Preventing security threats and stopping unwanted activities

CASE STUDY

Plan for better security

SITUATION ECSEC is one of the UK's leading retail design and retail shop fitting, restaurant and bar refurbishment contractors. It's also a small business. Like many small businesses, it found out its computer system had been hacked at the worst time — right in the middle of a big project.

"We're not large enough to have dedicated IT staff and there's no doubt our IT security was starting to creak," noted Brian Trundle, director at ECSEC. One incident in particular threatened to delay the company's work on a plum project: fitting out the studio restaurant for *Hell's Kitchen*, the popular British reality TV program.

Specifically, the company's server had been compromised by an intruder and was being used as a botnet to relay thousands of spam messages selling counterfeit software. This caused their server to be blocked intermittently by ECSEC's Internet service provider (ISP). The ECSEC team needed to properly secure the network and make sure they had all resources available to complete their project on time.

RESULT With no in-house IT resources, they turned to Vitality Consulting Services for a comprehensive technology audit, which revealed numerous server and network vulnerabilities, plus a critical gap in data protection. Ultimately, Vitality recommended and implemented "a combination of Symantec's Backup Exec™ System Recovery Desktop Edition and Symantec™ Protection Suite Small Business Edition, [to] offer a cost-effective, easy-to-use approach to tackling backup, malware and spam threats."

The solution is delivered as part of an automated, offsite backup service, managed by Vitality. "We simply pay Vitality a monthly fee and they take care of the rest," says Brian Trundle. "We now have the confidence that whatever happens, our entire systems are safe from a disaster." Beyond the ability to finish the *Hell's Kitchen* project on time, Brian Trundle estimates that general productivity has increased 25% thanks to "less time spent wading through spam [99.9% eliminated] or waiting for slow-performing PCs to respond."

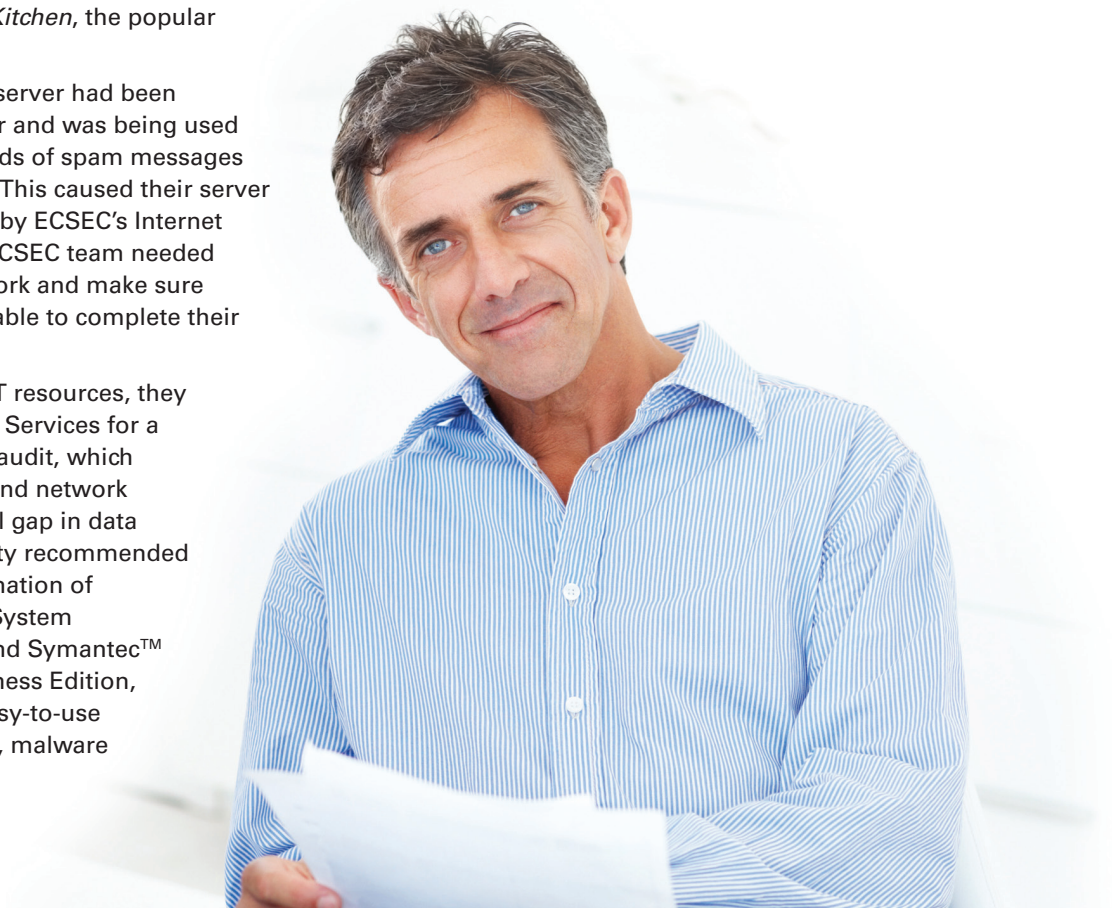

Photo source: Veer® stock photos.
Photo does not represent Mr. Brian Trundle, ECSEC, or any related associates or products.

CenturyLink™ Business

How do I protect my business without locking data down?

How important are computers and the Internet for small businesses today? Few companies of any size could manage many daily processes without them. But how many small businesses actively, consistently prevent threats to their computer networks and block unwanted activities? Achieving the right level of security for your business will take some homework and investment, but rest assured that there are good options and support for small businesses today.

What does it mean to prevent security threats?

Generally, it means putting the right policies, processes and tools in place to protect your:

- **Information**, especially confidential data related to finances, customers and employees.
- **Infrastructure**, including computers, networks, mobile devices and servers.
- **People**, who might otherwise become victims of email and Internet attacks (and expose your business to these risks).

What are the security threats?

- **Malware attacks —** Malware is short for "malicious software," which includes viruses, worms, Trojan horses, spyware and adware. These programs are the weapons hackers use to infiltrate computer work stations, laptops, servers and mobile devices in order to damage and disrupt your systems; corrupt and destroy your files; secretly monitor your Internet activity and infect other users.
- **Phishing —** Fraudulent emails, instant messages and websites or pop-ups that trick you into revealing personal or financial information by persuading you to click on links or enter your details. The sources pose as trusted businesses and brands (like a bank, auction website or popular social network) to fool you into revealing your usernames, passwords, credit card numbers, etc.
- **Spam —** Unsolicited junk email that's been sent out in bulk. Spam can range from relatively harmless but annoying marketing information to messages containing malware as a link or attachment.

How do these threats get in?

- **Email and instant messages —** Your communication outlets naturally provide the opportunity for hackers to deliver spam and malware.
- **Websites —** Threats hidden in Web pages can launch a malware attack when you simply visit a certain page, and popular social networking websites may contain applications that, once opened, may launch malware. Also, malware can infect your business website and use your own system to spread itself and attack other users.
- **Software weak spots —** Even the software you buy from legitimate, well-known vendors may have flaws that hackers can exploit. Once aware of vulnerabilities, vendors typically release security patches for you to download and install.
- **User activity —** Clicking on links or opening documents from dubious emails or websites (spam); entering your username, password or credit card details on unsecure sites; downloading and installing programs from unknown sources…all of these activities can be prevented with appropriate user policies and education about security threats. For example, when entering data online, look for a logo from a trusted security company such as VeriSign, or the "lock" icon that indicates an SSL certificate.
- **Internal sabotage —** In the intimacy of a small business you may feel you really know your people, but allowing everyone complete access to your files and systems invites destruction or theft of data and devices by that one person you didn't know so well.

"Small-to-midsize business (SMBs) fail to tackle their information security problems for three main reasons," says Jim Lippie, vice president of Staples Network Services. "Employees do not have the necessary skills, company managers are focused on day-to-day operations and they fail to budget enough for information security."

— Dark Reading Tech Center, 2010[1]

CenturyLink™ Business

What do I need to protect my business?

Here are the basic technology solutions that can help you keep your computers and data safe.

- **Network firewall:** Firewalls block unauthorized users from infiltrating your computer network, while allowing your authorized users access to the Internet and other applications. Firewalls can be installed as hardware or software and may be included with your Internet service.
- **Anti-virus/anti-spyware protection:** Installing and updating anti-virus software is a simple and essential way to prevent malware attacks. These solutions may be included in your Internet service.
- **Email spam filter (email firewall):** Spam filters block unwanted and possibly dangerous email messages. You can either install spam filtering software on your computer or network server, buy a dedicated appliance or outsource spam filtering to an online service provider.
- **Encryption for your files, hard drives and backup disks:** Encryption software encodes data into an unreadable series of characters with a secret key or password so you can send or store it securely.
- **Website hosting service:** Using a hosting service for your business website (instead of hosting it on your own server) will take care of your website's security needs and provide redundancy, meaning your website can be properly restored if attacked.

How will preventing security threats make my business better?

- **Avoid business interruptions and improve productivity —** Having the right protection in place will give you more time and power to do business instead of wading through spam and dealing with security issues.
- **Recover faster from security incidents —** No security plan is 100% foolproof, but appropriate protection can minimize damage and help you get up and running faster.

Are you protected against:

- **Hackers** who could break into your Web server or work stations?
- **Viruses or worms** (malware) that could access your systems via email?
- **Server or network failure,** which could bring order processing and other work to a halt?
- **Identity theft?** What could happen if someone stole your password(s)?
- **Internal sabotage** of your computer systems by unhappy employees?

If you answered "no" or "not sure" to any of these items, it's time to take control of your security needs.

Related guides:

Protecting your data

Managing data storage

Maintaining compliance

For more detailed information about preventing security threats and stopping unwanted activities, please refer to the accompanying white paper on this topic.

CenturyLink™ Business

- **Reduce legal risks —** Depending on your industry, you may be required by law to make sure sensitive data, such as credit card information or health records, is kept safe, private and intact. (See the *Maintaining compliance* brochure for more guidance).
- **Maintain customer confidence —** Nobody wants to be famous for a security breach, especially if customer information is involved. When you protect your systems, you're protecting your reputation and your brand.

73% of the small business respondents were victims of cyber attacks in the past year, and 100% of those victims suffered expensive downtime, loss of important corporate data and/or personally identifiable information of customers or employees.

— Symantec 2010 SMB Information Protection Survey[2]

Need more? We're with you.

Your community representative is always happy to help. You can count on them as a resource for compliance solutions to consider that fit your specific business needs, budget and level of expertise, as well as advice and resources on a range of small business technology issues.

Visit **http://centurylink.com/smb-resources** to contact your community representative, and learn more about how technology can boost your business. You'll find information sheets, videos, case studies and more.

[1] Dark Reading, http://www.darkreading.com
[2] http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=smbsurvey2010

Service not available in all areas. Contact CenturyLink for details.

CenturyLink™ Business