



GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

Hayslip, Gary

“5 simple steps for SMBs to ensure cyber resiliency”

Csoonline.com

IDG Contributor Network

21 June 2018

URL: <https://www.csoonline.com/article/3283252/5-simple-steps-for-smbs-to-ensure-cyber-resiliency.html>

Accessed: 02 July 2019

Synopsis: To summarize, for a business to meet the objective of resilient activities it needs to incorporate a security and risk management program, implement security controls to manage its risk exposure, and continually monitor for changes in risk over time. With that information in mind, this article offers small- and medium-sized businesses (SMBs) five simple steps for becoming cyber resilient.



ADAPTIVE SECURITY

By Gary Hayslip, Contributor, CSO
JUNE 21, 2018 05:04 AM PT

Opinions expressed by ICN authors are their own.

OPINION

5 simple steps for SMBs to ensure cyber resiliency

While these tips are by no means a complete guide for how SMBs can be resilient, they can be the start of a continuous process small and mid-sized business should implement to be better prepared.

The concept of businesses being cyber resilient has recently come into focus and is a significant question for many companies today due to the growing complexity of threats and vulnerabilities they face. In my previous article for CSO, "[What should a cyber-resilient business look like?](#)" I theorized that a good visual cue to demonstrate to organizations how they could be resilient is: *Cyber Hygiene Controls + NIST Resiliency Techniques = Objectives = Business value through resilient operations.*

To summarize, for a business to meet the objective of resilient activities it needs to incorporate a security and risk management program, implement security controls to manage its risk exposure, and continually monitor for changes in risk over time. With that information in mind, this article offers small- and medium-sized businesses (SMBs) five simple steps for becoming cyber resilient.

One of the most fundamental concepts CISOs follow is visibility. If the CISO and security team don't know an asset or service exists, how can they understand its potential risk? It's this context that led me to write about [cybersecurity as a lifecycle](#), a process of continuous interlinked operations and the first step in the cybersecurity lifecycle was "inventory," which I believe applies to our current discussion on cyber resiliency.

[Keep up with 8 hot cyber security trends (and 4 going cold). Give your career a boost with top security certifications: Who they're for, what they cost, and which you need. | Sign up for CSD newsletters.]

For an SMB to begin its effort to become cyber resilient, it needs to have visibility; it needs to have an understanding of what's essential to the business and what resources are required to protect its business operations. That leads us to our first step, which begins with executive leadership:

ADVERTISING



4

Step 1: Who are we, what is our purpose?

This step is about taking inventory. Do the leaders of an SMB genuinely understand not just their business operations and products or services, but also the critical resources they need to support them? This step should involve discussions with key stakeholders and business unit leaders to document vital resources and the types of data the business creates, processes and shares with its partners.

Answers to these questions will provide an SMB insight into the data types they have, who they share data with, and any compliance requirements the SMB must meet if they have a data breach.

All of this information should be used by the company's internal security team for risk management or a third-party managed service provider (MSP) or managed security service provider (MSSP) to provide risk mitigation services tailored to the SMB's specific needs.

[Prepare to become a Certified Information Security Systems Professional with this comprehensive online course from PluralSight. Now offering a 10-day free trial!]

Step 2: What resources and risks do we currently have?

Once an SMB has their initial list of critical operations, services, assets and data types documented, they need to look at what resources they have to protect the information and infrastructure. This step is about gaining insight into the current resources used for security, including internal assets and any contracted external services.



Treating the Customer Like an Individual with Adobe Experience Platform

In this step, it is on leadership within the SMB to look at their identified list from the previous step and discuss how resources are being allocated for security operations. In these discussions, they also need to speak about how risk is being identified, how it is being mitigated and who accepts any outstanding risk exposure for the business.

After completing this step, the SMB leadership should understand how its risk is being managed and if security operations are adequately staffed and funded or whether they need to reach out to external partners for assistance.

Step 3: How prepared are we?

By this stage in the cyber-resilient process, the SMB should have identified its critical assets and documented its risk management processes and the resources it has allocated for security operations. With this contextual information at hand, it's now time to ask some hard questions.

The SMB leadership team needs to review what types of risks (financial, competitive, regulatory, etc.) the company faces and whether they have the mechanisms in place to deal with them. They need to talk about what external partners they are connected to and what agreements are in place to safeguard the business in case of an external partners data breach. It is during this stage that a security process called incident response needs to be explored. Does the company have policies in place for how they will respond in the case of a cyberattack? Have these policies been tested and, if so, how often?

By the end of this step, the SMB leadership team should understand the risks associated with company operations, they should know who their external partners are and what documentation is in place to reduce liability. They also should have reviewed company procedures to deal with a cyber incident, and they have documented those areas that need to be addressed.

Step 4: Not all security is created equal

With assets, risks, procedures, resources and partners identified we come to one of the most critical aspects of preparing for resilient operations. This next step is for the leadership team and stakeholders to review the company's security program. The security program and its manager should have taken much of the previous information and incorporated it into security controls and processes to manage risk and add secondary resources for emergent operations.

During this security review, it is essential for the SMB leadership to work with its security program manager and review the company's current security plans and the maturity of its overall program. During this review, it should be noted whether the plans cover both internal and external business operations. The plans also should be reviewed to verify if they include new services that are now cloud based. This part of the process is for the business to understand how well the security program has identified critical assets and services and if any gaps need to be addressed.

Step 5: Creating an action plan

In the final step of the process, the SMB leadership team and security or IT manager should now have a list of legacy processes and security gaps. It is in this stage that the company should bring in stakeholders to review and prioritize the list of issues. Emergent issues should be identified for immediate action, and both short- and long-term plans should be created for the security program to manage.

This prioritized list can be used as a strategic plan by the SMB's security manager to establish the current risk baseline, and over time monitor its reduction in risk exposure as the issues are mitigated. I have found from personal experience the management of this plan should be periodically reported to leadership. It is a living document to be adjusted over time as the SMB and its security program mature.

SMBs that follow these five steps will be better prepared for the inevitable day they have to deal with a cybersecurity incident because they will know their risk exposure. Their security teams and MSP or MSSP partners will have a better understanding of what assets and operations are critical to the business and will have tailored incident response plans to reduce the impact of any successful breaches.

This article is by no means a complete guide for how SMBs can be resilient; it is just the start of a continuous process they should implement to be better prepared. The Homeland Security Department's US-CERT offers several resources I would recommend to assist SMBs as they start working their resiliency issues, including the following:

- [Critical Infrastructure Cyber Community Voluntary Program](#)
- [US-Cert Resources for Businesses](#)
- [US-Cert Resources for Small and Midsize Businesses \(SMB\)](#)
- [FCC Guide for SMB's Create Their Own Security Plans](#)
- [Geographically-Specific Security Resources for Businesses](#)

This article is published as part of the IDG Contributor Network. [Want to Join?](#)

Next read this

- [*The new CISO's playbook: 5 rules to follow*](#)
- [*12 tips for effectively presenting cybersecurity to the board*](#)
- [*Top cyber security certifications: Who they're for, what they cost, and which you need*](#)
- [*6 steps for building a robust incident response plan*](#)

- [8 cheap or free cybersecurity training resources](#)
- [Whip your information security into shape with ISO 27001](#)
- [Securing risky network ports](#)
- [Top 9 cybersecurity M&A deals of 2018 and 2019 \(so far\)](#)

Gary Hayslip is responsible for the development and implementation of all information security strategies, including Webroot's security standards, procedures and internal controls. Hayslip also contributes to product strategy to guide the efficacy of the Webroot security portfolio.

Follow     

💡 Get the best of CSO ... delivered. Sign up for our FREE email newsletters!

Sponsored Stories



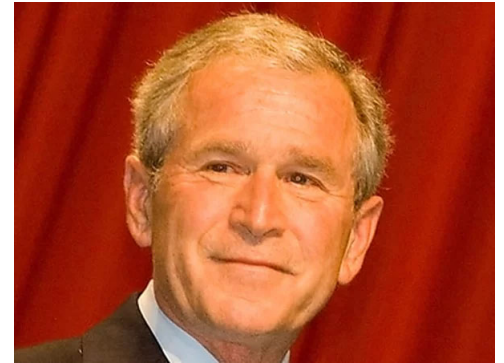
5 Thoughts on the Ever-Changing Role of the IT Executive and the Data Center Industry

Iron Mountain



All Star Billionaires: Shaquille O'Neal is One of the Richest Team Owners in Sports

Investing.com



Greatest Presidents In U.S. History Ranked. Guess Who Is No. 1

z.today



The 25 Richest Heirs in America [in Pictures]

Investing.com



What is Rheumatoid Arthritis? Look For Symptoms, Treatment & More

Yahoo! Search



Simple Way To Control Diabetes?

ouremedy.com