



Beyond Vulnerability Assessment: 10 Questions

Lenny Zeltser



Prepared in 2006.

This presentation explores common information security risks that organization face, and suggests 10 questions worth asking when establishing a robust IT security program. Attempting to go beyond traditional vulnerability assessment methodology, this talk reviews security breaches that were publicly announced in the past months, and addresses three types of attacks:

- Inadvertent Disclosure
- Attacks of Opportunity
- Targeted Attacks

The presentation was prepared by Lenny Zeltser, Information Security Practice Leader at Gemini Systems, a premier IT consulting firm headquartered in New York. For additional information about Gemini Systems' security services, please take a look at <http://www.gemini-systems.com/security>.




No matter how hard we try, we cannot close all the cracks in a system of even a moderate complexity. Building a room with no entrance, or unplugging a server from the network might prevent theft of information, but it will render the system useless. Most systems need to have “cracks” to allow its users to access the resources needed for legitimate business purposes. These are the same cracks that attackers attempt to exploit when compromising the system.

This situation reminds me of Leonard Cohen’s song Anthem, where he exclaims:

There is a crack in everything.
That's how the light gets in.

(If you’re interested, you can listen to a fragment from this song and read its full lyrics at <http://www.leonardcohenfiles.com/album10.html>.)



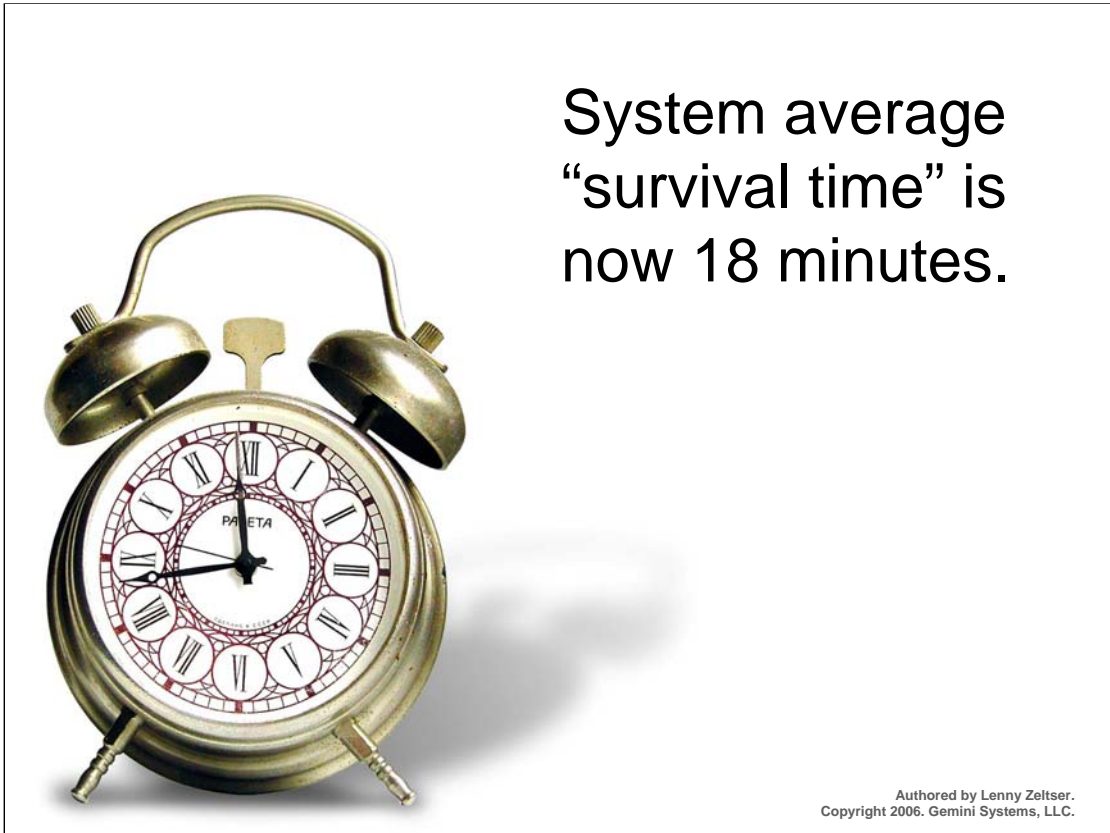
Exploits are released within 6 days
of the vulnerability announcement.

Patches come out within 54 days.

According to Symantec's *Internet Security Threat Report*, Volume VII, in the second half of 2005, "the average time between the disclosure of a vulnerability and the release of an associated exploit was 6.0 days. During the same period, on average, 54 days elapsed between disclosure of a vulnerability and the release of a patch by the vendor."

As a result, the window of opportunity for attackers to exploit a known vulnerability was, on the average 48 days. This highlights the ineffectiveness of environments that rely solely on the practice of routine patching to prevent system compromises.

(Symantec's *Internet Security Threat Report*, Volume VIII, published in September 2005, is available at the following URL:
<http://enterprisesecurity.symantec.com/content.cfm?articleid=1539>.)

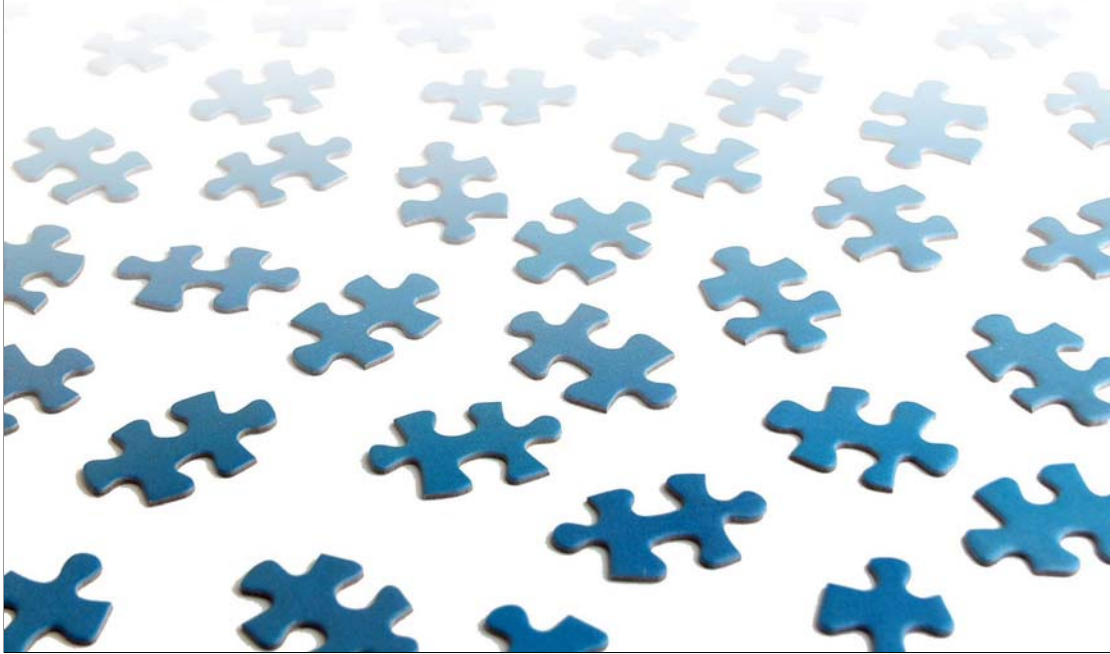


The complexities of addressing security risks tied to known and unknown vulnerabilities continue to increase, as can be seen by the surprisingly short system “survival time” period.

SANS Internet Storm Center tracks “survival time” as the average time between probes that target a single system. If such a probe resulted by a worm that attempted to propagate, a typical unpatched system would get infected within this time period.

(Additional information and historical records about “survival time” is available at <http://isc.sans.org/survivalhistory.php>.)

A security strategy must include multiple defense components.



Many organizations build their information security programs around vulnerability management efforts. While it is, indeed, important to patch known flaws in software, vulnerability management is only one aspect of an information security discipline. An effective risk mitigation strategy should incorporate several defensive components to protect the organization against threats.

In this presentation we will examine a wide range of threats that organizations face, using recent events as examples. We will also talk about risk mitigation strategies that are tied to these threats.

Three Categories of Threats



Inadvertent
Disclosure



Attacks of
Opportunity



Targeted
Attacks

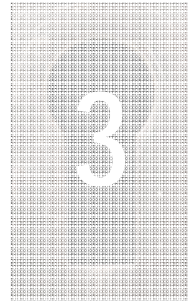
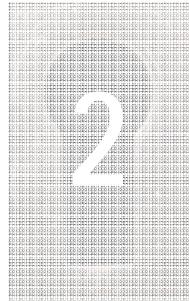


Authored by Lenny Zeltser.
Copyright 2006. Gemini Systems, LLC.

To better understand what risks organizations need to address, let's take a look at three categories of threats that have manifested themselves in recent security breaches:

- Inadvertent disclosure
- Attacks of opportunity
- Targeted attacks

As we examine each of these categories of threats, we will attempt to ask questions that, if asked early enough, could have lessened the security breaches discussed in the media in the last months.



Inadvertent Disclosure



Authored by Lenny Zeltser.
Copyright 2006. Gemini Systems, LLC.

First, we will take a look at *inadvertent disclosure* of sensitive information. These situations resulted, presumably, without ill-conceived motives or premeditated attack plans. Nonetheless, such attacks affected many thousands (perhaps even millions) individuals in the last year alone.

Inadvertent disclosure often takes one of the following forms:

- Website leaks
- Physical loss
- Communication snafu



Miami University's grade report breach affected 21,000 students.

In September 2005, officials at Miami University learned that a grade report from the Fall 2002 semester has been “unwittingly placed by a now-retired faculty member into a file that was accessible via the Internet. The report included the Social Security number and grade information on the more than 21,000 students.”

This is one of many inadvertent website leaks that has been reported in the media recently. Although a large number of such breaches occurred at universities, corporate sites were not immune from such problems. For instance, 19,000 Honeywell current and former employees were affected when their Social Security numbers and other information was inadvertently posted on a website. The affected individuals were notified of the breach in January 2005; the company blamed a former employee for the leak.

(For more information about the Miami University incident, please see http://www.miami.muohio.edu/documents_and_policies/privacyhelp.cfm. The Honeywell breach is described in an article at: http://news.yahoo.com/s/ap/20060201/ap_on_hi_te/honeywell_internet.)

A stolen Ameriprise laptop had data on 230,000 persons.



A laptop of an Ameriprise employee was stolen from the person's parked car in December 2005. The laptop contained personal information of approximately 230,000 customers and advisors associated with the company. The compromised information included Social Security numbers. The company spokesperson stated that it was unlikely that the thief knew that the information was on the laptop.

"The laptop was protected by a password but that the data was being stored unencrypted in violation of company rules. The employee involved has been fired."

(This incident is described in the article at <http://www.nytimes.com/2006/01/26/business/26data.html?ex=1295931600&en=683c419a10f58ef2&ei=5090>.)



In January 2006, two newspapers, Boston Globe and the Worcester Telegram & Gazette, accidentally printed delivery routing strips on the back of financial reports containing credit card details of their subscribers. The breach affected approximately 240,000 individuals. “How this sensitive data turned up in material to be recycled internally instead of been securely destroyed remains unclear, though it seems the material was generated from abandoned credit reporting runs.”

(The newspaper routing strips breach is described in http://www.theregister.co.uk/2006/02/02/globe_data_security_breach.)

Other recent security breaches associated with mailing mistakes are:

- H&R Block included Social Security numbers on the mailing label in January 2006 (See <http://www.eweek.com/article2/0,1895,1907596,00.asp.>)
- Blue Cross and Blue Shield of North Carolina included Social Security numbers on the mailing label in February 2006. (See <http://www.computerworld.com/printthis/2006/0,4814,108444,00.html.>)

ABN-AMRO's tape, misplaced by DHL,
contained data on 2 million individuals.



Authored by Lenny Zeltser.
Copyright 2006. Gemini Systems, LLC.

In December 2005, ABN-AMRO Mortgage Group, Inc. notified its customers that a computer tape has been lost by DHL courier service while being transported to a credit reporting company. The tape contained sensitive data, including Social Security numbers, of approximately 2 million individuals. The tape was recovered about a month later, and ABN-AMRO does not believe the data it carried was misused.

(This incident is described in the following article:
<http://www.computerworld.com/databasetopics/data/story/0,10801,107230,00.html>. An excerpt from the letter ABN-AMRO sent out is below.)

Dear Residential Mortgage Customer:

Please Read This Important Notice

We are writing to let you know that a computer tape containing information about you and your mortgage account with ABN AMRO Mortgage Group, Inc. has been lost while being transported by DHL courier service to a credit reporting company. We deeply regret that this situation occurred and are keenly aware of how important your personal information is to you. We have no reason at this time to believe this information has been misused. Even so, we want to inform you of the situation, provide background about what happened, suggest some steps you can take and assistance we can provide to protect yourself from identity theft now and in the future.

How to share documents?

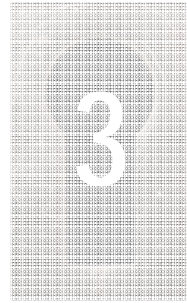
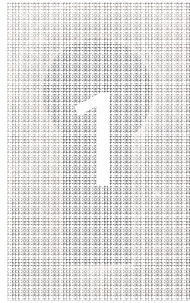
How to store data?

How to discard records?

From a security assessment perspective, what can we learn from the inadvertent disclosure breaches I just discussed? First, we have confirmed the theory that many security incidents can occur without any exploitation of traditional software vulnerabilities. Yet, they can affect a great many people.

Second, we have arrived at three of the many questions organizations must ask—and answer—when assessing their information-related risks:

- How to store data?
- How to share documents?
- How to discard records?



Attacks of Opportunity



Authored by Lenny Zeltser.
Copyright 2006. Gemini Systems, LLC.

Let's take a look at another type of threat, *attacks of opportunity*, which are also known as *low-hanging fruit* attacks. Such breaches occur as a result of the attacker looking for some system that is relatively easy to compromise, rather than targeting a particular resource.

The CME-24 worm infected at least 470,000 computers world-wide.



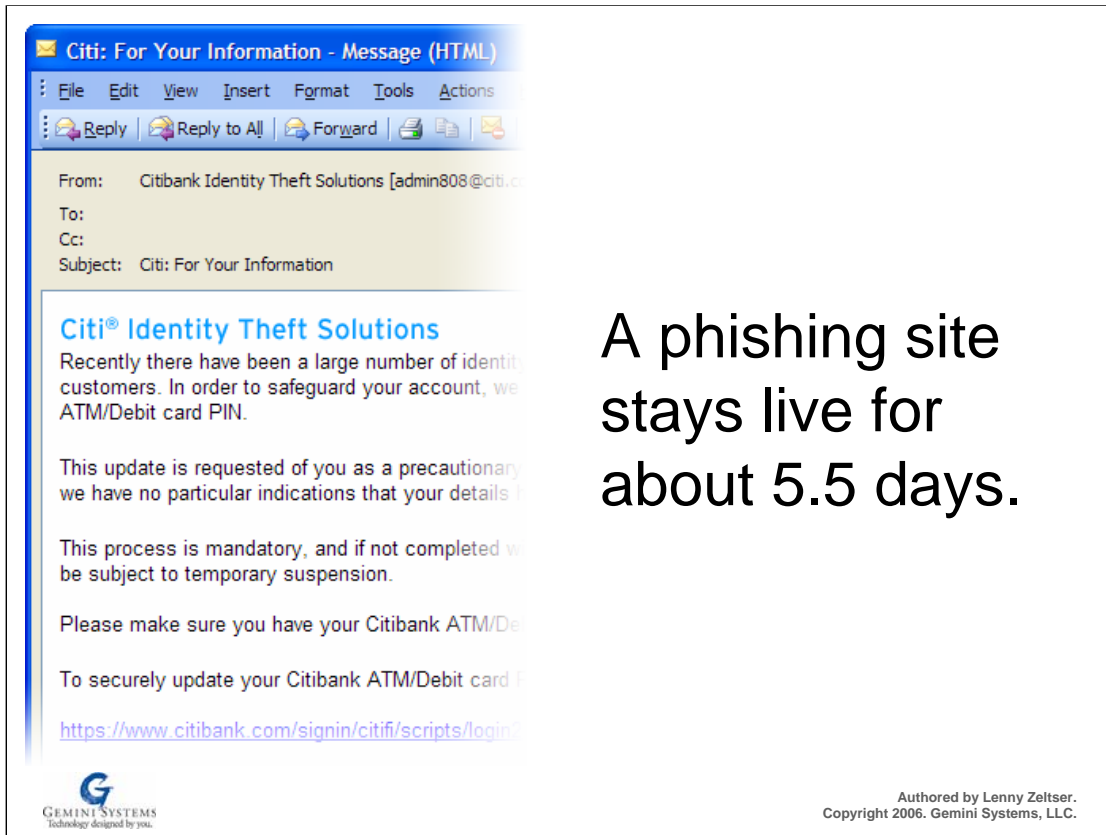
Authored by Lenny Zeltser.
Copyright 2006. Gemini Systems, LLC.

The CME-24 worm, also known by names such as BlackWorm, Nyxem, Kama Sutra, and MyWife, infected between 470,000 and 950,000 computers in the second half of January. The worm was designed to overwrite document files on the infected system on the 3rd of every month. Rather than exploiting a software vulnerability, CME-24's primary propagation mechanism was email, and the exploited "vulnerability" was the tendency of trusting email recipients to launch the malicious attachment that the worm generated.

(Statistical analysis of the worm's infection rates is documented at <http://www.caida.org/analysis/security/blackworm>.)

The following article mentions another, presumably custom-written worm that an attacker used to infect computers with bots, adware, and spyware. He justified his actions as follows, "All those people in my botnet, right, if I don't use them, they're just gonna eventually get caught up in someone else's net, so it might as well be mine."

(For details about the worm-propagated bot network, take a look at the article at <http://www.washingtonpost.com/wp-dyn/content/article/2006/02/14/AR2006021401342.html>.)



A phishing site stays live for about 5.5 days.

Phishing attacks involve unsolicited email messages that attempt to lure the victim into visiting a fraudulent website, in hopes that the person will be fooled into submitting sensitive information to the site. Such attacks have been a daily fact of Internet life for several years, and they don't seem to be going away.

According to Anti-Phishing Working Group, a phishing website remained online for an average of 5.5 days in November 2005. This gives the attackers plenty of time to harvest information from conned victims and disappear into abyss.

According to a study conducted by MailFrontier in Spring 2005, people are becoming better at identifying fraudulent emails, but often at the expense of incorrectly rejecting legitimate ones.

(Anti-Phishing Working Group's November trends report is available at http://antiphishing.org/reports/apwg_report_Nov2005_FINAL.pdf. The MailFrontier *Phishing IQ Test* study is described at http://spamdailynews.com/publish/MailFrontier_Phishing_IQ_Test.asp.)

Malicious sites used a Winamp exploit to spread spyware.



Authored by Lenny Zeltser.
Copyright 2006. Gemini Systems, LLC.

A vulnerability in Winamp media player allowed a malicious website to craft a custom playlist that, if loaded by Winamp, would allow the site to run arbitrary code on the victim's system. A February 2006 report by Sunbelt Software discussed an in-the-wild exploit that was used to install "Looking-For.Home Search Assistant" spyware software on unpatched systems. The exploiting activity was noticed less than 4 days after the vulnerability was announced.

(Sunbelt's Winamp exploit description is at: http://sunbeltblog.blogspot.com/2006/02/winamp-exploit-found-in-wi_113891339953448796.html. The "Looking-For.Home Search Assistant" spyware specimen is described http://research.sunbelt-software.com/threat_display.cfm?name=Looking-For.Home%20Search%20Assistant&threatid=14938.)

Another example of an exploit being used to distribute malicious software was documented by SANS Internet Storm Center, which discussed attempts to exploit a WMF flaw in Windows to install fake anti-spyware software Winhound. (For details about this flaw, please see <http://isc.sans.org/diary.php?storyid=972>.)

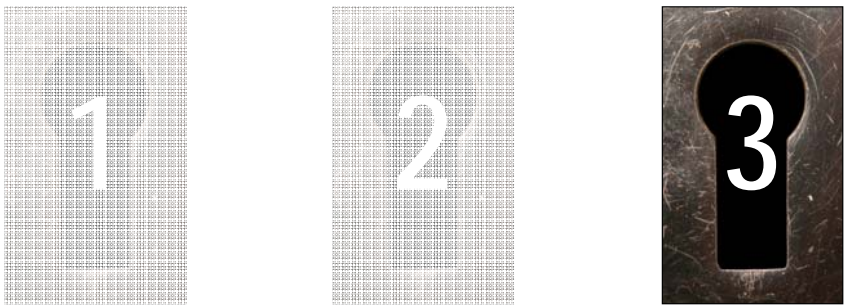
How to authenticate?

How to block malware?


How to patch software?

From a security assessment perspective, what can we learn from the attacks of opportunity I just discussed? These breaches have highlighted the need to consider a diverse set of threats when protecting the firm's information assets. Specifically, questions organizations must ask the following questions:

- How to block malware?
- How to authenticate?
- How to patch software?



Targeted Attacks



Authoring by Lenny Zeltser.
Copyright 2006. Gemini Systems, LLC.

Now, let's take a look at a third category of treats, *targeted attacks*. In contrast to opportunistic attacks that we discussed in the previous sections, these attacks are launched against a particular organization or resource, presumably because the targeted entity has something specific the attacker wants. A significant component of a targeted attack is an element of premeditation on the attacker's part.



Million Dollar Homepage was knocked offline for refusing extortion demands.

The Million Dollar Homepage (<http://www.milliondollarhomepage.com>) gained spotlight in January 2006, when its 21-year-old author Alex Tew reached his goal of earning 1 million dollars by selling all million pixels on his site to advertisers at \$1 per pixel. It was one of those ideas that was never supposed to work; however, now that it did, you are probably scratching your head wondering “Why didn’t I think of that?”

Days after the media attention brought Alex and his profitable site into spotlight, the Million Dollar Homepage was knocked offline under the weight of a distributed denial-of-service (DDoS) attack. Later reports confirmed that the attack was launched by extortionists, who demanded \$50,000 from Alex for the promise not to crash his site.

(Additional information about this site and the DDoS attack is available at http://blogs.washingtonpost.com/securityfix/2006/01/hackers_attack_.html. Another DDoS-based extortion incident is documented at <http://informationweek.com/story/showArticle.jhtml?articleID=172303265>.)

UK Parliament members were targeted via trojan-carrying emails.

Date: Mon, 02 Jan 2006 13:48:32 +0200
From: tommy@security.stat.gov
Subject: Confidential

Attached is the digital map for you. You should meet that man at those points seperately. Delete the map thereafter. Good luck.

Tommy



Authored by Lenny Zeltser.
Copyright 2006. Gemini Systems, LLC.

In January 2006, seventy government officials at UK Parliament were targeted with email messages that included an malicious attachment. The attachment was a trojan program that exploited the WMF flaw in Windows, for which no official patch was available at the time. (Microsoft released the patch 3 days later.)

This attack is believed to have originated from China. If the distributed trojan program got installed on the targeted computer, it would have provided the attackers with an almost unrestrained access to the PC.

Fortunately for the UK Parliament, the dangerous messages were blocked by MessageLabs email filters before they had reached their recipients.

(For more information about this attack, see <http://news.zdnet.co.uk/internet/security/0,39020375,39248387,00.htm> and <http://www.f-secure.com/weblog/archives/archive-012006.html#00000762>.)

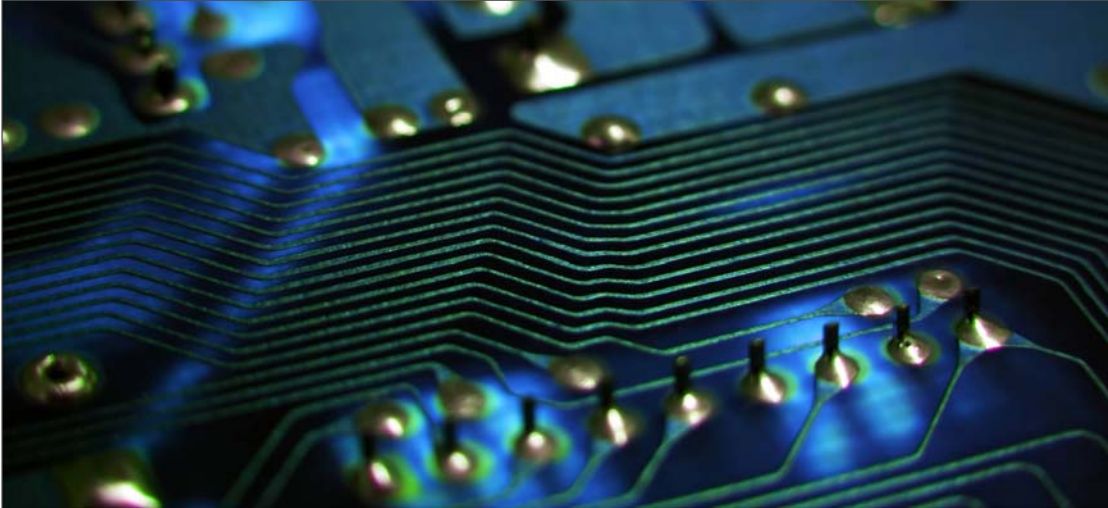


Michael and Ruth Haephrati, accused of creating custom spyware used for industrial espionage, were extradited from UK to Israel in January 2006. Trojan software, presumably created and sold by the couple, was designed to evade detection, and is thought to have been used by some of the largest Israeli companies to spy on their competitors.

According to *Haaretz* newspaper, "The companies suspected of commissioning the espionage, which was carried out by planting Trojan horse software in their competitors' computers, include the satellite television company Yes, which is suspected of spying on cable television company HOT; cell-phone companies Pelephone and Cellcom, suspected of spying on their mutual rival Partner; and Mayer, which imports Volvos and Hondas to Israel and is suspected of spying on Champion Motors, importer of Audis and Volkswagens. Spy programs were also located in the computers of major companies such as Strauss-Elite, Shekem Electric and the business daily Globes."

(The *Haaretz* article is available at <http://www.haaretzdaily.com/hasen/spages/676644.html>. Additional information about this case is available at http://www.theregister.co.uk/2006/01/31/spyware_suspect_deportation.)

Broadcom engineer was indicted on alleged theft of trade secrets.



Authored by Lenny Zeltser.
Copyright 2006. Gemini Systems, LLC.

Suibin Zhang was indicted in December 2005 on alleged theft of trade secrets. The charges allege that the Broadcom engineer downloaded proprietary files from Marvell Semiconductor Inc, Broadcom's competitor. It seems that Mr. Zhang retained access to Marvell's extranet because he was formerly employed with Netgear Inc. Because Netgear is a customer of Marvell, Mr. Zhang had access to Marvell's extranet when he worked at Netgear.

EETimes reported that, according to the indictment, two days after joining Broadcom, Mr. Zhang "allegedly loaded many of the files containing Marvell's trade secrets onto a laptop computer he had been issued by Broadcom." Several months later, he allegedly emailed some of the files to other Broadcom employees.

(The EETimes article on this subject is available at [http://www.eetimes.com/showArticle.jhtml?articleID=175400269.](http://www.eetimes.com/showArticle.jhtml?articleID=175400269))

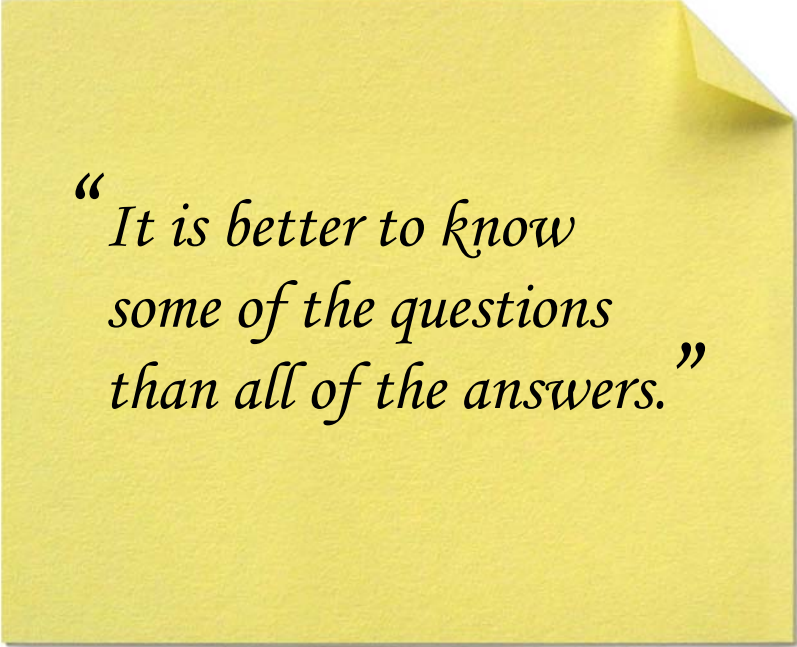
Who wants my data?

How to ensure availability?

How to share with partners?

What kinds of questions should organizations ask themselves to better withstand the targeted attacks we covered in the last section? There are a few that come to mind:

- How to ensure availability?
- Who wants my data?
- How to share with partners



*“It is better to know
some of the questions
than all of the answers.”*



Authored by Lenny Zeltser.
Copyright 2006. Gemini Systems, LLC.

James Thurber, an American writer and cartoonist, once said, “It is better to know some of the questions than all of the answers.” This is very applicable to the world of information security, where the continuously evolving threat landscape ensures that one cannot know all of the answers. Organizations can get very far, however, by taking the time to ask a few pointed questions about the threats they face and the vulnerabilities they possess.



In a world where most, if not all, systems have flaws, what kind of questions can organizations ask when designing their information security program? During this presentations we reviewed 9 of those questions, examining (with a 20-20 hindsight) some of the security breaches that happened in the near past:

- | | |
|-----------------------------|-------------------------|
| How to store data? | How to share documents? |
| How to discard records? | How to block malware? |
| How to authenticate? | How to patch software? |
| How to ensure availability? | Who wants my data? |
| How to share with partners? | |

These are some of the questions that address three key categories of threats we discussed in this presentation:

- Inadvertent disclosure
- Attacks of opportunity
- Targeted attacks

What questions have we forgotten to ask?



The last question, the one I'd like to leave you with is a more general one: What questions have we forgotten to ask? Posing this question to ourselves we can help dig a little deeper into the mysterious area of things we don't know we don't know.

This presentation has not covered all the questions organizations need to ask themselves when assessing risks or performing security assessments. Instead, we focused on those threats and vulnerabilities that were evident in the recently announced security breaches. For a much more comprehensive list, take a look at guidelines and standards such as SysTrust and ISO 17799.



Lenny Zeltser

InfoSec Practice Leader
Gemini Systems, LLC

lenny.zeltser@gemini-systems.com



Authored by Lenny Zeltser.
Copyright 2006. Gemini Systems, LLC.

If you have any questions or comments about this presentation, or if you'd like to discuss information security-related issues, feel free to drop me an email. I'll be glad to hear from you.