rubrik

Financial Services Sector Sees 13x Spike in Cyber Attacks

Ransomware threat, geopolitical tensions, and new regulations require zero trust approach

Ransomware attacks have grown dramatically over the last several years with the financial services industry particularly hard hit. ZDNet recently noted that attacks against banks were up a staggering 1,318% from 2020 to 2021.

$18.9M
average loss to a financial services company in the event of a ransomware attack

2ND
highest cost of a data breach per industry

1,318%
increase year over year in ransomware attacks

NEW CYBERATTACK REPORTING REGULATIONS

In response to the heightened threat, regulators around the world are increasing requirements for disclosure of cyberattacks. In the United States, the Federal Deposit Insurance Corporation (FDIC) requires banks to report an incident that has or is likely to affect operations, services, or the finance sector no more than 36 hours after the breach occurs. All banks must comply with these requirements by May 1, 2022.

GROWING GEOPOLITICAL TENSIONS

The current geopolitical environment has further increased the risk of cyberattack. As a result, in March 2022 the Biden Administration issued a statement encouraging all private sector companies to strengthen cyber defenses and signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 with reporting mandates for many industries, including financial services.

HOW SHOULD YOUR ORGANIZATION RESPOND?

All financial services companies must audit operations regularly to ensure compliance. Given the elevated threat levels and new regulations, it's important to reassess your cybersecurity posture to ensure that you are taking all necessary precautions to protect critical services and data—and that you are able to satisfy any new reporting requirements you are subject to.

The new 36-hour reporting requirement in the US stands to increase the costs of cyber risk management. Any increase in costs must be weighed against the reputational damage that would result from a successful attack or failure to meet disclosure requirements or both.

ZERO TRUST DATA SECURITY PROTECTS AGAINST RANSOMWARE AND OTHER CYBER THREATS

Zero trust data security assumes all users, devices, and applications are untrustworthy and may be compromised. By adopting a zero trust approach, organizations can enhance cyber defense and:

- Reduce the risk of intrusion
- Discover and manage sensitive data
- Prevent tampering with backup data
- Detect anomalous behavior

With zero trust data security, you can more quickly detect attacks, assess the extent of the damage, and recover quickly. As a result, your organization is better able to comply with new regulations, while controlling cyber risk management costs.

Rubrik, the Zero Trust Data Security Company™, is uniquely positioned to help financial services companies of all sizes protect against ransomware threats. Rubrik is so confident in its capabilities that we offer a recovery warranty up to $5M. For more information on Rubrik and zero trust data security, visit our financial services page.