

A High Bar for Cyber Recovery in FinServ

More Vigilance, Discipline, and Thoroughness Is Needed

Purveyors of large volumes of money and sensitive data, modern financial services operations must protect diverse and complex IT infrastructure, often changing at an accelerated pace and requiring more dynamic and resilient cybersecurity strategies. Enterprise Strategy Group research showed that, when compared to organizations in other industries, FinServ organizations often achieve higher results when it comes to overall cyber recovery. But it's important to recognize that for the FinServ industry, the bar is higher and requires more vigilance, discipline, and thoroughness, putting a strain on IT and security teams to deliver and achieve adequate levels of cyber resilience.

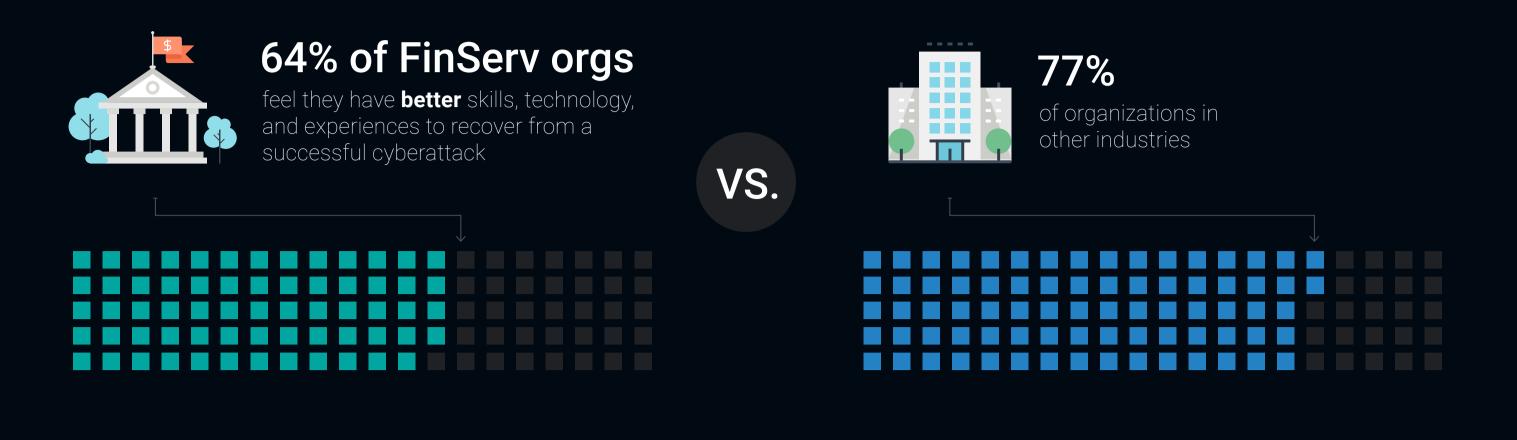
This Enterprise Strategy Group Infographic was commissioned by Commvault and is distributed under license from TechTarget, Inc.

Unique Cyber Recovery Issues for FinServ Organizations

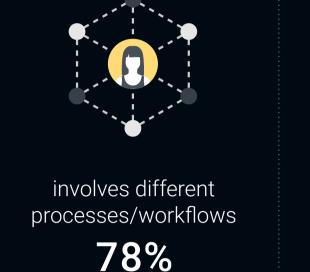
FinServ Organizations Feel Less Prepared to Recover From Cyber Incidents Than Organizations in Other Industries

In the aggregate, organizations' confidence in dealing with cyber incidents has eclipsed disasters. While the concept of cyber recovery is more nascent, the volume of cyberattacks and their potential damage have pushed organizations to rapidly build up their defenses and processes for response.

This dynamic holds true in the FinServ industry, but it is less pronounced than in other industries, indicating that FinServ organizations have lagged in pivoting their focus from natural disasters toward cyberattacks.









67%



involves different SLAs **62%**



takes more time **57%**

FinServ organizations also report more often that cyber recovery plan testing is challenging:



32% said they lack the clean, hardware test environment suitable for formally testing a full recovery.

Cyber Resiliency Confidence and Results



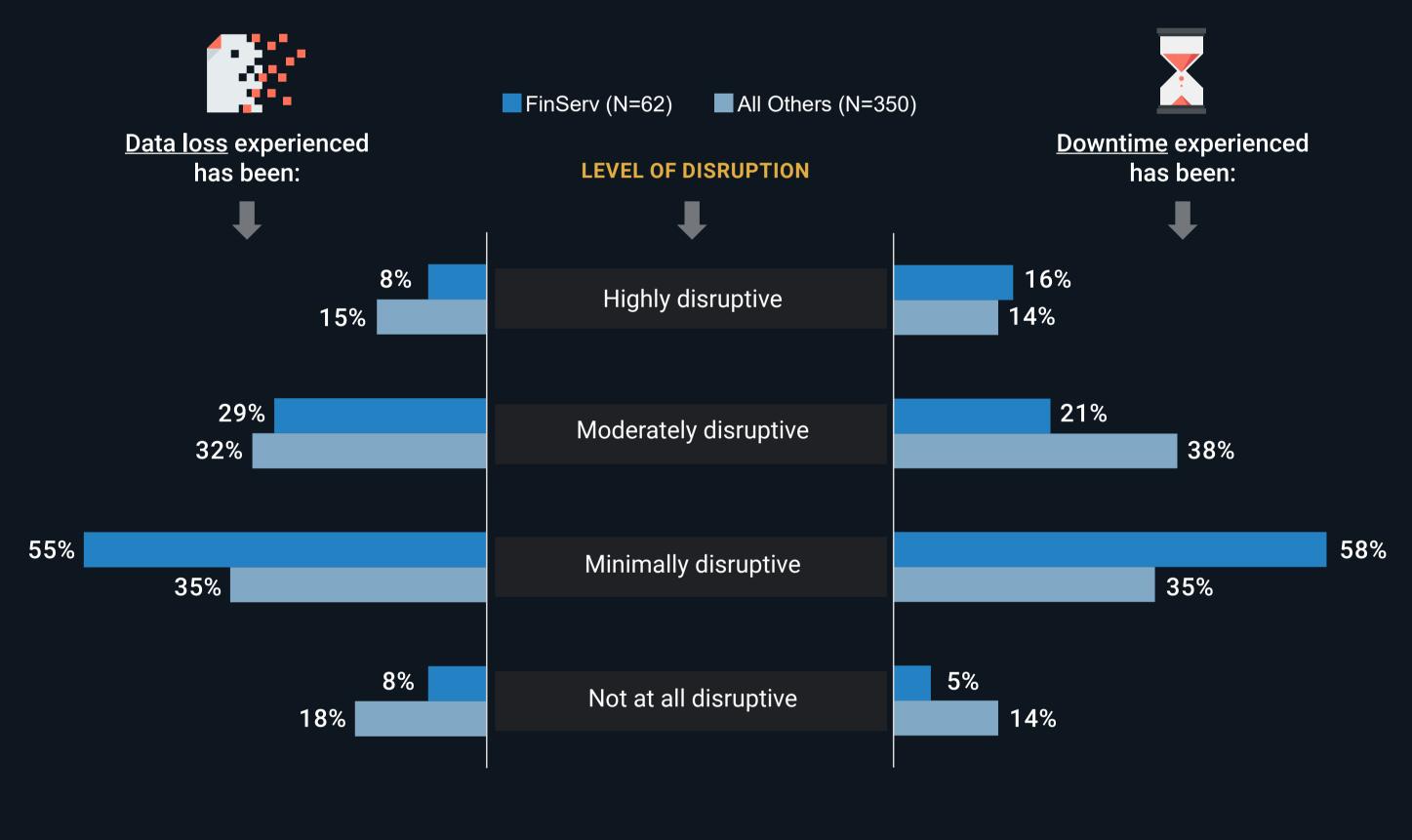
While FinServ orgs are

2x more confident

than organizations in other industries that their cyber recovery plans are able to protect all the apps and data the organization needs to remain operational (36% vs. 17%), these numbers are still relatively low, highlighting that work is still needed to achieve business continuity objectives.

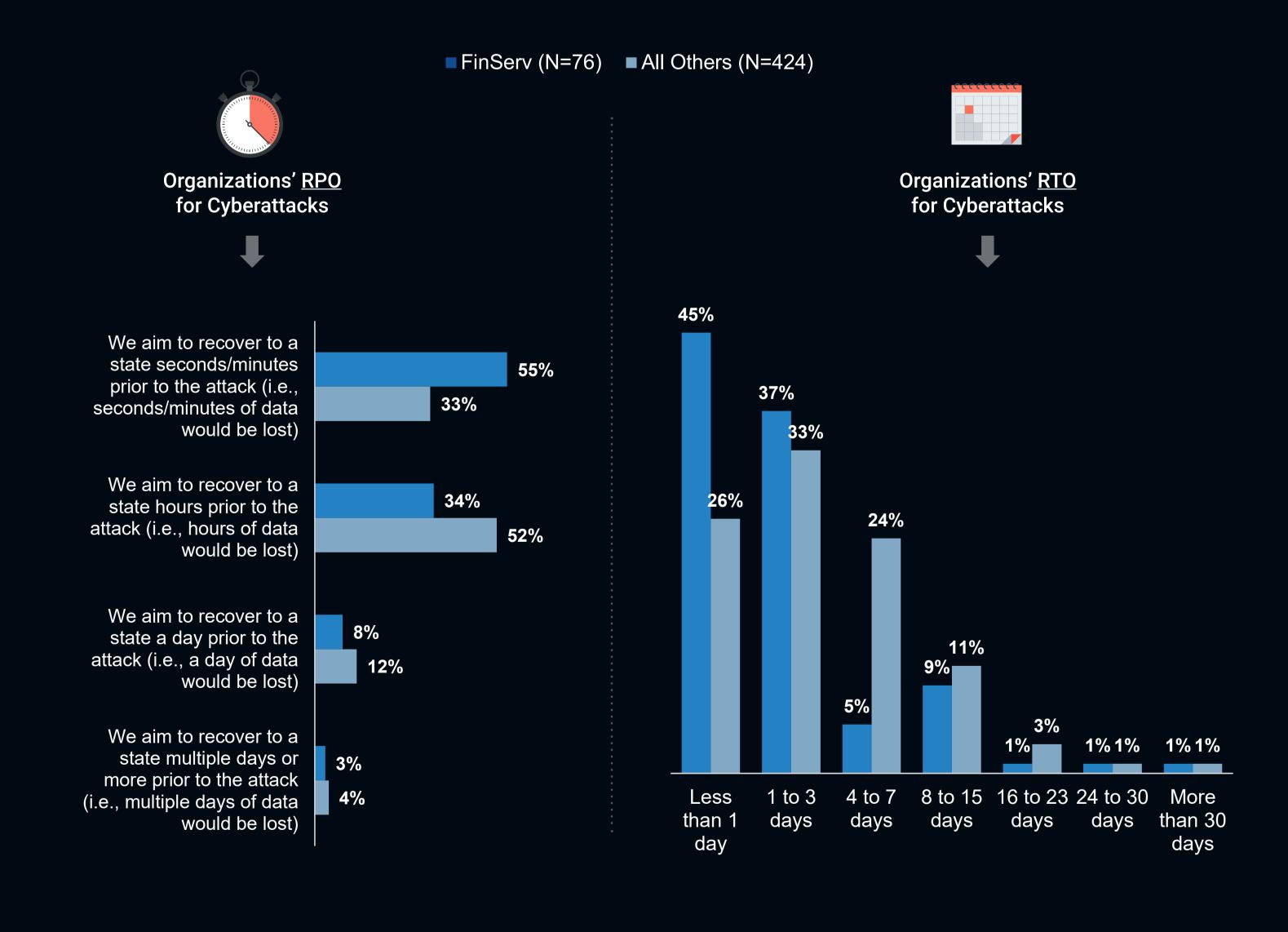
Data Loss and Downtimes: Dealing With Disruption

While most cyber recoveries are deemed successful in terms of meeting SLAs (75%, on average, across all respondents, and 77% among FinServ specifically), 37% said either downtime or data loss associated with recent attacks has been moderately or highly disruptive.



A High Bar

In the aggregate, only 36% of organizations targeted seconds/minutes of lost data. And in terms of outages, only 29% of organizations in the aggregate maintained an RTO associated with cyberattacks of less than a day. However, in both areas, FinServ firms targeted shorter SLAs much more often.



"We believe this is driven by the fact that the loss of financial transactions can result in widespread impacts to both firms' operating objectives and customer financials. In turn, **these more aggressive SLAs likely drive greater investments and a culture that prioritizes rapid recoveries**, which both likely help FinServ firms' performance."

Dave Gruber, *Principal Analyst, Ransomware, SecOps & Services*

Cyber Recovery: Critical to Cyber Resilience

Cyber resilience has become a mainstream objective for IT and security leaders alike. In examining the data from the FinServ industry specifically, these organizations' propensity to be subject to more stringent regulations, be more sensitive to outages and data loss, and operate extremely complex environments may be contributing to high levels of anxiety.

However, even as organizations in the FinServ industry "feel" less prepared than their peers, they comparatively enjoy better outcomes in practice. The bar is high, and the complexity continues, requiring FinServ organizations to continue investment in strengthening skills, discipline, and technologies that can support more aggressive SLAs, recovery testing, and overall operational cyber resilience.

Safeguarding and governing financial data provides FinServ organizations with a competitive edge. Learn how Commvault's cyber resilience solutions help protect, recover, and maintain continuous business operations.

LEARN MORE

