Cybersecurity in Financial Services Requires a Fresh Data Management Approach

Modern

Data management isn't just a competitive differentiator in banking and financial services — it's a core business requirement. Despite financial services changing rapidly in response to global disruption and new technology, the industry's data remains a key protected category in privacy regulations. Companies found to be out of compliance can experience devastating consequences, but a new data management paradigm can help banking and financial services protect data better than ever.

Data Risks in Financial Services

For the industry to evolve, it must put data in motion and rely on real-time insights to make decisions that once took days to make. However, opening data up to more stakeholders also creates security loopholes with potentially catastrophic consequences. The same data that makes it possible for banks to issue faster decisions for credit cards can also provide threat actors with everything they need to steal identities.

The consequences can be dire. According to a recent report by Allianz, the biggest non-financial threat to financial services isn't the pandemic disruption or the economy — it's cybersecurity incidents. Cyberattacks are the leading cause of value loss, and changing regulations continue to increase the fines and sanctions associated with successful cyber attacks. In fact, the average cost of cybersecurity events in financial services is estimated to be 40% higher than other industries, so finance leaders are well aware of the stakes. The challenge lies in knowing what to do.

Common Threats to Financial Services

Threat actors use a variety of methods to gain access to sensitive data. And while gaining access to financial data is the primary target, hackers also go after personal data to make it easier to steal identities in more than one location. Attacks come through these common avenues:

Ransomware
Ransomware is typically high risk/low reward for threat actors. Even with continuous data backups, ransomware is a risk because hackers can simply leak sensitive data if companies don't pay up or coordinate denial of service (DoS). In financial services, the threat of data leaks or losing services is just as bad as losing access to data.

Phishing
Phishing-as-a-Service has made it possible to deploy high-level phishing attacks without hacking the target's network. These spoofed websites, emails, and sign-in pages look authentic, leading to stolen credentials and data loss.

Web Application Attacks
Just because hackers don't need to attack the network directly doesn't mean they won't. Web application attacks are also common in the financial industry and often come from loopholes located with third-party vendors and partners.

Vulnerability Exploitation Attacks
Log4J, a significant vulnerability revealed just last year in late 2021, has many industries reeling and is a good example of what can happen when vulnerabilities aren't addressed. Vulnerability exploitation happens when threat actors gain access through security loopholes and then can move through the network to gain higher privileges and cause more damage.

Distributed Denial of Service Attacks
Threat actors can coordinate attacks by overwhelming the network from various device locations and preventing customers from accessing services. Interrupting daily operations can cause a loss of revenue and trust from financial services consumers.

Insider Attacks and Negligence
A lack of training and human error can cause security risks. In addition, disgruntled employees can also set off a series of events that lead to vulnerabilities. Even with safeguards in place, financial services often exist in a series of silos without visibility throughout the network.

Protecting Financial Services Begins With Visibility

The banking and financial services industry is undergoing a change in its cybersecurity maturity. Visibility into the network is a significant component of creating a cybersecurity plan that's proactive against emerging threats while continuing to protect against existing ones.

Visibility includes understanding where data is located, who is using it (including machine identities), and what dependencies exist. This due diligence helps reduce the rate at which an anomaly remains undetected for long enough to cause damage.

With the proliferation of "open banking" or services provided by third-party partners with access to customer data through data sharing, visibility is even more critical. Consumers expect, and in some cases, demand, these services, so the finance industry must determine how to provide them safely.

In addition, basic security standards can help reduce threats as well. Consistent, enterprise-wide native governance with granular controls can help financial services continue to provide data for daily operations — including third-party services — while ensuring security. Fewer security loopholes exist when leaders can apply these standards down to the granular level through a single dashboard.

Management and Reporting Form the Second Step

Once a financial services company has implemented universal governance controls and audited operations, automating reporting and management processes is the next phase. Security is not a one-time thing. It changes with new and emerging threats as technology evolves.

Excellent reporting and documentation help financial services companies identify and understand vulnerabilities. They should have a bird's eye view of the ecosystem through one organizational layer. Linking all tools, data sources, and applications helps companies reduce their attack surface and better control sensitive assets.

Better employee training is certainly part of the solution, but finance companies also need a scalable data management layer that evolves as the company does. This operational layer brings together everything within the data ecosystem so that visibility and reporting have no blind spots.

Leveraging a Data Operating System Is the Solution

A data operating system like The Modern Data Company's DataOS will tie everything together — data sources, third-party vendors, new tools, and legacy systems. A unified ecosystem helps make it harder for threat actors to gain access in the first place or escape detection once a security loophole is exploited. DataOS scales and evolves with the company, gets better over time, and changes the entire governance paradigm for a simplified approach to complex data.

To discover more about how DataOS is changing cybersecurity and data management for the banking and financial services industry, contact us for a demo to see it in action.

Schedule a demo →

BY E. WALLACE

TheModern DataCompany

The Modern Data Company
306 Cambridge Ave
Palo Alto, CA 94306
TheModernDataCompany.com
info@TMDC.io