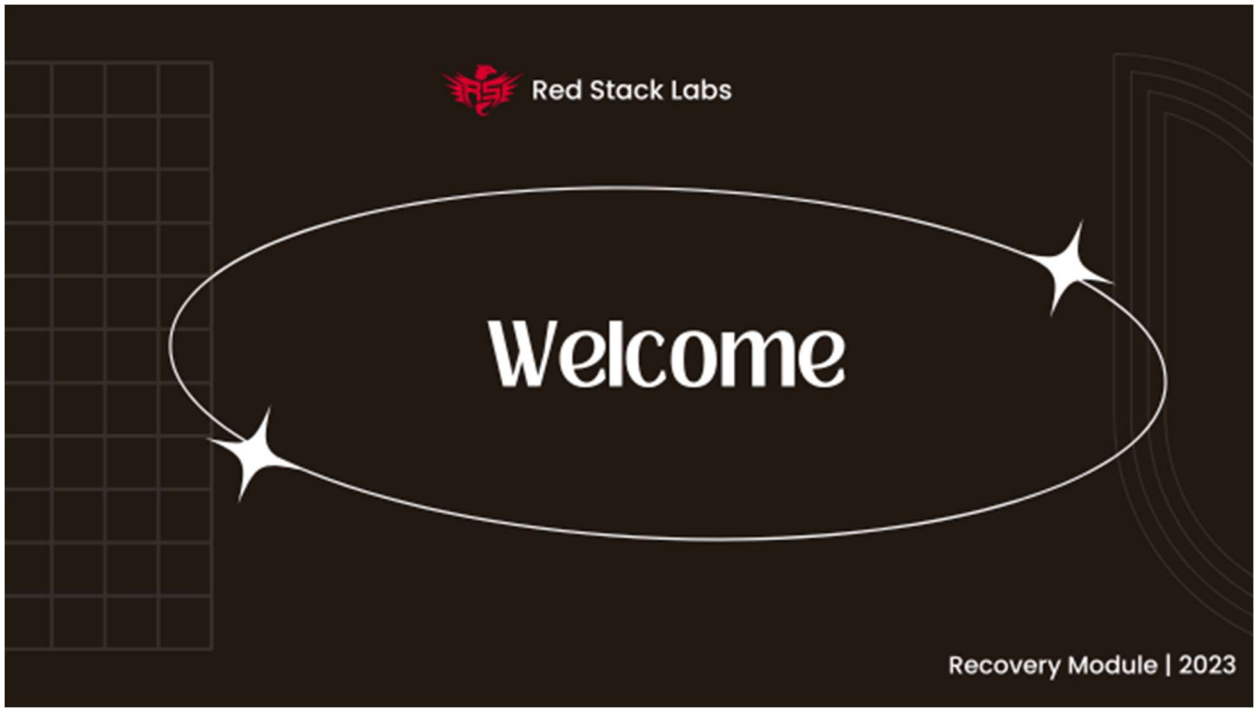
Recovery – Book 3

Corporate Liability Reduction

Ermis Catevatis
RED STACK LABS CORP

Version	Date	Author
0.1	August 03, 2022	Ermis Catevatis
0.2	Sept 12, 2022	Ermis Catevatis
0.3	Sept 25, 2022	Ermis Catevatis
0.4	Nov 04, 2022	Ermis Catevatis
0.5	Nov 16, 2022	Ermis Catevatis
0.6	Jan 10, 2023	Ermis Catevatis
1.0	Jan 15, 2023	Ermis Catevatis
1.1	Oct 02, 2023	Ermis Catevatis

Contents

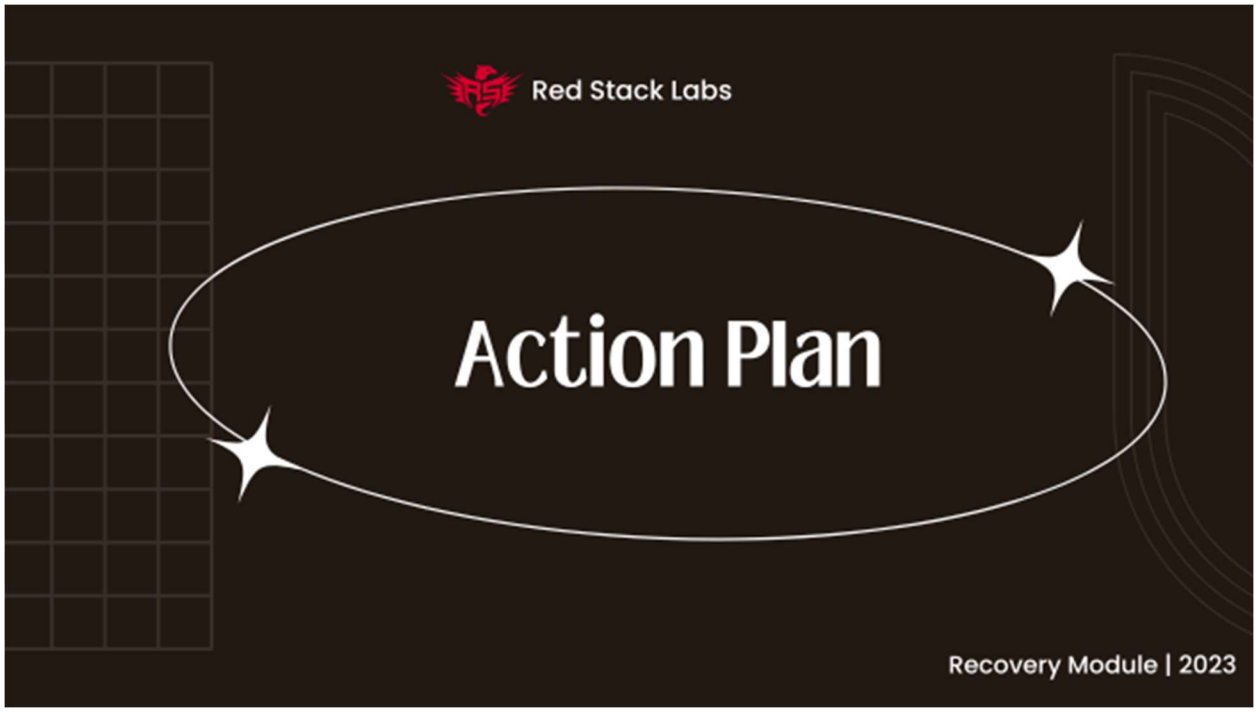


Welcome

We're delighted to welcome you to the "Incident Recovery" course. This program has been developed to provide you with a comprehensive understanding of handling and recovering from cyber incidents. As you embark on this adventure with us, bear in mind that each section is intended to equip you with the critical skills needed to protect your organization from cyber threats and enhance your incident response and recovery capabilities.

This course will guide you through the details of incident recovery plans, elucidate on roles and responsibilities in collaboration and response, and offer insight into establishing secure backup systems and effective recovery procedures. Our content, expertly curated, includes case studies and interactive tests to ensure you're not just absorbing information, but applying it practically.

Prepare to dive deep! We trust that the knowledge and skills you'll acquire from this course will significantly enhance your organization's readiness to handle cyber incidents. Remember, we're here to support you throughout this learning experience. Therefore, if you have any queries or need any assistance, don't hesitate to ask. Here's to a fruitful and enlightening journey ahead!



Action Plan

Welcome to the next step in your journey towards mastery in incident recovery. After studying the course material, undertake the following tasks to fully utilize the insights gained:

1. **Digest Course Material**: Ensure that you've thoroughly absorbed and understood the course content, from the necessity of an incident recovery plan to the core concepts of creating one.
2. **Use Our Template**: Make full use of the provided incident recovery plan template. This is a tool you'll have upon completion of the course, allowing you to build a tailored plan for your organization.
3. **Evaluate Your Existing Plan**: If your organization already has an incident recovery plan, review its details and potential gaps using the principles learned in the course.
4. **Develop and Refine Your Plan**: If your organization doesn't have a recovery plan, your objective should be to develop one. Use the guidance provided in the course to assess your needs and identify measures that align with your organization's requirements.
5. **Apply Your Knowledge**: Let's put your knowledge to the test. Evaluate how your recovery plan (or prospective plan) will assist your organization in the event of a cyber incident. Identify potential weak points and strengthen them. Understand the steps necessary to execute the plan during an incident. If there are uncertainties, use the course material as a reference to seek clarification.

This course aims to:

1. **Equip You With an Effective Recovery Plan**: Help your organization create a robust recovery plan to minimize downtime and damage during cyber incidents.
2. **Enhance Your Understanding of Recovery**: Raise your awareness of the intricate steps and factors that play a role in a successful recovery post-incident.
3. **Understand Cybersecurity Dynamics**: Educate you about potential cybersecurity requirements during recovery, which could impact the speed and effectiveness of your incident response.
4. **Stay Ahead of Evolving Threats**: Highlight the importance of regularly updating your recovery plan, in line with the ever-changing landscape of cybersecurity threats.

While an incident recovery plan cannot prevent a cyber attack, it will significantly aid in mitigating damage, reducing downtime, and controlling recovery costs. By mastering incident recovery, you'll boost your organization's resilience against cyber threats.

Incident Recovery Template

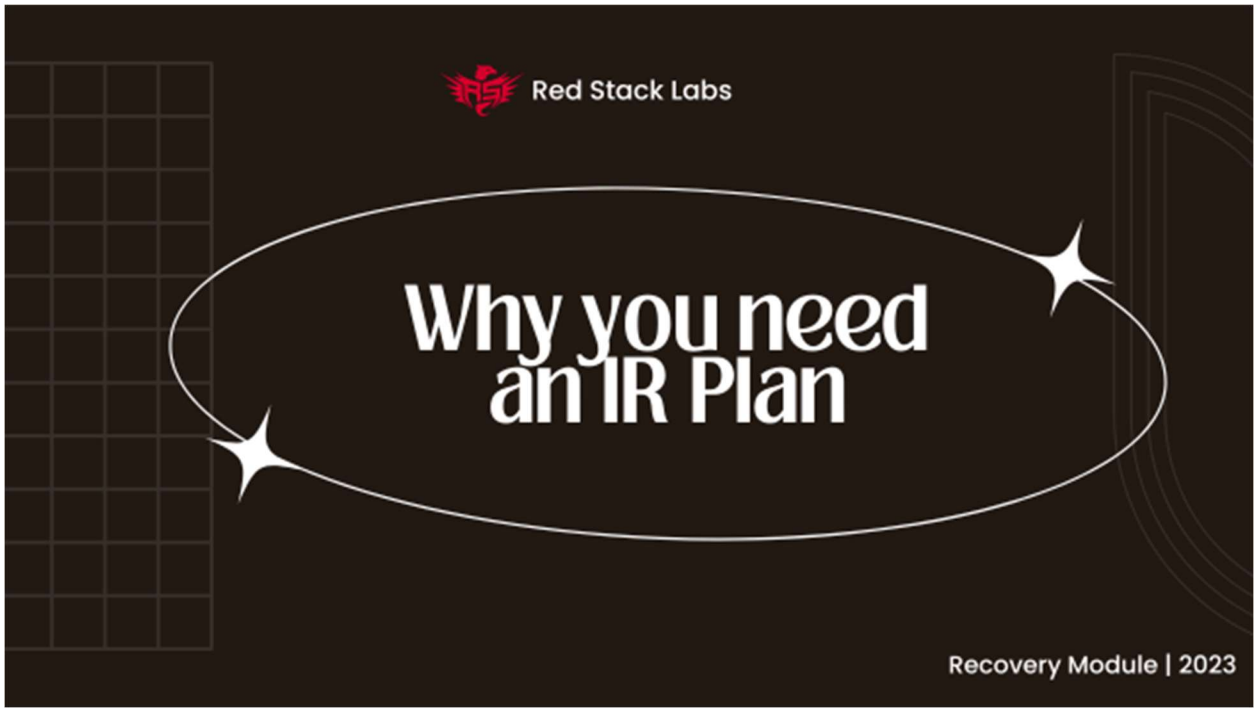
We use a single plan that the team will work against in this module. It will contain all information and become a source of truth. Various members of the team will be filling it out as they go through the program. As such it is imperative to maintain a single copy of this in a central repository ie. Google Drive, SharePoint, MS Teams channel, etc. Everyone working and needing to reference the document should have full access to the repository. You should also have versioning enabled so that changes can be tracked as the document meets business needs.

The Incident Recovery Plan Document contains everything you need to get started on the road to cyber incident preparation.

Next Steps

Download the template and save in a common repository.

Incident Recovery Basics



Why you need an Incident Recovery plan

Be Prepared

When a security incident happens, it can be without warning so its essential to prepare in advance. The first couple hours after an incident has been identified are severe and can be chaotic, it's best to be prepared during those critical hours and focus on the predefined tasks at hand.

Prioritized Objectives

There is going to be a combination of hunting forensics for cyber attribution and eradication of footholds and malware in parallel to recovery efforts. There needs to be a plan in place to prioritize the goals of the business in tandem.

Coordination

A lot of critical information needs to be shared hourly with different teams, ensuring everyone is consistently updated and working toward the common goal of keeping the business operational. Critical updates can create shifts of priorities for entire teams.

Expose Gaps

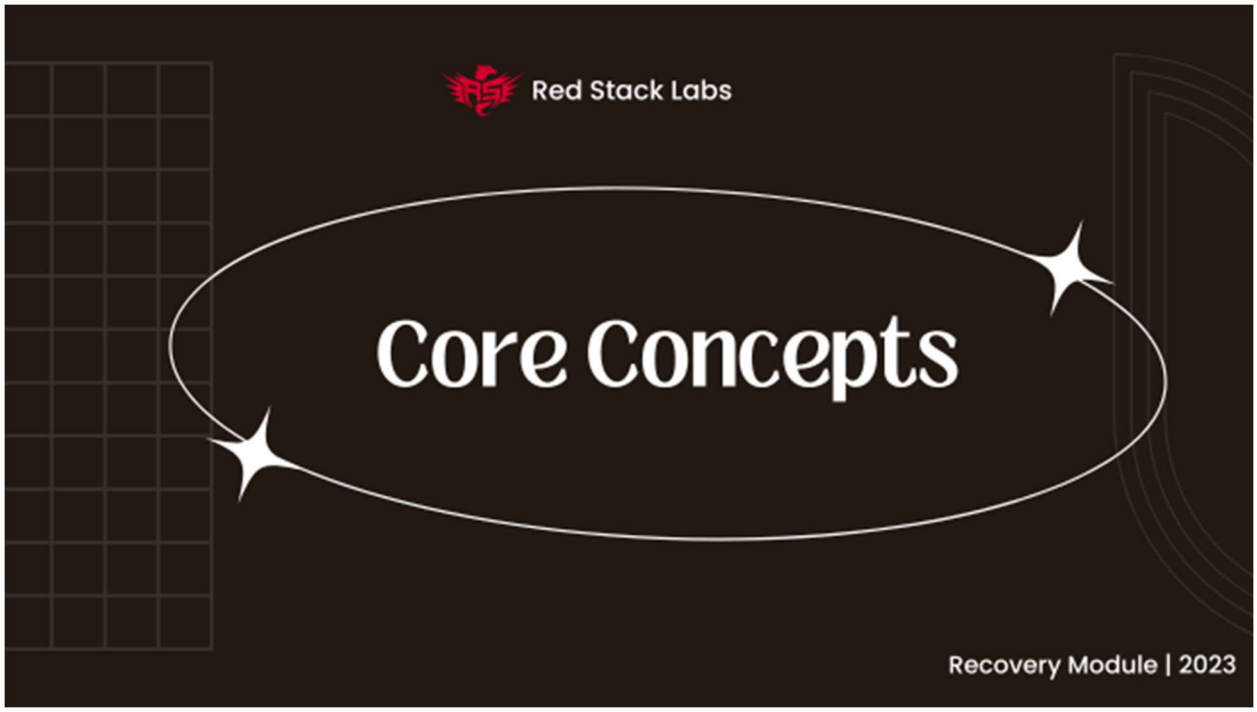
Subject Matter Experts (SMEs) will have gaps in knowledge and tooling, an Incident Recovery Plan (IRP) will help identify the weaknesses and plan will support them during a severe incident.

Documentation and accountability

Clear documentation of procedures will reduce the time to recovery, it will become auditable for compliance auditors and regulatory authorities on what was done to prevent the breach, what was identified during the investigation, and what was done during and after the recovery efforts to ensure cross-contamination of infections do not re-occur.

Repeatability

An **Incident Recovery Plan** is repeatable, and with previous incidents will be updated with lessons learned for the future of the business to operate and recovery smoother and quicker from future incidents.



Core Concepts

Incident Response vs Incident Recovery

Incident Response and Incident Recovery are not interchangeable terms. Incident Response focuses on the cyber attack and digital forensics and investigation, whereas Incident Recovery focuses on getting the business back to operational status.

Disaster Recovery

Disaster Recover (DR) is the ability to recover your business after an emergency or incident like a natural disaster or a cyber attack. A disaster recovery plan will help facilitate the internal organization confidence during a ransomware attack, that the business can be recovered and will remove the fear and stress of obtaining a recovery key from a criminal organization to decrypt important data. The better the disaster recovery plan is, the more the concept of recovery shifts from depending on others, to doing it all without dependence on outsiders and in the case of a cyber incident that would be a criminal organization looking to profit from doing harm.

For this program a disaster is defined as unplanned downtime and data loss which would lead to loss of revenue, productivity, reputation, and consumer loyalty. The goal is to get the business operational; this means getting servers, data and applications back online as quickly as possible.

The following concepts derive from disaster recovery and can help plan out backup/recovery options used in the Incident Recovery Plan. Become familiar with these topics, as decisions will need to be made when adjusting or improving the corporate backup systems.

Recovery Objectives

Ultimately the recovery objectives define how long your business can be offline and how much data loss it can endure. The more critical a system, application or data set is the higher the cost will be to reduce the RPO and RTO in terms of hours, minutes, or seconds.

"What type of backups should we run and how often should the backups happen?"

Different systems will have their own tolerances and criticality depending on their use and business impact. Your company will be prioritizing assets and data through the inventory portion of the workshop and will identify which systems are critical to the business and which ones are not, this is a good place to start once the assessment is complete, to assign recovery objectives to assets and to define what the tolerances are.

There is a balance between criticality tiers, their respective Recovery Point Objective(RPO)/Recovery Time Objective (RTO) definitions and cost to maintain those requirements. The lower the RPO and RTO is, the higher the cost will be.

Recovery Point Objective (RPO) of seconds

RPO is the target for the maximum data the business can tolerate losing during an incident or outage. A good example, an RPO of 48 hours would be if there was a failure and the last good backup was 2 days ago. The RPO is the distance of time from the last good backup to the time of the failure. An RPO of zero would mean that there is no tolerance for any data loss, this would be for a mission critical application, data set or server the business or clients rely on.

Examples

A zero RPO would be a payment processing web application that accepts credit cards, like Stripe. Stripe processes over 10,000 transactions per second and if the past 4 hours of transactions are lost in an incident it would be severely impactful and create an unfathomable amount of work for their company to recover if they don't have continuous replication backups and high availability systems.

Another typical zero RPO for many companies would be a mail server. Being the primary service for conducting business, emails can contain sensitive information that shouldn't be

lost, including signed documents and other important information and data. At other companies their email might be a 2-3 day RPO because they can just call up the original sender and have them resend an email if needed, it really depends on your specific business and how important emails, data and other services are prioritized and tiered for data loss tolerance.

A 1-2 day RPO would be an employee laptop working on regular day to day tasks. At most they would have to re-write a few documents, but they would have been written recently and wouldn't be a big loss or hinderance to the business overall. At some companies, employee laptops can be 7 day RPOs and it wouldn't make a difference to the business itself.

Recovery Time Objective (RTO) in minutes

Recovery Time Objective (RTO) is the target your company sets as the maximum length of time to restore the business back to normal operation. The RTO should be set differently not only for planned and unplanned events but also for emergency or high severity cyber incidents.

With enough cyber drills and practice runs, the expected RTO should become less of an estimate and more of a statistic for your teams to meet the recovery targets. The goal is to recover the business with the least amount of business interruption, downtime, and cost, and the more effort your company puts into practicing recovery, the better your results will become.

The lower the RTO goal is, the more it will cost the business to prepare and execute. With really good planning and practice a company can reduce its RTO without much additional storage expense because they become better at recovering their business. A well practiced recovery plan is executed better than one that's never practiced one.

Examples

An online service, web application or SaaS platform who is heavily dependant on their computer infrastructure might want to set a lower RTO because of Service Level Agreements (SLA) or Service Level Objective (SLO) and other contractual obligations. In these scenarios high availability would most likely also be designed into the service to ensure a higher level of uptime, and automation would be used to recover complex infrastructures and applications faster.

A manufacturing or services business might be able to tolerate a few days to recovery, there would be a downside, but the cost of a slower recovery would be offset against the importance and total expense compared to a quicker recovery time. This would have to

align with available resources and budget to support a recovery plan of that speed, compared to the cost of a faster recovery plan.

Incident Recovery Plan Goals

An **Incident Recovery Plan** (IRP) should support the business objectives. For your ease we've broken the goals into 4 sections, each of these contains necessary steps to ensure business objectives are met.

Defining Roles and Responsibilities

1. Planning the roles and responsibilities of individuals involved in incident recovery
2. Set dates to test the incident recovery plan to ensure employees know their roles and duties during the incident. Testing can be conducted as a tabletop exercise or a live fire drill. Testing the recovery plan is an audit and validation of the incident recovery plan's effectiveness, does it still function as designed and which areas can be improved.

Setting Expectations

1. Draft the procedures for each phase of the incident response process

2. Prioritizing which systems to recover and in which order. Starting with the highest priority systems that the business operation is dependant on, then recovering the optional systems after. Splitting up the system recovery into phases helps bring the minimal business operation back online quicker.
3. It's recommended to have two IT teams engaging in parallel (these can be in house or outsourced): the first team should prioritize building and recovering the network, firewalls, authorization/authentication services such as Active Directory, emails, shared file storage and phones; the secondary team should target employee devices such as workstations and laptops.
4. Understand the timeline and expectations of recovery. This includes when each phase of recovery should be complete while the timeline is followed, and recovery steps are not rushed or missed. These expectations would align to both the RTO and RPO goals, ensuring you are within the threshold of data loss, and recovery times.

Plan Continuity

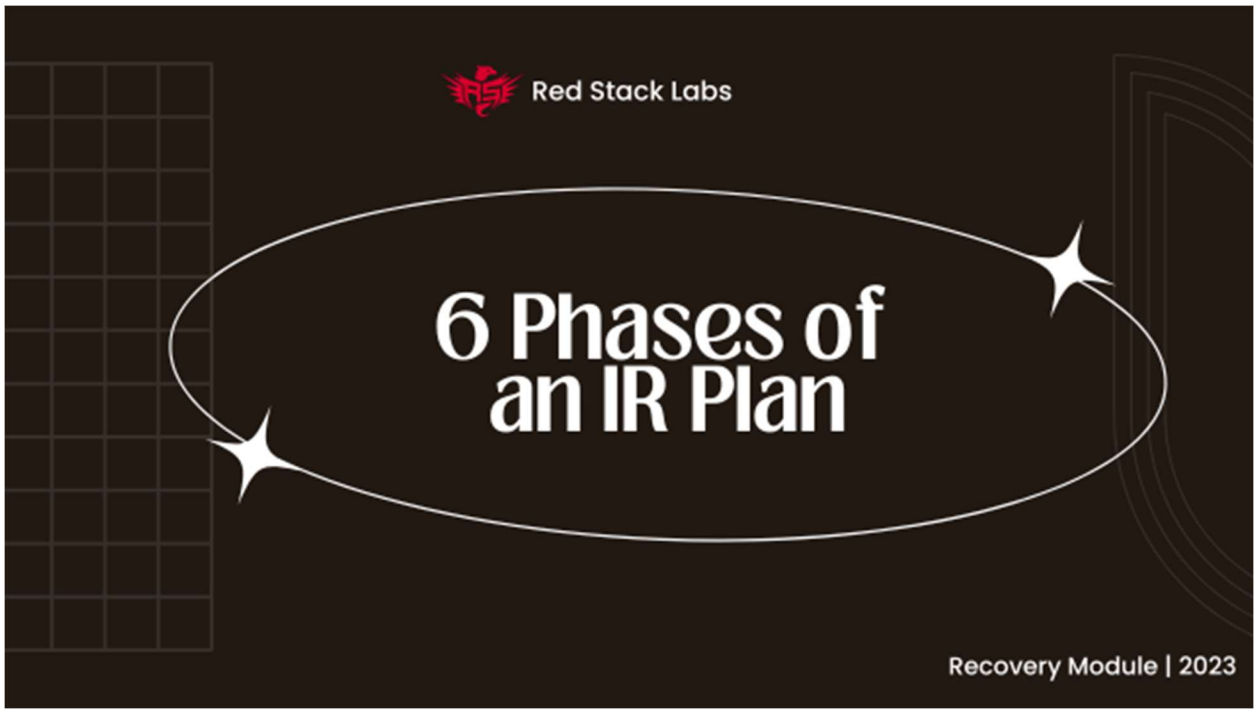
1. Continually update your Incident Recovery Plan as your business grows, shrinks, or changes over time. It's imperative that the incident recovery plan is updated to reflect the current state of the business, including updating its objectives and goals and then to re-test the updated version of the Incident Response Plan until it becomes like second nature. Don’t be afraid to remove or change sections of the Incident Recovery Plan that no longer suit the business, adapt with the current state of the company, and make the necessary changes.
2. Document the version number of the plan on each released iteration, this can help to ensure the employees are using the latest version during a test or actual incident.
3. Keep a backup copy of the Incident Recovery Plan in a remote and accessible location to ensure it is not destroyed during a cyber incident.

Improve

1. Learn from a previous incident to improve the organizations security posture and update the IRP with the latest information and lessons learned.
2. Plan the communication procedures for the staff, executives and external stakeholders to reduce distractions during an incident and to be well prepared. Remember that statistically an unprepared organization loses a lot of crucial time in figuring out a lot of these details during an incident.

Next Steps

In the upcoming sections we will dive deeper into the areas mentioned above. Review the Recovery Preparation List in the downloads, we will be recording these items later on.



6 Phases of an Incident Recovery plan

Since your company will be employing third-party digital forensics firm to run your investigation, some of the Incident Response Planning won't be going into detail. Instead we highlight what you should be aware of when working with vendors; some of the more suitable concepts that are in scope to this program will be covered throughout the **Incident Recovery Plan**.

Disclaimer: Digital forensics and investigations (DFIR) are not in scope for this program. Examples of DFIR are cyber attribution, live system snapshots, malware reverse engineering, threat hunting, packet sniffing, malware removal or ransomware decryption. These are jobs left to well trained professionals. This program is focused on preparation and recovery. Instead, we focus on the concepts of an **Incident Recovery Plan** that a small or medium business can do internally with an IT team.

Preparation

Proper planning is needed before an incident occurs so crucial time is not wasted during a critical cyber incident. In addition to having a proper strategy documented there should be policies developed to define the rules of engagement when dealing with cyber incidents of ranging severity. These rules of engagement should apply both to employees and to users. Staff should follow the policies and procedures mapped in the preparation phase, and adhere to the rules for the safety of the business and to ensure they do not act out of negligence to accidentally risk increase to the company liability in any way.

Identification

Identify the extent of the breach and what has been compromised. Checking the asset inventory and checking each system or device manually can assist to uncover more potential compromises during an incident. The identification phase also includes what malware or ransomware was used, if it is not obvious to your team this can be left to the cyber security professionals.

Questions to ask when identifying a cyber attack

- What happened?
- What made it stand out as a problem?
- When did you first notice it (Time/Date)
- Where did it happen (Device name/IP, Username, Location)
- What network was the device on (Office, Home, Library/Coffee shop)
- What device was this on (OS, host name)
- What data is potentially involved (database, file share, file types, confidential)
- What have you done so far to try and fix it? (record all of this information including the time that their attempts where made)

Containment

Contain the malware and the hackers access to stop the spread, the goal is to limit the damage. When a cyber attack is first identified it will be unknown if adversaries are still on your network or if malware is still spreading, isolate the compromised systems, devices, networks, and disable the accounts that have been identified as compromised and stop the spread. This includes disconnecting networks from the internet, and shutting down machines and devices to stop the spread

Eradication

Traditionally companies have tried cleaning malware from systems but with increasing sophistication in adversary tactics to evade antivirus and EDR systems there is no guarantee that a system is not infected. After cleaning the malware that has been found, there could still be agents or backdoor persistence on the device and because of that we always suggest wiping the machine completely and starting fresh. Do not wipe any machine until the investigation has been signed off by your insurer and cyber security firm doing the digital forensics. If your insurer does not care and gives you the go ahead, it is at your own discretion to destroy potential evidence. Other parties might want to know what happened, with evidence of a proper investigation, these might be partners, clients, investors.

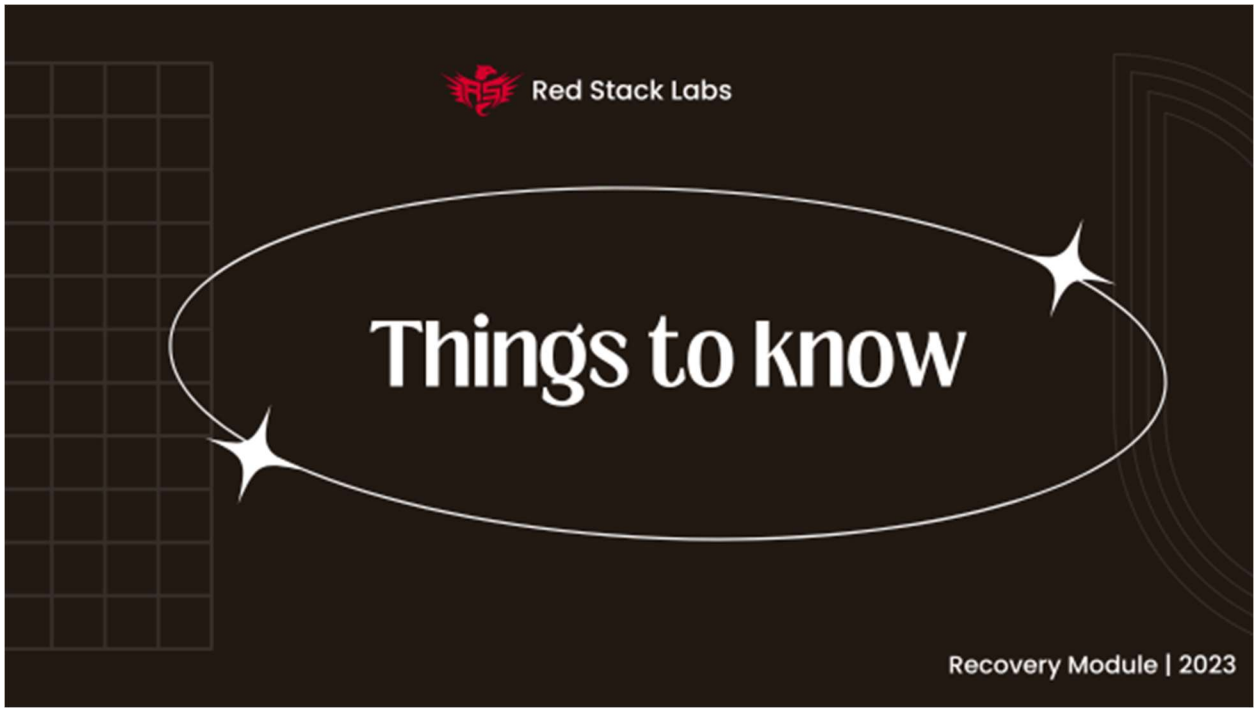
***Note*:** There are techniques to clone hard drives and investigate them offline allowing your company to continue its recovery phase quicker, speak with your cyber security team about this.

Recovery

Restore the systems from clean and safe backups or do a fresh installation of the OS and software. Recover the data from a safe and clean backup.

Lessons Learned

Lessons will be learned through every cyber drill exercise and real cyber incident, this is when you would want to reflect on what you have learned through the experience, but also to update the **Incident Recovery Plan Template**.



Things to Know

Preserve Evidence

During an incident it's easy to forget about gathering and retaining evidence when the primary focus on recovery of systems.

There could be legal requirements to collect evidence, claim insurance, for settlements and lawsuits. Plan to retain records of the incident and to notify affected parties if there is a risk of harm. There could be technical requirements to identify the vulnerabilities to improve your company's security to protect your business and to reduce the chance of a repeat attack using the same techniques or malware.

Regulatory Considerations

If your industry has additional compliance regulations like HIPPA or PCI, contact your compliance specialist and ensure you are preserving any additional evidence that might be required to remain compliant. This additional evidence may be required for a compliance audit or investigation that follows the cyber incident.

Legal obligations

It is recommended to have an independent legal counsel and to call them first before doing anything else and involving them in all conversations to preserve privilege. Including emails, texts and group chats.

External Teams

Hiring an external team may be necessary to do the cyber forensic investigation both from a legal and technical perspective.

You may require to hire an external I.T. administrator team to assist with the recovery efforts if your internal team is bottle necked on hours. Remember that administrators need to eat, sleep, rest, and the recovery phase is taxing and critical on everyone involved for multiple days consecutively.

Re-Hacking

It is important to acknowledge adversaries that breached your infrastructure might be trying to get in again to continue doing damage, its vital that systems in the green zone network (explained in the Recovery section) are patched and updated, and security software is installed and functioning prior to being brought online.

This will help reduce the potential attack vectors for a re-hack, where an adversary might attempt breaking into your networks using the same vulnerability they used during the first incident.

Backups

You need backups of everything, all company files and data, configurations of systems and devices, copies of all application or client data. Imagine your entire corporate infrastructure and all devices and data you use to do your job are inaccessible and will likely have to be rebuilt.

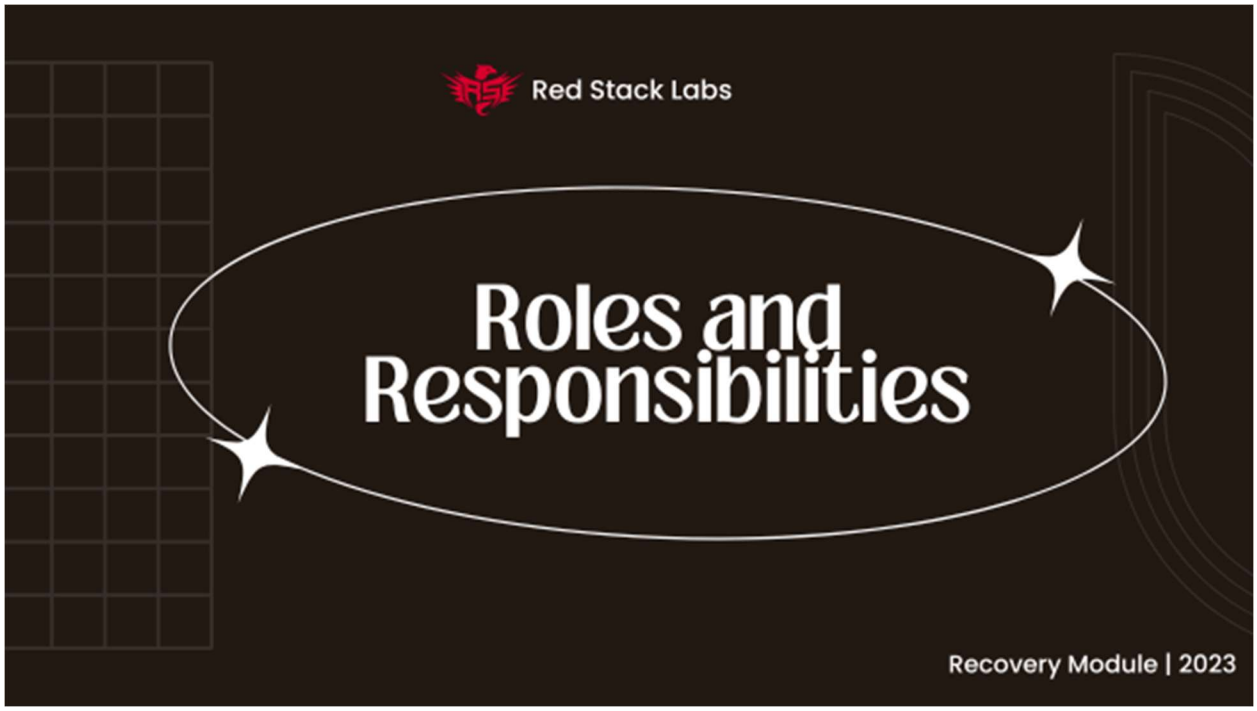
Communications

Informing stakeholders that a cyber incident has taken place, the severity of the incident, and then working on the incident itself all require proper communication channels and procedures to follow. Communication is dependant on pre-planning of roles and responsibilities, but also the information required to reach each stakeholder and employee if the entire infrastructure is inaccessible (emails, work phones, etc.)

Next Steps

Review the What to Document section in the **Incident Recovery Plan Template**.

Collaboration & Response



Roles and Responsibilities

Having clarity on roles and responsibilities is key to aligning the business when responding to cyber incidents. Keep in mind it's always best to have multiple people assigned to a role and duplication of responsibilities, it reduces the chance of bottlenecks and/or if the individual is unavailable the business can still recover operations.

Remember to review content from the program and coaching sessions as some of these will be outsourced either directly by the business or your insurer.

Refer to the list at the end of this section to determine who is assigned to each role.

Damage Assessment Team

The Damage Assessment Team (DAT) is responsible for assessing the scope and impact of a cyber incident and to propose its estimated severity. The DAT will determine if the Incident Management Team needs to be notified. The DAT will use their security assessment checklist to work through suspicious or unusual activity, security logs, event

logs or monitoring tools to determine if there is a cyber incident. If it is determined that the business will be impacted and/or is a high severity incident, the DAT will contact the Incident Management Team (IMT) and activate them.

Roles

1. Security Manager
    a. Management role to manage the team of analysts
    b. Gauge the business impact and severity
    c. Notify IMT if necessary and relay the findings
2. Security Analyst
    a. Technical role to investigate digital forensics
    b. Write a rapid report on the findings that could be sent to Security Manager, IMT and SET.

Incident Management Team

The IMT is the technical team dealing with the cyber incident at the ground level. They are working through the identification, and recovery phases of a cyber incident, including the technical preparation for backups. This team responds to the threats directly. The IMT also decides if the Senior Executive Team (SET) needs to be notified, depending on the business impact and severity.

Information you want on hand would be:

Name	Job / title	Incident Role	Contact Information
Marge Simpson	Senior IT Administrator	Incident Manager and System and Data Recovery Lead	555-555-0123

Roles

1. Incident Commander
    - This person makes all of the calls for the entire engagement, when to switch between phases, severity and priority, the incident commander will take on all of the responsibility for ensuring the incident management and recovery is handled properly, and efficiently. During a severe incident the Incident

Commander communicates directly with the Senior Executive Team (SET) and the CEO/President and/or Board of Directors.

2. Management
    - Backup and Recovery Manager (IT Manager)
        - Planning and operations of all backups, agents, backup servers, backup storage, and recovery.
        - Technical Advice
    - Investigation Manager (IT Manager / Security Manager)
        - Planning and operations
        - Technical Advice
3. Operations
    - Backup and Recovery Operations (IT Administrators) - technical operations
    - Investigation Operations (IT Team / Security Team) - technical operations
4. Digital Forensics
    - Cyber Security - Recovery, investigation, examination, and analysis of material found in digital devices.
5. Communications and Reputation
    - Include responsibilities from handling internal communications, client communications, vendor discussions, and handling public relations.

Senior Executive Team

When there is a serious cyber incident, the senior executive team will be involved for strategic direction and organizational accountability.

There needs to be priority list of decision makers in case the senior executive team is not available, or members of it are missing at different times during a severe incident.

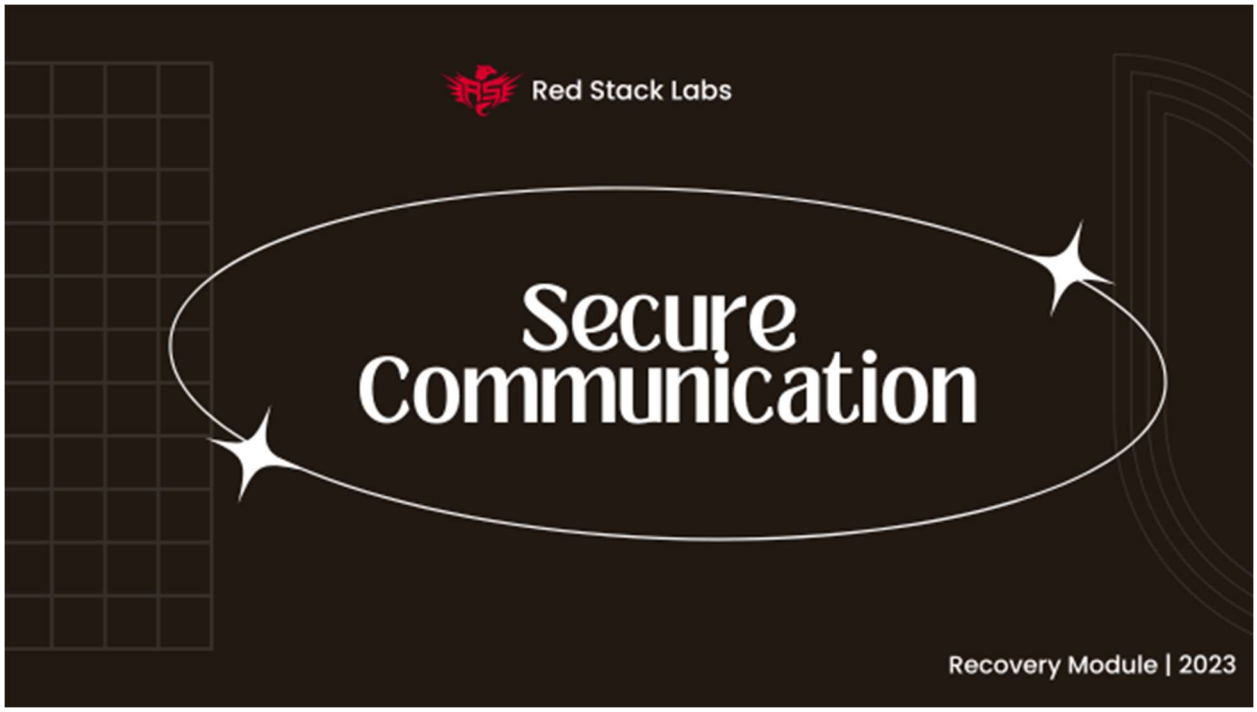
- Stakeholder engagement and management
- Manage resources and recovery budget.
- financial requirements
- communications with service providers
    - legal
    - insurer
    - reputation and brand recovery
    - public relations and communications
    - regulatory authorities
- General strategy of the organization on dealing with the severe cyber incident

Roles

1. Primary decision maker (typically CEO)
2. Secondary decision maker (typically CIO/CTO)
3. Third decision maker (typically CISO/CFO)
4. Regulatory Compliance (legal)
5. Legal
    - Legal Counsel (Lawyers)
        - Contact Information
        - Emergency Contact Information
6. Insurance
    - Insurance Broker
        - Contact Information
        - Emergency Contact Information
7. Emergency budgeting and expenses (CFO/Finance)
8. Staff welfare (HR)
    - Ensure the staff are taken care of during the cyber incident (Meals, drinks, sleep, exercise)

Next Steps

1. Review the roles within your organization, who would be responsible for each of these?
2. Record findings in the provided in the **Incident Recovery Plan Template**.



Secure Communication

This is the process of handling secure and encrypted communications with internal and external parties during a cyber incident.

Informing stakeholders that a cyber incident has taken place, discussing the severity of the incident and working on the incident all require proper communication channels. Communications depend on pre-planning of roles and responsibilities, but also the information required to reach each stakeholder and employee if the entire infrastructure is inaccessible (emails, work phones, etc.)

1. **Invites:** Only have a few dedicated admins for the Signal group, do not grant every member the ability to invite users. This might seem quicker but if the wrong person is invited, all your conversations and information shared through the Signal group are no longer safe.
2. **Last Minute Invites:** Have the admin of the Signal group invite only trusted phone numbers, if there is a request to add additional phone numbers to the group chat then call or facetime to ensure it is the correct employee and not an adversary trying to infiltrate the safe and encrypted group chat.
3. **Privileged:** Invite your lawyer into the chat for privileged conversations. The lawyer needs to be invited before the chat begins to retain privilege. This lawyer should be your corporation's independent lawyer, not the lawyer provided to you by an

insurance company, the insurance lawyer should not be invited into these secure communications channels.

Next Steps

1. Review the checklist in the downloads.
2. Refer to the **Incident Recovery Plan Template** and complete sections on Secure Communication List.

Response Action List

During a cyber incident a lot is happening simultaneously. To give visibility for the entire team below are the list of actions that need to be done.

1. **[Detection]**Identify if an incident has occurred or is occurring - what are common detection methodologies. precursors (current news, threats toward the company - they are rare), indicators / monitoring (EDR or event/security logs), accidental (too late, saw a ransomware note once files are encrypted, data was leaked, contacted

by a hacker that they have access to your network). tools that can help identify adversaries like EDR solutions. can include unusual or suspicious activity.

2. **[Analysis]**Identify the scope, impact and severity of the incident and classify it. Review logs and security alerts to identify suspicious behaviour. Standard Operating Procedures (SOP) for reviewing different systems, services, devices for intrusion (Windows/Linux/Network Equipment/Active Directory/Email/SaaS Products/Data and Files). Consult with knowledgeable experts if needed (can the unusual or suspicious activity or files be explained as legitimate or does it lead your team to believe an intrusion has taken place). Research the potential intrusion, security alerts, log files, file names, or system/network activity that seems suspicious (IP addresses, files, etc.), look through search engines, security alert platforms for indicators of compromise (AlienVault open threat exchange), upload and check suspicious files or scripts on virus total (if it is not confidential or personal or private data). Google scripts names, or functionality or even variable names to identify if they are used in adversary Tactics Techniques and Procedures (PowerShell, bash, python, etc.). *CAUTION- if there is a suspicious IP address do not try to connect to it directly. If it is a server own by an adversary it could alert them to your awareness of their presence on the network (that could force them to deploy ransomware immediately, etc.).*
3. **[Classification]**Now with the knowledge at hand classify the intrusion or cyber incident and rate it on a severity level. We gauge cyber incidents by severity levels that has a matrix of impact**.**
    - from no reduced function to critical function impacted,
    - data from none to personal/sensitive or classified/proprietary data,
    - reputation impact from negligible to severe,
    - and financial costs from negligible to severe.
    - This matrix can be used to classify the potential impact of the cyber incident at this time.
4. **[Contact IT and Executive Teams]** Contact the incident team and depending on the severity and classification, inform the senior executive team if needed. The senior executive team should be contacted if there is a severe cyber incident or one that could have a business impact. Minor cyber incidents like finding a virus on a computer might not be serious enough to alert the entire incident team or senior executive team.
5. **[Contact Internal Stakeholders]** Contact internal stakeholders that could be impacted by the cyber incident - send out notifications, call the mangers/leads. At this point only internal stakeholders should be contacted as part of the communication and discovery phase. This conversation should also seek to obtain information from stakeholders on suspicious activity or unusual changes to their systems, computers, services, files, data, because it is possible their departments

have also been breached but they may not be certain so they may not have mentioned any unusual or suspicious activity yet. *CAUTION – Before any outside correspondence occurs your legal counsel should be contacted.*

6. **[Documentation]**Document everything discovered up until this point and continue documenting throughout the entire process. The documentation should include each of the previous steps include who was contacted or notified, retain records of what was sent. At this point only internal communication and notifications, nobody outside of the company (except stakeholder contractors) should be notified. Insurance can cover services like reputation and brand repair, but also communications services for your clients, partners, investors - to ensure they are handled appropriately, and your business is not damaged. Those notifications could have a 24–72-hour timeline depending on your privacy regulation requirements or contracts, so they don't need to be notified in a hurry, the communication messaging can be sent out when more information has been gathered and worded with the help of a professional service.

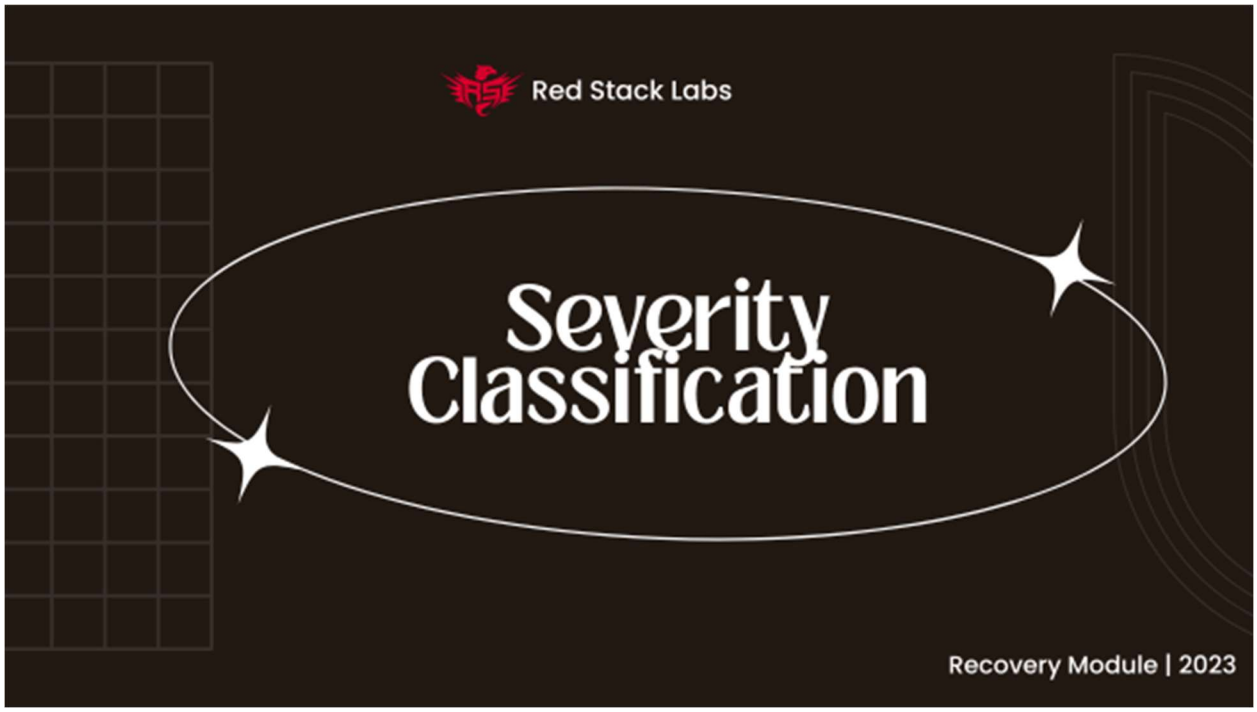
Response Action for Severe Cyber Attacks

1. **[Legal]**Contact the organizations legal counsel and seek legal advice - list of things to obtain legal counsel for instance how to make an insurance claim, regulatory authority notification, when to contact impacted third parties such as partnerships, customers, vendors, and to check on any contractual obligations.
2. **[Insurance]**Contact the insurer following the advice of the legal counsel on making the claim - ideally, they will provide the green light to use one of their panel vendors for cyber security investigation immediately or to receive written authorization to hire your own that has been previously approved by them. They should also have a list of other services you can start using immediately.
3. **[Police / Gov Agency (FBI, CSIS)]** You may be asked to contact the police or an agency to disclose a breach has occurred, this is usually for more severe incidents. You will want to take your lawyers advice on what information to provide, and if you should contact them. The insurer may also have requirements on complying with the police or government agencies like the FBI or CSIS, ensure that you are well informed of the requirements and legalities prior to contacting any of them. Your lawyer might recommend they call on your behalf and provide certain information. This step is incredibly important to take your lawyers advice on because the police do not work for your business, and any information that is released to them is not considered privileged, it becomes part of a case file and can be later used against your business in a lawsuit by a third party. Follow your lawyer's advice on disclosure.

4. **[Cyber Security Team]** Contact the cyber security team that will provide the investigation and digital forensics - confirm that they begin work immediately and that they are aware you are waiting for the systems and servers to recover your business operation.
5. **[External Notifications]** Identify the stakeholders affected by the incident and prepare communications notices to inform them - this might be done by a communications service provided by the insurer. Ensure that your legal counsel over sees the communication notifications and verifies every notice that is sent outside of the company. You will want your independent legal counsel to review it, as well as any lawyer that has been provided to you by the insurer. The messaging in these notices is incredibly important to get right and could protect you from further reputation damage, fines or lawsuits.
6. **[Check Backups]** With the other teams in full swing, your IT team will need to check the backup systems as some of them may have been affected by the incident. Verify if local backups are available for recovery, or begin the download process for the cloud backups, as that could take some time to complete.
7. **[Catch and Release]** Communicate with the cyber security team to identify which systems are safe to go through the recovery process - they will release selected systems intermittently to your IT staff that can be recovered. Be sure to speak with your cyber security team and make sure they know you are waiting for them to release each system back to you as they finish with them, so they can be recovered. Ensure that the cyber security team is aware that you will be wiping every system that they return to you, unless you get a stamp of approval from them that there is no chance of a compromise on a specific system.
8. **[Safe Network]** Build the green zone network to house the recovered systems and services - If the cyber incident is severe enough to require this.
9. **[Recovery Priority]** Determine the priority of the recovery - You will want to prioritize the core business functionality first, to regain minimal business operation. This list of servers and services need to be recovered first to start functioning as a business again.
10. **[Recovery Process]** Work through the incident recovery process to eradicate malware and compromised systems and services and recover them in the green zone network- This is going to be your IT staff working with the cyber security team,
11. **[IMT Disengage]** Disengage the senior executive team and the incident management team when the recovery requirements have been met and the business is operational.
12. **[Review]**Post incident review - what worked, what didn't and document.
13. **[Update]**Update the incident recovery plan.

Next Steps

Review the above list findings and understand which steps are applicable to your role. A copy of this list is available in the **Incident Recovery Plan Template**.



Severity Classification

The severity of the attack will need to be defined when creating a support ticket and reporting the incident to management. The severity levels are a measurement of impact an incident has on the business. In this section, define your company's response to different severity incidents.

Severity is not a prioritization but based on the current impact of an incident. The severity level will be adjusted according to the current situation and not the estimated situation. If a critical system is breached and it must be taken offline and will have a serious business impact, that is a severity 1 (SEV 1). If a critical system is being investigated for a potential breach with no evidence yet, it is not a SEV 1, that is probably a SEV 3. During any SEV level, which can be set to begin alerting management and other stakeholders.

The severity and level will be referred to as SEV 1 or SEV 2 in communications.

Not all incidents will require a severity classification from the team, it might not be worth the time and effort, especially with ones that can be easily handled. But any incident that can impact the business – even financially or legally, like a security breach of any kind

should be classified and escalated. All business impacting incidents should be reviewed with the senior executive team, the board, and the legal counsel.

Severity	Description	Examples
1	A critical incident with a very high business impact	Customer data loss, security breach, client facing service is offline. A critical business system or service is not functioning (The business cannot operate without it). This will affect SLA.
2	A major incident with significant impact	A business system or service is partially functioning and only effecting a subset of operations (The business can somewhat operate). This will affect some SLA.
3	A minor incident with low impact	All critical business systems and services are functioning but there is an inconvenience caused. This will not directly affect SLA, but could be annoying for the business operation or customers.
4	A support request that is irritating a customer	This could be a bug, a connectivity issue.

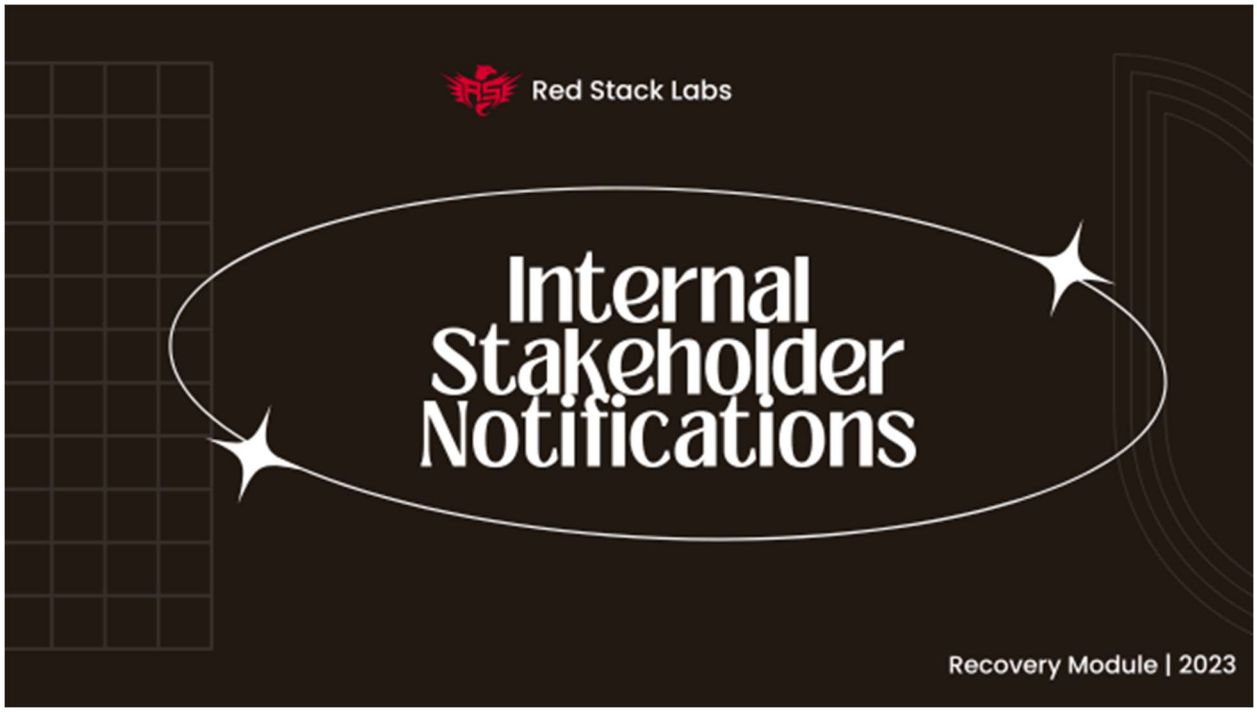
(*These severity descriptions are referenced from and aligned with Atlassian)

Contact IMT and Senior Executive Teams

When a cyber incident or breach is confirmed, with a severity level that would require a response, activating the Incident Management Team will be necessary. SEV-1 or SEV-2 classified incidents should activate the IMT, SEV-3 incidents may not need to activate the IMT.

Next Steps

1. Complete the response portion of the Severity Classification section in the **Incident Recovery Plan Template**
2. If you have a SEV-1/SEV-2 incident, complete the SEV-1/SEV-2 Cyber Incident or breach section in the **Incident Recovery Plan Template.**



Internal Stakeholder Notifications

When the severity, scope, the system, and business impacts of the incident have been determined, it is time to notify the internal stakeholders. At this stage, the stakeholder notifications are for internal staff members and teams only.

The stakeholders might include contractors or consultants that have ownership or support impacted systems or services in some way.

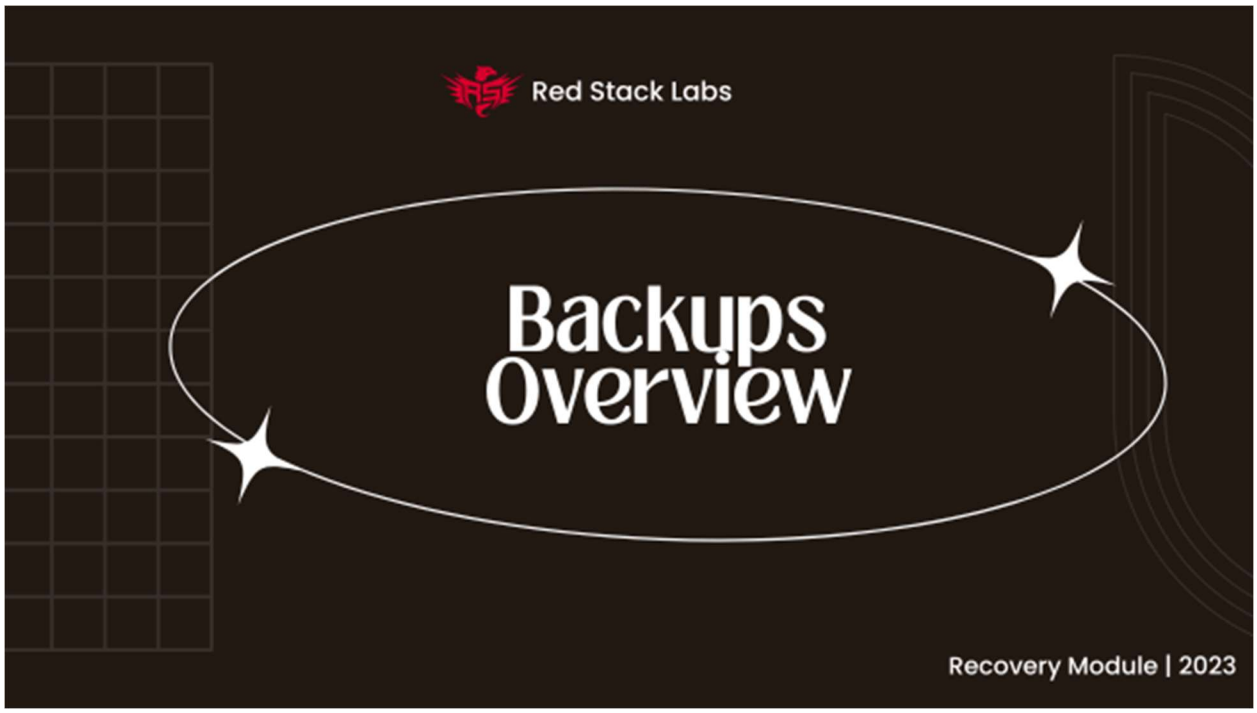
Ensure the notifications to the stakeholders inform them that this incident is confidential and internal only to the business and in no way at this time should the information be shared publicly with customers, partners, vendors, or on social media.

The only time external parties are to be notified is after senior executives authorize it, and legal counsel has provided guidance on notifying those contacts.

Next Steps

1. Complete the response portion of the Internal Stakeholders Notifications section in the **Incident Recovery Plan Template**.

Backups



Backups Overview

Importance of Backups

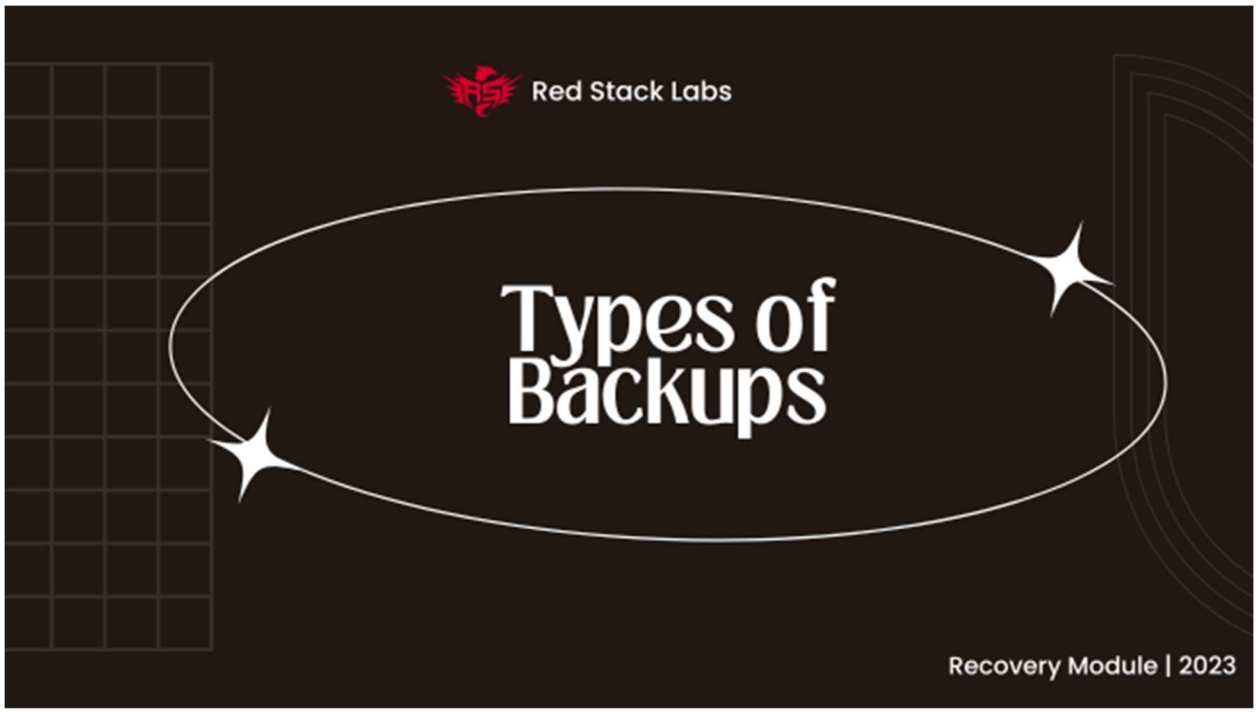
When experiencing a severe ransomware attack against your business, a lot is going on. You may not have access to email, file shares, servers, SaaS applications, and more. Leadership is worried about communicating with investors and stakeholders, partners, and dealing with impatient clients.

In this kind of a scenario backups can play a tremendous role in getting the business operational. We will cover the following and more in this section:

- **Proper Setup**
  - Investing in proper Backup Solutions, strategy, and planning
  - Versioning of the backups can help retain previous versions of a file, this is sometimes done in parallel to immutable version backups, so previous versions cannot be deleted for X amount of time.
- **Strategies & Considerations**
  - Corrupted Backups can be a problem, if the adversaries obtain access to the backups with write or modify access, they could corrupt the existing backups leaving them inoperable.

  - Backups do not prevent ransomware attacks, but if the backups are kept intact, they can be used to recover from an incident.
  - It's only a backup if you can recover from it.
- **Resiliency & Protection**
  - If they are not ransomware resilient, they won't help.
  - Ransomware attacks can encrypt data and corrupt backups - this can be the malware and adversaries' focus.
  - Infected files can show up in backups and when to engage EDR solutions and cyber security professionals.
- **How to Recover**
  - In case of an event, recovery should be done from a backup prior to the compromise of that specific data or system.
  - For example, the AD might have been compromised for 3 days, in this scenario you recover from an AD backup beyond 3 days ago.
  - Attackers may be resident for long periods of time before a ransomware attack is activated or malware is identified on a system, if that is the case the backups for that length of time could include malware or ransomware inside of the backups that could possibly later be triggered.

Note: If adversaries obtain access to the backups with write or modify access, they could corrupt the existing backups leaving them inoperable and unusable.



Types of Backups

Individual

Individual file recovery is the ability to recover a single file from a backup, this could include multiple folders or files in the recovery. For example a users home folder is corrupted, an individual file recovery can be used to recover the entire home folder.

Image

Image backups contain the entire hard drive contents, this includes the operating system, configurations, applications and data. Recovering an image would replace the contents of a hard drive or hard drive partition depending on the software being used to recover.

Granular

Granular recovery is the capability of certain backup tools to recover either an individual file or an entire image from a single pass backup. This allows the backup software to make one backup that can be used for multiple recovery options.

Full, Differential, Incremental backups

There are 3 options when looking to implement backups.

1. **Full** - Copy Everything: Recovery is very easy, just restore the one full backup
2. **Differential** - Copy everything changed since the last full back: Recovery only requires the most recent full backup and the latest differential backup
3. **Incremental Backup** - Copy everything changed since the last backup of any kind: Recovery can become convoluted on incremental backup dependencies, if the last 6 backups where incremental before the last full backup, all 8 incremental backups will be required with integrity in tact plus the last full backup in order to successfully restore the files.

Application recovery

The ability to recover a single application with its configuration and data intact. This can be used when a single application needs to be recovered quickly, and perhaps automation to rebuild the application and its configuration and import the data is not yet available.

Full site failover and recovery

This is for mission critical businesses that require 100% up time, they can have a second data centre or cloud account that can be cold; the servers are cloned, data is waiting near by to be replicated but most if not all the servers are turned off to save money. Or hot; servers are cloned, data is constantly replicated, and all of the servers are turned on and waiting to cut over to the fail over environment. The cost of a full site fail over can be as high as the original site.

Immutable data copies

With ransomware on the rise since 2017, immutable data copies are recommended for all image and data backup tools. This will ensure that existing backups cannot be over-written or deleted, and only new backups can be made and added to the backup storage. Having immutable backups will provide assurances that existing backups cannot be encrypted by ransomware or deleted by an adversary wanting to trap your business into paying a ransom fee.

What are mission critical backups?

Mission critical data is data that cannot be lost no matter what and requires continuous data replication - this can be costly to build high availability data replication onsite or offsite. It will require solid network and storage systems in high availability configurations to maintain continuous replication.

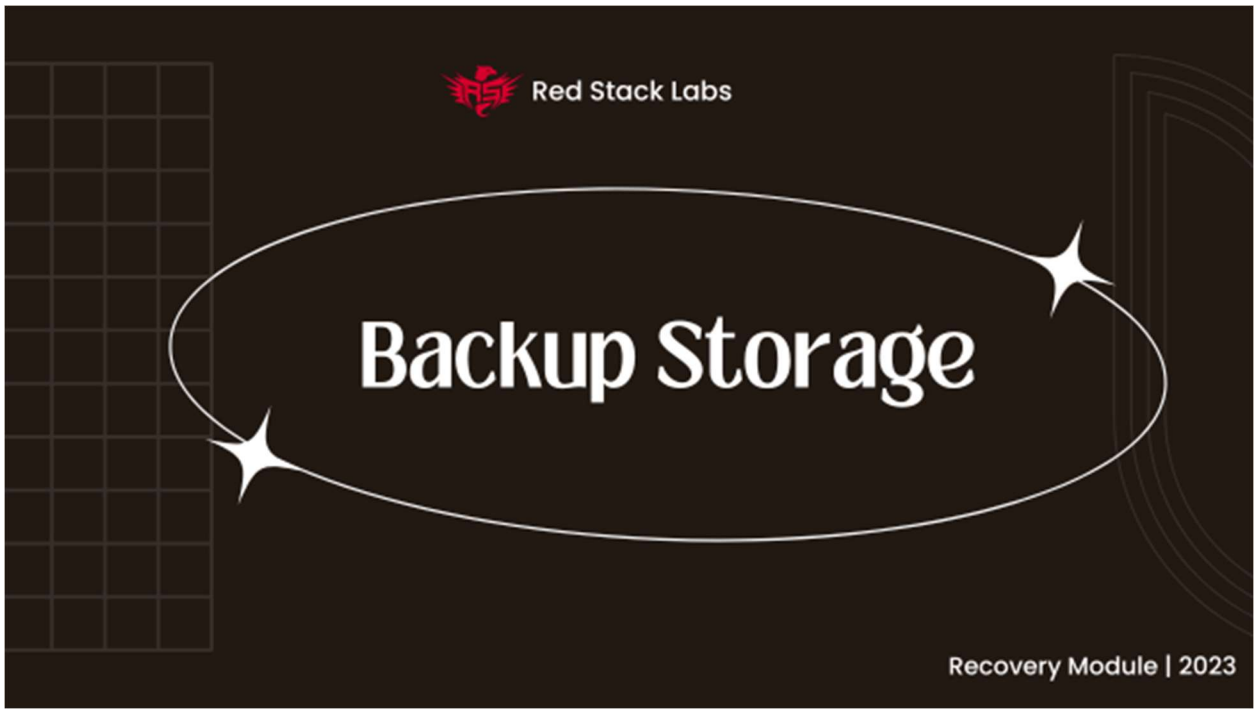
Cloud Backups

Cloud backups are becoming more common, most backup tools and software provide a cloud backup version which stores your data or system images offsite and, in the vendors cloud for you. The security demarcation for their infrastructure is their responsibility, and your access to their service is your security responsibility. Lots of common backup tools are now offering immutable backups in multiple backup configurations that provide resilience to ransomware attacks.

Non-disruptive disaster recovery testing

The goal is to not interfere with production environments, retaining up time of production networks and services. Ideally this type of testing uses additional hardware and infrastructure not connected to the production networks to test out the recovery strategy. Some companies will have additional hardware and resources available to do this type of testing, and it is always recommended to have an extra server and additional networking

equipment on hand just in case of a cyber incident as it can be used to create a safe green zone network (discussed in the Recovery section). The testing environment should be nearly identical to the production environment, using the same models of equipment is ideal to replicate the same recovery results.



Backup Storage

Magnetic Tape

As the cost of cloud backups and disk drives becomes affordable these days, tape becomes the less chosen option, but it continues to offer a great security feature that none of the other options provide easily and that is offline storage.

The downside to tape backups is the performance, the larger the data becomes the longer the backup and recovery time will take. Because of the Recovery Time Objective (RTO) requirements, it might make tape backups an ineffective option for some businesses or certain types of data.

Tapes do provide good security because they are stored offline, most modern tape devices like LTO-8 and LTO-9 provide larger capacity, compression and hardware-based encryption. One thing to note about tape backups is backward compatibility is limited, and the devices and tapes might require consistent technology upgrades and migrations every couple year.

Note*:* We **recommend** looking at the NAS and Cloud backup options while leveraging the 3-2-1, 3-2-2, or 3-2-3 rules.

External Disk Drive

External drives are USB drives that can remain connected to a system to continually backup, or they can be unplugged but then the backups would stop. With the speeds of Thunderbolt or USB-C ports, disk drives are a great choice for quickly moving large sets of data around, but when it comes to backups consider the additional manual maintenance of connecting and disconnecting the external drives for every system in your company.

This option isn't the most scalable, but it has its uses. Disk drives can be used as a logical air gap to isolate disks from the host but essentially the disk will probably always remain connected to the system providing some form of read or write permissions.

This can be a great option for a smaller company without too many computers to backup, and the disk drives can be repurposed with growth if the company moves into a NAS or Cloud backups in the future.

The security downside is if the disk remains connected to the host, even using software to try and manage the permissions it could still be bypassed, or the disk drives themselves could be stolen or damaged. Your RTO might demand disk performance for a quick recovery time, but security might demand an offline storage like magnetic tape for ransomware protection.

Network Attached Storage (NAS)

Network Attached Storage (NAS) provides data storage services to systems on the network.

There are enterprise grade NAS devices from companies like Dell and HP, commercial grade like Synology or QNAP, but we consider any network attached storage like a windows server hosting SMB shares, a server running a backup storage repository, or a network shared service like FreeNAS or Unraid to be a NAS device.

Note most of the servers can be virtual machines running on a Hypervisor like ESXi or Hyper-V.

The enterprise NAS devices can be pricy but over a longer period it can save money when comparing it to monthly cloud costs. Many factors can go into this decision including but not limited to determining needs beforehand (multi-year cloud storage is cheaper), your balance of capital expenses vs. operating expenses.

The upsides of a NAS is it is private and self hosted, meaning your company has complete control over the device and configuration. It does, however, require maintenance and

proper configuration to be secure. Regarding the maintenance this includes setting up redundancy and fail-over options in case of an individual drive failure or a NAS device failure. Depending on the RPO and RTO of your business you may need a more sophisticated backup solution for your company because downtime can occur.

NAS devices are quite easy to manage and maintain with some knowledge and effort required from a professional IT administrator. These devices are also dependant on the network they provide shared storage to, which means networking maintenance and functionality is also important for backups and recovery.

NAS devices use RAID arrays which can support automated drive failure tolerances depending on the kind of RAID that is being used. Most NAS devices also support directory (such as Active Directory) integration to make sign-on easy for your users, and they also support Cloud backups of the entire NAS device being stored in the Cloud as a redundant backup replication. Depending on the type of data being stored on the NAS this might be a good option to use both the NAS for local backups and the Cloud for off-site backups.

When configuring a NAS device or a backup repository on the network be sure to segregate its management web console from the network that is accessing it for backups. There should be a segregated network access to the management console.

Cloud

Cloud datacenters are operated by 3rd party companies that provides ease of use and scalable technology to build virtual infrastructure, host applications and other services remotely without having to invest in the cost of the hardware yourself. There can be small upfront fee(s) which can include automatic cloud infrastructure redundancy and maintenance by the provider. These notes are based on the 3 major cloud vendors: AWS from Amazon, GCP from Google, and Azure from Microsoft.

The cloud storage used for backups is low cost with a low upfront cost, which can be ideal for companies who want a monthly payment instead of tens of thousands of dollars up front in hardware costs. The cloud storage scales with your business, meaning as much storage as you need will be made available to you, and the cloud providers manage the reliability and maintenance of the cloud storage. Please note that additional reliability features can be enabled for certain cloud providers, like geo-location replication, ensure that these features are properly configured if they are needed.

Cloud storage provides remote access to the data from anywhere in the world, anywhere any time. This can be accomplished with very little configuration on your part either using access control lists (ACL) or a secure VPN tunnel.

The upside to cloud storage for backups is there is no maintenance required when using a 3rd party software like Veeam or BackBlaze to leverage their cloud storage.

The downside to cloud storage for backups is the time to download the backups over the internet, this becomes dependant on your office's internet bandwidth. The download time needs to be tested to comply with the companies Recovery Time Objective (RTO) because a wrong estimate could impair meeting the RTO requirements when it is time to recover.

Backup Strategy

The 3-2-1 rule is one of the original backup strategies that was promoted by the US-CERT. It is still a viable backup option, even with recent growth of cloud backups, the 3-2-2 and 3-2-3 rules are become better options.

Keep in mind when you're configuring backups to be resilient to cyber attacks, they will never be immune to all scenarios. The goal is to reduce risk and focus on getting business operations on track as soon as possible. The more certainty you plan for in the preparation phase, the better chances of meeting this objective.

Regardless of the strategy that is the best for your business and your RTO requirements, we always recommend to backup locally to a properly configured backup repository. You should also backup that same data to the cloud. This will ensure a local copy of the data

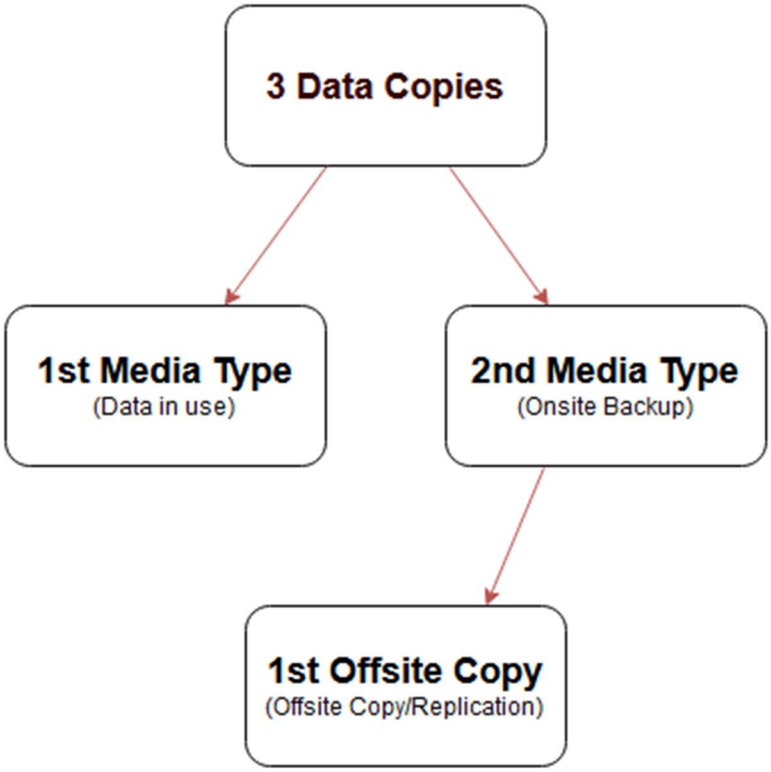
will be available to leverage recovery functionality similar to instant recovery, but in the chance that the local backup is somehow compromised, there is still the off-site cloud backup with immutable configuration to fail over to. This provides a safe copy of the data, being available to your business to recover, even if the worst scenarios occur.

Example

1. A company had a pipe burst and flood the local NAS in an office destroying the local data mid-emergency. They had an off-site replication (NAS to NAS) and could recover the data from the off-site NAS.
2. A company had a local backup storage server become compromised by a skilled adversary and the local backups deleted. They where able to recover from their cloud backups, it took a little bit longer, but the data was 100% recovered following a ransomware attack.

Rule of 3-2-1

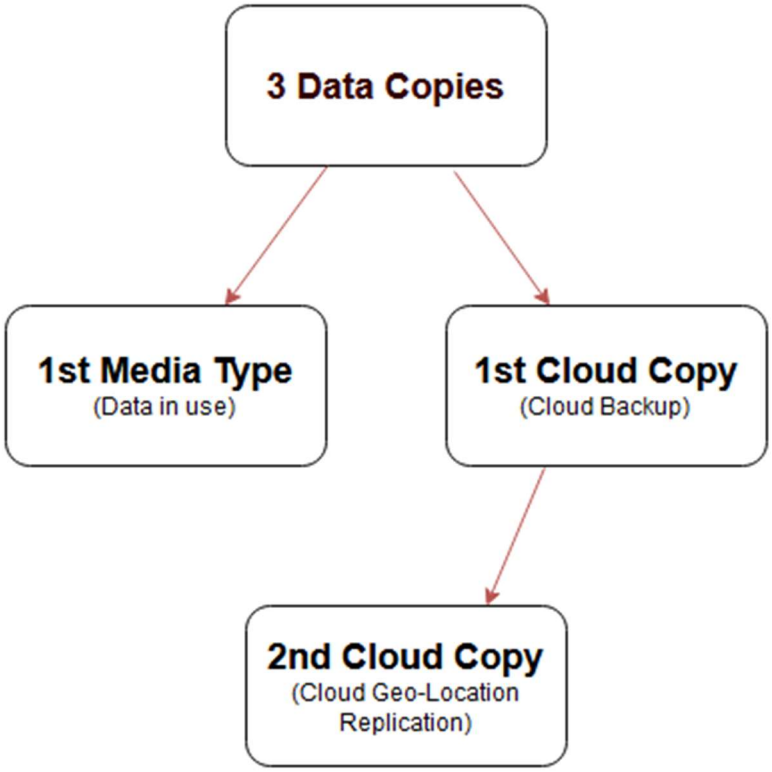
The 3-2-1 rule always retains 3 copies of the data to ensure data redundancy. One copy of the data is the production data in use, the second copy is on a backup device on premise and the third copy is stored on a backup device off-premises or in the cloud. This means that there are 3 copies of the data, 2 locally and 1 offsite, and this is meaning behind the name; “The 3-2-1 Rule". The purpose of the 3-2-1 rule is to store additional copies of the data onto different mediums and in multiple locations just in case something happens to the production data. For example, if a ransomware attack encrypts the production data, or if a natural disaster damages the storage devices. A backup of the data would ensure the data is kept in a safe place.



1. **1st media type** is the production data - the production data is the copy of the data that is in use by your staff, clients, or servers.
2. **2nd media type** is a backup stored onsite - this is the primary backup of the production data that is stored on a different storage medium. The storage mediums can be a NAS, SAN, external disk drive or magnetic tape.
3. **1st offsite copy** is a backup stored offsite or in the cloud - this copy is a replication of the backup data from the 2nd media that is stored offsite. The locations can be in the cloud, a second office location, or a home.

3-2-1 in Cloud

As cloud offerings evolved the 3-2-1 rule began evolving with it, and their backup solutions ignored the 2nd onsite medium and went straight to the cloud. This means that there are 3 copies of the data, 1 in production, and 2 off-site (two geo locations in the Cloud). This more evolved version of the 3-2-1 rule that only requires a backup agent installed on each device and an internet connection.

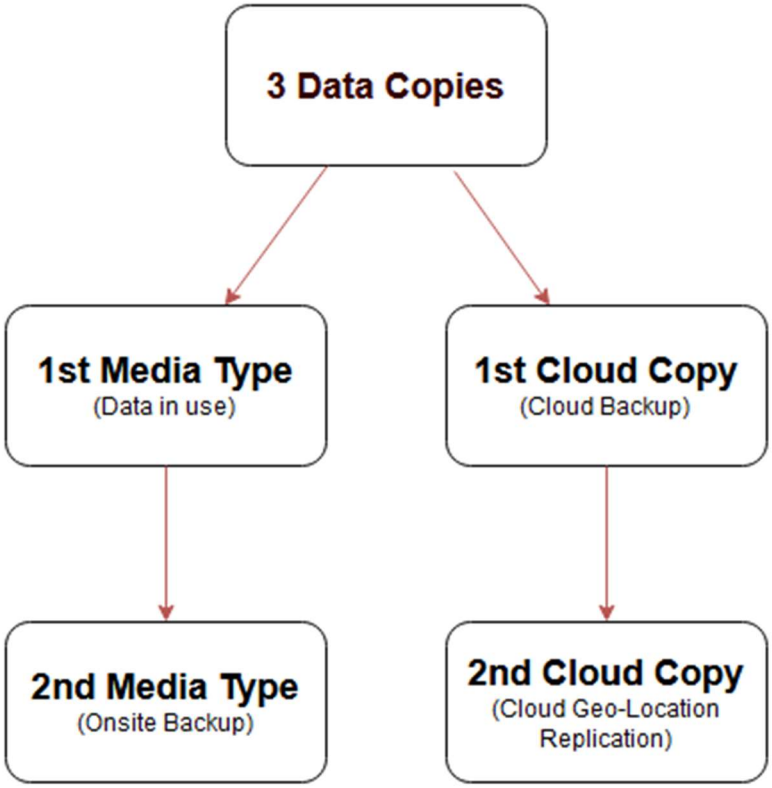


1. **1st media type** is the production data - The production data is the copy of the data that is in use by your staff, clients, or servers.
2. **1st cloud copy** is a backup stored in the cloud - this is the primary backup of the production data that is stored in the cloud. This can be a public cloud provider or a private one through a backup solution.
3. **2nd cloud copy** is a geolocation replication of the 1st cloud copy - this copy is a geolocation replication of the backup data from the 1st cloud copy which can be stored with the same cloud provider or a different cloud provider (often when the location of the storage is in a different physical location usually a different coast of a country). For example, the first backup is stored in Virginia, the geo-location replication would be stored in Oregon.

Rule of 3-2-2

The 3-2-2 rule is like the 3-2-1 rule except in addition to the 1st cloud copy it also retains another geolocational replication of the data, this can be accomplished with the cloud storage feature by enabling geo locational replication. The 2nd cloud copy will provide additional protection to your data from threats like a site outage with the cloud provider (it happens roughly once per year for one reason or another) or if a major disaster happens

top the cloud data centre and you require access to your data during that disaster. It will become available in a different data centre in another location. When calculating RTO and RPO it can be imperative to have geo-locational cloud backups to ensure that the data is accessible when calculating in the risk acceptance margins for data availability.

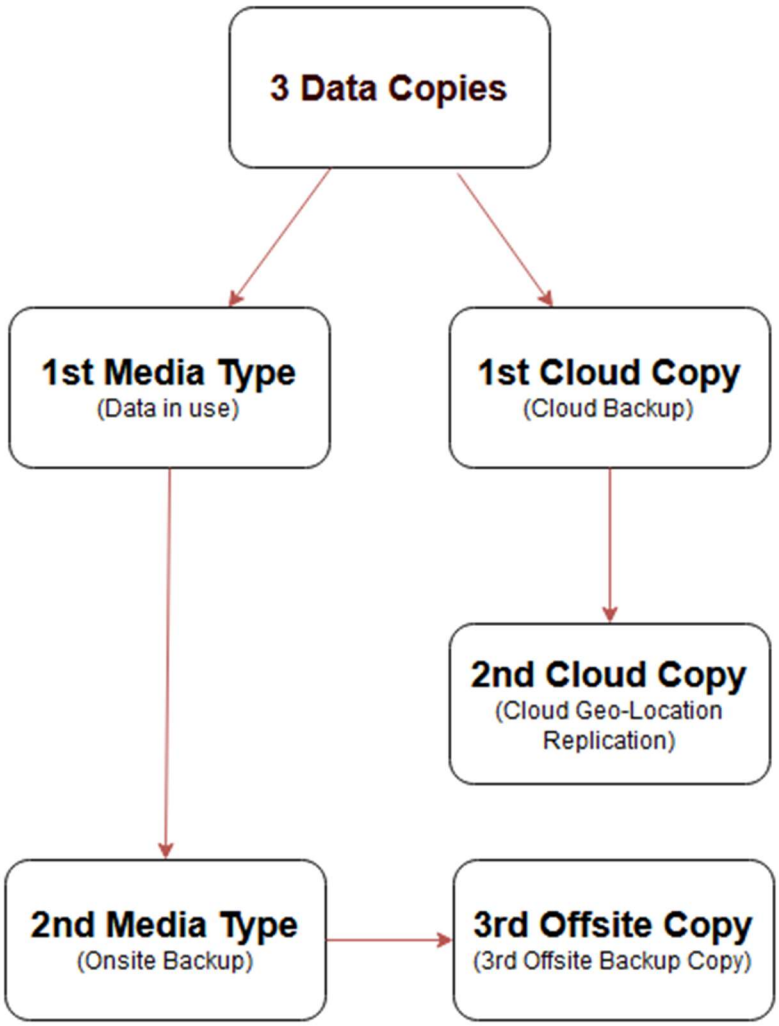


1. **1st media type** is the production data - the production data is the copy of the data that is in use by your staff, clients, or servers.
2. **2nd media** is a backup stored onsite - this is the primary backup of the production data that is stored on a different storage medium. The storage mediums can be a NAS, SAN, external disk drive or magnetic tape.
3. **1st cloud copy** is a backup stored in the cloud - this is second backup of the production data that is stored in the cloud. This can be a public cloud provider or a private one through a backup solution.
4. **2nd cloud copy** is a geolocation replication of the 1st cloud copy - this copy is a geolocation replication of the backup data from the 1st cloud copy which can be stored with the same cloud provider or a different cloud provider (often when the location of the storage is in a different physical location usually a different coast of a

country). For example, the first backup is stored in Virginia, the geolocation replication would be stored in Oregon.

Rule of 3-2-3

This 3-2-3 rule provides more resilience to incidents and disasters ensuring that data should be available in a stronger Cyber attack or throughout the strangest coincidences. There are 3 data copies, 1st is the local production data in use, the 2nd is the local backup. Now the 1st copy of the data is also backed up to the cloud for the 3rd copy. The 3rd copy of the data has Geo-location replication and sits in a 4th copy. Now in addition to all of this, the on-site backup is also replicated into a third offsite copy, this can a second office location, a storage locker at home, or a datacentre.



1. **1st media type** is the production data - the production data is the copy of the data that is in use by your staff, clients, or servers.
2. **2nd media type** is a backup stored onsite - this is the primary backup of the production data that is stored on a different storage medium. The storage mediums can be a NAS, SAN, external disk drive or magnetic tape.
3. **1st cloud copy** is a backup stored in the cloud - this is second backup of the production data that is stored in the cloud. This can be a public cloud provider or a private one through a backup solution.
4. **2nd cloud copy** is a geolocation replication of the 1st cloud copy - this copy is a geolocation replication of the backup data from the 1st cloud copy which can be stored with the same cloud provider or a different cloud provider (often when the location of the storage is in a different physical location usually a different coast of a country). For example, the first backup is stored in Virginia, the geolocation replication would be stored in Oregon.
5. **3rd offsite copy** is the offsite replication of the 2nd media type - this is a replication of the 2nd media type that is stored offsite. . The storage mediums can be a NAS, SAN, external disk drive or magnetic tape.

Recommendations

We recommend one of the latest rules that adopt a cloud backup strategy for incident recovery, the main reason being the cloud is a great place to store off-site backups, and most cloud providers offer geo-locational backup replication and redundancy for their cloud storage making it reliable and easy to maintain.

Schedules

Grandfather-Father-Son (GFS) Backup Schedule

The Grandfather-father-son (GFS) is the most common rotation scheme for backing up media and data. This typically follows a daily, weekly, and monthly backup schedule to reach the target goals of the RPO.

The GFS backup schedule can operate in tandem with the 3-2-1 rules. While the GFS scheduling strategy dictates the schedule of the backups, the 3-2-1 rules define the locations of the data backups. In addition to both strategies there will also be a retention rule that defines the length of time each one of these backups is retained in each location. These 3 strategies, GFS, 3-2-1 and retention will provide a solid foundation for your backups, configured in a way to meet both your RPO and RTO requirements.

The incremental or differential (Son) backup should only save files that have changed, while the full image or snapshot backups will save everything including the operating system.

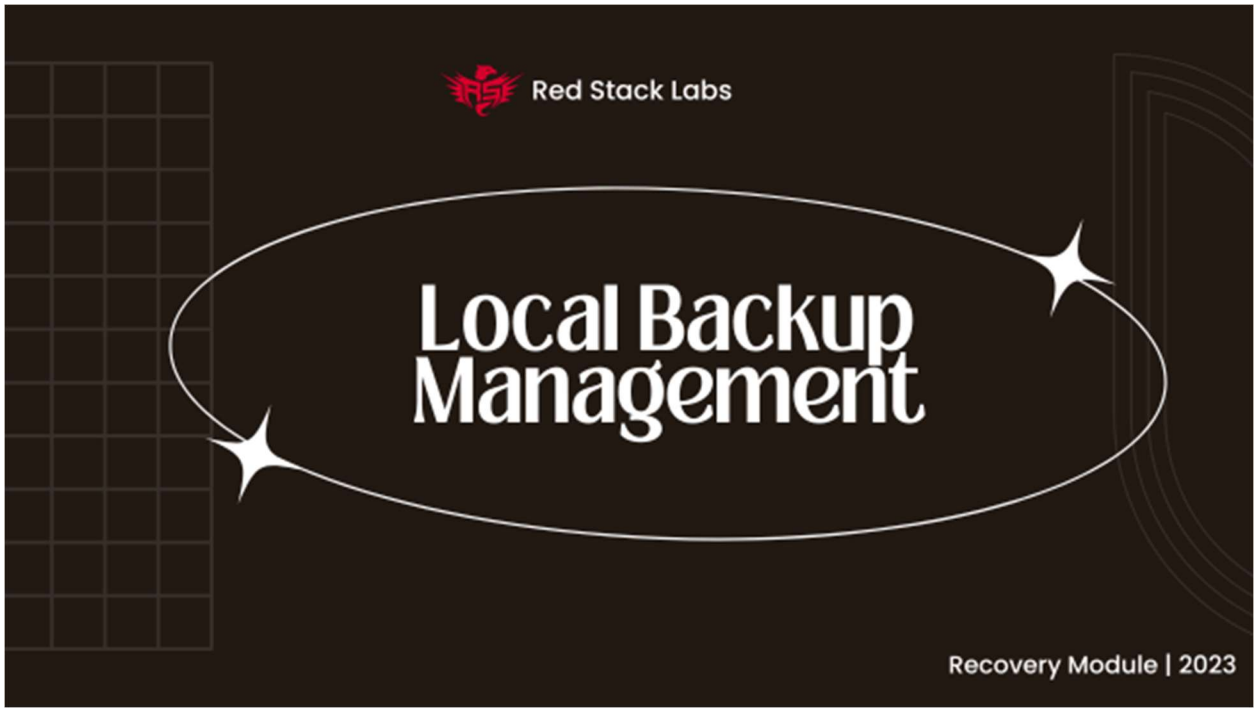
GFS Breakdown

1. **Grandfather** - A full image or snapshot backup of a system that is stored offsite with the longest backup cycle.
2. **Father** - A full image or snapshot backup that is stored onsite with a shorter backup cycle.
3. **Son** - An incremental or differential backup that can be stored onsite or in the cloud with the shortest backup cycle. Daily, per minute or per second guarantee the RPO.

The downside for GFS is that it is scheduled and does not instantly replicate data to a second device. Traditionally GFS will be used for non-critical RPO devices and systems but cannot replace data replication of a critical service or database.

First in First Out (FIFO)

A very simple rotation strategy that was primarily used with floppy disks, CD/Blu-ray, and magnetic tapes. The oldest backup, the disk at the bottom of the pile, is overwritten with the latest backup and then placed at the top of the pile. The storage media types in use today can still implement FIFO because the concepts remain the same. With incremental backups, when the oldest backup reaches its retention policy it is discarded, and a new backup is saved, virtually replacing it with the FIFO concept.



Local Backup Management

The following section discusses local backup servers residing on a production network, like a SAN/NAS with dedicated backup software used to backup a system. This section can also apply equally to hypervisor backups using a software like Veeam. Note that not all backup software is built the same and do not offer the same functionality, but we try to help by providing a backup comparison chart in the appendix.

The goal is to segregate the backup management console from the backup storage to provide a barrier of protection. This is done to prevent an adversary who has access to a system on the local network from accessing the management console of the backup system to change policies, permissions or even to modify and delete the backups. The goal is to segregate access through the network but also from the IAM policies and file/folder permissions, only allowing an administrator local access to the backup management console with no remote access rights.

Users Permissions to Backup Storage

User permissions should be configured with no modification access, revoking access to change existing backups in storage. The users should be granted the ability to write new backups but not modify existing backups. The reason users should not have modified access to existing backups is if a user or system is compromised, an adversary or

ransomware cannot leverage those permissions to encrypt or replace their good backups with an empty archive.

***Note*:** Ransomwares are being programmed with greater intelligence toward backups and shared file storage. Most modern ransomware malware seek out to discover backups and attempt to infect, delete, or sabotage them. If you revoke modification privileges to the users, the malware won't be able to leverage those users access to modify backups existing prior to the compromise.

Admin Permissions to Management Console

The admin access to the backup server should be a local admin user and not a remote one. This is done to prevent compromised admin credentials from having access to all the critical servers.

Management Console

A backup server should not be domain joined, because one of the major targets for a bad actors once inside a network is to compromise the domain controller (DC). It is very easy to access the backup server and its management console from a compromised domain controller.

There are a lot of techniques that bad actors use to move laterally from a domain controller to its joined systems. Even using automation to leverage the privileged access the domain controller has over these systems. It is important that all critical servers like backup servers and hypervisors are not domain joined, this will create a barrier of access from a compromised domain controller and its user credential list.

Management Console Networking

If your backup vendor supports segregating the network for their management console and backup storage, we recommend using a segregated VLAN for management traffic or secured network to access the management console from a Privileged Access Workstation (PAW). Or if not, we recommend using physical access to the server to access the backup management console.

The reason to keep the management console off the production network is to create a barrier between the ability to remotely login to the console, and the production network that could be under attack by a bad actor. This separation means that the only way to

make changes to the backup system, their policies, permissions, storage, or the backups themselves would be either through physical access to the server, or through a Privileged Access Workstation.

Privileged Access Workstation (PAW) - The air gap workstation

- Dedicated workstation, separating sensitive accounts and tasks from day-to-day tasks and users.
- Provide a secure method to access critical management consoles.
- Provide a secure system with minimal software installed.
- Usually on a segregated network or VLAN to protect the PAW.
- OS is hardened and secured, firewall is blocking all incoming connections, things like RDP, WMIC, SMB and all other services would be disabled and firewalled off.
- PAW is not domain joined and uses a local user.
- Validate integrity of the software being installed (md5 checksums)
- Use 2FA or password less login.
    - Smart card, biometric, RSA SecurID

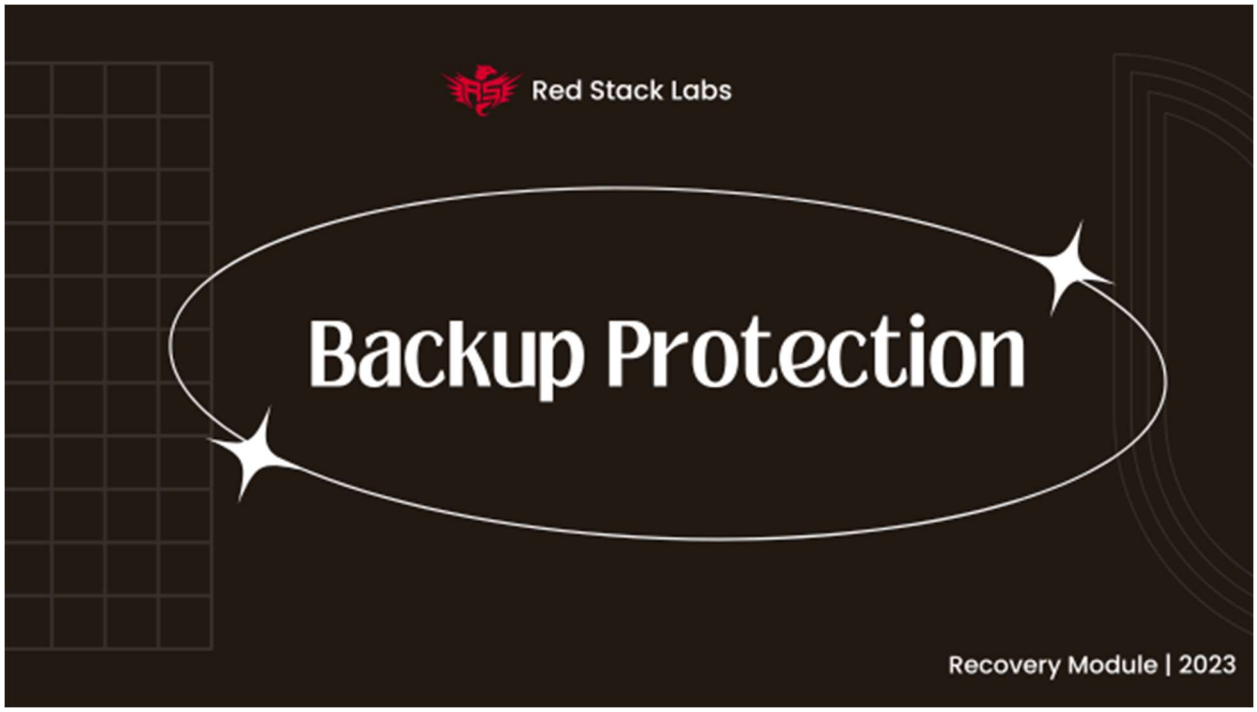
***Note*:** PAW reduces the risk from phishing emails, web-based client-side injection attacks, or physical attacks like a rubber ducky, bash bunny.

Hypervisors

If the backup server is running on a hypervisor like Hyper-V or ESXi, then the hypervisor host should not be domain joined and the remote access to the hypervisor management should be disabled from the production network. If a secured network is configured to a Privileged Access Workstation (PAW) for management access, all other remote access from production networks should be disabled on the backup server.

Next Steps

Review the PAW checklist in the downloads and confirm your systems adhere to best practices.



Backup Protection

Encrypted backups

Data is an important asset to your business, it is the objective of adversaries and insider threats to possess a readable format of your companies' sensitive data, and to encrypt your backups into an unreadable format. Your sensitive data can later be used against your business for profit, but it can also damage your company reputation and possibly cause legal issues depending on the type of information being stolen.

Knowing that your backups are protected by encryption means that the data residing inside those backups is protected from prying eyes. Your data is not just an electronic file or a database on a network, it is also the physical disk drive that the backups are stored on, which can be stolen. If the data on the disk drive isn't encrypted, then it can easily be read by a bad actor with physical access to the drive. This drive can be in a server, or a laptop that is stolen, or it can be an old disk drive that was replaced and now the drive is in the wrong hands.

We recommend using Advanced Encryption System (AES) 256-bit encryption which is also recommended by NIST.

Note: Encrypting backups does not prevent malware infected data from being backed up. The backup agent will encrypt all files including the malware and store it inside of a backup. While encrypted into a backup, the malware won't be able to function, it will idle there until its recovered through a restoration process and then it might require a manual trigger like

opening the file or executing it in some way. Malware infected backups could infect systems later, once they have been restored, remember that encryption is not a malware prevention mechanism.

Encryption Options

Symmetric Encryption

The same key can both encrypt and decrypt the data. AES is a popular Symmetric encryption.

Asymmetric Encryption

The encryption keys come in pairs, the public key can safely be shared publicly with anybody, and this key can be used to encrypt the data. The private key is considered sensitive and is not shared with any third party because it is used to decrypt the data.

RSA is a popular asymmetric encryption.

Legal Requirements

Compliances and data privacy regulations, for example, PCI DSS, HIPPA and GDPR have legal requirements for data encryption or secured hashing of certain types of data. PCI compliances even goes further to require key-management processes, and other specifics not covered here. Audit the compliance requirements to ensure you are compliant.

Key Management

Key Security

It's vital to retain the private decryption key of a key pair in a safe place. If it is compromised or read by a bad actor, it could be used to decrypt your backups.

You can use a USB stick that is kept in a safe with the encryption keys on it, or a password manager to store the private keys. The encryption key when it is generated should not remain on the hard drive of any device, and this includes word docs, spreadsheets, email or internet chat like teams or slack.

We recommend storing the key in a password manager and ensuring the password manager is securely accessed by an IT Administrator with very complex password and multi factor authentication configured.

Key Rotation

The regular rotation of sensitive keys is a recommended best practice and aligns with industry standards (PCI-DSS) and compliance requirements (NIST, CIS). Key rotation when dealing with backups requires some preparation and planning.

When a backup encryption key is rotated, the old backups will continue to function with the old key while the new backups will function with the new key. Over time the old backups will be phased out and replaced by newer backups, FIFO. Once that process is complete the old key can be discarded.

There is a period of phasing out an old key, by replacing the backups over time. This will align with your backup policies and retention periods. For example, if a backup key is rotated today, and your backup retention period for a full backup is 6 months, and the incremental backups are 2 months, then it will take 6 months to phase out the full backups, and 2 months to phase out the old incremental backups that are using the old encryption key. Meanwhile the new key will be used for all new backups and once the process is completed and the old backups no longer use the old encryption key, the old key pair will no longer be of use and can safely be discarded.

Key Takeaway: Research and understand the key rotation mechanism for your backup software before rotating the key pair.

Immutable backups

An immutable backup storage does not allow files to be modified or changed. This ensures integrity of existing backups and provides resilience against bad actors and ransomware attacks from deleting or encrypting your backups into an unusable format.

If one of your users has access to modify or change these backup files and that user is compromised by a bad actor, then the bad actor can modify or delete your backups. Destroying your backups ensures their chances of extortion payment for a decryption key, so this becomes a primary target for ransomware gangs.

Immutable backup storage is vital for business recovery, it will ensure that backups will retain their integrity throughout a cyber attack. Immutable functionality is more than file permissions, folder access control lists or storage protocol. Those protocols can be bypassed. Immutability is an additional feature of backup software or cloud storage that provides immutability.

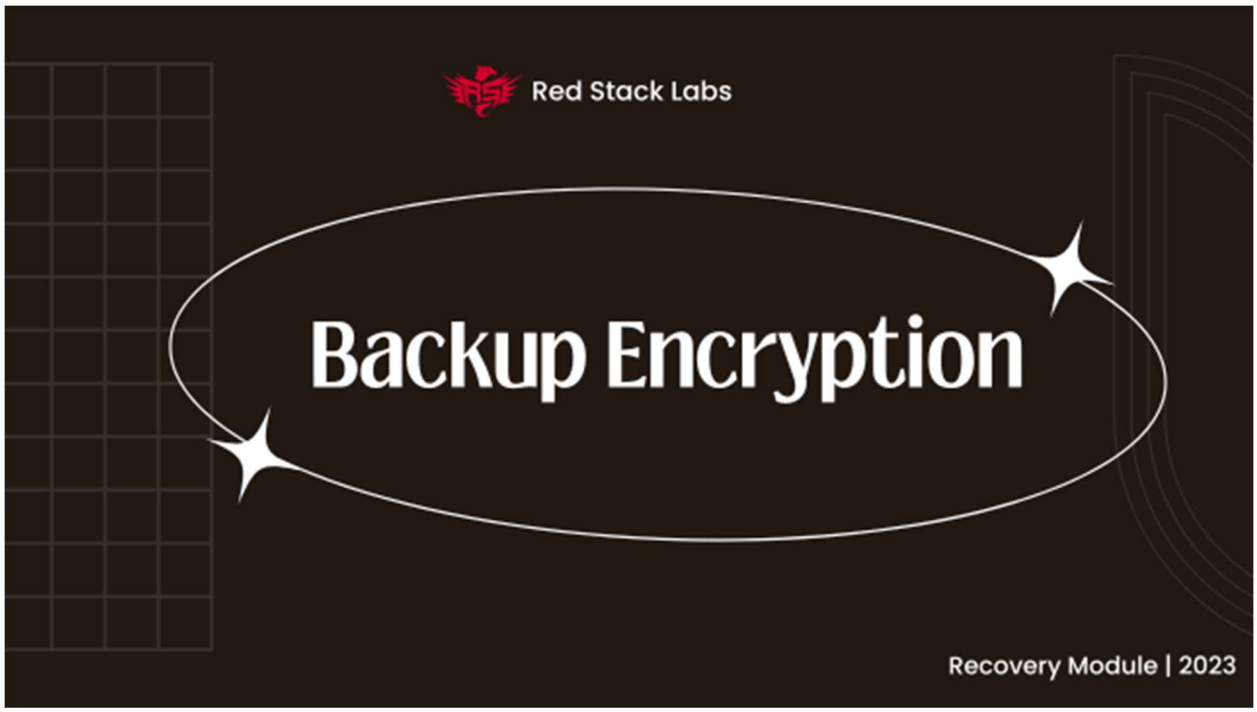
Ransomware resilience

The immutable backup storage feature and the encryption features should be a requirement for all backup systems being used, these provide ransomware resilience. In order for your backups to help protect your company from a severe ransomware attack or a cyber incident on your data, your backups need to be configured to be resilient to these types of attacks.

1. Enable backup encryption on the backup agent (Windows, Mac, Linux) and enabled on the backup storage repository (for hypervisors, databases, file shares, etc.)
2. Enable the use of encrypted network protocols for data in transit. Including HTTPS/TLS, SSH/SFTP, or another encrypted network transfer protocol.
3. Ensure the backup storage is configured to be immutable.

Next Steps

1. Review your current key rotation process.
2. Determine if your backups are ransomware resilient.



Backup Encryption

There are multiple methods available to encrypt your backups and one of the simplest is to use a backup software that supports backup encryption direct from the agent or backup repository server. This method makes it easy to track and audit configurations and to ensure that backups are being encrypted properly from all data sources. The agent will encrypt the data prior to leaving the device, retaining encryption and integrity as the data transfers over the local network or the internet and reaches the backup storage which can be a local storage, a remote storage or a cloud based one. Another method for data encryption is to encrypt the data using a 3rd party application before transferring that data with the backup agent. A dedicated encryption software uses a password or a key pair to encrypt the data, files or folders then the backup software would transfer those encrypted bits into the backup storage. Because this method requires more complexity and multiple tools, we don't recommend it as your primary option.

***Note*:** All of the popular backup software provide built-in encryption and integrity.

Recovery Overview

Having access to a clean copy of data for recovering normal business operations after a cyber incident is ideal. The ability to recover from backups is needed to avoid dependency on infected systems or the bad actors extorting you. Most companies say there is probably

no way to rebuild most of their data from scratch if they don't have backups, and in the case of a cyber incident, backups are only useful if they can be recovered from.

With a copy of clean data, the primary recovery process will be able to restore critical functioning and high priority servers and data to establish minimal business operation. At which time the minimal business operation will have some of the staff focused on regular productivity and client deliverable and some of the staff will continue to focus on restoring the remainder of the business.

The secondary recovery process will be to achieve regular business operation. The recovery staff will continue to focus on systems and data in priority sequence moving beyond minimal business operation and into regular business operation. The regular business operations should bring the company back into a profitable state and the staff back in their regular productivity and client deliverable.

Note: The **Incident Recovery Plan template** and the worksheets for this module will guide your company on identifying the critical, high, medium to low assets to create a recovery prioritization during the planning phase. This planning will help define your recovery efforts in a priority sequence when the time comes.

Backup Validation & Recovery Testing

A backup is only good if it can be recovered.

Recovery plans should be tested regularly to validate it is functioning properly. There are two procedures to validate a backup was successful:

1. Analyze the backup storage to verify the data was backed up.
2. Recover from those backups.

Numerous issues can arise that fail a backup in progress or stop the agent process from running on a system, and in some cases the agent can be uninstalled. This can be because of network failures, storage capacity or storage failures, malware, or bad actors compromising a system.

In case backups stop and they are not being monitored, a period can go by before it is realized that backups are not functioning. Don't want such issues during a cyber incident, this can be days, weeks, or months. The I.T. administrator should conduct a check to verify that backups are being done, and the backups appear to be the correct size in the backup storage.

Over time your administrators will have an estimate for how large each type of backup should be in megabytes, gigabytes, or terabytes. Checking the backup storage for the date and size of both full backups and incremental or differential backups would give a decent idea that backups are occurring from a specific device.

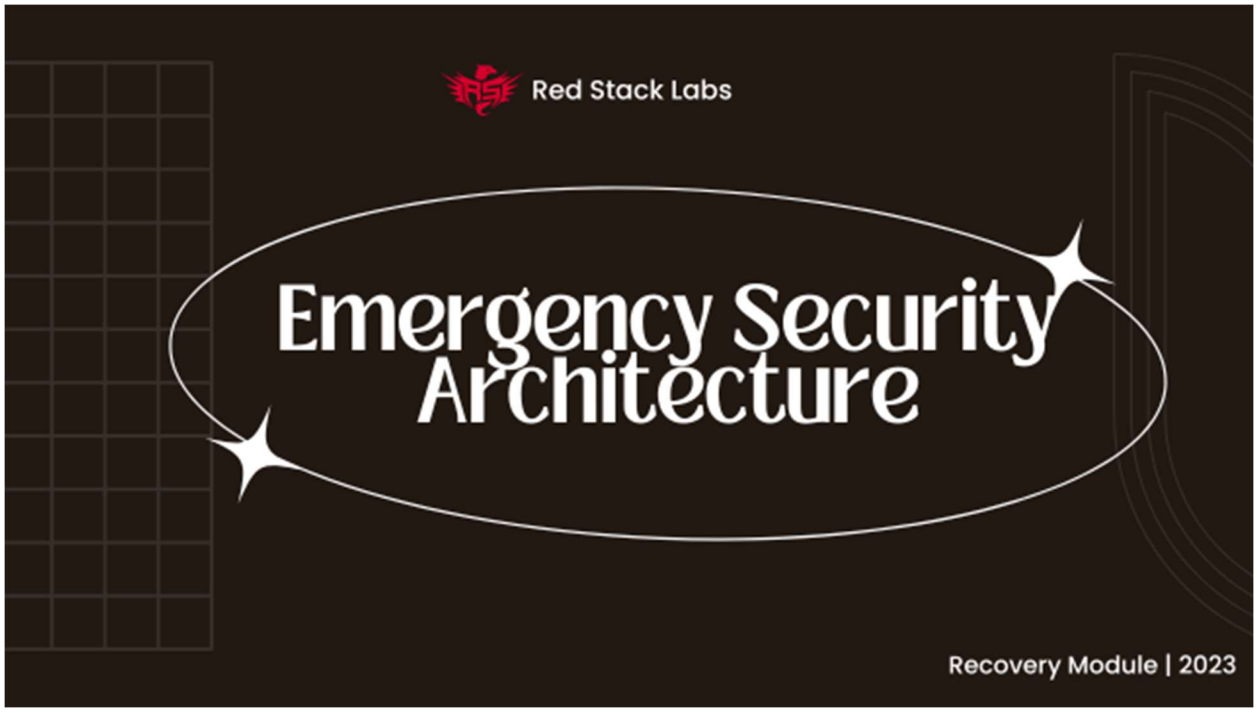
Keep in mind just because a backup is saved does not mean it can be restored.

1. When testing the recovery of a specific backup, it will have to be restored in accordance with the RTO that has been decided for each device or service.
2. Because RTOs will be different depending on your types of backups, you will want to test your types of backups periodically against their individual RTO. Once or twice a year, your staff should engage in a cyber fire drill and test the complete incident recovery plan.
3. Taking the time to verify your recovery plan works, provides the experience and confidence to your company that it can recover its way out of a cyber incident if one occurs.

Note: Your company should have a policy that defines how often backups are tested for restoration in alignment with the RTO. The success and failures should be tracked and recorded along with detailed metrics of the time to recovery, the date, the administrators name and which devices or services where being restored.

Next Steps

Build a schedule for backup validation and conduct regular recovery testing.



Emergency Security Architecture

When dealing with infected systems and compromised networks it takes additional effort to restore your infrastructure, and the best way is to keep the infected devices separate from the clean devices using a red and green zone approach. The infected devices stay in the red zone and the clean devices are rebuilt in the green zone. In order to achieve proper separation, we will use network segregation to achieve a clean green zone to recover into, while also using clean systems that will only be connected to the green zone network.

Network segregation and reinfection of malware

Network segregation is a different practice than network segmentation. Network segmentation breaks down a network into smaller networks whereas network segregation enforces the separation between networks.

The goal of using network segregation during the recovery phase is to divide the infrastructure into two separate networks, the red zone that contains the malware infected systems, and the green zone that contains the clean restored systems. The infected system remains isolated and offline without internet access and cannot reinfect the clean systems that are being restored.

The red and green zone concepts are primarily for severe cyber incidents that infect the systems of an entire network, if you are dealing with a single infected device, you may decide to follow partial portions of the advice.

Every system or device connected to the green zone network must be a clean machine. A clean machine can be defined by the following:

1. The clean device has never been connected to the infected network (red zone) and has never been domain joined.
2. AND
3. The clean device has been given an all clear by the cyber security team/firm that the device does not contain any malware or backdoors and is safe for the green network.

   OR

4. Either the device is brand new, it was formatted, and a clean operating system was installed on it, or a safe backup was restored on to the device.

A device would be considered clean if the former 2 are true or the latter one which can then be used on the green zone. In no circumstance should a device connected to the red zone be moved over to the green zone without being formatted and restored from a safe backup, or having a cyber security team inspect it and verify it is clean.

If the cyber security team provides a probability of infection response such as "There is a chance it could be infected but we can't tell", then it is up to the business to decide on the risk approach and if that device should be moved into the green zone. Ideally the time

would be spent to rebuild the device, but some companies might opt for risk acceptance in this scenario.

We would always recommend rebuilding and restoring from clean backups from a preventative perspective, but we also understand that some businesses are put into a situation and must make risk-based decisions for themselves.

Think about this - the worst-case scenario is to restore your environment only to be reinfected again because of a mistake or a risk-based decision such as accepting the risk of a system that may be infected and moving it from the red zone to the green zone. The reinfection could occur within days, weeks, or months and having to go through this process again, whereas restoring that system might take an hour.

The Red Zone Network

The red zone is the existing network that was compromised during a cyber incident, including all the devices and data sources that are connected to it. The initial compromise could have been a few days, weeks or months before the cyber attack was identified, that period defines what is part of the red zone.

This would include the following:

All networking equipment, servers, desktops, laptops, mobile devices, and even the printers, connected to the network during the period of the cyber incident.

All other devices that may have connected to the red zone during that period. Examples are remote devices that may be domain joined or using a VPN to access the network for shared file storage or other services.

During a major cyber incident like a ransomware attack, it is advised to power down all of the devices on the red zone network, to unplug the network cables from the switch and unplug the router from the internet. We recommend turning off the red zone WIFI network as well, to ensure that devices do not accidentally reconnect to the infected network for any reason.

When a device in the red zone is ready to be wiped and restored, it should be removed from the red zone network in isolation with no network connections and formatted. Once the device is wiped it is considered safe to connect to the green zone to restore it. A device should not be restored while it is still connected to the red zone network, and it should not be formatted while it is connected to the green zone network. Please take note that if the cyber security team has given a device an all clear that it is not infected with a backdoor,

persistence or malware, then that device should be safe to move over to the green zone network.

The Green Zone Network

The green zone is the clean and segregated network that is providing internet access to the recovered and rebuilt systems. The green zone is not connected to the red zone by any physical medium. If using VLANs there will be virtual segregation and enforcement between the two networks, ideally there is a physical separation for the network devices. The wireless access to the green zone can be configured after the red zone wireless is disabled, ensuring that devices don't accidentally connect back to the infected network using WIFI.

When building the green zone network the architecture should align with infrastructure requirements. Ideally it will be built with the models of networking equipment the staff is familiar with, especially on complicated infrastructures. Be sure to update the network devices and patch the vulnerabilities during the green zone build. If network devices from the red zone are being repurposed for the green zone, we recommend a cyber security team analyze them for backdoors and providing an all clear prior to use.

If you are rebuilding the network yourself as an IT Administrator, we recommend using physically demarcated networks, meaning the red and green zone are not connected to one another using any type of cable or WIFI connections.

After the green zone network is functional the next step is to rebuild the supporting servers for the infrastructure. If using hypervisors to host critical servers, build the hypervisor servers first to have the supporting infrastructure for the virtual machines. If your solution requires a backup server, this would be restored or rebuilt next. It is common for a business to run a backup server as a virtual machine on a hypervisor like ESXi or Hyper-V on a local network, if this is the case, these would be the first two servers to restore.

Note: Remember that network devices can be backdoored by adversaries or malware, you may want to reflash and reconfigure the devices or have a cyber security team investigate them for backdoors if these devices came from the red zone. The green zone should never be connected to the red zone in any way. If you are using VLANS to segregate your networks virtually, you should have certified network engineers that are configuring your devices to ensure the segregation is enforced properly or else we recommend a physical demarcation between the two zones.

Next Steps

Review the Clean Zone Procedure Checklist in the downloads.

Upgrades during Incident Recovery

It's natural to want to change things during an incident, like the software being used, company processes, education, hardware, and software upgrades, even moving critical servers to the cloud. Having the available resources to make these changes while still meeting the restoration metrics of your RTO is great. However, without available resources either the upgrades or the restoration will need to be prioritized.

In most cases it is best to recover first and achieve business operations. Once the incident recovery process is completed, prioritize your system upgrades or transition into the cloud.

Most scenarios we don't recommend doing both unless you hire an expert firm to help with the transition to ensure it can be done on time. Keep in mind, new products have a learning curve for your team and your staff will have to learn them and get experience with these new systems before using them in production.

Note*:* There is a process to procure new products and cannot expect it to function as needed out of the box. Your team may require extra effort to get a new product working, to maintain it, patch it, secure it, and create processes and policies that align with your cyber security programs and compliance.

Event Impacts

The initial foothold is where the adversary first gained access to your infrastructure. This could be through an internet facing service, a phishing email, or a more sophisticated technique. Depending on your detection program(s), it could be sometime prior to the business becoming aware of the incident.

The date and time of this first breach is what you want to document as the initial foothold. If the initial foothold has been verified by a cyber security team, and no other signs of compromise or infection have been identified then the assumption that prior to this date and time, your backups have a high probability they will be clean and free of infection.

The initial foothold is not the same as the date and time the ransomware malware is triggered across the network.

It's quite normal for an adversary to gain access to a network for a period prior to a ransomware attack and in some cases the bad actor could dwell inside the network for weeks or months. In the time leading up to the ransomware detonation, the adversary will be hacking into different systems, gathering user credentials, infecting machines with backdoors and persistence and potentially exfiltrating data. Then they will deploy and the ransomware malware to all the compromised machines and detonate it.

The backups that are considered clean to use for recovery are at any point prior to the initial foothold date and time.

Event Types

The following is a list of common cyber incidents the team needs to be aware of.

- Virus or malware found on a hard drive.
- Unauthorized access to a system.
- Antivirus or EDR has been disabled by a bad actor.
- Denial of Service (DoS) attack that affects service availability.
- Data is compromised (sensitive, confidential).
- Email accounts are compromised.
- Network(s) are compromised.
- Servers are compromised.

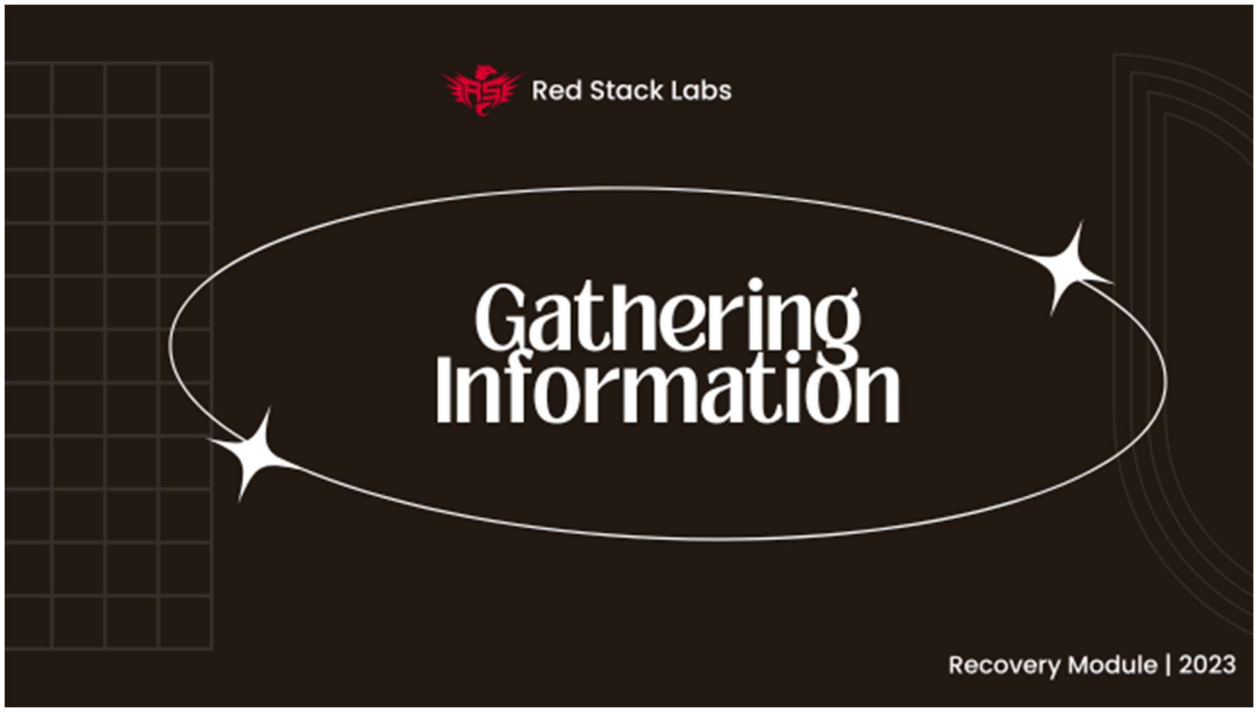
Determining severity for your organization

Level of severity is determined by the impact and time to recover. This will help when communicating, and decision making within the team.

- **low impact**: the business won't feel the impact of these events, only a couple employees might be impacted.
- **medium impact**: 1-2 days to recover workstations, servers, some data. Some of the organization might feel the impacts of these events, it will be compacted into certain areas but not affect all.
- **severe impact**: multiple days to recover critical servers and data. The entire organization will be impacted by these events.

Next Steps

1. Review cyber incidents and add to the events list low, medium, and severe impact ones in the IR Plan Template for your business.



Gathering Information

Contact information needs to be collected prior to initiating the recovery process, including the team members, contractors, vendors, and support providers. You want to have these available beforehand as it will support the recovery process.

Next gather the incident recovery plan and relevant documentation such as architecture diagrams, asset inventory, data inventory and compliance documentation.

Documentation collection checklist

Common items that you want to be collecting include:

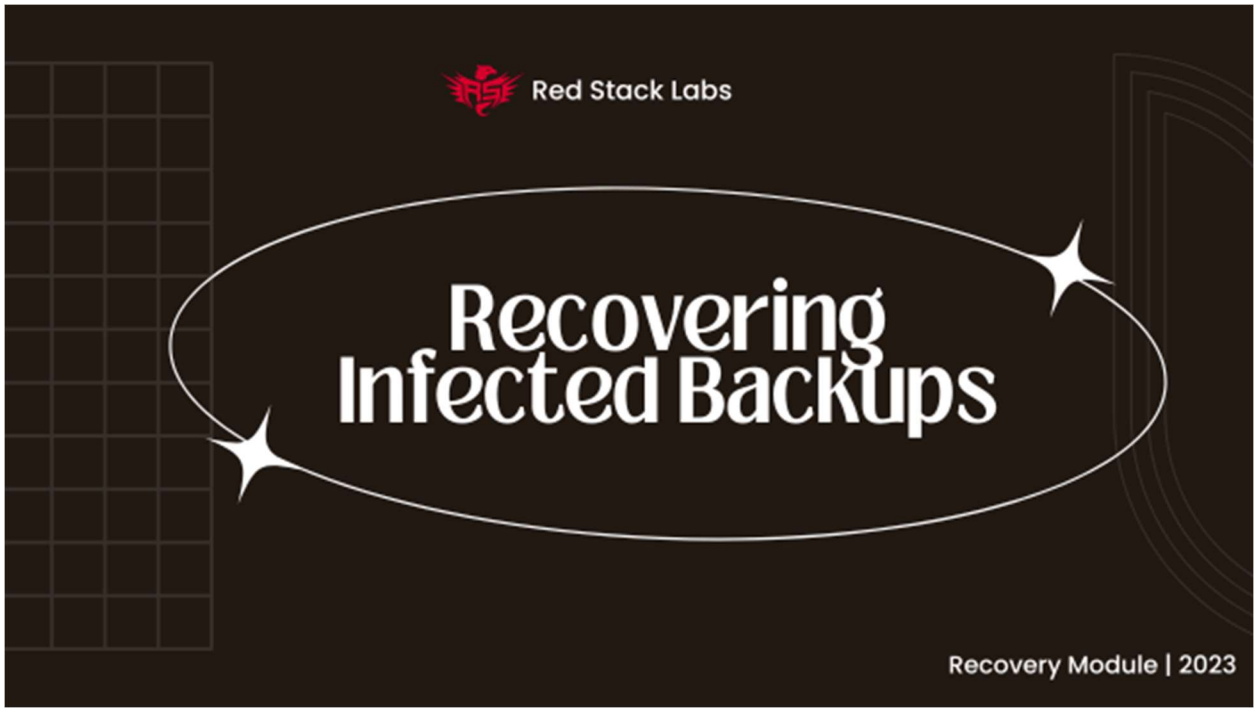
2. Contact Information - Inventory of staff, management and executives including contact information - at a minimum the department leads and managers for a larger organization so each department can be reached. Include personal phone number / email address, corporate email address so staff can be reached outside of regular work hours for emergencies. It would include team members, contractors, vendors & support providers.
3. Incident Recovery Plan - this would be the template we've been completing throughout this module.
4. Documentation

- Asset Inventory - we need to inventory all assets in your organization including servers, virtual machines, workstations/laptops, mobile devices, networking equipment, cloud and data assets (sensitive, confidential, corporate/financial/accounting, client data).
- Diagrams - inventory the architecture diagrams (including on-prem and cloud infrastructure, system design), network diagrams (including subnets, vlans, ports, protocols), data and backup architecture, security documentation (including security tooling and security architecture decisions, GPO's, security policies, compliance frameworks)
- Data Inventory - a list of all sources where data resides. It's important to consider the location due to residency requirements and other compliances, which team owns the data, and classification of it.
- Configurations - these are backups of the network configurations, and other configuration files that can help recover the good configuration of a device or service quickly. (Cisco routers/switches, WIFI, software services configurations)
- Backup inventory - inventory all the assets being backed up. Maintain records of the assets being backed up, include the date when the backups where verified, the date recovery was tested on that asset group, if something is not being backed up, include a reason why, and the name of the technician who did these checks, and the manager who signed off on each line item. Include the name of the backup software being used and the backup strategy, backup schedule, backup retention, backup locations.
- Compliance and regulations requirements - inventory the compliance and regulation requirements and reports - include any documentation that is relevant to maintaining compliance with each required privacy regulation.

Note: Should any of the above items change, this should be reflected within your documentation.

Next Steps

1. Refer to the IR Plan Template download and fill in sections on Inventory for assets, backups, diagrams, data, configurations, backup, compliance & regulatory requirements.
2. Complete the section for contacts.



Recovering Infected Backups

Free Decrypter Tools

A decrypter tool is designed to reverse the encryption of your files after a ransomware attack making them readable. There is an open-source project called "No More Ransomware Project" which provides free decrypter tools for different types of ransomwares. These tools do not support all types or variants of ransomware encryption but because it is a possibility you should know about this project. This project can be useful for recovering certain data, if a decrypter tool is available, but we recommend decrypting in isolation and safely shifting that data off an infected device.

Considerations

1. Free decrypter tools do not exist for the popular versions of ransomware by popular adversaries.
2. If decryption is successful, it should be done in isolation and the device should be considered infected after. Reversing the encryption on the data does not wipe the malware or backdoors used to compromise the device. The decrypted devices are still considered hot and in the red zone or in isolation.
3. The cyber security team should be doing the work to recover data professionally and safely from an infected device, if it is possible because it is possible to transfer a file with malware from an infected device onto a device in the green zone. Word,

Excel, Power point documents, PDFS, executables, and many other files can be used to carry malware, and most likely these are the types of files you will be transferring over for recovery, any one of them can be infected.

We hope that if you are lucky to find a free decrypter tool that works, you continue to follow the restoration plan and security architecture concepts provided here to avoid reinfection. A backup is better than decrypting an infected device because it has a lower probability of risk to reinfect.

Risk acceptance and probability of reinfection

Imagine trying to restore from a backup when you don't know the initial foothold into your infrastructure, what would be a safe backup date to restore from? The goal is to restore from a backup date prior to the initial foothold but if that is not possible then you must manage the risk and make decisions based off probability when choosing the backup dates for recovery.

Note: We cannot recommend which path is the best for your business because all companies and cyber incidents are not the same. These options of risk strategy are ones your executives and board will have to weight and decide based on the information provided. The risk strategies can be combined depending on the information provided for each individual system or data set.

Risk Options

1. **Risk Acceptance**: Because there is a chance that a backup chosen could be infected with malware or ransomware and it could reinfect your company, you must weight the risks. Ideally gather information about the cyber incident and identify the oldest sign of compromise, then recover from a backup a day or two before. The probability of infection is medium to high, because of unknown factors, this is accepting the risks.
2. **Risk Avoidance:** Do not restore from a backup and rebuild from scratch, this could cost more money but if your company cannot accept the risks of possible infection, this has a low probability of reinfection.
3. **Risk Mitigation**: Restore the systems into an isolated network and have the cyber security team investigate each system for signs of compromise. If the team provides an all clear to the system, then the reinfection probability is low.

Infected OS and Data backups

There may be instances where majority of systems and data are recovered, however, some are believed to have malware infections that predate the backup retention period. You have a several options including:

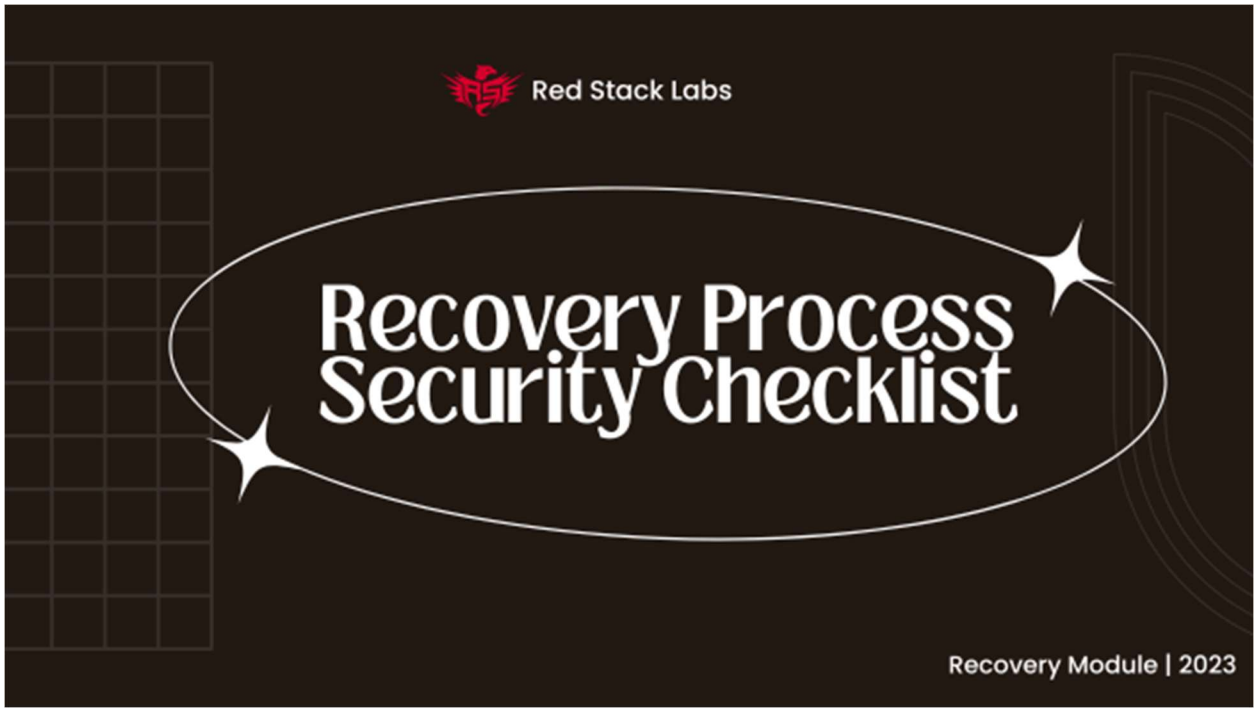
Automated

Backup software can include features that automatically run an antivirus scan prior to restoration. If a virus is discovered, the restoration will cease and fail. Should your company rely on a signature-based antivirus tool after being compromised by a bad actor with more sophisticated tooling? You would have to look at the probability of success and choose a risk strategy.

Manual

The process of manual data recovery for infected systems and data assets is to recover as much data as possible with the lowest degree of probability for reinfection. This task of infected data recovery should be handled by a cyber security or infected data recovery professional that is well versed with the adversary, tactics, techniques and procedures, and the type of infection that has occurred to properly extract the data cleanly. The manual procedure involves restoration of an image or data into a powered off state and accessing the data by attaching the drive to a special recovery system and extracting the data from the hard drive or virtual machine disk.

Note: Antivirus scans can be bypassed by bad actors and should not be the only line of prevention or assurance that a device is not infected. Endpoint detection and response (EDR) software can provide insight into the actions being taken by a device, a process, or a file then categorize and assess possible threats depending on the actions taken. EDR would provide better visibility combined with an Antivirus instead of just using one tool to assess possible infection.



Recovery Process Security Checklist

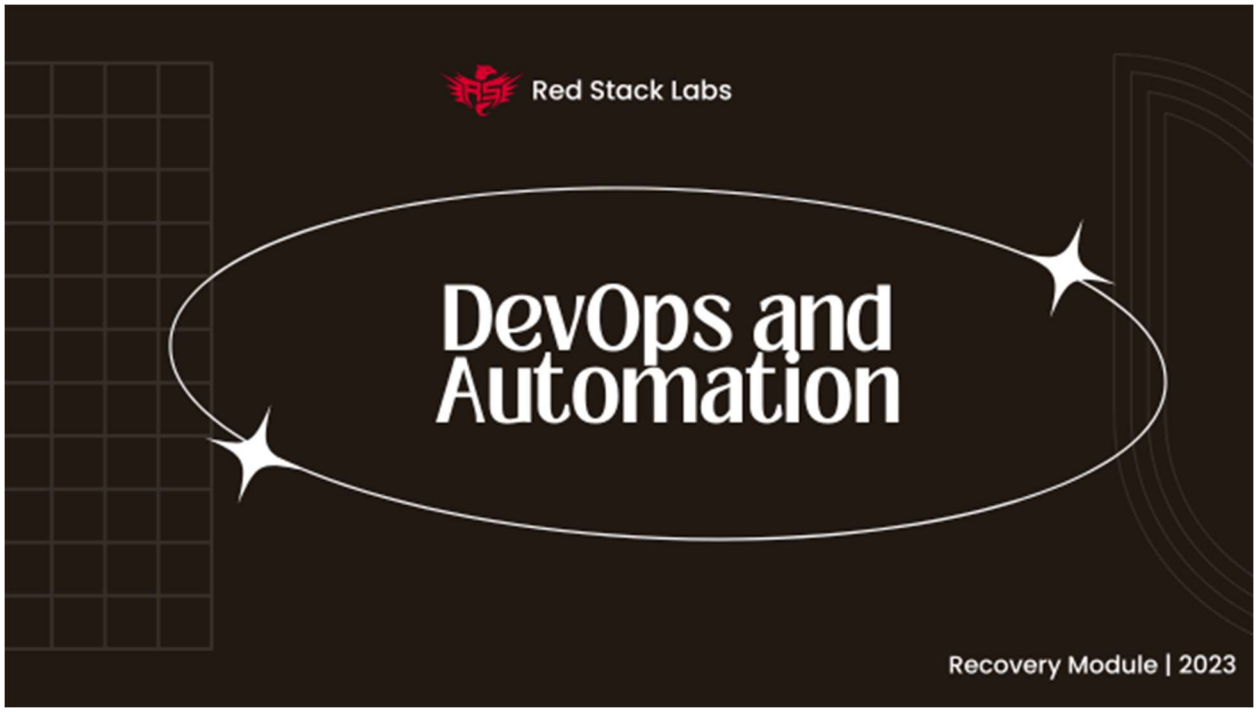
Security should be incorporated into the recovery process to ensure that each system being made available in the green zone is up to par and ready to face continued attacks.

Each server should be patched from vulnerabilities, security hardened and the backup agents needs to be installed and running. In addition, the passwords for all compromised users and services need to be changed, this includes all active directory accounts, local admin passwords, and 3rd party service users the adversaries may have compromised.

When bringing your recovered systems back online you want them to be more secure than the security posture at the time of compromise. This may also include additional recommendations from the cyber security team or insurer.

Next Steps

Download and review the Recovery Security Checklist. In the improvements section, review your current firewall and hardening controls.



DevOps and Automation

Infrastructure as Code (IaC)

For highly critical server and services, DevOps provides the luxury of quick recovery or rebuilding of an infrastructure environment. Infrastructure as Code (IaC) is used to create an infrastructure environment using code. Reasons IaC is used; repeatability, stability, and security, all of which can be managed at the code level and in the pipelines that are used to translate the IaC code and generate the environment. Throughout the pipeline process, policy checks conducted and enforced, like an automated auditing process that can review security controls through the CI/CD pipeline and enforce or alert if necessary.

If your company does not already use IaC but has been considering it, here are some things you might consider automating:

- Critical systems and services like Active Directory, DNS.
- Infrastructure for hosting applications and services like hypervisors, Kubernetes, and networking environments.
    - Application deployment into that infrastructure
    - Including dependant services like databases, webservers, etc.
- NAS / SAN that have a lot of files shares
- Hypervisors and virtual environments with a lot of VMs
- Database servers with a lot of databases
- Data for shared storage

State Management

State Management uses infrastructure code to change the configurations and state of a device or operating system. The state management system can automate the process to obtain the desired state. In terms of recovery this can be considered an additional automation to the IaC code, where infrastructure code can both build the infrastructure environment, and automate its state configuration for you as well. The outcome of state management is consistency, you can apply the same state to multiple servers, and this is especially helpful when dealing with larger groups of servers in your environment, this same consistency works the same when managing updates through the state management system, every server will receive the same exact update in the same exact way.