5 MUST-HAVE ELEMENTS

FOR YOUR IT SECURITY PLAN

Summit Business Associates

INTRODUCTION

Small and medium-sized Virginia companies may not have the resources to hire a staff that specializes in IT security, but they still need to find a way to protect themselves from threats. Cybercriminals specifically target small and medium-sized businesses (SMBs) because they know a lack of resources makes these organizations vulnerable. For this reason, companies need to be proactive about their security.

Data breaches can be costly, placing your business in jeopardy. According to the Ponemon Institute Cost of Data Breach Study, **the average total cost of a data breach is $3.8 million, reflecting a 23% increase over 2013**.[1] Fortunately, business continuity management can **reduce the cost by an average of $7.10 per compromised record**. While your data can be threatened by systems errors, human error, and natural disaster, **47% of breaches are caused by malicious or criminal attacks**. With the cost of data breaches, your business can't afford to take chances with security.

At Summit, our core business is working with SMBs throughout Virginia. Our hands-on experience helps us better address our SMB client needs, particularly when it comes to IT security.

In this eBook, we will reveal the five critical components to a comprehensive IT security plan:

1. **Efficient Backup and Recovery**
2. **Backup and Recovery Testing**
3. **Customized Disaster Recovery**
4. **Managed Data Security**
5. **Mobile Device Management**

[1] Ponemon Institute | http://www.prnewswire.com/news-releases/ponemon-institutes-2015-global-cost-of-data-breach-study-reveals-average-cost-of-data-breach-reaches-record-levels-300089057.html)

AREA #1

EFFICIENT BACKUP AND RECOVERY

The rise of big data makes the task of backing up data more difficult. The more information your business stores, the longer it takes to back this information up and the harder it is to meet backup window requirements. Optimizing data management creates more manageable backup windows and speeds recovery. Strategies such as deduplication and compression eliminate redundant data, reducing the amount of data you handle without losing information.

In deduplication, an analysis identifies and stores unique byte patterns. When duplicate patterns are detected, they are replaced by a reference that points back to the original byte pattern.

Compression involves identifying and eliminating statistical redundancy. Information is encoded using fewer bytes without losing any information.

With better data management, your business can reach your Recovery Time Objectives and Recovery Point Objectives more reliably. **Gartner estimates the cost of downtime at $5,600 per minute**.[2] The faster your recovery time and the lower your amount of downtime, the more dependable and profitable your business becomes.

[2] Gartner Blog Network | http://blogs.gartner.com/andrew-lerner/2014/07/16/the-cost-of-downtime/

AREA #2

BACKUP AND RECOVERY TESTING

Even large enterprises may only test their backup and recovery once a year. **Ideally, backup and recovery should be tested at least quarterly** and when a major hardware or software change takes place.

Failing to conduct routine tests of backup and recovery puts your company at risk. You don't want to wait for an event to happen before seeing if your plans work. You may be faithfully backing up data, but will you be able to recover it during a failure? Recovery testing will let you know if your applications are able to bounce back.

In a test, try to replicate the conditions that might occur when you need to restore operations. Conducting role-playing exercises and producing disaster scenarios will prepare your staff for what to do in the event of a traumatic event. Practice runs will let you know if your plan is effective and alert you of places where your plan needs to be improved.

AREA #3

CUSTOMIZED DISASTER RECOVERY

As far as Disaster Recovery goes, one size does not fit all. Make sure you have the right DR plan for your business by conducting a risk assessment and business impact analysis in preparation for developing a plan. What resources and information are vital for company operations? How much downtime can you afford?

Many small and medium-sized business don't have the budget to protect themselves 100%. Instead, they need to consider what applications and systems are critical to keep the business functioning.

No matter the size of your company, having a Disaster Recovery plan is essential. You wouldn't wait until a rain storm to buy an umbrella, so why wait for a traumatic event to happen before forming a DR plan? Unfortunately, many small business owners wait until it is too late. A nationwide survey showed that **3 in 4 small business owners do not have a disaster recovery plan**. Facing a disaster unprepared can cripple your business. More than half of these small organizations say **it would take at least 3 months to recover from a disaster**.[3]

Small and medium-sized companies may not be able to hire security experts as part of their IT staff, but they can enlist their employees to be part of the solution. Members of your staff should be made aware of disaster recovery strategies so that they can take an active role in protecting your business in an emergency.

[3] Continuity Central | http://www.continuitycentral.com/index.php/news/business-continuity-news/488-disaster-recovery-planning-in-us-small-businesses-surveyed

AREA #4

MANAGED DATA SECURITY

Managed security is gaining popularity. Transparency Marketing Research predicts that the **managed security services market could reach nearly $24 billion by 2019**.[4]

Managed services can provide the security expertise that your small or medium-sized business may not be able to acquire otherwise. While your staff may be unfamiliar with today's wide range of threats, a managed service provider will have experience with handling these situations.

Your staff can't be expected to focus solely on security. While they are tending to their regular duties, threats may get by your defenses. Managed services ensures that your data is being monitored 24/7. Continual monitoring can detect anomalies that reveal threats so they can be stopped before any harm is done.

Upgrades and patches are also hard to keep track of. Your managed service provider can ensure that antivirus protection is up to date and that you have the appropriate firewalls in place. With your managed service provider in charge of security, your staff is free to focus more on business innovation and growth.

[4] MSPmentor | http://mspmentor.net/managed-security-services/072114/managed-security-services-market-could-be-worth-over-24b-2019

AREA #5

MOBILE DEVICE MANAGEMENT

In our always-on culture, mobile use in the workplace is exploding. A Constant Contact Survey found that **66% of small business owners use mobile devices or mobile solutions**.[5] Employees enjoy a flexible workplace that frees them from their cubicles. Mobile devices enable employees to create an ideal work/lifestyle mix by working from home or while traveling.

Unfortunately, the increasing use of mobile devices in the workplace also creates security concerns that require unique solutions. A Mobility Device Management (MDM) solution helps guard against lost and stolen devices. In addition, the solution can also protect company data in the event of an employee leaving the company by remotely wiping sensitive data.

MDM is especially important in a BYOD environment where employees use their personal phones for company business. BYOD can leave your business vulnerable to phishing scams and malware. Employees should be made aware of specific BYOD policies that outline appropriate and safe use of mobile devices that are also being used for work. MDM solutions can also compartmentalize personal and company data so that sensitive business information can be removed from a device without harming personal information.

[5] Marketing Profs | http://www.marketingprofs.com/charts/2013/10791/how-small-business-owners-are-using-mobile-technology

CONCLUSION

Recently, the Virginia government has experienced several high-profile security breaches, most notably **at the Department of Veterans Affairs, where 5,351 records were compromised**.[6] This breach follows an earlier event in 2012 that compromised thousands of records. These breaches underscore the importance of strengthening IT security measures so that the sensitive and personal information of those who serve our country stays safe.

Local government agencies in Virginia trust Summit Business Associates to provide the highest quality security solutions. Summit is a small company that provides the kind of personal attention and friendly service that has helped them build a loyal customer base.

Summit Business Associates

[6] Fox News | http://www.foxnews.com/politics/2014/01/21/security-breach-at-va-puts-names-addresses-and-medical-information-vets-in/

DISCOVER HOW YOUR BUSINESS RATES ON SECURITY BY SETTING UP A DATA SECURITY ASSESSMENT WITH **SUMMIT BUSINESS ASSOCIATES. EMAIL US TODAY: SALES@SUMMITBIZ.NET**

WWW.SUMMITBIZ.NET

Premier Business Partner IBM