COMPASS
IT Compliance

Role of Digital Forensics in Cybersecurity

DANIELLE CORSA
GEORGE SEERDEN 2/28/18

Secure. Comply. Save.

COMPASS
IT Compliance

Agenda

- Digital Forensics Defined
- Types of Investigations
- Forensic Process; Roles & Responsibilities
- Forensic Considerations in Cybersecurity
- Preparing for a Forensic Investigation

COMPASS
IT Compliance

What is Digital Forensics?

- Computer forensics is the application of investigative and analytic techniques to collect and preserve the integrity of evidence from a device using reputable industry tools that are suitable in a court of law.
- The objective is to perform a thorough, forensically sound investigation while maintaining a documented chain of evidence to find out exactly what happened on a computing device and who may have been responsible for it.

COMPASS
IT Compliance

Types of Investigations

COMPUTER BASED

a computer(s) is used as the ***vehicle*** to commit a crime (child pornography, cyberbullying, cyberstalking, spamming, financial fraud, etc.)

COMPUTER FACILITATED

a computer is the ***target*** of a crime (hacking incident or information theft)

COMPASS
IT Compliance

Types of Investigations cont.

COMPUTER BASED

DEAD Analysis

evidence is collected in forensically sound manner and analyzed in a lab by a forensic examiner on an unnetworked standalone system using forensic tools

COMPUTER FACILITATED

LIVE Analysis

capture volatile information from RAM and other running processes, including networks.

COMPASS
IT Compliance

Forensic Process

- **DATA COLLECTION**
  - Obtain Search Authority (law enforcement only)
  - Document Chain of Custody
  - Data Acquisition
  - Image and Hash Verification

COMPASS
IT Compliance

Forensic Process cont.

- **EXAMINATION/ANALYSIS**
  - Validate Tools
  - Perform Analysis
  - Reproduce Findings (QA)

COMPASS
IT Compliance

Forensic Process cont.

- **REPORTING**
  -Deliverables: Technical & High Level Exec. Summaries
  - Chain of Custody
  - Expert Testimony in Court of Law (if needed)

COMPASS
IT Compliance

Forensic Process Summary

- The forensic analyst combines investigative procedures and computer science to conduct, handle, analyze, and report on evidence to present an objective opinion on the facts without prejudice.

COMPASS
IT Compliance

Forensic Considerations to Handle Cyber Incidents Effectively & Efficiently

- Perform and maintain regular system backups for a specific period of time
- Maintain regular audits of workstations and educate your employees on best practices
- Maintain database of file hashes of applications and OS.
- Regularly use file integrity software on important assets
- Maintain records of network and system configurations
- Establish a data retention policy that supports a historical review of system and network activity

Secure. Comply. Save.

COMPASS
IT Compliance

How to Prepare for a Forensic Investigation

- Observe company/employee right to privacy policies and procedures (i.e., probable cause with the exception of consent, hot pursuit or plain view)
- Secure perimeters; isolate computer of interest from network, if possible
- Remove any subjects of interest from accessing the computer/cell phone
- Gather all passwords, system logs, admin credentials
- Document any peripherals attached, time clock, documents open on desktop

COMPASS
IT Compliance

Resources

ISACA Overview of Digital Forensics

SWGDE Best Practices for Computer Forensics

Secure. Comply. Save.

COMPASS
IT Compliance

Contact Information

Danielle Corsa

Forensic Analyst

dcorsa@compassitc.com

George Seerden

Forensic Analyst

gseerden@compassitc.com

Secure. Comply. Save.

COMPASS
IT Compliance

Questions?

Secure. Comply. Save.