Master Custodians Focus on Cyber Security

Amed A. Avila, Managing Director and Relationship Manager

Fiduciary Trust International of the South

The Increasing Need for Cyber-Security

Advances in technology permeate all aspects of our lives, including how we communicate with one another, how we transact and move money and how we interact with financial institutions. In fact, extreme connectivity and the number of objects being computerized and connected to networks is reaching atmospheric heights.

Dubbed the "internet-of-things," it is the proliferation of everyday items—from watches, cars and appliances to industrial machinery, airplanes and roads—that are equipped with software to capture and transmit vast amounts of digital information. Gartner, Inc. has estimated that 6.4 billion connected things were in use worldwide in 2016, up 30% from 2015, and will reach 20.8 billion by 2020.

An Evolving Set of Risks

With this high online usage and connectivity comes an increased risk to information security. The internet-of-things results in significant amounts of data being collected about people and their lives. This means a rise in potentially insecure interfaces and heightened risk of unauthorized access.

Many of us have experienced some form of email hacking or identity theft, or at least know of someone else who has. Rarely does a week go by without reading about a private or government enterprise that has experienced a computer hack.

A focus on the security of computer systems has never been more important.

Defensive Mechanisms

As firms increase their technology-driven capabilities, many take important steps to ensure the right safeguards are in place to prevent cyber threats. Such controls may include 24/7 monitoring as well as intrusion tests and ethical hacks (engaging industry experts to attempt to hack their systems) to identify potential areas of weakness.

In addition, many firms are making it mandatory for employees to receive training on corporate policies and procedures for handling, transmitting and storing sensitive data, including technology that encrypts the information flowing between computers and servers. Encryption works by scrambling words and numbers before they travel across the internet so they can't be read or altered. Additionally, firms may also employ firewalls, a combination of hardware and software, to control the information that can pass from the internet to their internal systems and servers. Firewalls enforce a set of rules intended to bar intruders and viruses from gaining entry.

Protecting Yourself

While many firms are putting policies in place to limit cyber-threats, it's important to implement your own safeguards. These can include using strong passwords, and using different passwords for different accounts. Consider using a separate computer solely for online banking and shopping transactions. This can help limit viruses that can access computers through web browsing, social networking or gaming.

It is also recommended to periodically check financial accounts for signs of fraud. When using a smartphone, take advantage of the security options available, including the ability to remotely remove data from the device if it is lost or stolen.