The Net Effect, LLC
Your security is our business

A white paper from The Net Effect, L.L.C.
by Glenda R. Snodgrass (grs@theneteffect.com)
(251) 433-0196 www.theneteffect.com

Five Steps to Maximize Your Investment in Cyber Security

We are often contacted by people who are concerned about cyber security in their organization, but who have no idea how to begin the process of assessing and mitigating risk. You have probably found yourself in the same situation -- bombarded by IT vendors and other "solution providers" trying to persuade you that the purchase of This One Product or This One Managed Service will provide all the security your network requires. You don't feel qualified to evaluate these offerings in a meaningful way, and you keep thinking that you are missing something important.

You are!

Before you start buying expensive new technology to protect your office network, take some time to examine your internal processes. Follow these five steps to maximize your investment in cyber security:

. . . . . .

Step One:
Identify Organizational Problems

It is quite common for SMBEs to lack organization with respect to their information systems. 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. Occasionally the task is taken on by a willing volunteer, but when that person leaves, the baton is not passed. All too often the impact of organizational problems is realized only in a moment of crisis.

Typically lack of organization means there is no information security program, no one person or group in charge of information systems, no documentation on system configurations and accounts, etc. Basic security practices are not being followed. Policies aren't clear (or don't exist) and actions aren't repeatable.

- **Identify your "organization champion" and task this person with leading the development of an information security program.**

Step Two:
Gather Your Documentation

I always tell my clients: "*You can't secure it if you don't know it's there."* This is why inventory of hardware and inventory of software are the first two of the Center for Internet Security's 20 Controls. (https://www.cisecurity.org/controls/)

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

1 – Asset lists
2 – Network diagrams
3 – Device configuration information
4 – Maintenance/support agreements
5 – Account/access lists

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.

- **Gather what you have, and start working on the things you're missing. Focus on the low-hanging fruit!**

Step Three: Develop Policies & Train Employees

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, *e.g.*

- Out-of-date software with known vulnerabilities
- Potentially compromising software
- Personal accounts in use on company computers
- Personal assistants, location services, analytics/tracking active on 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 breach incidents 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.

- **Write down the informal policies you already have in place. Think about how to make them better. Add a few "best practices" you've read about online. Hold a simple training session with employees to discuss and refine your policies.**

Step Four:
Gain Control of Your Network

With inadequate organization, lack of good documentation, no written policies and no employee training program – *you don't actually have control over your information systems*. Without control, you cannot assure even a basic level of security.

The situation can be 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 back door 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.

- **Ask whoever manages your IT systems to provide admin credentials to you. Inform yourself on the details of your backup system, and develop an incident response plan.**

Step Five:
Have an Independent Assessment

How hard is it to proofread your own work?!?!

It's difficult to catch your own mistakes, especially when you aren't aware that you were doing something wrong. Or not doing something you should. Or doing something you shouldn't.

This is a situation we encounter nearly every time we conduct a security assessment for a new client. Even if your IT vendor or MSSP is truly competent and security-conscious, people still make mistakes. And it's hard to catch your own mistakes.

That's why it is critical to have a security assessment performed by someone who is not responsible for installing, configuring or maintaining your network. You need those fresh eyes and that outside perspective to identify gaps in your security program and develop a roadmap for improvement.

- **Talk to a qualified third party about conducting a security assessment on your information systems.**

Before you write the check for That One Product or That One Managed Service which will provide all the security you need, ask yourself this:

"If it seems too good to be true ..."

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

Following these five steps will maximize your investment in cyber security.

Contact Us to learn more!

The Net Effect, LLC
Your security is our business

Post Office Box 885
Mobile, Alabama 36601-0885 (US)
phone: +1 (251) 433-0196
https://www.theneteffect.com

The Net Effect, L.L.C. is a consortium of consultants experienced in providing technology consulting services to commercial, non-profit and governmental organizations. The company was founded in Mobile, Alabama in 1996 with a focus on information security, and has worked with businesses across the US, in Canada and in Europe.

Glenda R. Snodgrass, President and lead consultant for The Net Effect, specializes in information security training and compliance. She has extensive experience teaching and training security awareness and compliance requirements. She has conducted numerous workshops covering PCI DSS, GLBA, FAR 52.204-21, DFARS 252.204-7012, NIST 800-171, NIST CSF and CMMC. Her public speaking includes regional conferences of multiple organizations for security professionals. Glenda holds a B.A. from the University of South Alabama (1986) and a maîtrise from Université de Paris I - Panthéon-Sorbonne in Paris, France (1989).