The Confident SMB
IT AS YOUR BUSINESS ENABLER

Inside
- SHI International Corp. enables green efficiencies for MacDonald-Miller Facilities Solutions
- IT Health Check Delivers Quality Care
- Lock Up Your Data: The Importance of Encryption

Be Prepared!
A Checklist for Disaster Preparedness

Symantec.
Case Study
Sustaining Building Performance
IT solutions from SHI International Corporation and Symantec support green efficiencies for MacDonald-Miller Facility Solutions.
By Mark L. S. Mullins

Features
Lock Up Your Data
Ramiﬁcations of a data breach are often greater for SMBs; encryption plays an important role.
By Ken Downie

IT Health Check
Providing quality care comes down to information; recommendations on how to store, protect, and manage it.
By Courtenay Troxel

In Every Issue
Business Perspectives
Selling the Business and Increasing Efﬁciencies
Spend more time running your business in 2011 by relying on your IT partners.
By Carine S. Clark

ThinkTank
Looking Forward to 2011
Security and storage predicted to be critical focus for SMBs.
“Selling” the business and increasing efficiencies in 2011

Whether you believe the economy is still in a rut or it’s on track for a solid recovery in 2011 doesn’t change the fact that last year was a tough year for many SMBs. Because of that, you might have adopted a more cautious approach toward purchasing new hardware and software for your business. But lessons were learned. For example, the economy pushed many SMB leaders to focus on “selling” their business; that is, reemphasizing the importance of what they do for their customers and how it can benefit them, regardless of a weakened economy.

As an SMB owner, you know that selling the business means pounding the pavement not only to reduce costs, but to strengthen customer relationships. And because you know your customers best, your passion for your business shines when you speak to your customers. By keeping relationships strong during tough times, the investment is likely to pay off when economic times improve. Perhaps the biggest obstacle you face is getting around to speaking with everyone!

Pounding the pavement also means less time for other things. Maybe you had to delegate some decision-making to others. For example, relating to IT, many of you saw the need to assign the selection process to internal staff—perhaps IT administrators and office managers, depending on your business size and resources—or to external consultants. Simply put, you recognized the need for experts to help you make the right decisions to survive in this economy. So while you “sell” the benefits of your business to your customers, others—including IT consultants and VARs—are helping you to increase operational efficiencies, bolster security, and safeguard your data against disaster. Ultimately, you want to increase revenue and get more value out of your existing information assets.

Symantec and its partners are here to help you to focus on running your business and take advantage of the best opportunities in 2011. May you continue to “sell” your business by talking to more customers and by operating more efficiently. I wish you continued success and growth in 2011!

Regards,

Carine S. Clark
Chief Marketing Officer, Symantec
Looking Forward in 2011

Prediction: central role for security and storage

With 2010 in the books, Symantec’s security and storage experts offer their predictions for the year ahead, based on their observations of the information protection landscape. Here’s what they see: virtualization, cloud computing, mobile security, and social media taking center stage.

For starters, use of smart mobile technology by consumers will continue to grow, with Gartner, Inc. estimating that 1.2 billion people will be using mobile phones capable of Web connectivity by year’s end. As a result, the line between business and personal use gets even more blurry, with the devices finding their way further into companies through a back door. Cybercriminals will turn their attention to mobile devices, driving new IT security models to market.

In the virtualization space, IT managers attracted to virtualization cost savings will increasingly find that fragmented implementation and lack of standardization will expose gaps in the security, backup, and availability of virtual environments. Organizations are realizing that virtualization is simultaneously increasing management and storage costs. Without a plan to protect these environments, they may not realize the full return on investment.

Use of public and private clouds will also continue to grow as they become more available this year. For IT managers still unsure about the cloud’s capabilities, new tools will emerge to help manage the cloud’s complex storage environment and help administrators increase their understanding about unstructured data. In addition, regulators will start to address the trend toward more mobile and less centralized data, which will drive organizations to increasingly implement encryption technologies. See the full details on the predictions here.

SMBBEAT

Norton Security Software Included with HP PCs
Symantec recently announced that select HP PCs for small offices and small businesses are shipping with Norton Internet Security 2011 software. HP is providing its small office and small business customers with a full-featured, complimentary 60-day subscription to the solution, which detects and blocks online threats, preventing cybercrooks from stealing critical information and business data. Norton Internet Security also features Norton Insight, an industry leading reputation-based security technology, which far exceeds traditional security technologies in detecting new malware. In addition, Norton offers tips and information for HP business PC owners on best practices for minimizing online risks and maximizing data protection. HP noted that its small business customers trust Norton as a world leader in security solutions for PCs. The pre-installed
The Changing Face of SMBs

New tech trends reshape the small and medium office

What’s on the horizon for small and medium-size businesses for the coming year? According to technology analyst firm J. Gold Associates, a number of growing technology trends will reshape how SMBs operate.

In a trend that mimics personal cell phone use, SMBs will continue to ditch landlines for smart phones, with as many as 35 percent of SMBs predicted to use cell phones exclusively in 2-3 years. Especially useful for companies with a mobile workforce, deploying PBX business phone functionality to mobile devices will be a rising trend in the years ahead. Falling prices for smart phone technology will only accelerate the move.

While some tech prognosticators are predicting the demise of the laptop (on the heels of the desktop PC’s gradual passing), SMBs will continue to employ laptops in significant numbers. The flexibility of using laptops off-hours to complete complex tasks enhances its value, especially as more employees work remotely. J. Gold Associates predicts laptops will represent 65 to 75 percent of the total corporate PC market by 2013. But by 2014-15, tablets and lighter mobile computing devices will reduce the number of PCs in use by 20-25 percent.

As social media continues to become more business-friendly, SMBs will not only take fuller advantage of marketing opportunities, employees will increasingly turn to messaging platforms such as Facebook chat, Facebook Messages, and Twitter direct messages to communicate with clients and associates. While this offers a nimble means of contact, it also brings up archiving issues, especially for SMBs where monitoring communications is a legal necessity. As these and other technologies continue to evolve, SMBs will be on the forefront of new tech adoption for more efficient business operations. Read more here.

security suite will protect online businesses from online threats from the point of set-up. Read more here.

GeoTrust Top SSL Certificate Provider
GeoTrust, Inc., a leading certificate authority (CA), is the top provider of Secure Sockets Layer (SSL) certificates, according to the Alexa Netcraft SSL Index for January 2011. It’s the eighth month in a row that GeoTrust has earned the number one ranking. Acquired by Symantec as part of VeriSign, GeoTrust maintained its leadership over Go Daddy, securing 34,412 unique domains within the Alexa Top Sites list for the month. In comparison, Go Daddy registered 27,825 unique domains during the same period. Alexa Internet is a well-known site traffic measurement service that ranks the most visited sites in order of popularity. GeoTrust is the world’s largest low-cost digital certificate provider with more than 100,000 customers in 150 countries. Read more here.

Continued on next page
Symantec announced a new management plug-in for VMware vCenter Server available to Backup Exec 2010 users. The plug-in reduces the complexity of managing backups in virtualized environments that use VMware. It also provides a comprehensive view of virtual machines and displays granular details of virtual machine backups within the VMware vCenter Server console or vSphere Client. While virtualized environments offer cost savings and infrastructure flexibility, they also require new approaches to data protection. The plug-in works with core Backup Exec virtualization features to provide a consolidated protection status view of a number of VMware elements, including the last backup run and next scheduled backups, the type of backup (full, incremental, or differential), backup policy, specific backup job log information, and potential risk of certain policies. Backup Exec 2010 provides a single tool that allows companies to protect physical and virtual servers, manage disk and tape targets, and backup full machines and individual files. Read more here.

**Symantec Positioned in Leaders Quadrant**

Symantec has been positioned by Gartner, Inc. in the Leaders Quadrant of the 2010 Magic Quadrant for Endpoint Protection Platforms (EPP). As the security

---

**Holiday Shopping Blues**

*Generous spirit leaves shoppers vulnerable*

The holidays often bring out the best in people, such as generosity, philanthropy, and positive community spirit. Unfortunately, these same traits can also leave online shoppers vulnerable to cybercriminals. The “Connected by Careless” study conducted by Javelin Strategy & Research, and sponsored by Norton, showed that while the amount of online transactions increased during the holiday season, many consumers didn’t take even the simplest steps to protect themselves from cybercrime. For instance, half of people under 35 disclosed their real-time location on social networking sites such as Facebook and Twitter, potentially alerting thieves and leaving them at higher risk of home burglary and theft.

The study also revealed that consumers continue to take a casual approach toward Internet use, despite repeated warnings about lurking threats. This comes in their use of location-based services, mobile phone transactions, and online passwords.

Only 15 percent of survey respondents are able to explain geo-location, which informs people of a user’s whereabouts via mobile phone or social network, suggesting that mobile Internet users unknowingly engage in risky behavior. At the same time, 38 percent of consumers access their bank accounts or make online purchases via mobile phones, but more than half of these users don’t use basic protections such as an access password for devices. Read more about the study here.

---

**Read more here.**
landscape rapidly changes, traditional strategies toward endpoint security are failing to protect against a new breed of sophisticated attacks. The report notes that attention to better software management and maintenance is vital to reducing the attack surface and protecting users from social engineering attacks. The most effective forms of defense against malware include application control, configuration management, and vulnerability detection and remediation. To address the challenges of endpoint security in a changing landscape, Symantec has consistently augmented its endpoint security offering from a technology, efficacy, and performance perspective.

In a recent series of tests by PassMark Software, Symantec Endpoint Protection outperformed all competitive products. Watch PassMark video.

Symantec Launches Free Trial of SSL Certificates

Symantec recently launched free trials of its VeriSign Secure Sockets Layer (SSL) Certificates, which includes the free trial of fully functional Extended Validation (EV) SSL, an industry first. This allows website owners to try any class of VeriSign SSL on their websites free for 30 days without any obligation. Businesses that don’t require SSL encryption can also try the VeriSign Trust Seal free for 60 days. Get free trial now.

Cambridgeshire Bathrooms Ltd
Reduces data store by almost 80 percent with Backup Exec 2010

Erhardt and Warnell
Eliminates 99% of spam, with fewer than one false positive per million messages

Faiss Foley Warren, Public Relations & Government Affairs
Reduces back-up time by 75 percent with Symantec Protection Suite Small Business Edition

Gipe Associates, Inc.
Avoids virus attacks and other intrusions with Symantec Protection Suite

Touchstone Behavioral Health
Achieves 480-fold faster HIPAA audit preparation and 20-fold faster reporting

Winston-Salem Chamber of Commerce
Reduces recovery time 84-fold with data protection solution

Uh, you did remember to run the backup last night, right?
OFFERS
Save up to 50%: Switch to a Symantec Security Solution
Switch to Symantec Backup Solution and Save up to 30%
Download Symantec Protection Suite Trialware

WORD TO THE WISE
Symantec’s Small Business IT Trends for 2011
Top five trends for small businesses to look out for in 2011 that will help them achieve their IT goals.

Data Privacy Day
A checklist for protecting your information.

Symantec 2011 SMB Disaster Preparedness Survey
Study reveals that the cost of not being prepared is high, putting an SMB at risk of going out of business.

Meeting the Challenge of Endpoint Security
A mobile workforce has changed the nature of security. How do you meet the challenge of endpoint security?

Magic Quadrant for Endpoint Protection Platforms
Symantec named as a Leader in 2010 Gartner Magic Quadrant for Endpoint Protection Platforms.

Calculating the Cost: Email Threats and Financial Risks
Research provides a clear understanding to your level of exposure to email borne threats and potential cost to your business.

Best Practices for Financial Services Compliance
The fundamentals of financial services compliance makes the case for a combined archiving and security SaaS solution-based model.

Taxes & Security for SMBs
Online prep & filing make tax time easier

STREAMING
WEBCASTS
➤ The True Cost of a Healthcare Data Breach
➤ IT Consultants: Going Deep with Small Businesses
➤ A Cloud-Based Approach to Securing Today’s Distributed Workforce
➤ Threat Forecast 2011: Preparing for the Next Wave of Malware
➤ Protecting Your Information in the Age of WikiLeaks

PODCASTS
➤ Symantec’s 2011 Internet Security Predictions
➤ January 2011 State of Spam and Phishing
➤ Protecting Your Information in the Age of WikiLeaks
KNOWLEDGE SHARING

Calling all IT professionals!

*The Confident SMB* is looking for IT professionals to share their expertise on how they’re using Symantec technology to address small and midsize business challenges today and into the future. Submit your thoughts and analysis on lessons learned, tips and tricks, and best practices!

Send in your contributed article submissions to theconfidentsmb_editor@symantec.com for a chance to be featured in the next issue of the *Confident SMB*. To view the contributed article submission guidelines, click here.

iTUNES APP
Available for FREE at go.symantec.com/theconfidensmb-itunes

BUILDING CONNECTIONS

From best practices to troubleshooting, Symantec Connect is your place to find timely hints and get your questions answered. Check out some highlights from recent conversations on Connect.

**How to use Intel vPro Technology to decommission a system**
- Focus was on wiping a drive before recycling the system

**Need your WinPE image to be consistent across all DS servers, while being able to map to different drives**
- Solution: Tips on how to automate it all

**Why one company used USMT to migrate client PCs and end users to Windows 7**
- Tools and resources to deploy server 6.9 SP4, USMT, and Windows 7

**Packaging best practices for Symantec workspace virtualization**
- Packaging setup and special packing considerations

**Getting Symantec Software Workspace Virtualization (SWV) and Notification Server (NS) to work together**
- Steps to get newer versions of SWV and NS6 to work together to properly inventory your virtual applications

**To Virtualize or Not to Virtualize; that is the Question**
- Summary of value and key considerations
Be Prepared!

Checklist for Disaster Preparedness

In the 2005 animated production *Hoodwinked!*, Japeth the Goat sings an instructional ditty, “Be Prepared,” to Little Red Riding Hood (aka “Little Red”) when she comes to him for assistance to reach Granny Pocket’s house. He reveals in the song that he has horns for just about every occasion, ranging from horns for opening pickle jars to horns for hanging other horns. As he sings, Japeth shows Little Red a short cut through an old mine, and the two of them get in a mining cart and head out down the tracks for Granny’s house.

While on the way, however, an avalanche occurs, quickly rushing down the mountain and destroying everything in its wake. The avalanche consequently sends both Little Red and Japeth sailing into the air, and they disappear into the clouds as their mining cart crashes into the ground and splitters into thousands of pieces. Japeth reappears from the cloud wearing a new set of horns for just about every occasion.

By Patrick E. Spencer
horns outfitted with rotary propellers that miraculously lift him to safety and keep him from plummeting to an awaiting disaster—all the while shouting “I came prepared!”

Disaster preparedness disparity
Symantec’s 2011 SMB Disaster Preparedness Survey reveals that Japeth is several steps—or horns in his case—ahead of many SMBs. Published in January 2011, the survey revealed that half of more than 1,800 respondents do not have an IT disaster plan in place. Forty percent said that disaster preparedness is not a priority for them. Slightly less than half back their data up weekly or more frequently, and only 23 percent back it up daily.

Yet there is a significant disparity in the numbers: 44 percent say they would lose 40 percent of their data in the event of a disaster, and the typical SMB has experienced a system outage an average of six times in the past year—incuring an average cost of $12,500 per day. And this cascades down into the value chain: the customers of SMBs indicate that outages cost them an average of $10,000 a day.

This article aims to address two resulting questions. First, why are so many SMBs so ill-prepared for disasters? The time and cost of implementing a comprehensive disaster preparedness solution is a fraction of the repercussions of a disaster. Second, what are the steps an SMB needs to take to ensure it has the right disaster preparedness strategy in place?

Bridging the gap
Of SMBs with a disaster preparedness plan, only half put one in place after

Hoodwinked!

A 2005 computer-animated family comedy produced by Blue Yonder Films with Kanbar Entertainment, Hoodwinked! aspires to reveal the true story behind the events of the Little Red Riding Hood folktale. A rash of recipe book thefts (all credited to an anonymous figure called the “Goody Bandit”) serves as the underlying plotline. The movie opens with the discovery of the four main characters embroiled in an apparent fracas: Granny Pocket (Glenn Close), Little Red (Anne Hathaway), the Wolf (Patrick Warburton), and a Woodsman (Jim Belushi).

Detective Nicky Flippers (David Ogden Stiers) leads the investigation, contending that everything doesn’t always turn out to be the way it appears. After telling their side of the story, the four suspects are exonerated, and the identity of the “Goody Bandit” is revealed: a bunny named Boingo (Andy Dick). The storyline contains numerous references to personalities from other movies as well as the tale of Little Red Riding Hood itself. A minor character in the larger plotline, Japeth the Goat (Benjy Gaither), escorts Little Red on a shortcut to Granny’s Pocket house via a mine cart—at least until the avalanche races down the mountain and sends both of them sailing into the air.
suffering a system outage or data loss. Australian-based Symantec Partner eNerds specializes in serving SMBs that have between 20 and 250 employees, and many of them come to eNerds with either inadequate or no disaster preparedness plans in place. “In some instances, it can be attributed to the knowledge-level—or lack thereof—of the IT consultants they’ve previously engaged,” says the company’s Founder and President Jamie Warner. “Others have simply made the conscious decision not to deploy disaster preparedness solutions on the basis that they are irrelevant or the cost and time required to implement such a solution outweighs the risk.”

But this isn’t the reality, according to Jeremy Smith, technical services manager at another Symantec Partner The SoundSide Group, who reports that his firm received a flood of pleas for assistance following massive flooding that hit eastern North Carolina in October 2010. “We had some very painful conversations with potential clients who had previously thought that disaster preparedness planning wasn’t a priority or something that wasn’t relevant to them,” he conveys. “Most of them had a rapid conversion experience as the flood waters poured into their facilities.”

Disaster preparedness is something that needs to evolve and grow with the business according to Nick Joseph, the CIO at Orion Registrar, Inc., a Denver, Colorado-based small business that...
performs audits for clients in a variety of industries to verify their compliance with quality and environmental standards. “Our initial disaster preparedness plan was focused on protecting internal assets—basics around endpoint security,” he says. “We then began moving the dial as the business matured and grew, adding redundancy, backup and recovery, virtualization, and most recently offsite backup storage.”

The team at Crop Quest, Inc., which provides data analysis and consulting services to farmers across nine states in the Midwestern United States, concurs. “Our disaster preparedness strategy has evolved as our business has grown and matured,” says Jason Hooper, a precision ag specialist at the Dodge City, Kansas-based company. A decade ago disaster preparedness for Crop Quest meant protecting the network from viruses and regularly backing up data from the central server. Today, the company’s approach to security and data protection is much more sophisticated.

“Each of our agronomists carries a laptop computer in her or his vehicle, and they log critical information throughout the day on their clients’ soil quality and conditions, presence of insects, weeds, and disease, and much more,” explains Ron O’Hanlon, the company’s president. “We then take that information and run analyses—by field, by farm, or by region—and provide recommendations to our clients on everything from seed varieties, to planting dates, to fertilizers, to pesticides, to watering frequencies. All of this critical information must be backed up and protected.”

**Put to the test**
Based in Windsor, North Carolina, Cooper Insurance Agency understands...
the importance of disaster preparedness first hand. “We might not be in business without the precautions that we took around disaster preparedness,” reports Russell Phelps, the company’s president. The insurance agency experienced what he describes as a 500-year flood following Hurricane Floyd in 1999. “We had four feet of water all of the way through our offices,” he remembers. “Our server as well as desktop systems were all under water.”

Beforehand, Phelps had worked with The SoundSide Group to develop a disaster preparedness plan. This included implementation of Symantec Backup Exec for data protection and Symantec AntiVirus to protect the network from malware. The building was uninhabitable, and Phelps and his team relocated operations to the local funeral home for six months. The SoundSide Group retrieved the backup tapes from the prior night and had Cooper Insurance Agency up and running in a matter of a couple days.

Fast forward to early October 2010. “The weather forecast called for some rain, but not the torrents we ended up getting,” Phelps relates. “At one o’clock in the afternoon on Friday we knew that a flood was imminent, and we put out a sign indicating that we would close at three o’clock. When three o’clock arrived, while we were worried about the larger office space, we walked out and locked the door behind us with full

“Disaster preparedness is not only an issue of mischievous employees, or even well-intentioned employees doing dumb things.”

– Nick Joseph, CIO, Orion Registrar, Inc.

Nick Joseph, CIO, Orion Registrar, Inc.

WATCH
Symantec security and data protection solutions enable Orion Registrar to protect critical information while improving operational efficiencies.

LISTEN
CIO Nick Joseph explains how IT has evolved to meet new business requirements at Orion Registrar.
confidence that we could recover all of our data and systems with the help of The SoundSide Group and Symantec.”

On that note, The SoundSide Group had recently worked with Phelps to upgrade to Symantec Backup Exec 2010, Symantec Backup Exec System Recovery 2010, and Symantec Protection Suite and had tested out the disaster recovery capabilities as part of that process. “We simply didn’t realize how soon it would be put to test,” notes The SoundSide Group’s Smith. “Who could have predicted that we would experience two 500-year floods in a period of just over 10 years?”

On Monday morning, Andy Olsen, a technician from The SoundSide Group, met Phelps at his office, which had been besieged by more than two feet of water over the weekend, bringing with him a temporary server and storage system and replacement clients for each employee. Using Symantec Backup Exec and Backup Exec System Recovery Desktop Edition, he had the server and storage system, as well as each of the desktops, configured and running in less than one hour. “The ability to reimage disparate hardware systems using Backup Exec System Recovery was a real plus,” Smith says. “And just as impressive, there was no data loss, and the reimaging resulted in clients that looked and functioned exactly like the staff left them on Friday.”

The rapid recovery allowed Phelps and his team to focus on their customers. “We had just gone through...
the same disaster as our clients, and our office was a shambles,” he notes. “However, with a fully functional IT system, we were able to focus on servicing them. They were quite impressed and appreciative. Once again, The SoundSide Group and Symantec saved the day.”

Orion Registrar’s Joseph had an opportunity to see the value of his investment in Backup Exec System Recovery Desktop Edition when the laptop of an employee who was on business travel to the east coast for a three-day onsite audit at a client’s location became corrupted. “A quick analysis revealed the root cause as an operating system failure,” he explains. “Without Backup Exec System Recovery, we were faced with the prospect of either rescheduling the audit and flying the staff member back out to the east coast or flying me across the country to reimaged his machine.” Instead, Joseph used Backup Exec System Recovery to perform a full remote recovery in a matter of one hour.

What can you do to ensure that your disaster preparedness strategy will protect your systems and data when disaster does strike—whether natural or human made? Or if you don’t have one at all, what are the steps you need to follow to implement—and maintain—an ongoing solution? Regardless of your situation, the following checklist of five recommendations will provide you with a solid disaster preparedness foundation.

#1: Assessment
You need to gain a comprehensive understanding of your current disaster preparedness posture and compare that to your actual business requirements. This will enable you to identify gaps in your disaster preparedness plan and then map solutions to address those.

This is the exact approach that The SoundSide Group and eNerds take when they work with new clients. “We take a holistic snapshot of the entire

Checklist for disaster preparedness
The business case for a comprehensive disaster preparedness strategy is demonstrable. SMBs do not want to end up in the same situation as the desperate business owners who approached The SoundSide Group in the aftermath of the October 2010 floods in eastern North Carolina.
“We had some very painful conversations with potential clients who had thought that disaster preparedness planning wasn’t a priority or something that wasn’t relevant to them.”

– Jeremy Smith, Technical Services Manager, The SoundSide Group

IT environment—everything from security, to redundancy, to backup and recovery, to the network,” eNerds’ Warner says. “We go through a sequential process of analyzing the current IT environment against business requirements such as recovery time objectives, time for disaster recovery per user groups and systems, and risk acceptance versus cost and make recommendations accordingly.”

The SoundSide Group’s Smith concurs with this approach, adding, “We work with our clients to determine their business requirements and then pinpoint IT solutions that correspond with those.”

Orion Registrar engaged Mission Critical Systems, a third-party consulting firm and Symantec partner, for assistance in defining the company’s initial disaster preparedness strategy. “They helped us identify the areas for analysis and provided a template that we’ve used for documentation,” relates Orion Registrar’s Joseph. “We’ve honed this process, and the management team meets quarterly to review our disaster recovery plan and makes necessary course corrections.”

#2: The human element
Disaster preparedness is much broader in scope than just the technology element. “The human factor is just as important,” asserts eNerds’ Warner. Employees and contractors need to understand security best practices. These must be documented and staff should go through periodic training. “Disaster preparedness is not only an issue of mischievous employees, or even well-intentioned employees doing dumb things,” adds Orion Registrar’s Joseph. “It is a matter of everyone understanding their roles and responsibilities in the case a disaster strikes.”

For Crop Quest, the mobility of the business creates a human risk. “Our agronomists carry their laptops in their vehicles, and we want to ensure that those remain secure,” says Crop Quest’s Hooper. “As a result, we implemented a company policy requiring them to remove their laptops from their vehicles at the end of the day. Minimizing the possibility of lost data or productivity due to theft is important.”

#3: Comprehensive security
Downtime from a cyber attack for Crop Quest can also have a dramatic impact on the productivity of agronomists and their ability to deliver services to clients. “Each agrono-
mist has a schedule to maintain,” says Dwight Koops, regional vice president. “A few hours of downtime throws off the entire day’s schedule and their ability to deliver services to our clients.”

For years, Crop Quest used Symantec AntiVirus for protection against malware. The team opted to migrate to Symantec Endpoint Protection in 2009. “The integrated toolset of Endpoint Protection provides us with enhanced protection against the constantly expanding threat landscape,” says Crop Quest’s Hooper. In addition to antivirus and antispyware, the team has personal firewall installed on all clients and relies on intrusion prevention to proactively address potential threats.

Before Orion Registrar deployed Symantec Endpoint Protection, the company relied on different silo-based solutions for endpoint security. “Not only did we spend significant time managing these different solutions, but we had virus-related problems every other day,” recalls Orion Registrar’s Joseph. “Now we spend five minutes a day on endpoint security.” The results are impressive: Joseph estimates 2,000 staff hours are saved a year; time that is now spent on initiatives that drive the business.

SMB security measures must also encompass messaging security in addition to endpoint security. Beyond the operational benefits associated with staff productivity, an effective messaging security solution stops malware intrusions and disruptions to computing systems. “Symantec provides several messaging security options,” says eNerds’ Warner. “Depending on customer requirements, we can offer a software, appliance, or cloud factor.”

But messaging security is much more than simply blocking spam and malware. A comprehensive solution focuses on both inbound and outbound aspects. “In some instances, we’ve found that clients have been blacklisted because of marketing email campaigns, or even for sending email with malicious viruses contained within them,” Warner explains. “Emails from their staff aren’t reaching all of the destinations—sometimes unbeknownst to the client—because they’ve been placed on a blacklist.”

#4: Data protection
Increasingly, data is the lifeblood of many organizations—regardless of their size. For the three companies interviewed for this article, that is certainly the case; their operations, including the ability to serve clients, would be dramatically impacted in the event data loss.

It starts with understanding the physical location and the inherit risks—natural and human. For Crop Quest, it was a conscious decision to build its server room in the concrete basement of its headquarters. “We’re right in the middle of the northern part of ‘Tornado Alley,’ and we must protect our operations against the
risk of a tornadic event,” says Crop Quest’s O’Hanlon.

As part of its quarterly management review process, Orion Registrar concluded last year that off-site storage of its backups was necessitated. “The ultimate solution would be a collocated disaster recovery configuration, but that is simply not an affordable option for a small business,” says Orion Registrar’s Joseph. At about the same time, Orion Registrar decided to move its backups from tape to disk. “Disk is more reliable and easier to manage,” Joseph explains. “Plus, we can perform recoveries from disk much faster.”

Achieving successful backups is the lynchpin of a successful disaster preparedness plan. “Our clients typically have one of three data protection scenarios when they come to us,” reports eNerds’ Warner. “They have very old versions of backup software, their backup software is incorrectly configured, or they don’t have any at all. A discussion around recovery time objectives cannot take place until the backup challenges are solved.”

The teams from Crop Quest, Cooper Insurance Agency, and Orion Registrar concur with Warner. “Successful backups are the foundation for a successful recovery plan,” explains Orion Registrar’s Joseph.

Orion Registrar upgraded to Backup Exec 2010 and Backup Exec System Recovery 2010 and is reaping the benefits. The company began moving toward a virtualized server environment running VMware ESXi in late 2009 and currently has six physical servers and six virtual servers. “The ability to backup to both environments and then perform physical-to-virtual and virtual-to-physical recoveries is critical,” says Orion Registrar’s Joseph.

He uses Backup Exec System Recovery to capture images of our servers every hour in the case of a server meltdown. When the company’s physical Web server, which is used as the interface to auditors, customers, and employees, went down, he was able to reimage it onto a virtual server in 20 minutes. “Any measurable downtime would have been disastrous for us,” he observes.

**COMPANY PROFILE**

**Cooper Insurance Agency**

*Founded: 1944*

*Headquarters: Windsor, North Carolina*

*Employees: 6*

*Lines of Business: Auto, home, farm, business, boat, life*

*Symantec Technologies: Symantec Protection Suite, Symantec Backup Exec*

*Website: [www.cooperinsuranceagency.com](http://www.cooperinsuranceagency.com)*

**PARTNER PROFILE**

**The SoundSide Group**

*Founded: 2000*

*Headquarters: Plymouth, North Carolina*

*Services: Security and network assessments, disaster recovery planning, virtualization*

*Symantec Partner: Symantec Silver Partner, SMB Specialized, Authorized Technical Assistance Partner*

*Website: [www.soundsidegroup.com](http://www.soundsidegroup.com)*
The deduplication capabilities of Backup Exec 2010 shrank Orion Registrar’s backup windows by about 75 percent. In addition to time savings managing backups, the reduced data store cut the recovery window, since less data needs to be restored. “The benefits of deduplication are more than just cost and efficiency,” asserts Orion Registrar’s Joseph.

Shortly before the October flood, Cooper Insurance Agency upgraded to Symantec Protection Suite and added Backup Exec System Recovery with the help of The SoundSide Group. Its addition expedited the system and data recovery process. After the flood in 1999, it took a couple days for Cooper Insurance Agency to achieve full IT recovery; however, in the case of the October flood, The SoundSide Group had a full recovery of all IT systems and data in less than an hour. “Keeping on top of our software upgrades paid off for us—and big in this instance,” says Cooper Insurance Agency’s Phelps.

At the same time Cooper Insurance Agency moved to Protection Suite, the company also upgraded to Backup Exec 2010. “Cooper Insurance Agency’s backup window decreased from three to four hours to less than two,” reports The SoundSide Group’s Smith. “A smaller data store translates into faster recovery.”

**#5: Test frequently**

Confirmation that a disaster preparedness plan works should not occur when disaster befalls an organization. It is too late at that juncture. Rather, SMBs need to test their systems and processes. Make sure you have a well-documented process for remediating a threat if one does penetrate your network. This should include roles and responsibilities for each staff member involved and a step-by-step remediation process.

Prior to the October 2010 flood that beset Cooper Insurance Agency,
The SoundSide Group had tested the upgrade to Backup Exec 2010 and Protection Suite. “We knew the backups had been successful and that the systems and data could be brought back up again,” says Cooper Insurance Agency’s Phelps.

The time and cost of implementing a disaster preparedness strategy will seem insignificant once a disaster strikes, whether a malware intrusion, system outage, email blacklisting, or data loss. The immediate value may or may not be readily realized or in as dramatic a fashion as Cooper Insurance Agency. “But at the end of the day, when everything is tallied, the investment will pay for itself many times over,” maintains The SoundSide Group’s Smith.

Listen to Japeth the Goat
SMBs will do well to heed the words of Japeth the Goat: be prepared! Data volumes are growing at exponential rates and the threat landscape is quickly evolving and becoming more and more menacing. Don’t wait until disaster strikes to assess your disaster preparedness and then develop a strategy that meets your business requirements. Rather, as 2011 begins, move disaster preparedness to the top of your list of New Year’s resolutions. It might be one of your best-kept resolutions of your company’s lifetime; just ask Cooper Insurance Agency, Crop Quest, Orion Registrar, or Japeth.

1 Little Red avoids falling to her death by using her red hood as a parachute.

Patrick E. Spencer (Ph.D.) is the editor in chief and publisher for CIO Digest and The Confident SMB and the author of a book and various articles and reviews published by Continuum Books and Sage Publications, among others.
Residents of the Seattle area see them all over their region every day: white trucks and vans with a simple logo of two connected, white “M’s” within a red oval. After 45 years of existence, this fleet has afforded MacDonald-Miller Facility Solutions a level of brand recognition that most SMBs can only dream of.

The drivers of these vehicles support the heating, ventilation, and air conditioning (HVAC) systems of commercial and mixed-use buildings—and in some cases, plumbing and electrical systems as well. “We like to call our business the circulatory system of a building,” says Olwyn Palmer, marketing manager at MacMiller. “We are focused not only on making sure the heating and cooling works, but that it contributes to the overall performance of a building, and in an energy efficient way.”

By Mark L.S. Mullins
“From conception to optimization
“We can step in at any point in the life of a project,” Palmer adds. “We can be there for the inception and conceptual design. We might pick things up at the construction phase. Or we might get involved at the end, commissioning a building and getting it ready for service and maintenance for the rest of its existence.”

The company’s staff of mechanical engineers uses sophisticated technology for cutting-edge modeling and design of HVAC systems for new and existing buildings. “We have 3D, 4D, and even 6D design capabilities to help folks understand how their systems are supposed to perform,” Palmer explains.

For the construction phase, MacMiller has its own high-capacity fabrication facility that manufactures the ductwork.
New ways of doing business

Things are changing quickly in the industry, and MacMiller has maintained a competitive edge by staying current. One recent development is a trend toward the Integrated Project Delivery (IPD) model for commercial construction. “Under the old model, we generally served as subcontractor to the general contractor on a building project, and basically had responsibility for our part of the project,” Palmer explains. “Now, with IPD, everyone will be part of a collaborative team, and a lot of information will be shared among parties very early in the process.”

Early studies show that IPD improves the efficiency of building projects, increasing the likelihood of finishing on time and within budget, but the new model is not without IT implications. “We now have to have a platform that is compatible with a variety of software used by engineering firms, architects, and construction companies,” says Seth Henderson, network administrator for MacMiller. “In addition, we need to have storage available for all the information those firms send to us.”

Another relatively new trend combines the company’s interest in sustainability with its ethic of timely and effective customer service. “We have improved the speed and efficiency of our maintenance services while reducing fuel consumption by using mapping technology to plan the routes of our service technicians,” Henderson states.

Technicians have carried notebook computers with 3G connectivity for several years, but as their efficiency has improved, they now find even that technology to be cumbersome. “As a result, we are working on deploy-
“We’re playing a significant role in the effort to meet Seattle’s carbon emissions reduction targets for 2030.”

– Olwyn Palmer, Marketing Manager, MacDonald-Miller Facility Solutions

A need for availability and stability

All of these developments require an increasingly complex and robust underlying infrastructure. Henderson is responsible for about 450 desktops and laptops, plus the mobile phones carried by most employees. The company has deployed VMware Infrastructure in its data center, and at present, 12 of the company’s 35 servers are virtualized. “Since we strive to be a green business, we’re always looking for ways to minimize physical hardware and the power and cooling that it requires,” Henderson notes.

Since downtime is prohibitively expensive, MacMiller has developed a strategy for disaster recovery. It maintains backup copies of its VMware infrastructure and other critical systems at its metal fabrication facility, just over three miles from the headquarters office. “Although this strategy works well for us, one problem is the small pipe that connects our two sites,” Henderson states. “It’s a wireless bridge that shoots across the valley below our office. We have to do all of the data transfer after hours to avoid disrupting the business.”

Engaging the right service provider

This infrastructure has come a long way since Henderson arrived almost six years ago. After he was promoted from help desk technician to network
“We showed him how he could tackle the biggest part of his data volume problem by archiving, deduplicating, and compressing his messaging system.”

– Lauren Newman, Account Executive, SHI International Corp.

administrator, he was introduced to Symantec Platinum Partner SHI International Corporation. “I took a look at their company and realized that they could meet a lot of my needs,” Henderson recalls. “Their expertise in hardware and software helps me to select the right products, and if I need help with deployment or troubleshooting, I can access their professional services.

“But the main thing I liked about SHI was that they took the time to get to know our organization, our unique IT needs, where we plan to be in the future,” Henderson says. “This enables them to recommend technology that will serve our long-term strategies.”

Initially, SHI began managing the licensing for the company’s existing deployment of Symantec Backup Exec, as well as its Microsoft solutions. It also became MacMiller’s hardware provider, supporting the existing HP infrastructure and developing proposals for upcoming upgrades to the storage infrastructure. “The fact that SHI partners with HP and Symantec helped them to step into our environment and provide anything we need,” Henderson notes.

A data volume explosion
When MacMiller and SHI first formed a relationship last summer, Henderson’s biggest pain point was storage. “Architectural drawings are getting more complex and more memory-intensive every year, and we’re starting to get more of them because of IPD,” he says. “In addition, our engineering department is starting to create proof-of-concept videos to post on YouTube or share with customers. Microsoft Exchange is the default document management system for many of our employees, and the Exchange server contains a lot of duplicate files, as well as older files that are rarely accessed.”

And while MacMiller currently has about three terabytes in total data, it’s the growth projections that cause heartburn for Henderson. “Our data is growing at a compounded 2.83 percent per month, so our data store has actually doubled in less than two years. I needed a way of providing fast access to frequently-used data, while moving less frequently-used data off of key systems to preserve performance and stability.”
Maintaining core data protection
MacMiller had used Backup Exec for many years for data protection, and Henderson upgraded to Backup Exec 2010 soon after it was released. “I had just upgraded from Microsoft Exchange 2003 to Exchange 2010, skipping Exchange 2007,” he remembers. “I learned that Backup Exec 2010 was optimized for Exchange 2010, so I went through the upgrade.” Henderson purchased the Agents for Microsoft Exchange and VMware Virtual Infrastructures, enabling non-disruptive backups and granular recovery from those systems, and he plans to use the Deduplication Option as well. The problem is that he has never had the infrastructure available to back up to disk. “I won’t get the full value out of Backup Exec 2010 until we complete a hardware upgrade,” Henderson explains.

Toward a tiered-storage strategy
With MacMiller’s storage systems nearing capacity, Henderson approached the SHI team for ideas, and they introduced him to Symantec Enterprise Vault. “We showed him how he could tackle the biggest part of his data volume problem by archiving, deduplicating, and compressing his messaging system,” says Lauren Newman, account executive at SHI. “Once that is accomplished, we can turn on File System Archiving to take care of the rest of the unstructured data. And it all works seamlessly with their existing Backup Exec deployment.” Henderson purchased Enterprise Vault and has been testing it for a number of weeks. In the meantime, he is working with Newman to design a new storage infrastructure to include an Enterprise Vault server, a storage system that supports backup to disk, and enough capacity to support MacMiller’s data growth projections for a few years. “I’m excited at the prospect of moving less-used data to the archive server while keeping more crucial data...
on the Exchange and file servers, where they can be accessed instantly,” Henderson asserts. “Users will not notice a difference, as they'll still access their messages through Microsoft Outlook. And we'll dramatically reduce the amount of data on our Exchange server, which will help keep it stable and avoid the need for additional capacity.”

Once the hardware upgrade is complete, backups will become less of a problem as well. “Backing up to disk is faster than backing up to tape,” Henderson notes. “Combining deduplication with disk backup will dramatically reduce our backup window, which is good since we're barely completing backups within the overnight window today.”

Preparing for success
As final decisions are made on the hardware upgrades, Henderson is spending a lot of time reading manuals and documentation on Symantec Enterprise Vault. “I’m the type of person who likes to deploy technology myself when possible, so I’m reading up to prepare for this project,” he says. “But it’s a comfort to know that SHI is there if I get stuck or need assistance, as they know our environment and can make sure all the elements fit together.”

Henderson sees this project as nothing short of an investment in the future of MacMiller. “The current trajectory is unsustainable, but the new infrastructure will enable us to scale our business and continue to provide cutting-edge services.”

And a sustainable IT infrastructure at MacMiller will help enable a more sustainable future for the Pacific Northwest.

Mark L.S. Mullins is a managing editor of The Confident SMB and CIO Digest, and senior manager of Symantec’s Global Reference Program team.
Your data is the lifeblood of your business. Your customers trust you to keep their information secure. But what if it falls into the wrong hands? Laptops containing customer records sometimes get lost. Backup tapes disappear out of the backs of trucks. And while it may seem as if data breaches only happen to large enterprises or government entities, that’s a common misconception easily explained by the fact that high-profile organizations are the most likely to receive news coverage.

If you think data breaches are not a small business problem, think again. Risk consulting firm Kroll Associates, Inc. has released its forecast for data security trends in 2011, and “more small-scale breaches” tops the list at number one.¹ “We will most likely see an increase in reported, smaller-scale breaches,” the report reads. “This is not to say that the era of the massive [corporate] breach is over, but they may be matched by small-breach frequency.”

By Ken Downie
Although the aftermath of a data breach is always costly and damaging to a company’s reputation, large enterprises usually have enough resources to pick up the pieces and move on. Small and medium-sized businesses (SMBs), however, can be devastated and put out of business by a single breach. To mitigate this risk, more and more SMBs are using encryption, a process that uses an algorithm called a cipher to make information unreadable. Data is encrypted using a public key, making it unreadable to anyone except those possessing the public key and a corresponding private key.

The good news is that encryption can be faster and easier to put in place than many SMBs expect.

What’s driving encryption?
The drivers for encryption are multiplying, and so is its use. According to the Symantec 2010 Global SMB Information Protection Survey, 75 percent of small business owners are concerned about the possibility of a data breach. They
We use whole disk encryption to ensure that if a laptop or workstation is lost or stolen, the only damage would be the cost of the computer.”

– Kurt Smith, Systems Security Officer, HealthDataInsights

But it’s not just value creation and potential reputation damage driving SMBs to encrypt sensitive data. Governments are also getting into the act. In the United States, regulations such as the Health Information Technology for Economic and Clinical Health Act (HITECH) and the Payment Card Industry (PCI) Data Security Standard (DSS), as well as breach notification laws in at least 46 states, are forcing the issue in certain industries and locations (see sidebar: Encryption and Data Breach Laws in the U.S.).

Under HITECH, if any healthcare provider, even a small medical clinic, improperly discloses protected health information (PHI), the provider must notify the affected patients within 60 days of discovering the breach. If the breach involves 500 patient records or more, the healthcare provider must also notify the U.S. Department of Health and Human Services (DHHS) and the local media—not exactly a low-profile scenario. Even if a business is not a healthcare provider, it may have to comply with the U.S. Federal Trade Commission’s Health Breach Notification Rule if it handles healthcare information on behalf of a customer. But if sensitive data is exposed to unauthorized access and it’s encrypted, regulations don’t consider the incident a data breach, because it’s impossible to access the data without a private key.

SMBs may also be compelled to use encryption by their customers. As more and
### Encryption and Data Breach Laws in the U.S.*

Most states now have data breach laws, and expanded federal legislation is expected sooner rather than later now that HITECH has opened the door. While much of the current legislation is couched in terms such as “if reasonable and appropriate,” expect laws with more teeth shortly.

<table>
<thead>
<tr>
<th>Law</th>
<th>Who’s affected?</th>
<th>The upshot</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) – 2009</td>
<td>Companies that deal with protected health information (PHI)</td>
<td>HIPAA-covered entities must (if reasonable and appropriate) encrypt electronic PHI. Applies to data at rest and in transit. Breach notification requirements apply and are more severe for data breaches involving 500 or more records.</td>
</tr>
<tr>
<td>Gramm-Leach-Bliley Act (GLBA), Interagency Guidelines for Establishing Standards for Safeguarding Customer Information and FFIEC Information Security Booklet (2006)</td>
<td>Financial services companies</td>
<td>Financial institutions must adopt security measures, if appropriate, that include encryption of electronic customer information, including while in transit or in storage, on networks or systems to which unauthorized individuals may have access. Effective key management practices and endpoint encryption are also addressed.</td>
</tr>
<tr>
<td>Massachusetts General Legislature ch. 93H and 201 CMR 17.02-04</td>
<td>Every person that owns or licenses personal information about a resident of the Commonwealth and electronically stores or transmits such information</td>
<td>Mandates encryption of all transmitted records and files containing personal information that travel across public networks or are transmitted wirelessly; also mandates encryption of all personal information stored on laptops or other portable devices. Includes breach notification provisions.</td>
</tr>
</tbody>
</table>

*Continued on next page*
more organizations encrypt their data, they expect the companies they do business with to follow suit. Indeed, if your customers are encrypting, and you’re working with their data, then you’ll soon be encrypting and decrypting to comply with their security requirements.

At HealthDataInsights, a Las Vegas-based company that verifies the integrity of healthcare claims, encryption of protected health information is required by its customers—the Centers for Medicare and Medicaid Services, insurance companies, and government agencies such as the U.S. Department of Defense. “Even though we’re a small business and not a government agency, we still need to follow the Security Technical Implementation Guides set by the Defense Information Systems Agency,” explains the organization’s Systems Security Officer Kurt Smith. “Because we take in PHI, our government and commercial customers require and expect us to safeguard that data from unauthorized access.”

**What should you encrypt? And how?** Compliance concerns often dictate what data organizations choose to encrypt first. While no federal breach notification law currently exists in the U.S., states such as Nevada and Massachusetts have introduced their own laws that go a step

---

### Encryption and Data Breach Laws in the U.S.*

<table>
<thead>
<tr>
<th>Law</th>
<th>Who’s affected</th>
<th>The upshot</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nevada Revised Statutes (2010)</td>
<td>Any governmental agency, institution of higher education, corporation, financial institution, retail operator, or any other type of business entity or association that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with nonpublic personal information</td>
<td>Requires the use of encryption methods “adopted by an established standards-setting body” for all non-voice, non-fax electronic transmission of personal information. Includes breach notification provisions.</td>
</tr>
<tr>
<td>Nevada S.B. 227, 75th Legislature (2009)</td>
<td>Business accepting payment cards for goods or services in Nevada</td>
<td>Requires merchants to comply with the Payment Card Industry (PCI) Data Security Standard, which requires the encryption of cardholder data.</td>
</tr>
</tbody>
</table>

---

* Excerpted from *Summary of Selected Encryption Laws*, Stephen S. Wu, January 14, 2010
further and actually mandate encryption of certain types of data.

Doing business in Nevada? Encrypt email

In 2010, Nevada amended its existing legislation to require all entities doing business in the state to use encryption methods “adopted by an established standards-setting body” for all non-voice, non-fax electronic transmission of personal information—and that means email. Lyle Epstein, president of Kortek Solutions, a Symantec partner serving SMBs in the Las Vegas area, wanted to make sure his customers would be ready. “A lot of our clients were not aware of the new law, so we let them know we were able to provide a solution for them,” he says.

One of Kortek’s customers is Legal Aid Center of Southern Nevada, a full-service law firm that has provided free legal aid to Clark County’s low-income residents since 1958. Because the organization frequently sends emails containing sensitive personal information, it wanted to encrypt those emails to comply with the new Nevada statutes. “One of our requirements was that we didn’t want the emails sent to a third party for encryption,” says Terry Bratton, legal administrator. “We wanted to retain the messages at all times.”

Kortek recommended implementing PGP Universal Gateway Email running on PGP Universal Server from Symantec to provide centrally managed, standards-based encryption without sending the emails off site. “PGP Universal Gateway Email is very well suited to the SMB market,” explains Epstein. “When we looked at other competitive products, not only were they more geared toward the enterprise, but they weren’t priced within reach of the small and medium business community. It’s also very easy to deploy.”

Now, when users send an email containing personal information about a client, they can either click a toolbar button or type the word “confidential”
into the subject line, instructing PGP to encrypt the entire message, including any attachments. By encrypting data at the gateway, PGP Universal Gateway Email ensures data is protected from unauthorized access in transit and at rest on a recipient’s mail server. Email is delivered encrypted regardless of the recipient’s use of encryption, and recipients do not need to install any software to read encrypted messages.

“PGP has been working very well,” says Bratton. “The rollout was very easy, and our staff adapted to it quickly. It provided us with a very quick answer in response to Nevada’s amended encryption law.”

Handling protected health information? Encrypt whole disks and file shares
HealthDataInsights must encrypt more than just email to comply with its customers’ requirements. The company uses PGP Whole Disk Encryption and PGP NetShare, along with PGP Universal Server, to encrypt whole disks, backups, and data streams, as well as loose files and folders.

“We use whole disk encryption to ensure that if a laptop or workstation is lost or stolen, the only damage would be the cost of the computer, because none of the data on the hard drive is readable,” says Smith. “We have policies stating that people aren’t supposed to have any kind of sensitive data on their personal computer, but we didn’t want to take people’s word for it, because people make mistakes. Almost all of our customers use PGP and are happy with it, so it was the logical choice for us. PGP is even ahead of governmental requirements.”

For network file and folder encryption, PGP NetShare enables HealthDataInsights to create files that can be stored anywhere on the network, backed up, and moved as needed, but unlocked only by team members who have the proper keys. “PGP NetShare is one of the coolest features, especially when it comes to documents and contracts,” Smith explains. “Simply applying folder- and share-level security is inadequate, because high-level administrators still have physical access to all the data. With PGP NetShare, administrators are able to restore files or move them around, but they do not have access to read.
the data unless they’re part of the right security group.”

Will encryption be disruptive?
While having the right encryption tools in place is important, having the right key management tool is absolutely essential. Keys and encryption policies need to be managed centrally, notes IDC’s Domage. “Organizations using encryption need a centralized repository for key management.”

― Eric Domage, Western Europe Program Manager, Security Products and Solutions, IDC

encryption need a centralized repository for key management, whether the encryption technology is coming from vendor A, B, or C,” he says. “Businesses don’t want to be in a position where they lose an employee, lose a key, and therefore lose access to critical data.”

PGP Universal Gateway Email offers central management of encryption keys, helping Legal Aid Center of Southern Nevada minimize user confusion and disruption. “It’s actually very easy to use,” says Bratton. “One of the other things that we like about not going through a third-party provider is that we’re able to monitor the keys ourselves and report on exactly what the user access has been.” Currently, penalties for noncompliance with the Nevada law are unclear, but “we want to make sure that managing it centrally,” says IDC’s Domage. “Without a centralized policy, encryption can turn into chaos, and companies have no way of enforcing its use.”

“Organizations using encryption need a centralized repository for key management.”
HealthDataInsights runs PGP Universal Server in Guarded Key Mode, which stores a passphrase-protected copy of end users’ private keys on the PGP Universal Server. “Users don’t have to worry about backing up their keys, because Universal Server has taken care of that for them,” says Smith. “And if someone’s system dies, their keys are available on their rebuilt computer. As for public keys sent to us by our customers, we store them in our password database, but we don’t really worry about it too much.”

Smith continues: “One of the advantages of using the same encryption technology as our customers is that PGP Universal Server automatically takes every user’s public key and places it up on PGP’s Web-accessible directory. So when we need to transfer that data, we don’t need to have to send the customer our public key—they can just find it on the Internet, which makes it very straightforward. I can’t think of a better way to manage encryption keys.

**Where’s the ROI?**

Encryption can pay for itself very quickly by mitigating the risk of data breaches and demonstrating to customers and regulators that data is protected. In more and more cases, SMBs must encrypt to mitigate risks that could put them out of business.

Says HealthDataInsights’ Smith: “PGP paid for itself within the first month of deployment. We were able to use it as a sales tool and put our customers at ease. We’ve used other encryption technologies in the past, but PGP has been the simplest and most effective solution. It’s an integral part of how we safeguard our data.”

---


*Ken Downie is a Senior Writer at NAVAJO Company. His work has appeared in Business Finance, Business Credit, and CIO Digest magazines.*
IT Health Check

Protecting Patient Data in Compliance with Regulations

Unlike large medical centers, the first things I notice when I walk into my neighborhood physician's office are the many pictures of patients on the wall and the familiar faces of the office staff who know you by name. The clinic's personalized approach is also focused on one thing—the well-being and care of its patients.

But the business of improving the quality of care and saving lives is not so simple. Healthcare is one of the most complex and highly regulated industries, mainly because of the Health Insurance Portability and Accountability Act (HIPAA). In addition, the Health Information Technology for Economic and Clinical Health (HITECH) act was introduced in 2010 to provide financial support for the adoption of electronic medical record systems. Electronic records enable healthcare providers to quickly access patient data, but it also places increased responsibility on these providers to protect patient records from security breaches. In its recent “Benchmark Study on Patient Privacy and Data Security,” Ponemon Research found that data breaches cost healthcare providers $6 billion annually.¹

By Courtenay Troxel
With healthcare reform a top priority, small and midsize business (SMB) healthcare providers are faced with going from having just enough computers for the finance department to everyone having access to systems and data. This article details how SMB healthcare providers are tackling the changing IT landscape and complying with regulations.

Marc Holland, vice president of market research, HIMSS Analytics, explains: “This dynamic regulatory environment can be very challenging for many SMB healthcare providers. But the changes in healthcare regulations also represent opportunities to get funding for IT projects and, most importantly, to improve patient care.”

It’s all about the data
Providing quality care for patients comes down to data—collecting it, sharing it, and accessing it. From a technology standpoint, it means having the ability to store, protect, and manage the availability of patient information securely,

SMB healthcare providers are tackling the changing IT landscape and complying with regulations.

Marc Holland, vice president of market research, HIMSS Analytics, explains: “This dynamic regulatory environment can be very challenging for many SMB healthcare providers. But the changes in healthcare regulations also represent opportunities to get funding for IT projects and, most importantly, to improve patient care.”

It’s all about the data
Providing quality care for patients comes down to data—collecting it, sharing it, and accessing it. From a technology standpoint, it means having the ability to store, protect, and manage the availability of patient information securely,

Threat Report, Volume XV, healthcare ranked as number two targeted industry for attacks, with 60 percent of data breaches unintentional.2

“Electronic files, if properly managed, can be inherently more secure than paper records,” notes Holland. “Security should be a top priority not only for IT but for all employees.”

According to Holland, the following are key factors that an SMB healthcare organization needs to consider to enable an effective security policy:

> User training, including awareness of relevant state and federal legislative provisions and associated civil and criminal penalties and ongoing refresher training
> Effective password management
> Role-based security
> Encryption of data
> Annual penetration testing

Educating the staff
Washington County Hospital (WCH), a critical access hospital in North Carolina,
Healthcare Feature

Confident The

Contents

Cover Story Case Study

Encryption Feature

SMB

The SMB

Healthcare Feature

WCH materials management director and IT director Christina Craft is in charge of purchasing and maintaining everything from band-aids to equipment needed for the facility. Craft is also a one-person IT shop. Although WCH still has a paper trail, its accounts receivable, payroll, radiology images, and some patient data are now being processed electronically.

“Our biggest challenge is getting all our medical records online, a process that is incredibly complicated,” says Craft. “I have to find the funding, time, and energy to make everything digital, train our staff, and meet HIPAA requirements, all while making sure our patients healthcare needs come first.”

Craft’s top priority is to deliver high quality patient care through improved staff productivity and efficiency. “Moving patient records from a paper and physical filing system to computers will enable our providers to quickly access and share up-to-date patient information to facilitate more accurate diagnoses, which in an emergency can be life-saving,” Craft notes. “While the benefits of electronic health records promote improved quality of care, I also need to consider the importance of protecting patient data.”

Recently reported in Health Data Management, a clinical facility in Indianapolis learned that its employees unintentionally revealed their email login information to third parties, according to the notice. As a result, the third party was able to access certain email accounts within the facility that contained protected health informa-

“I consider Symantec a trusted vendor because they understand that our needs in the SMB healthcare space are the same as larger enterprises.”

– Steven Porter, Chief Information Officer, Touchstone Behavioral Health

Steven Porter, Chief Information Officer, Touchstone Behavioral Health

pvides itself on offering the latest in technological advancements in healthcare. The 49-bed, critical care facility has been providing healthcare services to Washington County and its surrounding communities for over 60 years.
According to Craft, everyone from doctors and nurses to technicians need to think about security and privacy in a different way and must be trained on processes such as how to deal with spam email that may contain malicious viruses or phishing attacks. “We have different levels of security,” Craft explains. “Our staff has access to information depending on their job title and what their function is when it comes to patient data.”

Security and data protection keeps things operating smoothly
To secure and protect its network of 98 workstations and 158 users running Microsoft Exchange Server, WCH relies on Symantec Partner The SoundSide Group and security and data protection solutions from Symantec.

With Symantec Endpoint Protection, The SoundSide Group is able to monitor the network, view each individual machine for potential threats, and prevent attacks to keep WCH operating effectively. “People often surf the Internet and click on things they shouldn’t, which can contribute to data breaches,” notes Jeb Gardner, support specialist, The SoundSide Group. “Symantec Endpoint Protection is the primary software we depend on to keep our clients up and running, and we’ve never had an outage with any system running Symantec Endpoint Protection.”

To safeguard systems in the event of data center failure, The SoundSide Group also uses Symantec Backup Exec System Recovery to protect WCH’s critical data and to restore mailboxes and emails on their Microsoft Exchange server.

“PGP... helped to define encryption standards that are ahead of even government requirements.”
– Kurt Smith, Systems Security Officer, HealthDataInsights
Server. “We use Backup Exec System Recovery as a business continuity tool, which helps me sleep at night,” Gardner states. “While Backup Exec System Recovery restores files quickly, we have never had to use this feature.”

**Going paperless securely**
The move to electronic medical records (EMR) gives SMB healthcare providers access to critical patient data at a moment’s notice; keeping that information secure is the challenge.

For Phoenix, Arizona-based Touchstone Behavioral Health, an EMR system gave them the ability to deliver improved patient care and better support to the therapists and counselors who provide outpatient, home treatment, and pre-

**Start With a Risk Analysis**

“T**he increased focus on protecting patient data and new industry regulations mandating frequent certifications and time-consuming audits, along with limited resources to develop and implement a security strategy, SMB healthcare providers are faced with IT environments that are becoming more complex,” says Marc Holland, vice president of Market Research, HIMSS Analytics.

According to Holland, healthcare providers should start with a risk analysis, also required by HITECH. Every organization is going to be different, including the risks. A risk assessment allows healthcare providers to understand their environment—what they’ve got today and how they want to use data going forward—then look at where the risks and vulnerabilities are, prioritize the issues identified, and fill in the gaps to make sure it’s protected and secure.

**Components of a Formal Risk Analysis**

- Internal Threats
- External Threats
- Compliance Requirements
- Risk to Confidentiality of Patient Data
- Effectiveness of Security Controls
- Evaluation of Policies and Procedures
- Risks to Integrity of Patient Data
- Risks to Availability of Patient Data
- New Opportunities to Improve Security

Source: 2010 HIMSS Security Survey, November 3, 2010
ventative services to children and their families. The EMR system also enables real-time access to the latest updates on patient records, allowing therapists to provide a more personalized and meaningful session for their clients—from anywhere.

To ensure the security of its data, network, and staff in the field, Touchstone Behavioral Health leveraged Symantec Endpoint Protection. “With end users, my biggest security threat, the EMR process involved training our mobile staff on computers and reminding them that security is really their job,” says Steven Porter, chief information officer, Touchstone Behavioral Health. “The nature of the work and the dedication of the staff mean they’re out at the fringes of the Internet looking for solutions to solve very serious and specific behavior issues, and the research sometimes leads them in areas you may not normally think of going.”

**Time saved avoids fines, improves billing cycle**

Touchstone Behavioral Health relies on Symantec solutions to help reduce the audit report times, avoid potential fines, and meet the security audit requirements set by HIPAA.

Symantec’s Endpoint Protection console provides a snapshot of Touchstone Behavioral Health’s endpoint security status—a dashboard of when machines last checked in, their A/V signature dates, potential risks, and current threats. The weekly update allows Touchstone Behavioral Health to drill down to specific events or hardware to analyze the root cause and remediation, without digging through multiple log files or screens, and is sufficient for most audits.

“The reality is HIPAA security compliance isn’t about the actual machines, it’s the report you give to the auditor,” Porter explains. “We’ve been able to reduce audit preparation time to a few minutes and more importantly, reduce the HIPAA report creation from 10 hours down to 30 minutes with Symantec Endpoint Protection.”

With Symantec security solutions enabling the EMR platform, Touchstone Behavioral Health has also reduced its billing time 17-fold through the electronic collection of updated medical records and signatures required upon completion of the visit. “We’ve gone from a billing cycle of 53 days down to three,” Porter notes.

**Safeguarding data beyond endpoints saves money**

Keeping protected health records secure as mandated by HIPAA goes beyond endpoints. Touchstone Behavioral Health safeguards its data with Symantec Backup Exec in the event of...
disaster or data center failure, citing a 97 percent success rate for backups and a 100 percent success rate for restores. “Symantec Backup Exec is a key component to my disaster recovery and business continuity plan.” Porter says.

As the IT environment evolved to virtualized servers and disk-based backups, Touchstone Behavioral Health upgraded its backup strategy with Symantec Backup Exec 2010. The integrated deduplication capabilities in Backup Exec 2010 significantly reduced redundant data that can occur with virtualized environments.

“Deduplicating our data with Backup Exec 2010 has increased our backup speed dramatically,” Porter says. “We’ve gone from a 14-hour backup window to under 3 hours—allowing us to avoid network latency issues during production hours.”

In addition, its ability to provide single-instance storage of its virtualized server data enables Touchstone Behavioral Health to save time, lower storage costs, and minimize backups.

“I consider Symantec a trusted vendor because they understand that our needs in the SMB healthcare space are the same as larger enterprises,” Porter concludes. “And they continue to provide us with the same enterprise-class solutions, which ultimately helps us deliver higher quality care to our patients.”

Encryption: the missing link
One of the requirements of HITECH is data breach notification, which means if a healthcare provider improperly discloses protected health information, the healthcare provider must notify the affected patients within 60 days of discovering the breach. In addition, if the breach is large enough—over 500 patients—the healthcare provider must also notify the U.S. Department of Health and Human Services (DHHS) and the local media. For breaches involving 500 or more individuals, the DHHS is also obligated to post a notice on a publicly accessible website.

According to the DHHS, two-thirds of all data breaches reported since this rule went into effect in August 2009 have resulted from the loss or theft of computers or backup media containing protected health information. This is where encryption is key. Encryption technology uses a cipher to make information unreadable to anyone except those possessing a key, ensuring that lost or stolen protected health information is not misused. What’s more, under HITECH, the data breach notification provisions are not required if the lost data is encrypted.

According to Holland, the frequency of data loss, the cost of corrective action, stricter regulations, and increased worker mobility are just a few reasons why encryption should be mandatory, not to mention the long-term effects of lost business and tarnished reputation. “Healthcare providers should make sure the data is encrypted not only where it originated, but in each instance where it is transmitted to other authorized users.”
of the data,” he says. “If encrypted data is obtained by an unauthorized party, it can’t be read or used.”

**Encryption drives data integrity**

For HealthDataInsights (HDI), a Las Vegas-based business that verifies the integrity of healthcare claims, encryption is required by its high-profile customers—the Centers for Medicare and Medicaid Services, insurance companies, and government agencies such as the U.S. Department of Defense.

To ensure HDI has rock-solid data protection, HDI uses PGP encryption technology from Symantec. “Since we handle medical claims, everything we do has to protect patient data,” says Kurt Smith, systems security officer, HDI. “We have 300 employees working remotely, and if someone’s laptop gets stolen or lost, the damage to HDI would only be the cost of the computer, because the data can’t be accessed.”

For its encryption requirements, HDI uses PGP Whole Disk Encryption, PGP NetShare, and PGP Universal Server running in Guarded Key Mode for backups, data streams, and files.

“PGP NetShare is one of the coolest features, especially when it comes to corporate documents and contracts,” Smith explains. “With PGP in place, administrators are able to restore files or whatever is required, but do not have access to the data unless the administrator is part of the security group that allows them to view it.”

**The keys to unlocking the code**

Smith explains the function of encryption keys using the example of the 1983 movie *WarGames*, where one officer has the unlocking code to “turn the key” upon order, and another officer has the key code to validate the order to engage in thermonuclear war. Very simply, encryption requires two keys: a primary key to encrypt information and verify signatures and a private key used to sign and decrypt information. “PGP not only created an encryption product that is second to none, but also helped to define encryption standards that are ahead of even government requirements,” Smith notes.

A major benefit of PGP encryption technology is the ability to segregate protected health information.
on a client-by-client basis. Data is segregated and encrypted under different groups, and privileges controlled based on client data. “PGP paid for itself within the first month of deployment, and it’s a great sales tool, because we can put our customers at ease,” Smith says. Holland notes, “Only encryption protects the data itself no matter where it is used, stored, or transferred.”

With the new regulations and enhanced data policies, healthcare providers are able to improve staff productivity and efficiency, and are able to access and share updated real-time patient medical records from anywhere. Ultimately, it’s the patients that benefit from the overall improved quality of care.

What if a laptop is lost?

PUT SECURITY FIRST.

Learn about Endpoint Encryption

Courtenay Troxel is managing editor for The Confident SMB and CIO Digest and manager of online content and newsletters at Symantec.
EVENTS

RSA Conference
San Francisco, California
February 14 – February 18, 2011

Parallels Summit 2011
Orlando, Florida
February 22-24, 2011

35th Annual Minority Business Opportunity Day
Los Angeles, California
February 24, 2011

6th Annual Small Business Summit 2011
New York, New York & Online
March 8, 2011

Growco 2011, an Inc. event
Las Vegas, Nevada
April 6–8, 2011

Virtual Small Business Tax Online Workshop

Symantec Vision 2011
Las Vegas, Nevada
May 2–5, 2011

RESOURCES

Visit us online at Small Business Solutions and Midsize Business Solutions and take advantage of a world of resources to help you have confidence in your connected world.

Find a Reseller
Find the perfect partner to help you manage your IT needs

Trialware Downloads
Trial version of Symantec products are available for download

Symantec eLibrary: A Subscription for Success
One-year subscription gives you access to hundreds of Symantec training modules

Chat with a Sales Specialist Now
Security made simple. Chat directly with a specialist now

License Renewal Center
Get continued protection for your product today

Customer Success
See how other SMBs succeed with the help of Symantec

Hosted Services
Secure and manage your information using the power of cloud computing

Education Services
Maximize your IT investment with a skilled, educated workforce

Symantec Connect
A technical community to help your IT team keep your systems up and running

SOCIAL MEDIA

The Confident SMB Blog
Get insights and highlights of new content, and interact with The Confident SMB team.

Symantec Facebook Page
Readers with Facebook accounts can connect and share ideas with Symantec while also receiving notification of each new issue. Become a fan today.

Twitter
Tweeting on everything from the new The Confident SMB articles, research reports, podcasts, webcasts, customer successes, and more, the Symantec Publishing Twitter account keeps Symantec customers and partners up to date. Start following the tweets today.

LinkedIn
Exchange tips and strategies with peers by joining The Confident SMB group on LinkedIn.com.
Is social networking attracting new threats to your business?

PUT SECURITY FIRST.

Social networks expose you to even more threats of data loss. Our endpoint protection blocks noncompliant devices from accessing corporate networks and resources. So your social network won’t include cybercriminals.

Copyright © 2010 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.