COBALT IRON WHITE PAPER

Building Cyber Resilience to Maintain Public Confidence in the Financial Industry: Sheltered Harbor and Cobalt Iron

cobalt IRON®

Executive Summary

A cyberattack can not only ravage an organization's reputation and its bottom line but can also have far-reaching economic repercussions, especially in the financial industry. Sheltered Harbor is leading the initiative to maintain public confidence in the U.S. financial system and to prepare the sector for worst-case-scenario disasters and cyberattacks.

Sheltered Harbor is the financial industry's established and leading not-for-profit organization responsible for defining and maintaining the sector's resilience standards. This includes the protection of isolated data, resilience, and data recovery; promoting its adoption; and ensuring adherence through independent audits and awarding certifications.

Acquiring Sheltered Harbor certification, as recognized by the regulators, is a critical next step financial services organizations (banks, brokerages, etc.) can take toward augmenting their business continuity plans and resilience. Sheltered Harbor Certification signifies that you have implemented the robust set of industry-prescribed safeguards and that the prescribed controls have been independently audited for compliance. This ensures public confidence in your institution and the financial system in the worst of scenarios, and that you have a lifeline for survival in an extreme cyber, data-corruption or data-deletion event.

Here is what you need to know about Sheltered Harbor, how to prepare for certification, and why it matters. This paper also explains how Cobalt Iron, a Sheltered Harbor solution provider Alliance Partner, can help accelerate your journey to certification with the Compass solution for Sheltered Harbor.

Increasing and ever more sophisticated ransomware and other cyberattacks around the world have business and IT leaders in the financial sector on high alert. Cyberthreats are unpredictable, ever-changing, and evolving to include political motivations, sometimes by highly sophisticated state actors. Should one of these attacks cause an institution's critical systems to fail, customers could lose access to their accounts. This could not only destroy an institution, but it could send shock waves through the entire financial system.

That's why it is crucial for financial institutions to join Sheltered Harbor, implement the prescribed industry standards and complete certification. The Sheltered Harbor process protects your data and allows you to become cyber-resilient.

The State of Data Vulnerability

First things first. What do we know about data vulnerability today? Unfortunately, cyberthreats are ever-present and growing. In 2021, nearly 20% of cyberattacks went after the institution's backup infrastructure, which is no surprise given that organizations invest in backup and recovery as the last line of defense against cyberthreats. Criminals know that if they can compromise the backup infrastructure, then they have hit the jackpot.

A recent report from Enterprise Strategy Group stated that most corporate boards identify cyber-resiliency plans as an important project for 2022 (which wasn't a top priority even just a few years ago). One reason leadership could be placing higher priority on cyber-resiliency is cost. IBM's 2021 Cost of a Data Breach Report, featuring research by the Ponemon Institute, puts the average cost of an attack at $4 million, not counting the loss of reputation and trust.

The Sheltered Harbor process protects your data and allows you to become cyber-resilient.

Another potential reason for the elevated priority level is that ransomware hit the U.S. hard in 2021, including in the financial sector, so the concern went from being hypothetical to reality. Today financial institutions are getting regular alerts from the FBI and U.S. Department of Homeland Security with warnings to prepare for attack, particularly because of the Ukraine situation and cyber-assaults that could come directly from Russia, one of the primary adversaries in this space.

Regulators are keenly aware that we need to have answers for people — particularly about their finances — should the unthinkable happen. You need to plan for it.

Enter Sheltered Harbor

Sheltered Harbor's No. 1 mission is to maintain public confidence in the U.S. financial system during an extreme event that causes critical systems — including backups — to fail. The idea was to create a very simple solution for that extreme case, and nothing more.

How did it start?

The Sheltered Harbor concept started as a joint public-private exercise. The U.S. Treasury postulated a scenario back in 2015 after the Sony Pictures hack wiped out the company's production and backup environments. What if data from a bank, broker, or other financial institution got wiped out by a cyberattack? What would happen to all of their customers? How could the situation be resolved when nobody knows who the customers are and what their balances are? How would those customers recover?

Sheltered Harbor was founded as a not-for-profit initiative to answer those very questions. Consumers and public confidence are the organization's main focus. If consumers know they're going to be able to recover their money, then it's easier for them to continue trusting the system.

Who is part of Sheltered Harbor?

Sheltered Harbor participants represent a healthy and growing cross-section of today's financial industry, including core service providers; national trade associations; alliance partners; small, medium, and large banks; brokers; credit unions; asset management firms; insurers; and even a few of the major utilities and clearinghouses — all dedicated to enhancing stability and resiliency in the financial sector.

Who pays for Sheltered Harbor?

Participants from the financial industry fund the entire initiative, not to make money from the solution, but to:

- Define and maintain the sector's resiliency standard
- Promote adoption across the industry
- Ensure adherence through independent audits and certifications

What does Sheltered Harbor provide?

Sheltered Harbor is laser-focused on providing a simple approach that financial companies can use to give customers continuous access to their account balances and funds during an extreme event that causes full loss of operational systems and data. Simply put, Sheltered Harbor provides the only industry-developed standards and certifications for resilience, data recovery, and protection of isolated data. It serves as a bridge in an extreme event while your institution recovers normal operations, which could take several days, if not weeks.

Specifically, Sheltered Harbor's collective of financial industry experts has developed the only standards that protect the integrity of critical customer account data, ensuring it is portable and recoverable. With this standard in place, financial organizations can continue to support essential business services in a worst-case scenario.

> Sheltered Harbor provides the only industry-developed standards and certifications for resilience, data recovery, and protection of isolated data.

To date more than 900 subject matter experts have contributed to the solution, resolving questions such as:

- What does it mean to protect data so that we can actually give people access to their balances and funds within 24-48 hours after an extreme disaster?
- What does a resiliency plan look like? What are the important elements? What critical decisions should be made with level heads in advance of an event?
- How do we certify data protection and resiliency plans for each organization?

When does the Sheltered Harbor solution come into play?

Sheltered Harbor protocols are invoked as an incident response when an extreme operational outage or data destruction event happens. The institution's incapacity to service its customers threatens a loss of confidence in the financial system. These protocols extend the responsiveness of traditional disaster recovery and business continuity plans.

How does it work?

Simply speaking, there are essentially five important components:

Daily Data Extraction by the Participating Financial Institution

This is how you isolate Sheltered Harbor-relevant data.

- Your institution backs up critical customer account and supplemental data each night in the Sheltered Harbor standard format.
- The data gets encrypted and transmitted to a data vault — either one you own or that of a service provider.

Daily Data Vaulting in Accordance With Sheltered Harbor's Specifications

This is how you store critical customer account data so that it is protected and recoverable even if an attack takes out your operational and backup environments.

- The data vault is unchangeable, air-gapped, survivable, accessible, and completely separated from the institution's infrastructure (including all backups).
- The data vault always remains under your control.
- Daily attestation messages provide assurance that all backups have been completed and successfully protected.

Resiliency Plan per Sheltered Harbor's Requirements

This is the business preparation that will allow you to restore customer accounts and service them in the event of an extreme operational outage or data destruction event (most likely from a cyberattack).

- Your institution prepares business and technical processes and makes key arrangements for a worst-case scenario.
- The plan gets activated in the case of a Sheltered Harbor event (i.e., when all other options to restore critical systems — including backups — will fail to ensure the maintenance of public confidence).

Restoration Platform Built in Accordance With Sheltered Harbor's Specifications

This is the platform you'll use temporarily to service your customers when the Resiliency Plan is activated. You can either build it yourself or designate a third-party platform provider in advance.

- If the Resiliency Plan is activated, then you can transmit data from the vault to the restoration platform.
- The restoration platform decrypts the data and restores customer access to account information and funds as quickly as possible.
- Meanwhile, it acts as an interim working platform while the institution employs its business continuity plan to restore full operational capability.

Sheltered Harbor Certification

This is how customers, regulators, and fellow financial institutions know they can trust your data — that your data vault conforms to the industry standards, that the data maintains its integrity and is safe to interact with when needed — so that they can support you during a crisis.

- Certification is a fundamental pillar of the Sheltered Harbor standard.
- Participants adopt a robust set of prescribed safeguards and controls, which are independently audited for effectiveness and compliance with the Sheltered Harbor standard.
- Upon completing the requirements for data vaulting in accordance with Sheltered Harbor Specifications, an institution is awarded the Sheltered Harbor "Data Protected" certification.

> Participation in Sheltered Harbor demonstrates a proactive approach in planning both a mitigation strategy and a response to a destructive cyberevent.

Why Get Sheltered Harbor Certified?

When you achieve Sheltered Harbor certification, you demonstrate that not only have you adopted the robust set of controls and safeguards required, but that you have the industry-validated resources and know-how necessary to stay connected with your customers, continue to serve them with essential services, and work with regulators while you take additional steps to fully recover from a catastrophic event. Plus, it's just the right thing to do for customers and for society.

The key benefits of participation:

- Exclusive access to the industry-developed standard today, which is easy to implement and certify.
- Low-cost access to high-value materials and best practices, developed specifically for you by the industry.
- Confidence in knowing that your institution is Sheltered Harbor-ready and that you can confidently communicate that to your customers, board of directors, shareholders, and regulators.
- Leverage the Sheltered Harbor standard approach and framework as the foundation for your broader operational and cyber-resilience needs.

Enhanced resilience, reputation, and public trust

By activating the Sheltered Harbor protocols, you can do the two most important things that instill confidence:

1. Reassure customers within 24 hours that you know what their balances are and that a resiliency plan is underway.
2. Also, within 24 hours, ensure that customers have access to funds against their balance.

With these steps completed, your institution is now prepared to respond and recover from an extreme zero-day event.

Acknowledged by U.S. financial regulators for data protection and resilience

Industry regulation requires that financial institutions prepare for a data destruction event. Participation in Sheltered Harbor demonstrates a proactive approach in planning both a mitigation strategy and a response to a destructive cyberevent. Because Sheltered Harbor started as a public-private partnership that was initiated by regulators, regulators have always been involved in vetting and supporting the solution.

Sheltered Harbor leaders return to those roots regularly to make sure everyone is up to date and in sync: the private sector that created the solution and the public sector that to some extent governs it. In fact, Sheltered Harbor leaders meet at least quarterly with regulators within various government agencies, who are keenly involved in understanding the solution and are very much on board with the approach. Sheltered Harbor certification helps solidify the financial sector and align it with consistent standards that regulators understand and agree with.

Industry Adoption

Sheltered Harbor is open to U.S. financial institutions of all types and sizes and already has significant industry adoption — principally among banks, credit unions, and brokers.

As of September 2021, participants hold about 70% of U.S. deposit accounts and about 70% of U.S. retail brokerage client assets.

Despite this strong adoption rate, the Sheltered Harbor protocols will be most effective when every single financial institution is on board. If you're not certified, then you're behind the curve and behind the regulatory conversation.

Working With Sheltered Harbor Alliance Partners to Prepare for Certification

The data vault must be in production in order to achieve Sheltered Harbor "Data Protected" certification. Sheltered Harbor is not a vendor and does not provide operational support, so you are responsible for implementing your own data vault technology and creating your own resiliency plan.

However, it's not easy or efficient to develop these solutions from scratch. As you prepare for certification, you don't have to go at it alone. In fact, now that the financial industry has figured out how to respond to a catastrophic data event, Sheltered Harbor has formed key alliances to expedite your data vaulting progress.

There is a growing ecosystem of verified Sheltered Harbor Alliance Partners that can help take you from the beginning of the project to the end in a seamless way with proven, endorsed technologies and processes. These partners have done it before and can help you do it efficiently and effectively.

Working with Sheltered Harbor Alliance Partners can accelerate the certification process. That's because you get a preordained solution that already meets Sheltered Harbor requirements. You don't have to spend extensive time and money building your own complex, difficult-to-manage, homegrown solution, which must go through Sheltered Harbor certification and then must be maintained to ensure that all controls and safeguards are sound.

Cobalt Iron and Compass for Sheltered Harbor

One of those partners is Cobalt Iron, whose Compass® for Sheltered Harbor SaaS platform is now in development. When complete, Compass for Sheltered Harbor will provide a ready-to-deploy data vault for financial institutions.

Because it will be available in cloud, hybrid, and on-premises deployment options, Compass will be the most flexible data vault option for institutions that choose to work with a solution provider. That means it will be able to accommodate every financial institution's requirements — whether you're a large enterprise with multiple data centers and multiple data vaults in separate locations, or a small organization (such as a small community bank) with a single data center and no secondary location. Compass will also be the more scalable and cost-efficient option in the long term.

Compass for Sheltered Harbor will have all of the essential elements for a certified data vault, which were already native to the Compass solution even before Cobalt Iron began customizing it for Sheltered Harbor:

- Secure (encrypted)
- Immutable (unchangeable, and not subject to deletion)
- Completely isolated from production and backup systems (air-gapped)
- Survivable and accessible after a complete system(s) outage
- Under constant role-based access permissions and controls

And because it will be a turnkey solution, Compass for Sheltered Harbor data vaults will be able to get up and running in days — not weeks or months — with no professional services required.

From there, Sheltered Harbor implementation partners can assist with the ingestion and validation of the data from the data vault.

> Compass will be the most flexible data vault option for institutions that choose to work with a solution provider.

Conclusion

After a catastrophic event, business and IT leaders in the financial industry are challenged to ensure public trust and to recover critical customer data quickly. Sheltered Harbor offers a simple solution to that challenge — a solution that has been vetted by regulators and financial institutions of all sizes. The majority of U.S. deposit and brokerage accounts are now covered by Sheltered Harbor-certified systems, but 100% participation is the goal. Not only does Sheltered Harbor certification unify the financial industry and help regulators support you during a crisis, but it is simply the right thing to do for customers. Getting certified is no small task, but working with Sheltered Harbor Alliance Partners on implementation and technology will help you accelerate the certification process.

About Sheltered Harbor

Sheltered Harbor LLC is a financial industry not-for-profit organization, founded by 34 financial institutions, clearing houses, core processing providers, and industry associations including: the American Bankers Association (ABA), Financial Services Forum (FSF), Bank Policy Institute (BPI), Securities Industry and Financial Markets Association (SIFMA), Credit Union National Association (CUNA), National Association of Federal Credit Unions (NAFCU), and Financial Services Information Sharing and Analysis Center (FS-ISAC) to enhance the stability and resiliency of the financial sector. www.shelteredharbor.org

About Cobalt Iron

Cobalt Iron was founded in 2013 to bring about fundamental changes in the world's approach to secure data protection, and today the company's Compass® is the world's leading SaaS-based enterprise data protection system. Through analytics and automation, Compass enables enterprises to transform and optimize legacy backup solutions into a simple cloud-based architecture with built-in cybersecurity. Processing more than 8 million jobs a month for customers in 44 countries, Compass delivers modern data protection for enterprise customers around the world. www.cobaltiron.com

Product or service names mentioned herein are the trademarks of their respective owners.

888-584-4766 • www.cobaltiron.com

cobalt IRON®

© 2022 Cobalt Iron, Inc. All rights reserved. Cobalt Iron, the Cobalt Iron logo, the Cobalt Iron agent logo, Compass, the Compass logo, "Data Protection Everywhere. Smart. Secure. Automated.", and Take Control of Your Data are trademarks of Cobalt Iron. All other trademarks or registered trademarks are the property of their respective owners. 060622