Forbes

Forbes Finance Council CommunityVoice

Execs in accounting, financial planning & wealth management share tips

INVESTING 6/28/2017 @ 8:00AM | 143 views

Security Overhauls Are More Essential Than Ever For Financial Companies

POST WRITTEN BY
Shazir Mucklai
Writer at Inc. and USA Today. My firm specializes in helping companies raise capital and PR.

As every new data breach story hits the news, we become a little more horrified. We are surrounded by corruption, with hackers looming over every process. From email servers to bank accounts to the State Department itself, we are vulnerable, and the truth is that the IT security companies we trust to protect us have not evolved as fast as the hackers they try to guard against.

Traditional companies work on container-related asset protection, also known as “CRAP,” which is technology to protect containers such as third-party browsers, operating systems, file systems, server farms or cloud infrastructure. The model bars entry to the container, but does not address what you really want to protect: the data itself.

If hackers get past the top level of security, everything is at risk. And given the number and scope of recent data losses, it can’t be that hard to get past typical safety measures.

Shutterstock

For finance companies and their clients, a loss of data can be catastrophic. And yet, a 2016 PWC report on cybercrime found "only 37% of respondents – most of them in the heavily regulated financial services industry – have a fully operational incident response plan. Three in ten have no plan at all, and of these, nearly half don't think they need one."

The 2016 Security Scorecard had more alarming news for the financial industry. Key findings include:

- 75% out of top U.S. commercial banks are infected with malware.
- 95% out of top U.S. commercial banks have a low ("C" or below) security grade.
- Nearly 20% of financial institutions use a vulnerable email service provider.

Data is increasingly mobile. We copy data to flash drives, email sensitive information, download to smartphones and access files using public servers while sipping unicorn drinks at Starbucks.

Given the mobility of the data itself, protecting the primary container is only a small part of the security problem, but nothing has really changed — until recently.

New Companies Bring New Approaches

ClusterHQ is a young, California-based company that focuses on the fear of losing control of one's data while sharing it. They strive to guarantee strong data governance so the convenient mobility of modern data-sharing remains an asset and doesn't become a liability.

Certitude Digital is a small company that pursues a new approach to data security. Their solutions aim to protect the data itself through encrypted email systems, files that cannot be accessed except under predefined circumstances based on a long list of criteria you can define, and asset protection for downloads to ensure artists are compensated for their work.

Like many tech founders, Certitude's CEO, Scott Deaver, has grandiose ambitions for his company.

According to him, his solution is peerless in the marketplace. “We are not kidding in the least when we say we can solve almost every cyber-security problem known today with the same lightweight, inexpensive technology,” Deaver explained in a recent LinkedIn article. “The real story here is that of a simple solution (from a tenth-grade high-school dropout, no less) to one of the world’s most vexing problems, obvious and oh-so-logical in hindsight.”

The bottom line is simple: by any measure, in terms of company reputation, consumer trust, or real cost of a breach, it’s wiser to protect your data than to deal with a severe data breach.
