

White Paper



Inc.

The Threats You Face: Why Total Protection Matters

Computer Associates International, Inc.
Published in Partnership with Inc.
June 2005

The Threats You Face: Why Total Protection Matters

A third of small- and mid-sized businesses have suffered at least some disruption due to security issues.^{1,1} Just as threatening are business losses caused by compromised data integrity or privacy — as well as disasters and accidents beyond anyone’s control. The first in a series of white papers designed to help you protect your business, this paper describes the dangers your business faces as well as the techniques that can help mitigate or even eliminate them.

The High Price of No Protection

- > **Productivity declines** as employees scramble to restore what’s been lost or vandalized rather than doing their normal jobs.
- > **Lost revenue** from disrupted transactions. Customers, suppliers, partners can be affected if, say, your key databases have been made inoperable by a hacker or virus.
- > **Vandalized systems** that take time and money to bring back to normal operation.

The Real Threats You Face

The Internet has become a universally adopted tool, not unlike the automobile or the telephone. Thus, even if the Internet doesn’t serve a primary role running your business, it certainly plays a secondary one — one that will only become more important (and critical) to your ability to compete as both consumers and other companies increasingly depend on the Internet to communicate and transact business.

Consider: more than two thirds of all the people in North America use the Internet, while there are already more Internet users in both Europe and Asia and where internet access is growing over 50% faster than in the United States.

Because of the Internet, email and instant messaging have become important modes of communication, speeding the exchange of information and tightening the time that’s needed to complete business transactions.

What’s more, how goods and services are marketed and sold is changing forever.

But Internet usage also poses a number of real dangers:

- With both home and business users comfortable using the Internet it has become the medium of choice for both product research and marketing. But there is no Internet police force to check the validity of claims and the authenticity of information, sites and sellers. So while sales and marketing professionals drool at the prospect of leveraging such an incredible source of customers, cash and information, the

The High Price of No Protection

- > **Lost data** when backups don't work properly, or when a virus or trojan horse infiltrates your system.
- > **Competitive secrets stolen**, along with the potential business opportunity and product/service revenue streams they represented.
- > **Compromised customer confidence** when security breaches result in late shipments, order errors, etc.
- > **Legal liability** when sensitive information is stolen and contributes to theft of customer or employee identity and/or is otherwise misused. Businesses can also be at risk if they fail to take precautions against unwanted pop-ups and other potentially upsetting occurrences.

Internet and its billion dollar sales channel is monitored using a "laissez faire" approach, creating numerous opportunities for hackers, thieves, spies and vandals to prey on the unsuspecting.

- When transmitting email the Internet acts like a giant broadcast system. Messages are broadcast to every listening station together with the addresses of all recipients. Stations connected to each recipient pick up every message. So it's very easy (and far quicker than traditional direct mail) to send a single message to hundreds or even thousands of people at one time. This means messages that contain viruses, scams or other forms of malicious code are quick and easy to send out to everyone on the Internet, too. And those that can self-replicate, repeat the process using each invaded PC's address list. It is email recipients themselves who must be aware, block or delete unknown emails dismissing the temptation to be lured by fantastic sounding offers and opportunities that are bogus.
- Despite the hype, it's not the Internet itself that poses the largest danger. Most businesses have become so reliant on information technology that the biggest threats are the more common or "traditional" ones: hardware failure, human error, software corruption, theft and natural disasters like fires, floods and power failures.

The Top 5 Technology Challenges and the Solutions You Need to Address Them

In order to continue to conduct business successfully, all firms must protect themselves against likely upheavals — whether caused maliciously or accidentally. Here, in brief, are the major challenges that businesses must face down:

Multiplying Malware and Other Intrusions: The Impact of Viruses, Phishing and More

Arguably, the Internet is the freest place on earth. While governments can police content held in and distributed from their territories to prevent criminal activity, generally in global cyberspace, anything goes.

So although the Internet is a great source of education and knowledge, of fact and opinion, and of history and prediction, you can just as easily find "recipes" for creating havoc, too. And many have used the Internet for criminal purposes. Hence, it doesn't pay to be complacent or to believe that because your company is small or relatively unknown, that your data, applications and systems are secure. The broadcast nature of the Internet means that malware can be designed to test everyone's defenses no matter how significant or complex a business. The goal is to find the gullible and the vulnerable.

The effects of such attacks and intrusions can be devastating:

- **Corruption of and/or loss of critical business data, applications, and systems**
- **Loss of productivity** as your systems slow down under the weight of covert software and as staff struggle to restore data and operations

Protecting Your Business: Avoiding the Most Common Mistakes

- > **Insecure passwords.** Passwords should not be weak (they need to be at least seven characters long and include a mix of numbers, upper- and lower-case letters, and !@#\$%^&*()+); should not be shared; should be changed at least monthly; and should not be written down for someone to find.
- > **Opening email attachments from strangers.** Remember: everyone knows someone named John, so make sure your employees check the sender's email address, the subject line, and confirm the validity of any/all attachments (these should be mentioned by name in the sender's email text).
- > **Asset ignorance.** If you don't know what you have, you will not be able to protect it. You need to know all about the data your business depends on (in databases and employees' PCs) as well as the software, systems, storage, and network configurations it uses. To keep up with it all, use an asset management solution and do not allow employees to add their own unprotected software or appliances.

- **Data privacy violations** that can leave your company susceptible to legal liabilities
- **Theft of sensitive information** (such as new product designs) that compromise your company's ability to remain competitive
- **Loss of customer confidence** when word of attacks or intrusions becomes spreads

According to the 2004 CSI/FBI Computer Crime and Security Survey, which queried nearly 500 U.S. corporate and government security practitioners, it was found that dollar losses from virus attacks cost more than twice as much as the next most costly kind of attack.^{1,2}

The good news: You can keep your business secure against threats both external and internal with a straightforward combination of sound security policy and a well-crafted, implementation of security tools — see sidebar.

Out of Compliance: The Cost of Breaking the New Laws and Rules

After 9/11 and an assortment of corporate scandals, governments worldwide have stepped in with new regulations affecting corporate governance, financial and reporting practices, data protection and privacy, consumer protection, preventing terrorism, and more.

Consider the penalties for violating the U.S.'s Health Insurance Portability and accountability Act (HIPAA), designed to protect patient health information: civil monetary penalties of up to \$100 per violation (up to \$25,000 per person); criminal violations can incur fines as much as \$250,000 and prison sentences of up to 10 years.

Initially, most of the new laws — some violations of which carry penalties substantially greater than HIPAA violations — have been aimed at large, publicly-held companies. But many new laws (particularly privacy laws aimed at protecting consumers and employees) affect small and mid-sized businesses, too. What's more, there's a decided trickle-down effect from large-enterprise customers being felt in many mid-sized and smaller companies.

Increasingly, staying compliant with new laws and standards will require that virtually all businesses adopt basic security, data backup, and records management practices and technologies. Regardless, in today's technology-reliant times, these safeguards have simply become good operating procedure for businesses of all sizes and types.

When Disaster Strikes: Can Your Backup Data be Trusted?

When your computers and networks go down — whatever the cause — your business is very likely in real jeopardy with most of the anticipated trouble coming from the loss of critical information needed to keep operations running.

Protecting Your Business: Avoiding the Most Common Mistakes

- > **Not keeping current on operating/application/antivirus software patches and updates.** Online hackers and criminals keep breaking their previous speed-of-defect-exploitation records. Failing to patch and update software means they'll be getting into your business sooner rather than later, so it is important to continually check with your software vendors to ensure your updates and patches are current.
- > **Poor handling of sensitive data.** Is it backed up — and if it changes frequently, do you have a process to back up those changes? Is it locked down? Will you be able to restore your backups in a timely manner? Make sure.
- > **Not deploying encryption where available.** Chances are your people are sending data over the Internet, which is like a series of post boxes the contents of which can be easily read and copied. If it needs to be private, then it must be encrypted.
- > **Sacrificing security for convenience.** Don't, for instance, let someone install a dial-up modem in their office so they can access their work PC from home. Don't let employees ignore security policy because they think it's a silly hassle. Establish a policy and stick to it.

According to one study, companies that suffer outages lasting more than ten (10) days never fully recover financially, and more than 50% of these firms are out of business within five years.^{1,3} Given such circumstances, it is prudent to develop an affordable strategy that provides rapid recovery and minimizes loss of business and customer satisfaction.

Key to surviving disasters large and small is finding ways to preserve your data. Without the information that is its lifeblood, your business is in jeopardy. Fortunately, you can take advantage of the pioneering that larger enterprises have done in working out the processes required to survive major disruptions and combining this knowledge with today's low-cost data storage and backup/restore products and services.

Coping with Business Growth: More Opportunity, More Servers and PCs, More Software

As your company grows, information technology becomes increasingly more important to your operations — but ensuring that it is well-adapted to your business gets tougher and tougher.

To keep your business and its processes functioning soundly, systems, networks, and data all need to be managed, cost-effectively, even as your business's entire infrastructure becomes more complex. The right data storage, software license management, PC migration, and business modeling solutions will make all the difference.

Putting the Internet to Work for Your Business Brand

With all the information on the Internet, it's an increasing challenge to get your brand to stand out and attract the attention you seek. Most companies have web sites but only a relative few take advantage of the tools and capabilities available to drive up visibility. Despite the hundreds of millions of daily visitors to the Internet many sites attract hardly any of them.

Among the techniques that can help you in this effort are not only effective website design but also web-based marketing activities such as lead generation, opt-in customer communications, search engine optimization, content management aids, and, for those wanting to sell online, an e-commerce website. The final paper in this series is devoted to the topic of best practices for e-business and online marketing and will help guide you in the right direction.

The Bottom Line

These days, getting the protection your business needs to survive and thrive — and enhancing your online presence to boost the bottom line — has never been more affordable.

And, smaller enterprises are no longer forced to adapt products and services built for large enterprises — current offerings are designed to meet the needs of businesses of all sizes with an emphasis on simplicity and ease of use.

Protecting Your Business: Avoiding the Most Common Mistakes

- > **Ignoring physical security.**
That means don't leave your computer unattended. Don't leave unsecured laptops lying around anywhere, not even in the office. Keep the right doors locked, even if it's inconvenient.
- > **Ignoring strange behavior.**
Most security breaches are inside jobs. When someone's activities are notably unusual and nobody knows why, pay close attention.
- > **Lack of adequate training for system administrators and users.** Potential results: installation of unnecessary programs and services which become points of vulnerability because no one remembers them; forgetting test machines that are still "live."
- > **A disconnect between security policy and security implementation.** Your security systems and tools should be configured to enforce your security policies. If not, your business is dangerously vulnerable.

Endnotes

- 1-1 Security breaches affect majority of SMBs, The Yankee Group, September, 2004
- 1-2 2004 CSI/FBI Computer crime and Security Survey, The Computer Security Institute
- 1-3 Jon Toiga, Disaster Recovery Planning: Managing Risk and Catastrophe in Information Systems, Yourdon Press, 1989

For more information on CA's small and medium business solutions, please visit ca.com/smb.



Computer Associates®

© 2005 Computer Associates International, Inc. (CA). All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. This document is for your informational purposes only. To the extent permitted by applicable law, CA provides this document "AS IS" without warranty of any kind, including, without limitation, any implied warranties of merchantability, fitness for a particular purpose, or non-infringement. In no event will CA be liable for any loss or damage, direct or indirect, from the use of this document, including, without limitation, lost profits, business interruption, goodwill or lost data, even if CA is expressly advised of such damages.

Inc. and Inc. 500 are registered trademarks owned by Gruner + Jahr Printing & Publishing Co.

MP282960605