Financial Services: A Complex Industry with Simple Cyber Threats

Cybersecurity Series

By Tony Lutz, Chief Technology Officer
Financial Service, Verizon Business

The financial services industry today is highly complex. From exotic derivatives to collateralized loan structures, the more complicated financial instruments are inaccessible to the financial layperson. This complexity may lead one to assume that cyberattacks targeting the financial sector, including retail banks, must be equally sophisticated to succeed. In reality, some of the most widespread attacks are simple, but that doesn't make them any less effective and serious.

Simple attacks can cause huge problems for financial institutions, including widespread breaches that leak both personal and financial information of their customers. Leaked information not only represents a potential immediate risk, but it can also present ongoing challenges, such as credential stuffing, a cyberattack method in which hackers use the identifying information to gain access to user accounts on other systems. These breaches can exact a huge reputational toll as well as cause great financial damage.

Sometimes, the most effective attacks are the simple ones

Compromised credentials

According to the 2023 Data Breach Investigations Report (DBIR), nearly half of all breaches (49%) in the financial sector are attributed to compromised credentials. They can be obtained through a brute-force attack, in which a hacker attempts to guess a password based on contextual information, sometimes aided by automation tools — hardly a sophisticated method. A bad actor may also obtain a password that was already leaked in a previous hack, a tactic known as credential stuffing.

Basic password authentication does not offer sufficient protection against these kinds of hacks. It's essential to use multi-factor authentication. It's a straightforward solution for a straightforward attack, but rolling it out across an organization, especially a large

one, is not simple. Implementing a phased rollout, with administrators upgrading before the entire team will allow them to educate the workforce about the changes. Engaging a provider that specializes in these kinds of rollouts can also improve adoption. Thankfully, there are simple and effective solutions that we offer our partners in support of cleaner cybersecurity practices. For example, Verizon has an identity and access management consulting team focused on multi-factor authentication solutions that can help make it more difficult for bad actors to access sensitive data.

Basic web application attack

This is the most prevalent pattern in this sector and another attack type that can be used to obtain payment card information. Because web applications are often accessible from anywhere–and by anyone–with an internet connection, they can be an easy target for remote attackers. And, because web applications often handle sensitive information, such as login credentials and financial data, they're a very attractive target. As web applications become susceptible for intrusion, this attack usually involves stolen credentials to gain access — in 86% of basic web application attacks across all industries, in fact. While these may be simple attacks, they can lead to complex challenges.

These kinds of attacks are seldom isolated, often leading to breach escalation. Attackers can use existing access to conduct additional attacks, including introducing ransomware or other malware in an endpoint, which can then spread across a network. That's why it's so important to regularly test and scan for any vulnerabilities within the system to rectify immediately and regularly update cybersecurity software.

Misdelivery

This may not be a malicious attack, but it's a data breach all the same. Misdelivery, the most common error in this sector, refers to transmitting either electronic or paper documents, sometimes with sensitive information, to unintended recipients. This error type highlights a broader vulnerability –- people. The human element factors in the vast majority of incidents and almost three-quarters (74%) of total breaches.

Training employees can help mitigate the impact of the human factor. Making sure staff are updated on the latest security policies, including how employees should handle critical data, how it can be shared, and who can access it, can help reduce incidents of misdelivery.

Breaches cause as much reputational damage

Consumer data and bank account information account for 74% of the overall impact. Payment card data, one of the most common data types, amounted to more than a third (37%) of breaches this year. This is a lucrative market for hackers, as evidenced

by how widespread it is, but its financial impact on banks and lenders can be matched by the reputational damage of such breaches.

Trust in the financial industry is paramount. Financial institutions have to protect their reputation just as much as their assets. Consumer skepticism of the financial industry persists following the Great Recession of 2008. Widespread breaches, in which the personal information of huge numbers of consumers are compromised, represent enormous financial losses and debilitating reputational damage, and can even open larger organizations up to additional regulatory oversight. Financial institutions have no choice but to redouble their security measures to protect sensitive consumer information and financial assets if they're to avoid scandals moving forward.

Keep it simple

If you're looking to help mitigate cybersecurity risks in your business, remember these three steps:

1. Start with data protection and implementing strong encryption protocols to help safeguard your sensitive financial data.
2. Enforce access security, including implementing multi-factor authentication for accessing critical systems and providing a comprehensive cybersecurity training to all staff members.
3. Conduct routine security audits and assessments to help identify vulnerabilities and potential threats and develop a well-defined incident response plan to handle potential breaches effectively.

The digitalization of the financial services industry, as with virtually all industries, has brought incredible benefits, but it has also created new potential points of entry for threat actors. Putting common-sense cybersecurity protocols and solutions in place is an absolute necessity, and the key to success is prioritizing.

System intrusion, a more involved attack pattern than those listed above, is a top-three pattern in the sector, but it's on the decline. Responsible for more than a quarter (27%) of breaches last year, system intrusion represented just 14% of breaches in this year's report. System intrusion still represents a serious threat and proves that threat actors are still willing to bring out their more sophisticated techniques, but increasingly simple mistakes are taking their toll and simple attacks are finding their targets.

Organizations should defend against the more complex attacks too, but they can't underestimate or overlook the simple attacks, especially when they're proving so effective. If the easy approach is working, what's the motivation to change? So, don't make it easy on them.