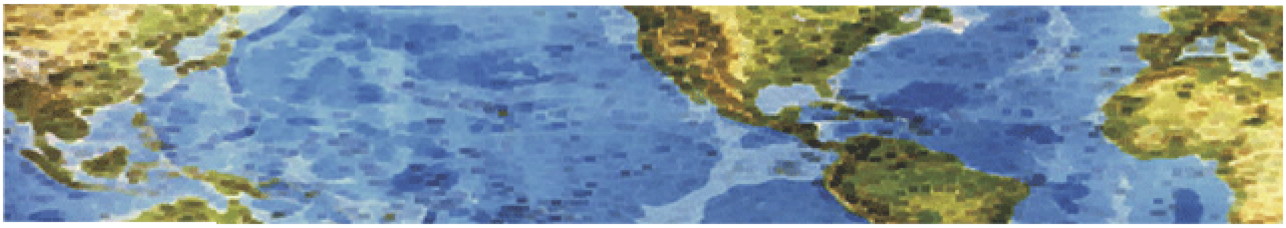
HALL ASSOCIATES



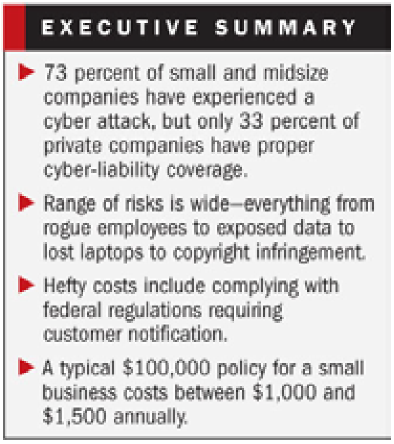
Risk-Based Decision Making Commentary
28 February 2014 Newsletter

Cybersecurity is a Big Deal for Small Business

Cyber attacks against big businesses tend to get a lot of attention. Media extensively covered the incidents involving AT&T in 2010 (over 14,000 emails stolen), Sony in 2011 (over 77 million credit card numbers stolen), and Target in 2013 (over 40 million credit card numbers stolen). While big businesses may get all the press, small businesses are not immune from a cyber attack. The 2013 Verizon Data Breach Investigations Report (http://www.verizonenterprise.com/DBIR/2013/) found that over 40 percent of all data breaches occurred in companies with less than 1,000 employees.

Small businesses may be more vulnerable to attacks because cyber criminals assume they have weaker network security. The 2012 Small Business Study, conducted by the National Cyber Security Alliance and Symantec, found that 83 percent of small businesses do not have written cybersecurity plans, with 11 percent of small businesses reporting that they have no one responsible for cybersecurity. With small businesses increasingly dependent on the Internet to conduct business, the effect of cyber incidents can be devastating. So how can small businesses protect themselves? It helps to start with the basics. Follow these tips from the Small Business Tip Card:

1. Keep a clean machine. Use and regularly update antivirus and antispyware software on all computers.
2. Connect safely. Secure your Internet connection by using a firewall, encrypting information, and hiding your Wi-Fi network.
3. Safeguard information. Establish security practices and policies to protect sensitive information; educate employees and hold them accountable to the Internet security guidelines and procedures.
4. Focus on people. Require that employees use strong passwords and regularly change them. Educate your employees on the importance of safe cybersecurity practices.

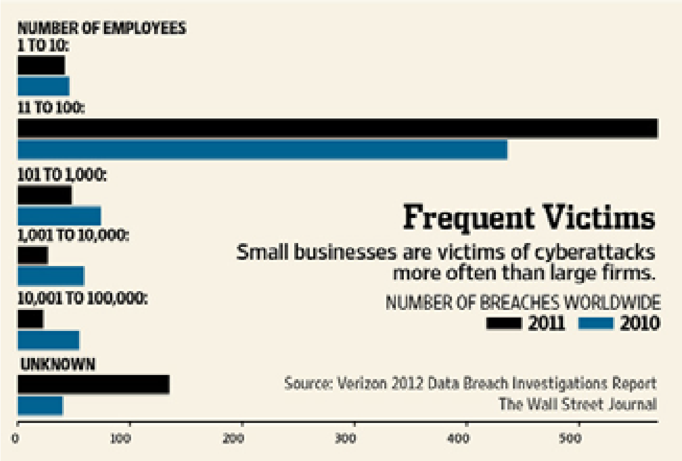


EXECUTIVE SUMMARY

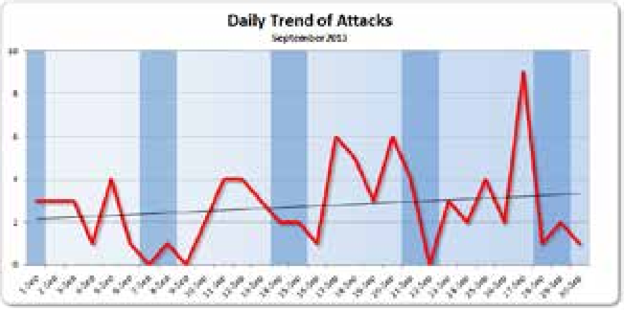
- 73 percent of small and midsize companies have experienced a cyber attack, but only 33 percent of private companies have proper cyber-liability coverage.
- Range of risks is wide—everything from rogue employees to exposed data to lost laptops to copyright infringement.
- Hefty costs include complying with federal regulations requiring customer notification.
- A typical $100,000 policy for a small business costs between $1,000 and $1,500 annually.

There are a number of government resources specifically for small businesses available:

The National Institute of Standards and Technology has issued a Cybersecurity Framework that provides best practices for use in all critical infrastructure sectors. The Framework also provides a comprehensive set of Cybersecurity Best Practices for ANY organization/business regardless of size. Contact me if you are interested in learning more about this resource and how to apply it.



Source: Verizon 2012 Data Breach Investigations Report
The Wall Street Journal



The Federal Communications Commission (FCC) Small Biz Cyber Planner (http://transition.fcc.gov/cyber/cyberplanner.pdf) is a tool for businesses to create custom cybersecurity plans. Developed in partnership with the Department of Homeland Security (DHS), the National Cyber Security Alliance, and private sector partners, the Small Biz Cyber Planner includes information on cyber insurance, advanced spyware, and how to install protective software.

The U.S. Chamber of Commerce Internet Essentials for Business 2.0 guide (https://www.uschamber.com/internet-security-essentials-business-20) for business owners, managers, and employees. The guide focuses on identifying common online risks, best practices for securing networks and information, and what to do when a cyber incident occurs.

The U.S. Small Business Administration Cybersecurity for Small Business training course (http://www.sba.gov/tools/sba-learning-center/training/cybersecurity-small-businesses) covers the basics of cybersecurity and information security, including the kind of information that needs to be protected, common cyber threats, and cybersecurity best practices.

Another helpful resource for businesses looking to improve their cybersecurity and manage their cyber risks is the SANS Institute’s Top Critical Security Controls for Cyber Defense (http://www.sans.org/critical-security-controls/) . For each security control listed, SANS recommends quick actions to more advanced cyber activities to help protect against cyber attacks and intrusions.

IF YOU’VE BEEN COMPROMISED

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