TREND MICRO

Data: Here Today, Gone Tomorrow

A TrendLabs Primer

TrendLabs

Global Technical Support & R&D Center of TREND MICRO

Things Every Small Business Should Know About Data Storage

Data is the lifeblood of any business, and small businesses are certainly no exception. Critical data such as email messages, financial documents, as well as project and personnel files all make up vital company information that most businesses cannot function without.

Data loss has been plaguing enterprises and small businesses alike for a long time now, often representing a point of liability for many. This emphasizes the importance of having a location fail-safe method for storing, protecting, and recovering critical company data.

What would happen, however, if a small business discovered that its critical data has been compromised? Small businesses may back up their files with a security solution in place but protection measures can still be affected by a single small oversight. Just like everything else, digital data can easily get lost and destroyed unless a company has the necessary knowledge and skills to protect and recover it.

FACT 1

Human error is the leading cause of data loss.

A 2010 Kroll Ontrack study on the leading causes of data loss revealed that 40 percent of home, business, government, and channel users of IT believe that human error is the leading cause of data loss.[1] This indicates that even though users' technological knowledge has indeed improved over the years, human error continues to be the key contributor to data loss. Common instances of human error include deleting files by accident and forgetting to back up data. Other cases include accidentally formatting a system's hard drive and unknowingly deleting important but unrecoverable system files or folders.

AMI Research reported that more than 21 million of over 68.5 million small businesses worldwide have multiple PCs but do not have servers on which they can securely store data.[2] This means they do not enjoy the benefits of having a centralized system that makes data available to their employees, partners, and/or customers. All kinds of information stored in PCs are prone to accidental deletion due to human error.

[1] http://www.krollontrack.com/company/news-releases/?getpressrelease=61462

[2] http://www.zdnet.com.au/10-tips-for-designing-a-small-business-network-339271594.htm

FACT 2

Backing up critical data is a necessity, not a luxury.

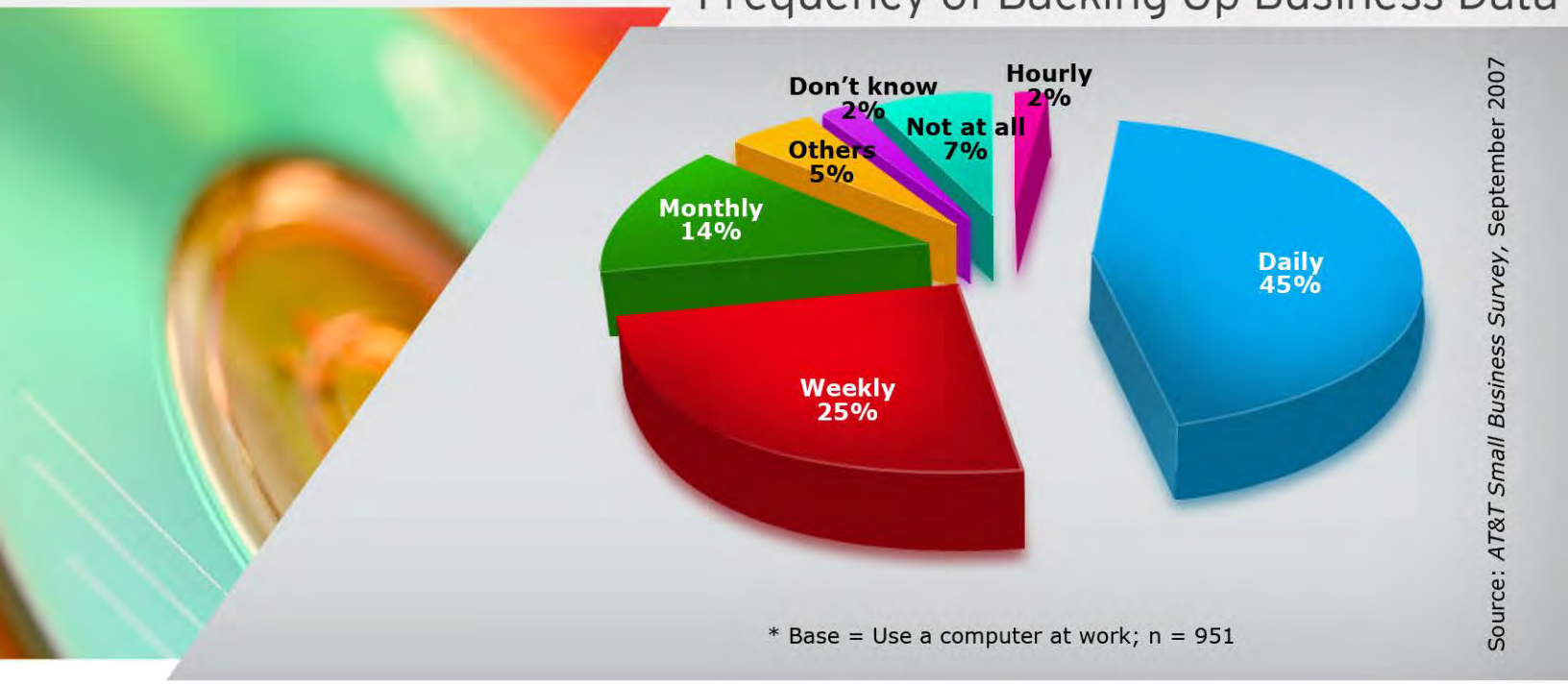
Using a data backup solution is important to businesses that want to protect core documents. Database and accounting files can get lost from a hard disk crash or from other kinds of system failure. Unfortunately, most businesses realize this too late.

According to an AT&T study, almost half of the total number of small businesses (47 percent) back up data at least once a day while almost three-fourths do so weekly.[3] However, 7 percent do not back up data at all. Among them, 62 percent do not back up data because they do not believe it is necessary. Contrary to this belief, however, public and private sector organizations alike have compelling reasons to protect sensitive data.

Many small businesses may face insurmountable financial liabilities if they lose sensitive data. They may, for instance, face the inevitable task of recreating lost data from scratch after a loss occurs. Losing sensitive customer data can expose them to legal, apart from financial liabilities, as well. The cost of notifying customers, partners, and/or stakeholders should a widespread hardware failure occur is also worth considering. Companies that are subject to regulations imposed by the government may also suffer from financial and/or legal sanctions if they do not adopt required data protection measures.

Even though 75 percent of the total number of small businesses use on-site data backup resources such as tape or external hard drives or CDs, their data is not completely safe from the risks natural disasters or break-ins pose. They should store backup file copies off-site or in the cloud.

Frequency of Backing Up Business Data



[3] http://www.att.com/Common/merger/files/pdf/smallbiz/SMBSurvey-Security-Presentation.pdf

FACT 3

Data leaks can occur within a small business.

A Trend Micro global survey revealed that small businesses are becoming more worried about losing important data through leaks.[4] A data leak refers to the intentional or unintentional release of sensitive information outside a corporate network. The occurrence of data leaks is a scary proposition among enterprises; this is true for small businesses as well.

Data lost due to leakage may be financial (e.g., net income) or personal (e.g., employees' names) in nature. The majority of data leak incidents, whether accidental of deliberate, begin with users who have access to information stored in a corporate network.[5] Employees can, for instance, compromise the security of company data by transferring files onto a USB drive then taking this out of the office. As such, a company's greatest asset—its employees—can also be its greatest security liability.

[4] http://trendmicro.mediaroom.com/index.php?s=43&news_item=842&type=current&year=0

[5] http://trendmicro.mediaroom.com/index.php?s=43&news_item=595&type=archived&year=2007

FACT 4

Information-stealing malware persist as online threats.

Just like enterprises, small businesses are also prime cybercriminal targets since they hold valuable employee and customer information. Cybercriminals can steal several kinds of confidential corporate information ranging from employees' social security numbers to their personal information and to the company's online banking credentials. If these fall into the wrong hands, anyone within the company or the organization itself can succumb to information theft or, worse, identity fraud.

Malware such as ZeuS Trojans are primarily designed to steal confidential information from various online banking, social networking, and e-commerce sites.[6] ZeuS Trojans may arrive via spammed messages or may be unknowingly downloaded from compromised sites. The recent attack on sites under the *.KR* domain, however, showed that other malware, apart from ZeuS Trojans, can also steal data from their chosen targets.[7] Even though the attack was easily thwarted, leaving minimal damage, an increasing number of institutions are likely to suffer from a similar fate in the future.

[6] http://about-threats.trendmicro.com/RelatedThreats.aspx?language=us&name=ZeuS+and+Its+Continuing+Drive+Towards+Stealing+Online+Data

[7] http://blog.trendmicro.com/zombie-cleanup-becomes-crucial-in-recent-kr-cyber-attack/

FACT 5

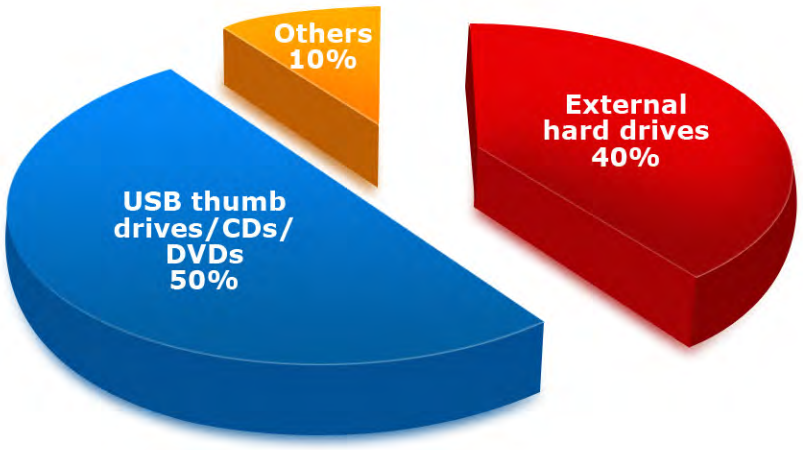
Opting for in-the-cloud storage can go a long way.

Companies that create and maintain customer databases to run their business can lose potential revenue and may be exposed to significant legal and/or financial liabilities if they fail to recover lost or stolen data. The only surefire way to recover lost data is to restore it from a reliable backup storage device. However, the normal small business practice involves saving company data on USB thumb, external hard, or tape backup drives. In fact, 40 percent of small businesses back up files to external hard drives while 50 percent use thumb drives to store important information. Only 13 percent use an online storage service.[8]

Whether users opt for an online computer backup program or for an external data backup tool, preventing nonrecoverable data loss is crucial to a business's ongoing success. It is all about saving one's business and about avoiding financial loss, especially for companies that do not have an effective data recovery plan in place. Data loss can not only result in the loss of critical business information but also of resources. Data backup, or the lack thereof, can make or break a business. Provisioning for data loss can, however, greatly reduce risks.

As small businesses increasingly transition to cloud computing, online services will save companies the trouble and expense of setting up and of managing their own backup and archival storage systems.[9] Small businesses do not require a lot of storage, which makes using a local physical backup solution feasible. However, these backup solutions are still prone to complete hardware failure or can be destroyed by a catastrophic force of nature. To withstand such occurrences, a secure online backup solution is a better option.

Means for Backing Up Critical Business Data



Source: Lenovo

[8] http://news.lenovo.com/article_display.cfm?article_id=1393

[9] http://www.crn.com/news/cloud/226700149/smb-cloud-spending-to-approach-100-billion-by-2014.htm;jsessionid=bVZxeUAaShMvIanKZYne6Q**.ecappj01?itc=refresh

What Trend Micro Can Do to Protect You

Every company is prone to losing data, especially with the ongoing threats and risks businesses face. This is why Trend Micro continues to strive to protect its customers from every possible threat with the aid of the Trend Micro™ Smart Protection Network™.

- *Trend Micro™ SafeSync™ for Business* stores irreplaceable and critical documents in a single safe location administered by Trend Micro. It takes care of a business's file management needs by replacing traditional backup and file server solutions as well as VPN or similar remote access solutions. Small businesses can securely manage, access, and share files with employees and external partners. As such, *Trend Micro SafeSync* acts as a great insurance plan for all of a company's important electronic data. Simple to set up and easy to use, it silently works in the background, automatically backing files up for quick restoration in the event of a disaster, of an accident, or of loss.
- *Trend Micro™ Worry-Free™ Business Security 7—Advanced* protects *Windows*-based systems, Macs, as well as file and mail servers from malware, threats, and dangerous websites. This latest edition keeps business information private by locking down USB drives and other storage devices as well as by preventing data loss through email. It also blocks spam both before it reaches and while on *Microsoft Exchange* servers.
- *Trend Micro™ Worry-Business™ Security Services* is a cloud-based security solution that provides protection for business data anytime and anywhere. It secures PCs, laptops, servers, and other *Windows*-based devices such as point-of-sale (POS) machines and media tablets.

In addition to providing industry-leading security solutions, we also provide information on the latest threats and threat trends to let users know what they can do to stay protected in today's digital world. For more information on the threats featured in this primer, please refer to our materials in the following portals:

- *Threat Encyclopedia:* Our malware, spam, malicious URL, and Web attack entries like "ZeuS and Its Continuing Drive Toward Stealing Online Data" provide more information on the vectors cybercriminals use to infect users' systems and corporate networks.
- *TrendLabs Malware Blog:* Our blog entries like "Zombie Cleanup Becomes Crucial in Recent KR Cyber Attack" provide threat news and information direct from the experts.

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

ABOUT 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 and analyze technologies to combat new threats
- Respond in real time to targeted threats
- Help customers worldwide minimize damage, reduce costs, and ensure business continuity

TREND MICRO™ Securing Your Journey to the Cloud

ABOUT TREND MICRO™

Trend Micro, Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our website at www.trendmicro.com.

TREND MICRO

10101 N. De Anza Blvd.
Cupertino, CA 95014

US toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003
www.trendmicro.com