

Fostering Incident Response and Digital Forensics Research

Bruce J. Nikkel
nikkel@digitalforensics.ch

October 4, 2014

Abstract

This article highlights different incident response topics with a focus on digital forensics. The purpose is to identify areas of recent change or areas in need of deeper understanding and exploration, and to foster further research and study in the field.

Introduction

IT incident response, especially in the private sector, typically focuses on re-establishing the defenses of IT infrastructure, patching vulnerabilities, filtering and blocking malicious activity, cleaning up damage, and reporting to management. Digital forensics, if it is included at all, is often seen as a peripheral or secondary priority in managing incidents. The typical incident landscape has changed over the past few years, becoming more complex, more global, and typically involves multiple organizations. There are growing benefits to positioning digital forensics as a central and fundamental component of incident response, and conversely, there are increasing risks to leaving it peripheral. This article encourages further research and advancement in the area of incident response in relation to digital forensics, and presents a number of areas where further study would be valuable to the community. The types of research include both theoretical and practical, and may include abstract conceptual models, legal research, standard operating procedures, creating international standards for evidence exchange, and developing technical capabilities for acquisition and analysis of digital evidence across multiple jurisdictions. The examination of incident case studies is also encouraged to identify 'real world' factors contributing to successful outcomes, and revealing pitfalls to avoid.

Global Organizations

If you are on the Internet, you are a global organization. Your organization is accessible from around the world, and can be targeted by any malicious group or individual. The implications to forensics here are primarily jurisdictional. For example, suppose an organization is located in country A, has an incident involving an attacker from country B, who uses anonymizer/relay services in country C, to compromise infrastructure via an outsourcing partner in country

D, and finally exfiltrates data to a dropzone in country E. This example crosses five jurisdictions and is typical of incidents today. Collecting digital evidence for incidents involving multiple countries and jurisdictions is a challenge, especially in cyber-criminal incidents where multiple law enforcement agencies may need to be engaged. There are opportunities for research here, to explore cross border and multi jurisdictional aspects to incident response, evidence collection, evidence exchange, the role of threat intelligence, and forensic investigation processes.

Forensic readiness

Forensic readiness is a decade old concept that many organizations have taken steps to address and implement. It involves taking steps of preparation in anticipation of a particular type of incident. This includes ensuring adequate logging for monitoring, detection, post-mortem investigation, and event reconstruction. It includes enabling investigative access into IT infrastructure, and developing investigation and incident response processes in advance. It may include testing playbooks and running exercises. There have been recent industry cyber exercises that various organizations have participated in, sometimes coordinated by regulators and governmental bodies. Forensic readiness ensures that adequate staff, training, tools, and external support (retainer contracts, partnerships, etc.) are all in place in advance. In the event of an incident, appropriate action can be swiftly taken to manage the incident, collect and preserve forensic evidence, investigate the incident to conclusion, and appropriately communicate to relevant parties (both internally and external to an organization). Forensic readiness is becoming a crucial part of risk management, and good incident preparedness helps to increase efficiency, reduce the costs of incident response, and help organizations prioritize resources. While forensic readiness is well developed today, it tends to be internally focused in organizations. In the area of multi-party outsourcing arrangements in particular, forensic readiness needs further research and study with regard to incident response and digital forensics.

Further Understanding Incidents

Responding to incidents and triggering appropriate forensic processes depends on the type of incident experienced. There are criminal incidents which may need law enforcement involvement, policy violations which may trigger internal organizational processes, industry specific incidents which may require regulatory reporting or involve regulatory bodies, incidents which may lead to civil litigation activity (either for or against an organization), and also "accident" incidents which might not be a violation at all, but still have an impact on an organization. All of these incident types may affect how incident response is conducted, and influence the corresponding digital forensic activity needed. Research work to more clearly describe the different incident types in this context would be helpful in further developing appropriate digital forensic processes and strategies. Comparative analysis and the use of case studies will help to illustrate the various incident types, their similarities, differences, and challenges faced.

Industry Specific Incidents

There are many types of incidents that affect all industries. For example, malware outbreaks, DDoS attacks, website defacements, spam waves, etc. affect all organizations. There are also incidents that are more industry specific, and create a heightened threat to some organizations, while being less of a problem to others. For example, the banking industry deals more with phishing attacks and banking malware targeting online banking applications, the music and entertainment industry deals more with copyright violation issues like file sharing, the pharmaceuticals industry deals more with intellectual property theft that may lead to cloning/copying drugs, internet marketing and advertising firms deal more with click fraud, etc. Each industry has a particular pain point that they deal with more than their peers in other industries. It is useful to recognize and understand those incident types that affect each industry, and give them special consideration and focus when developing incident response and forensic capabilities. There are possibilities for research here, in particular, clearly understanding and documenting industry specific incidents, and providing guidance to incident responders and forensic practitioners working in those affected industries.

Changing Infrastructure Landscape

In the past, organizations had a good overview of their infrastructure and IT asset inventories, but this is becoming more difficult. BYOD is becoming more popular, staff are increasingly using mobile devices, more infrastructure is becoming outsourced and/or operated in external cloud environments. Even the notion of a physical "system" or "device" is changing as both servers and client desktops become virtualized. This has an impact on digital forensics as traditional forensic methods in some cases can no longer be conducted in the same way (SSD and flash memory for example). There are also new opportunities and advantages arising, such as the trend towards increased logging (big data), new capabilities such as CoW (Copy on Write) filesystems allowing multiple snapshots across time, and the ability to dump live memory with ease on virtual machines (without affecting the running VM system). While much work is being done to understand technical forensic acquisition and analysis capability in these areas, there is room for further study in linking this with incident response and developing end-to-end integrated processes.

Pan-Organizational Aspects

Cyber security incidents have moved well beyond traditional borders of IT and IT infrastructure. Today, cyber security incidents typically involve multiple areas of an organization. In addition to IT, these may include financial departments, public relations units, human resources, legal and compliance teams, corporate security departments, and other non-IT areas. Cyber incidents are no longer limited to technical exploitation of vulnerabilities, but today include social engineering, social media incidents, cyber-bullying, intellectual property infringement, brand abuse, and direct business impacting incidents. It includes industry specific incidents like financial fraud, targeted phishing, click

fraud, industrial espionage, employee data leakage, and other incidents taking place outside the traditional IT infrastructure domain. Larger organizations are also starting to experience a split between traditional digital forensics and e-discovery, and new incident response teams are becoming established outside the traditional incident response homeland of IT departments. These relatively recent changes need closer examination and understanding to guide organizations in planning their forensics and incident response activities.

Emotional Response

Depending on the severity or frequency of a particular incident, it may generate an emotional response from people affected. People involved in the incident may experience fear, anxiety, anger, shock, or excitement. These human emotions can adversely affect the process of incident response and forensic investigation. The people directly affected (the individual victims), the people who discovered and reported the incident, the people overseeing or managing the impacted business, and even the incident responders themselves, all have emotional reactions which need to be recognized and managed. These emotions may compromise incident response processes through over-reaction, increased risk of error, interference, and impulsive decision making. There are often two opposing forces at play during an incident, one side wants to clean up and contain the incident as fast as possible, the other side wants to take time to gather evidence and understand what is happening (while it is happening). For example, in some APT incidents, leaving things vulnerable or broken a little bit longer for observation, forensic evidence collection, or for investigative purposes to understand the malicious activity better, could be highly beneficial. In cases where malicious activity has been ongoing for weeks or months, letting it continue for additional hours or days might not add significant increased risk to the organization. But the emotional impulse to hurriedly shut everything down could result in more damage in the long term, and compromise investigation attempts. This illustrates an interesting area of incident response where the social and psychological aspects could be more clearly understood. Such research would make organizations more comfortable in such situations, and less impulsive in reacting to serious malicious or criminal activity.

Threat Intelligence

In recent years, threat intelligence has become important, especially in large complex organizations. Threat intelligence may come from sources both internal and external to an organization, and may be both open source and from commercial vendors selling threat intelligence data feeds. This information is useful to identify new vulnerabilities and newly discovered threats, identifying stolen data (often from analyzing compromised datasets published to the Internet by anonymous third parties), and for identifying past compromises. The correlation of various data sources using analytical methods can also be used to discover incidents that were not otherwise detected. Threat intelligence is useful for short term operational/tactical actions, and may trigger new incident response processes, or aide ongoing investigations. Threat intelligence can be

useful for more strategic purposes, allowing management, architecture and design teams, risk units, etc. with longer term planning, resource allocation and prioritization. Industry specific intelligence sharing groups and communities also exist to facilitate threat information sharing between similar organizations, and a corresponding set of protocols such as STIX and TAXII are being introduced. There is a need to more formally research and develop the integration of current threat intelligence activity into existing incident response and forensic investigation models.

The Internet of Things

Is your toaster on the Internet yet? The Internet of things promises to connect everything to the Internet. This provides a number of new possibilities for investigation and forensics. Embedded devices in home appliances, entertainment systems, wearable computers, personal health monitors, electronic medical devices, smart cars, smart buildings, etc. are all potential evidence sources (often rich with timestamps). Many of these connected devices are sending continuous telemetry data to remote servers or clouds. These sources can be useful for event reconstruction when managing incidents and conducting forensic investigations. Continued research into embedded device analysis and the corresponding network activity could enable new ways of reconstructing and correlating past events and allow more thorough evidence collection when responding to an incident.

Privacy and Ethics

Although privacy and ethics are the last topic of this article, they are arguably the most important. Traditionally the boundaries surrounding forensic and incident response activity have been largely defined by technological, legal, and organizational policy constraints. But a fourth boundary, ethics, is growing in importance. Technology and tools are becoming more powerful and more invasive. Information is retained longer, correlation and analytics of big data allows further derivation of information. More people have easier access to sensitive incident data over longer periods of time. All of these factors are driving the need to explore voluntarily set ethical boundaries to reduce the risk of abuse, and protect the privacy of individuals touched by incident response and forensic investigation activity. Research on the topic of ethics and privacy related to investigation and response capability is becoming increasingly important.

Conclusion

This article has presented a number of new challenges and room for further research and study in the field. Readers are encouraged to advance the current state of knowledge in this field, especially in the context of forensic investigation as it relates to incident response.