



Interested in learning more about security?

# SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

## Deterring Cyber Attacks

In the past, many companies chose not to share information on cyber attacks with authorities or with watchdog groups for fear that negative publicity would decrease consumer and investor confidence and lead to potential profit losses. In the wake of the recent terrorist attacks, some companies, especially those in "commercial infrastructure" areas [telecommunications, energy, transportation, banking & finance and emergency services], may decide that protecting homeland security requires overlook...

Copyright SANS Institute  
Author Retains Full Rights

AD

A banner advertisement for FireEye. On the left is the FireEye logo, which consists of a stylized red and white eye with a flame-like shape above it. To the right of the logo, the text reads: "Protect critical data from the cyber theft pandemic." in white, followed by "Learn how in this FireEye white paper." in yellow. On the far right of the banner is a black and white photograph of a man wearing a hard hat and a yellow bird in a cage.

**Protect critical data from the  
cyber theft pandemic.**  
Learn how in this FireEye **white paper.**

### Summary

In the past, many companies chose not to share information on cyber attacks with authorities or with watchdog groups for fear that negative publicity would decrease consumer and investor confidence and lead to potential profit losses. In the wake of the recent terrorist attacks, some companies, especially those in “commercial infrastructure” areas [defined by the National Infrastructure Protection Center (NIPC) as telecommunications, energy, transportation, banking & finance and emergency services]<sup>i</sup>, may decide that protecting homeland security requires overlooking legitimate corporate concerns and working with outside groups to deter and defend against cyber attacks.

If your company decides to rethink its policy and you are asked for recommendations, here is a Strengths, Weaknesses, Opportunities and Threats [SWOT] Analysis<sup>ii</sup> to help you analyze three alternatives and recommend the best one to upper management. The three alternatives are: (1) inform the authorities and, if possible, prosecute the perpetrators (2) share the attack/recovery information with an Information Sharing and Analysis Center [ISAC] group or (3) share the attack/recovery information with the CERT [Computer Emergency Response Team] Command Center. A Next Steps guide is also included for each alternative to help you implement your new policy.

### Choice No. 1: Alert the Authorities

**Overview:** After an attack occurs, your technology security group fixes the problem, saves the evidence, presents it to the proper authorities and works with them to build a case against the attackers.

**Scenario 1:** An attack may be public [e.g. your web site is defaced] or private [e.g. your network is infiltrated and trade secrets are stolen]. Either way, once you alert the authorities, publicity is assured.

**SWOT Analysis:** Ask yourself the listed questions [Note: depending upon what industry your company is in, some questions may not apply]. If the majority turn out to be Strengths and Opportunities, then consider recommending this option to senior management. If not, recommend another choice.

<b>Strengths/ Weaknesses:</b>
<ul style="list-style-type: none"><li>• Company and/or Brand Strength: Can your company/brand goodwill overcome any negative publicity about the internet attack or attempts to catch those responsible?</li><li>• Market Position: Will negative publicity cause your company to lose a lot or a little market share? What effect will this have on future stockholder value?</li></ul>

- Ability to raise Capital: Will any negative publicity hurt your company's chances of acquiring needed capital from the financial markets?
- Future Growth Strategies: Will negative publicity [and potential decrease in future profits] derail necessary strategic growth plans?
- Management of Change: Does your company have the people and processes in place to handle the publicity surrounding an attack and possible prosecution of the perpetrators?

#### **Opportunities/Threats**

- Customer & Supplier Bargaining Power: What will your company have to give up [coupons, rebates] to try to keep its consumers, investors & suppliers?
- Customer, Investor & Supplier Loyalty: How loyal are your customers, investors & suppliers? Will they jump to your competitors at the first sign of an internet attack?
- Competition: Are your competitors in a position to take advantage of your negative publicity? If so, what might they do and how can your company overcome the competition?
- Political climate: Is the political climate such that your company might receive subsidies, grants or tax breaks from the government to file charges against computer attackers? Is the climate such that new laws or insurance policies might go into effect that may favorably/unfavorably sway your decision to file a lawsuit?
- Substitute Products/Services: How easy is it for your customers to buy similar products and services from competitors?
- Technical Development: Now that the public knows that your network is vulnerable, are there any software, hardware or process improvements on the market to decrease future computer attacks? If so, will you company pay the price? If not, can your company's technical department stop attackers (using the same method as the initial attacker) from further disruptions?

- **NEXT STEPS:** If upper management chooses to inform the authorities if an attack occurs, there are several things you should do to expedite the process.
  - First, create or update your security policy. If you do not have a policy, follow the SANS Incident Handling Steps [Preparation, Identification, Containment, Eradication, Recovery and Lessons Learned.] as taught in the Security Essentials course.<sup>iii</sup> As you work through these steps and decide how/when to contact the authorities, pay special attention to Preparation and Identification. Attention to detail here will help the authorities investigate and prosecute those responsible.
  - Preparation: Determine what types of cyber attacks warrant calling the authorities. [For example, you may decide to report when an attacker defaces your website, but not report a theft of trade secrets]. Once you determine when to call,

determine who to call – local, state and/or federal authorities. The following contact information is a useful reference:

Authority	Contact information
Guidance on Federal investigations	<ul style="list-style-type: none"> <li>The National Infrastructure Protection Center (NIPC): <a href="http://www.nipc.gov/contact.htm">http://www.nipc.gov/contact.htm</a> or call 202-323-3205.</li> </ul>
Guidance on state & local investigations	<ul style="list-style-type: none"> <li>National Association of Attorneys General: <a href="http://www.naag.org/issues/20010724-cc_list_bg.cfm">http://www.naag.org/issues/20010724-cc_list_bg.cfm</a></li> </ul>

- Identification: Once you determine that a reportable attack occurred, make a backup copy of the logs, altered files and any files left by the attacker. Preserve evidence integrity by storing the backups in sealed bags in locked rooms. Also, keep a record of who handled the evidence from the time the attack occurred until the time it is handed over to authorities.
- Consider following these additional suggestions, which make police investigations run more smoothly:<sup>iv</sup>
  - Quantify the damages. Include “personnel hours spent on response and recovery, cost of temporary help, cost of damaged equipment, value of lost data, loss of revenue, credit given to customers due to down time and loss of trade secrets.”<sup>v</sup>
  - Create a “starter” kit for investigators that includes a “network map, list of applications and operating systems, system logs/files and personnel information on those with access to critical information systems. Useful personnel information includes names, job descriptions, access rights and written acknowledgements of company network policies.”
  - Identify witnesses and make them available for statements.

### **Choice No. 2: Share Information with an ISAC group**

**Overview:** In 1998, President Clinton requested that companies in critical U.S. industries [such as telecommunications and electrical power] create Information Sharing and Analysis Centers [ISAC]s to disseminate data about computer security attacks.<sup>vi</sup> To date, ISACs are active in the finance, telecommunications, electrical power and information technology sectors. ISACs are in the works for the aviation, railroad, water and oil & gas sectors. In general, companies voluntarily and anonymously share information on attacks and solutions via a central database. Within the Information Technology ISAC specifically, once a threat is received, “the technical specifications ...go out to the ISAC members. Those ISAC members...then immediately launch an action and...collaborate with one another, sharing solutions, analysis and problems.”<sup>vii</sup> Due to the sensitive nature of some of the information, the general public is not notified and the government is not always notified of a threat or an attack; however, the government shares useful intelligence information with the ISACs.

**Scenario 2:** An attack may be public [e.g. your web site is defaced] or private [e.g. your network is infiltrated and trade secrets are stolen]. In this particular scenario, the public only knows about the public attack, not the private attack or any subsequent information sharing.

**SWOT:** Ask yourself the listed questions. [Note: depending upon what industry your company is in, some questions may not apply]. If the majority turn out to be Strengths and Opportunities, then consider recommending this option to senior management. If not, recommend another choice.

<b>Strengths/Weaknesses</b>	
<ul style="list-style-type: none"> <li>• <b>Competitive Advantage:</b> Will your company give away any business or technology secrets by sharing solutions to computer attacks?</li> <li>• <b>Downtime:</b> Will participation in this group decrease website or network downtime?</li> <li>• <b>Labor Costs:</b> Is it still necessary to hire high priced consultants to fix security brecches?</li> <li>• The next five bullets refer to the following scenario: what happens if your company sustains a public attack and shares information with its ISAC, but does not take any apparent public action to find and prosecute the attackers or to safeguard your computer network:               <ul style="list-style-type: none"> <li>• <b>Company and/or Brand Strength:</b> Can your company/brand goodwill overcome any negative publicity about the internet attack?</li> <li>• <b>Market Position:</b> Will negative publicity cause your company to lose a lot or a little market share? What effect will this have on future stockholder value?</li> <li>• <b>Ability to raise Capital:</b> Will any negative publicity hurt your company’s chances of acquiring needed capital from the financial markets?</li> <li>• <b>Management of Change:</b> Does your company have the people and processes in place to handle the publicity surrounding an attack?</li> <li>• <b>Future Growth Strategies:</b> Will negative publicity [and potential decrease in future profits] derail necessary strategic growth plans?</li> </ul> </li> </ul>	
<b>Opportunities/Threats</b>	
<ul style="list-style-type: none"> <li>• <b>Alliances:</b> Will this group help minimize or prevent computer attacks?</li> <li>• <b>Competitor’s Learning Curve:</b> Will your company carry the rest of the group or will all groups equally participate in fixing/detecting attacks? Will companies be able to benchmark other participants participation?</li> <li>• <b>Costs:</b> Is the cost to join prohibitive? Is the cost of entry worth the alleged benefits?</li> </ul>	

- **Political Climate:** Is the political climate such that your company may be forced to share certain information [which may not be in your company's best interests] with the government?
- **Technology Developments:** Will fellow participants share other technology breakthroughs or just work together to fix computer attacks?
- The next several bullets refer to the following scenario: what happens if your company sustains a public attack and shares information with its ISAC, but does not take any apparent public action to find and prosecute the attackers or to safeguard your computer network:
  - **Customer & Supplier Bargaining Power:** What will your company have to give up [coupons, rebates] to try to keep its buyers & suppliers?
  - **Customer, Investor & Supplier Loyalty:** How loyal are your customers, investors & suppliers? Will they jump to your competitors at the first sign of bad press?
  - **Substitute Products/Services:** How easy is it for your customers to buy similar products and services from competitors?
  - **Technical Development:** Now that the public knows that your network is vulnerable, are there any software, hardware or process improvements on the market to decrease future computer attacks? If so, will your company pay the price? If not, can your company's technical department stop attackers (using the same method as the previous attacker) from further disruptions?

- **NEXT STEPS:** If upper management chooses this option, there are several things you should do to facilitate the process. First, join the appropriate ISAC. Here is a checklist to help you determine if there is an ISAC available for your company:
  - If your company is in banking/finance, telecommunications, electrical power or information technology, see the following ISAC web sites for membership details:

ISACs
Finance, see <a href="http://www.fsisac.com">www.fsisac.com</a>
Telecommunications, see <a href="http://www.ncs.gov/ncc/main.html">www.ncs.gov/ncc/main.html</a>
Electrical Power, see <a href="http://www.energyisac.com">www.energyisac.com</a>
Information Technology, see <a href="http://www.it-isac.org">www.it-isac.org</a>

- If you work in the aviation, railroad, water or oil & gas sectors, ISACs are currently forming. For more information, see the following web sites:

Future ISACs
Railroads, see <a href="http://www.aar.org">www.aar.org</a>

Water, see [www.amwa.net/isac/index.html](http://www.amwa.net/isac/index.html)

Oil & Gas, see [www.npc.org](http://www.npc.org)

- If your industry is not represented above, contact the governmental agency charged with overseeing your industry or contact an interest group in your industry. If information is not available, consider spearheading the formation of a new ISAC.
- Second, create or update your security policy. If you do not have a policy, follow the SANS Incident Handling Steps [Preparation, Identification, Containment, Eradication, Recovery and Lessons Learned.] as taught in the Security Essentials course.<sup>viii</sup> As you work through these steps, pay special attention to Preparation and Identification.
  - Preparation: Determine what types of cyber attacks warrant sharing information with your ISAC. [For example, you may decide to report when an attacker breaks into an industry-specific application program, but not report when one breaks in and steals trade secrets].
  - Identification: Once you determine that a reportable attack occurred, make a backup copy of the logs, altered files and any files left by the attacker. Send this information to your ISAC.

### **Choice No. 3: Share Information with CERT**

**Overview:** The Computer Emergency Response Team [CERT] Command Center was created with federal funds in 1988 to “work with the Internet community in detecting and resolving computer security incidents, as well as taking steps to prevent future incidents.”<sup>ix</sup> The Command Center maintains a 24 hour hotline as well as incident report forms on its web site to facilitate the flow of information. CERT also proactively publishes press releases on known security issues and solutions, and sends information to list-serv members. The Command Center stays busy. Since 1988, companies emailed CERT 403,000 times, called the hotline 20,000 times and asked for 4,400 vulnerability reports.<sup>x</sup>

Jittery about revealing company secrets to a federally funded group? CERT does not release information about a company [either to the public or to the government] unless permitted by the company. It will release information on the attack though.

**Scenario 3:** An attack may be public [e.g. your web site is defaced] or private [e.g. your network is infiltrated and trade secrets are stolen]. In this particular scenario, the public only knows about the public attack, not the private attack or any subsequent information sharing.

**SWOT:** Ask yourself the listed questions. [Note: depending upon what industry your company is in, some questions may not apply]. If the majority turn out to be Strengths and Opportunities, then consider recommending this option to senior management. If not, recommend another choice.

#### **STRENGTHS/WEAKNESSES**

- Competitive Advantage: If help is solicited and received, your company’s problem is solved. Your competitor’s may not be

privity to the same information so your company may get back on its feet faster.

- Downtime: Will participation in this group decrease website or network downtime?
- Labor Costs: Is it still necessary to hire high priced consultants to fix security breeches?
- The next several bullets refer to the following scenario: what happens if your company sustains a public attack and informs CERT, but does not take any apparent public action to find and prosecute the attackers or to safeguard your computer network:
  - Company and/or Brand Strength: Can your company/brand goodwill overcome any negative publicity from the internet attack?
  - Market Position: Will negative publicity cause your company to lose a lot or a little market share? What effect will this have on future stockholder value?
  - Ability to raise Capital: Will any negative publicity hurt your company's chances of acquiring needed capital from the financial markets?
  - Management of Change: Does your company have the people and processes in place to handle the publicity surrounding an attack?
  - Future Growth Strategies: Will negative publicity [and potential decrease in future profits] derail necessary strategic growth plans?

#### **Opportunities/Threats**

- Political Climate: Is the political climate such that your company may be forced to share certain information [which may not be in your company's best interests] with the government?
- Technology Developments: Will fellow participants share other technology breakthroughs or just work together to fix computer attacks?
- The next several bullets refer to the following scenario: what happens if your company sustains a public attack and informs CERT, but does not take any apparent public action to find and prosecute the attackers or to safeguard your computer network:
  - Customer & Supplier Bargaining Power: What will your company have to give up [coupons, rebates] to try to keep its buyers & suppliers?
  - Customer, Investor & Supplier Loyalty: How loyal are your customers, investors and suppliers? Will they jump to your competitors at the first sign of bad press?
  - Competition: Are your competitors in a position to take advantage of your negative publicity? If so, what might they do and how can your company overcome the competition?

- **Substitute Products/Services:** How easy is it for your customers to buy similar products and services from competitors?
- **Political Climate:** Is the political climate such that your company may be forced to share certain information [which may not be in your company's best interests] with the government?
- **Technical Development:** Now that the public knows your network is vulnerable, are there any software, hardware or process improvements on the market to decrease future computer attacks? If so, will your company pay the price? If not, can your company's technical department stop attackers (using the same method as the previous attacker) from further disruptions?

**NEXT STEPS:** If upper management chooses this option, there are several things you can do to facilitate the process. First, create or update your security policy. If you do not have a policy, follow the SANS Incident Handling Steps [Preparation, Identification, Containment, Eradication, Recovery and Lessons Learned.] as taught in the Security Essentials course.<sup>xi</sup> As you work through these steps, pay special attention to Preparation and Identification.

- **Preparation:** Determine what types of cyber attacks warrant sharing information with your CERT. The following contact information is a useful reference:

Ways to Communicate with CERT	
Email	<a href="mailto:Cert@cert.org">Cert@cert.org</a>
Incident & Vulnerability Report forms	<a href="http://www.cert.org/contact_cert/contactinfo.html">http://www.cert.org/contact_cert/contactinfo.html</a>
24 Hour hotline	1-412-268-7090
Fax	1-412-268-6989
Postal address	CERT® Coordination Center Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213-3890

- **Identification:** Once you determine that a reportable attack occurred, make a backup copy of the logs, altered files and any files left by the attacker. Send this information to CERT, via the means above.

**Choices, Choices...**

Here are some general ideas to think about as you determine what recommendation to give to upper management. Keep in mind, the best recommendation may be all three. After all, different scenarios usually require different responses. For example, if the incident is public knowledge, consider notifying the authorities and prosecuting the attackers. No reason to try and cover up the event if your customers know about it. Also, acting to catch the perpetrators may make your company look good in the public eye [i.e. your company is trying to protect its customers]. And, who knows, trying to prosecute the attacks may help repair any customer relations damage that may have taken place when customers learned of the attack.

If your company remains averse to additional publicity, then, at the very least, consider sharing the information with either (a) your ISAC group [if the attack information is specific to one industry [i.e. financial industry software] or (b) with CERT [i.e. for all general computer attacks]. Your company may sustain some bad public relations for seemingly not defending itself and its customers from attacks, but the more your company allies itself with other businesses and groups in the fight against computer attacks, the less likely it is your company will sustain an attack and the more likely it is your customers will benefit, abet unknowingly.

If the attack is not public knowledge, surely it is in your company's best interest to keep the news out of the public eye. Why stir up supplier, investor and consumer trouble? Instead, consider sharing the information with your ISAC or with CERT, as mentioned above, so other companies might not have to suffer the same consequences. In general, what goes around comes around. The money you save other companies by reporting an incident should, in theory, be repaid back to you many times over when your company is alerted to potential problems or given information on how to clean up an attack.

---

<sup>i</sup> Power, Richard, ed. "2001 CSI/FBI Computer Crime and Security Survey" Computer Security Institute 2001. January 22, 2002

<sup>ii</sup> "SWOT Checklist" BusinessMajors.about.com November 29, 1999. January 22, 2002  
[www.businessmajors.about.com/library/weekly/aa112999a.htm](http://www.businessmajors.about.com/library/weekly/aa112999a.htm)

<sup>iii</sup> "Incident Handling Foundations." SANS Institute Security Essentials online course, Part 2: Network Security. June 6, 2001. December, 2001.

<sup>iv</sup> Unless noted, all information is from:  
Shipley, Todd G. "Supporting Cyber Sleuths." InfoSecurityMag.com, July 2001. January 22, 2002  
[http://www.infosecuritymag.com/articles/july01/features\\_cybercrime.shtml](http://www.infosecuritymag.com/articles/july01/features_cybercrime.shtml)

<sup>v</sup> "How the FBI Investigates Computer Crime." Cert.org July 27, 2000. January 22, 2002  
[http://www.cert.org/tech\\_tips/FBI\\_investigates\\_crime.html](http://www.cert.org/tech_tips/FBI_investigates_crime.html)

<sup>vi</sup> Hurley, Edward. "IT-ISAC: A Matter of Trust." SearchSecurity.com January 29, 2001. January 22, 2002  
[http://searchsecurity.techtarget.com/originalContent/0,289142,sid14\\_gci517824,00.html](http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci517824,00.html)

<sup>vii</sup> Johnston, Margret. "Center for cyber security detailed." Infoworld.com January 17, 2001. January 22, 2002  
[www.infoworld.com/articles/hn/xml/01/01/17/010117hntisac.xml?p=br&s=4](http://www.infoworld.com/articles/hn/xml/01/01/17/010117hntisac.xml?p=br&s=4).

<sup>viii</sup> "Incident Handling Foundations." SANS Institute Security Essentials online course, Part 2: Network Security. June 6, 2001. December, 2001.

<sup>ix</sup> "Meet the CERT Coordination Center." Cert.org January 24, 2002 [www.cert.org/meet\\_cert/meetcertcc.html](http://www.cert.org/meet_cert/meetcertcc.html)

<sup>x</sup> "Meet the CERT Coordination Center." Cert.org January 24, 2002 [www.cert.org/meet\\_cert/meetcertcc.html](http://www.cert.org/meet_cert/meetcertcc.html)

<sup>xi</sup> "Incident Handling Foundations." SANS Institute Security Essentials online course, Part 2: Network Security. June 6, 2001. December, 2001.



# Upcoming SANS Training

[Click Here for a full list of all Upcoming SANS Events by Location](#)

SANS SOS London 2009	London, United Kingdom	Jul 13, 2009 - Jul 18, 2009	Live Event
SANS Future Visions 2009 Tokyo	Tokyo, Japan	Jul 15, 2009 - Jul 17, 2009	Live Event
SANS IMPACT 2009	Kuala Lumpur, Malaysia	Jul 27, 2009 - Aug 01, 2009	Live Event
SANS SEC563: Mobile Device Forensics Debut	Baltimore, MD	Jul 27, 2009 - Jul 31, 2009	Live Event
SANS Boston 2009	Boston, MA	Aug 02, 2009 - Aug 09, 2009	Live Event
SANS WhatWorks in Virtualization and Cloud Computing Security Summit 2009	Washington, DC	Aug 17, 2009 - Aug 21, 2009	Live Event
SANS Atlanta 2009	Atlanta, GA	Aug 17, 2009 - Aug 28, 2009	Live Event
SANS Virginia Beach 2009	Virginia Beach, VA	Aug 28, 2009 - Sep 04, 2009	Live Event
SANS SCDP SEC556: Comprehensive Packet Analysis - Sept. 2009	Ottawa, ON	Sep 09, 2009 - Sep 10, 2009	Live Event
SANS Critical Infrastructure Protection at Oceania CACS2009	Canberra, Australia	Sep 10, 2009 - Sep 11, 2009	Live Event
SANS Network Security 2009	San Diego, CA	Sep 14, 2009 - Sep 22, 2009	Live Event
SANS SCDP Cutting Edge Hacking Techniques - June 2009	Ottawa, ON	Sep 15, 2009 - Sep 15, 2009	Live Event
SANS Rocky Mountain 2009	OnlineCO	Jul 07, 2009 - Jul 13, 2009	Live Event
SANS OnDemand	Books & MP3s Only	Anytime	Self Paced