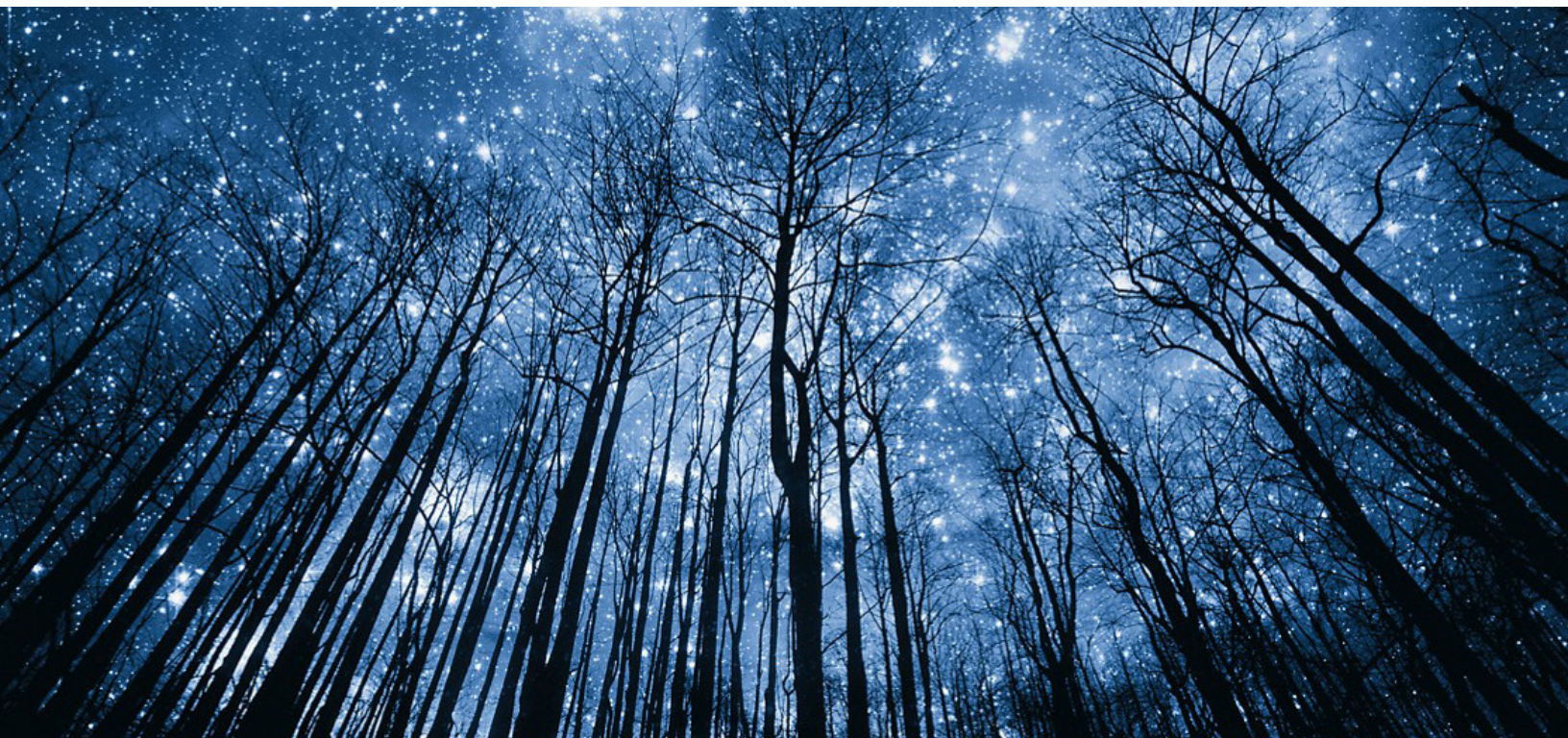


CAN'T JUDGE A BOOK BY ITS RECOVER



Faisal Choudry

GEOS: Senior Principal Engineering Technologist
Dell Technologies
Faisal.choudry@dell.com

Shreyash Nalamwar

Staff Solution Architect
Cloud Infrastructure Business Group
VMware
Snalamwar@vmware.com

Padraig Devane

Advisor, Solutions Architect
Dell Technologies
Padraig.devane@dell.com

The Dell Technologies Proven Professional Certification program validates a wide range of skills and competencies across multiple technologies and products.

From Associate, entry-level courses to Expert-level, experience-based exams, all professionals in or looking to begin a career in IT benefit from industry-leading training and certification paths from one of the world's most trusted technology partners.

Proven Professional certifications include:

- Cloud
- Converged or Hyperconverged Infrastructure
- Data Protection
- Data Science
- Networking
- Security
- Servers
- Storage
- Enterprise Architect

Courses are offered to meet different learning styles and schedules, including self-paced On Demand, remote-based Virtual Instructor-Led and in-person Classrooms.

Whether you are an experienced IT professional or just getting started, Dell Technologies Proven Professional certifications are designed to clearly signal proficiency to colleagues and employers.

[Learn more at \[www.dell.com/certification\]\(http://www.dell.com/certification\)](http://www.dell.com/certification)

Contents

Contents	3
Introduction	4
Let us have a look at some significant cases: Cyber Attack on the healthcare system in Ireland (HSE)	5
Norsk Hydro Attack	7
Colonial Pipeline: The largest publicly disclosed U.S. Cyber Attack.....	8
Attack trends.....	9
Cyber Recovery vs Disaster Recovery	10
A New Segment of Data Protection	11
Inability to Successfully Recover	12
Legislation	13
Maybe, You can hire the A Team?	14
Repeat Attacks	15
CDOT Repeat Attack.....	16
Backups: Vaults, Air gaps and Immutability.....	16
The Use Case	19
Questions to ask when building a recovery solution for cyberattack:	20
The Recovery.....	22
Conclusion.....	31
Bibliography	32

Introduction

This year, an increasing number of customers began asking us the same question relating to their infrastructure powered by VxRail and VCF on VxRail:

“How do we recover from a cyberattack?”

They elaborated further:

“We have to assume that the attack has compromised our existing data protection and Disaster Recovery!”

The next requirement further complicated matters:

“Also, the existing servers may not be safe due to the cyberattack. A forensic team may isolate the hardware for investigation and analysis. The recovery may have to take place on new servers/hardware.”

Well, that threw most of the options previously assumed relevant for recovery, out of the Window.

Reading on the topic and brainstorming with colleagues on the use case and subject matter experts, it becomes evident how unprepared most are.

The objective of this paper is to discuss cyberattacks and recovery in the context of the infrastructure and the above use case. The wider topic surrounding Cyber Recovery, particularly the common misconception that traditional Disaster Recovery (DR) and Backups are adequate, will also be discussed.

Statistically, enterprises are more likely to suffer a cyberattack than a disaster such as an earthquake, flood, or explosion. However, most enterprise organizations are only prepared for traditional disasters. Cyberattacks should not be viewed through the same lens as disasters. They require a vastly different approach to protection and recovery.



Preferred targets tend to be 'largish' companies including manufacturing, government agencies, financial institutions, and their infrastructure. They tend to be preferred targets because they are more likely to pay the ransom rather than suffer larger monetary loss. However, target types can change based on trends which we discuss later.

Common themes among the below use cases:

Large organizations with various IT systems ranging from legacy to new systems. The attacks were initiated over proxy from inside, for example, an email or an attachment was used. Once the components were installed, the attackers gained further access over weeks or months, but nothing prevented or detected that. By the time the attack took place, it was too late. A complete shutdown followed, as an attempt to stem the attack. Recovery took months and involved entire rebuilds.

A lot of the DR systems in place could not be used due to their current design of being connected to the production systems.

Let us have a look at some significant cases:

Cyber Attack on the healthcare system in Ireland (HSE)

On Friday, May 14, 2021, The IT systems of the entire health service of Ireland, the Health Service Executive (HSE) were subjected to a cyberattack. Once the HSE IT security teams realized what was happening, the HSE declared a Critical Incident. They began a sequence of events that led to the only option available: Switch off all their IT systems and disconnect all networks to avoid any further penetration or damage from the attackers.

Figure 1



(PricewaterhouseCoopers, 2021)

Independent Report by PricewaterhouseCoopers (PWC)

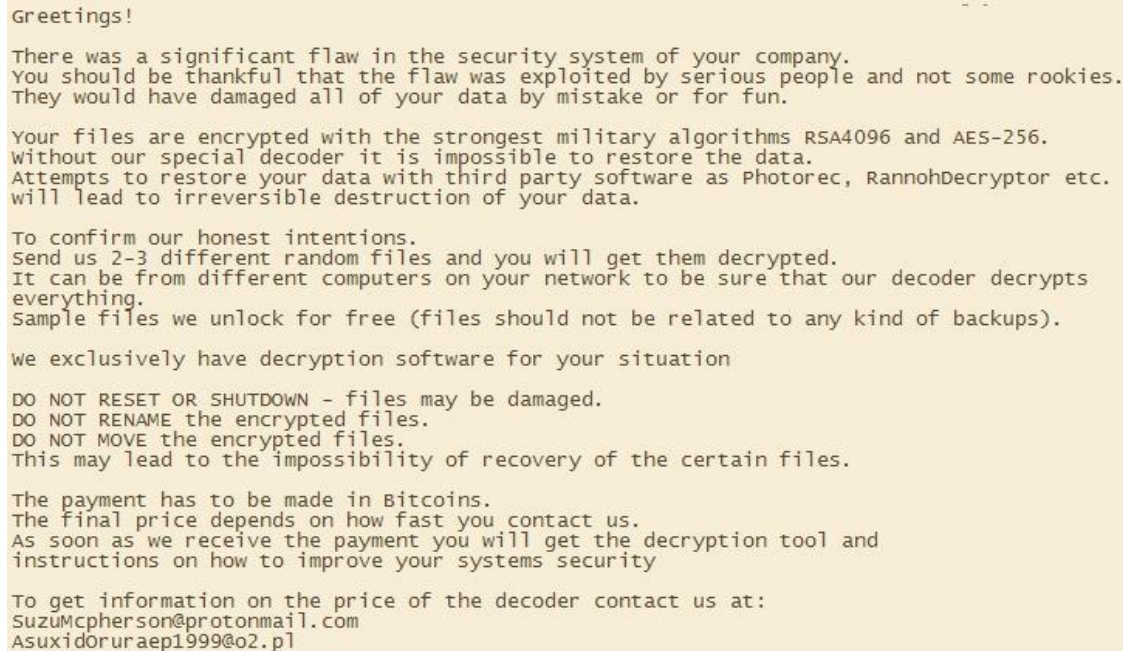
<https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf>

PricewaterhouseCoopers was brought in to analyze and review the HSE cyberattack. A 150-page report was published (see link above) which examined all events, including the aftermath, and the implications for the health service when all systems were shut off. Every aspect of the health service from patient record access, appointments, referrals, and surgery to Covid vaccine deployment was affected. Staff was forced to use pen and paper and produce manual systems. All recovery and business continuity systems in place were designed to recover from a traditional type of disaster, hence were of no use in this situation.

Norsk Hydro Attack

Norsk Hydro is one of the largest aluminum and renewable energy companies, headquartered in Oslo Norway. On 19th March 19th, 2019,com at 4 am, a call came from the CEO. “We are under a severe cyberattack; This is not a drill.”

Figure 2



Greetings!

There was a significant flaw in the security system of your company. You should be thankful that the flaw was exploited by serious people and not some rookies. They would have damaged all of your data by mistake or for fun.

Your files are encrypted with the strongest military algorithms RSA4096 and AES-256. Without our special decoder it is impossible to restore the data. Attempts to restore your data with third party software as Photorec, RannohDecryptor etc. will lead to irreversible destruction of your data.

To confirm our honest intentions. Send us 2-3 different random files and you will get them decrypted. It can be from different computers on your network to be sure that our decoder decrypts everything. Sample files we unlock for free (files should not be related to any kind of backups).

We exclusively have decryption software for your situation

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME the encrypted files.
DO NOT MOVE the encrypted files.
This may lead to the impossibility of recovery of the certain files.

The payment has to be made in Bitcoins.
The final price depends on how fast you contact us.
As soon as we receive the payment you will get the decryption tool and instructions on how to improve your systems security

To get information on the price of the decoder contact us at:
SuzuMcperson@protonmail.com
Asuxidoruraep1999@o2.pl

The attack cost the company \$71 million. They had to completely shut down all IT. Operations and production had to run manually with pen and paper even to the point of recalling retired employees, more experienced with manual procedures for production.

Norsk Hydro took a different approach. They refused to pay the ransom. Instead, they went public with the news. They let the media onsite to watch Microsoft’s Detection and Response Team (DART) and Norsk Hydro’s IT teams work through recovery. Norsk’s share price increased and much of the industry learned valuable lessons from their openness. Recovery took months and is still ongoing.

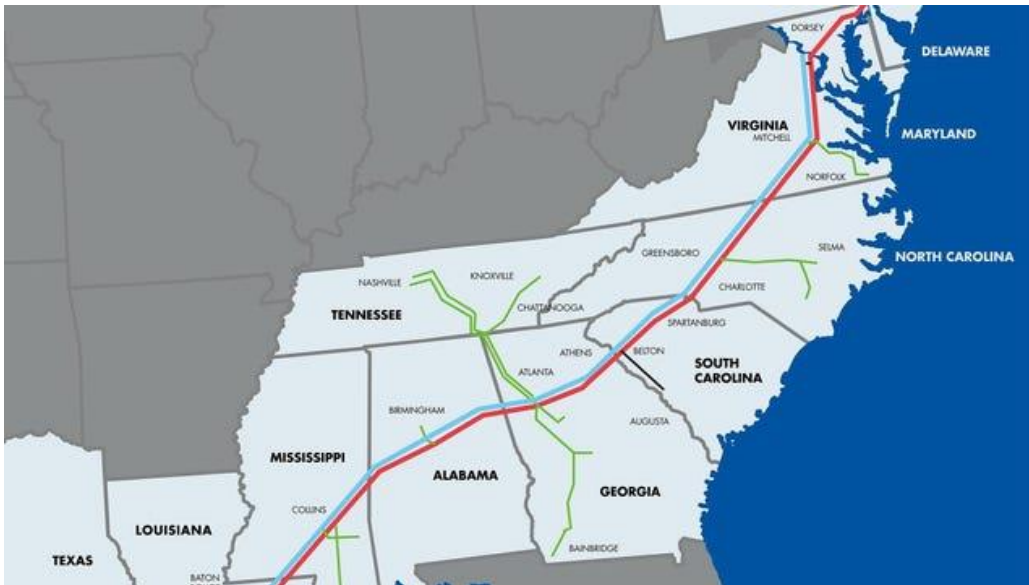
<https://www.hydro.com/en/media/on-the-agenda/cyber-attack/>

(Insights, 2020)

Colonial Pipeline: The largest publicly disclosed U.S. Cyber Attack

This is the largest disclosed attack against critical infrastructure within the USA.

Figure 3



Colonial Pipeline is the largest pipeline operator in the U.S. and provides approximately 45% of the East coast's fuel supply. The attack took place in April 2021 and resulted in the shutdown of operations.

<https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/colonial-pipeline-investigation/>

(Panettieri, 2022)

Following the attack, President Joe Biden declared a U.S Federal State of Emergency. The President signed an executive order relating to cybersecurity which included a Bill of Materials definition requirement. That gives a sense of perspective on the scale of the threat that is posed by cyberattacks to society and world economies.

<https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>

(JR., 2021)

The attack disrupted systems that control supply lines and so caused fuel shortages including at gasoline stations. This resulted in panic buying, fuel price fluctuations, flight cancellations with major airlines, and even disruption of fuel supplies to the military. Supplies and operations were run manually to resume services.

The example below of one of the measures taken to counter the far-reaching effects of the attack:

“To keep supplies flowing, the USDOT Federal Motor Carrier Safety Administration (FMCSA) issued a [Regional Emergency Declaration](#) on Sunday 9, easing standard restrictions on the land transport of fuel and the permissible working hours of drivers.”

Source: Federal Motor Carrier Safety Administration (FMCA) (Osborne, 2021)

The link below is a broadcast on how the group responsible for the attack are being tracked down:

<https://www.wsj.com/video/investigators-seize-bitcoin-paid-in-colonial-pipeline-ransomware-attack/3D9073C5-2E24-4855-9CCE-23148BFA08B1.html>

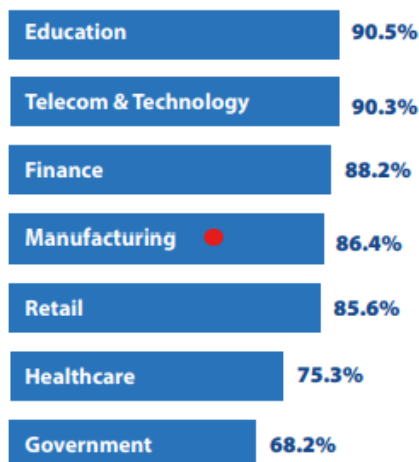
(NETWORK, 2021)

Attack trends

Trends are visible in the attacks and victims. The Cyber Edge Group surveyed industries for their report “Cyber Threat Defense Report 2022.” **Figure 4** can see the distribution of attacks across the industry. Solutions, tools, and external group/agency availability vary by industry, which we will see in further examples.

Figure 4

Percentage Compromised by at least one successful attack in the past 12 months, by Industry



Source: 2022 cyberthreat Defense Report (CrowdStrike, 2022)

Overall, the percentage of companies that were attacked in 2022 compared to previous years has increased. The amount of ransom and the number of organizations paying up has also increased. The preferred size of an organization that is attacked tends to be medium and large organizations. They are more likely to pay the ransom because they can afford to. However, there is a sweet spot. If the organization is too large, it can also attract too much attention, as can be seen from the above use cases. Therefore, enterprises with greater than 25,000 employees which could easily afford ransom amounts, are not the highest targeted groups. The sweet spots are enterprises with 10,000 to 24,000 employees.

Cyber Recovery vs Disaster Recovery



“Disaster Recovery (including DRaaS) has numerous shortcomings when used for ransomware recoveries.” - **Source IDC**

Let us first summarize the key differences between Disaster Recovery (DR) and Cyber Recovery (CR):

Disaster Recovery (DR)	Cyber Recovery (CR)
Physical destruction or loss of assets	Direct attack on systems or data
Standard backups used	Air-gapped backups required
Incremental backups	Immutable backups
Synchronous or Asynchronous Replication	Full rebuild/recovery
Recovery target: can be same or different h/w.	Recovery target: must guarantee hardware is clean/safe, pre-recovery.
Data Integrity	Security Audits/Detection capability requirement

Figure 5: Differences between Disaster Recovery and Cyber Recovery

A New Segment of Data Protection

Figure 5 lists the differences and appropriate tools and methods that are required for either a DR event or a cyberattack and CR. They are not the same. I have attended several meetings now where the assumptions are that traditional DR recovery post-cyberattack, is sufficient.

Cyber Recovery is a new segment of data protection (DP). The term data protection traditionally includes technologies that are geared for the more traditional types of disaster or failure. Unless already experienced in the field or a previous victim, the assumption tends to be normal DR-based procedures are sufficient for recovery from Cyberattack using a mixture of replication-based solutions, backups, point-in-time snapshots and restore. However, a cyberattack by nature is different in terms of how the attack takes place and more importantly, the primary target of the attack.

The definition of a cyberattack is when there is unauthorized system/network access by a third party. The critical difference is the data or system is the target, not a consequence. The effect of the attack can lead to data breach, data loss, encryption, or manipulation. The attack also aims to render any connected recovery systems useless, particularly if the objective is to gain control or coerce a ransom payment.

The **World Economic Forum's 2018 Global Risks Report**, listed the top three risks as natural disasters, extreme weather, and cyberattacks. Companies are well versed in “boarding up windows” when preparing for physical disasters. This cannot unfortunately be said when protecting against cyberattacks.

This has though started to improve. Teams have gotten better at protecting, although the entry points for hackers are numerous and are constantly moving and expanding. Security services and government agencies are also more sophisticated in tracking down teams of hackers. For example, in the past, they have used trails that are left by cryptocurrency transactions to track down members. But the ever-adaptable adversary remains the key threat within the e-Crime landscape, it is a constant cat-and-mouse game.

Inability to Successfully Recover

Figure 6 below shows a scale from 1 to 5, where 5 is the highest. The question asked was “How much does each of the below inhibit your organization’s ability to successfully defend or recover against cyberattack?”

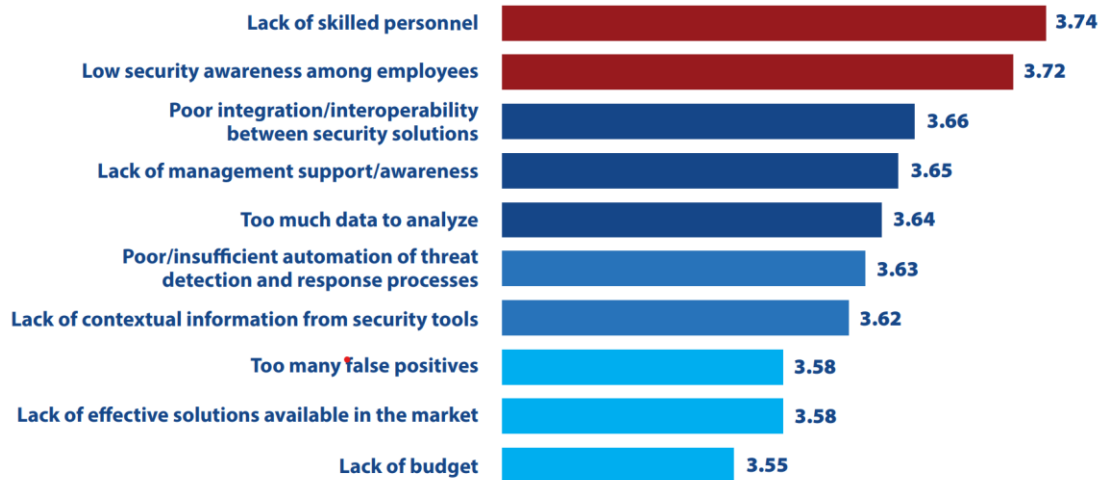


Figure 6: Source CyberEdge 2022 CDR Report

(<https://cyber-edge.com/wp-content/uploads/2022/04/CyberEdge-2022-CDR-Report.pdf>, Cyberthreat Defence Report, 2022)

(Eliad Kimhy, 2022)

(Hadley, 2022)

In Figure 6, the top two reasons are knowledge and expertise. Staff with relevant experience or knowledge is hard to come by. The United Kingdom (UK) Cyber Security and Cyber Crime division commented within a report that “the vast majority of businesses show a clear reactive approach when breaches occur” rather than proactive. Due to a lack of availability, knowledge, and skilled staff, they are also more likely to outsource the required services for protection and recovery. This can in turn creates additional problems such as securing third parties, which can be difficult. Breaches from captured credentials using third parties have occurred in past and are on the increase.

Which of the below security-related services does your organization outsource to third parties? In the below **Figure, 7** can see “outsourcing responses to cyber threats”, listed as number two in the list of detection and response to attacks.

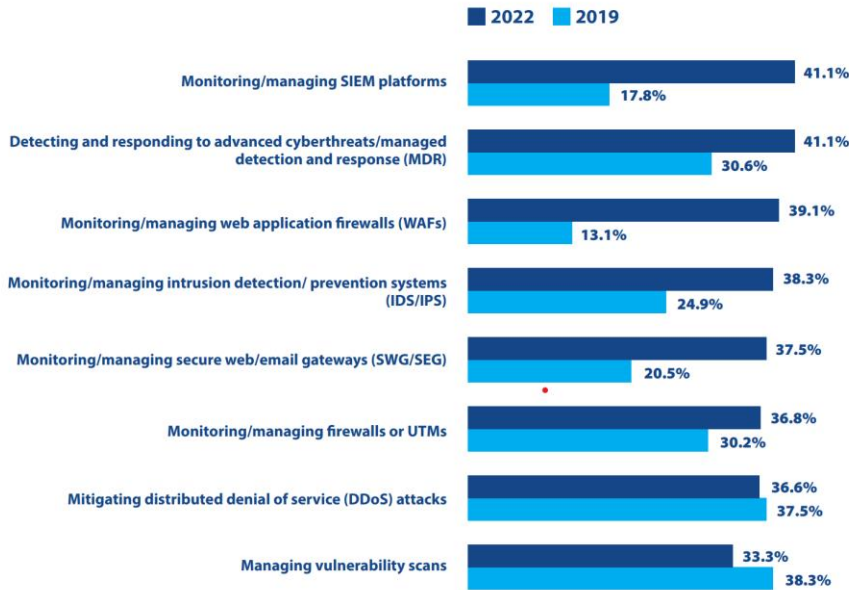


Figure 7: Source CyberEdge 2022 CDR Report

(<https://cyber-edge.com/wp-content/uploads/2022/04/CyberEdge-2022-CDR-Report.pdf>, Cyberthreat Defence Report, 2022)

Legislation

Some sectors in the industry have tried to address the threat by creating some form of legislation that governs the design and implementation requirements. Infrastructure and data are targets and so to protect critical infrastructure within countries and governments, the European Commission agreed on a directive in 2016 to increase the security of Network and Information Systems within the European Union (EU). The Network and Information Systems (NIS¹) Regulations came into force on 10 May 2018 in the UK. This all aims to protect the sectors vital to the economy. These sectors are heavily reliant on network and information systems to function. These include energy, transport, drinking water, healthcare, and digital infrastructure. A similar action by the U.S. government took place with the signing of an executive order, following the Colonial Pipeline attack.

The NIS Regulations established regulation in the UK to ensure operators of essential services (OESs) and relevant digital service providers (RDSPs), put into place requirements to ensure the security and recoverability of their infrastructure and services in the event of an attack.

¹ NIS is European based, not to be confused with NIST framework which was a result of a U.S. executive order, developed by the National Institute of Standards and Technology. NIS and NIST are closely aligned.

Security Engineering, vulnerabilities, architecture, and design have become a larger concern since the pandemic. Disciplines such as patch management, penetration testing, and security configuration management have risen in the list of importance due to the increased use of mobile devices being used from less protected environments. Mobile devices have always been the most difficult devices to secure and lock down.

Add into that mix that fact the weakest link within security tends to be the user/employee that has internal access. Whether the users unknowingly click a link, an internal email string that has been weaponized, or possibly an angered employee. The Pandemic and global move to remote work and mobile devices has increased the challenge to security.

Approximately 54 million U.S. users must access their office networks remotely at least once a week according to the Cyber Threat Defense Report 2022. Factor in the rest of the world. **Figure 6** showed that the second highest concern is, security awareness among employees.

Maybe, You can hire the A Team?

You need a team within your organization to oversee the design and implementation of any recovery plan. The role does not need to be dedicated; it can be part time. But the team does need to be responsible for any decisions that are made when preparing or designing systems for Disasters or Cyber Attacks. This team is responsible for testing recovery procedures at regular intervals.

The report by PriceWaterHouse Coopers following the attack on the HSE in Ireland, recommended within their findings:

- Establish an initial cybersecurity incident team and appoint an interim senior leader.
- Set clear responsibilities for IT and cybersecurity across all parties that share health data or access shared health services.
- Create a 'code of connection' that sets minimum cybersecurity requirements for all parties.
- Establish an executive-level cybersecurity oversight committee to drive continuous assessment of cybersecurity risk and a cybersecurity transformation program across the health services.
- For cybersecurity (a CISO) to be responsible for driving forward tactical cybersecurity improvements, managing third parties providing cybersecurity services, and lead the cybersecurity response to cyber incidents.

Source: **Independent Report by PricewaterhouseCoopers (PWC)**

<https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf>

The above is not radically different from teams that would have been set up for the purposes of DR. This must take place to avoid using standard DR practices in the event of a cyberattack.

Repeat Attacks

Standard DR procedures have a high likelihood of failure, either immediately due to encryption or later as something may have been left behind, so threat actors maintain access to the environment. This is another security-related issue to consider, what can you trust after an attack? It is not just the restore or rebuild to consider but pre and post-rebuild. Has anything been left behind which can be used for a repeat attack once all is restored? Can you add anything to help detect future attacks?

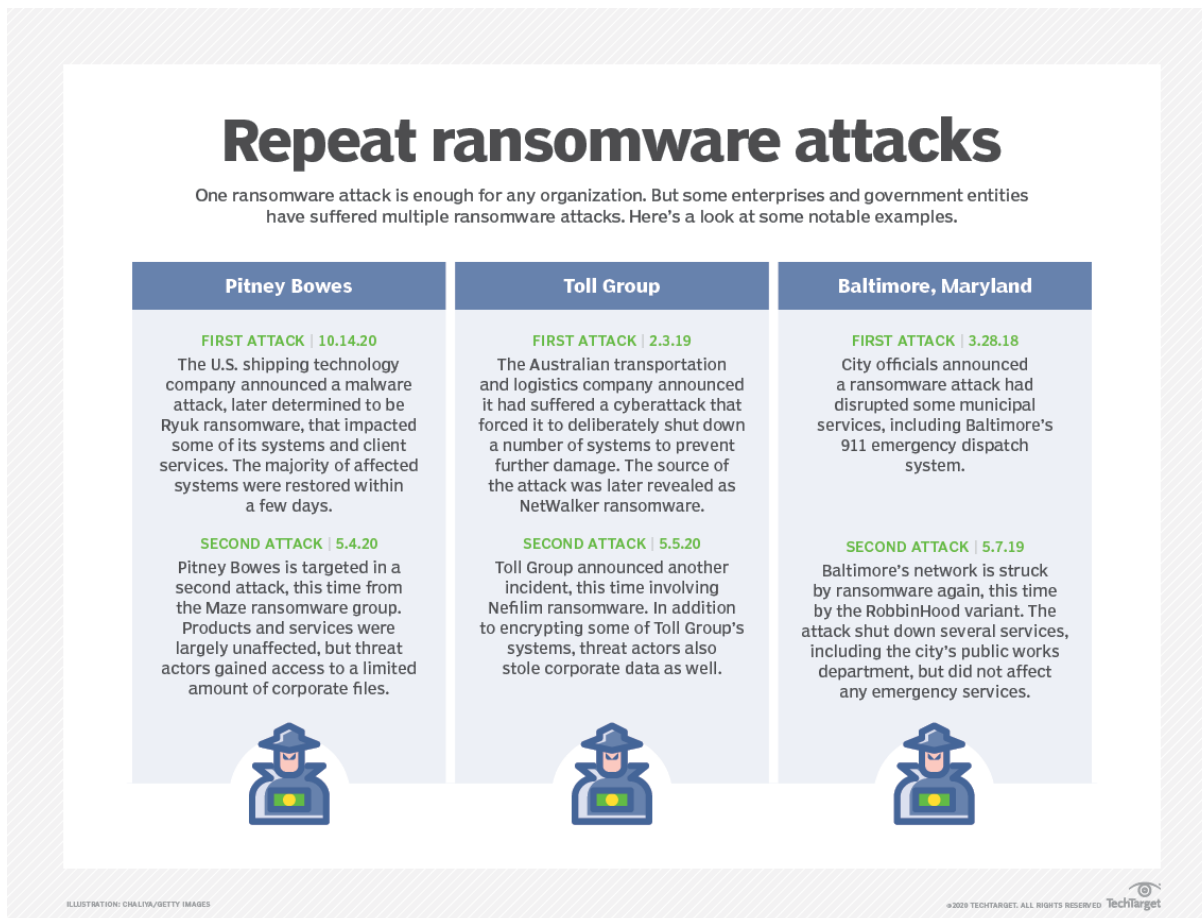


Figure 8: Source: Repeat ransomware attacks: Why organizations fall victim
<https://www.techtarget.com/searchsecurity/news/252484720/Repeat-ransomware-attacks-Why-organizations-fall-victim>
(Alexander Culafi, 2020)

CDOT Repeat Attack

The Colorado Department of Transportation (CDOT) was repeat attacked in 2018. The actors got entry using a virtual server, which had less security, and then used the domain controller to push out the ransomware attack (SamSam ransomware attack). Luckily, security policies did limit access to all parts of the network. However, CDOT's back-office systems including 1300 workstations and 400 servers were attacked and instantly encrypted.

The CDOT security team did restore and rebuild, and thought they had contained the attack, but a week later were attacked again. This time the state of Colorado had to declare a State of Emergency. This was the first time a State had declared a state of emergency for a cyberattack. Following the declaration, several events were triggered. The CDOT was given access to:

- The State's Office of Emergency Management
- The National Guard
 - The National Guard has a cyber security expert team (infosec experts)
- Colorado's State Fusion Centre
- Governor's Office of Information Technology
- The Department of Homeland Security
- US-CERT
- The Federal Emergency Management Agency
- The FBI
- Other security vendors

All the above teams coordinated efforts in recovery and investigation, The FBI was on-site. No ransom was paid according to reports. Over 130 people were involved from the above parties in the recovery effort. Two weeks were spent detecting any further threats and malware and then a further two weeks of recovery.

After 9 months, the Department of Justice indicted two suspects.

(Goud, 2022)

Backups: Vaults, Air gaps and Immutability

Backups are seen as a fundamental antidote to cyberattacks. We have already discussed, and given examples of, use cases where replication and always connected-based systems for recovery have critical weaknesses within the given scenario. Attackers infiltrate backups as part of their attack to make any chance of recovery unsuccessful. It is a growing trend with attacks, to make all backups unusable. Then there are also "Sleeper Attacks." This is where malware has been installed and backed up. The malware remains dormant until the attack begins possibly months later. Then the data and backups are encrypted.

Immutability is a solution here. Immutable means unchanging over time or unable to be changed. So immutable backups offer a solution where data is written once and then is read-only, it cannot be altered later. Some vendors provide immutable solutions including cloud-based solutions.

The Second problem relating to backups, is connectivity. If a device or some aspect is connected, an attacker can find it and attack. We require a way of isolating our backup target from connectivity when not in use. During an attack, actors attempt to identify and remove backups and any other methods of recovery.

The terms “Air-Gapped” and “Vault” are used here to reference the relevant technologies and design to protect and recover from cyberattack. The architecture includes two distinct areas: The Production Network and Vault area. These are created by network design and secure policies, separated by a temporary connection or “Air-Gap” as in **Figure 9**. The Vault Area is a completely isolated section (logically and physically) which contains the necessary infrastructure and protected backup data. When a backup is created and saved, the “connection” between Production and Vault is brought online. Once the backup has been completed the connection is “cut” so the target systems within the Vault area where backups are finally written, are isolated.

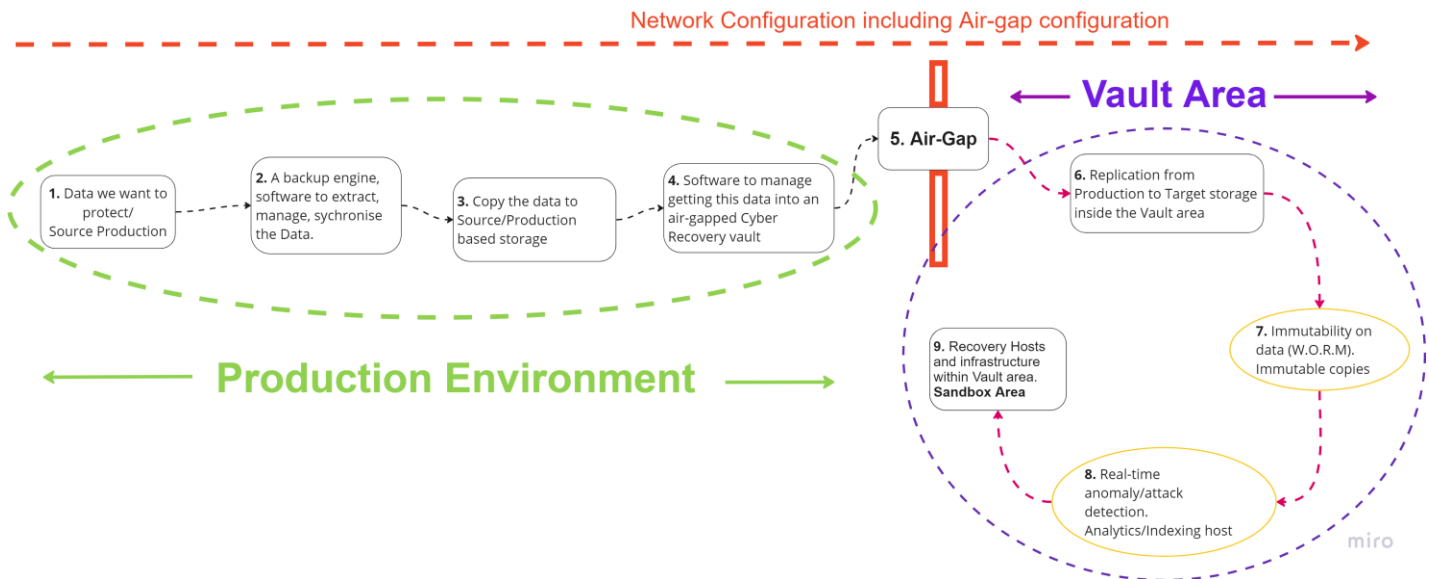


Figure 9: Architecture for Protection and Recovery from Cyberattack

This architecture does come with challenges. If based on-premises, physical security can be a challenge, in addition the volume of data being backed up can be huge. Within this design systems copy data to a target and then cut the connection logically using policies within the software. During this time, the data is synchronized to the vault device which is the final destination. The volume of data being backed up is increasing immensely, due to the threat posed by cyberattacks. And synchronization of all the data can be slow if the solution is either incapable or has not been designed or sized with the required capacities in mind.

Specification of machines that are used is as important as the network architecture and the throughput available and stitching this architecture and all the relevant pieces together, can be complex. It is a very different design to a traditional DR type design.

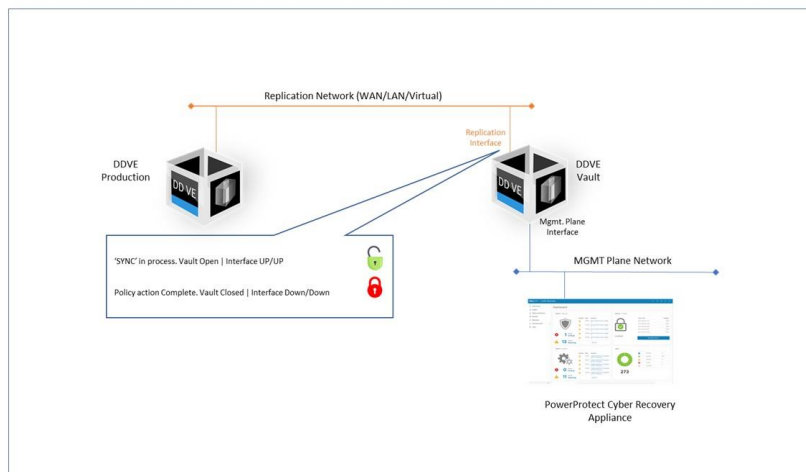


Figure 10: Diagram of the PowerProtect Cyber Recovery host and PowerProtect DD (Previously Data Domain) in a Vaulted configuration

On premise or cloud-based solutions are available. Cloud-based backups do offer an alternative method. The effectiveness and security of the solution depends on the vendor. Only copying data into some form of cloud-based storage is not going to protect backups from attack. One requires solutions which Airgap and Vault the data at the final destination, and so have various network and security policies to make it difficult for an attacker to connect and manipulate or destroy the recovery data.

These designs however are not foolproof or a complete guarantee of safety. Attackers have been known to penetrate isolated systems by attacking the software that runs them. There is some form of connection or device sitting somewhere and attackers are becoming more sophisticated in finding these entry points. The proliferation of Internet of Things (IOT) devices has only given attackers more opportunities.

In the case of the attack on the Iranian nuclear facility, a computer worm infected the Programmable Logic Controllers (PLCs) controlling the spinning centrifuges. PLCs are industrial computers that control machinery and industrial processes. They can scale from small module-type devices with inputs and outputs, to large rack-mounted systems with thousands of inputs and outputs. The attacker (later reported by the Israeli government as a joint cyberattack operation by Mossad and the CIA) planted Stuxnet into a Command-and-Control System Update, and then attacked centrifuges that were refining uranium. The attack caused the fast-spinning centrifuges to spin beyond their capability and destroy themselves. (Ronen Bergman, 2021)

The Use Case

So now let us look at the problem at hand. How do we protect and more importantly how do we recover/restore VMware Cloud Foundation (VCF)? As said at the beginning of this paper, VCF customers had begun asking us for this particular use case. How do they recover if cyber-attacked?

Customers did ask for several assumptions to be used for the use case:

- (i) Assume any existing replication (DR) systems have been affected so unusable.
- (ii) Existing backups that were not held within a Vaulted Area with an air-gapped, are unusable.
- (iii) Demonstrate a worst-case scenario for VCF so assume that the Management Cluster, Workload domain, and data have been affected.
- (iv) Existing hardware can we trust this post-attack?

So where does one begin? The protection and restore method to use depends entirely on the technologies and the location of the infrastructure. The method also depends on the scenario as discussed earlier, a disaster event or cyberattack.

Initially, when the requests began coming our way, we did start to look at DR-type solutions but quickly became aware these solutions would not work. The other problem that we came across was the lack of documentation within the technology and attack surface we were dealing with. There are many attack surfaces around cyberattacks and confidence and expertise in securing each area does vary. This also includes existing documentation and whether companies that have been attacked even went public with their experience, which generally tends not to be the case.

Norsk Hydro was an exception to this rule. Post-attack they went public with their attack and Recovery effort. This was welcomed by the community. A lot of valuable knowledge was shared from their experience.

The attack entry points tend to change as the actors do. Over time they find certain methods of entry become more difficult to penetrate, so they move to a new attack surface. Therefore, there are trends in where attacks take place. Types of organizations that are targeted and the size of the enterprise do also change over time. **Figure 10** shows companies that are surveyed and where they have either the most or least confidence in securing against attack.

On Scale of 1 to 5 with 5 being the highest, rate your organizations ability to defend against attack in each area

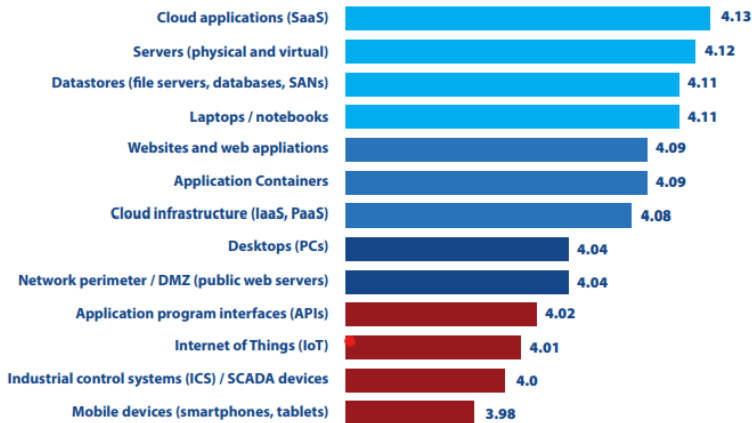


Figure 10: Source CyberEdge 2022 CDR Report

(Group, 2022)

In preparation, there are questions must be asked. This is not an exhaustive list and predominantly deals with the recovery aspect. These are the questions that we began asking ourselves to help us narrow down the correct approach. Hopefully, the list gives an idea to “start the ball rolling” on questions a team should consider:

Questions to ask when building a recovery solution for cyberattack:

- Are the hosts, systems, laptops, and such, on-premises or off?
- Which operating systems are being used?
- Any adjoining critical systems and which?
- How much time do we have to recover?
- What is the minimal viable product or functioning system that we can restore?

- How do we guarantee the hardware is safe after an attack so can restore it?
 - Can we restore on existing hardware and hosts?
 - Do we need new hardware or hosts?
 - If we restore on different hardware, will this still function?

- Will the attacked systems and hosts be isolated by a forensics team for investigation once the attack has been discovered? In which case, see above point.
- What else must be restored or recovered? Data or applications?
- If dealing with ransomware or encryption, are we able to wipe and rebuild, or do we have to get hold of the decryption key?

- Which other teams do we need to call in for help?
 - Possibly government, vendor, security agency involvement?
 - Should we go public with information about the attack? For example, Norsk Hydro
 - What additional software do we add to help detect attack signatures within our environment?

- For backups which solution or product shall we use?
 - Does this need to be an “air-gapped” solution architecturally?
 - Which components do we need to back up?

- Does the backup need to be stored externally and air-gapped?
- What should we use as external storage?
- What is the restore/recovery procedure?
- Can we document this?
- Can we test this procedure?
- Does the procedure change with versions or updates?
- Can we automate any of these procedures?

I am not going to discuss or give a 101 explanation of the VCF or VCF on VxRail architecture here as there are dozens of papers and documents describing this online including on VMware's site. The assumption here is that the reader has knowledge of VCF and VxRail. What I will mention briefly though is a key difference between VCF and VCF on VxRail. VxRail automates the ESXi cluster build of the hosts and the vCenter creation, and this must be considered during restore and rebuild procedures.

The configuration of our system within our lab is standard. The VCF system is deployed across eight nodes or hosts. Four nodes are used for the Management Cluster and the other four are used for a VI Workload domain or second cluster. Our objective is to try to recover this system after a total loss. The assumption is that our infrastructure was attacked, and all content encrypted hence the complete loss of infrastructure components and data.

The components that are listed below will need to have been backed up and then recovery procedures will need to take place. This scenario assumes a complete loss of VCF including the management cluster. The following components will need to be restored:

- SDDC Manager
- vCenter server
 - The vCenter Distributed Switch(s) vDS – single or multiple
- NSX-T data center
- VxRail install including the VxRail Manager if this is being used (VCF and VxRail)
 - Standard VCF deployment will not use VxRail nodes or manager

The network architecture and switches may also need to be part of the recovery procedure. I will not cover the switch recovery here. Suffice to say the switch configurations will have been backed up and so a restore and rebuild of the network switches may also be required.

The Recovery

The restore/recovery procedure can be much more complex than backing up. This is something that I do want to focus on within this paper. I have read a lot of documentation discussing backups (air-gapped, vaulted, cloud, and so on) and other solutions to save in the event of a cyberattack. However, the restore procedure depends on the technology being used and may not be straightforward. It is important to not assume that because components were backed up using the correct technology and architecture, the recovery is guaranteed or an easy procedure. This is also why we must think of Cyber Recovery, differently from Disaster Recovery. A lot of the mechanisms available during Disaster Recovery which help simplify recovery procedures are unfortunately not available to us. In our case, the recovery is going to be a manual and a complex procedure.

We began working with the Solution Center in Cork. In terms of equipment and complex configurations, it is something this team does every day, they are experienced, and they have all the necessary equipment. The team had attempted to build a VCF VxRail setup, back it up, and then a complete restore including the recovery of the Management Cluster. But the restore procedures were not straightforward, particularly in restoring VCF's SDDC manager. A simple restore did not work and resulted in a non-functioning SDDC manager/VCF system. Part of the challenge was related to the databases contained within SDDC and the build/system, including the vCenter configuration.

After a lot of digging, hitting dead-ends, and coming up empty-handed, we finally came across a paper² that was written for a Disaster Recovery Scenario. The paper was not specific to cyber recovery but because of the procedure that it used to rebuild and recover, we thought it was a perfect fit for our scenario.

The following figures and flow charts summarize the overall recovery procedures for VCF/VCF and VxRail. The procedures below are manual procedures that involve restoring the backed-up components from VCF and then restoring them in a particular order. There are additional procedures that are involved in addition to the recovery steps. As a note, a partial restore of VCF is not supported within this use case as the simulation here is of a complete loss.

NB: A newer version of this document with updated and additional procedures has been created based on our findings from testing this use case. The document is made available. I have included the older version of the document here as this is available online now (see footnote below).

² PowerProtect Data Manager: Recovering VMware Cloud Foundation
[PowerProtect Data Manager: Recovering VMware Cloud Foundation \(delltechnologies.com\)](#) (Kantor)

NB: a newer version of this document has been created based on the findings from our testing of this use case. The document will be made available. I have included the older version of the document here as this is available online now.

I have summarized the recovery procedure in a series of diagrams. The first diagram is a high-level view of the steps involved. Each major step is numbered, and this is further expanded in subsequent diagrams.

Figure 11: Summary of the Overall Recovery Procedure

At a high level, we begin with a VxRail deployment. This builds the ESXi hosts, the cluster, and a new vCenter. This vCenter is referred to as a temporary vCenter. The second paragraph in box 1 also mentions a VCF only environment which will require deploying the ESXi cluster before restoring any components. The original vCenter goes through a restore process including several manual procedures to restore vCenter related components including networking, vDS. Then NSX-T is restored and rebuilt followed by VxRail components (if running VxRail) and then finally the SDDC manager. Again several manual procedures required here.

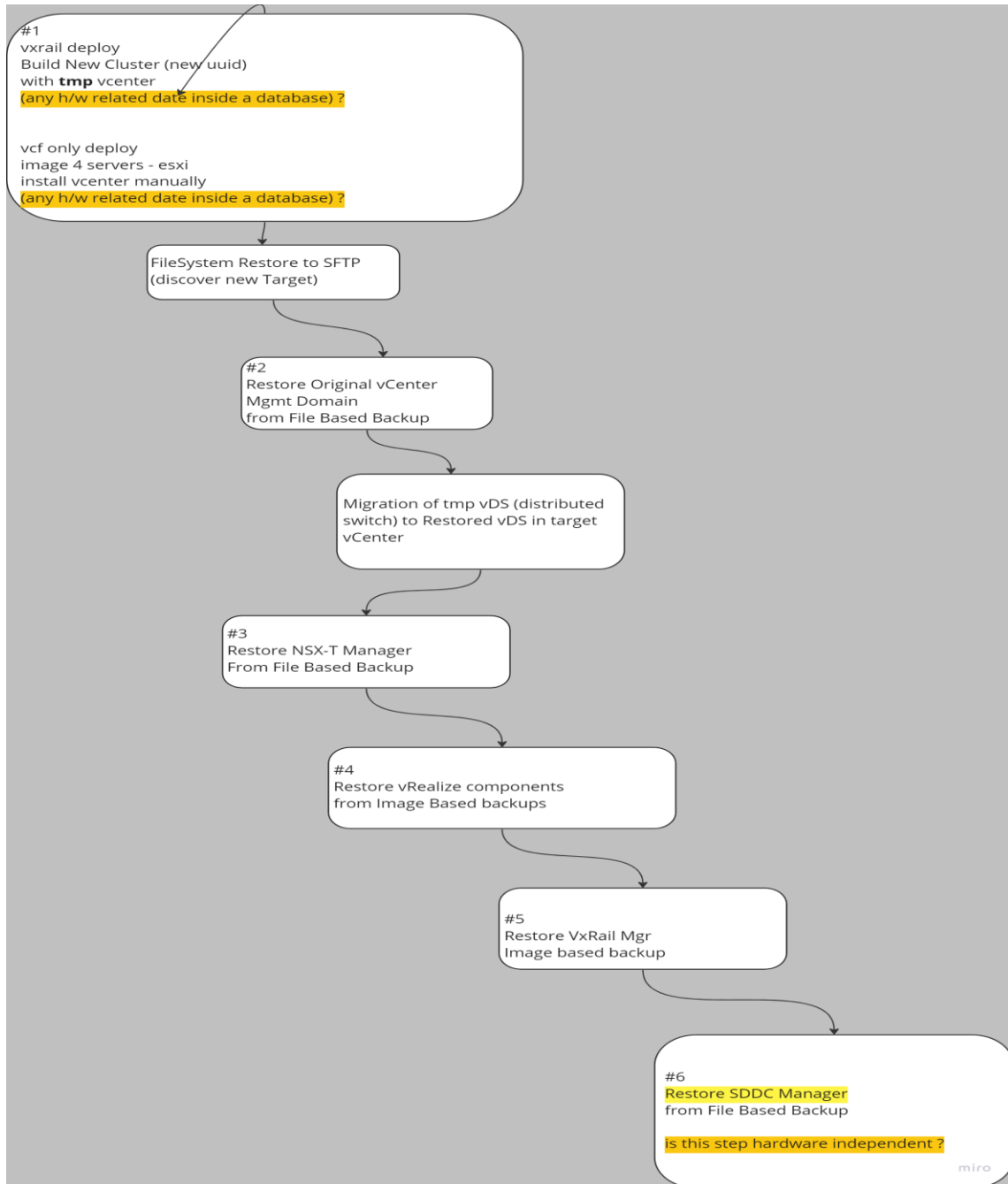


Figure 12

A four-node cluster is built here either using the VxRail bring-up procedure or the standard VCF procedure. The same ESXi Management VM IP addresses and FQDNs as the original system will be configured here in this rebuild. If using the VxRail bring-up, the Temporary vCenter built by this process will have different IP and FQDN as later the old vCenter from backup will be restored. There is a solve (<https://solve.dell.com>) procedure which is a document covering the procedure on how to migrate a cluster from a temporary vCenter to a target vCenter. The procedure does include the execution of a PowerShell script.

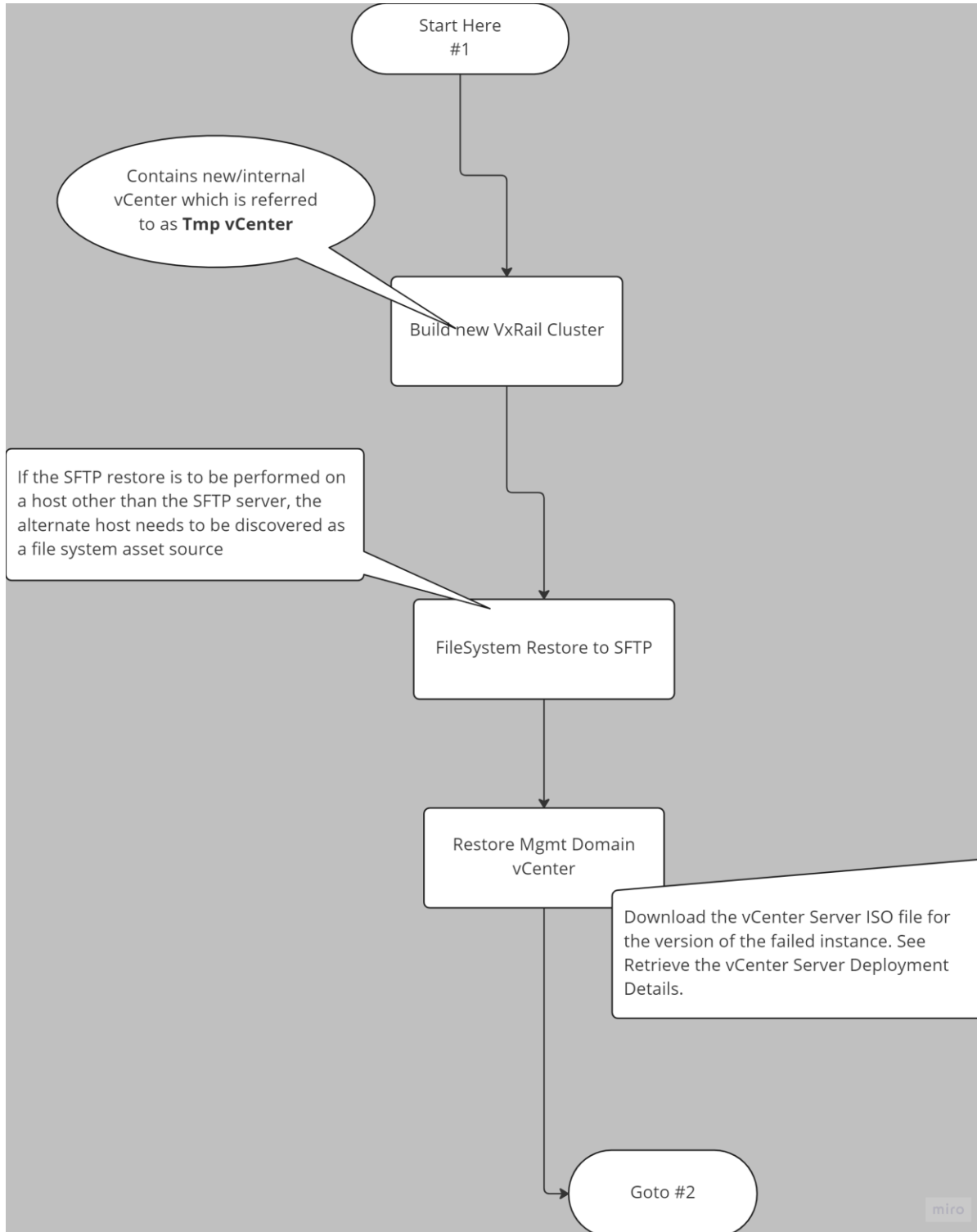


Figure 13 Restore vCenter and migration of Distributed Switch(vDS).

(This diagram is enlarged across the next two pages)

This part of the procedure includes migration of the Temp Distributed Switch to the Restored Distributed Switch in the target vCenter Server. The Target vCenter was the original vCenter from the destroyed system, now restored.

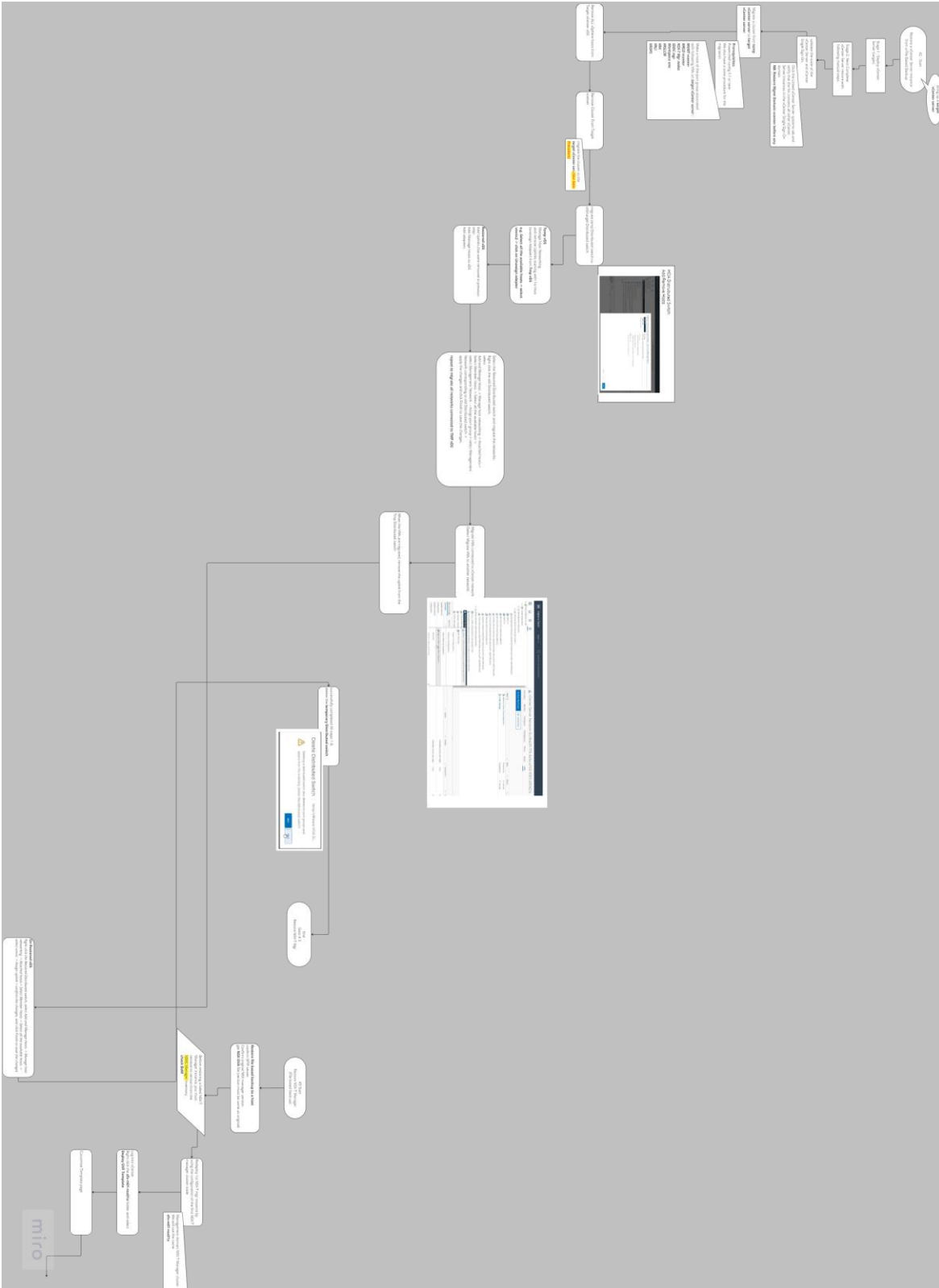


Figure 14 (enlarged view of figure x, across two pages) – Restore vCenter and migration of Temp. Distributed Switch(vDS) to the Restored Distributed Switch.

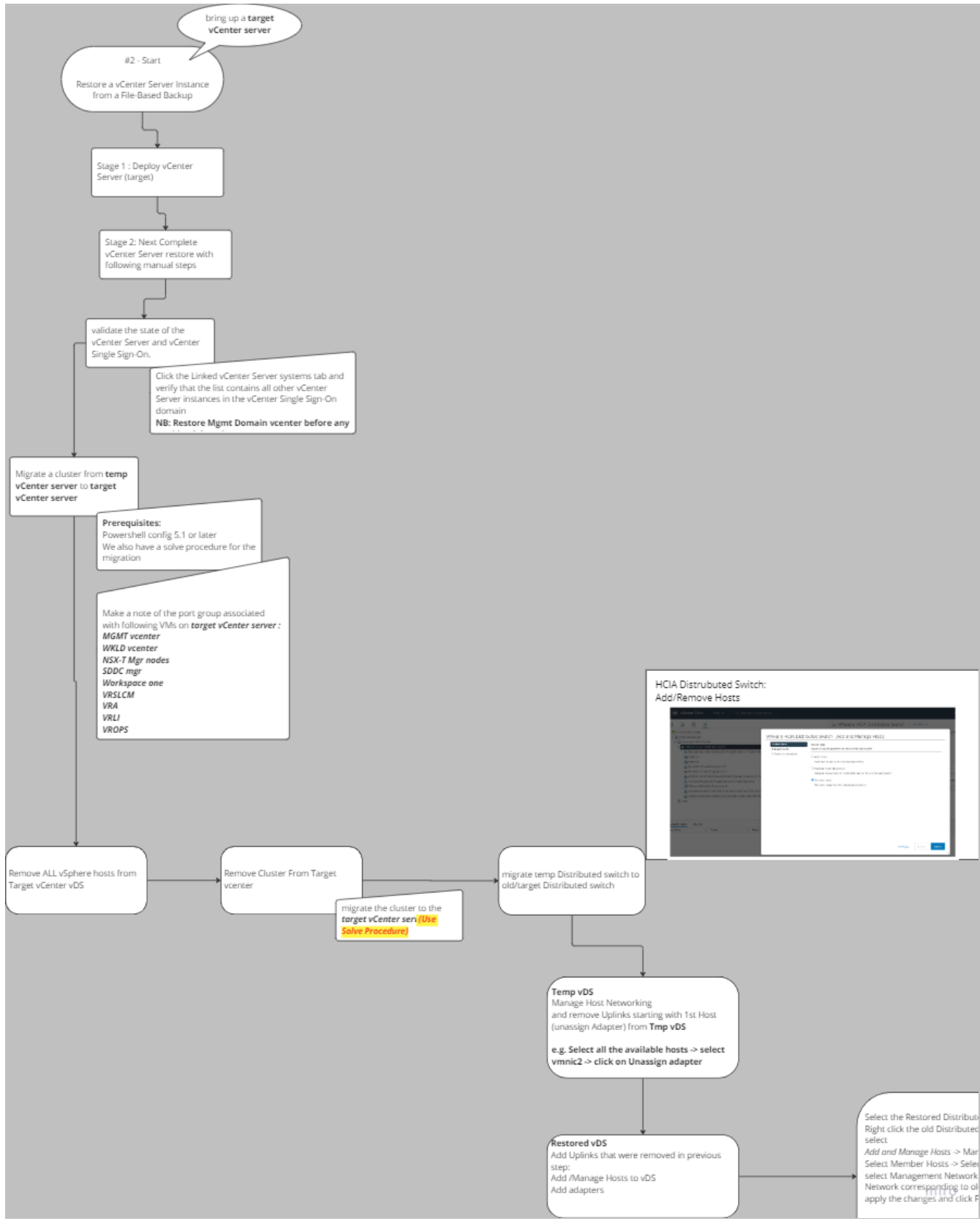


Figure 15 Restore vCenter and migration of Distributed Switch(vDS) - continued.

The steps included here are on the restored Distributed Switch (vDS), summarized as follows:

- Uplinks and hosts are adjusted.
- Networks are migrated.
- VM kernel adapters are configured.
- All VMs connected to the vCenter network on Temp vDS are migrated to the network on restored vDS.
- All VMs connected to the Management network on Temp vDS are migrated to the restored vDS.
- When migration steps have been completed, temporary vDS is deleted.

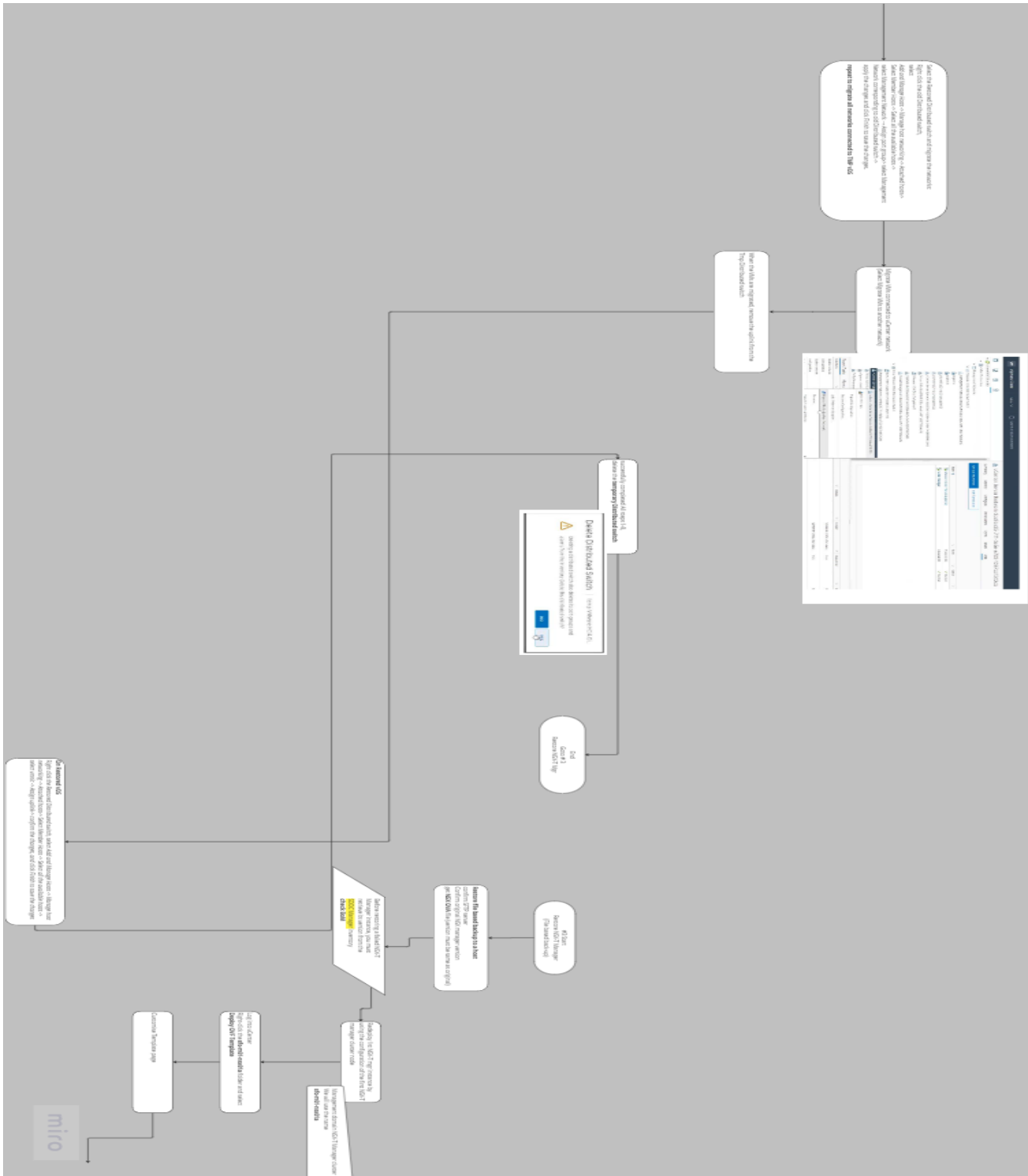


Figure 16 NSX-T Manager Restore

The NSX-T restore procedure includes the following steps in summary:

- The new NSX-T manager is deployed using the correct version of OVA.
- The File based backup of NSX-T is restored from an SFTP source, using the NSx-T manager UI for the restore.
- Once restored completely any appliances are added with original Ips and FQDNs.
- Steps are repeated for each host within the cluster.
- Then Any NSX-T Edges are restored.
- Temporary Edges are first deployed, and failed nodes are removed.

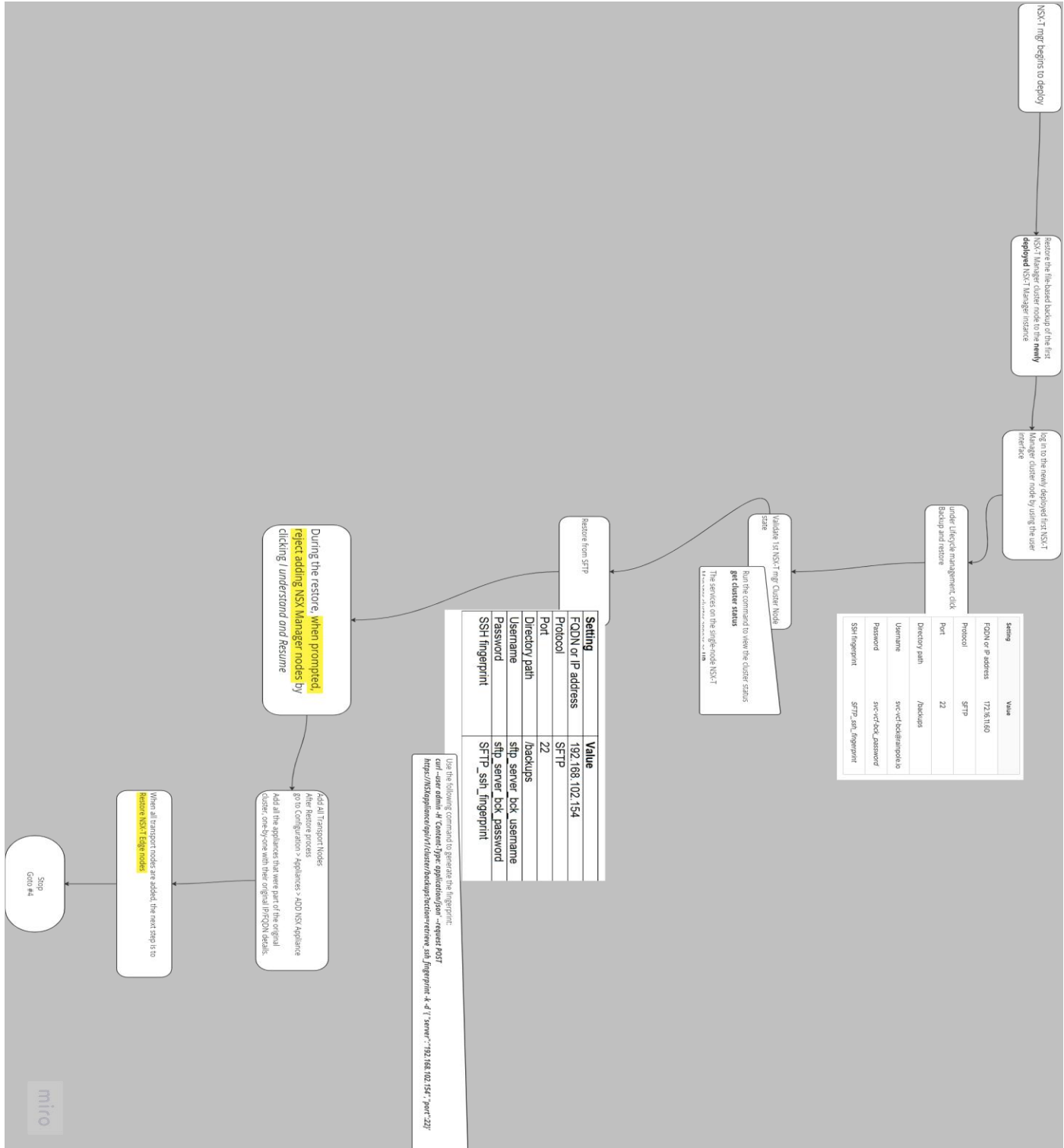


Figure 17 Restore Applications including vRealize components and Restore SDDC Manager.

- If the system did include a vRealize deployment, and then this must be restored before the SDDC manager is restored. Bear in mind vRealize is not a mandatory installation so a customer may or may not have had this in the previous install. In which case skip straight to the VxRail restore if this is a VCF and VxRail restore, as opposed to a standard VCF restore.
- The Following VMs are restored in the following order. Note the VxRail manager is last in this list, if this is a VCF and VxRail based system:
 - vRSLCM
 - VIDM
 - VRA
 - VROPS
 - vRealize LOGINSIGHT
 - VRNI
 - vRealize Business
 - VxRail Manager

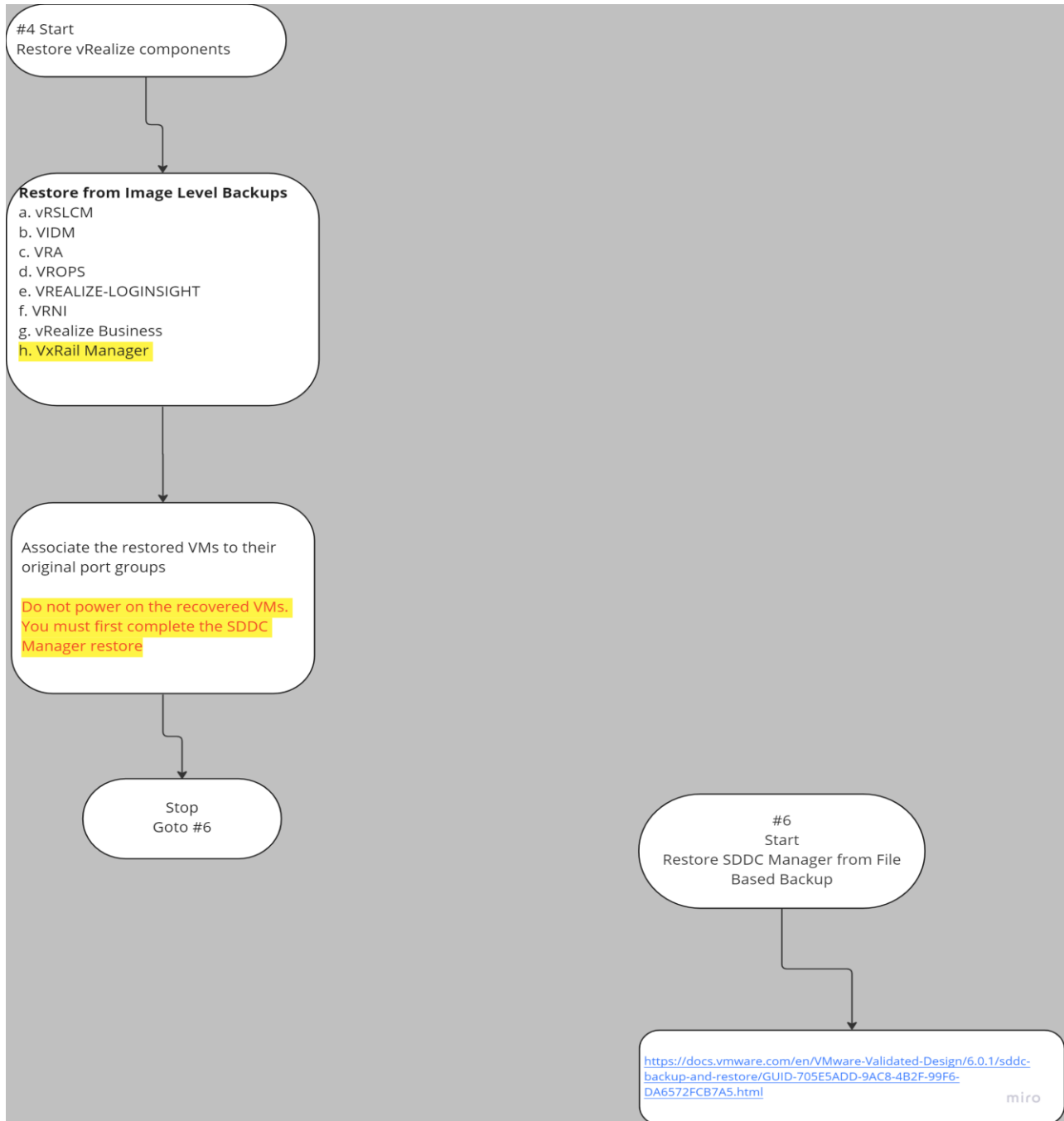
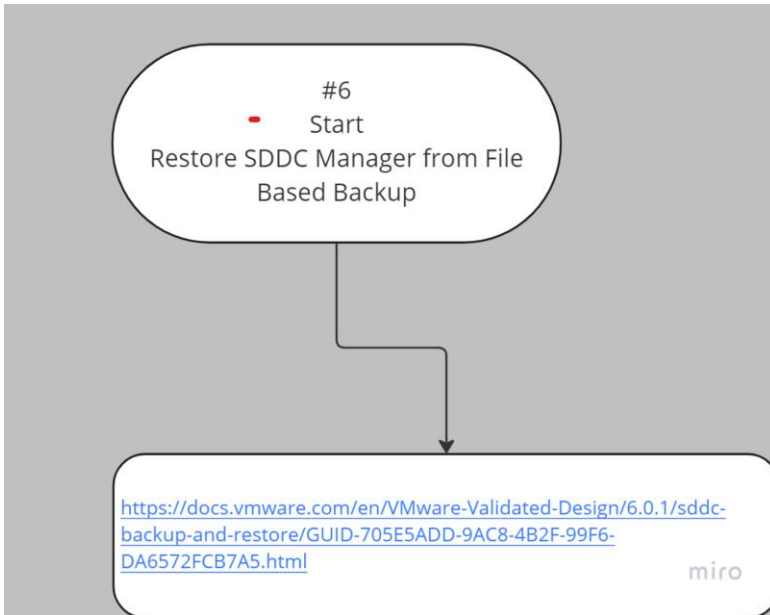


Figure 18 SDDC restore procedure

- The SDDC³ restore procedure is the last step and a critical part. It is complex due to the databases held within.
- First, a new SDDC manager using the correct OVA version is downloaded and deployed.
- Then the file-based backup of the original SDDC manager is restored. The host access to SDDC requires OpenSSL. Refresh any SSH keys stored within the SDDC inventory.
- Any static routes that are configured within the SDDC manager must be manually reconfigured.
- A recovery script must be run, available from VMware⁴. The documentation on VMware's site covers the restore procedure. See also the footnote below.



³ The restore procedures for SDDC are covered at VMware's site [Restore SDDC Manager from a File-Based Backup \(vmware.com\)](https://docs.vmware.com/en/VMware-Validated-Design/6.0.1/sddc-backup-and-restore/GUID-705E5ADD-9AC8-4B2F-99F6-DA6572FCB7A5.html)

⁴ See [VMware Cloud Foundation SDDC Manager Recovery Scripts \(79004\)](#)

Conclusion

The current geopolitical situation in Europe has made the reality of cyberattacks, headline news. Companies have been coming to us for advice largely because of this situation. China and Taiwan have been involved in an invisible war for several years, either targeting infrastructure or government agencies or spreading fake news to demoralize public opinion. In addition to that, several high-profile past cases mean that the topic now has a high level of visibility.

On a positive note, security teams are more effective in stopping or detecting attacks. When attacks bring critical services within countries to a standstill, big players become involved. These attacks have led to greater exposure and the direct involvement of governments and their agencies. In several cases, new legislation has been created to help combat the threat and legislate how certain organizations operate and secure themselves. Government agencies have become more experienced and coordinated in finding these attack groups. This is not good news for the actors.

However, as these attackers change targets or widen their scope and target more types and sizes of enterprises, we must also become better and more versed in protection and recovery against these attacks. There is no “Magic Bullet” to this challenge. Each solution depends on a host of factors as seen earlier in this paper. Attack surfaces vary, types of attacks that are encountered, and technologies that are targeted, so the solution must be appropriate. What must be consistent though is the approach to tackling the issue. It is a constantly moving target.

We have tried to demonstrate in this paper the correct approach to this type of scenario. Compared to normal Disaster type events, the approach must be different, particularly as many technologies we use for recovery during normal disasters, would be of no use post-cyberattack. Do not assume what works for a disaster event, will work for a Cyberattack. Categorize the events differently. Have a team that is aware of each of these types of scenarios and is capable of building plans to protect and recover appropriately and test it.

As Mike Tyson, a famous Boxer, once said “Everyone has a plan until they’re punched.” He said this before his fight with Evander Holyfield. Tyson went on to bite a chunk of Holyfield’s ear off due to Holyfield’s constant head butts. Sure, that was not part of the plan!

Bibliography

- Alexander Culafi, S. N. (2020, June). *Repeat ransomware attacks: Why organizations fall victim*. Retrieved from Techtarget: <https://www.techtarget.com/searchsecurity/news/252484720/Repeat-ransomware-attacks-Why-organizations-fall-victim>
- CrowdStrike. (2022). *The CrowdStrike 2022 Global Threat Report*. The CrowdStrike 2022.
- Eliad Kimhy, L. R. (2022). *Slipping Through the Security Gaps: The Rise of Application and API Attacks*. Akamai. Retrieved from <https://www.akamai.com/resources/state-of-the-internet/slipping-through-the-security-gaps-the-rise-of-application-and-api-attacks>
- Goud, N. (2022). *Ransomware Attack strikes CDOT for the second time!* Retrieved from Cyber Security Insiders: <https://www.cybersecurity-insiders.com/ransomware-attack-strikes-cdot-for-the-second-time/>
- Group, C. (2022). *Cyberthreat Defence Report*. CyberEdge Group. Retrieved from <https://cyber-edge.com:https://cyber-edge.com/wp-content/uploads/2022/04/CyberEdge-2022-CDR-Report.pdf>
- Hadley, J. (2022). *Cyber Workforce Benchmark*. immersivelabs. <https://www.immersivelabs.com/>. Retrieved from <https://www.immersivelabs.com/wp-content/uploads/2022/05/cyber-workforce-benchmark-2022-immersive-labsfinal.pdf>
- <https://cyber-edge.com/wp-content/uploads/2022/04/CyberEdge-2022-CDR-Report.pdf>. (2022). *Cyberthreat Defence Report*. CyberEdge Group. Retrieved from <https://cyber-edge.com/wp-content/uploads/2022/04/CyberEdge-2022-CDR-Report.pdf>
- <https://cyber-edge.com/wp-content/uploads/2022/04/CyberEdge-2022-CDR-Report.pdf>. (2022). *Cyberthreat Defence Report*. CyberEdge Group. Retrieved from <https://cyber-edge.com/wp-content/uploads/2022/04/CyberEdge-2022-CDR-Report.pdf>
- Insights, N. H. (2020). *Cyber-attack on Hydro*. Retrieved from <https://www.hydro.com/en/media/on-the-agenda/cyber-attack/>
- JR., J. R. (2021, May). *Executive Order on Improving the Nation's Cybersecurity*. Retrieved from The White House : BRIEFING ROOM: <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>
- Kentor, I. (n.d.). PowerProtect Data Manager:Recovering VMware Cloud Foundation.
- NETWORK, T. W. (2021, July). *Investigators Seize Bitcoin Paid in Colonial Pipeline Ransomware Attack*. Retrieved from The Wall Street Journal: <https://www.wsj.com/video/investigators-seize-bitcoin-paid-in-colonial-pipeline-ransomware-attack/3D9073C5-2E24-4855-9CCE-23148BFA08B1.html>
- Osborne, C. (2021, May). *Colonial Pipeline ransomware attack: Everything you need to know*. Retrieved from <https://www.zdnet.com/>: <https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/>
- Panettieri, J. (2022, May). *Colonial Pipeline Ransomware Attack*. Retrieved from <https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/colonial-pipeline-investigation/>
- PricewaterhouseCoopers, (. (2021). *Conti Cyber Attack on HSE*. HSE Board.
- Ronen Bergman, R. G. (2021). *Blackout Hits Iran Nuclear Site*. Retrieved from The New York Times: <https://www.nytimes.com/2021/04/11/world/middleeast/iran-nuclear-natanz.html>

Disclaimer: The views, processes or methodologies published in this article are those of the authors. They do not necessarily reflect Dell Technologies' views, processes, or methodologies.

Dell Technologies believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." DELL TECHNOLOGIES MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying and distribution of any Dell Technologies software described in this publication requires an applicable software license.

© 2023 Dell Inc. or its subsidiaries. All Rights Reserved. Dell and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.