Cybersecurity for digital financial service

Law, Security

New digital technologies are innovating financial services for people and businesses faster, cheaper, and more conveniently than ever before—perhaps more so than in any other industry. A remarkable feat is how this is expanding access to financial services to previously unbanked and underserved populations at a remarkable rate.

Some large “ legacy” financial institutions are struggling to keep pace with the revolution, while more flexible non-bank innovators such as digital financial service providers offer biometric ID authentication, online loans, robo-advisors, cryptocurrencies, and other online services at dizzying speed. These technologies allow service providers to not only offer a wider range of services with greater reach, but also improve their own efficiency and lower their operating costs.

Slow or fast, they all face a common threat: the “ dark side” of cyber-insecurity. The rapid growth of online platforms makes the digital financial service industry and its customers uniquely vulnerable to breaches in IT security networks.

A fine regulatory balance is needed; one that enables innovation, protects the business community, and ensures safe services for customers whether they are young, urban, and tech savvy, or older, rural and opening the first bank account of their life.

Financial information is an increasingly attractive target for cyber criminals

Digital financial service providers are often quick and flexible because they may not be subject to the same laws and regulations as traditional financial service providers.

They know consumer trust is critical to their success and cybersecurity is critical to trust. But in this hyper-competitive space, some may also see the concept of security-by-design as an overhead cost and a barrier to consumer adoption.

That can leave consumers' funds as well as the vast amounts of increasingly valuable information collected when they use these services—from sensitive personal information to financial records and online spending behavior—at risk.

Yet many consumers, unbanked or otherwise, don't understand cybersecurity in all its permutations and are especially vulnerable to hacking if targeted.

Combined with growing consumer expectations, a long-term view of trust, safety, and confidence is needed in the online environment. We need to find a balance between protecting consumers, enabling innovation, and encouraging cybersecurity as a consumer value proposition, while promoting consumer personal responsibility. These points do not need to be mutually exclusive.

The greatest challenge becomes to detect well-cloaked threats rather than react when the have become imminent.

The best way to incentivize development of the financial services ecosystem is through profits and good social outcomes. Digital financial service providers who fail to offer adequate safety and security measures face imminent failure. As such, authorities should consider a self-regulatory framework that encourages digital financial services to offer current and potential clients cybersecurity using known frameworks and simple communication.

Online platforms make it easy for plugged-in customers to shop around for services and easily post online reviews. While most comparison will be based on individual requirements—including price, availability, and product differentiation—consumers should be encouraged to also consider online trust and safety issues.

A healthy online financial service marketplace should highlight the pros and cons of specific offerings, and provide customers with redress options when expectations are not met. With enough negative reviews, public trust wanes, tarnishing a company’s reputation and undermining its bottom line.

Innovative financial services products will continue to find new customers, particularly through mobile smart devices. Some of the unbanked and underserved entering this online environment will fall victim to phishing, scams, and bullying.

Empowering this next cohort of customers will require education, tools, and techniques to make them competent digital citizens, reduce bad online experiences, and allow them to participate and gain from digital innovation.

Smarter and more responsive measures are needed to maintain trust, safety, and confidence in the financial services industry

Even as businesses aim to safeguard data, it is the human factor in cybersecurity that makes businesses vulnerable from within. Taking cybersecurity requirements lightly can lead to significant consequences for businesses and organizations, and employees—whether innocently or willingly—are often contributing to the problem.

The human factor played a major role in the 2017 spread of the WannaCry ransomware that endangered businesses worldwide.

WannaCry exploited a vulnerability in a Windows operating system file-sharing protocol. But even two months after the disclosed vulnerabilities had been patched with new updates from Microsoft, many users had still not updated their systems. The weakest links were non-IT personnel: Employees with local administrator rights were found to have disabled security solutions on their computers, letting the virus spread to entire networks.

To boost cybersecurity, both digital financial service providers and the traditional banking sector need open communication. Openness is also needed between the public and private sectors. Greater transparency can protect the financial sector against inevitable cyberattacks and help mend bridges between society and government.

It will take the right mix of innovation, competition, and regulation to bring light to the dark side of digital financial services. Digital financial service providers and regulators will need to work together to secure the open, digital financial ecosystem upon which sustainable economic growth will depend.