Whitepaper

A Sheltered Harbor in a Cyber Storm

A joint whitepaper from Sheltered Harbor and Dell Technologies.

Introduction

Destructive and ransomware-based cyber attacks have unfortunately become commonplace, with frequent headlines about successful attacks. Overall, criminals were paid over $350 million in cryptocurrencies for ransoms in 2020[1]. With such a lucrative opportunity, cyber criminals have banded together to create a sophisticated and flourishing underground economy which is unlikely to disappear, according to Threat Post[2].

These attacks are more than just a painful nuisance or expense. They threaten critical infrastructure, the ongoing viability of institutions and organizations, as well as consumer trust and confidence that drive worldwide economic activity. They can also lead to injury or death. What's more is that the White House released a memo in June 2021 that stated "all organizations must recognize that no company is safe from being targeted by ransomware, regardless of size or location"[3]. Three attacks in May 2021 prove the point: an attack on a critical US pipeline provider created almost immediate gasoline shortages on the East Coast; another disrupted the meat supply chain; and the third disrupted health care throughout most of Ireland.

To many, the pace of the attacks seems to be escalating. But the attacks are not new, and organizations continue to struggle with how to best prepare for and respond to them. Cybersecurity controls to prevent or limit attacks remain important, but ultimately insufficient. Challenges created by human interaction with IT systems, sophisticated supply chain attacks, zero-day vulnerabilities and other sophisticated techniques mean that some attacks will be successful. An organization must be prepared to be resilient, including recovering IT systems after a successful attack to a previous, "known good" state.

This paper provides an in-depth review of two similar frameworks that help to form an overall resilience strategy.

A singular approach to an extreme but plausible event

In early 2015, after the now infamous cyber attack against a global entertainment corporation by a nation-state, many organizations began trying to address the problem of destruction by a cyber attack. Previously, most criminal cyber activity focused on stealing data from organizations, usually taking special efforts to avoid detection and any type of disruption that might call out the presence of the bad actors. A cyber attack designed to directly impair or destroy an organization through attacks on its IT infrastructure presented novel issues.

In response, in 2015, leading financial institutions, industry trade groups and large service providers established the Sheltered Harbor initiative to evaluate and solve for the risk that these attacks posed to the US Financial System. Dell Technologies (at the time as EMC Corporation) also began working on the problem at the behest of some of its most important customers in both financial and other industries.

Although working on slightly different goals, both organizations attacked the problem with the same basic three-part framework:

- Identify the most critical business services that must be protected and resilient in the face of an "extreme but plausible event", and ultimately map these to the IT data and/or applications necessary to support them.
- Protect the data and/or applications supporting the processes in a highly secure data vault, defining the requirements necessary for such a vault.
- Enable planning and processes to enable recovery from that event within parameters (such as an extreme event RPO and RTO) required to meet the base goal.

For each of these requirements, Sheltered Harbor and Dell took slightly different approaches that should prove useful to anyone looking to improve their resiliency.

Concern #1: Determine what must be protected

Initially, it seems a simple task to determine what is most important to an organization's ongoing viability – what must be protected to enable the recovery from an extreme event. However, in reality the process can be very complex, and it is imperative to get this first step right as it drives the remainder of the process.

[1]Ransomware Task Force, "Combating Ransomware A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force": https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force_Final_Report.pdf
[2]Threat Post, "A Peek Inside the UnderGround Economy": https://threatpost.com/inside-ransomware-economy/166471/
[3]White House Memo, June 2, 2021: "What We Urge You To Do To Protect Against The Threat of Ransomware": https://docs.google.com/viewerng/viewer?url=https://www.mainstream-tech.com/wp-content/uploads/2021/06/White-House-Memo-what-we-urge-you-to-do-to-protect-against-the-threat-of-ransomware17.pdf&hl=en

A first key is to clearly establish the main goal of the undertaking in specific terms. This must be driven by a broad view of the business needs that are critical to survival, i.e. beyond mere IT functions and not just those who are involved in cybersecurity, or even risk or compliance. From this first key step, capabilities required to support the services can be identified. In this digital world, that most often is focused on information technology.

The components required for business processes and information technology also need to be determined in great detail. These include data that can change rapidly or frequently (for example, a list of depositors and their account balances); it may require off-the-shelf or custom applications to interact with that data (a database application, a core banking application, a trading platform); and usually also requires technology "plumbing" such as domain controllers or authentication technologies, Domain Name Service (DNS) to resolve server names, etc.

Sheltered Harbor had a very clear and focused goal – to protect consumer confidence. This led to further refinement, such as a goal that their process would operate only until the institution was able to recover itself, or in the worst case, was resolved. With their laser focused goal and short operational timeframe, Sheltered Harbor was able to boil everything down to two capabilities and essential services: providing customers continued access to their account balance information and cash. In turn, this enabled the Sheltered Harbor Specification to laser focus on a specific, industry-standardized data set. By narrowing the focus to this specific data set, Sheltered Harbor could avoid the complexity of having to also protect myriad applications and underlying technologies, enabling the creation of a common restoration platform (which is covered in Part 3) for those two critical business services.

The Sheltered Harbor standards combine secure data vaulting of critical customer account information and a resiliency plan to provide customers timely access to their data and funds in a worst-case scenario. Sheltered Harbor resiliency standards are proven, mature and have an ecosystem to support adoption, implementation, and certification. Financial institutions that successfully implement the standards achieve Sheltered Harbor certification. Sheltered Harbor is currently open to U.S. financial institutions of all types. It has grown beyond its original base of banks, credit unions, broker-dealers, industry associations, and core service providers. The newest standards now accommodate insurers, custodians, asset managers, clearing houses, etc. Visit shelteredharbor.org for more information.

The Dell process is similar in how it begins but rapidly differs because it is specific to each customer, which normally focuses on maintaining its own viability. In addition, Dell customers can be from any industry and of various sizes and levels of sophistication. The question in practice therefore becomes slightly different - what are the most critical services that power this organization? Determining the key services can be based on the organization and are often focused on revenue or profit, protecting a brand or intellectual property, or satisfying regulators.

Once established, the technology components underlying these applications must also be identified so they can be protected, such as databases, configuration files, application code, etc. And finally, any key underlying technologies required by the application, which are frequently Active Directory, DNS, etc.

Concern #2: Characteristics of a data vault

After determining what must be protected, the next question becomes: how should it be protected? Organizations protect their data in various ways – through role-based access controls; encryption in flight, at rest and sometimes at the application or database level; through replication and backup; etc. Many common controls are designed to protect the confidentiality of data, so that unauthorized access is not permitted. For this use, the availability and integrity of the data are paramount.

In this use case, it quickly became clear that data had to be protected in the strongest possible method. The data had to survive a sophisticated - and intentional - worst-case event - bad actors who completely controlled production and had access and knowledge to compromise most normal security methods. This quickly led both Sheltered Harbor and Dell to the concept of a data vault – an ultra-secure environment where data can be safely stored, which remains inaccessible but secure even while being updated.

Sheltered Harbor specifies a handful of critical requirements for data vaulting:

- Immutable (Unchangeable, and not subject to deletion)
- Air-gapped (Isolated from your production and backup systems)
- Survivable and Accessible (Non-reliant on infrastructure that can be compromised)
- Decentralized (Not reliant on any single production environment)
- Data fully Owned, and vault Controlled by the financial institution

These key tenets became the foundation of the Sheltered Harbor data vaulting Specification.

Dell landed on similar requirements, which ultimately have been expressed as three key capabilities:

- **Isolation.** The components of the vault must be isolated, i.e. inaccessible to bad actors. This resulted in the use of the term “air gap”, where the components of the vault are in a physically separate area and are generally in an “off” state so that they cannot be accessed. In addition, this on/off mechanism had to be controlled from the secure side so that a bad actor controlling production could not manipulate it.

- **Immutability.** Once written, the data in the vault needs to be “immutable”. For Dell, this meant the compliance retention locking capability in its Data Domain platform, which had been attested years prior as meeting a well-known records standard under 17a-4(f)(ii). This capability was further hardened to take into account various attack vectors, such as time-based attacks, which were not necessary in the records standard.

- **Intelligence**. This capability is intended to answer the question of whether the data being protected is valid for recovery. Doing this requires scans of vaulted data looking for evidence of corruption – not for malware.

Concern #3: Restoration Planning and Processes

Ultimately, the goal is not to protect data, but to use the protected data and other systems to restore critical operations and services as quickly and efficiently as possible after an event or attack. Once again, given their different goals, Sheltered Harbor and Dell diverged on their processes but began with the same initial concerns.

Sheltered Harbor’s unique focus on maintaining public confidence, initially for deposit and brokerage account holders, allowed it to focus exclusively on the business processes that provide account balance information and fund access from those accounts. Since these processes are fairly universal, the Sheltered Harbor community was able to define specifications for a common ‘restoration platform’ that would understand a standardized set of data for brokerage or deposit accounts. And with the industry coordinated to rely upon such services, getting existing industry service providers to build and make such ‘restoration platforms’ available allows for a common solution, which lowers everybody’s cost and risk. Here, the Sheltered Harbor community has done the work of defining the critical business processes as well as the technical capabilities that are required for a quick restoration that is of mutual benefit to all participating institutions.

The Dell model encourages customers to have a good foundation of the post-attack recovery processes so that they can establish reasonable cyber attack specific recovery point objectives (RPOs) and recovery time objectives (RTOs). Normally those vary substantially from their counterparts in Disaster Recovery (DR), where active-active architectures can be built with zero or minimal RPOs and immediate RTOs. Those just are not possible in a sophisticated cyber attack, where data centers may need to be temporarily shut down while the attack is investigated, forensics processes must complete, and root cause is determined before clean-up / recovery procedures can begin.

From there, recovery can take many forms but typically involves restoring critical rebuild materials (eg AD, DNS), applications and data securely back to the original environment after it has been re-secured. The process typically depends in large part on the scope and sophistication of the attack and related breadth of destruction. Applications can be restored directly to production, or they can be initially recovered in a “clean room” environment to allow for in-depth forensic testing before being pushed back into production. Run books are developed and then tested to ensure that organizations know how to proceed in a recovery scenario.

Dell believes that the recovery process is beginning to mature with a focus on enabling recoveries to alternate locations, such as public or private clouds, or shared or otherwise available infrastructure from third parties such as IT service providers. For example, a data vault protecting on-premises applications could be used to immediately begin recovery operations to a shared infrastructure environment, rather than waiting for forensics, root cause, clean-up, etc. This will still require secure recovery processes, and fail-back considerations have to be resolved, but the opportunity exists to substantially minimize the RTO.

This alternate recovery process has interesting similarities to the Sheltered Harbor model but is likely to involve infrastructure and not a full restoration platform which requires only data to be operative.

Conclusion

A successful ransomware or destructive cyber attack on a financial institution poses significant compliance, financial, legal, regulatory, and reputational risks and interferes with the institution's ability to operate, which can threaten consumer confidence and perhaps its ongoing viability. As a financial institution, it is your responsibility to protect your customers' accounts. Help us protect public confidence in the U.S. financial system – join Sheltered Harbor today.

What will you get?

- Exclusive access to the industry-developed standard for protecting and recovering customer account data
- Specification; Subject Matter Experts; Working Groups; Forums; Implementation Guides; Incident Playbooks
- Help continue development of more resilient data protection and grow with Sheltered Harbor as it expands protected asset classes and geographies
- Be prepared to respond to and recover from an extreme event
- Acknowledged by the U.S. financial regulators for data protection and resilience
- Easy to implement and certify
- Enhances your financial institution's resilience and reputation
- Low-cost, high value
- Leverage the Sheltered Harbor best practices beyond just the Sheltered Harbor extreme case

How much does it cost?

Participation fees to join Sheltered Harbor are minimal. Annual Participation fees range from as low as $250 to a max of $50,000 depending on asset size. Implementation costs vary by size and complexity of institution as well as infrastructure, operations, and skills base.

Authors

Carlos Recalde
President & CEO
Sheltered Harbor

Jim Shook
Director, Cybersecurity & Compliance Practice
Dell Technologies