A white paper from The Net Effect, L.L.C.

Protecting Company Data with Simple Security Policies

by Glenda R. Snodgrass
(grs@theneteffect.com)
www.theneteffect.com
(251) 433-0196

Data breach incidents are in the news daily, yet so many are preventable! Here we present five simple rules for employee network usage that will help you NOT be the next headline.

Top Five Rules That Should Be in Every Organization's Network Security Policy (and Why!)

1. Employees shall not provide their own hardware.

While it's easy and inexpensive to buy a printer or other small network device, employees must resist the urge! All hardware on the company network needs to be installed with security in mind. Why? What could happen? Well …

> **Flaws in popular printers can let hackers easily steal printed documents**
>
> *Thousands of internet-connected printers could allow an attacker to steal sensitive data, as well as passwords that could allow further compromise of a network.*
>
> https://www.zdnet.com/article/flaws-in-popular-printers-can-let-hackers-easily-steal-printed-documents/

> **NASA hacked because of unauthorized Raspberry Pi connected to its network**
>
> *The point of entry was a Raspberry Pi device that was connected to the IT network of the NASA Jet Propulsion Laboratory (JPL) without authorization or going through the proper security review.*
>
> https://www.zdnet.com/google-amp/article/nasa-hacked-because-of-unauthorized-raspberry-pi-connected-to-its-network/

2. Employees shall not provide their own software.

Copyright 2020 The Net Effect, L.L.C. All rights reserved.

Sure, it's easy (and often free) to download software off the Internet, but employees must resist the urge! Here's why:

> **CISA Security Tip (ST18-004) Protecting Against Malicious Code**
>
> *It is not uncommon that free software contains a Trojan horse making a user think they are using legitimate software, instead the program is performing malicious actions on your computer.*
>
> https://www.us-cert.gov/ncas/tips/ST18-271

3. Employees shall not use business passwords on personal accounts, and vice versa.

I know that everyone finds it frustrating to keep track of multiple passwords, but it's important not to mix-and-match between work and home! Passwords are stolen and sold on the dark web every day, and those stolen credentials are used in attacks.

> **Sellers Lose Thousands As Amazon Marketplace Is Hit By Hackers**
>
> *The fraud seems to be the net result of other hacks — password credentials lifted and resold on the dark web and sold to criminals who then use them (because consumers often recycle passwords with little to no variation) to hijack other accounts that consumers may have. PayPal and eBay have both faced similar hacks of late…*
>
> https://www.pymnts.com/amazon/2017/sellers-lose-thousands-as-amazon-marketplace-is-hit-by-hackers

Copyright 2020 The Net Effect, L.L.C. All rights reserved.

4. Employees shall use Internet access on company resources only for business purposes.

All too often, malware of various types sneaks onto a computer while the user was aimlessly browsing, shopping online, using social media or checking email on personal accounts that bypass company email protections.

> **How Do Employees Cause Security Breaches?**
>
> *Suppose, for example, that a [user] mistypes the URL of a website and lands on a website containing malware. That malware could infect the employee's computer and eventually cause a breach in your corporate network.*
>
> *https://www.continuous.net/2017/03/employees-cause-security-breaches/*

> **Social Media Platforms Double as Major Malware Distribution Centers**
>
> *Because many organizations tend to overlook or underestimate the threat, social media sites, including Facebook, Twitter, and Instagram, are a huge blind spot in enterprise defenses.*
>
> https://www.darkreading.com/vulnerabilities---threats/social-media-platforms-double-as-major-malware-distribution-centers/d/d-id/1333973

5. Employees shall store company information only on company resources.

It may be tempting to use a personal cloud storage account like DropBox, Box, Google Drive, etc. to access work information outside the office, but resist the urge! Company data needs to stay on company resources.

Copyright 2020 The Net Effect, L.L.C. All rights reserved.

Dozens of companies leaked sensitive data thanks to misconfigured Box accounts

Security researchers have found dozens of companies inadvertently leaking sensitive corporate and customer data because staff are sharing public links to files in their Box enterprise storage accounts that can easily be discovered.

https://techcrunch.com/2019/03/11/data-leak-box-accounts/

Finally, having written policies is important, but it's equally important to **train your employees** in these policies. Use real-world examples like these to bring the policy alive. Help employees understand that they are an important part of data security.

We'd love to help you develop an effective information security program, including written policies and employee training.

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 organizations 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).

Copyright 2020 The Net Effect, L.L.C. All rights reserved.