Cybersecurity Concerns for the Financial Industry: It's Worse Than You Think

Companies that operate in the financial sector have always faced some special challenges. It's not an easy industry.

Fickle and fluid financial markets, ever-increasing regulatory pressures, and a host of other risks and potential problems combine to cause some serious headaches for executives.

If your company is a financial institution, you have lots to worry about. It's a long list. And you can add one more relatively new threat to that list: cybercrime.

In fact, you'd be wise to move that threat to the very *top* of your list of concerns.

A Two-Trillion-Dollar Pie

In 2016, a *Forbes* article predicted that companies globally will share a pie worth $2 trillion by 2019. But you don't want a slice of that pie; that's the estimated yearly impact of cybercrime in 2019.

It's a pie that's growing rapidly.

If the projected $2 trillion is reached in 2019, that sum will represent a quadrupling of cybercrime costs in just four years. As the *Forbes* article notes, the term 'crime wave' doesn't quite convey the risks that companies face. It's more like a global epidemic; a pandemic.

The CEO of IBM has even labelled cybercrime as the greatest threat currently facing every company in the world.

It's Even Worse for Financial Companies

The specter of cybercrime should haunt the dreams of *every* company executive. But for finance execs, the threat of cybercrimes might chase away those dreams altogether, replacing them with sleepless nights.

Computer Weekly recently reported that the financial sector currently faces the highest number of organized cyberattacks, and that the threat is increasing at explosive rates. During a recent 12-month period, cybercriminal activity that focused upon financial companies increased by 40%.

Financial institutions are ill-prepared to withstand this onslaught of cybercriminal activity. According to SecurityScorecard's *2016 Financial Industry Cybersecurity Report*, 3 out of 4 top U.S. banks are currently infected with malware (multiple

varieties, in many cases). And the network security at almost all top U.S. banks is graded at “C,” or worse.

What types of cybercrime do financial institutions face? The list is long, but these are some of the more prevalent threats that specifically target the financial sector, as identified by the FBI:

- Account takeovers
- Third-party payment processor breaches
- Securities and market trading exploitation
- ATM skimming and point-of-sale schemes
- Exploitation of insider access

And the fastest-growing cyberthreat facing financial companies comes through advancements in mobile technologies.

More Risk from Mobile

The advent of mobile technology has been a game changer—in more ways than one.

Mobile technology has enabled work to be performed from any location at any time, enabling quantum leaps in worker satisfaction and productivity. But there’s a dark lining to that silver cloud: Mobility exposes your financial organization to unprecedented levels of risk.

No matter the strength of your in-house cybersecurity defenses, mobile devices are difficult to monitor, secure, and defend. According to a recent RSA white paper, nearly two-thirds of all fraud attempts occur through mobile devices.

As Wharton professor Kevin Werbach wrote, “It’s more difficult for corporate IT to manage and control something that leaves the building every night. The reality, though, is that workers want to use their own mobile devices, with their own apps, so fully locking them down is not an option.”

Quite simply, mobile technology increases the risk that your company will be forced to choke down a larger slice of that $2-trillion cybercrime pie.

Just Say ‘No’ to Dessert

The ongoing global cyber-crimewave has generated considerable heartburn for many financial companies. And adding insult to injury, many financial institutions have been served a side dish of humble pie to accompany their slice of the cybercrime pie. That’s what happens when a cyberattack slashes profits *and* diminishes public goodwill and consumer trust.

The unfortunate truth is that most companies are simply unprepared to thwart—or even detect—the highly sophisticated cyberthreats that are part of today's technological landscape. (A recent IBM study revealed that two-thirds of companies ***know*** that they aren't prepared to handle cyberattacks!)

If your company's cybersecurity defenses aren't adequately equipped to defend against cybercrime, it's time to act—or prepare for a very unpalatable serving of pie.