The Cybersecurity Threats Presented by Financial Services Remote Employees

Security and IT professionals at large enterprises across all industries are faced with the daily task of having to secure an expanding attack surface. Vulnerable points of entry used to live within the organization's walls, where firewalls and inline security tools could protect them. But networks have now evolved into a constantly evolving, borderless environment thanks to cloud usage, the Internet of Things (IoT), and an increasingly mobile workforce.
Technological advances, paired with a surge of digitally savvy employees flooding the workplace, has led to more individuals working from home or other out of office locations, and doing so on an increasingly diverse array of connected endpoint devices. And, while it may come as a bit of a surprise, this rise of the mobile workforce has even become commonplace in highly regulated industries like financial services.
Let's take a closer look at some statistics around the financial services mobile workforce, the threats that security teams are faced with as a result, and what can be done to strengthen cybersecurity in financial services.

Financial Services Employees on the Move

When a group of global business leaders were asked what percentage of their workforce would be working remotely by the year 2020, about a third (34 percent) said that they'd expect more than half to be doing so. Even more striking, 25 percent said more than three-quarters would work outside the office by the turn of the decade.
The technological capabilities (cloud services, file sharing tools, etc.) are already in place for this shift to become a reality.
Additional data reveals that nearly two-thirds of employees use their own personal devices to do work, thereby blending their work and personal lives, and also increasing the chances that they're using productivity applications and tools, often cloud-based, that may not be approved by the enterprise (such as Dropbox).
While worker flexibility and technological tools may enhance productivity, recklessness can be detrimental to an enterprise's reputation and bottom line. The same dataset shows that 69 percent of all employees ignore corporate policies and use unauthorized, and often unsecured, free file-sharing services to access and send out corporate files. In fact, more than three-quarters (78 percent) of employees in the financial services industry are reported to be using free file sharing applications.
In terms of mobile workers, 45 percent of employees claim that they are not concerned about the security of business data they store and access from mobile devices, often believing that the security on these devices, or the online applications they are using, is either good enough, or someone else's responsibility.

The Threats Presented by Remote Employees

The financial services industry has consistently been one of the most popular targets for cybercriminals, as the value of its data can go a long way on the Dark Web. Now, with a growing number of financial employees taking their work home with them, it has become an even more attractive target.
Employees using their tablets, mobile phones, personal laptops, and file sharing services to access sensitive information all contribute to a rising number of access points, resulting in more open doors through which cybercriminals are able to gain access to valuable data. In addition, remote employees often times fall victim to phishing scams, or have their devices hacked due to weak authentication methods, creating new security challenges for corporate IT teams.
With all of this in mind, it should come as no surprise that one of the largest thefts of customer financial data in recent memory stemmed from cybercriminals gaining access to an employee's computer as they worked from home.

Protecting Against Cyberthreats Presented by Remote Employees

Financial services organizations need to make sure they're up to the task of protecting their expanding ecosystem of networks, and its often highly mobile data from cyberthreats. To do so, they must have solutions in place that can defend against today's sophisticated attacks.

Today's threat actors can strike at anywhere and at any time. Organizations need to strengthen their security posture, identify where their critical assets are located, and respond to threats in real time. Security fabric solutions are integrated to allow IT teams to monitor threats across the borderless network and wrap all security devices into a single management platform, providing the access and visibility needed to have success.