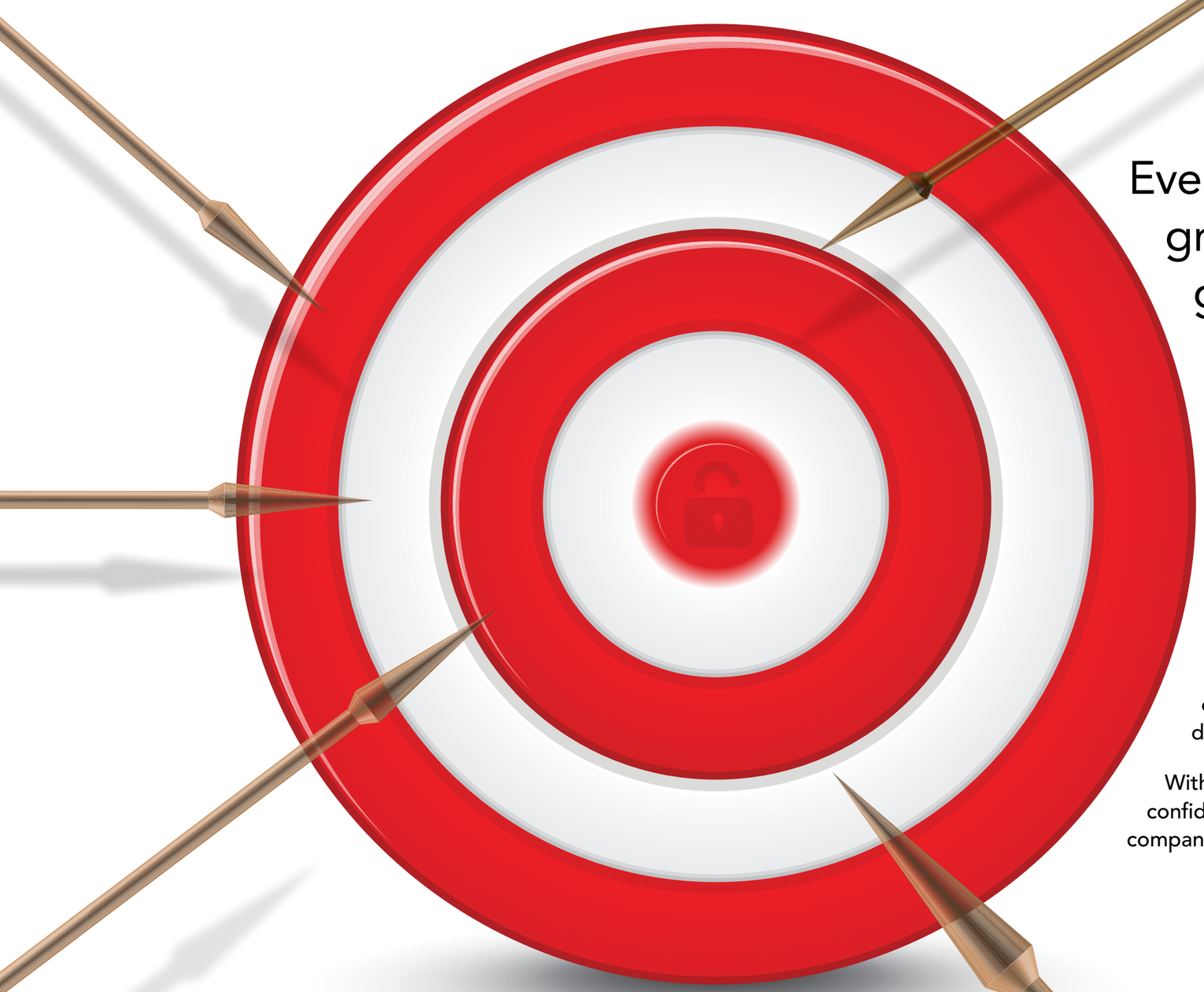
Keep Cyber Threats from Destroying Your Company

VIRUS

LabTech®



Every year, security risks are growing, and that growth isn't going to stop.

Every company is a target, no matter its size, function or annual revenue. Security risks come from every direction – malware, social networks and even employees. Every company has information worth protecting, and you owe it to your users to keep every byte safe and secure.

The increased attention from corporate America and the federal government has helped transform cybersecurity from a niche area to a key growth sector that is likely to receive a larger and larger chunk of private and public sector budgets. In 2012, the 56 companies in one study experienced 1.8 successful attacks per company per week, an increase of 42% from the previous year. Yet only 19% of companies say they are "very confident" in their security defenses.

With so many companies reporting cyber intrusions and a lack of confidence in IT security, it's a great time to make sure that your company is protected. Here's what to consider.

"Even though the US Department of Homeland Security has recognized cybercrime as a serious threat to the country's critical infrastructure and economy, 67% of US cybersecurity professionals said that their agency is 'not ready to fend off hackers'."

– Melanie Watson, IT Governance [iv]

1 Threats Get More Common and Malicious

The past five to six years have seen the growth of threats like spam, phishing, malware and malicious websites. While those threats continue to grow, new ones are also being added to the mix. Attacks are getting more disruptive and costly as they target sensitive information and reduce productivity.

The threats are so malicious that even the United States military is on the offensive. The chief of the military's newly created Cyber Command is establishing 13 teams of programmers and computer experts who could carry out offensive cyberattacks on foreign nations if the United States were hit with a major attack on its networks.[v]

"The most costly cybercrimes are those caused by denial of service, malicious insider and web-based attacks. These account for more than 58% of all cybercrime costs per company on an annual basis."

– PONEMON INSTITUTE [x]

Some of the newest threats that target companys and the government include:

- **Advanced Persistent Threat (APT) –** These attacks combine social engineering and malware to target a specific entity and steal trade secrets, customer data or other confidential information. APT attacks increased 42% overall in 2012, with a significant increase against small businesses.[vi]

- **Denial of Service (DoS) –** DoS attacks are created to make a machine or network resource unavailable. Recently, computer resource-reliant call centers have come under attack with a new version of DoS – TDoS, which floods telephone lines at a call center with repeated calls from spoofed numbers.[vii]

- **IPv6 Protocol Threats –** The latest revision of the Internet Protocol, IPv6, has become a new target. Cybercriminals are finding ways to exploit vulnerabilities in the protocol and areas where system administrators left openings during their transition from IPv4.[viii]

- **Mac-targeted Malware –** The popularity of iPhones and iPads has helped fuel the laptop market, and the MacBook market share has steadily grown. That success has created a viable target. In April 2012, 600,000 Macs were infected with the Flashback Trojan.[ix]

2 Changing Technology Drives Threats Up

Changes to how technology is used are contributing to growth in cybersecurity threats. Cloud computing, mobile devices, Internet-based applications and social networking have become major security concerns. This interconnectivity of devices, systems and users creates virtual highways for threats to spread.

While mobile computing and "bring your own device" (BYOD) have many advantages, the lack of corporate ownership and control adds to the security challenges. Mobile attacks are increasing, and 32% of all mobile threats steal information. A lost or stolen device is a common mobile security incident, and thefts of smartphones in major cities have become a national crime epidemic.[xii]

Cloud computing is convenient, but it presents additional risks. When a company uses a cloud provider, it leaves data protection in the hands of someone else. Even if the cloud provider has platforms that are more secure than the company that uses it, the provider may be a more desirable target of cybercriminals because of the high volume of data the cloud provider manages.[xii]

As business gets more social, security concerns rise. Users may view a social site as a safe place, but spammers and cybercriminals take advantage of that trust to launch attacks. They're finding new ways to introduce malware and viruses through shortened URLs that appear to come from a friend, corrupted applications and malvertising. Some of these bring worms and Trojans onto a system and can create a serious corporate threat.[xiv]

"Despite the risks associated with a lost or stolen smartphone, only 67% of companies require passcodes to unlock mobile devices."

– COMPTIA [xi]

3 Integrated Solutions Manage Threats

Companys can secure the data they protect by employing a wide range of tools. It's important to realize that it takes more than one tool to protect sensitive data.

Together, the right set of tools can help win the war against IT security breaches:

Mobile Device Management (MDM) – Monitoring and managing mobile devices can help protect devices and the data they hold with location tracking, selective wiping and built-in reporting.

Email Security – A well-designed hosted email security service can block unwanted email before it reaches a corporate network. The service should also audit outbound mail to help protect the company's brand and avoid email disruptions.

Patching – Keeping systems up-to-date with current patches is the key to keeping vulnerabilities at bay.

Security Awareness Training – While technology tools can help with IT security, employee education plays a major role as well. Companies should provide education and training while enforcing policies to mitigate human error. Employees are the root cause of many data breaches, with over 78% of IT security practitioners saying negligent or malicious employees or other insiders were responsible for at least one data breach within their companys over a two-year period. [xvi]

Antivirus & Anti-malware – McAfee catalogs more than 100,000 new malware samples every day, which translates to about one new threat every second.[xvii] This only reinforces the need for integrated, real-time protection against zero-day attacks.

One View For All – Developing a unified view of all endpoints, including mobile devices, is key. The easiest and most efficient way to do this is with a single underlying framework.

Add Value With Security Solutions

Security is a critical function for any company. IT departments need to make sure they have a comprehensive security solution. Your company cannot afford to be down for any amount of time, so IT professionals need to choose the right solution to avoid downtime for their company.

> **"It's easier to analyze and respond to security threats when data is integrated within a single platform."**
>
> **– PONEMON INSTITUTE** [xviii]

When seeking an IT security solution, look for one that:

- Integrates with your client management platform and allows you to manage multiple solutions and brands from a single-pane-of-glass.
- Provides double protection from viruses and malware. An on-demand second opinion scanner can detect and remove Trojans and rootkits found deep inside an operating system.
- Not only protects email accounts from spam and viruses, but provides hosted email services for email archiving, e-discovery, recovery and business continuity.
- Provides a comprehensive patch management solution that is easy to implement. It should immediately begin auditing, patching, documenting and billing updates of third-party applications.

Summary

As security threats grow and become more malicious, the risk of security breaches becomes even more serious. Keeping up with the threats and methods of protecting sensitive data places a huge burden on IT departments.

When choosing the right platform, look for a wide range of security solutions, so you can provide your employees with comprehensive, efficient and effective protection and management.

About LabTech Software

LabTech Software is the brainchild of an IT professional who struggled with the usual challenges and inefficiencies of a reactive IT maintenance and support model. LabTech—its flagship solution—was born out of the urgent need to eliminate technician inefficiencies and the desire to provide preventive and proactive service for an company. Developed with cutting-edge, agent technology, LabTech is the only global client management platform created by system administrators for system administrators to automate your IT services and eliminate inefficiencies. For more information, please visit labtechsoftware.com or call 877.522.8323.

LabTech®
4110 George Road, Suite 200 | Tampa, Florida 33634
877.522.8323 | labtechsoftware.com

[i] Egan, Matt, "As Cyber Threats Mount, Business is Booming in the Security World," http://www.foxbusiness.com/technology/2013/03/12/as-cyber-threats-mount-business-is-booming-in-security-world/#ixzz2S3rmt200, Fox Business, March 12, 2013.

[ii] 2012 Cost of Cyber Crime Study: United States, Ponemon Institute, October 2012.

[iii] "10th Annual Information Security Trends," CompTIA, November 2012.

[iv] Watson, Melanie "Fighting Cyber Crime in the US" http://www.einnews.com/pr_news/219826621/fighting-cyber-crime-in-the-us-infographic-released-by-it-governance

[v] Mazzetti, Mark and Sanger, David E., "Security Leader Says U.S. Would Retaliate Against Cyberattacks," New York Times, March 12, 2013. http://www.nytimes.com/2013/03/13/us/intelligence-official-warns-congress-that-cyberattacks-pose-threat-to-us.html

[vi] "Internet Security Threat Report 2013: Volume 18," Symantec Corporation, April 2013.

[vii] Nachreiner, Corey, "TDoS: The Latest Wave of Denial of Service attacks," net-security.org, April 15, 2013, http://www.net-security.org/article.php?id=1828.

[viii] "10th Annual Information Security Trends," CompTIA, November 2012.

[ix] "10th Annual Information Security Trends," CompTIA, November 2012.

[x] "2012 Cost of Cyber Crime Study: United States," Ponemon Institute, October 2012.

[xi] "Internet Security Threat Report 2013:Volume 18," Symantec, April 2013

[xii] Scherer, Michael, "Law Enforcement Sounds Alarm on Cell-Phone-Theft Epidemic," Time, March 25, 2013, http://swampland.time.com/2013/03/25/law-enforcement-sounds-alarm-on-cell-phone-theft-epidemic/

[xiii] Shrum, Sandy and Murray, Paul, "Common Risks of Using Business Apps in the Cloud, United States Computer Emergency Readiness Team," March 7, 2013.

[xiv] "10th Annual Information Security Trends, CompTIA," November 2012.

[xv] "10th Annual Information Security Trends," CompTIA, November 2012.

[xvi] "Infographic, The State of Malware 2013," April 1, 2013. http://www.mcafee.com/us/security-awareness/articles/state-of-malware-2013.aspx

[xvii] "Infographic, The State of Malware 2013," April 1, 2013, http://www.mcafee.com/us/security-awareness/articles/state-of-malware-2013.aspx

[xviii] "Emerging Security Trends and Risks," IBM Institute for Business Value, June 2012.