

The **ONE** must-attend event for Direct-to-Customer  
Operations & Fulfillment Management!

**NCOF**  
National Conference on Operations & Fulfillment

**KD**  
Mailing & Fulfillment  
Est. 1951  
Postage Discounts  
773-889-Mail

THE  
**DMA**  
Catalog Council

[Tell a friend  
about this page](#)

[Update Your Profile](#)

[Suggestion Box](#)

## (More Than) Five Questions With . . . Cybersecurity expert Peter Gregory.



When it comes to cybersecurity, there's good news *and* bad news.

The bad news, of course, is that cyberattacks and other threats to American businesses' Web infrastructures are on the rise – and the onset of war with Iraq further elevated risks. *USA Today* last week reported that, since the war's start, Internet security experts say several thousand Web sites have been defaced with anti-war images and slogans at the hands of "hactivists." And perhaps even more troubling is the vulnerability of vital business data if a company fails to secure its cyberspace.

The cost to your business, should a cyberattack occur, could mean hundreds of thousands of dollars in lost revenue due to Web inactivity while the situation is rectified, not to mention expenses associated with undoing the damage and the immeasurable cost of bad public relations and the lost trust of your customers. Cybersecurity is no longer just an "IT" issue; it's something that could have a dramatic and long-lasting impact on your entire company.

Now, the good news: the solution is easier than you think. To get to the "bottom" of this important issue, *The Bottom Line* consulted Peter Gregory, the author of several books on information security, a frequent conference speaker, and a ComputerWorld magazine columnist. We learned, among other things, that when it comes to cybersecurity, a little prevention goes a long way.

We also learned that, sometimes, five questions just don't cut it. Following you will find Peter's responses to our *nine* questions about cyberattacks, spanning what they are, how they could impact your company, and what you can do to prevent them.

*Q. The word cyberattack has become a popular buzzword, which can make it difficult to distinguish between what's hype and what's reality. What exactly constitutes a cyberattack?*

*A. A cyberattack is an effort, perpetrated by one or more persons, intended to disrupt or damage an organization's*

information processing functions. The most frequent targets are an organization's Web site, attacked from a distance over the Internet. However, any other computer system that is accessible via the Internet, or by dial-up modem, can also be a target.

*Q. What forms could it take?*

A. Cyberattacks generally fall into four categories: denial of service, defacement, the stealing of sensitive information, and mechanized attacks by viruses or "worms."

A "denial of service" attack is essentially a flood of data that is sent to the target in order to overwhelm it with useless data. It is called "denial of service" because the primary result of the attack renders the attacked system unable to provide the legitimate service that it is designed to perform.

The example that I most often like to bring up that illustrates a denial of service attack is a strike by French farmers in the 1970s. Hundreds of farmers in France were fed up with some economic condition (I cannot recall whether it was high fuel prices, low market prices, or something else – but it doesn't matter), and so they organized and drove their farm tractors into Paris and parked them on the freeways. No legitimate users of the freeways (commuters, delivery trucks, etc.) were able to use the freeways because the tractors had them completely jammed up. The farmers had successfully attacked the Paris freeway system with a denial of service attack.

The second type of attack is commonly known as "defacement." It is so-called because the perpetrator breaks into the victim Web site, erases its home page, and substitutes his (or her) own home page content. Let me illustrate with a hypothetical – but plausible – example. A company's Web site is defaced by one or more vandals. People who visit the Web site do not see the expected company's Web page, but instead some text and perhaps photos, all regarding some political situation somewhere in the world.

Defacements cause more embarrassment than actual damage. This is because the victim's Web site code is probably backed up (copied to another system or to computer tapes or CDs), so it is likely that in a matter of a few hours the company is able to restore their original Web site code. However, the defacement can be a matter of great embarrassment, both because of the fact that the perpetrators were *able* to deface the Web site, but also because of the nature of the content that the perpetrators placed on the Web site. Some people who deface Web sites use statements or images depicting violence, pornography, or other content that is shocking or embarrassing in nature.

The third type of cyberattack is one where the perpetrator is able to steal or sabotage sensitive information in the organization's computers. While these types of attacks occur frequently, only high-profile cases garner any publicity. In early 2003, someone was able to break into a large credit-card processing company's computers and steal several million credit card numbers. In another recent incident, the Social Security numbers of thousands of students were stolen from a computer at a university in Texas. A few years ago, an individual in Russia was able to

illicitly transfer millions of dollars from a large U.S. financial institution to several off-shore bank accounts.

Now, so far I've been discussing the kinds of cyberattacks that are carried out "one on one" – that is, a sole perpetrator attacking an individual Web site or organization. And while this type of attack is common, another type of attack is having far more impact on the e-commerce community: mechanized attacks by viruses, Trojan horses, and "worms."

Viruses and Trojan horses have been around for many years. These are little bits of nasty computer code called "malware" – for "malicious software" – in the industry. Viruses and Trojan horses are typically embedded into computer programs and e-mail attachments, and do nothing until the recipient "activates" them by opening an attachment, for instance. This is why we hear more and more often that it is unsafe to open e-mail attachments from people we don't know or attachments contained in unusual messages from people we do know. A common type of Trojan horse in the late 1990s would spread from user to user via e-mail, by sending copies of itself to persons in one's e-mail address book.

By far, the most spectacular attacks have taken the form of "worms." The ultimate in malware, worms spread automatically with no human intervention required. The NIMDA and Code Red worms in 2001 encircled the entire worldwide Internet in just a few days, infecting hundreds of thousands of vulnerable systems. On January 25, 2003, the Sapphire/Slammer worm infected nearly 100,000 vulnerable hosts within ten minutes. The impact of the Sapphire/Slammer worm was so great that some large banks' ATM networks failed, some airlines had to cancel flights, and elections in some areas were disrupted.

Worms spread by "scanning" networks for vulnerable computers. When a worm finds a vulnerable computer, it sends a copy of itself to that computer, which fires up a new copy of the worm and begins searching for more vulnerable computers.

*Q. How are these attacks performed?*

A. The computer software programs that are used to create Web servers and other Internet services is extremely complex, so much so that it is impossible to prove that these programs are 100-percent accurate and 100-percent safe. Security research companies and universities spend a lot of time looking for flaws – including security flaws – in computer software.

Occasionally, a security flaw is found. For instance, it may be determined that the popular Web server program, Microsoft IIS (Internet Information Server), has a particular flaw that permits an attacker to take over the server program – and the computer that it is running on – if the attacker transmits a special combination of characters to the Web server program.

This actually occurs a few times each year. The person(s) who find a flaw will contact either the CERT/CC

(Computer Emergency Response Team Coordination Center – the clearinghouse for reporting security flaws and attacks) or the software vendor. The software vendor will confirm the existence of the flaw and – if it is real – will engineer a fix, usually called a "patch," that will eliminate the flaw.

Once the patch is available, CERT/CC and the software vendor (in this example, Microsoft) will announce the existence of the flaw and instructions on how to obtain the patch that will fix it.

Most of the attacks that are perpetrated on the Internet involve an exploitation of these known flaws in software. But you might ask yourself, how could these attacks be successful when the existence of the flaw – and the fix – has been publicized? The answer may surprise you: it is because over half of the organizations that run Internet applications such as Web servers never install these security patches!

I agree that this is amazing news. There are two reasons why organizations do not install security patches: many do not ever learn of the existence of security patches, and those that do often fail to take the time to install them because they are too busy with other things.

Yes, even to the present day, vast numbers of organizations continue to ignore the security alerts. Many do not install the security patches because they do not wish to incur the "downtime" associated with the installation of patches. Most patches require that the computer be taken offline for several minutes to an hour – and doing so may mean that an organization's Web site is unavailable for that period of time.

As we have seen lately, this often turns into a cruel irony: an organization chooses not to schedule the hour or so of downtime required to install security patches, so instead the organization is attacked at a time of the attacker's choosing, often resulting in downtime of several hours – if not days or longer – and far more damage to the organization's integrity and reputation.

But wait, there's more irony. One could argue that the organization could not install the security patches quickly enough to protect itself from attack. Well, okay, but let me tell you this: most cyberattacks that exploit known security weaknesses occur four to eight months after the existence of the weakness – and its fix – is publicized.

So let me summarize: most cyberattacks are perpetrated against known security flaws on Web sites that have not had recent security patches installed, even though the existence of these patches had been known for half a year or longer.

*Q. How concerned should businesses be about this?*

A. Any business with an Internet connection must be aware that there are risks associated with being connected to the Internet. The amount of risk that any one business faces is dependent on many factors, including the number and type of Web servers the business may have, the functions that are performed on its Web servers, the types of

firewalls, anti-virus, and intrusion detection systems that the business is using, and the amount of security knowledge possessed by the persons who manage the Web site.

Every business with a connection to the Internet is being automatically "probed" by hackers using sophisticated tools. These probing tools are searching thousands of computers' sites each day for specific weaknesses. A skilled hacker can exploit a specific weakness in order to take over and control the computer. Once the hacker controls the computer, he or she may choose to deface it, or steal credit card numbers, social security numbers, and other sensitive information that it may contain.

*Q. Specifically, how might those engaged in e-commerce be at risk for cyberattacks?*

A. The most common method used to attack an e-commerce server is the use of a program or script that is designed to exploit known flaws or weaknesses. Organizations that are at risk are those that have failed to apply all security patches or have not followed "best practices" for securing their systems.

*Q. Are there any warning signs? What factors would identify a company as a likely target?*

A. At the risk of sounding repetitive, the primary warning sign is the failure to install security patches and follow best practices for securing systems. Hackers can use automated programs to search the Internet and find vulnerable systems. It really doesn't matter if you're a highly visible site such as Amazon.com, or a small startup company that no one has heard of. If you have vulnerable systems connected to the Internet, the hackers will find you.

But the playing field isn't exactly level. Some sites are targeted more often and more aggressively than others. In times of international conflict, U.S. government and military sites are attacked around the clock. Web sites associated with certain opinions, racial, cultural, or religious affiliations can be targets as well. Any Web site that may be considered a "lightning rod" will attract hackers who wish to disrupt it, deface it, or take it "off the air."

Warning signs can also be recognized by Intrusion Detection Systems (IDS), which take the form of devices connected to the network (Network Intrusion Detection Systems, or NIDS) and software programs installed on computers (Host-based Intrusion Detection Systems, or HIDS). IDSs are designed to recognize the signs of anomalous activities associated with cyberattacks, and will generate "alarms" that can be sent to the individuals who are responsible for maintaining Web servers and other systems.

Intrusion Detection Systems have been around for only about the past five or six years, and the companies that make them are still making vast improvements to them each year. Companies that purchased IDSs in years past were plagued with scores of "false positives" – alarms that the IDSs generated that did not constitute real threats. Like the boy crying "Wolf," many companies began to ignore their IDS alarms after being conditioned by so many false positives. But the IDSs being produced today are far more accurate, although it would be stretching it to say that the problem of false positives has been completely solved.

*Q. We've read about some Web sites being vandalized with anti-war messages and the like. How can this be prevented?*

A. Ninety-nine percent of defacements – as they are called – can be prevented simply by following well-known best practices such as installing security patches and "hardening" Web servers by configuring them to be as secure as possible.

Best practice information and security patches will not grow legs and try to find every organization that needs them. Rather, one or more informed and motivated individuals in each company must realize that such information is needed – then find and retrieve it, study and understand it, and apply it. All of this takes time.

Two excellent and respected sources for best practices for securing computer systems are the CERT/CC at [www.cert.org](http://www.cert.org), and SANS at [www.sans.org](http://www.sans.org).

The best source for vendor-neutral security alert information is CERT/CC at [www.cert.org](http://www.cert.org). You can sign up to have CERT/CC automatically e-mail you security alerts the minute they are available. But, you should also sign up for security alerts from your hardware and software vendors, to make sure you are getting the most complete and accurate information.

Hackers and their arsenals of tools are becoming increasingly complex and sophisticated; understanding and preparing for cyberattacks requires a great deal of specialized knowledge. Companies that do not have this knowledge should retain the services of a respected information security consultant. Any such consultant should have one or more industry-recognized security certifications such as CISSP (Certified Information Systems Security Professional, the most respected certification) or CISA (Certified Information Systems Auditor), and have a solid track record of being able to identify security risks in any company's computers and networks.

*Q. Should a cyberattack occur, how should companies react?*

A. A company that has been cyberattacked must take steps to identify and isolate the attack. This will take skills known to computer security experts who have been trained in forensics, the art of locating and preserving evidence on a computer should an organization decide to prosecute the perpetrator(s) of an attack.

By isolating the attack, the company is trying to prevent the attacker from harming other computers. Once an attacker has successfully penetrated one computer, it is often easy for the attacker to then locate and penetrate other computers in the company.

Next, the company must rebuild the computer(s) that has been attacked. It is tempting to restore software and data files from backup tapes; however, this is a risky venture, since the attackers may have infiltrated the computer days or weeks before the attack was evident. Restoring data from tape may clean up the computer, but it may also

preserve any "back doors" that the attacker used to penetrate the system in the first place. The best course of action for the company is to do a "bare metal restore" – this means that system engineers will need to completely erase all software and information from the computer and reinstall everything from the original "release media" – the tapes or CD-ROMs containing the software purchased from its manufacturer(s).

A bare metal restore will ensure that all "back doors" and other hacker tracks and damage will be eliminated, but you have to realize that a full metal restore takes hours or – more likely – days to complete. Few companies can afford to have their Web sites or other systems down for that long. The prospect of such an ordeal makes the task of making computers more secure in the first place – in order to prevent these incidents – more reasonable and justifiable.

*Q. Is this specifically an IT matter, or should other departments be briefed on what to look for and how to respond?*

A. Remember, IT exists not for its own sake, but to support important business functions. IT should have the sole responsibility for developing security knowledge and expertise, for securing computer systems, and for watching for signs of attacks. However, the company departments that depend upon IT support for their functions should participate in the planning needed for responding to incidents such as cyberattacks. IT and business departments should jointly develop contingency plans so that critical business functions can continue despite events such as cyberattacks.

*Peter H. Gregory, CISSP, CISA, is the author of several books on information security, a frequent conference speaker, and ComputerWorld magazine columnist. Mr. Gregory resides in the Seattle area with his wife and three daughters. He can be reached at [phg@hartgregorygroup.com](mailto:phg@hartgregorygroup.com), and at <http://www.hartgregorygroup.com/>.*

[© Direct Marketing Association](#) | [Privacy Statement](#) | [Disclaimer](#) | [Contact Us](#)