

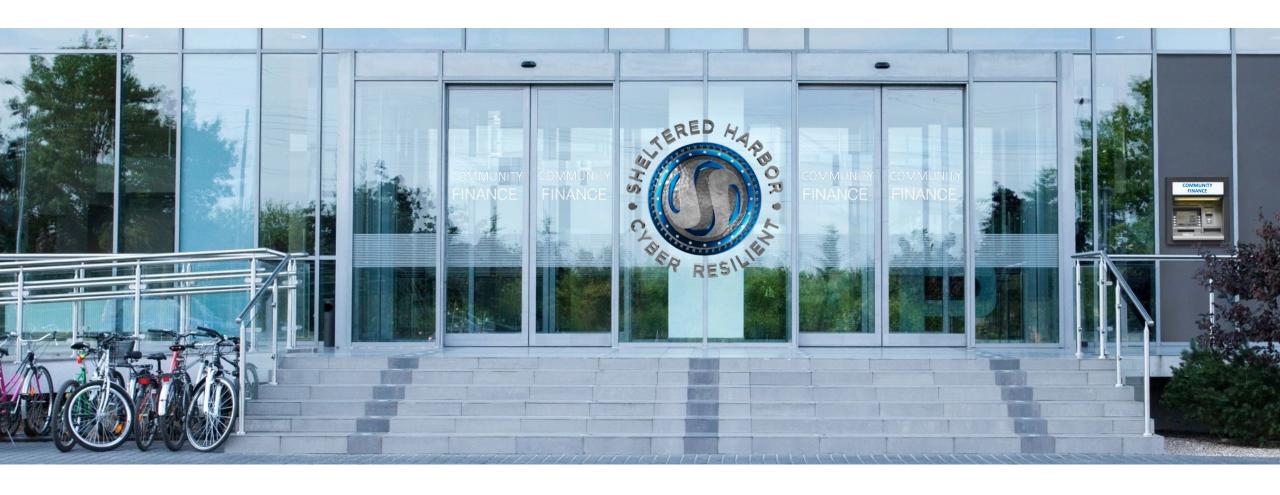
Norges Overview Deck

June 2025

Copyright © 2025 by Sheltered Harbor LLC All rights reserved. This document or any portion thereof may not be reproduced or used in any manner whatsoever without the express written permission of the publisher.

https://shelteredharbor.org

SHELTERED HARBOR MISSION



To preserve public confidence in the financial system when a catastrophic event like a cyberattack causes an institution's critical systems - including backups - to fail.

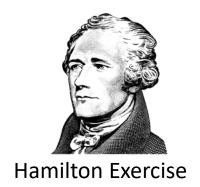


2015 THE FORMATION OF SHELTERED HARBOR



- 24th November 2014 by "Guardians of Peace"
- Deployed a variant of the rare destructive "Shamoon wiper malware" that erased Sony's computer infrastructure
- All critical systems, including backups, failed
- Cost Sony \$35M in IT repairs
- Took 27 days to restore basic operations and several months to fully recover
- Key takeaway: Companies should make sure they're wellprepared to respond to attacks.

- The concept for "Sheltered Harbor" arose in 2015 as a result of a series of successful cybersecurity simulation exercises between public and private sectors known as the "Hamilton Series."
- A Hamilton Exercise simulated the Sony Pictures attack, where all critical systems, including backups, failed.
- Hamilton Series/exercise are run by US Treasury (quarterly) introducing stress points into the system to assess overall risks and remediation strategies.
- The conclusion of the exercises was that the financial services industry, and by extension, the U.S. economy, could be vulnerable if a cyber attack disables one or more financial institutions, it could lead to a loss of public confidence
- In response, leading financial institutions, national trade associations, core service providers, and clearing houses established Sheltered Harbor to promote the stability of the U.S. financial markets by protecting critical account information of market participants in order to maintain public confidence during such a scenario.









FOUNDERS AND BOARD MEMBER FIRMS













BLACKROCK





































































SHELTERED HARBOR

The *only* participant-driven, not-for-profit, industry-led organization founded to enhance the resilience and stability of the financial sector.





THE SHELTERED HARBOR COMMUNITY

EINANCIAL INDUSTRY PROTECTION -72 % U.S. deposit accounts ~70 % U.S. retail brokerage assets 150+ Participants

SHELTERED HARBOR

- Data vaulting standards
- Resiliency planning standards and guidance
- Industry ecosystem
- Quality assurance through certification
- Regulatory engagement
- Implementation tools and resources
- Ecosystem development

FINANCIAL INSTITUTION

~41% U.S. AUM and plan assets

- Initiate program
- Implement data vaulting
- Formulate and implement resiliency plan
- Select restoration platform
- Test recovery
- Adhere to the standard, up to and including certification

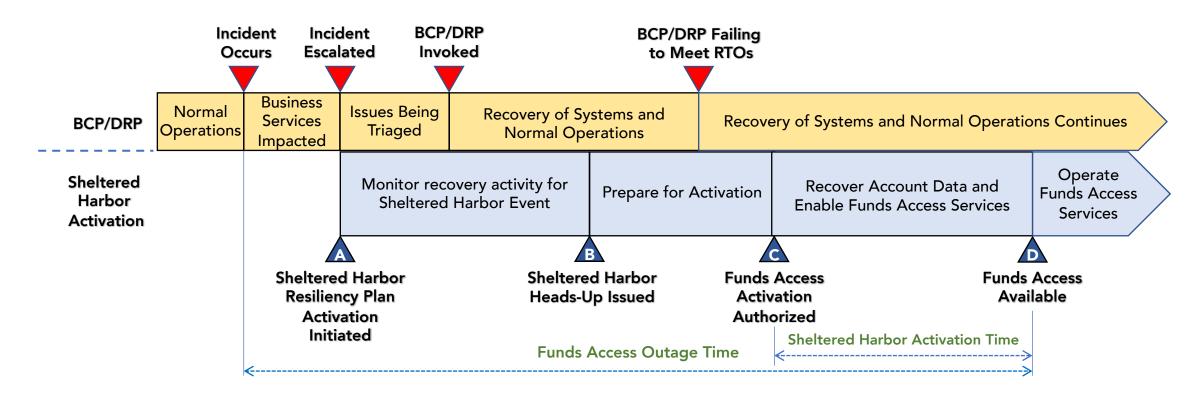
ECOSYSTEM

- Core and solution providers develop data vaulting and restoration platforms
- Advisory, assurance and solution provider Alliance Partners provide services and turnkey solutions
- Trade associations provide industry voice and support
- Regulatory agencies reference and discuss **Sheltered Harbor**



PROMPT RECOVERY OF CRITICAL SERVICES

Not an objective of most traditional business continuity (BC) or disaster recovery (DR) plans



A successful Sheltered Harbor Resilience Plan will buy the organization the time it needs to complete a full business restoration



Recognized for **Data Protection** and **Resilience**

Regulators recognize Sheltered Harbor as the financial industry's standards setting and certification body for cyber resilience

























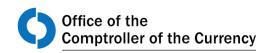


















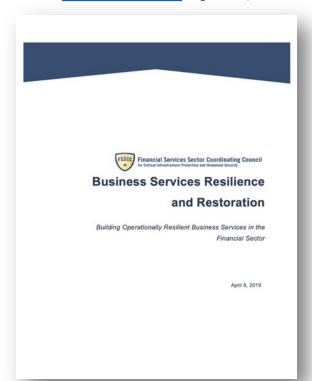




Recognized for **Data Protection** and **Resilience**

April 2019

Sheltered Harbor included in **FSSCC Business Services Resilience and** Restoration Guide (Pages 10-12)



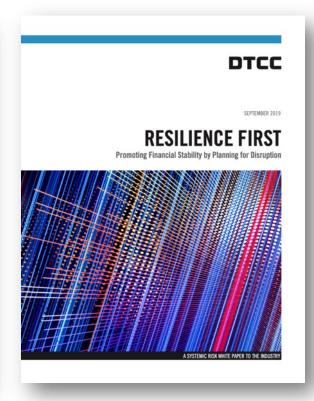
May 2019

Industry Trade Letter



September 2019

Sheltered Harbor included in **DTCC** Resilience First - A systemic risk white paper to the industry (Page 6)





A GROWING SHELTERED HARBOR PARTNER ECOSYSTEM

We continue to expand the ecosystem to support the industry with a broad menu of options

SERVICE PROVIDER COMMUNITY

• Firms implement the Sheltered Harbor vaulting and data recovery standards within their organization, certify their adherence through independent audits (initially and annually thereafter), promote Sheltered Harbor participation to their clients and prospects, assist with enrollment and provide them with the services necessary to enable their participation in and implementation of the Sheltered Harbor Standard.





jack henry







ALLIANCE PARTNER COMMUNITY

Advisory: Consulting Services	Solution Providers	Assurance: Audit Services	Marketing: "Brand Ambassadors"
Firms promote Sheltered Harbor participation and support Participants with planning, implementation and Independent Control Readiness Assessments and Reviews, necessary for Sheltered Harbor Certification.	Firms promote Sheltered Harbor participation and provide Participants with Sheltered Harbor validated turnkey Data Vaulting solutions, implementation and services to accelerate adoption efforts.	Sheltered Harbor Qualified Assessor firms promote participation, provide Participants with Independent Control Readiness Assessments, Reviews and Attestation Services to complete their Sheltered Harbor Certification	Firms create Sheltered Harbor awareness, promoting participation and adoption amongst their financial sector clients and prospects.
aws Capgemini cobalt IRON DELLTechnologies OVERITAS O		Grant Thornton	21CS PASPG
	pwc RSM	COHESITY C CYBER RISK INST	









Overview

Recognized for **Data Protection** and **Resilience**

November 2019

Sheltered Harbor included in FFIEC IT update to Examination **Handbook and Examiner Work Program** (Page 21)



FFIEC Information Technology Examination Handbook

Business Continuity Management

NOVEMBER 2019

January 2020

Sheltered Harbor included in FDIC/OCC Joint Statement on Heightened Cybersecurity Risk (Page 3)

> Federal Deposit Insurance Corporation Office of the Comptroller of the Currency

Joint Statement on Heightened Cybersecurity Risk

January 16, 2020

The Federal Deposit Insurance Corporation and the Office of the Comptroller of the Currency are is suing this statement to remind supervised financial institutions of sound cybers equity risk management principles. These principles elaborate on standards articulated in the Interagency Guidelines Establishing Information Security Standards 1 as well as resources provided by the Federal Financial Institutions Examination Council (FFIEC) members, such as the FFIEC S tatement on Destructive Malware. 2 When financial institutions apply these principles and risk mitigation techniques, they reduce the risk of a cyber attack's success and minimize the negative impacts of a disruptive and destructive cyber attack. While preventive controls are important, financial institution management should be prepared for a worst-case scenario and maintain sufficient business continuity planning processes for the rapid recovery, resumption, and maintenance of the institution's operations.

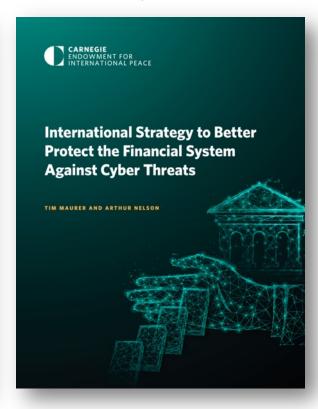
Implementing and maintaining effective cybers ecurity controls is critical to protecting financial institutions from malicious activity, especially in periods of heightened risk. Sound risk management for cybersecurity includes the following:

- . Response and resilience capabilities: Review, update, and test incident response and
- . Authentication: Protect against unauthorized access.
- . System configuration: Securely configure systems and services.

Heightened risk from cybers equity threats, such as increased geopolitical tensions and threats of aggression, may result in cyber attacks against U.S. targets and interests. In recent years, disruptive and destructive attacks against financial institutions have increased in frequency and seventy. Cyber actors often use malware to exploit weaknesses in a financial institution's computers or networks. They often obtain access to financial institution systems and networks by compromising user credentials and introducing malware through social engineering financial institution employees and contractors with phishing or spear phishing attacks. Another method of attack is to introduce infected external devices to computers and networks through removable

November 2020

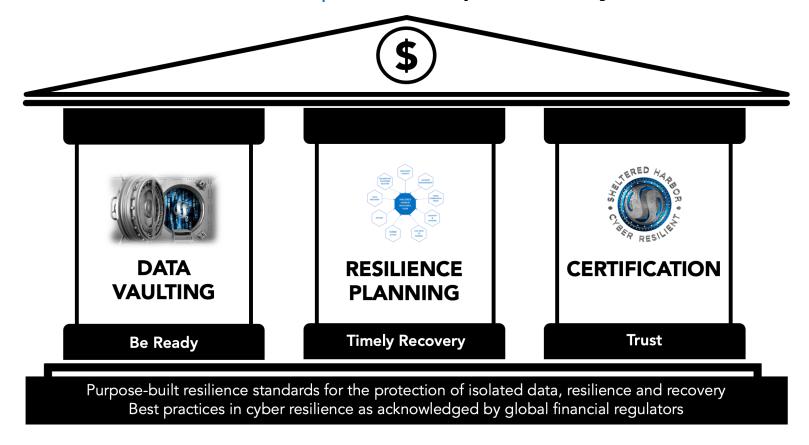
Sheltered Harbor included in Carnegie's 'International Strategy to Better Protect the Global Financial System from Cyber Threats' Report' (Multiple Pages)





PROMPT RECOVERY BY DESIGN

Sheltered Harbor provides industry standards and certifications, enabling organizations to proactively plan for and recover from a crisis, like a devastating cyber attack. When all critical systems - including backups - have failed, it buys the organization time to recover normal operations. Preparation is key!



RESULT: Recovery of <u>critical business services</u> in a crisis and preservation of public confidence in the financial system.

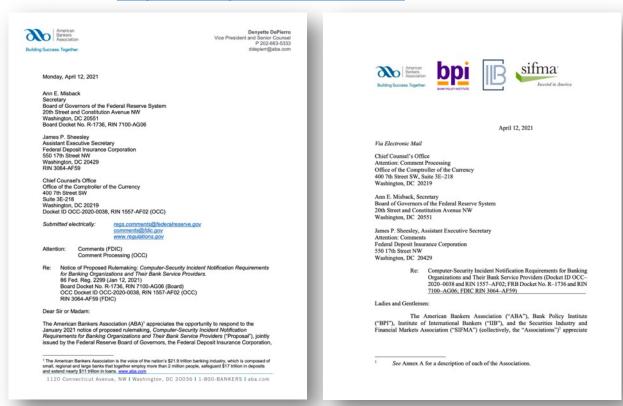


Response to a Notice of Proposed Rulemaking (NPR) regarding Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers

April 2021

Sheltered Harbor included in

ABA and the Joint Trade Associations comment letters submitted in response to the Computer-Security Incident Notification NPR (Page's 5 and 10)





Overview

Recognized for **Data Protection** and **Resilience**

August 2022

Sheltered Harbor included in

Office of the Comptroller of the Currency (OCC) News Release 2022-94, Remarks (Page 5)

Acting Comptroller of the Currency Michael J. Hsu Remarks before the Joint Meeting of

the Financial and Banking Information Infrastructure Committee and the Financial Services Sector Coordinating Council

August 2, 2022

Thank you for the kind introduction and for inviting me to speak today. I'm very glad to be speaking at this forum given the important roles that the FBIIC and FSSCC play in enhancing cybersecurity and resilience, and the significant progress in collective action for which those bodies have been responsible

My remarks today are framed by three intersecting risks that require our individual and collective vigilance: the risk of evolving cybersecurity threats, the risk to critical operations, and the risk of complacency

To date, the industry overall has done a good job of building cyber defenses and working with law enforcement and the regulatory community to guard against attacks. Those efforts and the cooperative engagement underlying them deserve recognition.

My sense, however, is that success can breed a false sense of security. We cannot be complacent. In a world of constantly evolving threats, vigilance must be maintained, especially when things are quiet. And with increasingly complex dependencies in the provision of financial services, heightened focus on the resilience and recovery capabilities of critical operations is imperative.

the next most common contributing factor to cyber breaches at financial institutions has been the result of misconfigured or unpatched systems. Malicious actors are very familiar with the security settings of commonly used software products throughout the industry and often seek misconfigured or unpatched systems applications to exploit.

While these fundamental blocking or preventive controls—threat monitoring, vulnerability patching, identity and access management, cyber incident response planning-are important to reduce risk, financial institutions should also be prepared for potential cyber disruptions and maintain sufficient resilience through effective incident response processes and rapid recovery in the event that preventative controls are not sufficient to safeguard against a cyber event. A key component of these capabilities is to establish controls to safeguard the integrity and availability of critical data against the impact of destructive malware. Recovery from such incidents may include procedures for the restoration of immutable, off-line data. Industry groups are leading various efforts, such as Sheltered Harbor and the Global Resilience Federation, to ensure that there are standardized, developed practices and frameworks to supp ation of critical data. We have observed that the integrity of backup system

ta has greatly influenced banks' ability to respond to ransomware and other

malware events.

Cyber Preparedness and Resilience at the OCC

Cyber threats to the financial sector are not limited solely to financial institutions, and the OCC recognizes that the scope of these threats is much broader. The OCC recently released our spring 2022 Semiannual Risk Perspective, 1 highlighting the current cyber threat environment and

¹ See https://www.occ.gov/publications-and-resources/publications/semiannual-risk-perspective/files/semiannual-risk-perspective-spring-2022.html





DATA VAULTING

You must have a Sheltered Harbor certified cyber-resilient data vault.

Cyber Resilient

 Immutable, Isolated, Survivable, Accessible, Decentralized, Controlled by the financial institution

Secure Process

 Incoming data validated and malware-free, controls to ensure immutability, recovery tested

Prompt, zero-trust recovery platform

Isolation is critical, distinct security zone, independently validated

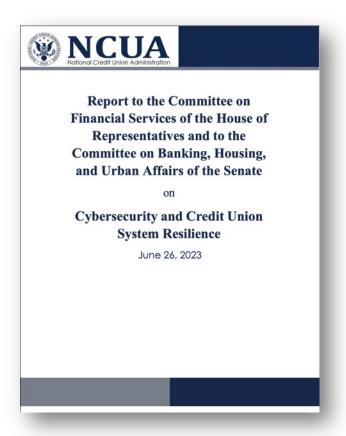


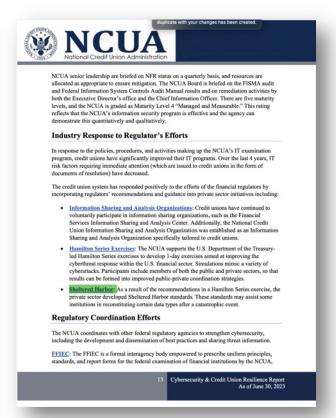
Recognized for **Data Protection** and **Resilience**

June 2023

Sheltered Harbor included in

NCUA Cybersecurity and Credit Union System Resilience Report, Industry Response to Regulator's Efforts (Page 13)









RESILIENCE PLANNING

Enables SPEEDY recovery of critical business services.

Planning to become resilient is a team sport that requires everyone to react promptly as needed when all systems and data are unavailable. All their actions must have been:

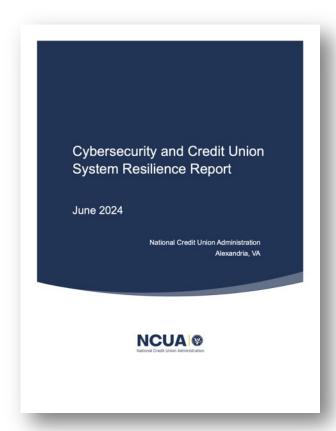
- Anticipated
- Planned
- Designed
- Implemented / Negotiated
- Tested
- Rehearsed
- Automatic ...



Recognized for **Data Protection** and **Resilience**

June 2024

Sheltered Harbor included in Cybersecurity and Credit Union System Resilience Report - Industry Efforts (Page 13)



short- and long-term solutions. This analysis supports the shaping of the NCUA's internal policies and procedures related to cybersecurity, critical infrastructure protection, supply chain risks, national security, insider threats, counterintelligence continuity of operations, and emergency response. The NCUA's staff also participate in the following interagency initiatives: CISA security operations center information and collaboration sessions; Treasury sector cybersecurity collaboration and information sessions; The Federal Chief Information Security Officer Council; and The Small Agency Chief Information Security Officer collaboration forum Credit union participation in the following initiatives reflect the credit union system's proactive engagement with the broader information security community to enhance cybersecurity and . Information Sharing and Analysis Centers & Organizations. Credit unions actively participate in the Financial Services Information Sharing and Analysis Center (FS-ISAC), where the financial sector shares intelligence, knowledge, and practices. The National Credit Union Information Sharing and Analysis Organization was established to tailor these efforts to the unique needs of credit unions and provides security coordination and collaboration to identify, protect, detect, respond, and recover from threats and Sheltered Harbor. Comprised of financial institutions, core service providers, national trade associations, alliance partners, and solution providers dedicated to enhancing financial sector stability and resiliency. Sheltered Harbor is a subsidiary of the FS-ISAC It developed standards to assist financial institutions prepare for catastrophic events. The standards are designed to help institutions to plan for and recover from catastrophic events, and to be able to continue to provide essential services until normal operations · Hamilton Series Exercises. The NCUA supports the Hamilton Series exercises through its membership on the joint FSSCC - FBIIC Exercise Committee. These one-day exercises simulate various cyberattack scenarios to enhance cybersecurity threat responses within the U.S. financial sector. They also aim to improve public-private coordination strategies by including diverse participants from both sectors.7 . CISA Cyber Hygiene Services. Over 200 credit unions have engaged with CISA's Cyber Hygiene Services program, which offers vulnerability scanning and web application scanning to help institutions mitigate cybersecurity threats. https://www.fsisac.com/hubfs/Resources/FS-ISAC_ExercisesOverview.pdf

arity and Credit Union System Resilience Report



Overview

NCUA @

CERTIFICATION



TRUST

The organization has adopted the prescribed industry-developed safeguards and controls, which have been independently assessed for compliance. Critical data supporting key business processes will survive a destructive cyber event.

SUMMARY

SPEED OF RECOVERY is essential. PREPARE NOW to recover critical business services.

- Collaboration among peers expedites practical solutions that can be used today
- The concept of minimum viable operation must be incorporated in the recovery strategy
 - o It narrows the scope (and therefore the timeline) for what needs to be recovered, and in what sequence
 - o It also keeps a broad population focused on a commonly recognized, valuable objective
- Public-Private Partnership is essential to ensure that all perspectives are reflected in a common/standardized approach.
 - Regulations support achievable and measurable objectives, where necessary
 - Examinations monitor with support from industry developed standards
- Institutions are responsible for their resilience in accordance with their own risk tolerance and business priorities



Overview

LEARN MORE ABOUT SHELTERED HARBOR AND FOLLOW US ON SOCIAL MEDIA









GET PREPARED

- Join Sheltered Harbor to access its resources
- Start planning your resiliency approach
- Vault your critical data
- Validate the data from your vault and get Data Protected and/or Vaulting Process Certified
- Define how you want your customers to experience such a devastating event
- Select your restoration platform
- Test and exercise your resilience plan
- Get your organization Resilience Certified



