Global Information Assurance Certification Paper

Making a case for reporting and prosecution of a cyber incident

Abstract

There are numerous types of cyber incidents. A recent survey indicates that the majority of these go unreported. Many of the objections to reporting and prosecution of cyber attacks are no longer valid. Resources for information sharing abound, tools for collecting and preserving evidence are plentiful, and laws modified to support litigation. Businesses and corporations can no longer afford to hide the extent to which cyber attacks are impacting their business. Security managers have an ethical and in some cases legal obligation to report incidents.

This paper makes a case for reporting and prosecution of a cyber incident by addressing some of the concerns expressed by the victims and security managers responding to these attacks.

GIAC-GSEC Practical Assignment Version 1.4b:
Research on topics in Information Security

Michael Klebes

19 January 2003

Introduction

From simple intrusions to actual crimes – cyber attacks are many and varied. Some are simply nuisances such as pings and probes that are easily detectable and pose no real problems, others are much harder to detect because of their criminal nature, with the attackers proficiently hiding their tracks.

Types of cyber crimes include:

- Copyright (software, movie, sound recording) piracy
- Internet Fraud matters that have a mail nexus
- Computer intrusion (i.e. hacking)
- disruption of computer
- Trafficking in prohibited items
- Internet harassment
- Denial of Service (DoS) attacks
- Email bombings
- Eavesdropping
- attacks on Internet servers
- introduction of virus or contaminant
- Manipulation of computer for financial benefit
- Password trafficking
- Theft of trade secrets
- Internet fraud
- Internet bomb threats
- Unauthorized extraction of data
- Viruses and worms
- Web page defacements

Reporting and prosecution of a cyber attack or any breech of a corporation's technology infrastructure are what should be the final steps in the larger more complex issue of creating and maintaining a secure information technology (IT) environment, that includes:

1. Creation and adoption of a corporate security policy
2. Creation and testing of a response plan
3. Planning and implementation against the policy
4. Prevention, monitoring and detection of attacks or breaches to the environment
5. Methodical response to an incident in accordance with the defined plan

The precursors of the defense-in-depth strategy necessary to thwart these attackers are the owners, security managers, and system operators of the computer networks. They are also in the best position to detect attacks and have an inherent responsibility to report intrusions to appropriate law enforcement agencies.

However, the most recent survey[1] by the Computer Security Institute and the San Francisco FBI shows that greater than 74% of survey respondents failed to report computer intrusion incidents to law enforcement. The reasons most often cited were that a company's reputation or their client's confidence might be at stake and a fear that competitors would use the information to their advantage.

This paper outlines the benefits of reporting and sharing information about cyber intrusions within your IT infrastructure, along with some of the issues associated with criminal prosecution.

Reporting

There are many compelling reasons for reporting an incident…

- Reporting may be required under regulatory laws or local and federal legal law. This makes it mandatory to report certain cyber attacks that involve actions such as violating the Bank Secrecy Act or an attack on a federal facility. In addition, if the cyber crime constitutes a felony, concealing (not reporting) would also be considered a crime.
- The sharing of cyber attack information will help other businesses, law enforcement, and developers to detect or prevent similar activities. For example, by providing information on a cyber security breech other business become aware of the issue and can take preventative actions. Knowing there is a problem, software developer's can repair the vulnerability.
- Investigators can combine the information from a number of sources to help facilitate the identification and subsequent prosecution of a perpetrator.
- By taking a preemptive position and releasing information related to a cyber attack you can thwart competitor attempts to take advantage of the situation. In most cases, customers and the hackers themselves will tend to make an incident public anyway.
- Reputation enforcement – tell the world, position your corporation as having the security infrastructure processes in place to not only detect but to protect sensitive information and to respond and prosecute cyber threats.
- Liability is another compelling reason to report and prosecute attacks. If during an attack your customer's private information is compromised, they might sue for loss of privacy. By reporting and prosecuting the perpetrator the business shows due diligence and might also recover any losses from the accused.

[1] 2002 CSI/FBI Computer Crime and Security Survey

- CSI/FBI Computer Crime and Security Survey[2] respondents identified financial losses associated with cyber crime at over $450 million in 2002. Thief of proprietary information and financial fraud accounted for the majority of these losses. By reporting and prosecuting the perpetrator of a cyber attack, the victim gains a greater chance of obtaining restitution for losses in addition to legally substantiating any insurance claims. Prosecution also provides a significant deterrent effect on the perpetrator and as a value lesson to others.

Misunderstanding often bars reporting of an incident…

- Law enforcement investigations may interfere with a corporation's ability to conduct business. Yes, forensic investigation does take time but capturing a perpetrator removes them from the field and sets an example to others who might not take the chance of hacking a business that is willing to prosecute.
- Businesses feel a need to minimize publicity in order to protect the corporation or client's reputation. In some cases, this might seem like a valid business justification but if the truth were ever to leak out the impact to a company's reputation might not be salvageable. Turn around the situation. Reinforce your corporation's reputation by taking a definitive stance and positive action.
- The costs associated with law enforcement investigation, prosecution, and other related business losses might seem high, but in reality allowing an individual to think they have gotten away with something simply increases the number of attacks and sends the wrong message to other perpetrators. This allows them to believe that they will not be prosecuted, even if they are detected and caught.
- Law enforcement will seize my equipment. Actually, it is the hacker's computers that are seized not the victims' equipment. Investigators now use forensic image copies of disks and perform remote searches having far less impact on systems operation. These new advances in forensic investigation have dramatically decreased the need to remove systems from service for extended periods.
- While competitors might use publicly disclosed information to their advantage, law enforcement agencies generally do not make the details of a case public unless there has been an arrest. In addition, the Freedom of Information Act exempts from release certain information required by government agencies during an investigation.
- Privacy concerns sometimes drive businesses to seek civil remedies over criminal prosecution. This is because civil suits generally do not require the public release of information. Even when pursuing this course of

[2] 2002 CSI/FBI Computer Crime and Security Survey

action corporations should consider sharing sanitized information with agencies such as the ISAC so that others can gain from the benefit of their experience.

- Being unaware of what constitutes a cyber crime and how to report one, along with a fear of calling the wrong agency is no longer a valid excuse. There are now numerous resources available to help. Law enforcement and other investigative groups are sharing data and in some instances have reciprocal agreements. In addition, education and resources on reporting have increased significantly.

Reporting and Information Sharing Resources

The following resources are available to facilitate information sharing and reporting:

Criminal Division's Computer Crime and Intellectual Property Section (CCIPS)

Need to know which agency to report a cyber related crime – this is the place to go. Sponsored by the Department of Defense, it is devoted exclusively to cyber crime. "Internet-related crime, like any other crime, should be reported to appropriate law enforcement investigative authorities at the local, state, federal, or international levels, depending on the scope of the crime. Citizens who are aware of federal crimes should report them to local offices of federal law enforcement."[3]

Information Sharing and Analysis Centers (ISAC)

Feel obligated to share information about a cyber attack on your business but wish to remain anonymous for some of the reasons above – there is a way. A partnership between the public and private sector has formed the Information Sharing and Analysis Centers (ISAC) to achieve just that. The centers span multiple geographies and industries providing access to a secure database of electronic security threats, vulnerabilities, incidents, and solutions. Many of the established ISACs have signed memoranda of understanding or operating agreements with the National Infrastructure Protection Center. The following industries and sectors have established ISACs:

- Electric Power
- Telecommunications
- Information Technology
- Financial Services
- Water Supply
- Oil & Gas
- Emergency Fire Services
- Food
- Chemicals Industry
- Emergency Law Enforcement

[3] How to Report Internet-Related Crime

- Surface Transportation
- Interstate

NIPC Cyber Threat and Computer Intrusion Report

Established to help solve crimes related to unauthorized intrusions of the nation's critical infrastructures and commercial sites, the National Infrastructure Protection Center (NIPC) is a partnership with government and private sector representation. These supported infrastructures include telecommunications, transportation, energy, banking and finance, water systems, government operations, and emergency services. The center also serves as a clearinghouse providing intelligence information related to computer crimes and infrastructure protection to the private sector Information Sharing and Analysis Centers (ISAC) mentioned above.

A reporting form prepared by the NIPC documents the information required to report a cyber crime or computer intrusion. Use this form as an off-line guide or on-line, to report an incident to the NIPC or other law enforcement agencies. To foster report submission the NIPC commits to treating as confidential any information concerning the identity of the reporting agency, department, company, or individual(s).

CERT/CC Incident Reporting Guidelines

Funded by the federal government and operated by Carnegie Mellon University the CERT Coordination Center (CERT/CC) for Internet security expertise has developed guidelines for reporting incidents to the CERT/CC as well as other security incident response teams. The guidelines discuss the what, why, who, how and when of reporting an incident.

The CERT Coordination Center is also a valuable informational resource publishing security alerts, researching security practices, offering training to help improve security, and researching security practices.

CIO Cyber Threat Response & Reporting Guidelines

Law enforcement and industry security professionals have collaborated to produce a guideline and template for reporting computer security incidents to law enforcement. The guidelines provide general information on the planning, people and process for developing a cyber threat response and reporting capability. Included is a report template and information on the what, when, and how of reporting an incident. Unsure about whom to contact during an incident this guideline provides contact lists for law enforcement, cyber threat support resources, incident handling, and planning resources, and a list of FBI and USSS field offices.

FinCEN Suspicious Activity Reports

The Bank Secrecy Act (BSA) requires that financial institutions keep records and file reports on certain financial transactions or suspected criminal offenses, including cyber related incidents.

The Financial Crimes Enforcement Network (FinCEN) of the Department of the Treasury maintains a Web site as a vehicle to provide BSA guidance and other information that can be downloaded. A variety of Suspicious Activity Report (SAR) report forms are provided including preparation and filing guidelines. Submitted SAR content is electronically available to appropriate law enforcement agencies and financial institution regulators.

Prosecution

Your corporation has a firm policy on the reporting and prosecution of cyber crimes especially when they might affect the company's reputation or a client's trust, or perhaps they are only looking to mitigate the risk of an unfair dismissal lawsuit against an employee suspected of an internal cyber breech. When you do not plan to prosecute, investigating, reporting, and sharing information about a cyberattack is much less threatening. There is not the overwhelming need to preserve evidence or follow rigorous investigative procedures. To protect you and your clients privacy and confidentiality you only have to release the amount of information with which you are comfortable.

However, if you do decide to report or prosecute cyber crimes consider the following.

When you report a cyber crime to law enforcement for investigation their ultimate goal is prosecution. When prosecuting any crime evidence makes the case. Whether a computer is the target of a crime or a repository for evidence the need to apply proper forensic techniques is crucial to securing evidence. The preservation of evidence during an investigation is an important legal issue and is both critical and central to a corporation's ability to investigate and take action against the cyber criminal. Therefore, the primary rule in any computer forensic investigation is not to tamper with the evidence, thus making it suspect when presented in court.

The best place to address this is in your response plan, which should provide explicit details on what needs to occur. It is too late to plan how you are going to investigate an incident and protect the evidence after the fact. Proper training in forensics investigation is crucial to the development and execution of a response plan that will protect the evidence necessary to identify the cyber criminal and subsequently prosecute them successfully. This requires documenting the entire investigative process – from the moment of detection to the time law enforcement becomes involved. By adhering to a strict response plan, developed by a security officer trained in computer forensics, you stand a much greater chance of having viable, qualified evidence for use in prosecuting a case.

Investigative Alternatives

What investigative alternatives are available if you do not initially plan to prosecute or an attack does not require reporting under applicable legal or regulatory requirements? Many businesses are turning to internal forensic research or hiring cyber forensics investigators as an alternative to law enforcement investigations into cyber attacks.

Computer forensics investigation is a branch of law enforcement that includes many of the activities performed by IT security professionals in their everyday tasks of managing corporate IT resources, protecting servers and computers, and detecting and tracking intruders on their networks. Using an internal resource can certainly limit exposure of an incident to outside parties but will require some initial investment.

Proper training in computer forensics, skills in using the varied forensics software packages, and experience in conducting forensic investigations must be obtained. In addition to obtaining training from such institutes as SANS, many of the software forensic applications vendors provide training as well. This training is usually specific to the firm's product offering but in many cases is transferable to other technologies as well, e.g. Guidance Software's EnCase. Remember there is no substitute for security training, not only the security manager but for the support and operations staff as well.

Creating or obtaining an internal resource capable of cyber crime forensic investigation can be costly and time consuming. Business with smaller security budgets or those that cannot justify a full-time security officer trained in computer forensics can hire a cyber forensics investigative firm. These firms provide varied techniques and levels of support tailored to the specifics of a particular investigation. Examples are available in the report; Firms increasingly call on cyber forensics teams from IDG.net.[4]

Some firms offering computer forensics investigative services, training, and software include:

- Vogon International – http://www.vogon-international.com
- Guidance Software – http://www.guidancesoftware.com
- Predictive Systems – http://www.predictive.com
- Foundstone Inc. – http://www.foundstone.com
- New Technologies, Inc. – http://www.forensics-intl.com

Regardless of how you decide to investigate a cyber attack you should always report the incident, even if this requires sanitizing the content and submitting it anonymously. This allows other business and agencies to benefit from your experience.

---

[4] Firms increasingly call on cyberforensics teams

Some Legal Issues

There are a number of legal issues to consider when conducting an investigation or determining whether to report or prosecute a cyber attack.

From a liability perspective, colleges and universities may be held responsible for the actions of students who use the institutes' resources to perpetrate a cyber attack or crime. In certain situations, the institutions are liable if they fail to monitor and prevent these types of attacks from occurring.

How you respond to an attack can also have profound affects legally. Consider what would happen if you detected a denial of service attack on your web server and were able to trace the source of the attack to an inordinate number of download requests from a specific IP address. Subsequently you turn-around and return all the download requests to the originator. It so happens that a previously compromised (zombie) system was used to perpetrate the original attack on your system. Now an innocent target is the subject of your attack. Al Potter, manager of network security labs at ICSA Labs in Carlisle, Pa. says don't retaliate -- "Fighting back is a bad idea. I wouldn't do it, if it's illegal for them to attack you, then it's also illegal to attack them."[5]

The area of privacy is a Pandora's box. Applying technical solutions such as traceback to determine the source of an attack may push the limits of privacy laws. For example, examining packet headers invokes no liability or privacy issues, examining the contents of the same packet does as these are legally protected – while accessing the contents of a digest falls into the gray area of undecided.

You can gain an advantage by reporting a cyber attack to law enforcement and having them become part of the investigative team. They have the ability to obtain permission to access information as part of a formal investigation.

In summary, your IT security staff knows how systems can be exploited and are the ones most capable of detecting intrusions. Professionals trained in cyber forensics understand the legal issues and litigation process necessary to prosecute a cyber crime. Whether you are preparing a response plan, conducting an investigation, or initiating prosecution you should always consult your corporation's legal consul. Leave legal matters related to cyber attacks to the lawyers.

[5] Can You Hack Back?

Conclusion

Drawbacks to reporting and prosecution continue to drop by the wayside as new laws protecting privacy and increased criminalization of incidents and penalties for cyber offenses go into effect. Industry, law enforcement, and the government continue to expose the fallacies and mitigate the objections to the reporting and prosecution of cyber attacks.

Cybercrime is costing our economy billions of dollars per year. Victims include the owners and maintainers of compromised data, the clients and users of internet businesses, and indeed almost everyone in this new information age.

The best defense against cyber attacks is an even better offense – by not reporting a cyber incident victims actually contribute to the continued build up of malicious attacks. It is imperative that businesses report and potentially prosecute intrusions.

Do your part to lower the incidence of cyber related attacks. As the security manager for your business:

– Enforce your security policy –

– Secure your environment –

– Monitor and detect intrusions –

– Implement your response plan –

– *Report and prosecute the perpetrators* –

List of References

1. Power, Richard. "2002 CSI/FBI Computer Crime and Security Survey." Computer Security Issues & Trends. Vol. VIII, No.1. Spring 2002. http://www.gocsi.com/forms/fbi/pdf.html (23 Jan 2003).
2. usdoj-crm. "How to Report Internet-Related Crime." Computer Crime and Intellectual Property Section. 6 Dec 2002. http://www.cybercrime.gov/reporting.htm (23 Jan 2003).
3. Radcliff, Deborah. "Firms increasingly call on cyberforensics teams. Computer World an IDG.net Site. 16 Jan 2002. http://www.cnn.com/2002/TECH/internet/01/16/cyber.sleuthing.idg/index.html (23 Jan 2003).
4. Radcliff, Deborah. "Can You Hack Back?" Network World Fusion. 1 Jun 2000. http://www.cnn.com/2000/TECH/computing/06/01/hack.back.idg/index.html (23 Jan 2003).
5. Ashcroft, John. "Criminal Division's Computer Crime and Intellectual Property Section (CCIPS)." US Department of Justice. 21 Jan 2003.http://www.cybercrime.gov/ (23 Jan 2003).
6. Dick, Ron. "Information Sharing and Analysis Centers (ISAC)."National Infrastructure Protection Center (NIPC). 17 Jul 2002.http://www.nipc.gov/infosharing/infosharing6.htm (23 Jan 2003).
7. Dick, Ron. "Cyber Threat and Computer Intrusion Report." National Infrastructure Protection Center (NIPC). 17 Jul 2002. http://www.nipc.gov/incident/incident.htm (23 Jan 2003).
8. "CERT® Coordination Center (CERT/CC) Incident Reporting Guidelines." http://www.cert.org/tech_tips/incident_reporting.html (23 Jan 2003).
9. Lundberg, Abbie. "CIO Cyberthreat Response & Reporting Guidelines." Security and Privacy Research Center, CIO.com. 16 Jan 2002. URL: http://www.cio.com/research/security/incident_response.pdf (23 Jan 2003).
10. Sloan, James. "BSA Forms and Filing Information." Financial Crimes Enforcement Network (FinCEN). URL: http://www.fincen.gov/bsaf_main.html (23 Jan 2003).
11. Lee, Susan C. and Shields, Clay. "Technical, Legal, and Societal Challenges to Automated Attack Traceback." IT Pro May - June 2002. URL: http://www.computer.org/itpro/it2002/pdf/f3012.pdf (24 Sep. 2002).
12. Olsen, Florence. "Logging in with . . . Thomas J. Talleur". The Chronicle of Higher Education - Information Technology. 5 Jul 2000. URL: http://chronicle.com/free/2000/07/2000070501t.htm (24 Sep. 2002).

13. Goldstone, David. "Deciding Whether to Prosecute an Intellectual Property Case". United States Attorneys' USA Bulletin. Vol. 49, No. 2. March 2001. URL: http://www.cyber crime.gov/usamarch2001_1.htm (27 Sep. 2002).
14. Shenk, Maury and Schneck, Melanie. “Should a Corporation Report a Breach to Law Enforcement?” Secure Business Quarterly. Vol.1, No.1. Q3, 2001. URL: http://www.sbq.com/sbq/digital_forensics/sbq_forensics_reporting_breachs.pdf
15. Bridis, Ted. “Feds pursue secrecy for corporate victims of hacking.” Associated Press. 31 Oct 2002. URL: http://lists.jammed.com/ISN/2002/11/0005.html (23Jan 2003).
16. Law, Gillian. “Report: Firms want computer forensics training.” Sci-Tech 1 Mar 2002. URL: http://www.cnn.com/2002/TECH/industry/03/01/computer.forensics.idg/index.html?related (23 Jan 2003).
17. “EnCase Enterprise Resources.“ Guidance Software. URL: http://www.guidancesoftware.com (23 Jan 2003)
18. Sheldon, Andrew. “Forensic Auditing – The role of computer forensics in the Corporate Toolbox.” TECS Library of Information Security Papers. URL: http://www.itsecurity.com/papers/p11.htm (23 Jan 2003).
19. Kessler, Gary C. and Schirling, Michael. “Computer Forensics: The Issues and Current Books in the Field.” Information Security Magazine. April 2002. URL: http://www.garykessler.net/library/computer_forensics_books.html (23 Jan 2003).
20. Scalet, Sarah. “Fear Factor.” CIO Magazine. 15 Oct 2002. URL: http://www.cio.com/archive/101502/fear.html (23 Jan 2003).
21. Salgado, Richard P. "Working with Victims of Computer Network Hacks." United States Attorneys' USA Bulletin. Vol. 49, No. 2. March 2001. URL: http://www.cyber crime.gov/usamarch2001_6.htm (27 Sep. 2002).
22. Carr, Jim. "Strategies & Issues: Thwarting Insider Attacks." Network Magazine. 05 Sep. 2002. URL: http://www.networkmagazine.com/article/NMG20020826S0011 (30 Sep. 2002)