Defend Your Stored Data Against Cybercriminal Attacks

cyber security ransomware

Summary: With big threats of ransomware, financial institutions rely on their back-up systems to avoid paying a ransom and indemnify them, if their systems are not unlocked by the thieves. This has prompted cybercriminals to go straight to the source and target stored data. With 69% of financial institutions stating that an attack on their stored data would have a catastrophic effect on their business, data protection is critical. Here are three ways to do it effectively.

Confucius is credited for saying, "*It does not matter how slowly you go, as long as you don't stop.*" Well, that may be true for some things, but definitely not in fighting cybercrime. The entities that work slowly to protect their data will get hit time and time again by crafty cyberthieves.

Many community financial institutions (CFIs) are working hard and fast to store their data away from the bad guys. However, it has become more challenging as these thieves find vulnerabilities leading them even into data back-up systems. We bring you up to speed on the ongoing risk of data breaches and how best to protect your institution against them.

Ransomware attacks have doubled

In the past several years, as ransomware has become more prolific, financial institutions have become increasingly dependent on their systems of backups, to avoid paying a ransom and indemnify them, if their systems are not unlocked. According to cybersecurity vendor Kroll, ransomware attacks increased more than 2x from Q1 2021 to Q3 2021, hitting 46% vs. 20%.

"*An ounce of prevention is worth a pound of cure when it comes to ransomware,*" says Ioan Peters, managing director and co-regional lead in EMEA for Kroll's cyber risk practice, "*so we encourage all businesses to constantly evaluate the security controls they have deployed, rather than waiting for an incident to occur.*"

Stored data is the target

Yet, knowing that financial institutions (FIs) and other enterprises have gotten wise to the growth of ransomware attacks, many cybercriminals are starting to go right to the source. They are now hitting the stored backups that would allow these companies to more easily recover in the case of a ransomware attack, without paying the ransom. Meanwhile, 69% of financial services institutions say that an attack on their backup or stored files would have a "significant" or catastrophic effect on their business, rendering them unable to easily come back from a cyber onslaught, according to a report released recently by data storage provider, Continuity.

In fact, nearly 60% of financial industry respondents say they are "not confident" in their enterprise's ability to recover quickly or easily from a ransomware attack even if they are regularly backing up vital customer data and other files. Continuity surveyed 200 FIs in 45 countries and found that many FIs have yet to reach a

"mature" level of data backup. The latest warning from the Department of Homeland Security on Russia's offense cyber tools for attacks on infrastructure underscores that data protection is more critical than ever.

"*When organizational data is compromised, the last line of defense lies in the storage and backup environments,*" the Continuity report states. "*In the financial and banking industries, digital data worth may be so high that a well-orchestrated attack on both storage and backup could wipe out a significant amount of the organization's value, potentially affecting entire economies.*"

With the stakes so high, what can a CFI do?

1. **Perform regular IT security audits, specifically including storage and data backup.** This is the best way to stay on top of breaches and vulnerabilities. Ensure that there are procedures focused on data storage best practices, especially as backup options and technologies continue to develop. More than two-thirds of financial institutions surveyed by Continuity said that securing storage and back-up systems have been specifically addressed in recent external audits.
2. **Prioritize incident response planning.** CFIs must accept that ransomware threats, like breaches in general, are not a matter of "if" but "when." Incident response planning around ransomware attempts is essential, even for smaller institutions. Staying on top of the latest threats and monitoring your systems continuously will allow you to perform the most effective incident management. This frontline of defense helps prevent major issues in the back end i.e., for data storage and backup.
3. **Unify IT teams.** Having your information technology staff collaborate on their projects and tasks will help cover all aspects of cybersecurity at your institution. With silos of responsibilities, gaps can happen. Sharing knowledge is key in combating cyber threats. "*Sooner or later, every organization will experience a security incident, especially since cyberattacks from phishing and social engineering are only getting worse now that so many people are working from home,"* says Nick Santora, CEO of Curricula, a security awareness training provider. *"The key is knowing how to respond to that incident.*"

INTERNATIONAL SERVICES TO GROW WITH YOUR CUSTOMERS

Capture more customers and increase fee income with our international services. Contact us today to learn more.

ECONOMY & RATES

Rates As Of: 02/15/2022 05:40AM (GMT-0800)

Treasury	Yields	MTD Chg	YTD Chg
3M	0.43	0.21	0.37
6M	0.76	0.27	0.57
1Y	1.11	0.33	0.73
2Y	1.58	0.41	0.85
5Y	1.94	0.33	0.68
10Y	2.03	0.25	0.52
30Y	2.33	0.23	0.43
FF Market	**FF Disc**		**IORB**
0.08	0.25		0.15
SOFR	**Prime**		**OBFR**
0.05	3.25		0.07