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

Building a Culture of Security

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

Information security is becoming increasingly important (and more difficult to maintain) as more data is stored electronically, as businesses and individuals become more dependent on electronic data for daily functions, and as cyber criminals become better at breaking into systems.

Take note: no business is too small to be the victim of a cyber attack. In fact, Verizon's 2020 Data Breach Investigations Report[1] reported that 43% of data breach victims are small businesses:

> "*While differences between small and medium-sized business (SMBs) and large organizations remain, the movement toward the cloud and its myriad web-based tools, along with the continued rise of social attacks has narrowed the dividing line between the two. As SMBs have adjusted their business models, the criminals have adapted their actions in order to keep in step and select the quickest and easiest path to their victims.*"

No matter the security standard for your industry, a common theme runs throughout -- **building a Culture of Security in your organization**. This means that all employees, at all levels, understand and appreciate the importance of information security, and work to safeguard your company data.

☆ *Where to Begin?*

- Recognize that security is not a one-time event, nor a state to be achieved, but rather a continuous process.
- Security starts at the top! If management don't take security seriously, no one will.
- Policies and procedures must be established and consistently followed.

1 https://enterprise.verizon.com/en-gb/resources/reports/dbir/2020/smb-data-breaches-deep-dive/

- Employees should receive regular training on security policies and procedures. Without employee "buy-in," the most sophisticated security controls can and will be bypassed.

- Physical security is as important as virtual or network security. Your IT security and physical security departments need to be working together, along with your operations people.

- Pay attention to details. Every single item on your network -- computers, software, printers, cameras, thumb drives, phones, tablets, temperature monitoring systems, vending machines, multifunction machines, CNC equipment, security systems, telephone systems -- all must be provisioned and configured with security in mind.

- Clearly define employee duties and responsibilities and limit employee access to data based on the "need to know" for their particular job.

- Be prepared: screen employees prior to hire, and have an incident response plan in place.

✯ *Want to learn more?*

Contact us.

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 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).