Symantec Comprehensive Cloud Security 1

Taking a Comprehensive Approach to Cloud Security

You can better protect your data, reduce costs, and make your security infrastructure more flexible and easier to manage

Inc.

Confidence in a connected world. Symantec™

Introduction: The Benefits of Re-Thinking Security

News reports about costly and reputation-scarring data breaches are becoming almost commonplace. The *SMB Threat Awareness Poll,* conducted in late 2011, indicated that small businesses are well aware of hackers, spam, and other cyber risks that can lead to data loss. And small businesses understand the consequences of a data breach. Forty-six percent of the 1,900 small businesses surveyed said a targeted attack would cause a revenue loss, and 20 percent said it would drive customers away.

On the other hand, many small businesses don't appreciate their own risk for these incidents. Half did not think they would be targeted for cyber attacks simply because they were small businesses. In reality, though, the opposite is true—during the past two years, 40 percent of cyber attacks have been directed at small businesses. That's much larger than the number of attacks that large enterprises experienced during that span. In fact, the number of hacker attacks on small businesses doubled in the first half of 2012, according to Symantec's mid-year Intelligence Report.

> *During the past two years, 40 percent of cyber attacks have been directed at small businesses. That's much larger than the number of attacks that large enterprises experienced during that span. In fact, the number of hacker attacks on small businesses doubled in the first half of 2012.*

Mayank Sharma, network systems engineer/project manager for Child Advocates, a Court Appointed Special Advocates (CASA) program that helps abused, neglected, and abandoned children in the Child Protective Services (CPS) system in Houston, is under no misconceptions about the need for data security, though.

Every business needs to consider security

"A small business doesn't have less of a need for security than a Fortune 500 company," he says. "We have a lot of sensitive and proprietary information, such as case information related to child abuse as well as donor information. Our biggest nightmare would be to get on the 6 o'clock news about how donor information or people's social security numbers were lost."

In an environment of heightened cyber threats, you might need to rethink your security practices and look for ways to improve the integrity of information without diminishing the effectiveness of your employees. According to *Convergence Evolution,* a March 2012 study by KPMG, companies should take a comprehensive approach to securityÐone that ensures that all aspects of the business receive the same attention without any duplication.

> *In an environment of heightened cyber threats, you might need to rethink your security practices and look for ways to improve the integrity of information without diminishing the effectiveness of your employees.*

Many small businesses are turning to cloud computing to enable such a comprehensive approach to security. "There are a lot of innovative services in the cloud with email security, endpoint security, as well as backup and recovery, that can fortify small businesses against the many cyber threats they face today," says Andrew Singer, director, product marketing at Symantec.

This paper will explore how small businesses can implement a comprehensive approach to security, as well as explain the cloud security approaches how those small businesses to better protect their data, reduce costs, and make their security infrastructure more flexible and easier to manage.

Step 1: Assessing Your Risk

Businesspeople use the phrase, “You can’t manage what you can’t measure.” In security, the phrase might be, “You can’t protect data unless you know where it is.” A single data breach can mean financial ruin for your business. It’s important to understand where your risks and security gaps are so that you can take steps to protect your information.

To implement a comprehensive security strategy, you should first identify and classify confidential information. This means knowing where sensitive information resides, who has access to it, and how it is entering or leaving the organization.

For example, most small businesses only focus on protecting their servers. While this is critical, 60 percent of data resides on PCs and laptops, according to the University of North Carolina’s Information Technology Service.

First define what business data is critical by asking these three questions:

- Would losing this data significantly affect revenues and profits?
- Would the small business owner want to be informed if this data was lost?
- Would the small business owner take action if he were told this data was lost?

For example, information like customers’ credit card numbers and source codes are obvious examples of critical information. But only by going through a methodical exercise can you identify all the sensitive data whose loss could bring significant financial and regulatory consequences and also damage your reputation.

To implement a comprehensive security strategy, you should first identify and classify confidential information. This means knowing where sensitive information resides, who has access to it, and how it is entering or leaving the organization.

After you have identified the critical data, determine where it is kept in the company:

- What data is stored on PCs, laptops, tablets, or smart phones?
- What kind of data is being taken outside the corporation on mobile devices?
- What information is being shared with, and stored by, vendors, contractors, or others outside the organization?
- What kind of data do employees put on portable storage devices, such as CDs and USB flash drives?
- What business data is being shared in emails and attachments?

This step-by-step exercise can provide the clarity that is necessary to develop a comprehensive security strategy.

In assessing your data security strategy, you also need to consider laws and regulations specific to your industry, such as the Health Insurance and Portability Act (HIPAA, **www.dol.gov/ebsa/newsroom/fshipaa.html**) and the Payment Card Industry Data Security Standard (PCI DSS, **www.pcisecuritystandards.org/security_standards**), which applies to an array of businesses that handle credit and debit card transactions.

Step 2: Minimizing Your Risk

A multi-layered protection strategy should provide your business with proactive protection for laptops, desktops, servers, mobile devices, and messaging and Web environments.

Cloud services provide an efficient and cost-effective way to perform the ongoing monitoring and management that a comprehensive security strategy demands. With cloud computing—which is sometimes referred to as Software as a Service (SaaS) or Storage as a Service—a small business is relieved of the burden of purchasing, maintaining, or managing its own technology infrastructure, hardware, and management software. Instead, these resources are provided on an as-needed basis by the cloud provider. Because this is what the cloud provider does full-time, it can offer economies of scale, and keep up with the latest technology advances and safety mechanisms.

A multi-layered protection strategy should provide your business with proactive protection for laptops, desktops, servers, mobile devices, and messaging and Web environments.

This is important, because cyber criminals are constantly looking for new ways to exploit networks. "One of the reasons that small businesses like the cloud is that it allows them to stay ahead of the threat," Singer says. "Security software in the cloud is usually updated faster than they can do themselves with an in-house system."

Malware and spam, in particular, pose enormous risks to a small business. Malware can be introduced into an environment via two primary routes: the endpoints (laptops, desktops, servers) or from the Internet via Web and email traffic. Securing both of these points of entry is critical, but in the past, the task was daunting and time-consuming. The next sections examine some of the ways these threats can be mitigated through cloud services.

Risk mitigation A: Begin with the end(points)

A comprehensive strategy should minimize the risk of exploited endpoints, making use of anti-virus, firewall, and host-intrusion protection technology. "A lot of small businesses treat their business like they treat their home computer, not updating or giving it sufficient attention," says Mike Dickersbach, vice president of information technology for Thayer Lodging Group.

Indeed, sometimes a small business will use consumer-grade, free, or anti-virus-only solutions, not realizing that those approaches don't provide all the safeguards that business-critical data requires. A small business might not appreciate, for example, that the lack of intrusion protection puts them at significant exposure to data loss. Anti-virus-only solutions don't protect businesses against hackers breaking in and stealing financial, customer, or employee information. And, as noted before, these types of attacks on small businesses are on the rise. This is partly because cyber criminals hope to exploit security weaknesses at small businesses to find information about larger enterprise business partners that the small businesses might possess. That's just one reason why a small business needs just as much protection as a larger enterprise.

Anti-virus-only solutions don't protect businesses against hackers breaking in and stealing financial, customer, or employee information. And, as noted before, these types of attacks on small businesses are on the rise.

Among the best practices for protecting endpoints:

- **Be methodical about updates.** Less than half of companies kept their endpoint devices current with operating system and application updates across their virtual and physical servers and devices.
- **Use virus and spyware protection.** Only 20 percent of companies' physical endpoints—including desktops, laptops, and mobile devices—do so.
- **Implement the latest security technology.** Only half of small businesses considered technologies such as encryption, access control, data loss prevention, and reputation-based security as somewhat or extremely necessary.

A cloud-based solution can ensure endpoints have all these safeguards, are regularly scanned for active infections, and have up-to-date security levels.

Improving software management

Dickersbach provides a telling example of the benefits of using the cloud for security. As of late 2010, his firm still hosted its endpoint security in-house. Unfortunately, the software was neither centrally managed nor effective. "We ended up with a lot of workstations with malware, because it never got detected," he recalls. "We spent considerable time fixing them."

He sought a product that would not only secure the endpoints, but also help Thayer Lodging comply with centralized reporting, event logging, and other Payment Card Industry (PCI) rules.

He estimates the cloud solution has reduced the amount of time spent managing security by at least half, while improving coverage—especially for Thayer Lodging's executive management team, who spend substantial time on the road visiting the various properties. Because endpoint protection is now cloud-based, it follows them wherever they travel.

"It was perfect," he says. "We wanted something that was easy to deploy, manageable from any Internet connection, and accessible on our schedule."

With the cloud solution "if any machine gets a virus on it, the virus is locked up, and I get an extra report on the machine, detailing what virus was blocking, and where the attack came from, so I can be proactive."

Uniting anti-virus systems

Josh Cook, IT director for the Cardiac and Vascular Institute of Gainesville, Florida, switched to the cloud for backup and anti-virus protection on the medical practice's endpoints. Before the change, the organization had three different anti-virus systems, which made management difficult.

"I needed a good, centralized solution," he says. With the cloud solution "if any machine gets a virus on it, the virus is locked up, and I get an extra report on the machine, detailing what virus was blocking, and where the attack came from, so I can be proactive."

A key benefit was that the cloud technology provided an easy way to safeguard the network from the large number of medical transcriptionists who VPN in. “A lot of them didn’t have anti-virus on their personal machine, or they had out-of-date anti-virus, which was a big concern,” Cook says. “I don’t like the idea of someone accessing our system with their home computer that their whole family is using.” If a transcriptionist stops working with the practice, Cook can go to the management console and uninstall the anti-virus rather than having to go to his or her home.

Another important aspect of cloud technology is that using a cloud provider ensures the endpoints will be protected with business- or commercial-grade technology. Even if contractors, partners, or employees are protecting their personal devices with anti-virus, they may only be using consumer-grade solutions. However, a consumer solution only manages one machine and provides no centralized view of what’s happening across the user base. A commercial solution, in contrast, provides management tools that give a small business crucial visibility into its entire network.

> *However, a consumer solution only manages one machine and provides no centralized view of what’s happening across the user base. A commercial solution, in contrast, provides management tools that give a small business crucial visibility into its entire network.*

Risk mitigation B: Evaluating your email

A cloud-based solution can help combat malware and spam threats at the Internet level, before they reach your network. It can also help to control sensitive information (including email, select attachments, and images) by preventing it from leaving the network or entering your environment. “With email security, the solution can inspect the email traffic in the cloud before it reaches your company,” Singer adds.

At the Thayer Lodging Group, Dickersbach relies on virtualization and the cloud to run his very efficient operation. His first experience with spam filtering was in 2003, when half of Thayer’s incoming email was spam; that number quickly dropped to zero.

There are two variations of cloud-based email protection:

- **Hosted email security** features help to defend organizations from email-borne malware and unsolicited messages, and it delivers clean, approved content and promotes secure and productive email use. The result is a multi-layered defense against known, new, and targeted email-based threats and spam messages.
- **Email policy management** capabilities help identify and manage oversized, confidential, malicious, or inappropriate email content and images sent or received by an organization. This helps to reduce the risk of data loss and reinforces a company’s email Acceptable Use Policy, so that employee email use can be more productive and safe. Email messages and attachments can be scanned for keywords, phrases, URL lists, or alphanumeric formulas (such as credit card, National Insurance, or Social Security Numbers), as determined by the administrator. This provides comprehensive content analysis across all email components, helping to maintain the appropriateness of all incoming and outgoing messages.

> *A cloud-based solution can help combat malware and spam threats at the Internet level, before they reach your network.*

Another benefit of cloud-based services for security and management: organizations don't have to restrict how, where, and when their employees can take advantage of working remotely.

Another benefit of cloud-based services for security and management: organizations don't have to restrict how, where, and when their employees can take advantage of working remotely.

Risk mitigation C: Implementing a disaster-recovery plan

According to the Symantec 2011 *SMB Disaster Preparedness Survey,* 57 percent of small businesses do not have a disaster recovery plan in place. One reason may be that, in the past, disaster recovery required a significant investment in physical infrastructure. However, cloud services provide a way to get this protection at less cost.

According to the Symantec 2011 SMB Disaster Preparedness Survey, 57 percent of small businesses do not have a disaster recovery plan in place. One reason may be that, in the past, disaster recovery required a significant investment in physical infrastructure. However, cloud services provide a way to get this protection at less cost.

For Sharma, implementing a disaster recovery plan for Child Advocates was a key consideration in moving to the cloud. "Houston is in a hurricane zone," he explains. "Even though we back up our data on a regular basis, the backup copy is still kept in Houston. If we get a level 5 hurricane that could mean that we lose *both* our production data and our backup data."

Sharma's previous backup process was simply to regularly put a copy of the data on an external hard drive, and transport that to the data center. "It requires manpower and wastes a lot of time," he says. "Moving to the cloud gave us a lot of peace of mind, because no matter what happens, we know the data is safe outside the state of Texas."

The move also reduced management time for backup—a common benefit from cloud-managed solutions. "It requires manpower to manage the daily backups," Sharma says. "Every six months, we would have some kind of issue like a hardware failure, and there would be panic. Sometimes hard drives fail. Sometimes the data crashes, and you have to back-up again. When you have only two people to manage the technology, these become big problems. If neither is available, or both are occupied with other tasks, we can forget to take the hard drive to the data center. The cloud technology makes the process automatic and takes out the manual steps."

What's more, using the cloud for backup shifts costs from Child Advocates' capital budget to its operating budget. "That's a big benefit for us," Sharma says.

Step 3: Educating Your Employees

Studies have pinpointed three primary agents of data breaches in classic enterprise LANs/WANs: well-meaning insiders, malicious insiders, and malicious outsiders. In many cases, breaches are caused by a combination of these perpetrators. For example, attacks by malicious outsiders are often enabled inadvertently by well-meaning insiders who fail to comply with security policies.

In *The Human Factor in Data Protection,* a January 2012 Ponemon Institute survey, 77 percent of small business employees said they will or have already left their computer unattended, compared with 62 percent from their enterprise counterparts. This is a growing concern in a world where a significant amount of computing is now done on mobile devices.

What's more, the Ponemon Institute report found that employees at smaller businesses were more likely than employees at larger enterprises to engage in "risky" behavior that can lead to data loss, (e.g., opening attachments or links in spam email). To make matters worse, small businesses have a slightly higher risk of data breaches resulting from employee negligence. In fact, 58 percent of them will or have already opened attachments or Web links in spam, versus 39 percent from larger enterprises.

Your employees need to be trained on the basics of safe computing, such as frequently changing their passwords, and be held accountable for their actions. The importance of protecting their mobile devices, systems, storage devices, and the confidential data these contain, from loss or theft, needs to be stressed.

"Any organization should have a good, written document that clearly states your acceptable use policy," Dickersbach says. "You want people to be productive, but you also don't want them to do anything malicious." Currently, though, only 66 percent of companies trained their employees at least once a year, according to the 2012 *Endpoint Security Best Practices Survey.*

Your employees need to be trained on the basics of safe computing, such as frequently changing their passwords, and be held accountable for their actions. The importance of protecting their mobile devices, systems, storage devices, and the confidential data these contain, from loss or theft, needs to be stressed.

Conclusion: Finding Peace of Mind in the Cloud

A single, comprehensive approach to security covers an array of related areas, such as risk management, compliance audits, regulations, data protection, storage-level security, policy management, and much more.

Given the constrained resources of most small businesses, it can be difficult to implement a comprehensive security strategy without a high degree of automation. Cloud services take away many of the crucial—but routine—elements of risk management, such as patching, that can often be overlooked in the rush of business, leaving small businesses extremely vulnerable to data loss.

Sharma says a cloud-based approach can lower administration costs through automatic content updates and feature enhancements while delivering exceptional accuracy. "It works perfectly for us," he says. "We just set it and forget it."

Small businesses using the cloud spend 32 percent less time each week managing security than companies not using the cloud, and they are five times more likely to have reduced what they spend on managing security as a percentage of overall IT budget, according to *Cloud Security Benefits for Small & Midsize Businesses in the U.S.*, a May 2012 Microsoft study.

Sharma says a cloud-based approach can lower administration costs through automatic content updates and feature enhancements while delivering exceptional accuracy. "It works perfectly for us," he says. "We just set it and forget it."

No wonder 35 percent of U.S. companies have experienced noticeably higher levels of security since moving to the cloud. In addition, almost a third say they spend less time worrying about the threat of cyber attacks. Given the risk of data loss, and the amount of other things you need to focus on, the value of that kind of peace of mind may well be incalculable.