Incident Response: Investigating Computer Crime

Chris Prosise; Kevin Mandia; Inc NetLibrary

Evidence Technology Magazine - Computer Forensics Dec 28, 2001. This is one of the first books available that explains what to do after you’ve been hacked. Written by FBI insiders, this book reveals the computer crime investigation and computer forensics. It’s significant that the first edition’s title was Incident Response: Investigating Computer Crime. Authors Chris Prosise and Kevin Mandia provide an insider’s look at the legal, computer security, and computer crime investigation aspects. This article discusses incident response issues and then provides detailed guidance on the role of information technology in fraud response, computer crime investigation and computer forensics.

- **Intrusion cases**: These incidents range from organized crime to cyber attacks and data breaches.
- **Criminology**: The FBI will seek to collect digital evidence of cyber crime and incident response to address cyber law enforcement agencies in investigating cyber crime. The Federal Bureau of Investigation (FBI) estimates that computer crimes affect our daily lives and national security.
- **Computer incident response plan**: The planned response to any given incident is crucial. This plan should be formulated, and a Computer Security Incident Response Team (CSIRT) should be formed to respond to any computer crime.
- **Digital Intelligence and Investigation Tools**: These tools are necessary to perform successful investigations that involve technical evidence.
- **Fraud and Forensics**: The effective response to computer crime requires a multidisciplinary science that resolves computer crime and complex legal issues.
- **Chronological methodologies and technical computer crime**: Investigating Computer Crime - ACM Digital.
- **Computer Hacking Forensic Investigation**: The process of detecting hacking attacks and properly extracting evidence to report the crime and conduct audits to prevent future attacks. The CHFI Incident Response: Investigating Computer Crime - SC Magazine.
- **Computer response to any given incident**: The planned response to any given incident (including the investigation) is crucial. This plan should be formulated, and a Computer Security Incident Response Team (CSIRT) should be formed to respond to any computer crime.