AVG Internet Security

Business Continuity in the Internet Era

A Security Briefing for Small and Mid-sized Business Owners and Managers

Introduction

Business Continuity is no longer simply about the major natural or manmade disasters like hurricanes, floods, fires, or power blackouts.   It is now also about the threats originating from the Internet that can adversely slow or even shut down your company's computer systems and networks.

In this Business Brief, you will learn why you as a business owner or manager need to put the same priority on protecting your business against Internet threats (and managing those costs), as you now do with all the other "classic" threats that can interrupt your business operations. Business owners and managers may mistakenly believe that their company is too small to be a target for these Internet-based threats, but it is important to realize that the new threats negatively affect all companies equally, regardless of size.

You will learn how these new threats can affect the profitability and sometimes even the survival of your business, how these threats work, and how you can protect your business against these threats. Finally, this Business Brief will introduce you to Grisoft and its Internet security products that protect computer systems and networks against these Internet-based threats. Grisoft products are effective, simple to use and very economical compared to other vendors' offerings.

Table of Contents

This Business Brief is for informational purposes only. Grisoft, Inc. makes no warranties, express or implied, in this document.

1. “Classic” Business Continuity Risks and Plans

1.1. Definition

A business continuity plan identifies the threats that can affect the continued operation of that business and describes the actions that will restore the business to normal activity levels in response to these threats. This is important for businesses of all sizes today and there are even web sites that specialize in this area.

This description from a federal government planning guide for large financial institutions[1] could apply to almost every business with just minor changes in wording:

> “Business continuity planning is the process whereby financial institutions ensure the maintenance or recovery of operations, including services to customers, when confronted with adverse events such as natural disasters, technological failures, human error, or terrorism. The objectives of a business continuity plan (BCP) are to minimize financial loss to the institution; continue to serve customers and financial market participants; and mitigate the negative effects disruptions can have on an institution's strategic plans, reputation, operations, liquidity, credit quality, market position.”

Business continuity is not about ON-OFF-ON again situations without shades of grey. The description above includes the “maintenance or recovery of operations.” In other words, a threat doesn’t have to cause a complete shutdown of the business to have a bad impact on “financial loss.” The impact of a threat could include a significant slowdown in operations, or the ongoing extra expense needed to maintain normal operations.

1.2. Threats to Business Continuity

People often associate business interruptions with headline-making natural disasters like *Hurricane Katrina* or the 9/11 terrorist attacks. In reality there are other, more mundane causes for an interruption or just a slowdown in normal business activities, such as fire, power outage, or vandalism and theft. All these are the *classic* threats to a business.

Because these threats are very real, yet hard to predict, there are a lot of business articles devoted to advising business on how to deal with these threats. A search of the websites[2] of *Business Week*, *Fortune*, *Forbes*, and *Wall Street Journal* in March, 2007 for “business continuity” found the following:

Total articles mentioning Business Continuity:	77
Articles focused on *IT Risk*	only 5
Articles focused on *security risks* to IT	only 1

Looking at the articles, it is clear that most are focused with the headline-making disasters. In addition, many of the articles were actually about companies or industry sectors that provide products and services to companies in support of their business continuity plans, rather than guidance for companies needing to improve their business continuity plans. Business continuity itself is a big business these days.

The five articles that actually provided advice to readers recommended solutions such as an alternate emergency location for call center employees. Only one of the IT focused articles even mentioned security as a major threat source. Instead they mentioned solutions such as backing up computer data offsite, or having an emergency generator.

Neither of these are realistic solutions for small and mid-sized organizations. As an anecdotal example consider the case of an architectural firm from the Boston, MA area. Several times each week the firm world back up their critical data to tape and send it on a round trip via Federal Express arriving several days back at their office. Their reasoning is that Federal Express' insured carrier service provided more security for their data than leaving it in the office. This may have protected the data from fire or theft in the short term but still left it exposed to general data security issues during the course of normal business. And this approach *guarantees, at worst,* several days of complete downtime in case of a successful data attack on their data or, at best, a slow down of business in the case of a successful viral attack.

> It's hard to imagine, but many companies don't even know they've had a security breach until long after they've been attacked. …
>
> Go the extra mile and build in hardened layers of security at every connection edge of the IT network, especially if you are a small business that someday hopes to work with larger, publicly traded corporations.
>
> – "Is My Small Business Required To Comply With Regulations That Big Businesses Are Subject To?"
> http://www.allbusiness.com/legal/laws-government-regulations-business/11330-1.html

These steps address the issue of an IT facility affected by one of the "classic" threats. However, they appear to ignore the issue of security threats. In some ways, this lack of understanding is not surprising. Security threats have become a "corporate issue" only in the last few years, probably because the significant business continuity threats themselves are relatively new. Although there were security issues caused by thrill-seeking hackers five years ago, there was no real lasting impact on business operations. The "Melissa" virus outbreak in 1999 is a very good example of a thrill-seeking virus.[3]

However, in recent years computer security threats have become a very serious issue for business continuity, but the business press, hasn't "caught up" yet, as shown by the numbers cited above. Thus, the business press *has yet to understand the seriousness of this issue and properly educate its readership.*

However, you can't afford to be uninformed, not with your responsibility for the continued profitability and survival of your company.

This Business Brief will educate you, and suggest solutions to address the issue.

1.3. Importance of the Internet to Business Today

In recent years, the Internet has emerged as a major technology for improving business productivity. Using email and Web sites, businesses have been able to grow revenues and decrease costs in ways that would not be possible in any other way. It is hard to imagine a business of any size that can compete successfully today without leveraging these benefits.

- Break down geographical boundaries, to reach customers and suppliers on a regional, national and even international level.
- Extend business hours for sales and customer information to 7x24x365.
- Communicate with customers one-on-one through email and instant messaging.
- Use web sites to advertise a company and its products.
- Use national auction sites such as *eBay* as a cost-effective way to reach consumers and other businesses.
- Create a whole new sales channel using the Web, in addition to, or sometimes instead of retail stores.
- Improve employee productivity through tele-commuting, “day extension” (working at home) and keeping in contact with the office while traveling.
- Improve employee efficiency through better internal communications with email.
- Driving down the cost for sales by using online stores on web sites.
- Reducing costs for supplies and services, through increased efficiency and accuracy and wider range of choices via the Web.
- Eliminating the expense of express services and postal services by using free and instantaneous email, and instant messaging.

A key aspect of these benefits is the always on, 7x24x365 nature of IT systems. Even when the office is closed, employees can still exchange email with each other and with customers and suppliers. The web site can accept orders at any time of day or night.

From a revenue point of view, it doesn’t matter what caused the business continuity interruption. In many ways, an interruption caused by a classic threat has less of an impact on your business than a security attack that shuts down your IT systems. If your factory or store is open normal business hours, then you still have the late evenings and nights, and possibly even the weekends or holidays to restore normal operations. However, your website and email systems are supposed to function every minute of every day of every month. Thus, any interruption, at any time of day or not, will start to have immediate impact on productivity and revenues.

1.4. Why a Business Continuity Plan is Important for the Survival of a Business

A recent study[4] by AT&T and the International Association of Emergency Managers surveyed 1,200 businesses from January to August 2005 and found that, “Nearly one-third of U.S. businesses do not have emergency continuity plans in place – up from 25 percent one year ago. (The survey did not break down the data by company size; some experts said that larger and/or publicly traded companies are far more likely to have plans in place than smaller companies.)”

The survey also found that two thirds of companies that suffered through a disaster lost business, with "16 percent losing between $100,000 and $500,000 per day and 26 percent saying they *did not know how much it cost* their company per day." [Italics added for emphasis.]

Former New York City Mayor *Rudy Giuliani* on security

Q: What are some areas of security that companies ignore?

A: *There's an attitude of either not wanting to face the realities or not wanting to spend money on facing the realities. …*

There are companies that have the foresight to do it, and there are companies that still worry about the bottom line. They keep betting that it's not going to happen.

– "Giuliani: Ignorance of Terror Isn't Bliss," *Business Week,* August 5, 2004, http://www.businessweek.com/bwdaily/dnflash/aug2004/nf2004085_8377_db008.htm?chan=search

An unplanned IT shutdown can actually force your company out of business. Another study[5] reported that forty-seven percent of the risk managers surveyed said that, "Unplanned downtime of information technology systems lasting 24 hours or more could *jeopardize the survival of their entire business*." [Italics added for emphasis.]

2. Internet-Based Threats: Why Small Businesses Are Now Being Targeted

2.1. Evolution of Internet Threats: From Maladjusted Thrill-Seekers to Organized Crime and Cyber Criminals

As everyone now recognizes, the Internet is not a risk free tool. Most computer users today are aware of viruses and related threats that can affect their systems at home.

However many people are not aware that computer hacking is now a large lucrative, and growing area of activity for organized crime worldwide targeting businesses. Compared to drugs or other forms of "physical" crime, cyber crime is a lot safer and practically risk free.

"Globally, cyber crime is now a bigger problem than drug trafficking. "Last year (2005) was the first that proceeds from cybercrime were greater than proceeds from the sale of illegal drugs, and that was, I believe, over $105 billion."

– Valerie McNiven, advisor to the US Government.

The cyber criminal can be located halfway around the world from his targets. Equally, the cyber crime servers will usually be located in a country with non-existent or lax law enforcement against cyber crime. There is even some anecdotal evidence from the US Government that government officials in Nigeria are complicit in the numerous "Nigerian Letter" email scams[6]. A "Nigerian Letter" is a "confidence scheme. It claims to come from a family member or friend of the (deposed) dictator of a third-world country. The author of the letter claims to have a fortune of many million dollars, and seeks the email recipient's help in transferring the money outside of the country. The recipient will be well-compensated of course. To get this process started, the recipient must email back details of his or her bank account. The cyber thieves then promptly empty out this account. Hokey as this all sounds, cyber thieves continue to send Nigerian Letters because there are always new victims.

2.2. Why Popular Software Make Your Business Vulnerable

A few key software programs are used by almost all businesses, large and small, worldwide. A cyber criminal can attack millions of business with a successful attack directed against just one of these applications. This list isn't meant to single out Microsoft. Quite the contrary. It reflects the success and popularity of these products.

- Microsoft *Windows* operating system.
- Microsoft *Internet Explorer* browser.
- Mozilla *FireFox* browser.
- Microsoft *Office* for word processing, spreadsheets, presentations, email, task lists, and calendaring.
- Microsoft *MDAC* as the database "building block" for other applications.
- Adobe *Acrobat* PDF reader.

Most businesses will use the following server applications, even on a "hosted" server:

- Microsoft *Exchange* email server.
- Microsoft *Internet Information Server* for web sites.
- *Apache* web server.
- Microsoft *SQL Server* for applications and web sites that use an internal database.
- *MySQL* server for web site databases.

These attacks target either a "bug," a programming error, or a weakness in the design of the software. In either case, the result is an opening for a successful attack.

Because these applications are in such widespread use in both large and small businesses, a successful attack against of these applications can be hurt companies of all sizes. *The key takeaway is that small businesses are now just as vulnerable to hacker attacks as the large multi-national enterprises.*

Many businesses also use very specialized vertical line-of-business applications such as *Mitchell OnDemand*[7] for auto body repair shops, or *AbacusLaw*[8] for legal time and billing and case management. Intuit *Quickbooks*[9] is very popular with smaller businesses. Such specialized applications are generally not as "interesting" to cyber criminals because they are not as popular as the horizontal applications listed above. *Yet such vertical market applications can be just as vulnerable to attacks by cyber criminals* because they need a built-in database to keep track of customers or transactions or product items, or they contain a built-in browser.

Rather than write all this software themselves, the vendors of these specialized applications use Microsoft software developed for just that purpose. Examples include database tools *(MDAC* “building blocks” or SQL Server*)* and special “hooks” built into *Internet Explorer.* Thus, even when you don’t think you’re using an application that is highly vulnerable to cyber criminal attacks, you might actually using one of them anyway

2.3. How Businesses Get Infected by Internet Threats

No employee deliberately sets out to have their computer infected with a virus or other malware. But no “intent” is necessary. Carelessness, combined with insufficient protection against these threats, is quite sufficient.

Some Definitions Of The Various Ways That Cyber Criminals Can Attack Your Systems and Networks.

As computer security becomes important for the business community, some esoteric terminology has entered common usage.

Malware - The generic term for software that is designed to do harm - a contraction of 'malicious software' including viruses, Trojan Horses, worms, and others.

Virus - A virus is a 'infects' other programs and has the ability to copy itself to other computers or disks, without being asked to do so by the computer user.

Macro Virus - A virus hidden in an MS *Office* document.

Worm - Worms are similar to viruses, but they do not infect other applications. A virus can delete files, alter content, reconfigure the system, display a graphic or graphics, or install other software such as spyware, backdoor, or a zombie.

Trojan Horse or **Trojan** -Trojan horses may appear to be useful or interesting programs (or at the very least harmless) to an unsuspecting user, but are actually harmful when executed. Examples include online music and video players.

Spam - Spam refers to unsolicited e-mail, mostly advertising a product or service that is mass mailed to huge number of e-mail addresses at a time, filling recipients’ mail boxes. Spam is not only annoying, but also can often be a source of scams, viruses or offensive content.

Spyware - Software that gathers information from a user's computer without the user's knowledge or consent. Spyware can infect a computer from a website with potentially dangerous content, e-mail, worms and viruses. Spyware often contains advertisements, or window pop-ups for pornographic web sites, or installs a new home page in the user’s browser.

Phishing - A criminal activity using social engineering techniques. Phishers attempt to fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading in email as eBay, PayPal or a bank.

Backdoor - A backdoor is a hidden entry for remote hackers. Once installed, the hacker can come and go at will. Backdoors are often used to hiding the true location of the spammer.

Keystroke logger - Also known as “keylogger.” A program or in some cases a hardware device that captures every key stroke on the computer. When used by a cyber criminal, it steals passwords and confidential information.

Drive-by download - A program that is automatically installed in a computer by merely visiting a Web site, without having to explicitly click on a link on the page. Drive-by downloads are deployed by exploiting flaws in the browser and operating system code. Internet Explorer and Windows are the primary targets.

Sources: Grisoft, http://www.itsecurity.com/dictionary/, http://www.techweb.com/encyclopedia/

Email is an extremely effective method to distribute all forms of malware. An employee clicking on an attachment from an unknown or spoofed sender can introduce malware into the system. Likewise, an employee clicking on an electronic “greeting card” or opening up a picture (*jpg* file) of a supposedly nude tennis star, could actually infecting his system with a Trojan.

Web sites are the other major source of infection. Cyber criminals will often introduce "exploit code" for a "drive by download" from a legitimate site. But "social networking sites" like *MySpace* or video download sites like *YouTube* allow users to upload movies or pictures. These files can certainly include malware, and thus make it almost too easy for hackers to introduce viruses or Trojan Horses into a business. All these risks are magnified when employees use company email to pass around their latest downloads.

Hackers attack computers every 39 seconds, according to new research.

Unlike the sophisticated hackers portrayed on TV and in films, these hackers weren't targeting specific computers.

"Most of these attacks employ automated scripts that indiscriminately seek out thousands of computers at a time, looking for vulnerabilities."

– "Hackers Attack Every 39 Seconds,"
http://www.livescience.com/technology/070207_hacker_attack.html

Of course, your employees aren't *supposed* to be using company computers for online shopping, checking their stocks or downloading music and videos, or worse, downloading pornography. But if you have teenagers at home then you already know how hard it is to totally stop such activities. Is it that different in your office?

And even if your employees aren't being careless or engaging in risky behavior, your network is still at risk due to the constant bombardment of threats from the Internet.

Cyber criminals are spreading *LdPinch.ZO*, a *trojan* that specifically targets corporate data. The malware reaches networks via email attachment or concealed internet download. Once activated, the *trojan* installs malicious code designed to steal passwords, login details and other private data.

–
"http://www.first.org/newsroom/globalsecurity/92312.html

3. Consequences of a Successful Cyber Criminal Attack

A recent report from Forrester Research of Cambridge [Mass] estimated breaches have cost companies between $90 and $305 per lost record, including notifying customers, hiring contractors to fix computer systems, fines, and lost business.

–[1] Kerber, Ross, Analysts: TJX case may cost over $1b," Boston Globe, April 12, 2007, "http://www.boston.com/business/personalfinance/articles/2007/04/12/analysts_tjx_case_may_cost_over_1b?mode=PF

3.1. What If The Computers In Your Office Gets Infected?

Plenty can go wrong for your business, it seems.

- Loss of revenue, capital expenditure, or personal liability resolution.
- Additional operations expenses incurred due to the disruptive event.
- Financial loss from resolution of violation of contract agreements.
- Financial loss from resolution of violation of regulatory or compliance requirements

And if all this isn't enough there is also:

- Loss of competitive advantage or market share.
- Loss of public confidence or credibility, or incurring public embarrassment.[10]
- Above all, the loss of reputation, which is further discussed below.

State disclosure laws on the books in California and over 35 other states now mandate notification if any consumer personal information has been disclosed by accident or by cyber criminal theft. The California law affects any company doing business with California customers, regardless of the location of the company, in effect forcing notification of customers globally.

These consequences are non-trivial and can affect the well-being or even the very survival or a business in the same way as that headline-grabbing natural disaster. The business needs to devote resources to monitor spam, etc. These resources are diverted from projects such as making the external web site easier to navigate, leading to increased revenues, or developing an internal web site to improve employee productivity and supply chain efficiency. As a business owner or manager, you have always had to protect your company against a variety of threats. Now you must take the necessary steps to ensure business continuity in the face of these new threats.

> *Suddenly, with almost a universal flash of clarity, technophobic boards of directors the world over realized that crashed servers meant crashed sales. And they began to hustle.*
>
> – When Disaster Strikes, Kevin Ferguson, *Forbes*, Feb. 22, 1999, http://www.forbes.com//1999/02/22/feat.html

3.2. TJX: A Sad Case Study That is Still Unfolding

Sometime in 2005, a hacker managed to infect computers at the TJX corporate headquarters with a Trojan[11] designed to steal account information and passwords. TJX is a retailer based in Framingham, MA, with 2,500 stores in the US, Britain, and Ireland. Its major brands include T.J. Maxx, Marshalls, and HomeGoods.

The outcome has been a major disaster for TJX in multiple dimensions and the story is still unfolding as of April, 2007. There are news stories appearing almost weekly in major newspapers, trade journals, and electronic media. Each new revelation makes the situation worse and worse for TJX.

The public first learned on January 18, 2007 that TJX computers were hacked and customer credit and debit card information was compromised. At the time, the company would only say that, "It does not yet know how much data was taken … .[12]

In late January, the company announced that it was recording a quarter cent charge per share against earnings, $4.5 M, "Including the costs to investigate and contain the intrusion, enhance computer security, and communicate with customers[13]."

> The lawsuits are starting to fly, alleging that TJX and one of its credit card partners, Fifth Third Bank, failed to secure the personal data of millions of customers. A class-action lawsuit was filed last week in U.S. District Court for the District of Massachusetts on behalf of several banks affected by the breach, including AmeriFirst Bank of Union Springs, Ala. A consumer-based class-action suit was filed Jan. 19 in U.S. District Court for the Northern District of Alabama.
>
> – Greenemeier, Larry, "Hack Attack Means Headaches For TJ Maxx," *Information Week*, Feb. 3, 2007, http://www.informationweek.com/news/showArticle.jhtml?articleID=197003041

By January 31, 2007, lawsuits were already being filed and a powerful congressman called for a Federal Trade Commission investigation[14].

On March 23, 2007, news reports announced the arrest of six people in Miami, FL, on charges of stealing credit card data. By then, banks had already replaced the credit cards of hundreds of thousands of their customers. There were numerous reports of card fraud as far away as Sweden and Thailand, according to a story in the *Wall Street Journal*[15].

> Paul Stephens, policy analyst at the Privacy Rights Clearinghouse, told SCMagazine.com today that ..."It appears that the suspects had purchased this information from the hackers, so it's clear that there is a black market for this type of information. This may just be [the beginning], because there are probably many other individuals throughout the country who have purchased this information," he said. "Hackers do not do all of this work to only sell the information to one small group of people."
>
> Vijay Bisani, eIQnetworks CEO, told SCMagazeine.com, … "We all know that the bad guys don't just go and do everything at once. They do it over time, and they do it in multiple locations, and see what systems are vulnerable to them and how they can get the sensitive data."
>
> – Washkuch, Frank, Jr., "Stolen TJX data used in Florida credit card fraud ring; Arkansas organization sues to see firm's data protection," *SC Magazine*, March 21, 2007, http://scmagazine.com/us/news/article/645273/stolen-tjx-data-used-florida-credit-card-fraud-ring-arkansas-organization-sues-firms-data-protection

And by March 29, 2007, TJX disclosed in a regulatory filing that at least 45.7 million credit card holders were affected by the data thefts, and there were calls for Congress to pass a new federal breach notification and data security standards law[16]. A few weeks later, on April 12, independent analysts estimated the total cost to TJX at over ***1 billion***

dollars[17]. Finally, on April 25, 2007, three New England state bank associations and some individual banks filed suit against TJX, claiming that the banks have suffered large financial losses because they had to replace customers' credit cards and absorb large losses due to fraudulent usage. Further the head of the Massachusetts bank association is inviting other state bank associations to join the lawsuit and will also seek class-action status[18].

"If we are successful against TJX, the nation's major retailers will finally wake up to the fact that *not protecting consumer data is an unfair trade practice* and that investment in data management systems to protect consumers and shield consumers against fraud and identity theft is required," Daniel Forte, president and CEO of the Massachusetts Bankers Association, said in a statement.
--Lemos, Robert, "New England bankers sue TJX for breach," April 6, 2007, http://www.securityfocus.com/brief/490

As of this writing (April, 2007), the TJX case continues to unfold. No doubt it will take years and many millions of dollars for TJX to put this situation behind them.

3.3. The Number One Concern: Loss of Reputation

As a business owner or manager, you have worked hard to build up your business and maintain your position in the global marketplace. Your reputation is why customers are loyal to you and why you get new customers. Lose that good reputation, and you might very well have to close your business.

Reputation is the biggest concern
But among respondents questioned for this survey, damage to reputation is seen as the biggest threat, with 43 percent of respondents saying that this is their main concern.

– "Economist Intelligence Unit survey highlights the extreme criticality of IT systems," March 2, 2007, http://www.continuitycentral.com/news03100.htm

Recent experience with natural disasters and the 9/11 attacks showed that customers can be very understanding and flexible about some business continuity interruptions, because they understand that the interruption was external and that the same sort of interruption might happen to them. Not so for business continuity interruptions caused by computer security issues, because the real cause was *internal –failure to protect against the threats*.

Larry Ponemon, founder and chairman of the Ponemon Institute, which conducted a study last year on the cost of a data breach to an organization.[said] "… we believe the true cost of a data breach will result in the loss of customer trust and goodwill. This is going to stick in the memory of the public for a long time."

– Kaplan, Dan, "45.7 million-victim TJX Companies breach could lead to federal notification law," *SC Magazine,* March 29, 2007, http://scmagazine.com/us/news/article/647277/457-million-victim-tjx-companies-breach-lead-federal-notification-law/

Both the TJX story and market surveys and studies demonstrate this stark fact: *The most significant loss to a business because of an interruption caused by an Internet threat is the loss of reputation.*

In a *Wall Street Journal* story on January 25, 2007, a TJX spokesperson is quoted as saying, “We’re not commenting on what others are saying about this situation.”[19] That defensive response certainly didn’t win the company any friends. The spokesperson was responding to a statement issued by the Massachusetts Bankers Association.

And when a major business leader criticizes you in public and a congressman uses your company as the justification for a new law regulating business, you have indeed suffered a huge, if unquantifiable, loss in reputation.

> "As a CEO running a company of your size in 2007, it is beyond comprehension that you would make a decision not to provide the proper level of security within your company to protect the personal and private information of customers," Blake [chairman of the Massachusetts Credit Union League and chief executive of HarborOne Credit Union in Brockton] wrote in the Jan. 26 letter.
>
> – Abelson, Jenn, and Ross Kerber, “Markey calls for FTC probe of TJX, Bank files lawsuit as pressure rises over data breach,” *Boston Globe,* January 31, 2007, http://www.boston.com/business/articles/2007/01/31/markey_calls_for_ftc_probe_of_tjx/?rss_id=Boston+Globe+--+Business+News

And while a front page story in the *Wall Street Journal* is usually great publicity for a company, it is “different” when the story reminds all the readers about the widespread impact[20] of what is probably the worst data breach so far in the US.

> MBA spokesman Bruce E. Spitzer said that "we're hearing of hundreds of thousands of customer accounts that have been affected."
>
> – Pereira, Joseph, “Wide Credit-Card Fraud Surfaces in TJX Hacking,” *Wall Street Journal*, p. D3, January 25, 2007, http://online.wsj.com/article/SB116969301962887162-search.html?KEYWORDS=tjx&COLLECTION=wsjie/6month

4. How to Select a Solution to Protect Your Small and Medium-Sized Business

For a small or medium-sized business, it is important to select an Internet threat solution that is effective, simple to install and operate without a large in-house IT staff, and doesn’t impose too many costs of its own. Otherwise the “cure” could be worse than the “disease.”

Many small and mid-sized businesses prefer to work with solution providers other than the monolithic market leaders because they have a well-deserved reputation for being more nimble and responsive to customers. As a business owner or manager, you understand that intuitively and you are always working hard to ensure that your company continues to be responsive to your customers.

If you want your business to run at top efficiency, you cannot rely on a security solution that consumes an inordinate amount of computing resources and, as a result, degrades your business' overall productivity. The net result is that the company as a whole will not be running at top efficiency, nor be able to compete effectively in the marketplace.

That being said, the market share leaders in security solutions today are far too complex and do in fact cause significant lost time, increased costs and decreased productivity. In some cases, end-users will even will try to deactivate desktop security software, because it slows down their systems so much, thus exposing the company to risk.

4.1. Criteria for Security Software Applications and Tools

4.1.1 Comprehensive Security

A good perimeter firewall on the perimeter (the network point that connects your company's network to your ISP and the Internet) is *absolutely essential* for good security to stop a lot of the older hacker threats that are still in circulation today. However, hackers and cyber criminals in particular have learned to work around the perimeter firewall. For today's wide-ranging malware threats, it is necessary to have a range of security applications running on each desktop: a firewall that also includes "intrusion detection and prevention," anti-virus, and email anti-spam tools. All servers should also have a local firewall installed. And the best way to get all these tools is to get a "suite" from a recognized security software vendor.

4.1.2 One Vendor Rather Than Many

It is certainly possible to get all these tools from separate vendors. It sounds appealing but in practice this piecemeal approach produces high costs *and* poor security. Each security application or tool will have its own control panel for setup and administration, meaning that instead of one control panel with a suite, there are now three or four control panels to work with. And there is the additional risk that these applications will actually *conflict* with each other, producing unexpected system crashes and lockups, leading to productivity loss and potential data loss. There is also the risk that the applications still leave gaps in security that can be exploited by a clever hacker. By getting all these tools from a single vendor, you can avoid these problems and get truly effective protection.

4.1.3 Ease of Installation and Use

For a small or medium sized business, simplicity and ease of installation are key issues. Smaller companies usually have only one or two full-time IT employees at most, or perhaps only a part-time contractor or consultant. These few people are responsible for the entire range of information systems including all servers, employees' desktops and laptops, the printers and routers, and the telephone and voicemail systems. Because of this range of responsibilities, no one area, including security, can use too much of these peoples' limited time. An overly complex security solution will never work properly.

4.2. Rare Industry Event: Frustrated Symantec Partners Go Public With Dissatisfaction and Seek Alternatives

The software business is one of constant change, including frequent new products. There are always going to be some issues about deadlines, new features that don't work as expected, missing features, or older features that somehow don't work right in the new release. For people in the software business this is normal and predictable. The issues get resolved quietly, and everyone moves on.

So it was an extremely unusual and rare event when a number of resellers *publicly* expressed their frustration about a key Symantec security product in a story published in the trade paper *Computer Reseller News* in March 2007[21].

> Symantec's enterprise antivirus software has performance issues that are causing some frustrated channel partners to consider other vendors' offerings.
>
> Symantec Antivirus Corporate Edition -- also a component of the vendor's Antivirus Enterprise Suite -- has been breaking applications, bogging down PC performance and slowing systems to a crawl, some solution providers told CRN.
>
> 'Our customers have been seeing a lot of Symantec antivirus-related problems, such as delaying applications unnecessarily, and it's reached the point where we're disabling it on many clients,' said a Symantec partner who asked not to be named.
>
> Reader comment on article: *I have installed both AVG and others instead of symantic. [sic] Relationships aside the customers needs should come first.*

4.3. Software Resellers Now Prefer AVG Software

Just about the same time that Symantec partners were publicly expressing their dissatisfaction with Symantec, nearly 1 million software resellers ("VARs," or Value-Added Resellers) voted Grisoft and its AVG product the preferred alternative for security software[22].

> Lawrence M. Walsh, editor of *VARBusiness* magazine, which covers the business of technology integration, explains that there are numerous reasons why such brands are preferred to category leaders. *"Products such as AVG often provide value-added resellers with superior performance, innovative technology and preferential price opportunities," says Walsh.* [Italics added for emphasis.]

5. Introducing Grisoft Security Solutions for Business

5.1. Overview

Grisoft *AVG Internet Security* products provide complete centrally controlled protection against all of the new forms of Internet-based threats. They provide iron-clad, affordable protection against threats, and are easy to install and operate, even for a company with only a small IT department or a company using an outside IT consultant.

Grisoft products have been tested and validated by third party certification entities to be equal to market leaders without the bloat and overhead of those vendors' products. Grisoft also provides free 7x24 support.

5.2. Key Differences Between Grisoft and "Market Leaders"

Anti-Virus today is a mature technology. All the major products today offer effective protection. There is no real reason to move from one product to another because of the differences in protection. However, there ARE valid reasons to change products.

5.2.1 Performance and Manageability

AVG has been designed to use very little system resources. This is no accident. Grisoft had the *vision* several years ago to recognize that despite increases in computer speed, the slow performance of security software was becoming a significant issue to corporate users. AVG designed their products to so the user "doesn't even know it's there," even while actively scanning.

Thus, AVG users do not have issues with "bloatware" or system slowdown. These differences are dramatically illustrated in a recent comparison published online.

AVG is also very easy to uninstall, if a company wants to switch to a different product. Products such as Symantec *Norton Internet Security* or McAfee *Total Protection* are well-known to be difficult to install in many situations, and impossible for the average person to uninstall completely.

Selected results of a test to see which applications affect Windows performance. Tests were done on the latest version of Windows XP SP2. For clarity, only the security product results are shown. The only version of AVG tested was AVG 7.1 Free but this result would be very similar to AVG 7.5.

Software	**% Boot Delay**	**% Prime Delay**	**% FileIO Delay**
Norton Internet Security 2006	46	20	2369
Norton Internet Security 2007	45	8	1515
McAfee VirusScan Enterprise 8	7	20	2246
AVG 7.1 Free	**15**	**0**	**19**

– "What Really Slows Windows Down,"
http://www.thepcspy.com/articles/other/what_really_slows_windows_down/5

5.2.2 Economic Considerations

The market-share leader Internet Security products cost average about $70/year/user.

AVG Internet Security Suite is only $69 for a two year license, thus cost/user/year is less than half of that of competitive products. Thus, for better performance and a lower cost and equal protection, AVG users enjoy the same or better level of security.

6. Action Item: Try Out Grisoft *AVG Internet Security*

If you have read this Business Brief and agree that your business needs a Business Continuity plan for the Internet-based threats to your company's computer systems and networks, we invite you to learn more about Grisoft and its security products.

You can visit the website at www.AVG.com to learn more about the company and its products. Click on the Downloads tab to try out a 30-day free trial of *AVG Internet Security* suite, either AVG Internet Security Network Edition or AVG Internet Security SBS Edition. The SBS Edition has all the protection contained in the Network Edition, and also adds support for mail servers such as Microsoft *Exchange*, Lotus *Domino*, or Kerio *MailServer*.

[1] Federal Financial Institutions Examination Council, Business Continuity Planning, IT Examination Handbook, May 2003, http://www.ffiec.gov/ffiecinfobase/booklets/bcp/bus_continuity_plan.pdf

[2] www.businessweek.com, www.fortune.com, www.forbes.com., www.wsj.com

[3] “Man charged with unleashing 'Melissa' computer virus,” April 2, 1999, http://www.cnn.com/TECH/computing/9904/02/melissa.arrest.03/index.html

[4] Cantrell, Amanda, “Is your company prepared? One company's experience, plus tips for preparing.” October 4, 2005: 12:23 PM EDT, http://money.cnn.com/2005/10/04/technology/disaster_recovery/index.htmBusiness after disaster

[5] “*Economist Intelligence Unit survey highlights the extreme criticality of IT Systems,”* http://www.continuitycentral.com/news03100.htm

[6] http://en.wikipedia.org/wiki/Nigerian_Letter. Wikipedia defines the “Nigerian letter” as “An advance fee fraud is a confidence trick in which the target is persuaded to advance relatively small sums of money in the hope of realizing a much larger gain.”

[7] http://www.mitchell1.com/

[8] http://www.abacuslaw.com/

[9] http://quickbooks.intuit.com/

[10] Kurtz, Ronald, L., and Vines, Russell Dean, The CISSP® Prep Guide: *Mastering the Ten Domains of Computer Security*, Wiley Computer Publishing, 2001, p. 277.

[11] Washkush, Frank, Jr. “Hackers use Trojan to access server with personal information of 70,000 Vermont residents,”, Jan, 30, 2007, http://scmagazine.com/us/news/article/629642/hackers-use-trojan-access-server-personal-information-70000-vermont-residents/

[12] Kerber, Ross, “TJX credit data stolen; wide impact feared,” January 18, 2007, Boston Globe, http://www.boston.com/business/globe/articles/2007/01/18/tjx_credit_data_stolen_wide_impact_feared/

[13] Greenemeier, Larry, “Hack Attack Means Headaches For TJ Maxx,” Information Week, Feb. 3, 2007, http://www.informationweek.com/news/showArticle.jhtml?articleID=197003041

[14] Abelson, Jenn, and Ross Kerber, :Markey calls for FTC probe of TJX, Bank files lawsuit as pressure rises over data breach,” January 31, 2007, http://www.boston.com/business/articles/2007/01/31/markey_calls_for_ftc_probe_of_tjx/?rss_id=Boston+Globe+--+Business+News

[15] “6 charged in TJX credit-card hack case,” UPI, http://www.upi.com/NewsTrack/Business/6_charged_in_TJX_creditcard_hack_case/20070323-050215-2086r/

[16] Kaplan, Dan, “45.7 million-victim TJX Companies breach could lead to federal notification law,” SC Magazine, March 29, 2007, http://scmagazine.com/us/news/article/647277/457-million-victim-tjx-companies-breach-lead-federal-notification-law/

[17] Kerber, Ross, Analysts: TJX case may cost over $1b,” Boston Globe, April 12, 2007, “http://www.boston.com/business/personalfinance/articles/2007/04/12/analysts_tjx_case_may_cost_over_1b?mode=PF

[18] Brenner, Bill, “Banks prepare lawsuit over TJX data breach,” April 25, 2007, http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1252778,00.html

[19] Pereira, Joseph, “Wide Credit-Card Fraud Surfaces in TJX Hacking,” Wall Street Journal, p D3, January 25, 2007, http://online.wsj.com/article/SB116969301962887162-search.html?KEYWORDS=tjx&COLLECTION=wsjie/6month

[20]“Stolen Credit Cards at T.J. Maxx,” Wall Street Journal, March 29, 2007, http://online.wsj.com/article/SB117518748036953348-search.html?KEYWORDS=tjx+security&COLLECTION=wsjie/6month

[21] http://www.crn.com/security/197800616

[22] “AVG Security Software Named a Leading Alternative Brand By VARBusiness Magazine Readers,” February 20, 2007, http://www.allbusiness.com/technology/computer-software/4054116-1.html