FS-ISAC

Executive Risk Report

17 April 2024 EP - 04 - 2024

Recommended Distribution | Chief Executive Officer | Chief Compliance Officer | Chief InfoSec Officer | Chief Resilience Officer

How to Survive a Severe Cyber Outage

Most financial organizations have mature disaster recovery (DR) and business continuity (BC) plans, yet they are still unlikely to survive a devastating cyber attack that wipes out all operational systems and data.

This is an issue the US financial regulators and a broad collection of leading financial institutions recognized back in 2015. Which led to the creation of Sheltered Harbor, the leading financial services standard setting and certification organization, that enhances cyber resilience in the global financial system.

Its primary goal is to solve the challenge of maintaining public confidence should this scenario ever arise. A scenario that is ever more likely with the interconnectedness of the financial industry and severe escalation in cyber attacks globally.

These leading financial institutions determined that it is possible to survive a devastating cyber attack, however, it is only likely with comprehensive cyber resilience preparations that fit neatly into existing resilience practices in BC and DR. The FFIEC updated its manuals to reflect these.

One of the benefits of preparing for the worst is that you also prepare for less severe cyber attacks. For example, in the US Cybersecurity and Infrastructure Security Agency's Ransomware Guide, first mitigation step is to "Maintain offline, encrypted backups of critical data."

This is something that implementing Sheltered Harbor's defined set of standards will ensure. Meaning that your critical data will still be available, even if a catastrophic "zero-day" cyber attack, data corruption, or data deletion event occurs, causing critical systems, including backups, to fail.

With secure, immutable data, you'll be able to provide essential services to customers within 24-36 hours, providing a lifeline to survival, while you reestablish normal operations.

Planning For Survival – Steps to Take

Preparing today, by effectively securing your customers' data and reassuring them that their assets will always be accessible, is the key to surviving any severe cyber incident.

To achieve this, organizations must have a resilience plan. Validate your plan. Train staff on your plan. Educate your customers and stakeholders on what to expect in this scenario. Rehearse your plan; maintain and update it as your business changes. Your plan should cover:

1. A focused scope including a few viable critical business services.
2. A clear understanding of enough information necessary to support the delivery of critical services.
3. A set of playbooks to ensure the prompt recovery and delivery of those services only, distinct from your BC and DR plans.
4. A method of proving that you are prepared to survive a severe outage regularly.

Has your organization…

- Designated a person or team to prepare to quickly deliver your most critical services to your customers in a very short timeframe following a crippling cyber attack?
- Defined, tested, and rehearsed your plan regularly?
- Trained your staff who are supporting customer operations on what to do before, during, and after such a devastating event?
- Provided all your stakeholders clear, independently validated evidence of your ability to survive such an attack?

For internal discussion…

- Are you confident that you distinguished how your organization will handle a severe outage, where your DR plans may take many days to complete? Has an approach been tested to deliver critical services sooner than that?
- Are you confident that critical third-party providers and counterparties are aware of how such a scenario will be handled, and what they might need to do differently?

Sheltered Harbor is recognized by regulators globally as the financial industry's standards setting and certification body for cyber resilience. Providing financial institutions, a Sheltered Harbor in a cyber storm.

Events

Join us for an informative webinar discussing continuity, resiliency, recovery, and your organizations participation in Sheltered Harbor.

Date: 15 May 2024

Time: Noon ET, 3:00 PM PT

Duration: 60-minutes

Guest speaker: Carlos M. Recalde, President & CEO of Sheltered Harbor

Register to Attend

About FS-ISAC

FS-ISAC is the only member-driven, not- for-profit organization that advances cybersecurity and resilience in the global financial system, protecting the financial institutions and the people they serve. Founded in 1999, the organization's real-time information-sharing network amplifies the intelligence, knowledge, and practices of its members for the financial sector's collective security and defenses.

Contact

Jeffrey Korte

Director and Executive Sponsor,

FS-ISAC Community Institution and Associations Council

Reach out to Jeffrey on LinkedIn

+1 703.962.7901 ext. 583