The Future Of Cyber Threats

cyber security risk management

Summary: A recent Accenture report describes how various threats could evolve in the future. We give you the highlights.

Digital transformation is all the rage right now as financial institutions work to retool themselves to meet fintech and other competitors head on. The goal is to maximize/better leverage human resources, as you streamline/automate basic processes and enhance the customer experience along the way.

As your team works to do that very thing at your bank, a recent Accenture report serves as a good reminder to also keep a close eye on digital security too. The report discusses how various threats could evolve in the future, so understanding where financial institutions are most vulnerable is a good starting point.

Threat No. 1: Credential and identity theft. Incidents of stolen system credentials and consumer data are becoming more frequent, sophisticated and larger-scale. The possibility of thieves using compromised credentials to simultaneously attack multiple entities is becoming a more potent threat, according to the report.

Threat No. 2: Data manipulation. Many banks today are on guard against data theft, a nettlesome problem in which cyber criminals delete or disrupt access to data. But banks also need to guard against data manipulation. The latter is much harder to detect--often because changes are slight enough to go unnoticed, but large enough to wreak havoc. Countermeasures aimed at early detection are becoming increasingly more important. Financial institutions that keep careful track of their data from the origin and throughout its life cycle will be better situated to certify and recertify the authenticity of their data.

Threat No. 3: Malware. In recent years, financial services organizations have been among the most targeted in ransomware attacks. The attacks have been and continue to be more sophisticated, and some will even fight back after they are detected. This raises the stakes. Data manipulation and theft, followed by ransomware or a wiper malware, makes it all the more difficult to perform forensics, halt attacks, and purge interlopers from systems. Accordingly, stay on alert against destructive network attacks that seek to destroy and corrupt.

Threat No. 4: Emerging technologies. As financial institutions dabble with new technologies, they need to remain vigilant against emerging threats. Accenture notes a rising number of attacks seeking to exploit machine learning models. Blockchain has become a target for cyber thieves and more opportunities may surface, as banks continue to explore applications of newer technologies.

Threat No. 5: Disinformation. Troll farms, Twitter bots and fake news are all areas of growing concern. In January 2019, a firm was targeted by an intricate hoax involving a spoofed letter in the CEO's name. Complete with a fake webpage and mass distribution techniques, the incident serves as a stark warning of how easy it is to launch an effective disinformation campaign. Central banks around the globe are attempting to batten down the hatches against such attacks, but the threat remains potent.

Only by understanding these rising threats, collaborating with third parties, investing in people, security, processes, and strengthening defenses, can financial institutions help make these types of devastating attacks

less likely.

AUTOMATED INTERNATIONAL SERVICES FOR YOU

Community banking teams can automatically send international wires using existing domestic platforms. Learn more by contacting us today.