



INDUSTRY LEADERSHIP TIP CARD

DID YOU KNOW?

- The yearly cost of cyber crime per organization spanned a range of **\$1.3 million** to **\$58 million**.¹
- The cost of cyber crime increased **26 percent**, or **\$2.6 million** from 2012 to 2013.
- **Seventy-five percent of cyber attacks are opportunistic** – not targeted at a specific individual or company – and the vast majority of those are financially motivated.²
- **Seventy-six percent of network intrusions** exploited weak or stolen credentials. Strict policies are required to reduce this easily preventable risk.³

SIMPLE TIPS

1. Implement a layered defense strategy that includes technical, organizational, and operational controls.
2. Establish clear policies and procedures for employee use of your organization's information technologies.
3. Implement technical defenses, such as firewalls, intrusion detection systems, and Internet content filtering.
4. Update your anti-virus software often.
5. Following your organization's guidelines and security regulations, be sure to regularly download vendor security patches for all of your software.
6. Change the manufacturer's default passwords on all of your software.
7. Monitor, log, and analyze successful and attempted intrusions to your systems and networks.

RESOURCES AVAILABLE TO YOU

US-CERT.gov

The United States Computer Emergency Readiness Team's (US-CERT) has numerous resources and tips for both technical and nontechnical individuals. US-CERT desktop software tool can be used to assess control systems and information technology network security practices.

¹ Symantec, "Mistakes are costing companies millions from avoidable data breaches", 2013

² Business News Daily, "Inside Job: How to Prevent Employee Data Breaches", 2013

³ SHRM, "SHRM Workplace Forecast: The Top Workplace Trends According to HR Professionals", 2013.



FBI.gov

The Federal Bureau of Investigation (FBI) leads the national effort to investigate high-tech crimes, including cyber-based terrorism, computer intrusions, online sexual exploitation, and major cyber frauds.

Cybercrime.gov

The Department of Justice (DOJ) component responsible for implementing national strategies in combating computer and intellectual property crimes worldwide.

StaySafeOnline.org

The Stop.Think.Connect.™ Campaign is a cooperative agreement between the Department of Homeland Security and the National Cyber Security Alliance (NCSA). Get more information from NCSA about the Stop.Think.Connect.™ Messaging Convention, which is the formal way that industry participates in Campaign activities.

IF YOU'VE BEEN COMPROMISED

- Be sure to follow your organizations rules and regulations regarding cyber threats. Report computer or network vulnerabilities to US-CERT via the hotline: 1-888-282-0870 or www.US-CERT.gov.
- Inform local law enforcement of the state attorney general as appropriate.
- Report stolen finances or identities and other cybercrime to the Internet Crime Complaint Center at www.ic3.gov.
- Report fraud to Federal Trade Commission at www.ongaurdonline.gov/file-complaint.

Stop.Think.Connect.™ is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. The Campaign's main objective is to help you become more aware of growing cyber threats and arm you with the tools to protect yourself, your family, and you community. For more information visit <http://www.dhs.gov/stopthinkconnect>.



**Homeland
Security**

www.dhs.gov/stopthinkconnect



STOP | THINK | CONNECT™
