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

Author: Snodgrass, Glenda R.

Title: "Back to Basics: Infosec for Small and Medium-Sized Businesses"

Website: tripwire.com

Organization: tripwire

Date: 16 July 2019

URL: https://www.tripwire.com/state-of-security/security-data-protection/basics-infosec-small-medium-businesses/

Accessed: 15 October 2019

Synopsis: Too many small and medium-sized businesses (SMBs) are under the belief that purchasing "This One Product" or "This One Managed Service" will provide all the security their network requires. If this were true, large corporations with huge IT budgets would never have data breaches!

Before you start buying expensive new technology to protect your office network, take some time to examine your internal information security processes—make sure you are covering the basics.

Back to Basics: Infosec for Small and Medium-Sized Businesses

Too many small and medium-sized businesses (SMBs) are under the belief that purchasing "This One Product" or "This One Managed Service" will provide all the security their network requires. If this were true, large corporations with huge IT budgets would never have data breaches!

Before you start buying expensive new technology to protect your office network, take some time to examine your internal information security processes––make sure you are covering the basics.

Organization

It is quite common for SMBs to lack organization with respect to their information systems, particularly if they have experienced steady and/or rapid growth over some period of time. In the early days, organization seems superfluous. At some point, it becomes clear that organization is needed, but the job isn't assigned to anyone. Often, there simply isn't anyone with the time, energy or expertise to take on the job. Occasionally, a willing volunteer takes on the task, but when that person leaves, the baton is not passed.

All too often, the impact of organizational problems becomes clear only in a moment of crisis. Typically, a lack of organization means there is no infosec program, no one person or group in charge of information systems, no documentation on system configurations and accounts, etc. The organization isn't following basic security practices because policies aren't clear and actions aren't repeatable.

In turn, a lack of organization generally affects another basic that is often overlooked: documentation.

Documentation

I always tell my clients: "You can't secure it if you don't know it's there." This is why an inventory of hardware and an inventory of software are the first two of the Center for Internet Security's 20 Controls. Yet few SMBs take even these first two steps to securing their information systems.

Without good documentation, it is difficult (if not impossible) to secure information systems. Good documentation for information security includes:

1. Asset lists
2. Network diagrams
3. Device configuration information
4. Maintenance/support agreements
5. Account/access lists
6. Organizational chart with roles & responsibilities identified
7. Network security & acceptable use policies

8. Incident response plan
9. Disaster recovery plan
10. Business continuity plan

With good documentation, you know what you have, you know how it's configured, you know who has access to it, you know why you need it and you know how to replace it in an emergency.

Control

With inadequate organization and lack of good documentation, you don't actually have control over your information systems. Without control, you cannot assure even a basic level of security. In addition to organization and documentation, achieving control requires two more things: policies and training.

> ***In the absence of written policies and an employee training program on acceptable computer use, you have no control over how employees are using your company assets. Legal liability and labor law issues can become even more complex in the absence of written policies and a training program.***

When employers don't have good written policies and employees don't receive effective training (why these policies are important and how to develop good security habits), the result is often violations of standard security best practices, such as:

- Out-of-date software with known vulnerabilities
- Potentially compromised software
- Personal accounts in use on company computers
- Personal assistants, location services and analytics/tracking that are active on many devices
- Shadow IT/clandestine purchases attached to the network
- Cloud document storage outside company control

Each of these examples presents a unique opportunity for cyber criminals to steal your data. For example, many data breaches begin with a phishing email that exploits a known vulnerability in a common software. A computer running that older, unpatched version can easily provide attackers with access to your network.

The situation is even more critical when you do not have login credentials for key components of your network such as firewall, wireless access points, servers, databases, etc. Without login credentials, you have no control over the configuration or security of these devices. Each of these represents a potential backdoor to your network.

Without control of your data backup plan, you have no way of recovering your data in the event of a significant event (such as a ransomware infection). Indeed, you don't even know whether it would be possible to recover your data, as you don't know the status of available backups.

> ***Security products are, of course, an important part of your information security plan, but they should not represent the entirety of your plan.***

You Can't Replace the Basics

Too many SMBs think that purchasing "This One Product" or "This One Managed Service" will provide all the security their network requires. If this were true, large corporations with huge infosec budgets would never have data breaches. Ask yourself this: "If it seems too good to be true…"

Good infosec requires going back to the basics! Regardless of the size of your business, your information security program should be founded on effective organization through documentation and control, including well-written policies and effective employee training.

About the Author: *Glenda R. Snodgrass*, *@Glenda_TNE*, *has been President, lead consultant and project manager at The Net Effect since the company's inception in 1996. She is primarily engaged in cyber security training, threat analysis and mitigation for commercial, nonprofit and governmental organizations. In addition to conducting securityrelated workshops, corporate training and delivering cyber security defense presentations at professional conferences and conventions, she spends time drafting network security procedures and developing employee security awareness training programs for clients.*

Currently President of Gulf Coast Industrial Security Awareness Council, Vice Chair of Mobile Chapter 117 of the American Society or Industrial Security (ASIS International), member of the steering committee for Gulf Coast Technology Council, and serving on the Board of Directors of the Mobile Area Chamber of Commerce. Ms. Snodgrass is also an active member of InfraGard and recently graduated from the FBI Citizens' Academy. She holds a B.A. from the University of South Alabama (1986) and a maîtrise from Université de Paris I PanthéonSorbonne in Paris, France (1989).

Editor's Note: *The opinions expressed in this guest author article are solely those of the contributor, and do not necessarily reflect those of Tripwire, Inc.*
