

Barnes Wendling

"One of the 99 Best Places to
Work in Northeast Ohio"

North Coast WINNER

[Home](#) [About Us](#) [Network](#) [Industries](#) [Valuations](#) [Corporate Finance](#)

[Personal Info](#) [Configure Niche Content](#) [Calculators](#) [Saved Articles](#) [Refer Colleague](#) [Unsubscribe](#) [Feedback](#)

Hi, Robin. Here is your e-newsletter for July 26, 2011.

Glossary: [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#) |

Help Combat Cyber Attacks with These Steps



Sophisticated Cyber Criminals Target Company Networks

Cyber attacks have the potential to inflict tremendous economic damage. The attacks can even rise to the level of "cyber warfare" when one nation infiltrates another nation's computer systems or networks in order to inflict damage. In fact, the threat is so great that a number of government agencies, including the Department of Defense, National Security Agency, U.S. Secret Service, FBI, and Department of Homeland Security, have joined the fight against cyber attacks.

To make matters worse, data security violations have become a regular occurrence. According to the Privacy Rights Clearinghouse, more than 2,500 data breaches involving nearly 600 million records have been made public since 2005.

Specifically, cyber attacks waged against companies include the following threats:

Intellectual property theft - U.S.-based companies are known throughout the world for developing cutting edge inventions, designs, and other intangible assets. Therefore, these assets are vulnerable to online theft.

Fraud - Stealing credit card information and then selling the information on the black market can be highly profitable.

Attacks upon infrastructure - A country's power grid or water supply is particularly vulnerable to attack. So too are financial institutions and trading systems such as the New York Stock Exchange and the NASDAQ.

"As more information is stored in cyberspace, target-rich environments are created for sophisticated cyber criminals. With proper network security, businesses can provide a first line of defense by safeguarding the information they collect. Such efforts can significantly limit the opportunities for these criminal organizations. Furthermore, the prompt reporting of major data breaches involving sensitive personally identifiable information to the proper authorities will help ensure a thorough investigation is conducted."

-- U.S. Secret Service Deputy Special Agent Pablo A. Martinez in testimony before a U.S. House of Representatives subcommittee on May 4, 2011

Telecommunications - Attacking a telecommunications system could provide a foreign government with the ability to force the network's failure as well as intercept communications.

Ensuring that unauthorized users are not granted access to your company's information and infrastructure poses considerable challenges. There are no quick fixes. Instead, combating cyber attacks requires a highly organized and integrated program of activity that can include the following steps:

Require Employees to Assist in the Fight.

An information security program can only be effective if it is fully understood and followed by employees. The program should include a detailed set of information security policies and procedures that are frequently reviewed and updated to reflect the latest intelligence and countermeasures. On an annual basis, employees should complete mandatory testing to assess their knowledge and understanding of the company's information security policy and procedures. Part time employees (as well as contractors using a company's systems) should also be required to complete annual testing. To ensure compliance, consider revoking system access for those who do not complete the testing.

Ensure your company's information security policies and procedures contain clear and concise guidance for employees regarding:

- *Login credentials* - Employees should be instructed on how to protect their system login credentials. Passwords should be changed at least every 90 days.
- *Paper document storage and destruction* - Confidential documents should be stored in locked cabinets and ultimately destroyed in a secure manner.
- *Software installed without prior approval* - Commercially available software may include security flaws that can provide hackers with an open "door" to an organization's infrastructure. Prohibit installation on company computers.
- *Phishing e-mails* - Educate employees on the dangers of responding to unsolicited emails that appear to be sent by a legitimate organization. In fact, the e-mail originates from a third party that intends to gain unauthorized access to your company's data by stealing an employee's credentials.
- *Personal use* - Provide clear and consistent guidance regarding how and when the company's e-mail and Internet access can be used for personal purposes.
- *Company equipment use* - Provide frequent communications and enforce the company's policy regarding the use of thumb drives, external hard drives, personal laptops, PDAs and unsecured WiFi networks.

Remember that an Ounce of Prevention is Worth a Pound of Cure. Verifying or authenticating a user as having permission to access a network can dramatically reduce the probability that intruders will gain access to your company's data and infrastructure. There are a number of third party authentication tools available. Your company's information technology department



**Government Contractors
Are Vulnerable to Attacks that
Can Threaten National Security**

Federal, state and local governments routinely engage companies from the private sector to provide products and services. The connections formed and facilitated online between the public and private sector are especially strong in the United States. Companies that contract or subcontract to the federal government often have classified material in their possession. As a result, government contractors can easily find themselves subjected to cyber warfare. Breaches can potentially harm national security.

can assess which tools may benefit your organization. Authentication is far from foolproof, but your company can take steps to strengthen its defenses. This can help convince online intruders that their time and efforts are better spent elsewhere

Be Open to Working with the Government. The federal government has invested in cyber attack prevention and detection and frequently steps into investigations. The FBI is now working with federal prosecutors to determine the origin of the the Sony cyber attack that jeopardized the personal information of millions of PlayStation Network customers.

Depending on the industry, there are regulations that require quick reporting and co-operation with law enforcement.

In addition, various federal government departments tasked with combating cyber attacks are actively looking to partner with the private sector. Any partnership with the government is not without its challenges. Before the partnership can be initiated, your company's corporate counsel must be involved in the reviewing the arrangement. Combining best practices from the public and private sector can create an exceptionally strong defense against cyber crime. Your company may be able to benefit from the deployment of technology developed in the public sector that far exceeds the capabilities of commercially available solutions.

Protecting your company's assets against cyber attacks requires employee awareness, a robust set of policies and procedures that are consistently enforced, and the implementation of high performing authentication tools. Depending on your company's industry and overall exposure to cyber warfare by foreign nations, it may also involve cooperation with the federal government.

[Email to a Friend](#)

[Save Article](#)

[Email Firm](#)

[Share This](#)

Feedback

Is this item worthy of implementation?	Yes	No	Maybe
Is this item worth sharing with other associates?	Yes	No	Maybe
Did this item present value to you and your business?	Yes	No	Maybe

Comments:

[Personal Info](#)

[Unsubscribe](#)

[Your Privacy](#)

[Disclaimer of Liability](#)

© 2011. Powered by BizActions

Our firm provides the information in this e-newsletter for general guidance only, and does not constitute the provision of legal advice, tax advice, accounting services, investment advice, or professional consulting of any kind. The information provided herein should not be used as a substitute for consultation with professional tax, accounting, legal, or other competent advisers. Before making any decision or taking any action, you should consult a professional adviser who has been provided with all pertinent facts relevant to your particular situation. Tax articles in this e-newsletter are not intended to be used, and cannot be used by any taxpayer, for the purpose of avoiding accuracy-related penalties that may be imposed on the taxpayer. The information is provided "as is," with no assurance or guarantee of completeness, accuracy, or timeliness of the information, and without warranty of any kind, express or implied, including but not limited to warranties of performance, merchantability, and fitness for a particular purpose. www.barneswendling.com

1215 Superior Avenue, Suite 400 Cleveland, OH 44114