



Forensic Incident Response

What to Do in Case of a Security Incident

Contents

- 3 Purpose**
- 3 Background**
- 4 What is Forensic Incident Response?**
- 4 Does This Apply to My Business?**
 - 4 Would a breach of security have a major impact on our organization?**
 - 5 Can our information be accessed by unauthorized users?**
 - 5 Do we work with sensitive information?**
- 5 Where to Start**
 - 6 Standard Incident Response Methodology**
 - 6 Initial Incident Response**
 - 7 Investigative Methodology**
- 8 Evidence Collection**
- 9 Vulnerability Scanning**
- 9 Evidence Processing**
- 10 Reporting**
 - 11 Areas of Consideration**
 - 11 Classification of Information Involved**
 - 12 Criticality of Systems Involved**
 - 12 Desire to Restore Operations A.S.A.P.**
 - 12 Technical Complications**
 - 13 Desire to Criminally Prosecute**
 - 13 Desire to Receive Civil Restitution**
- 13 Choosing a Forensic Incident Response Team**
- 14 Trends in Incident Response**
- 14 IBM Emergency Response and Forensic Analysis Services**
 - 14 Immediate Incident Management and Attack Response**
 - 15 Computer Forensic Analysis, Discovery and Litigation Services**
 - 15 Incident Preparedness Planning**
- 15 Conclusions**
 - 16 About the Author**
 - 16 About IBM Professional Security Services**
 - 17 About IBM Emergency Response Service**
 - 17 About IBM Internet Security Systems (ISS)**

Purpose

Organizations involved in collecting, processing, storing, or transmitting sensitive information need to understand what to do when a compromise is detected or reported. This whitepaper will explain the concepts associated with forensic incident response and describe many of the various actions that can be taken during a security incident. In addition, this whitepaper will outline the benefits of preparing for an incident as well as the potential ramifications for not being prepared.

Background

Safeguarding customer data has become increasingly important to our society over the last few years. As more personal data becomes compromised via the Internet, it is clear that protecting information is extremely difficult and becoming a victim of identity theft is more likely. As a result, lawmakers and industries have enacted legislation and standards that require the timely investigation and notification of suspected security breaches.

On September 25, 2002, the Governor of California approved Senate Bill 1386 which states that “Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.”

In 1996, congress passed the Health Insurance Portability and Accountability Act (HIPAA) and tasked the Department of Health and Human Services (HHS) to draft the HIPAA Privacy Rule which became effective on April 14, 2003 and requires covered entities to adopt incident reporting procedures, although according to HHS, “This regulation does not specifically require any incident reporting to outside entities. External incident reporting is dependent upon business and legal considerations.”

In January 2005, in a collaborative effort between Visa and MasterCard, the Payment Card Industry (PCI) Data Security Standard was placed into effect requiring that “A member or the member’s service provider, or a merchant or the merchant’s service provider must immediately report the suspected or confirmed loss or theft of any material or records that contain Visa cardholder data.”

What is Forensic Incident Response?

Broadly defined, forensic incident response is the process of reacting to known and unknown host and network events and subsequently analyzing these events for anomalous and unauthorized activity while collecting and preserving evidence for presentation in legal proceedings.

Does This Apply to My Business?

Not all organizations are absolutely required to conduct a forensic incident response assessment when a security breach is discovered or reported. Although regulatory requirements and other standards may not apply to your organization, best practices suggest that organizations have an incident response plan that is tested and updated on a regular basis. Even the smallest organizations who do not think they would be targeted or impacted by an incident are at risk. If you are not already a believer, ask yourself the following questions from a risk-based perspective:

Would a breach of security have a major impact on our organization?

A security breach can have many effects on an organization from bad publicity to loss of available resources, both negatively impacting brand name, customer retention and ultimately, the bottom line. Additional liabilities associated with a security breach may stem from civil contractual obligations to customers to protect information, regulatory fines and sanctions, or in some cases, criminal charges.

Can our information be accessed by unauthorized users?

If the infrastructure is accessible from the Internet or other remote means such as dial-up or wireless access, it is inherently vulnerable, to some extent, regardless of preventive and detective IT security. If your organization uses laptop computers and other mobile devices, the information on these devices can be lost, misplaced or stolen.

Eighty-one percent of companies surveyed reported the loss of one or more laptops containing sensitive information during the past 12 months, according to the survey, which queried nearly 500 information security professionals.

Do we work with sensitive information?

Sensitive information can be proprietary, private, protected, regulated, privileged, confidential or secret. Certain legal requirements and customer expectations require investigations of suspected breaches where this type of information may have been involved. In addition, organizational policies and procedures may require investigations and can have significant administrative ramifications.

If there is uncertainty as to whether specific requirements apply to your business, IBM Internet Security Systems™ (ISS) recommends seeking further advice from legal counsel.

Where to Start

Follow your approved Computer Security Incident Response Plan (CSIRP). If you do not have a CSIRP and you are experiencing a current incident, this paper can help assist you in making decisions. However, forensic incident response is a field that requires experience and expertise to be successful. If the requisite specialty skills do not exist within your organization, consulting a professional trained in incident response and forensics is highly recommended.

Standard Incident Response Methodology

There are a number of different incident response methodologies that can be found on the Internet. Generally, these methodologies will consist of the following phases:

- 1. Planning*
- 2. Identification*
- 3. Confirmation*
- 4. Containment*
- 5. Preservation*
- 6. Analysis*
- 7. Eradication*
- 8. Remediation*
- 9. Reporting*

The methodology chosen by an organization or vendor should conform to best practices such as ISO 17799 (27001).

Initial Incident Response

Typically it is a good idea to start by drafting a high-level description of the incident. This might include the type of activity in question, when it was discovered and by whom. Because a suspected incident can be legitimate anomalous activity or the result of an improper configuration, it is necessary to confirm that the activity is truly malicious or unwanted. Once the incident has been confirmed, then the extent of the compromise should be determined. Although the extent may not be fully known for some time, it is best to get an idea of how many systems are involved or affected, what the primary role and criticality of each system is, and how these systems are configured. The availability of applicable host-based logs should be determined.

It is necessary to obtain a current understanding of the network architecture including subnets, security and network devices, and external connections. Methods established for remote access such as dial-up or Virtual Private Networking (VPN) should be scrutinized carefully. If recent changes have been made to the architecture or infrastructure, these changes should be noted as they may have created an unexpected or unintentional vector for compromise. The availability of applicable network device logs and content captures should be determined.

Any current host- or network-based vulnerabilities known to exist within the environment should be discussed as possible leads to investigate. All potential clues identifying the attack vector used or applications involved should be listed and reviewed by the response team at this time. Depending on the evidence presented, a determination should be made as to whether the incident resulted from a manual or automated attack.

Systems should be queried to see if unknown user accounts exist. If a root\ admin level compromise is suspected to have occurred, the passwords for these accounts should be changed. Critical and sensitive files can be examined for modifications, especially if file integrity monitoring is in place. Systems should also be examined for hidden processes and unexplained encrypted files or encrypted traffic. Additionally, the most relevant backup tapes should be secured for potential forensic analysis provided the logs are not present. All actions taken and commands entered by first responders should be documented thoroughly to include the system name, time and exact syntax.

Investigative Methodology

Although there is no silver bullet for all security incidents, there are several reactive hands-on steps that should be taken to limit the overall risk associated with the incident. Because each case involves different components, the decision regarding which steps apply in any given situation will be based on the unique circumstances of the case. This will generally include ongoing inquiry, collection of evidence and forensic analysis.

Evidence Collection

Normally, unless there are unfortunate circumstances, an analyst should begin collecting the most volatile data first and then capture persistent data. Volatile data is data that is no longer available without power to the system. Persistent data is data that is physically written to some form of magnetic media. All evidence collected and the procedures used should be documented extremely well, verified and validated using a hashing algorithm, and maintained in a strict chain of custody.

Finally, if applicable, the analyst should also concurrently begin collecting real-time network traffic to monitor ongoing activities and ensuing analysis as this is also volatile in nature. Capturing live content can provide insight into unusual network activities, large file transfers and the execution of remote commands. When reviewing content on a system, the responder needs to be sure that explicit authorization exists so as to not violate individual civil liberties and privacy rights.

Memory is the most volatile data that is found on a system. Depending on the operating system, memory is physically written to a pagefile or a swapfile and may be found on magnetic media if the system was improperly shutdown, but it is not always a safe bet to assume that remnants of memory will be found on a system after the power has been turned off. Since memory can contain extremely valuable evidence, it should be collected unless there is a specific reason or need not to do so.

The next most important thing to gather would be the remaining volatile data. In order of volatility, network connections should be collected prior to running processes. Both network connections and running processes change less often than memory changes, therefore they are less volatile. However, they often provide some of the best leads and evidence relating to a remote attacker. In addition, network connections and running processes tend to help identify what a remote attacker is doing on the system, and what information may be leaving the network.

After volatile data is collected, the responder should begin collecting persistent data. The choice regarding which systems to start with should be based on information gathered thus far and may involve the use of several different techniques. Provided the techniques used are forensically sound, or can otherwise be explained in a court of law if no forensically-sound options are viable, the responder should be given the freedom to choose the most appropriate technique.

Generally, a physical acquisition of magnetic media is considered to be the best evidence and this method should be used whenever practical. In cases where an extraordinary amount of data is considered to be within scope, the analyst may choose to preview certain systems prior to acquisition and simply acquire the logical files needed. Another possibility in these types of cases would be to use a forensically-sound script using statically linked binaries to collect the most pertinent, logical evidence files. Whatever choice is made, both the responder and incident manager need to be aware of the implications of collecting a physical versus a logical image.

Vulnerability Scanning

When responding to an incident, it is often beneficial to know the specific current weaknesses that exist within the environment in question. Conducting a vulnerability scan can provide this information to the analyst who can in turn use the information to potentially identify the attack vector used. This information also helps the analyst see the infrastructure in a manner that provides system information and configuration details.

Evidence Processing

Properly processing evidence is usually the most time-consuming phase of an investigation. There are a variety of different tools and techniques that can be used to accomplish this task. Below are a few of the most common, standard computer forensic evidence processing techniques.

Volatile Evidence Analysis

Volatile Evidence Analysis gives the analyst the ability to see what state the system is currently in by peering into connections, processes and cache tables.

Timeline Analysis

Timeline Analysis is the process whereby a timeline of events is created and analyzed based on the modified, accessed and changed times associated with all files that were imaged.

System File Analysis

System File Analysis refers to analyzing system binaries for unauthorized changes.

Data Recovery

Data Recovery includes recovering and analyzing deleted files that have not been overwritten, as well as carving out portions of files and text from unallocated and slack space.

String and Keyword Searching

String and Keyword Searching involves looking at known and unknown files, as well as unallocated and slack space, to identify readable text within a binary file or to find a file that contains a specific string.

Reporting

The success of a forensic incident response engagement depends on the ability to show evidentiary integrity and report in a factually accurate manner. A formal report should be written in the requested format providing an executive summary and all of the requisite details. The formal report should contain at a minimum, a high level summary, background information, compliance status if applicable, the investigative procedures used, all positive and negative findings, and evidence disposition. The report should also include additional mitigation and remediation recommendations for all items not in keeping with industry or security best practices.

Areas of Consideration

Areas of concern that will impact the actions taken during an investigation may include:

Classification of Information Involved

Organizations should consider risk when making decisions on how to proceed with an incident investigation. When systems on or adjacent to a network involved in collecting, processing, storing, or transmitting sensitive information are suspected to have been compromised, the risks associated with the intrusion are higher and are directly proportional to the classification level. For example, if an organization uses the following information classification levels, then the lowest risk resides with Level One and the highest risk resides with Level Three:

- *Level One (Public) – Information is available to the general public and is not restricted in any manner. Investigations are typically not required or requested provided that the information within or adjacent to the compromised network is not sensitive in nature. However, investigations are often requested or conducted in order to understand what happened and fix the associated weaknesses.*
- *Level Two (Proprietary) – Information is deemed somewhat sensitive but can be protected appropriately. Investigations are conducted at the proclivity of the organization, provided that the information within or adjacent to the compromised network is not protected by law.*
- *Level Three (Private) – Information is regulated and must be protected by law in the specified manner. The information is restricted to a limited number of authorized personnel based on role and the need to know. Investigations are generally required and reporting/notification is often required as well.*

Criticality of Systems Involved

In many cases, the systems involved in an incident are highly critical to the organization's mission and therefore may not be taken offline. When systems may not be taken offline, an additional burden is placed on the analyst to properly collect live evidence. While this is relatively simple for a trained responder to do, it can be complicated and generally increases the amount of time required to collect evidence.

Desire to Restore Operations A.S.A.P.

The desire to restore normal operations as soon as possible can have a significant impact on the ability to collect relevant evidence for investigation. Therefore, it is important to consider that continuity of operations may heavily depend on your organization's ability to analyze an incident and not necessarily just the ability to restore from backup tapes. If the attack or automated malicious code is not properly analyzed, the event could easily reoccur or may actually remain dormant within the environment on systems that were not identified as being involved or affected.

Technical Complications

During an investigation, any number of problems can occur ranging from complex configurations and the use of proprietary hardware to uncommon or outdated operating systems and proprietary software. If the potential complication is known ahead of time, planning can be done to address the situation. If the potential complication is simply unknown, then decisions will need to be made on the fly. An experienced analyst usually will be able to foresee these potential complications or make appropriate decisions spontaneously.

Desire to Criminally Prosecute

The latest trends indicate that cybercriminals are motivated primarily by financial gain. While this makes quite a bit of sense, it is not the only motivation for conducting illegal activities on-line. Depending on the type of incident and the attack vector used (Worm, Botnet, Backdoor, DDOS or Active Attacker), an attorney may be able to show knowledge and intent. These are two critical elements of fraud that should be considered when gathering evidence during an investigation. While gathering all potential evidence may increase the time and effort to complete the investigation, if the goal is to criminally prosecute the perpetrator then it is necessary to look at all evidence, both incriminating and exculpatory.

Desire to Receive Civil Restitution

Often an investigation will uncover the identity of an attacker or the responsible parties. If the investigation is done properly, and the identity of the perpetrator is known, an organization may be able to collect damages from the perpetrator or the organization that the perpetrator is working for. If an organization conducts an investigation with this goal in mind, it will typically increase the amount of time and effort required to get the job done.

Choosing a Forensic Incident Response Team

When choosing an external vendor to augment or act as the forensic incident response team, diligent scrutiny should be given to the following items:

- *Experience and qualifications of the team*
- *Ability to respond in a timely manner*
- *Tools and techniques used by the team*
- *Availability of ancillary resources*
- *Financial position of the vendor*

Trends in Incident Response

Industries are beginning to require qualified, comprehensive response to security breaches in order for organizations to continue operations in good standing. Even if your organization has the capability to conduct incident response internally, it may be required to use an external qualified forensic incident response assessor to provide objectivity.

IBM Emergency Response and Forensic Analysis Services

IBM Emergency Response Services (ERS) include incident response, preparedness planning and forensic analysis conducted by our security experts. Available both as a subscription service and as an on-demand service, the ERS team responds quickly to attacks in progress 24x7x365 and works with your organization to develop customized emergency response plans to minimize the effect of future attacks. In addition, security experts can assist with computer forensic analysis, discovery and litigation to help find and prosecute perpetrators of information security breaches.

Immediate Incident Management and Attack Response

The IBM Internet Security Systems emergency response team responds 24x7x365 to stop attacks in progress, minimizing the effects of an information security breach. IBM ISS security experts follow a thorough incident response methodology, including:

- *Analysis – analyzing incident data to determine the incident source, cause and effects.*
- *Containment – preventing the spread of the incident’s effects to other computer systems and networks.*
- *Eradication – stopping the incident at its source and/or protecting your computer systems and networks from the incident’s effects.*
- *Recovery – restoring the affected computer systems and networks to normal operation.*
- *Prevention – ensuring that your computer systems and networks are protected from future occurrences of the incident.*

Computer Forensic Analysis, Discovery and Litigation Services

The IBM ISS expert consultants are available to support criminal, civil and administrative matters resulting from an information security breach. These efforts include assisting organizations with forensic examination of digital evidence and media in the following areas:

- *Employee/insider investigations*
- *Pre-discovery consulting*
- *Electronic evidence discovery*
- *Expert witness support*

Incident Preparedness Planning

Our ERS experts can help you prepare a customized emergency response and business continuity plan so that your organization is prepared for action in the event of an attack. Your customized plan will help you stop attacks quickly, limit their impact, recover lost data, as well as properly protect and analyze the forensic evidence.

Conclusions

Legislation and regulations have evolved as the threat landscape has evolved. Organizations that collect, process, store or transmit sensitive information need to be prepared to respond to incidents in an efficient and effective manner to avoid legal problems, maintain compliance and protect their brand name.

While conducting a forensic incident response assessment is not required in all cases of a security breach, certain legal requirements and customer expectations require investigations of suspected breaches. Best practices suggest that organizations maintain an incident response plan. Being prepared in advance may prove extremely helpful in tracing the origin and impact of security incidents, prosecuting the perpetrators and even recovering damages. Choosing an experienced forensic response team often yields the best results.

About the Author

Jeffrey Palatt is a manager with the IBM Internet Security Systems X-Force® Emergency Response Services Forensic and Litigation Support Team, bringing nearly ten years of experience as a professional in assurance and advisory services. He has been with IBM Internet Security Systems since 2005, functioning in a senior consulting role for customers that experience information security incidents. Prior to joining the company, Mr. Palatt's experience includes working as an information security engineer, a forensics examiner, an information security analyst and an information systems auditor. Mr. Palatt holds a Bachelor of Science in Business Administration from Old Dominion University and a Master of Forensic Science with a concentration in High Technology Crime Investigation from George Washington University. He is a Certified Information Systems Security Professional (CISSP) a Certified Information Systems Auditor (CISA), VISA Qualified Data Security Professional (QDSP), a Certified Information Security Manager (CISM) and a Global Information Assurance Certification (GIAC) Certified Forensic Analyst (GCFE).

About IBM Professional Security Services

IBM Professional Security Services deliver expert security consulting, helping organizations of all sizes reduce risk, achieve regulatory compliance, maintain business continuity and reach their security goals. IBM ISS Professional Security Services consultants are 100 percent security-focused and utilize proven consulting methods, based on ISO 17799 best security practices. Supported by the IBM Internet Security Systems X-Force research and development team, IBM ISS Professional Security Services consultants are highly-skilled, senior security professionals. This team of security experts employs proprietary toolsets, the latest threat intelligence and advanced countermeasures to help build effective security programs that protect and enhance business operations.

About IBM Emergency Response Team

The IBM Emergency Response Service team combines real-world incident response experience, forensic analysis and X-Force security intelligence to provide an unparalleled level of service. Our expert consultants are highly-experienced in Windows and UNIX security, intrusion detection systems, penetration testing, computer crime and computer forensics. Each ERS team member has responded to dozens – if not hundreds – of actual incidents. The team has been exposed to a wider variety of systems, network configurations and attack methods than any single customer's in-house team. In addition, many of our consultants have backgrounds in computer security, the military, law enforcement and academia. In the event of an incident, our ERS team can act as your primary response team, providing expert advice and assistance to your own personnel. They can also help you build and test an incident response plan to ensure that you are prepared in advance for any potential threats. The IBM ISS Emergency Response Service team's skills and experience can make the difference in protecting your information assets, maintaining your ability to do business and preserving your reputation.

About IBM Internet Security Systems (ISS)

IBM Internet Security Systems is the trusted security advisor to thousands of the world's leading businesses and governments, providing preemptive protection for networks, desktops and servers. An established leader in security since 1994, the IBM Internet Security Systems protection platform automatically protects against both known and unknown threats, keeping networks up and running and shielding customers from online attacks before they impact business assets. IBM Internet Security Systems products and services are based on the proactive security intelligence of its X-Force® research and development team – the unequivocal world authority in vulnerability and threat research. The product line is complemented by comprehensive Managed Security Services and Professional Security Services.

For more information, about IBM Professional Security Services, contact your IBM representative or IBM Business partner. You may also call 1 800 776-2362 or visit ibm.com/services/us/iss.



© Copyright IBM Corporation 2001

IBM Global Services

Route 100

Somers, NY

U.S.A, 10589

Produced in the United States of America.

12-07

All Rights Reserved.

IBM and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.