ISSN (Online) 3134-884X

Advanced Research Journal of Computer Science

Received: November 20, 2025 | Accepted: December 19, 2025 | Published: December 30, 2025
Volume 2, Issue 2, Pages 14-22

DOI https://doi.org/10.66590/arjcs2025020204

Research Article

OPEN ACCESS

Check for updates

Development of an Air-Gapped Dark Site Prototype for Enhanced Business Continuity Resilience

Muhammad Faizan Afzal[1*]
[1]Depatment of Computer Science, Government College University, Faisalabad, Pakistan

Abstract | This study presents the motivation, design scope, and implementation of a Dark Site integrated with an air-gapped environment to enhance Business Continuity and Disaster Recovery (BCDR) capabilities. The proposed framework is developed in alignment with organizational objectives aimed at improving system resilience and operational reliability. The research explores the conceptual foundations and architectural characteristics of both Dark Site and air-gap solutions, highlighting their roles in ensuring secure and isolated backup infrastructures. A Proof of Concept (PoC) is designed and implemented to validate the feasibility of the proposed approach. The study provides a comprehensive overview of the system architecture, including platform specifications, deployment setup, data schema, and operational workflow. Experimental evaluation and testing results demonstrate the effectiveness of the proposed solution in improving system availability, security, and recovery readiness. The findings further outline the key advantages of integrating air-gapped environments within disaster recovery strategies. This work also serves as a foundational reference for future research and practical implementations in resilient infrastructure design.

Key Words Business Continuity, Disaster Recovery, Crisis Management, Resiliency, Dark Site, Air Gap, Architecture, Cloud Computing, Cybersecurity, Tails, TOR, Linux, Windows

Author Designation: [1]Researcher

*Corresponding author: Muhammad Faizan Afzal (e-mail: Malikfaizan0000123@gmail.com).

How to Cite the Article:
Afzal, Muhammad Faizan "Development of an Air-Gapped Dark Site Prototype for Enhanced Business Continuity Resilience." *Advanced Research Journal of Computer Science*, vol. 2, no. 2, December 2025, pp. 14-22. https://doi.org/10.66590/arjcs2025020204

INTRODUCTION

Ensuring the continuous operation of business processes in the presence of unexpected and large-scale disruptions is the core objective of Business Continuity (BC) and Disaster Recovery (DR). These capabilities, often integrated with crisis management strategies, enable organizations to prepare for, respond to, and recover from critical failures that may affect primary operational environments. However, a fundamental challenge remains: ensuring that BC/DR infrastructures themselves remain accessible, reliable, and functional during extreme failure scenarios [1,2].

To address this challenge, this study explores the design and implementation of a resilient infrastructure based on Dark Site and air-gapped environment principles. The proposed approach focuses on establishing an independent and isolated system capable of supporting essential business and technical operations when primary production systems become unavailable or compromised. The goal is not only to provide backup capabilities but also to ensure the survivability and accessibility of critical recovery resources under adverse conditions.

The research is motivated by the needs of a large global information services organization seeking to enhance its existing BC/DR readiness. Although conventional disaster recovery plans and crisis management frameworks were already in place, limitations were identified in areas such as secure access to critical documentation, availability of essential computing resources, and command-and-control support during crisis situations. These gaps highlighted the necessity for a more robust and independent solution [4].

In response, this work investigates modern practices related to Dark Site and air-gapped architectures and develops a Proof of Concept (PoC) to evaluate their feasibility and effectiveness. The study presents the conceptual foundations of these approaches, followed by

the design and implementation of a prototype system. The PoC includes detailed system architecture, deployment strategy, operational model, and evaluation results, providing insights into scalability and practical applicability.

A Dark Site, often complemented by an air-gapped environment, serves as an independently maintained backup infrastructure designed to operate during disaster scenarios. In the proposed design, the Dark Site is intended to host essential services such as a standby corporate communication platform and critical static resources, including contact information, operational guidelines, and configuration data. These resources are securely preloaded and periodically updated to ensure readiness [5].

The air-gapped component further enhances system resilience by providing a physically and logically isolated repository for critical data, ensuring protection against cyber threats and systemic failures. Unlike traditional disaster recovery systems, the proposed architecture is not intended to support full transactional recovery. Instead, it focuses on delivering a minimal yet reliable set of functionalities required to maintain business continuity, communication, and recovery coordination.

The developed PoC serves as a validation platform for these concepts, offering a foundation for future large-scale implementation. By combining independence, security, and operational readiness, the proposed solution contributes to strengthening organizational resilience and advancing modern BC/DR strategies.

Dark Site and Air Gap Background

Dark Site and air-gapped solutions are well-established concepts in the domain of cybersecurity and business continuity. However, to effectively understand their role in resilient system design, it is essential to clearly define their characteristics, operational principles, and practical applications [6].

Dark Site Concept

A Dark Site refers to a pre-developed and fully functional web platform that remains inactive or hidden until it is required during a crisis situation. These sites are typically maintained in a standby state and can be rapidly activated to provide critical information to stakeholders. The primary objective of a Dark Site is to ensure timely, accurate, and controlled communication during emergencies, particularly in scenarios where misinformation can spread rapidly through digital and social media channels.

Unlike conventional corporate websites, which are designed for branding and marketing purposes, Dark Sites are intentionally minimalistic and focused. They prioritize clarity, reliability, and immediacy of information delivery. By preparing such platforms in advance, organizations can significantly reduce response time and maintain control over crisis communication.

Benefits and Applications of Dark Sites

One of the most significant advantages of a Dark Site is its ability to enable rapid organizational response during critical events. In crisis situations, delays in communication can negatively impact public trust and organizational reputation. Dark Sites allow institutions to quickly deploy structured and consistent messaging, ensuring that stakeholders receive verified information without delay.

Additionally, Dark Sites serve as alternative communication channels when primary systems are unavailable or compromised. They can support multiple stakeholders, including customers, employees, partners, and regulatory bodies, by providing centralized and coordinated updates. This capability enhances transparency and demonstrates organizational preparedness in managing unexpected events.

Key Features of Dark Site Architecture

Effective Dark Site implementations typically include:

- Consistent and verified content delivery
- Clearly identified communication sources or spokespersons
- Integration with social media platforms for real-time updates
- Centralized information management for diverse stakeholders

These features enable Dark Sites to function not only as communication platforms but also as coordination hubs during crisis management.

Air Gap Concept

An Air Gap is a security mechanism that ensures complete physical or logical isolation of a system from external networks, including the internet and local network infrastructures. This isolation prevents unauthorized access, cyberattacks, and data corruption from external sources [7].

In practice, air-gapped systems often maintain a duplicate copy of critical data stored in an offline environment. Since these systems are not continuously connected to production networks, they provide a highly secure backup that remains protected from cyber threats such as malware or ransomware attacks.

Types of Air Gap Implementations

Air-gapped solutions can be implemented using various architectural approaches, including:

- Storage-based isolation mechanisms
- Backup-driven offline systems
- Object storage architectures with restricted connectivity

Each approach offers different levels of security and operational complexity. However, improper integration

with production systems may introduce risks such as unintended data transfer or system coupling.

Operational Considerations for Air-Gapped Systems

The effectiveness of an air-gapped environment depends not only on its design but also on its operational practices. Strict security measures must be implemented to maintain system integrity, including:

- Controlled physical access to systems
- Secure handling of data transfer mechanisms
- Encryption of stored data
- Limited and monitored connectivity during updates

Despite these precautions, air-gapped systems are not entirely immune to security threats. Advanced attack vectors, including electromagnetic or social engineering techniques, may still pose risks. Therefore, a combination of physical security, operational discipline, and architectural isolation is required to ensure maximum protection.

Integration of Dark Site and Air Gap Solutions

The combination of Dark Site and air-gapped architectures provides a comprehensive approach to business continuity. While Dark Sites ensure rapid and controlled communication during crises, air-gapped systems provide a secure and isolated environment for safeguarding critical data [8].

Together, these solutions enhance organizational resilience by ensuring that essential services, communication channels, and recovery resources remain available even under extreme failure conditions. This integrated approach forms the foundation for developing robust and secure Business Continuity and Disaster Recovery (BC/DR) systems.

The DARPA GAPS Challenge

Based on these known issues (even if many extreme hacks are contrived or laboratory based) the US research body DARPA has commenced a study and a competition around improving Air Gap solutions [9]. In their words:

Keeping a system completely disconnected from all means of information transfer is an unrealistic security tactic. Modern computing systems must be able to communicate with other systems, including those with different security requirements [9].

To put this in further context, Walter Weiss the DARPA program manager states that "…as cloud systems proliferate, most people still have some information that they want to physically track – not just entrust to the ether. Users should be able to trust their devices to keep their information private and isolated [9]". As a result of these concerns and needs, ARPA launched the Guaranteed Architecture for Physical Security (GAPS) program. The goal of GAPS is to develop hardware and software architectures that can provide physically provable guarantees around high-risk transactions, or where data moves between systems of different security levels. While this project may yield results in the future some best practices in this area are understood. This paper offers one such practical implementation of an Air Gapped Dark Site for consideration.

POC Experiment Approach

The objectives of the Proof of Concept (POC) project described here included:

- Developing a Dark Site platform design along with a supporting process
- Designing and building an Air Gap environment for key data elements residing on the Dark Site
- Scaling up the architecture to a Production footing; and 4) creating a plan for implementation

The details of the entire project are beyond the scope of this document. Instead focus will be given to the Dark Site approach and the design and build-out of the Air Gap platform [10].

Planning the Prototype Project

To organize the effort, a high-level plan resembling the below steps was developed. Over time this plan was refined and further detailed out. As a deeper understanding of the technical options emerged it was possible to improve the planning accuracy and approach.

- Conduct research on Dark Site and Air Gap methods and technologies. Define project needs statement
- Draw up initial Dark Site and Air Gap POC architecture based on early research
- Develop staff skill profile to populate the team and secure team members for the project
- Build and document Air Gap POC platform
- Definition of requirements for scale-up solution including data inclusion on Dark Site
- Develop multi-environment-based solution architecture
- Identify critical data and process for populating Dark Site safely
- Develop operational procedures and determine deployment location and operational teams
- Implement Dark Site (with Air Gap buffer)

Following this plan, the first step was to research state of the art methods and tools as well as to develop use cases for the application of a Dark Site and an Air Gapped solution. This research was conducted iteratively during the project, yet the early phase saw the bulk of the discovery work. Based on the knowledge gained from published industry experience, various internal discussions with leaders and architects with experience in related solutions, and reflecting on the intended goals of the platform, a direction was forged.

The Detailed Plan

To realize the objectives of the POC, the work was broadly separated into two threads:

- Design and development of the Dark Site, and
- Design and build-out of an experimental Air Gap platform

These two environments were to be integrated to allow content to flow from Production sites to the Dark Site and the Air Gapped system, however, the conceptual architectures could be pursued in a more or less decoupled fashion and then tied together. The approach to creating each of these solutions is detailed below.

Dark Site Development Approach

- The core element of the Dark Site centered on content and data. As such, the Business users were queried on required content for Dark Site hosting which was then prioritized
- The design and provisioning of the Dark Site included a computing environment, servers, networking, storage, and website infrastructure. The Dark Site also required a dedicated hosting provider separate from any current vendors to reduce simultaneous outage risk
- Develop and configure secure replication methods following low to high trust methods. This allows the population of the Dark Site from Production sources and enables testing
- Define operational procedures governing and enabling secure content provisioning and routine operations
- Create transition plan to activate Dark Site including a toggle method to initiate reconfiguration should a crisis condition be triggered

Air Gap Development Approach

- Develop design for the Air Gapped computing implementation (i.e., physical or logical Air Gap)
- Develop and demonstrate a POC for the selected Air Gap solution
- Define "low-side" and "high-side" data classification model and apply to Air Gapped systems content
- Implement the Air Gapped environment on standalone platform to create a physical separation
- Create procedures to operate and protect data migration to the Air Gapped environment

A Notional Architecture

In order to galvanize support for the proposed POC approach a vision of the solution environment was developed. This notional architecture (Figure 1) drew on the objectives of the project, the industry research into best practices for Dark Sites and Air Gap solutions, as well as local drivers such as existing environment and operational methods [11].

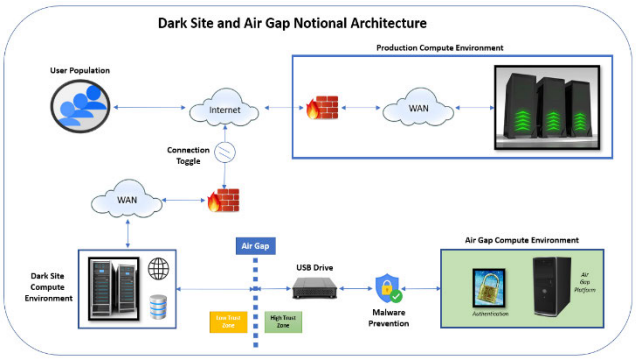

Figure 1: Notional Architecture for Dark Site and Air Gap Platforms

As can be seen in this architectural concept representation, users, including all stakeholders, interact with Production systems via the Internet or internal networks under standard operational modes. There is essentially no limit to the application or data types and hosting methods (e.g., Cloud or onsite datacenter) which can be supported. Should these facilities be degraded, or a critical communications requirement necessitates the use of the Dark Site, access to the environment can be initiated via a standby Internet connection and a straightforward DNS change to promote the site to a publicly visible state on the Internet. This design also allows for periodic replication of data to the segregated Dark Site in a controlled manner via this connection toggle.

The Air Gap protected compute environment, also shown in Figure 1, is buffered still further from Production and the Dark Site. The only data allowed into the Air Gapped environment has first been periodically replicated from Production to the Dark Site in advance. Furthermore, a logical and physical Air Gap exists in this model with zero network connectivity to any other devices. Data only moves from Production (least trust environment) to the Dark Site (intermediate trust environment) to the Air Gapped fenced environment (highest trust platform). The migration of data to the Air Gap environment is conducted manually and not via any network. Instead, data is transferred to portable USB drives and then connected to the Air Gapped server(s) located in a secure facility. All data is scanned for vulnerabilities prior to loading into the environment. This method can be modified or enhanced using other approaches which provide for equivalent or greater data separation and protection. However, the approach taken for this POC offers significant levels of isolation and data availability assurance enhancing BC and DR resiliency.

An important point regarding this architecture is that should any lower trust environment become corrupted it is possible to utilize the data in the Air Gapped platform to guide recovery efforts. While this platform is not a Disaster Recovery environment and would not support transactional processing it can act as a critical repository

for the retrieval of vital documents and data to be able to execute DR processes. Consider a condition where all systems are down and unreachable including the document repository where all your DR plans are stored. In such a case the Air Gapped platform can provide an essential recovery jumpstart location to rehydrate fundamental artifacts, data, and configurations [12].

Dark Web Content Plan

Typically, the content of a Dark Site would be restricted to an informational web presence to manage public communications during a crisis or Business Continuity event. However, such an environment can also serve as an expanded repository for other critical data files including DR plans themselves, contact lists, operational process documentation, last known configurations, and more. For this POC project, exactly such a heterogenous data schema was developed, initial data was populated, and a process defined to refresh this data periodically. In a Production model the Dark Site data can even be housed in separate Cloud environments sourced from diverse hosting vendors to enhance resiliency. As part of the POC activities a feasibility demonstration was paramount as was building in the hooks for the operational isolation from the Air Gapped environment. Following this success further Production rollouts can expand or extend the data schema as required as long as the Low Trust to High Trust protocols are maintained [13].

Selecting an Air Gap Demonstration Platform

The team analyzed several practical approaches to implementing either logical or physical air-gapped environments or both. A simple approach to create a Dark Site environment is to backup Production data, spool it off to physical tape, and finally ship that tape off-site to a 3rd party DR support vendor. This process in essence creates a logical and physical "Air Gap" which can be very effective and is relatively low cost. In a future phase more elaborate and secure Air Gapped solutions might be implemented and the utility and flexibility of the approach might evolve.

An alternative option would be to create a physically isolated Air Gapped environment with a logical connection to the Dark Site. In this scenario a periodic low to high trust network connection would be allowed where all content would be suspect and filtered. The goal of this solution is balancing the risk of exposing any data corruption to the Air Gapped environment with ease of administration. This architecture generally prevents the possibility of an intruder traversing the network from Production to Dark Site to the Air Gap environment as that end-to-end loop would simply not be available on a continuous basis. Moreover, the "hardwire" connecting the environments could be cut at any time [14].

The final approach considered, and in fact adopted, for the Air Gap POC was based on a physically separate node with no external network connections and no permanent data storage. In this extreme scenario, data is transported from Production to the Air Gap environment "manually" thereby eliminating any risk of cross-connection or network-to-network infiltration. Mock-up plans for scaling this approach were also drafted. Such a Production level approach can be achieved by locating the Air Gapped platform in a secure physical location and allowing for routinized data transfer off-network through defined procedures. This model was closest to what became the notional architecture introduced in Figure 1.

Platform Construction

The POC attempted to implement the essential computing attributes found in the notional architecture discussed earlier. The primary effort was focused on creating an Air Gap platform, defining operational procedures around it, and securely populating it with an initial set of data. The results of this POC were also meant to provide a template or implementation path for other teams and projects interested in achieving the same Business Continuity and DR resiliency support [15].

Specifically, the POC's goal was to prove out the concept of being able to operate a single standalone computer isolated from Production as well as any network so as to establish a physical and/or logical air gap to protect a selected set of static data following the conceptual architecture previously documented.

The POC machine was an HP EliteDesk 800 G2 TWR originally running Windows 10 provided from surplus inventory (inset right). The PC (Personal Computer) employed for this purpose was based on a 64 bit Intel® Core™ i7-6700 CPU @ 3.40GHz processor. In addition to the primary POC device a matching HP tower PC was used as the pseudo-Production environment. Also, several supporting peripherals were purchsed to condut the POC activity. These included:

- 1 each BYEASY USB Hub, providing a 4 Port USB 3.0 Hub
- 2 each SanDisk Cruzer Glide CZ60 256GB USB 2.0 Flash Drives
- 1 each Micro Center SuperSpeed 2-Pack 16GB USB 3.0 Flash Drive, Gum Size Memory Stick, Thumb Drive Data Storage Jump Drive

The total price of these additional items totaled $89.51.

Tails OS Installation

To realize a secure environment the Tails Operating System was selected for the Air Gap platform. Tails is a compact Linux distribution which is designed to run from a USB stick. It is run in a transient and "amnesiac" mode leaving no trace behind (Klosowski, T., & Murphy, D., 2020). It also runs in stealth mode on the network masking its presence or running without any network requirements at all. This makes it ideal for an Air Gap platform OS. To run Windows or even other Linux platforms network connectivity is assumed and simply booting the machine becomes problematic without a

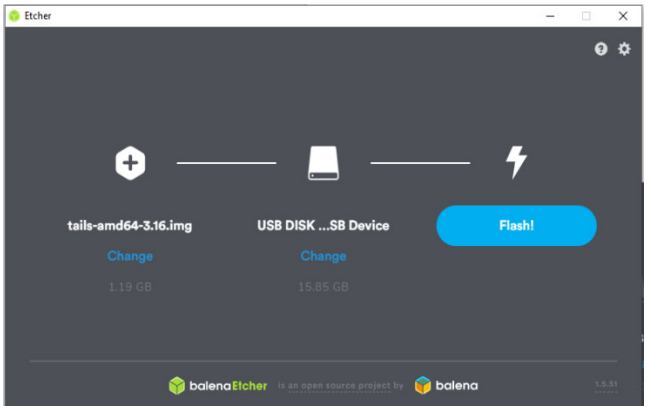

Figure 2: Tails OS Installation

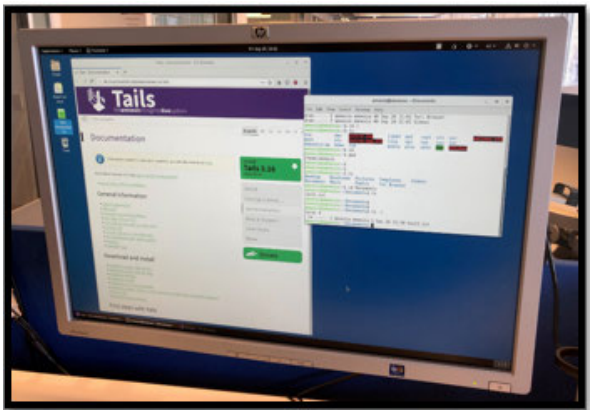

Figure 3: Tails OS and GUI Environment

network attached. Using Tails, the Air Gap machine automatically inherits a level of logical separation from other computing environments as it simply is not attached to any network nor is it visible to any other computing device on the network.

The steps to downloading and installing Tails are all provided on the Tails homepage (https://tails.boum.org/). The image applied in this case was the AMD64 bit 3.16 version. The process of installing the OS as bootable on a 16GB USB 3.0 stick required about 45 minutes to complete (Figure 2).

Initial Platform Configurations

Once the Tails boot disk was prepared the POC platform required some configuration changes to start from the Tails USB stick. Importantly, these changes included disabling the "Fast Boot", "CD Boot", and "Network Boot" options on the PC. This resulted in only allowing "Windows Boot" or "USB Boot" to operate. Finally, USB boot needed to be set as the primary boot source. The instructions for this were provided by HP Support documentation [14].

Upon initial attempt the boot from the Tails USB drive did not work. The source of the problem was determined to be that "Secure Boot" in the BIOS was enabled [13]. Additionally, BitLocker encryption provided one final hurdle to the boot process. By disabling these features, the boot process was able to proceed. To boot from the Tails USB the machine was powered on while hitting F9. Selecting "boot from file" then allows the system to initialize using the EFI BootX64 image. In the startup menu there are some additional configuration choices to be made around the root password and network options. In this area all network connections can be disabled.

Tails provides a full Linux environment including a help system, man pages, a browser, graphical tools, folder manager, and more (Figure 3). Since Tails runs in "amnesia" mode this means that it does not leave any trace behind after it terminates. That is, there are no persistent files or configuration traces remaining on the machine once the OS is shutdown. However, Tails does allow for a persistent storage option if the administrator chooses to create one.

RESULTS AND DISCUSSION

The essential purpose of the Air Gap machine was to be able to receive, manage, and retrieve off-line data in a secure non-networked environment. Operationally this followed the process and infrastructure model shown in Figure 4. Based on the configuration described above the POC machine provided the capability of being booted without any logical network connectivity using a single dynamic command at boot time. Also, during the test period the machine was essentially invisible to other devices on the LAN, WAN, or Internet. Thus, the machine was in effect already protected with a virtual Air Gap as it was not detectable by other computers or network surveillance tools.

Several fundamental tests were run to demonstrate the efficacy of the Air Gapped platform. These included creating files on the Air Gap machine and saving them locally. As per design, these files were not persistent and were not found after reboot. Another key test was the transfer of sample Dark Site data files from the pseudo-Production server to the Air Gap server via an external 256 GB USB Flash Drive. This was conducted over what is known as "sneaker net" as depicted in Figure 4 [15]. The actual hardware used for this approach was the pseudo-Production server, the Air Gap PC itself and the two USB drives, one containing the Tails OS and the other the test data shuttle as shown in Figure 5. Once the sample data from the pseudo- Production site was copied to the Tails based Air Gap machine it could be scanned, stored, and then manipulated or further copied to alternative external storage or target servers where users would be able to then access the protected data.

TOR and Network Security

While running Tails in a network connected state the OS masks itself by bouncing TCP/IP traffic through intermediaries on the Internet [16]. This is accomplished via TOR (Onion Router). Thus, as part of the POC when pinging the test Air Gap machine from the pseudo-Production

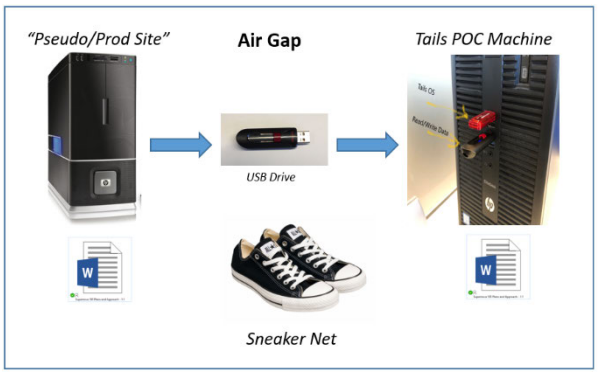

Figure 4: Data Transfer to Air Gap: High Level Process

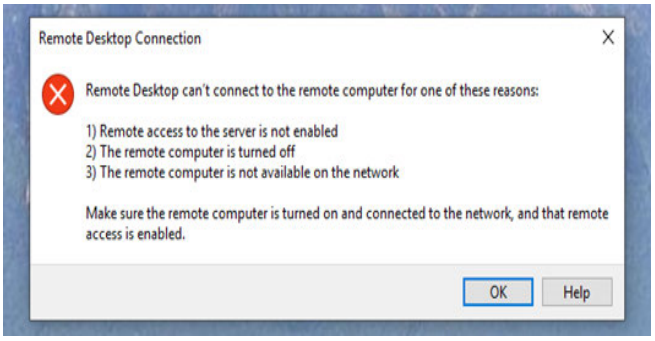

Figure 6: RDP Connection Refused While Tails is up and Running on the Network

Figure 5: Air Gap boot disk and Read/Write Sneaker Net Data Transfer Flash Drive

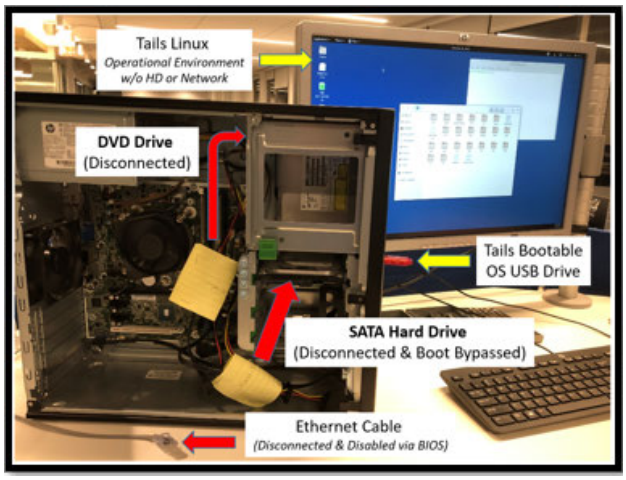

Figure 7: Reconfigured Air Gap machine internals with Operable Tails Environment

machine on the same LAN segment the POC machine was not discoverable. One confirming test result was an attempt to reach the Air Gapped machine from the pseudo-Production machine which was physically co-located and on the same LAN. Both ping and RDP attempts failed (Figure 6). At the same time, the Air Gapped machine had full access to all devices on the network and could ping the pseudo-Production machine successfully. Helpfully, at boot up time, Tails can be toggled into fully detached mode so as to run without any network dependency. It can alternatively boot into a connected mode if an Ethernet interface is installed and detected.

Hardware Modification and Testing

The initial system tests were conducted with the Tails based Air Gap machine connected to the network but with network access disabled. The test environment utilized a standard PC hardware configuration. To advance the testing the next phase included physically removing the Ethernet card and also disabling internal storage. Each hardware change was made sequentially with a boot attempt between each of the singular changes to confirm system health progressively. This followed the age-old Proven technique of changing only one thing at a time so as not to confuse the results. Also, internal cabling was labeled to assist in debugging or reversion to prior state (Figure 7).

The initial boot attempt failed following removal of the hard drive. The error message received was "No OS Found". Upon investigation it was determined that the boot sequence did not bypass the SATA drive to proceed to the USB drive. The solution was to modify the BIOS feature called "Embedded LAN Controller". By disabling the "Wake on LAN: Boot to LAN" the POC Air Gap machine now booted without any network connection possible. This modification path also required that "Internal Speakers" and "Audio Alerts during boots" to be disabled. Following this series of changes, once started, the environment could no longer resolve the network. To confirm this, no IP address was assigned to the machine as reported by ipconfig, and a ping test reported "Temporary failure in name resolution". Also, IP identification failed via curl ifconfig.me which responded with "could not resolve host".

Data Testing Across the Physical Air Gap

Following the successful booting of the newly reconfigured Air Gap platform, data creation, transfer, and

modification tests were repeated. First, the only allowable boot option for the machine was through the Tails USB media. Also, as noted, the machine could not electronically reach the network nor could any device on the network reach across the Air Gap to the platform as no physical network connection existed. However, within the machine, a fully operational OS was running which could manipulate any on-board files or files accessible via external hard drives through standard Linux file system commands. As a result, the hardware reconfiguration and creation of a truly standalone server demonstrated that the physical Air Gap was present and could continue to support data file operations in a fully isolated mode.

Scale-up and Usage Scenarios

With the POC completed successfully and its objectives proven, attention turned to scaling-up the environment and defining usage scenarios and processes for the Dark Site and Air Gapped environment. Again, these followed two but related threads. The first focused on solution development for an isolated and prepopulated Dark Site in a Cloud hosted environment. The second thread focused on how to Productionize the concept of the Air Gap environment as demonstrated by the POC. The former followed a fairly typical Cloud computing architecture but the later was by definition more unconventional.

For the Dark Site a computing architecture was defined, and several selectable operational modes were established including normal operations, a standby state connected to the network, and a fully disconnected network state. Additionally, for the Air Gap solution, multiple Production approaches were modeled to allow for the essential elements of the POC to be replicated in a supportable and large-scale mode by an IT Operations team. Each of these problem domains were now guided by the lessons of the POC and a newly detailed requirements statement including usage scenarios and process flows to aid in design, maintenance, and operations.

Observations and Summary

The POC described here was able to prove out a number of key points in adding resiliency to BC/DR environments. These learnings also point the way towards full-scale Production build-outs of both a Dark Site and an Air Gap implementation. The data approach for the Dark Site and its architecture as well as the construction and proving of an essential Air Gap platform have been completed. Notable steps in conducting the POC included researching and selecting appropriate technologies, developing a concept architecture to fit the needs of the POC, configuring the POC environment including a secure Operating System (Tails), demonstrating network security (or lack thereof) using TOR, and modifying the platform to create both a logical and physical Air Gap environment. Various tests were conducted to establish the capabilities of moving and manipulating data across environments. Throughout each step detailed POC approach logs were maintained to inform the deployment and scale-up approach. The overall result of the POC was to validate both the Dark Site and Air Gap architecture as proposed. To take this work further, full-scale deployment solutions would be required and would need to consider operations, system administration, Cybersecurity, file encryption, data definition and propagation, additional use cases, physical security of the Air Gap platform, and more. As it is, the POC was documented, presented to management, and used for planning next steps. This experience can also be useful for those interested in Dark Sites and Air Gap solutions in general or when attempting to construct such environments to support Crisis Management, Business Continuity, and Disaster Recovery more favorably.

CONCLUSIONS

The project as described can provide a template for others attempting to understand how a Dark Site enhanced by an Air Gap capability can help fill the need of providing added system resources and resiliency for Crisis Management, Business Continuity, and Disaster Recovery. This POC demonstrates successfully how to design, build, and test such environments providing independent and standby computing capabilities for customer communication, internal coordination, and redundant data protection. With the Dark Site, critical data can be assured to be ready at a moment's notice. The Air Gap as shown here creates a facility to isolate selected data from harm and enables access to or repopulation of such data if required. This study mentions the challenges of administering such specialized sites. Yet the benefits to operational resiliency in a BC or DR scenario by adopting a few customized administrative procedures to support such platforms can be highly valuable.

REFERENCES

[1] Agudelo, Wendy Bulawa. "Dark sites: What are they?" *Axiapr*, November 2015, https://www.axiapr.com/blog/dark-sites-what-are-they.

[2] Beerworth, Robert. "What is a 'dark site' and why would you need one?" *WilliamBlog*, June 2014, https://www.wiliam.com.au/wiliam-blog/what-is-a-dark-website.

[3] Lloyd, Tim. "Dark sites in crisis communication: six reasons to consider." *Social Simulator*, March 2015, https://socialsimulator.com/dark-sites-fad-fundamental/.

[4] Johnson, Derek B. "Solving the air-gap dilemma." *DARPA*, January 2019, https://gcn.com/articles/2019/01/08/darpa-air-gap.aspx.

[5] Livens, Jay. "What is an air gap and why does it matter?" *Actifio Blog*, May 2018, https://www.actifio.com/company/blog/post/what-is-an-air-gap-and-why-does-it-matter/.

[6] Nohe, Patrick. "What is an air gapped computer? everything you need to know about air gapped systems and their security." *HashedOut*, March 2018, https://www.thesslstore.com/blog/air-gapped-computer/.

[7] Schneier, Bruce. "Air gaps." *Schneier on Security*, October 2013, https://www.schneier.com/blog/archives/2013/10/air_gaps.html.

[8] Fernandez, Aaron. "Extreme security measures for the extra paranoid." *Wired*, December 2017, https://www.wired.com/story/extreme-security-measures/.

[9] Dunn, John E. "What comes after air gaps? DARPA asks world for ideas." *Naked Security by Sophos*, February 2019, https://nakedsecurity.sophos.com/2019/02/11/what-comes-after-air-gaps-darpa-asks-world-for-ideas/.

[10] Mudgil, Pooja *et al.* "Air gap penetration." *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 2019, pp. 437–442. https://doi.org/10.32628/CSEIT1952109

[11] DARPA. "DARPA explores new computing architectures to deliver verifiable data assurances." *Defense Advanced Research Projects Agency*, January 2019, https://www.darpa.mil/news-events/2019-01-16.

[12] Klosowski, Thorin *et al.* "What is tor and why should i use it?" *Lifehacker*, December 2020.

[13] Parsons, Rob. "How to disable UEFI secure boot in windows 10 computer." *AppGeeker*, April 2022.

[14] HP Support. "HP EliteDesk 800 Desktop PC Series – BIOS Setup." *HP Customer Support Knowledge Base*, 2022, https://support.hp.com/us-en/document/c03840403.

[15] Rist, Oliver. "Hack tales: Air-gap networking for the price of a pair of sneakers." *InfoWorld*, May 2006, https://www.infoworld.com/article/2655459/hack-tales--air-gap-networking-for-the-price-of-a-pair-of-sneakers.html.

[16] Tiwari, Aditya. "Tor explained: What is tor? How Does It Work? Is It Illegal?" *Fossbytes*, February 2021.