ESG SHOWCASE

Enhancing Cyber Resiliency and Recovery for the U.S. Financial System

Date: August 2022 **Authors:** Vinny Choinski, Senior Analyst; and Monya Keane, Senior Research Analyst

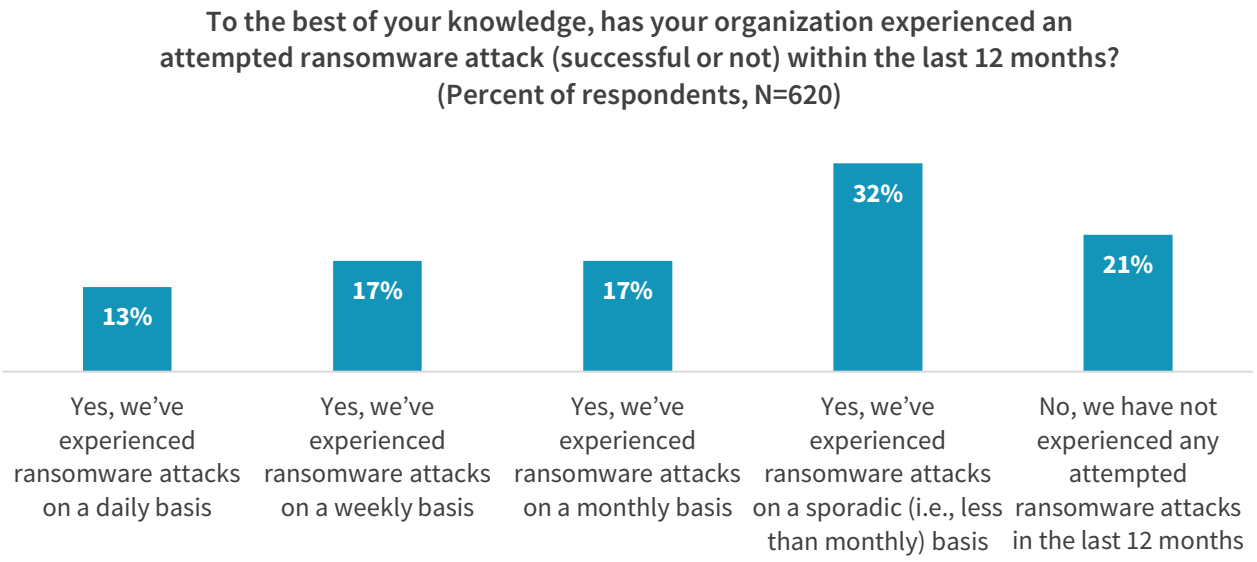
ABSTRACT: You don't have to be an IT security professional to understand that cyber-risks are on the rise. And as cyber-risk increases, so, too, does the likelihood of a successful cyber-attack. When an attack hits a financial institution, its customers want to know how quickly access to their account balance information and the ability to transact against those balances will be restored. In this showcase, we explore how Sheltered Harbor can help financial institutions successfully navigate a cyber recovery and how Dell Technologies, an endorsed Sheltered Harbor Solution Provider, can accelerate the process.

Market Landscape

Ransomware attacks make the news on a regular basis, so it should come as no surprise that ESG research survey respondents confirm the high frequency with which they are occurring. Indeed, a combined 79% of respondent organizations reported having experienced a ransomware attack within the last year, and among that population, nearly three-quarters (73%) reported that they have been financially or operationally impacted by ransomware, making those attacks "successful."

It is also notable that one in three organizations (32%) reported having been attacked successfully more than once, indicating that ransomware is not only a significant source of business disruption, but also a recurring one (see Figure 1).[1]

Figure 1. Ransomware Attack Frequency



Source: ESG, a division of TechTarget, Inc.

[1] Source: ESG Research Report, *The Long Road Ahead to Ransomware Preparedness*, June 2022. All ESG research references and charts in this showcase are from this research report.

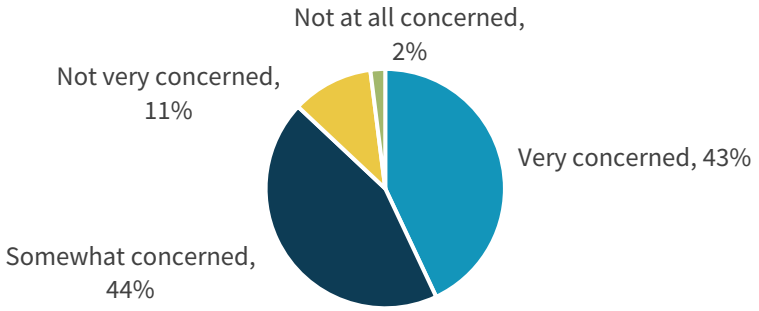
The Increasing Scope of the Cyber-attack

When primary data becomes corrupted or lost, an IT organization traditionally leverages backup copies for recovery purposes. This process has made the backup infrastructure a very desirable target for cyber-criminals, who clearly understand that secondary data environments are a key tool enabling IT teams to mitigate or neutralize attacks.

Thus, if the attackers can take out backup-centric defenses, they optimize their chance of success. IT leaders also are aware of this situation, and they are significantly concerned. As Figure 2 shows, nearly nine in ten organizations are worried that their backup copies could be corrupted by ransomware attacks, with 43% saying they are very concerned.

Figure 2. Concern that Backups Could Become Ransomware Targets

Generally speaking, how concerned are you that your organization's data protection copies (e.g., backup, snapshot, replication, etc.) could also become infected or corrupted by ransomware attacks? (Percent of respondents, N=620)



Source: ESG, a division of TechTarget, Inc.

What Is Sheltered Harbor?

An independent, not-for-profit subsidiary of the Financial Services Information Sharing and Analysis Center (FS-ISAC), the Sheltered Harbor organization is dedicated to coordinating the development and refinement of the Sheltered Harbor standard, promoting the standard's adoption across the financial services industry, supporting implementations, and ensuring ongoing adherence. The purpose of the standard is to protect public confidence in the U.S. financial system if a devastating attack such as a cyber-attack causes an institution's critical systems, and their backups, to fail.

Without data, nothing else can happen to support recovery. Therefore, the first thing Sheltered Harbor set out to do as an industry group was to make sure that a copy of a banking institution's data would be available in an extreme scenario. That scenario relates to occurrences in which a financial institution is completely wiped out operationally—all computer systems and data are gone.

In other words, Sheltered Harbor ensures that on the worst of days, data retrieved from the vault for restoration after an attack—when failure is not an option—is exactly the same pristine data that went into it from the system of record. This vaulting process is the core of the Sheltered Harbor data protection certification, although Sheltered Harbor emphasizes all components of the standard, not just the vault.

Sheltered Harbor Solution Provider Program

Sheltered Harbor is building relationships with technology providers who can provide solutions supporting Sheltered Harbor processes. The first endorsed technology solution for data vaulting is available today with Dell Technologies, and more offerings are coming.

Dell Technologies saw the importance of Sheltered Harbor's standard to protect public confidence in the U.S. financial system, thus becoming the first solution provider to join the alliance program. Dell already had a solution in the market that did most of what Sheltered Harbor wanted in terms of capabilities, but they reinforced the existing solution with new capabilities to meet the required controls. Specifically, Dell enhanced PowerProtect Cyber Recovery with the Sheltered Harbor concept of a secure envelope, which includes very specific encryption and validation protocols. Dell also added an external attestation message, which is another element of the Sheltered Harbor standard.

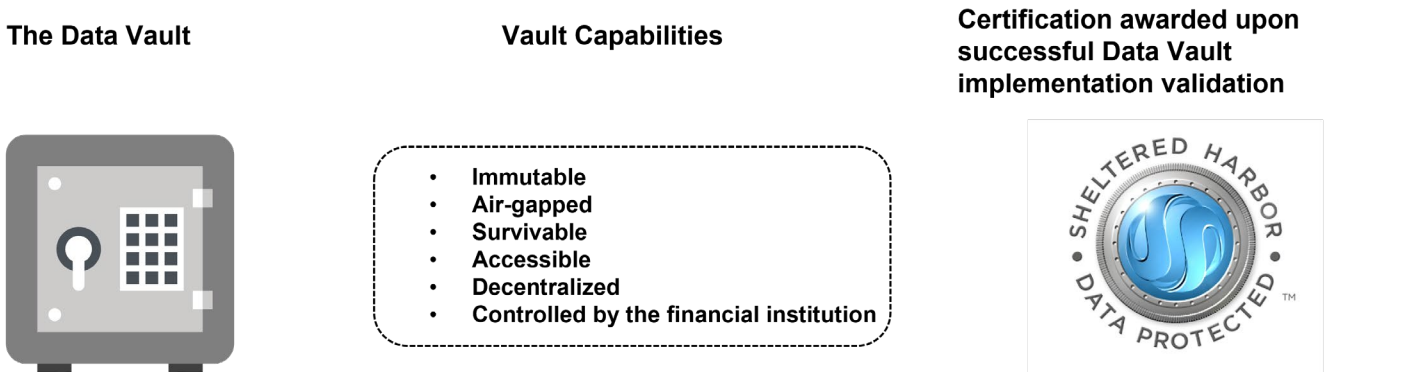
Engineers from Dell and Sheltered Harbor worked side-by-side to endorse a solution that could validate that data in the vault was untampered with without having to look inside at the data itself—people's financial data is obviously highly private and sensitive information.

The Sheltered Harbor Approach

Sheltered Harbor certifies financial institutions for resilience, but it does not certify specific vendors' products. It merely endorses them as having the right approach and controls necessary for financial institution certification.

From a financial institution's perspective, the Sheltered Harbor approach is straightforward: Protect the data by putting it into a cyber-resilient vault, and getting that certified. Then have an alternative restoration platform that could receive the data and support basic banking services (see Figure 3).

Figure 3. Key Sheltered Harbor Architecture Elements



Source: Sheltered Harbor

Following a ransomware attack or other disaster, it is imperative to start rebuilding the environment in a hurry. Sheltered Harbor data is a small subset of bank data. Further recovery work is going to be necessary after the Sheltered Harbor restoration platform is in use; it will take many days for IT to fully restore every system and application the bank might use.

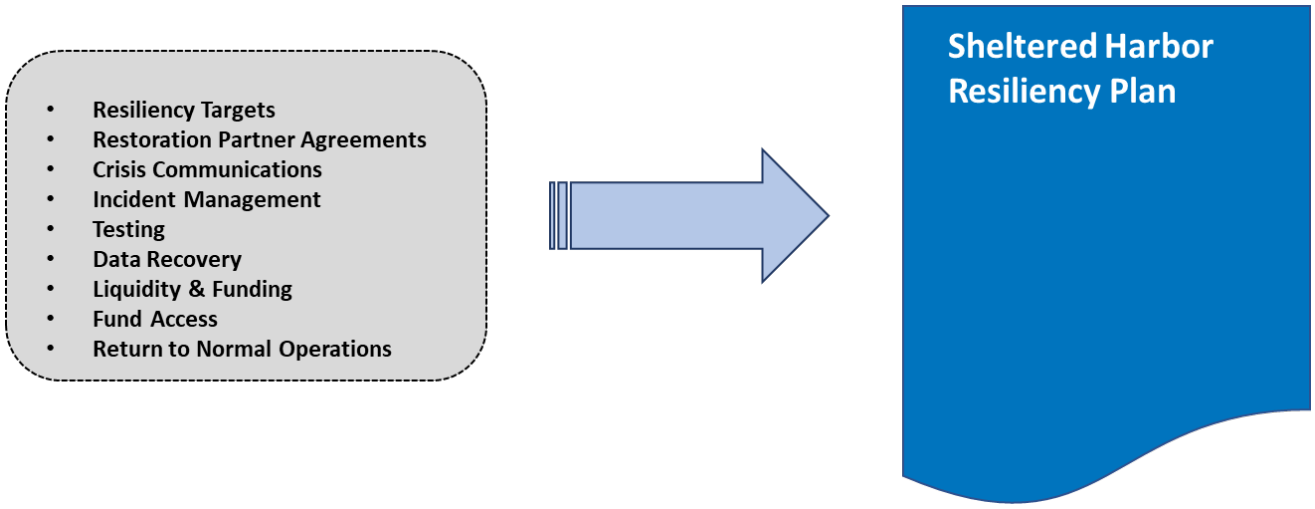
But what does the bank do in the meantime? That's where Sheltered Harbor's daily data vaulting process comes in. All of its participants implement this daily vaulting process, which is defined at a generic-requirement level. In other words, Sheltered Harbor does not require an organization to use specific vendors' tools, but rather, it specifies the general technologies, plans, and security controls that need to be part of the process for recovering private information.

Sheltered Harbor does not stop there, however. The data being stored every day is almost useless if it can't support the financial institution's primary need, which is to continue to give banking customers access to critical functions such as viewing account balances or making withdrawals. The overarching mission of Sheltered Harbor is to help financial institutions maintain public confidence during the worst moments of a worst-case scenario, when systems' operational capabilities are lost and customers are disconnected from their assets.

Sheltered Harbor accomplishes this effort by essentially removing all the noise from the process. To preserve public confidence, it is necessary to maintain simple business services. Customers must still be able to access their balance information. They have to remain confident that the bank knows what their balance is, that the amount is accurate, and that they can continue to make withdrawals, deposits, and transfers. That is the job of the restoration platform for the data. (An institution transmits data to the restoration platform, the platform decrypts the data, and then it restores customers' access to account information and funds.)

The missing piece was the resilience plan. Right now, every institution requires its own bespoke resilience plan, but the fundamental, basic core of those plans—the decision-tree templates, so to speak—are the same. The timing, settings, and people who get involved may differ at each bank, but the essence of what needs to be done in the worst of days—within 24 hours of an attack—is well outlined in the Sheltered Harbor resilience planning guides (see Figure 4).

Figure 4. Resiliency Plan Component Summary



Source: Sheltered Harbor/ESG

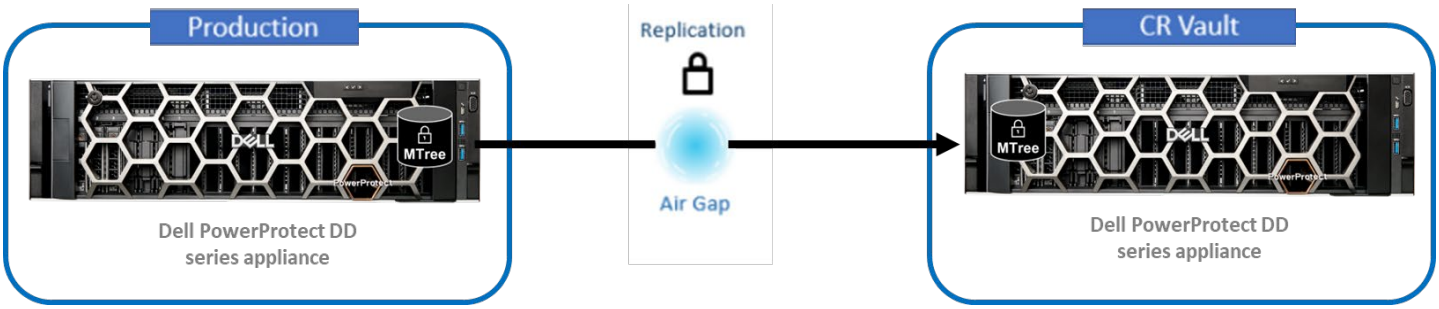
The Dell Technologies Difference

Sheltered Harbor does endorse products that meet its requirements, which include controls around security and confidentiality. But it only formally *certifies* the implementation as a whole, not particular products running within it. As we know, an organization could have the best tool in the world and misuse it. The product may be endorsed but be improperly installed or deployed in an unsecure environment. If the upfront data validation wasn't right, the bank won't get a formal certification from Sheltered Harbor.

A financial institution implementing Dell's solution only needs to run a test (which the Dell product enables very easily) to confirm the data matches properly. Sheltered Harbor will then certify that institution's protection of critical account data. Implementing Dell PowerProtect Cyber Recovery for Sheltered Harbor accelerates a participating institution's journey to certification. Several control points are built into that process, all fully validated, that an auditor doesn't have to check anymore.

Sheltered Harbor's goal is for Dell Technologies and the rest of its partner ecosystem to become the extended voice of Sheltered Harbor to the marketplace—not just to evangelize, but also to actually provide capabilities for institutions to implement Sheltered Harbor more quickly. Dell PowerProtect Cyber Recovery enables banks to do just that (see Figure 5). This is the first solution of its type to come to market—Dell received its solution endorsement in August of 2020, and the solution is now well established.

Figure 5. How Dell Technologies Supports the Sheltered Harbor Approach



Source: Dell Technologies

The Bigger Truth

It's one thing to put a bunch of specifications for cyber recovery down on paper. It's an entirely different matter to make that paper "come to life" when trying to overcome a ransomware attack or other disaster. The reality is that most organizations—even the biggest banks—don't have the ability to make most of it happen by themselves.

It is not sufficient to simply vault data by taking backups, encrypting them, and moving them offsite. That's not going to meet the requirement for recovery of critical banking services within 24 hours. Fortunately, Sheltered Harbor has come up with very specific standards tied to that requirement.

Sheltered Harbor is a de facto representative for the financial industry. The Sheltered Harbor solution enjoys favorable support from U.S. regulators, although it originated with funding from financial institutions interested in closing their data protection gaps.

Sheltered Harbor does not foresee or want a situation in which banks are fined if they are not certified. Rather, its whole goal is centered on protecting consumers, maintaining public confidence, and giving banks some breathing room in those first terrible hours following a disaster or successful ransomware attack. Becoming certified remains a voluntary effort, and the process is being continuously improved to minimize the time and cost required for implementation and certification.

Regarding Dell Technologies, its solutions have been inside most banking institutions for a long time, providing trusted, dependable, enterprise-level services. Dell Technologies is now helping those financial industry customers to bring Sheltered Harbor's concepts to fruition in a true better-together fashion, in a spirit of mutual aid to overcome the most extreme worst-case scenarios.

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188