A TrendLabs Primer

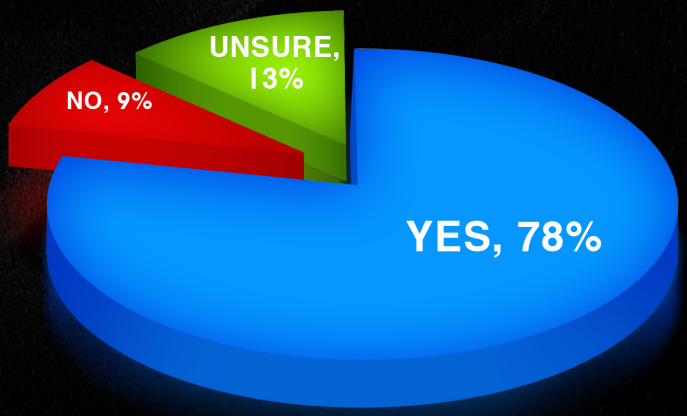
IS YOUR BUSINESS AT RISK OF LOSING DATA?

5 DATA SECURITY RISKS EVERY SMALL BUSINESS SHOULD KNOW ABOUT

Companies, regardless of size, rely on critical business data in order to succeed and flourish. What would happen to their business if they lost sensitive information?

Based on a Trend Micro-sponsored Ponemon Institute study, more than 78% of organizations have suffered from at least one data breach over the past two years.[1] Regardless of who's responsible for the loss of data—negligent employees or other insiders, or those with malicious intent—unless an organization has the necessary knowledge and skills to protect and recover lost data, data breaches will continue to be a problem.

Source: Ponemon Institute, 2012



PERCENTAGE OF ORGANIZATIONS THAT SUFFERED FROM DATA BREACHES

Organizations may face insurmountable financial liabilities if they lose sensitive data. Data breaches can result in direct costs such as reimbursement to customers and data recovery costs. Companies may, for instance, face the inevitable task of recreating lost data from scratch after a breach occurs. Even worse is the damage to one's reputation, especially since most consumers—their customers—said they would entirely stop dealing with an organization in the event of a security breach.[2]

In line with the data threats small and medium-sized businesses (SMBs) face, we've come up with five reasons why an organization may be on the brink of a data breach.

1 http://a248.e.akamai.net/f/248/25855/14d/ig.rsys1.net/responsysimages/trm/_RS_CP_/TrendMicro_rpt_the-human-factor-in-data-protection_analyst-ponemon.pdf

2 http://www.prnewswire.com/news-releases/unisys-security-index-shows-americans-will-take-action-against-organizations-that-compromise-their-personal-data-133063783.html

Data Security Threats Every Small Business Should Know About

REASON

Employee negligence puts an organization at risk.

A company's greatest asset—its employees—can also be its weakest link, especially in an era wherein mobility and accessibility play a huge role in enhancing productivity.

77%
of employees leave their computers unattended.

The top reasons cited for data loss were SMB employees' tendency to open attachments to or click links embedded in spam, to leave their systems unattended, to not frequently change their passwords, and to visit restricted sites. This negligence puts critical business data at risk from data-stealing cybercriminals and malicious insiders.

Especially since 3.5 new threats are created every second,[3] the number of court cases where SMBs have had six-figure amounts stolen by cybercriminals from their bank accounts has risen. Based on estimates, cybercriminals steal as much as US$1 billion a year from SMBs in the United States and Europe alone.[4]

3 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_a-look-back-at-2011_information-is-currency.pdf
4 http://www.scmagazine.com/keep-your-pcs-closed-to-online-criminals/article/214333/

REASON

2 SMBs aren't protected enough.

The majority of SMBs said that, in general, they can't do enough to protect their data using the measures and technologies they currently implement.

65%
of SMBs said that, in general, their organizations' sensitive or confidential business information is not encrypted or safeguarded by DLP technologies.

Most SMBs also doubt their organizations' capability to thwart advanced persistent threats (APTs) or hack attacks,[5] especially since detection or discovery of data breaches among SMBs mostly occurs accidentally.

Companies are no longer just at risk of losing data due to external threats such as hacking and compromises. They are, in fact, in even graver danger due to employee negligence or maliciousness. Even worse, 64% agree that their organizations need to rearchitect their security infrastructure against hackers or malicious insiders attempting to steal data. This effort may require focusing on data-centric security for confidential information, which entails relying on not only traditional outside-in protection but also on protection from the inside-out.[6]

5 http://about-threats.trendmicro.com/RelatedThreats.aspx?language=us&name=Anatomy+of+a+Data+Breach

6 http://www.trendmicro.com/cloud-content/us/pdfs/about/wp_trends-cloud-journey.pdf

REASON

3

Employee mobility may prove disastrous.

Mobile devices enable the workforce to access data from virtually anywhere at any time, allowing greater flexibility and productivity. Freedom, however, may come at a price.

56%
of employees very frequently or frequently stored sensitive data on their laptops, smartphones, tablets, and other mobile devices.

Research shows that 56% of employees very frequently or frequently stored sensitive data on their laptops, smartphones, tablets, and other mobile devices. This means there is more than a 50% chance that confidential information can land in the wrong hands should they lose these devices.

The Bring-Your-Own-Device (BYOD) Era is here to stay. As more and more business data is stored in or accessed by devices that are not fully controlled by IT administrators, the likelihood of data loss incidents caused by improperly secured personal devices will continue to rise.[7]

7 http://it.trendmicro.com/imperia/md/content/uk/12_security_predictions_for_2012.pdf

REASON

4

SMBs fail to routinely back up data.

Less than 50% of SMBs routinely back up data. This, along with risky employee behaviors, the BYOD trend, lack of adequate security protection, and various other threats to data, is putting them at great risk.

62%
of SMBs do not routinely back up data.

Without an automated backup and recovery strategy in place, SMBs have very little ammunition should a disaster strike. In fact, according to another Ponemon Institute study, 62% of SMBs were not confident of avoiding substantial downtime in the event of a serious incident.[8] About a third of U.S. companies also had no backup and disaster recovery strategies in place, citing lack of budget and resources as primary reasons.

8 http://www.eweek.com/c/a/Midmarket/Virtualization-Cloud-Pose-Backup-and-Recovery-Challenge-Survey-304397/

REASON 5

SMBs do not enforce data security policies.

SMBs run the risk of losing data, employee productivity, revenue, and their reputation with the exponentially increasing number of data breaches. While technologies are important in data protection, properly managing the "human factor" will also help prevent your organization from becoming a data breach victim.

SMBs should ensure data protection policies are put in place, communicated to employees, insiders and customers, and strictly implemented. In fact, 80% of organizations, regardless of size, believe managing and monitoring end-user privileges and entitlements is the most important security measure against data breaches.

Data Protection and Security Measures	Percentage
Manage and monitor end-user privileges and entitlements	80%
Conduct criminal background checks before granting privileged access	57%
Ensure security governance practices are consistently applied	52%
Attract and retain high-quality IT security personnel	48%
Train employees about IT security policies and procedures	47%

Source: Ponemon Institute, 2012

TOP 5 DATA PROTECTION AND SECURITY MEASURES TO ADDRESS HUMAN FACTOR RISKS IN DATA PROTECTION

Knowing "who, what, when, and how" data is accessed is key. SMBs would hugely benefit from creating policies for the use of social media and personal email, as most attacks begin with the simple act of falling for a social engineering lure.

WHAT YOU CAN DO TO HELP YOUR COMPANY AGAINST DATA BREACHES

To help protect your company's assets and data from breaches, follow these tips and best practices:

- **Close your organization's doors to malware.**[9] Installing and using effective anti-malware solutions in systems and devices that contain or have access to sensitive information is important. Just as you would never leave your house's doors open at night or when you're not at home, your company's doors should never be left unguarded against people with malicious intent as well.

- **Stress how important protecting data is.** Inform your employees and other insiders about your company's security policies. Stress the personal and business consequences of not protecting their mobile devices, systems, storage devices, and the confidential data these contain from loss or theft.

- **Don't let social networking endanger your network.** Teach your employees how dangerous oversharing in social networking sites can be. Even if you cannot stop them from sharing information in social media, you can opt to limit the amount of time they spend on these sites while at work to lessen the chances of your company's security perimeter from being breached.

- **Think of passwords as keys.** The stronger the passwords to accounts are, the harder they are to crack. Keep in mind that without the right keys in hand, malicious insiders and outsiders alike will have a much harder time getting to your company's crown jewels.

- **Patch holes in your organization's walls.** Identify which information is critical, who could and should be able to access it, then investigate the best ways to protect it with the aid of a trusted IT advisor. Like holes or cracks in walls, areas where your company data is most vulnerable can cause your security perimeter to crumble.

- **Knowing is half the battle.** Tell your employees that although losing unencrypted and improperly protected data stored in mobile devices may get them into trouble, failing to report such incidents is worse. This does not only put them but also their colleagues, customers, and the entire organization at great risk.

9 http://www.techdata.com/(S(kdgthp454u1wuzuwdmyrbf45))/techsolutions/softwareconnections/files/sep10/TREND%20MICRO_top_10_tips_to_keep_your_small_business_safe.pdf

TREND MICRO™

Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years' experience, we deliver top-ranked client, server and cloud-based security that fits our customers' and partners' needs, stops new threats faster, and protects data in physical, virtualized and cloud environments. Powered by the industry-leading Trend Micro™ Smart Protection Network™ cloud computing security infrastructure, our products and services stop threats where they emerge—from the Internet. They are supported by 1,000+ threat intelligence experts around the globe.

TRENDLABS℠

TrendLabs is a multinational research, development, and support center with an extensive regional presence committed to 24 x 7 threat surveillance, attack prevention, and timely and seamless solutions delivery. With more than 1,000 threat experts and support engineers deployed round-the-clock in labs located around the globe, TrendLabs enables Trend Micro to continuously monitor the threat landscape across the globe; deliver real-time data to detect, to preempt, and to eliminate threats; research on and analyze technologies to combat new threats; respond in real time to targeted threats; and help customers worldwide minimize damage, reduce costs, and ensure business continuity.

TREND MICRO™

Securing Your Journey to the Cloud

TrendLabs
Global Technical Support & R&D Center of TREND MICRO