peters & associates
simplify solve succeed

CISCO

IT Security Action Plan

For Fast Growing Small Businesses

Table of Contents

Executive Summary

For most businesses, data is their most valuable asset and the crux of revenue generation, making data protection critical to their overall success. However, hackers continuously find new ways to infiltrate company networks and exploit their digital assets. Without an iron-clad IT security system in place, businesses risk breaches to company and customer data.

In this climate, IT security becomes increasingly difficult to manage, especially for small businesses that can't afford to train and maintain their IT team's data storage and protection skills.

Cybersecurity Concerns Pressing Small Businesses

- U.S.-based companies must comply with data privacy laws including GDPR (European Union) or even the forthcoming California Consumer Privacy Law (effective January 1, 2020).
- BYOD policies are becoming more and more commonplace; however, mobile devices can expose companies to reputational risk and data breaches without the right security in place.
- As cyber-attacks become an inevitability, mitigation strategies or incident response plans are a critical part of a security plan. The U.S. government warned there are two types of businesses: those that have been hacked, and those that don't know they've been hacked.
- Without proper mitigation strategies or incident response plans, the damage from an attack can be irreversible. One news story about a data breach can cost a publicly traded company millions.

No small business can afford to leave its data vulnerable. Small businesses need enterprise-level capabilities to protect their growth opportunities. New technology and solutions put that within their reach.

Learn how to secure your assets affordably and maintain a competitive advantage through managed IT security services.

Significant Changes to the IT Security Landscape

Today, business expansion can expose more than cash flow problems; it can introduce gaps in IT security. In minutes, one new employee with access to customer data can destroy a reputation built over many years.

To effectively ensure ongoing security, businesses need to develop plans for both data security and compliance with government agencies, important customers, vendor requirements and other protocols.

Such demands can drain resources and constrain operations – especially for businesses that don't have a rock-solid security plan in place.

IT Security Principles Drive the Action Plan

The solution to successfully addressing IT security needs lies in strategic planning and efficient business tactics. These days, the business should operate with an appreciation of the value that reliable IT security brings to the business and its customers.

IT security best practices adhere to key principles.

What follows is a proven IT security action plan based on the guiding principles of IT security.

Step #1: Align IT Security to Your Business

Businesses don't exist to be secure; businesses exist to make money. An IT team's understanding of this is critical to ensure IT aligns with overarching business goals. Hardware and software must allow the company to progress and operate effectively, with little hindrance. Therefore, take a good look at your IT infrastructure and operation. Is it aligned with your business strategy? Does it benefit the customer or the operations people?

For instance, old firewalls may be fully depreciated, but do they make the network slow and unresponsive during peak business hours? If the plan is to expand into other markets, will your network devices provide security event details to a single monitoring system, or will someone need to be hired just to supervise them locally?

If the business could operate more effectively and less expensively with modernized security infrastructure, there is little reason not to do so. In fact, there is business incentive to accelerate the fix.

Step #2: Watch IT Carefully

Ignorance is blissful only to those with nothing to lose. Businesses need to know what's happening with their digital and network assets. IT security must provide real-time intelligence on everything, from the endpoints, to the data traffic, to the servers.

- The system must be able to monitor events without disrupting or slowing down the business
- Should be able to see all suspicious activity from someone reading the CEO's email to files being transferred at abnormal rates

There are many security solution providers, each with a discrete set of objectives and parameters. All of them should be working to provide core security intelligence to a single pane of glass. If they aren't, find those that can.

Step #3: Act on What You Know

In IT security, survival is the difference between wisdom and knowledge. This truth escapes the notice of many a security architect. It is no help simply to know that sensitive information may have been breached. Management needs details to react appropriately to an attack.

In the event of a breach:

- Customers need to know what of their sensitive information is potentially exposed. Was it their account number, password, children's names?
- Law enforcement will need to know facts about the attack and actor(s) behind it. When did the event occur, affecting what digital assets, over which devices and for how long? What indications suggest imminent threats, and what will be done to eliminate those threats?

- Vendors will need to know their extent of risk or involvement
- You will need to know whether the event violated terms of agreement with third parties or key vendors, and if so, to what extent?

New technology provides more than real-time security monitoring of sensitive data. Microsoft, for example, includes very good information rights management tools as part of its Office 365 product suite. Much like the explosive dye packs banks use to recover stolen money, Azure Information Protection (AIP) can ensure business data remains within the control of its owners.

There are many more new technologies available to streamline operations while protecting key business assets. But they can be extremely complex to provision and maintain. Worse, poor configuration can be counterproductive and expose risk or operational vulnerabilities. Meaningful security intelligence comes through specialized core competencies rarely within the means of small businesses.

Step #4: Maintain a Culture of Awareness

A good IT security program should address human elements as well as electronic ones. Employees are in a good position to help protect sensitive data and should be skilled in carrying out data protection practices.

The strength of business security is measured by its weakest link. Social media accounts have introduced dramatically enlarged attack surfaces for bad actors. Through social media, they target employees who may be susceptible to blackmail or misguided loyalty. Often, employees may not know to remain diligent to suspect emails and web site encryption.

Employees should understand the business objectives. They should be regularly reminded of the ways and means at their disposal to both protect and develop the business.

Managed Security Services Help to Reliably Secure Company Assets

The only hat nobody in a small business should wear is the IT security hat. Most small businesses don't make money developing ITSEC skill sets. They can ill afford to cover all the costs associated with training, configuration and monitoring in an ever-expanding landscape full of bad actors.

The solution? Find a qualified IT security partner who understands your business – a partner who can be trusted to help, not harm, business continuity and growth.

- Growing businesses need to focus on revenue generation
- They should not have to deal with IT distractions

For many thriving businesses, their owners developed a reliable system to support sales. That system is the key to their success. The same principle works to their benefit in the area of IT Security. Managed security services providers (MSSPs) deliver a good system that supports customer growth by protecting business assets.

The key word here is "managed." A good MSSP helps businesses reach their market and profitability goals, mitigating the prohibitive overhead elements of modern IT security "table stakes."

The Strategic Path Forward

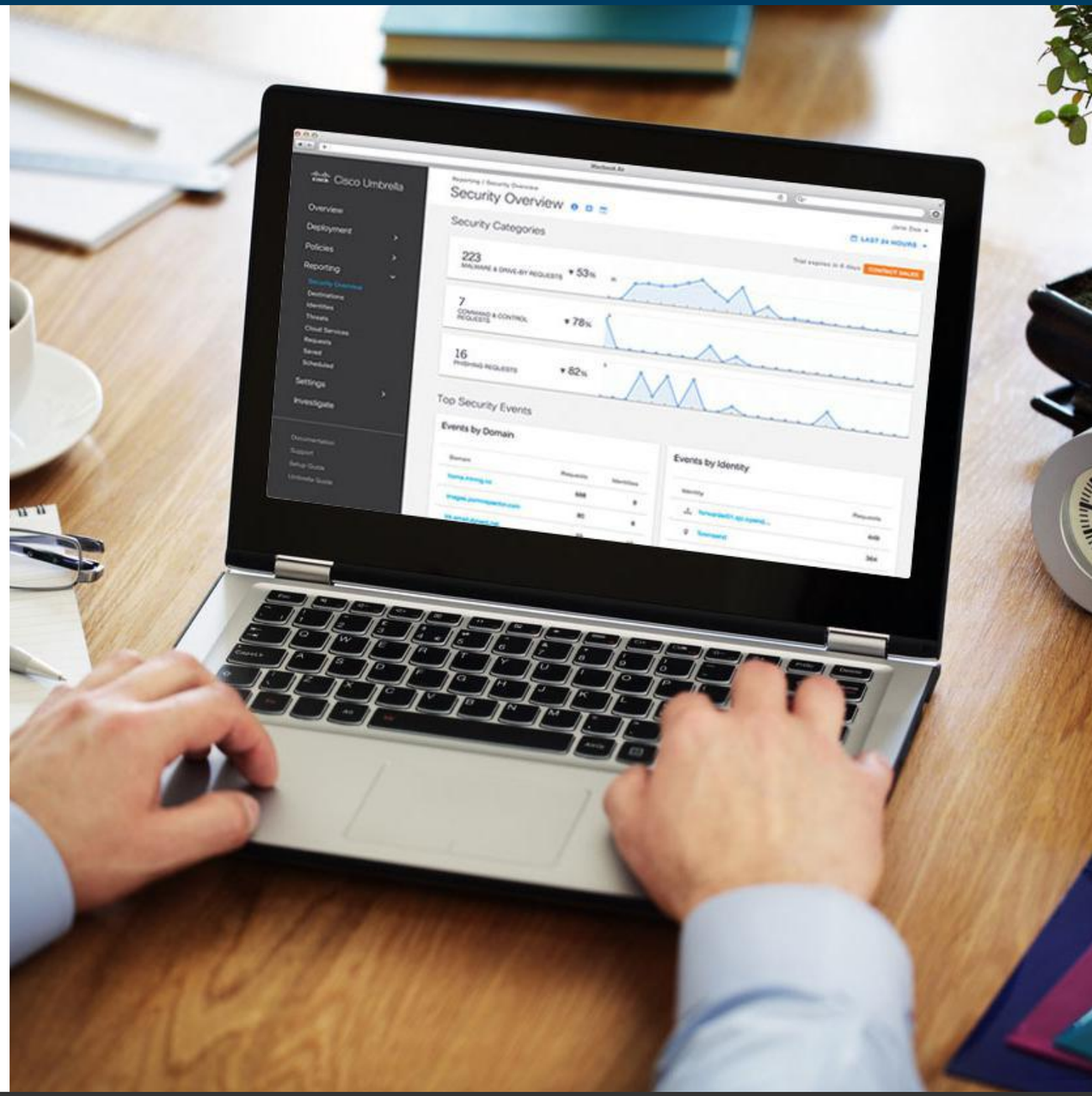
Outsourcing highly specialized IT security skill sets allows business to gain a market advantage. It affords small and mid-sized businesses the opportunity to experience enterprise-grade IT security performance without enterprise-size budgets.

For small and mid-sized businesses looking to focus on their competitive advantage, hiring a managed security services provider makes good business sense. With a professional MSSP, business owners benefit from:

- A broader range of options best suited to their business strategy
- A better tool for managing IT security during economic and business climate changes
- An accountable party who adds incremental value to a non-revenue producing asset

Perhaps more importantly, retaining an entire team of skilled IT security professionals makes business owners good stewards of customer information; the data that will continue to fuel growth.

TALK WITH AN IT CONSULTANT



To learn more about Peters & Associates' managed security solutions services, schedule a meeting with one of our representatives today.

CONTACT US

peters & associates
simplify solve succeed

cisco