Knueven, Schroeder & Co.
CERTIFIED PUBLIC ACCOUNTANTS
Jerome B. Schroeder, CPA
Douglas E. Schleucher, CPA
Ann E. Woolum, CPA
Timothy J. Gephart, CPA
Mark L. Schroeder, CPA
Richard D. Hillabrand, CPA
Angela L. Bursby, CPA
Jeffrey C. Quinlan, CPA

Balance sheet

CYBERSECURITY

By Brian Sampsel

Today's world is more interconnected than ever before. Yet, for all its advantages, increased connectivity brings increased risk of theft, fraud, and abuse. As Americans become more reliant on modern technology, we also become more vulnerable to cyberattacks such as corporate security breaches, spear phishing, and social media fraud. Complementary cybersecurity and law enforcement capabilities are critical to safeguarding and securing cyberspace.

Being online exposes us to cyber criminals and others who commit identity theft, fraud, and harassment. Every time we connect to the Internet, whether that be at home, at school, at work or on our mobile devices, we make decisions that affect our cybersecurity. Emerging cyber threats require engagement from the entire American community to create a safer cyber environment.

As with physical security, the motivations for breaches of computer security vary between attackers. Some are thrill-seekers or vandals, some are activists and others are criminals looking for financial gain. Additionally, recent attacker motivations can be traced back to extremist organizations seeking to gain political advantage or disrupt social agendas. The growth of the internet, mobile technologies, and inexpensive computing devices has led to a rise in capabilities as well as the risk to environments that are deemed vital to operations. All critical targeted environments are susceptible to compromise and has led to a series of proactive studies on how to migrate the risk by taking into consideration motivations by these type of actors. A standard part of threat modeling for any particular system is to identify what might motivate an attack on that system, and who might be motivated to breach it. The level of detail of precautions will vary depending on the system to be secured. A home personal computer, bank, and classified military network face very different threats; however, their underlying technologies that are being used are the same.

The Stop.Think.Connect. Campaign is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. Cybersecurity is a shared responsibility. We each have to do our part to keep the Internet safe. When we all take simple steps to be safer online, it makes using the Internet a more secure experience for everyone. The Campaign provides free resources available to everyone that are tailored to multiple demographics, including small businesses, students, educators and parents, and many others.

A successful cybersecurity approach has multiple layers of protections spread across the computers, networks, programs, or data that one intends to keep safe. Users must understand and comply with basic data security principles like choosing strong passwords, being wary of attachments in email, and backing up data.

In today's connected world, everyone benefits from advanced cyber defense programs. At an individual level, a cybersecurity attack can result in everything from identity theft, to extortion attempts, and to the loss of important data like family photos. Everyone relies on critical infrastructure like power plants, hospitals and financial service companies. Securing these and other organizations is essential to keeping our society functioning.

Items presented are not intended to be technically complete. Additional information may be required to make an informed decision. You cannot rely upon this information for avoiding tax penalties.