HOW TO PRIORITIZE CYBER SECURITY

ISSUE 7 • NOVEMBER 2020 • VOL. 2

THINK..

"PEOPLE, PROCESS, TECHNOLOGY"

Did you know? *

- Since COVID-19, the US FBI reported a 300% increase in reported cybercrimes
- There is a hacker attack every 39 seconds
- 43% of cyber attacks target small business
- THE GLOBAL AVERAGE COST OF A DATA BREACH IS $3.9 MILLION ACROSS SMBS
- 95% of cybersecurity breaches are due to human error

*Sources:
Milkovich, Devon. (2020, June). 15 Alarming Cyber Security Facts and Stats. Cybint. cybintsolutions.com/cyber-security-facts-stats/

10 ORGANIZATIONS THAT PROMOTE DIVERSITY IN INFOSEC

WE MADE THE LIST! - VISIT THE ARTICLE HERE

MESSAGE FROM THE CEO

DEAR MIC COMMUNITY,

We keep on hearing that cybersecurity (and privacy) is huge and that organizations should know their risks in these areas and do everything they can to reduce those risks. Everybody knows that right? Then why is it so difficult to define? Why is it so hard to do? Why do organizations continue to press their luck?

The answer is because it is hard! Cybersecurity touches every single area of the business and it cannot be done in a vacuum. For example. someone recently asked me to create a business continuity plan (BCP). My next question was to ask for the leader of their third-party risk program. They said, how does that relate to the BCP? I explained that in this business they rely on third-party vendors to get their product to market and for us to figure out their BCP we need to know exactly how their vendors handle a disruption that would hinder their ability to deliver to their clients. If they can't service us, our business is disrupted which would then trigger our BCP and we have to figure out what we do from there. There was a huge pause, then a sigh, then recognition that a BCP is much broader than this person thought.

One of my favorite phrases since programming in college is "GIGO" garbage in, garbage out. It's the concept that flawed, input data, produces flawed, output data. The reason cybersecurity is hard is because if your foundation is flawed, or worse yet, nonexistent, then you can't build an effective cybersecurity program. It just won't work. Organizations need to realize that in order to have a really good understanding of cybersecurity risk, there needs to be a granular understanding of how processes within your business are interconnected with others. If an organization focuses on fixing their foundational cybersecurity issues they can reduce their overall cybersecurity risks.

Organizations that prioritize cybersecurity recognize that by improving their foundation and expanding cybersecurity beyond their information technology (IT) teams along with embedding cybersecurity security in multiple areas of the business goes a long way in reducing cybersecurity risks.

Sincerely,

Mary N. Chaney,

Esq. CISSP, CIPP/US