of custody is required for digital evidence to be admitted as a detailed account of the location of each document/file from the beginning of a project until the end. It verifies that no one altered any digital information in any way. Scalet recommends the following steps to safeguard digital evidence:

- Guard digital evidence. In the eyes of the court, "a carefully protected image of a hard drive is as good as the original hard drive."
- Create a second set of the best evidence for use as a working copy for the investigators.
- Follow a chain-of-custody plan that typically answers these six questions:
    1. What is the evidence?
    2. How did you get it?
    3. When was it collected?
    4. Who handled it?
    5. Why did that person handle it?
    6. Where has it traveled, and where was it ultimately stored?

Procedures to create a chain of custody vary depending upon the forensics provider. Providers generally follow a version of these steps:

- Step 1: Create documentation that provides the date and time the evidence was collected, where it was collected, who collected it, what exactly was collected, why it was collected, and how it was obtained.
- Step 2: Document all the places the evidence has traveled and who has had access.
- Step 3: Log errors produced by the analysis. **Logging** is the process of recording system events, such as errors, in a file that can be accessed for review.
- Step 4: Review all the information obtained by the forensics process to determine the organization's future steps to securing its network.

Forensics

Forensics is the processes and specialized techniques for gathering, retaining, and analyzing system-related data (digital evidence) for investigative purposes. "Computer forensics is the equivalent of surveying a crime scene or performing an autopsy on a victim." (Source: James R. Borck, "Leave the Cybersleuthing to the Experts," *InfoWorld*, April 9, 2001.) A company investigating breaches typically collects evidence that includes snapping an image of its digital infrastructure while executing the recovery plan.

An **image** is "an exact bit-stream copy of all electronic data on a device, performed in a manner that ensures that the information is not altered." (Source: NIST glossary.) Devices

include servers, workstations, and other networked operating systems. Images are examined for differences from the normal operating state of the organization's network and used as evidence. The investigation team assembles all collected evidence and reviews it in an effort to determine the source of the breach and to provide the proof needed to penalize the guilty party.

FIGURE 4. An image is "an exact bit-stream copy of all electronic data on a device, performed in a manner that ensures that the information is not altered." (Source: NIST glossary.) This portable write blocker is attached to and copying a hard drive for forensic purposes. (Source: Wikipedia.)

According to Rodney McKemmish ("What Is Forensic Computing?," *Trends & Issues in Crime and Criminal Justice*, June 1999), computer forensics is "the process of identifying, preserving, analyzing, and presenting digital evidence in a manner that is legally acceptable."

- Identifying: Identifying evidence that is present, where and how it is stored, and the operating system that is being used is essential. This step assists in conducting the appropriate recovery strategy.
- Preserving: Preserving maintains the integrity of the digital evidence and ensures that the chain of custody is not broken. This step includes copying the evidence to stable media and using reproducible methodologies. The steps used to capture the data are also documented.
- Analyzing: The data copied to stable media is reviewed and examined without risk of damaging the data's integrity.
- Presenting: Digital evidence is presented in a legally acceptable and understandable manner. A judge and jury must understand what is being presented and how it relates to the case.

Giving up evidence to the court should be avoided unless absolutely necessary. A digital image is not always needed. Rather, writing a legal document that describes the evidence and then providing the credentials of the individuals who examined the evidence will often serve the purpose.

Open-source forensic software is a program that analyzes source code or binary code to determine whether intellectual property infringement or theft occurred. Open-source software is free to all for use and modification. A company will use open-source software to investigate breaches and abnormalities found in its network. Such software has become the centerpiece of lawsuits, trials, and settlements when disputes over software patents, copyrights, and

ON THE JOB...

CAREER CONNECTION: Cyber Investigator

Cyber investigation is a relatively new career cluster. Network security is nothing new, but as the volume of cyber events grows each year, a forensic cyber investigation industry has been spawned. While the basic elements of cyber investigation are constant, the techniques, strategies, and footprint of the hacker on a network is a moving target. It is up to investigators to stay ahead of the game and "study up" on the latest research and tactics to combat cyber attacks.

The FBI plays a major role in the investigation of many cyber crimes. Its jurisdiction spans the Internet and often deals with hacks originating from overseas servers. FBI cyber investigators are involved in the recovery process. To find out more about careers in cyber investigation at the FBI, visit the agency's Cyber Crime web page at https://www.fbi.gov/investigate/cyber.

The FBI's Criminal, Cyber, Response, and Services Branch (CCRSB) oversees all computer-based crime related to counterterrorism, counterintelligence, and criminal threats against the United States. The CCRSB deploys FBI agents, analysts, and computer scientists and uses traditional investigative techniques, such as sources and wiretaps, surveillance, and forensics.

trade secrets occur. Forensics software is run against an image to identify various characteristics sorted for analysis.

Sleuth Kit is open-source forensics software that, among other commands, returns files sorted by file type. Many breaches use specific file types to infiltrate, and when the software returns these files sorted by type, the investigation is made more focused and less time consuming. [NOTE: A Sleuth Kit example is found on the rationallyPARANOID website at http://rationallyparanoid.com/articles/sleuth-kit.html.]

In contrast, a **heuristic software program** is a program that looks for known sources, common text phrases, and other patterns derived from previous knowledge to scan network emails. An employee could have possibly launched the breach by allowing a virus to run through a devious email attachment.

Summary:

Security is the protection of data from threats by controlling how the data is used, consumed, and provided. Security programs are designed to keep an organization secure daily, whereas compliance regulations change slowly and rarely catch up with the constantly changing security environment. The basic rule of cyber security compliance is, "We trust but verify."

An incident is a "violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices." (Source: NIST glossary.) Its actual or potential result is an adverse consequence to an information system or the information that the system processes, stores, or transmits. A response action may be required to mitigate the consequences. A data breach is the intentional or unintentional release of personally sensitive, protected, and/or confidential data, such as social security numbers and personal health records.

Regulatory compliance is an organization's adherence to laws and guidelines relevant to its business. Organizations governed by an authoritative body comply with that body's current legislation. Businesses and organizations that practice the rules of the authoritative body are said to be "in compliance."

Chain of custody is the "process of validating how any kind of evidence has been gathered, tracked, and protected on its way to a court of law." (Source: Scalet.)

Checking Your Knowledge:

1. Differentiate between security and compliance.
2. At what point does an incident become a breach?
3. Describe the relationship between regulatory compliance and consumer protection.
4. How do cyber investigators use image, forensics, and heuristics?
5. What is the advantage of using open-source software?

Expanding Your Knowledge:

The threat of cyber attacks keeps network administrators alert. You can easily find stories of hackers and spammers infiltrating companies and organizations. These threats may span the spectrum from interfering with personal interest to jeopardizing national security and are handled on a case-by-case basis. If our nation is compromised through digital means, our lifestyles could be altered forever. Find three websites with cyber attack statistical information. Compare and contrast the three sets of figures. What can you generalize from the facts, figures, and statistics?

Web Links:

Cybersecurity: Legislation
https://www.lawfareblog.com/topic/cybersecurity-legislation

How to Catch Threats Anywhere on Your Network with AlienVault USM (video)
https://www.youtube.com/watch?v=P93XR4qYwuo

Legal Considerations
http://www.iacpcybercenter.org/topics/legal-issues/