

AHEAD

The Six Pillars of Ransomware Recovery



Ransomware

The word that scares and petrifies IT organizations and cyber insurance companies alike is on the rise – and companies are looking everywhere for ways to avoid paying the ransom. As ransomware grows to be a top concern for enterprises, vendors across the IT landscape are offering recovery solutions that they claim will help stop ransomware in its tracks and ensure that businesses can quickly recover and resume normal operations. While those promises sound great, that is only one small piece of a much bigger pie.

Ransomware resiliency is a multi-faceted approach that requires support across many different IT teams, such as security, governance, operations, data protection, networking, and incident response, just to name a few. These teams must collaborate and align their visions to stitch together a solution that identifies what data needs to be protected, how that data should be protected, and how to build in operational governance and compliance to ensure recovery.

With this in mind, AHEAD has identified six key pillars to build out a comprehensive ransomware recovery strategy for organizations.

01 Enterprise Skills Initiatives

02 Application Analysis

03 Modern Ransomware Recovery Solution

04 Incident Response Integration

05 Governance & Management

06 Security Integration

Each of these pillars requires thoughtful planning to baseline where an organization stands today and how to build maturity around ransomware recovery.

Ransomware Recovery Operating Model

01 ENTERPRISE SKILLS INITIATIVE



Education & Skillsets

02 APPLICATION ANALYSIS



Service Mapping

03 MODERN RANSOMWARE RECOVERY SOLUTIONS



Data Protection - Cloud, DC, SaaS & Edge Targets



EDR, Backup & Cyber Recovery



Network Design & Zero Trust Maturity

04 INCIDENT RESPONSE INTEGRATION



Monitoring, Logging & Alerting



Enterprise Service Management



Runbooks & Recovery Plan

05 GOVERNANCE & MANAGEMENT



Roles & Responsibilities



Policy & Procedure

06 SECURITY INTEGRATION



Identity & Access Management



Security & Compliance

01

Enterprise Skills Initiatives

Among the most common tactics, techniques, and procedures (TTPs) that bad actors utilize to gain unauthorized access to systems are email phishing attacks and the exploitation of vulnerable web applications running on unpatched systems. Education and training are fundamental elements that reduce the risk of an attacker being able to successfully implement these common methods. Users must understand the risk of clicking on malicious links or leaving systems unpatched, as these actions keep the door open for bad actors to infiltrate their environment, install command and control software, and encrypt and exfiltrate sensitive data.

When beginning the process of building out a ransomware recovery journey, organizations need to ask themselves if they have an effective training and education plan with their workforce. There are plenty of third-party organizations dedicated to providing such training if it is beyond the capabilities of the internal IT staff to deliver and test the organization on phishing and security preparedness.

Training the organization is just scratching the surface, however. When a business is compromised, it is critical that the IT organization (and others within a company) knows exactly what to do in the event of a ransomware attack. The first step is for organizations to simply ask their teams if they are aware of what should be done. There is a strong chance that teams may not be educated on the proper procedures to preserve as much forensic evidence as possible – not only for internal security/incident response teams, but for law enforcement and cyber insurance purposes. Properly documenting these procedures and building in alerts and automation to assist with the process ensures that evidence is well preserved, the blast radius of an event can be reduced, and that in a cyber incident, nobody hits the panic button. Performing tabletop or cyber-readiness exercises are good ways to provide reinforcement learning for the organization.

02

Application Analysis

Understanding what applications, data, and services are critical to an organization is a necessary step in building out an effective ransomware recovery strategy. The most common effort that most organizations will undertake is building a Business Impact Analysis (BIA). Some key questions that organizations should ask themselves include:

- What is the cost of downtime to my business?
- Is there a defined list of applications that are required to run the business and other key services that need to be provided?
- Depending on the vertical, are there external, non-monetary factors that could impact

people, clients, and external parties if there is downtime (e.g., Colonial Pipeline attack, a healthcare organization losing access to critical care systems, etc.)?

- What is the current cybersecurity insurance policy, what does it cover, and what safeguards need to be in place to ensure the claim will be processed?

Once this and a number of other questions have been considered, calculating the cost of downtime, loss of reputation, and other fines can help define the current state and build a business justification for pursuing ransomware prevention and recovery solutions to enhance an organization's cybersecurity posture.

SERVICE MAPPING

In addition to building a BIA, gaining complete visibility of applications and their dependencies allows organizations to make more precise decisions when sizing a vault and/or recovery environment. While the easiest approach may be to build an environment to support a certain percentage of the workloads, truly understanding service mapping is key to architecting a solution that is not over or undersized.

There are many tools in the industry that can help build out these service maps (e.g., ServiceNow Discovery, Flexera One Cloud Migration Planning, Guardicore) to ensure that the applications,

data, and services are accounted for in the vault. Some of these tools either integrate with—or are native to—platforms that might already be in place inside an organization or have multi-purpose use cases that can provide additional value. This means that choosing the right service mapping tool requires a firm understanding of whether there are any other overlapping projects with similar use cases. Additionally, depending on the solution, some may offer the flexibility for a one-time assessment or a long-term subscription that will update and maintain these service maps. Without utilizing a service mapping solution to understand the applications and related services, the organization runs the risk of missing an interdependency. While ransomware recovery solutions protect the data that is part of the protection workflow, additional missed data or applications could render the recovery obsolete and prevent the protected application/service from resuming normal operations.

Lastly, building these service maps can assist with vendor selection for ransomware recovery solutions because they will define which applications, operating systems, locations (e.g., cloud, edge, on-premises data centers, SaaS applications, etc.), and data sets need to be protected. This will also ensure that any applications or data not currently protected by a data protection

offering are accounted for in the vault design(s). As the maturity of a ransomware recovery solution evolves within an organization, maintaining an up-to-date service map is crucial. The service map should be validated at a specified interval (i.e., quarterly, semi-annually, annually) so that as applications are upgraded or retired, the ransomware recovery solution can be updated to protect all mission critical data.



03

Modern Ransomware Recovery Solution

The pillar that gathers all the headlines and focus from organizations is the selection of a ransomware recovery solution. When evaluating these solutions, it is important to understand, first and foremost, where the data that is being protected resides, as that will influence the types of solutions that are supported.

Here are a few examples of initial key questions to help understand an organization's requirements for a ransomware recovery solution:

- Where does this application or service reside (e.g., cloud, data center, SaaS application, at the edge)?

- What operating systems need protecting (e.g., Linux, Windows, AIX, mainframe, etc.)?
- Are there application-consistent backups that need to be taken (e.g., MS SQL, Oracle, Exchange, etc.)?
- What are the subcomponents required to bring the application online?
- What are your Recovery Time Objective (RTO) expectations for restoring your applications from a breach?
- How will the solution achieve an immutable copy of the data?
- What level of analytics needs to be run against the protected copy of the data?
- Are there any systems not protected by a data protection solution that need to be accounted for (e.g., multi-PB file systems, AWS S3 buckets, etc.)?
- What is the size of the blast radius you want to be able to recover (e.g., single app or the entire environment)?
- Does the solution need to support all locations/use cases or is there a preference for best-of-breed solutions?
- Are there regulatory requirements that drive recovery objectives and timelines?
- Does your cyberinsurance policy mandate a particular method or partner for recovery efforts?

Answering these initial questions will provide a good baseline of requirements to aid in the vendor selection process. Most organizations have some data protection solution(s) in house already. However, based on defining the above requirements, it is possible that a new solution may be necessary to meet the ransomware recovery needs.

The type of vault (and the requirements of what is needed) is important because it will typically drive cost and complexity as more features and capabilities are added. For example, a solution that provides only an immutable backup architecture will typically be cheaper and less complex than a full clean room and data forensic capabilities, where immutable backups are complimented by analytics that search for anomalies to alert to a potential ransomware infection prior to an event taking place. Mileage will vary based on the variant of ransomware and attack vector, but these features can add an additional layer of resilience if this is mandated by the security organization or if there is a requirement from a cyber insurance policy.

Data protection vendors have various strengths and weaknesses based on their offerings. It is vital to align the organizational requirements against a vendor's capabilities to make a thoughtful, defensible argument when it comes time to procure the solution.

GOOD

Data Protection Best Practices

- Protect data everywhere (on premise, cloud, end-point)
- 3rd copy on disk or tape
- Network segregation, separation of duties
- Recovery drills
- Immutable snapshots
- Up to date code and firmware
- Access controls in place

BETTER

Immutability (Hardening)

- Product specific hardening guides
- Encryption in flight and/or at rest
- Multi-vendor Support
- Retention lock with separate security officer credentials
- Two-person authentication

BEST

Air Gap with Immutable Copies & Analytics

- Network, management, and physical Isolation
- Isolated immutable copies of backup data and catalog
- Data analytics to validate data and provide quick insight into compromise
- Control planes

As the environments that need to be protected expand to public cloud, SaaS, and other use cases, the vault build-out will also require time spent properly setting up the network itself as well as network security capabilities. This is where certain ‘Zero Trust’ solutions (e.g., Privilege Access Management systems, micro-segmentation policies, etc.) can be augmented to support the network and security build-out.

RANSOMWARE RECOVERY VERSUS DISASTER RECOVERY

One point that organizations should understand is the difference between ransomware recovery and disaster recovery. While their approaches will be similar, the solutions an organization builds out will be fundamentally different and most likely use separate environments or infrastructure. Disaster recovery is focused around providing operational recovery of applications and systems when the production location of these applications is impacted by an event (e.g., hurricane, fire, building collapse, etc.). Ransomware recovery, on the other hand, is about being able to protect and recover data in an isolated recovery environment. See the figure below for key differentiators between ransomware recovery and disaster recovery.

CATEGORY	DISASTER RECOVERY	CYBER RECOVERY
Recovery Time	Close to Instant Based on SLA	Reliable & Fast, Tested and Validated Immutable Backups
Recovery Point	Ideally Continuous	1 Day Average (Reduce Time Vault is Open)
Nature of Disaster	Flood, Power Outage, Weather	Cyber Attack, Targeted
Impact of Disaster	Regional; typically contained	Global; spreads quickly
Topology	Connected, multiple targets	Isolated, in addition to DR and operational backup and recovery capabilities
Data Volume	Comprehensive, All Data	Selective, includes foundational services/ critical rebuild materials (ex. DNS, AD, application binaries, etc.)
Recovery	Standard DR (e.g. failback) Hours to Days based on Recovery SLA	Iterative, selective recovery; part of IR Days to Weeks depending on IR response

DEFINING RECOVERY POINT & RECOVERY TIME OBJECTIVES

One important item that is worth discussing involves recovery point objectives (RPO) and recovery time objectives (RTO). With ransomware recovery solutions, vendors will highlight their capabilities in driving these two points as low as possible. In reality, it is much more difficult to quantify exactly what the RPO and RTO of a solution will be.

RPO will be based on when the last known uncompromised backup took place. Depending on how long the ransomware might have been in the environment, the organization may need to roll back to an older backup. This is where it becomes absolutely crucial that the security and IT operations teams agree to a worst-case data retention length (based on needing to recover data). In the event that all other prevention or detection mechanisms are bypassed, this will be vital in determining what the RPO can be if a long rollback is necessary.

From there, RTO is also a challenge to properly define, since a ransomware recovery solution is distinct from a disaster recovery solution. The problem being solved is not one of a fire hitting a data center. Rather, it is a

cyber incident whose recovery time is determined by an incident response plan, forensic scanning of the data that is required, and the process to recover and promote an uncompromised application back into service.

This can vary in time (depending on the extent of the infection) from potentially days to weeks or months. Even with the resources and infrastructure needed to support the volume of recovery, the process of rehydrating, scanning, processing, and validating these workflows can take a long time. If the application needs to move environments (e.g., cloud to on-premises or vice versa), this can further extend recovery times.

While these solutions are an integral element in ensuring that an organization can recover from a cyber incident, it is important to account for the other pillars to ensure that a solution that meets all technical, business, and operational needs.

04

Incident Response Integration

During the vendor evaluation process for a ransomware recovery solution, it is essential to align the organization's incident response processes and workflows. One of the primary items that an organization must address is their incident or ransomware response plan. Depending on the size of the organization, an incident response team (IRT) can be defined internally or contracted to a third-party managed service provider who can assist in building out the process, identifying resources that need to be involved, defining the necessary tools or technologies, and determining the response plan itself.

Once the incident response (IR) process has been defined, it is important to incorporate

the ransomware recovery workflows into that process. These IR requirements influence both the solution types and the vault definitions. Some open questions that are key to address for incorporating the IR process and ransomware recovery solutions include:

- Where is the location of the target recovery environment?
- Is there a need to have a clean room, isolated network environment to assist in the restoration, data scanning, forensic data collection, and validation processes to promote back to production?
- What security logging solution is in place today and where does that reside (on-premises or cloud/SaaS)?
- What DNS is in place?
- What monitoring and IR tools (e.g., Endpoint Detection and Response, Data Loss Prevention, DNS, IPAM, Privileged Access Management, etc.) are in place today?
- Where do you store application binaries?
- What are the service dependencies for recovering critical applications and have those services been accounted for in recovery processes?

If a clean room is needed when building a recovery environment, there are items outside of the recovery tooling that are required

to help with the overall scanning and cleaning process. It is pivotal to understand which critical components need to be protected in this isolated, clean room environment. Ransomware attackers have grown more sophisticated and will not only attack production applications and the backups of those applications, but they will often encrypt or poison DNS and Active Directory (AD) services to get organizations to pay the ransom. Essentially, if organizations cannot log-in and authenticate to recover the backups, then all of these recovery solutions are rendered ineffective. Depending on where the vault resides, there may be a need to add infrastructure or reserve compute/storage/network capacity in a public cloud provider, guaranteeing the ability to recover. Templatizing and automating as much of this as possible will further reduce the amount of time it takes to recover, scan, clean, and promote the workloads back into a working, production state.

Once this clean room and recovery process is established, it is important for the IRT and application teams to work together to define the recovery process and build in the run books. Particularly when certain components of the applications need to be rebuilt from scratch or deployed in a different environment entirely (e.g., workloads migrating to the public cloud), it is a good idea to document those run books and validate during scheduled tests. Much like organizations that run disaster recovery tests or simulations, a business will want to take all of these processes and run similar exercises for ransomware recovery. This requires joint partnership throughout the organization to understand what this process looks like and validate that everything worked as expected. If it does not, it is important to make any adjustments and update the necessary recovery processes and procedures to ensure that if a worst-case scenario happens, the organization is prepared to spring into action.



05

Governance & Management

The pillar that likely draws the most groans within any organization is governance and management. When building a ransomware recovery solution, it is important to establish roles and responsibilities for who owns the solution and who needs to be involved and engaged at the various stages of recovery. Further, those roles and responsibilities should be established with any third-party vendors or managed services providers who are in the mix as well. Building out this documentation and responsibility matrix (commonly known as a RACI matrix) helps in task definition across the recovery workflow and assists in avoiding conflict between the many teams and resources that are frequently engaged in a cyber incident.

By confirming that all teams are aligned and in agreement with these definitions and responsibilities, it also ensures that the stakeholders are properly engaged and can build out the communication and action plan to the rest of the business.

In addition to roles and responsibilities, it is essential to establish policies and procedures specific to the vaulted capability. These include defining aspects such as:

- What is the process for an administrator to request PAM access to the vault? Who approves it?
- What is the frequency of re-certification of vault access?
- What is the process for promptly terminating access for departed personnel or changes in job function?
- How is change management being implemented for the vault?
- How is patch management being done in the solution?

No matter how organizations define these processes and procedures, they are a critical component for a ransomware recovery operating model to ensure an effective plan.

06

Security Integration

The final pillar of the ransomware recovery operating model is security integration. It is critical to harden and secure the solution in alignment with best practices focused on leading security frameworks to minimize both the vault surface area and risks to the solution. It is also essential that teams across the organization have the right mentality to understand that the solution is not simply another application or backup. Rather, this environment needs to be heavily secured as it is the last option for recovery in the event of a ransomware attack. With this in mind, incorporating capabilities for secure access through privileged access management (PAM) using least privilege principles is of the utmost importance.

As the solution is designed and implemented, the organization-specific approach to PAM for the vault must be defined. In many cases, using existing instances of an enterprise PAM solution tied to existing AD users poses a risk, because if the PAM instance or AD were compromised, unsanctioned access could be gained to the vault. To avoid this, it is generally recommended that a separate PAM solution with non-enterprise AD accounts be used to access and manage the recovery solution. Additionally, even within PAM, least privilege access is a well-established rule for reducing access to the minimum level needed to perform functions. With Zero Trust solutions driving these concepts forward, it is important for a ransomware recovery solution to integrate at least one element of Zero Trust around identity and access management. An example of this might include workflows that prevent compromised credentials from being able to expire or compromise backups. Some vendors can even require support to be engaged to add additional administrator accounts, expire backups if retention locks are enabled, or alert to unusual activities with privileged access/admin-level accounts. These capabilities can also help separate roles and responsibilities to prevent insider threats from being able to negatively impact a ransomware recovery environment by ensuring that administrators do not have full access to some of these activities. Integrating multi-factor authentication is another important feature that helps to verify that even if credentials are compromised, there are additional controls in place to avoid bad

actors from performing malicious activities in the ransomware recovery environment.

If there are key administrator accounts that need to be reserved strictly for use in a recovery environment as the clean room environment is built for ransomware recovery, PAM can once again be useful in limiting access on a timed basis.

Beyond access management, the cyber recovery solution must implement additional controls and approaches to minimize risk. This includes aspects such as: hardening vault infrastructure; ensuring vault assets are monitored 24x7; establishing a plan for vulnerability management and patching of vault assets; establishing a secure NTP source that is not tied to production; and lastly (but certainly not least), maintaining the overarching mentality that aside from the backup data being replicated into the solution, the vault is an outbound-only solution. All of these activities are done to guarantee compliance, reduce access to what is required, and ensure proper security controls are in place to align to best practices.



Where Do We Go from Here?

Ransomware recovery is more than just a backup and recovery solution, and it does not serve as an alternative to disaster recovery. Rather, it is meant to help organizations recover from a cyber incident and ensure that an organization's most critical applications and data are protected from threat actors that want to gain access, exfiltrate data, and encrypt systems to get companies to pay ransom. And as threat actors become more sophisticated in their approach, it is increasingly vital to have a sound ransomware recovery plan in place.

By prioritizing the crucial applications and services that require protection, organizations can begin to develop a thorough ransomware maturity roadmap. Companies should review this roadmap, validate their capabilities at a defined interval (quarterly, semi-annually, annually), and take proactive steps to ensure that goals are being met. If there is additional maturity that needs to be built into their processes or tooling, organizations can prioritize and budget for open items (e.g., building or expanding the size of a clean room, expanding what is protected by the ransomware recovery solution, integrating additional security safeguards or measures, etc.).

As Bruce Schneier wrote in his essay, *The Process of Security*: "Security is a process, not a product." The same can be said for ransomware recovery. It is only when an organization's process maturity compliments the available ransomware recovery tooling that they truly have the ability to deliver a sound operating model to the business. By leveraging the six pillars outlined above, organizations will provide a foundation for maturing their journey in the fight against ransomware threats.



Contributors

Mike Caplan

PRINCIPAL CLIENT SOLUTIONS ARCHITECT

About AHEAD

Combining cloud-native capabilities in software and data engineering with an unparalleled track record of modernizing infrastructure, we're uniquely positioned to help accelerate the promise of digital transformation.

National Hubs

ATLANTA

1117 Perimeter Center
W406
Atlanta, GA 30338

CHICAGO

401 Michigan Ave.
#3400
Chicago, IL 60611

SAN FRANCISCO

2000 Crow Canyon Place
Suite 250
San Ramon, CA 94583