

Reporter, The -  
Camden, Miller,  
Morgan  
Camdenton, MO  
Circ. 2000  
From Page:  
10  
11/26/2008  
14415



## Tips for protecting your business from cyber attacks

**LAKE OF THE OZARKS** - Businesses today rely on corporate technology networks and Internet connections, however, this global connectivity comes with the risk and liability of a data network breach.

No business or organization is immune to cyber attacks, which is why many business owners are allocating time and resources towards network security.

According to The Economist, 45 percent of companies have appointed a Chief Risk Officer, with another 25 percent planning to recruit one in the future.

Computer viruses can halt work productivity and pose a threat to business continuity by corrupting operating systems, applications, programs and files.

"Train employees on how to update anti-virus software and download security patches from software vendors," said John Weant, business account technician at Socket, a Missouri telephone and Internet provider. "New vulnerabilities and weaknesses are exposed every week, so it is important to stay on top of fighting them."

It's crucial to have a security policy in place, but if staff members aren't aware of how and why it operates, the policy's strength will be diminished.

The Department of Homeland Security has a National Cyber Alert System that provides

free, timely information and updates on how to better secure computer systems.

These notifications can be delivered by e-mail or RSS feed, and interested businesses and individuals can sign up at [www.us-cert.gov](http://www.us-cert.gov).

Weant also recommends changing passwords frequently and using passwords that aren't easily guessed.

"Never provide your password, personal or financial information in response to an e-mail request," said Weant. "Also, refrain from typing or saving your password on computers that you do not exclusively control."

Hackers are continuing to increase in boldness and creativity, but simple negligence can also leave a company's Web site vulnerable.

"A company could forget to register their domain with an official registrar on a Friday, and by Monday their domain could be redirecting people to a malicious Website," said Weant.

Companies and other organizations spend significant resources in developing an online presence, so failing to update and maintain leases on domain names or Internet Protocol (IP) addresses could be devastating.

Having a compromised Web site poses a great risk to a company's name and reputation.

The legal costs of recovering hijacked

domain names are extensive, but losing the trust of customers, many of which will move on to a competitor they perceive to be better able to protect their personal information, is much worse.

Every company should start by assessing risks and then building effective response capabilities.

Hold a security audit to expose strengths and vulnerabilities within the network as well as give a complete overview of an organization's security requirements. Sometimes this requires a fresh, outside perspective.

"Consider contracting a third-party organization to perform the audit," said Weant. "Third-party agencies have the objectivity and expertise to ensure audit goals are met."

Believe it or not, most cybercrimes are instigated by people within a company. For this reason, the physical removal of data from corporate facilities should be strictly controlled and monitored.

Prohibit employees from installing unauthorized software and applications from any source.

Most importantly, make sure security education and training of employees is a permanent and ongoing exercise.

"It's important to be proactive, because by the time law enforcement officials get involved, the damage will have





already been done," said Weant.

Information security has become an essential part of the corporate culture. Cyber criminals are constantly watching for small oversights in a business' network infrastructure, so it is extremely important that organizations dedicate

specific resources such as staffing, budget and time towards cyber security.

Unfortunately, very few cyber security conflicts, once solved, remain solved. Cyber security requires an ongoing assortment of measures and approaches that must be updated

and tested regularly to ensure the security of essential operating and financial systems. By taking a versatile and innovative approach towards information security, business owners can remain confident about their company's resiliency to cyber attacks.

Reporter, The -  
Camden, Miller,  
Morgan  
Camdenton,MO  
Circ. 2000  
From Page:  
10  
11/26/2008  
14415