Uptime Institute® | INTELLIGENCE

RESEARCH BRIEF
UI INTELLIGENCE REPORT 50 • Q3 2021

Sheltered Harbor — a corporate IT survival model?

The financial services industry has developed a certifiable methodology designed to help banks recover from the complete loss of all IT systems for an extended period. Is this a blueprint for improving corporate resiliency?

Author Andy Lawrence

In November 2014, Sony Pictures suffered a severe and now notorious cyberattack. The incident resulted in the forced withdrawal of a new movie, the release of sensitive corporate and personal data, and a $15 million recovery bill. To deal with the loss of data integrity, Sony was forced to shut down its IT infrastructure for 27 days.

It was a near-disastrous episode for Sony, but it raised the prospect of a more frightening scenario: What if the same thing happened to a provider of critical services? Or a large bank? How would such an organization ride through even a few days without its IT systems? How would customers and trading partners react?

At one time, information security breaches were considered damaging and costly, but not a threat to business continuity. This has now changed: cyberattacks have already brought down the entire IT systems of a number of organizations for days or weeks, and many more will join the victim list in the years ahead. Among them to date are Sony; Maersk, the global shipping company; Travelex, the UK currency exchange company, which later went into liquidation; Garmin, the fitness tracker company; and recently, the Colonial Pipeline, which distributes fuel in the US East Coast, and the Irish Health Service Executive (HSE). Several of these organizations, and many others, have paid large ransoms as they desperately tried to recover their data.

After the Sony incident, the US Treasury Department ran a series of exercises (known as the Hamilton Series) to test the resiliency of banks in this situation. The conclusion? Banks and various services providers had a serious gap in their resiliency planning and needed a way to survive the complete and extended loss of their operational IT systems.

The result is the Sheltered Harbor initiative, founded by 34 financial industry organizations — including a cross section of small, medium and large banks, brokerages and credit unions; trade associations; clearinghouses; and core service providers — with the specific purpose of maintaining public confidence should an extreme outage affect all operational systems, including backups. It is now incorporated as an independent subsidiary of the Financial Services Information Sharing and Analysis Center (FS-ISAC), a global nonprofit that facilitates the confidential sharing of information about cybersecurity threats among financial institutions.

While Uptime Institute has historically focused primarily on the resiliency of the physical IT infrastructure, ransomware and other malicious attacks present a new dimension to ongoing IT operations, spanning both the logical and physical domains. Operational resiliency has entered a new phase.

This report discusses the strategies of Sheltered Harbor for the retail banking sector. The approaches used, involving an isolated, secure vault, may point to strategies that all industries can adopt to some degree. Even data centers themselves, increasingly dependent on intelligent systems for continuing operations, may be able to increase their resiliency by securely storing and rapidly recovering operational data.

Ransomware to terrorware

Ransomware attacks have become a top issue for those concerned with business continuity. In June 2021, the US Department of Justice said it was giving the investigation of ransomware the same priority as terrorism.

There are many types of ransomware. Usually, the attack involves burying lines of code capable of locking, encrypting, corrupting or stealing data into critical software systems. This code may be buried months or years ahead of activation, which means operators struggle to identify a point — and certainly not a recent point — before which the data was indisputably clean. One particularly concerning form of ransomware is a supply chain attack, which involves hiding the malicious code in a trusted provider's software, which is then distributed to clients. **Table 1** lists some notable ransomware attacks.

The Sheltered Harbor initiative is not intended to address ransomware per se, but rather any event in which the entire IT infrastructure is rendered unusable. However, adoption of Sheltered Harbor may provide a last line of defense. The Ransomware Task Force (a group of IT suppliers, government and law enforcement agencies and others) has published a report with 48 recommendations to reduce the risk of attack.

Table 1 **Some notable ransomware attacks***

Event	Date	Impact
JBS Meat	2021	Shut down for several days. $11M paid in ransom
Colonial Pipeline	2021	Multiple-day disruption of US East Coast fuel supplies. Estimated $4M ransom paid.
Irish Health Service	2021	Four-week disruption to services. Many IT systems shut down. $20M ransom not paid.
Garmin	2020	Fitness device Garmin allegedly paid $10M after its services were frozen for five days.
Travelex	2019	IT systems and business shut for several weeks. $2.3M ransom paid. Company went into administration shortly after (COVID a contributing factor).
UK National Health Service	2017?	88 Health trusts in UK health service suffered IT shutdowns. Millions in ransom not paid.
Maersk/Merck/TNT Express and others	2017	A ransomware-type attack resulted in billion-dollar losses for major companies. Data was encrypted, but no ransom was ever requested.
Sony Pictures	2014	Sony suffered months of disruption from attack. The attackers did not demand money, but rather the withdrawal of a movie about North Korean leader Kim Jong-un.

*Uptime Institute category 5 (Severe) outage or notable for long-term impact.

Uptime Institute | INTELLIGENCE

What is the Sheltered Harbor initiative?

Sheltered Harbor was developed by and for the financial industry, and its focus is narrow: to ensure a bank's critical and core retail services can be restored quickly, even when all its IT systems, and all its backup systems, are compromised or critically damaged.

One of the findings of the Hamilton Series of simulations was that traditional approaches to ensuring resiliency and continuity — such as establishing redundant physical systems, cyber defenses and business continuity plans — provide good protection against infrastructure failures, physical events, and the great majority of cyberattacks. But a severe malware attack will very likely also infect redundant systems, disaster recovery and backup sites, which would present the IT staff with critical new challenges.

Significant hurdles

A severe malware attack will very likely also infect redundant systems, disaster recovery and backup sites.

The Hamilton Series made it clear that any solution to this must overcome some signature hurdles:

- First, it would be necessary to have clean, isolated copies of the most critical data. This data must be free of any executable code that can store or enable malware.
- Second, a secure and safe physical/logical vault for this data would be needed that is separate from the rest of the IT.
- Third, the data would have to be reliably recoverable, quickly, even without the continuing availability of the original systems. This last part is particularly challenging and is one of the reasons why recovery from ransomware attacks has proved so difficult.

The founding members of Sheltered Harbor realized that one organization alone would find it prohibitively expensive to solve the problem — it would need to have fully separate and fully operational redundant IT systems. Timely recovery of a bank's systems would therefore require the use of another organization's systems — likely a service provider or possibly another bank.

Challenging requirements

Financial systems architect Carlos Recalde, an advisor to the new initiative and now the Sheltered Harbor president, led the working groups that identified another challenging requirement: To avoid a crippling crisis of confidence, critical data (such as customer accounts and balances) would need to be recovered and available within a day. And the recovery point objective must be short — the previous day's closing.

Recalde also advised that it would be not realistic for the new entity to become an independent utility to protect and store all the data — apart from the expense, it would be a point of failure and a target in its own right.

Sheltered Harbor, set up in 2015, therefore focused on developing processes and standards for the secure storage and timely recovery of data that any retail bank could implement by working with others. It issued its first Data Vaulting Specification in September 2016 and has been improving on it ever since to make it more attainable, while maintaining the integrity of the data required to address the extreme scenario.

It now has over 130 participating institutions, which represents nearly three-quarters of US deposits and brokerage accounts. The initiative is backed by most of the relevant regulatory and advisory financial services organizations in the US.

By its own admission, Sheltered Harbor cannot protect a bank against any eventuality, nor can it protect all of a bank's operations, because of the huge variety and number of financial applications and data sets and the short recovery points that are needed in many cases (although the range may be extended over time). But it can provide a solid base — a harbor — from which recovery operations can begin. While every industry, and perhaps every set of services, is different, the model may prove one that could be more widely adopted.

How it works

Participants in Sheltered Harbor must create a secure data vault or arrange to use one operated by a partner or service provider. Sheltered Harbor has developed the specifications for this vault, focusing on the IT and data aspects. But, of course, the vault needs to be in a facility that is secure and designed against physical risks and possible failures. In addition to having the required data protection controls and the physical security, it may be wise for the vault to be protected from electromagnetic pulse (EMP).

The media must be nonvolatile and the data, immutable, encrypted and isolated.

Each night, key account and customer data is sent to the secure offline data vault. This storage media must be nonvolatile — the need for rapid recovery and data analysis will likely favor disk. The data must be immutable (meaning it cannot be changed even by an administrator with a key), encrypted and isolated (that is, not connected to any system that might be potentially infected).

Hidden threats

An issue of obvious concern is that malware can be hidden in data or an application for days, weeks or months. For this reason, the data sets, and the processes and standards used, must be rigorously specified to block infiltration, and processes must be strictly followed (see **Where Sheltered Harbor fits in**). Sheltered Harbor shares the full specifications only with participants and auditors.

Participants in Sheltered Harbor must have a recovery plan for when a critical event occurs. This will include designating an IT platform — which could be at an approved service provider or another financial services company — that can read the files in the vault and make the data available to customers. In the meantime, the afflicted company can work to restore its own IT using the best-available tools and recovery processes.

Certification is an important component of Sheltered Harbor, to ensure that the vault conforms to agreed technical specifications, reducing the likelihood of data contamination and increasing the likelihood and speed of recovery. Certification is currently only issued in North America, and only after the successful completion of assessments by qualified Sheltered Harbor auditors.

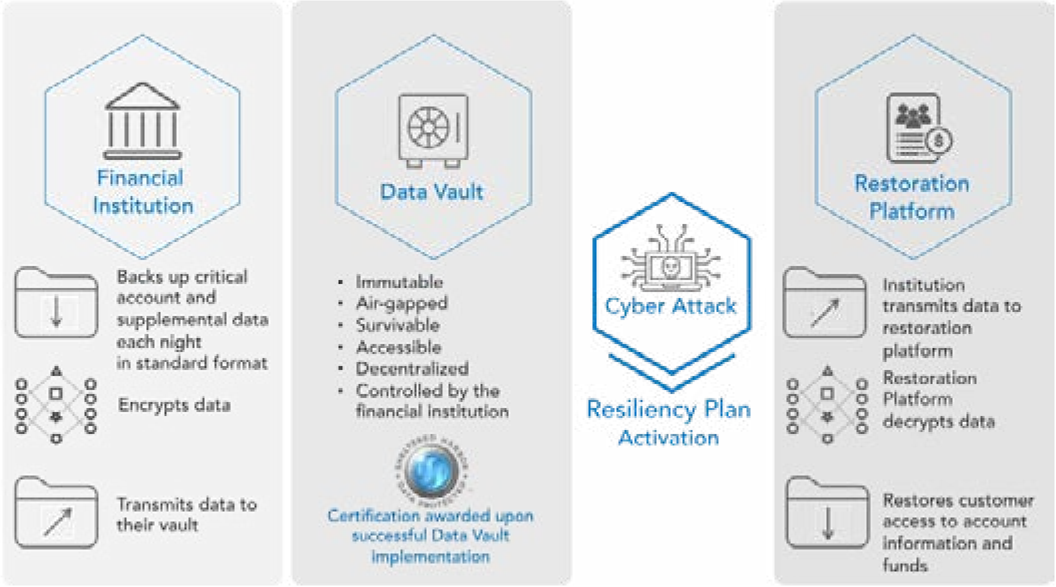
Sheltered Harbor has specifications covering the encryption and storage of the data, the process of recovery/decryption, and the restoration of access. Full testing of the recovery process is required. Recertification is required every 12 months. **Figure 1** shows how Sheltered Harbor works.

The cost of implementing Sheltered Harbor is not high, given the common availability of the technology and technical skills required. Membership, which gives access to standards and advice, ranges from $250 for small financial services organizations to $50,000 for a large bank.

Some technical investment will likely be needed, depending on the scale of the financial institution and the infrastructure already available. Implementation will likely take months.

Sheltered Harbor partners with a small number of product and service providers to help clients. Dell has an endorsed disk-based product for vault storage called PowerProtect Cyber Recovery; Ernst & Young, IBM, Capgemini, PricewaterhouseCoopers, RSM, Grant Thornton and others provide services ranging from implementation advice to certification audits.

Figure 1 **How Sheltered Harbor works**


Financial Institution
Backs up critical account and supplemental data each night in standard format
Encrypts data
Transmits data to their vault
Data Vault
• Immutable
• Air-gapped
• Survivable
• Accessible
• Decentralized
• Controlled by the financial institution
Certification awarded upon successful Data Vault implementation
Cyber Attack
Resiliency Plan Activation
Restoration Platform
Institution transmits data to restoration platform
Restoration Platform decrypts data
Restores customer access to account information and funds

SHELTERED HARBOR UptimeInstitute | INTELLIGENCE

What does it protect against?

The invocation of the Sheltered Harbor vault and recovery process will be extremely rare and extremely serious. A full-scale malicious attack can mean that all critical data becomes inaccessible — because it has been encrypted, corrupted or destroyed.

This may include backups. Sheltered Harbor expects that most ransomware attacks probably can be isolated and dealt with without using the vault.

Extended and regional critical power outages, terrorist attacks, natural disasters or other known or unknown issues (e.g., EMP) could, in theory, also disable an organization's core IT. But these events are most likely local, and in most cases the vulnerability will already have been addressed using redundant IT and data centers, distributed systems, and business continuity failover plans.

Even so, a Sheltered Harbor-style vault and recovery plan, for all industries, may add a final layer of defense.

Where Sheltered Harbor fits in

Many (but not most) organizations have, over the past several years, developed strategies for dealing with extreme malware/ransomware attacks.

A ransomware defense strategy will likely involve the use of scanning and anomaly detection tools to identify attacks as early as possible; the separation of immutable backup files from operational systems and replication to multiple sites; the separation of backup and recovery administration, including console and network, from the rest of the IT; and finally, the creation of an Isolated Recovery Environment (IRE) from which recovery can begin. In most cases, it will have to be assumed that even the backed up immutable copies are potentially infected and will therefore have to analyzed and scanned before recovery can begin.

Quick recovery

Sheltered Harbor builds on many of these principles, but takes it further, to ensure clean copies of at least some data can recovered quickly: first, by standardizing on a minimal data format that should be malware-free; and second, by organizing a method for the data to be accessible to customers while the long recovery process is undertaken.

The Sheltered Harbor initiative is a formalized and standardized approach to shoring up resiliency against extreme events. But it is not the only approach that has been proposed or used in the financial sector.

Reciprocal arrangements

Some smaller banks, for example, have formed reciprocal backup and recovery arrangements with other similar banks. These are private arrangements and details are confidential —but a close partnership can enable a wider range of services than just balances and accounts to be recovered. In Europe, many larger financial organizations also have reciprocal recovery arrangements, although these are less likely to involve a formal isolated-vault approach and instead focus on disaster recovery situations, where services such as ATMs or certain applications can be shared.

The approaches (Sheltered Harbor uses) may point to strategies all industries can adopt to some degree. Even data centers may be able to increase their resiliency by securely storing and rapidly recovering operational data.

There is now growing interest in Sheltered Harbor in major banking centers around the world; UK, European and some Asian banking authorities are evaluating if and how similar schemes could be set up. Sheltered Harbor currently advises European banks to set up their own schemes and is supportive and willing to share expertise.

Recent incidents suggest, however, that more thinking and action may be needed beyond financial sectors — especially as the failure of major services such as power, telecommunications or health systems can threaten national security.

In creating Sheltered Harbor, it was necessary to make some compromises. Only a few banking operations are covered, and the recovery point (to the previous day's closing) is short enough to prevent a crisis — but is still too long for many banking operations. This will likely encourage financial services companies to continue to look for strategies where they can make immutable but safe copies of key data with greater frequency.

The role of cloud and blockchain

Uptime Institute research shows that a significant minority of banks are planning to put critical transaction-based or core systems into the public cloud. This has raised many strategic questions, especially regarding accountability, transparency and incident management.

Can the cloud be used for Sheltered Harbor? Public clouds can play a role, but a key point is that they offer only a portion of what is necessary for a financial institution to survive a Sheltered Harbor event.

Cloud-based systems involve moving data off-site (to multiple sites), which offers a level of resiliency. But although leading providers such as Amazon Web Services (Glacier) and Microsoft do offer some secure and encrypted vault services, they do not fully prepare and isolate data or take it off offline. All the work necessary to ensure the data is clean must be done first. The certification focuses on all aspects of data control that the financial institution must address before they would ever have to use their cloud provider during a live event.

The use of blockchain would still require a network of trusted partners, as well as the use of agreed data formats.

If one of the goals of Sheltered Harbor is to create an immutable, recoverable, and secure database — and one that is not vulnerable to a single point of failure — why not make use of blockchain?

The potential use of blockchain has been discussed, and the technology could be used in the future. Blockchain could enable an immutable copy of a bank's accounts to be distributed across many participating systems, reducing the risk of single points of failure. The immutability of the blockchain could also mean that cloud-based solutions, which are always online, could be used.

However, there are many questions to be worked through. Blockchain could face issues of performance and scalability and could be more complex to implement than simpler partnering arrangements. The use of blockchain would still require a network of trusted partners, as well as the use and verification of agreed data formats and agreed recovery formats.

Uptime Institute recommendations

The first line of defense against most malware attacks is in reducing the opportunities to the attacker. This means that more attention should be paid to data security policies and hygiene and to software development, deployment and use.

Sheltered Harbor is concerned with corporate survivability after a most extreme event. It is not an alternative to business continuity planning, ransomware strategies or operational resiliency strategies, but rather is a part of such plans.

Sheltered Harbor is of necessity narrow in its scope. But its narrow scope makes it practical and affordable for retail banks, given the huge risks that it may help defend against. Uptime recommends US banks engage with Sheltered Harbor and that those outside the US consider adopting its principles. Beyond this, it may be an example for other industries to follow.

Public cloud, blockchain and other technical solutions are not part of the Sheltered Harbor approach at present, but these technologies are being or will be adopted by many organizations as part of their ransomware defenses. There will continue to be concerns around aspects of these solutions — in terms of cost, complexity and the ability to seal the data — but they may prove sufficient for many organizations.

About the author

Andy Lawrence is Uptime Institute's Executive Director of Research. Mr. Lawrence has built his career focusing on innovative new solutions,emerging technologies and opportunities found at the intersection of IT and infrastructure.

Contact: alawrence@uptimeinstitute.com

About Uptime Institute

Uptime Institute is the Global Digital Infrastructure Authority. Its Tier Standard is the IT industry's most trusted and adopted global standard for the proper design, construction, and operation of data centers – the backbone of the digital economy. For over 25 years, the company has served as the standard for data center reliability, sustainability, and efficiency, providing customers assurance that their digital infrastructure can perform at a level that is consistent with their business needs across a wide array of operating conditions. With its data center Tier Standard & Certifications, Management & Operations reviews, broad range of related risk and performance assessments, and accredited educational curriculum completed by over 10,000 data center professionals, Uptime Institute has helped thousands of companies, in over 100 countries to optimize critical IT assets while managing costs, resources, and efficiency.

Uptime Institute is headquartered in New York, NY, with offices in Seattle, London, Sao Paulo, Dubai, Singapore, and Taipei.

For more information, please visit **www.uptimeinstitute.com**

All general queries:

Uptime Institute
405 Lexington Avenue,
9th Floor, New York,
NY 10174, USA
+1 212 505 3030
info@uptimeinstitute.com