ESP-JETA
ESP Journal of Engineering & Technology Advancements
ISSN: 2583-2646 / Volume 5 Issue 3 July 2025 / Page No: 43-53
Paper Id: JETA-V5I3P107 / Doi: 10.56472/25832646/JETA-V5I3P107

Original Article

Digital Systems Security: Case Study of an IT Consulting firm

Upendra Kanuru[1], Odiase Irumudomon[2]
[1]*Software Engineer, Texas, USA*
[2]*Sr Incident Response Analyst & Professor, Texas, USA*

Received Date: 20 April 2025 Revised Date: 11 June 2025 Accepted Date: 13 July 2025

Abstract: *This case study looks at Adler Consulting's digital systems security architecture in depth and makes suggestions for how to improve it. Adler Consulting is a well-known organisation that provides IT solutions all around the world. Adler Consulting has more than 20,000 workers and brings in more than $1 billion a year. Because of this, they need to have strong security to deal with new cyber dangers that come up. The study goes into detail on the organization's existing security setup, which includes SIEM/SEM, WAF, and multi-cloud environments. It also points out the most relevant flaws and threats. The plan for making things better involves hiring security engineers who are dedicated to the task and putting up a modern Security Operations Centre (SOC) with a Chief Information Security Officer (CISO) in charge. Important policy ideas have been made around Acceptable Use, Security Awareness and Training, Change Management, Password Management, Remote Access, and Third-Party involvement. The paper also gives ideas for making the decentralised network design stronger, such using Intrusion Detection/Prevention Systems (IDS/IDPS) and always keeping an eye on how well the network is working. Finally, it explains how to have solid procedures for Incident Response and Business Continuity Planning so that the organisation is strong and security incidents don't cause too much trouble.*

Keywords: *Digital Systems Security, Enterprise Security Plan, Enterprise Security Strategy Framework, Risk Management, Security Policies, Network Security, Incident Response, Business Continuity Planning, Cloud Security, SIEM, SOC, Cyber Threat, and more.*

I. INTRODUCTION

Adler Consulting is an IT Solutions company that says it is based in the U.S. but works with customers all around the world. The company started in 2030 and currently has more than 20,000 direct and indirect employees that serve businesses in several industries with their technology needs. Adler Consulting is a top tech solutions firm that cares a lot about security. They leverage cloud services from WS, Microsoft Azure, and Google Cloud, as well as SIEM/SEM and WAF.

The company has sold more than $1 billion worth of goods and wants to improve its security system so that it can better service its many customers. The corporation will directly pay for recruiting the best security engineers to help it reach its goals and secure its most important asset: its information assets. The company's future plans include building a modern Security Operations Centre that will be managed by a well-known CISO who will report directly to the CEO. The CISO will need to hire more than simply Insider Threat Specialists. They will need to hire professional Incident Responders, Pen Testers, Sr Cybersecurity Analysts, Security Engineers, Cloud Architects, Cyber Threat Intelligence Analysts, Detection Engineers, and more.

This group will be responsible for protecting the company's most important data and network infrastructure. They will also protect the business from assaults from both inside and outside.

II. ENTERPRISE SECURITY PLAN

A. Organizational Asset Description

An asset is better stated as something that gives a person, business, or country economic value and gives the holder power to make money in the future. The balance sheet demonstrates that the company can buy or make assets that will make it more valuable or help it run more smoothly. If a patent or manufacturing equipment may help a business make money, save money, or increase sales in the future, it is an asset [10]. He also adds that a company's assets are its money and the knowledge that only it can get to. This definition explains that a corporation should have complete ownership of its assets as of the date of the financial statements for them to be current. An economic resource is anything that is hard to find and can produce money by changing the quantity of money that comes in or goes out. There are several types of assets, including short-term (or current) assets, physical assets, financial investments, and intangible assets.

Adler Consulting has both physical and financial assets that are distributed out throughout the organisation. This includes all the crucial things that need to be kept safe, like PCs, laptops, network printers, network servers, financial records, and more. The business employs more than 5,752 employees at all of its sites and produces more than $6.26 billion

in revenue. Based on these numbers, the organisation likely has around 5,500 computers, including laptops, desktops, printers, and servers. The Phoenix group reported that they made £4,706 million in the second half of 2020 and had £334.33 billion in financial assets. There is a definite approach that the personnel should protect all of these assets.

a) Asset's Prioritization

The first step in establishing an Enterprise security plan for assets is to undertake an asset criticality evaluation, which is also known as Asset Criticality and Prioritisation (ACAP). This will assist you find out which assets are the most important. The ACAP method needs to be as complete as feasible because it is needed for the corporate security strategy to succeed. One asset deserves more protection than another [27]. The first stage in the ACAP method is to give each asset a score based on how vital it is to the others. These rankings show where the finest security plans should be used and where the worst ones shouldn't be used. The phoenix group holdings will put the following assets at the top of their list:

- Employees: The most crucial thing in a business will be given the letter "E."
- The value "PA" will be ascribed to land, buildings, machinery, and tools.
- "CA" stands for "current assets," which are things like stocks, cash reserves, marketable securities, and prepaid debts.
- The word "NCA" will be used to describe non-current assets, such as tangible fixed assets, goodwill, and long-term investments.
- The value of fixed assets accounts receivable will be "OA" for operational assets.

b) Environmental Risks

The UK is home to Phoenix Group Holdings' main office. This group might have to deal with difficulties in the environment, like toxic air, noise pollution, and the harmful effects of climate change. To protect employees and other company property, a business security plan must be put in place to deal with these threats. A string of devastating wildfires hit the UK in June 2018. The worst and longest-lasting fires were in England, where some flames lasted for more than a month. In 2019, some parts of the Midlands, Central, and Northern England recorded the wettest year ever.

c) Tools and Methodology for Risk Assessment

Risk assessment is the process of detecting and analysing possible future events that could hurt a business, as well as how likely each category of risk is and what it could do. Businesses do risk assessments in several areas, including finance and security. Cybersecurity risk assessments solely look at digital assets and data [17].

Quantitative and qualitative risk assessments are the two most common types. Statistics are used to figure out how risky something is. A team does a quantitative risk assessment by looking at and figuring out risk using data that can be assessed. A qualitative risk assessment is more concerned with what would happen on a daily basis if one of the hazards on your list came true. We did the risk evaluation using a qualitative approach. The risk matrix, failure modes, decision tree, and bowtie model are all employed in the risk assessment.

d) Technologies to Mitigate Environmental Risks

The quick reaction water-gate can aid with flooding. This quick reaction device is made of PVC and can be put up right immediately. It holds in place because of the pressure of the water pouring towards it. This means that they are using the water from the flood to build their dam. The device is compact and may be put up quickly by one person, depending on how big it is. This is because it is made of PVC, which is light, and it inflates when water pressure is applied. The water-gate produces a dam that goes all the way around a building. It can also be fully recycled, which is ideal for people who live in areas that are likely to flood [22].

Scrubbers can help you get rid of harmful air. Scrubbers are equipment that assist keep the air clean by getting rid of harmful gases including sulphur dioxide, chlorine, hydrogen sulphide, and hydrogen chloride from industrial emissions. Scrubbers assist keep neighbourhoods surrounding power plants, water treatment plants, and other industrial centres clean by keeping dangerous air pollutants out. Also, businesses and factories may keep functioning without making the air more filthy because these gadgets don't stop the manufacturing process.

B. Policy for Security

It's not only up to people or departments to keep sensitive information safe; the whole company is responsible for doing so. For this reason, the highest-ranking officials in charge of securing the institution's benefits must make sure that a solid and comprehensive security plan is put in place and followed by everyone in the company. Policies are a fantastic approach to start solving problems, but they don't always work all the way. If they aren't made and carried out correctly, they can sometimes make situations worse. They do, however, establish the standard for everything that happens in the organisation [5]. A security policy is a set of clear and simple rules, regulations, and procedures that tell people who can use an organization's infrastructure. According to Chapple (2016), a robust policy protects all the data about a corporation. As we talked about in phase 1 of this project, the results of a risk assessment must be the basis for a security policy that can be

defended. A risk assessment helps policymakers see clearly how safe their business has to be [13]. Planning is the basis of a strong security strategy. It directs activity and, ideally, becomes a part of the whole organization's culture. A good security policy makes a short set of goals that assist employees execute their tasks every day. It takes into account things like legal and contractual duties, regulatory concerns, and other factors.

One goal of a good security plan is to make individuals less dependent on the system [20]. This may look like giving up, but it keeps both the workers and the business safe. Before security can be useful, employees need to be informed on their roles, duties, and what the business expects of them [7].

It is necessary for Phoenix Group Holdings personnel to have written notification of a variety of key security risks. First and foremost, they should know that someone will be keeping an eye on how they use company resources. This openness is vital so that workers know the organisation is serious about making the workplace safe and holding people accountable. It should be apparent that performance appraisals will now include a section on security. This change makes it apparent how crucial it is for everyone to be accountable and for all employees to take security seriously as part of their job.

The group should also stress that letting people use resources without enough responsibility is a recipe for disaster. Workers should realise that the company owns all of its assets, like computers and other gadgets, and that these assets are only for work. Employees should be aware that any data that is stored on or communicated through the company's technology is not private. This expectation makes it clear that the business has the right to watch over and protect its own property and information.

Finally, employees should have to sign a Security Agreement to show that they understand and agree to the restrictions. This document is an official record of their duties and shows that they are serious about following the organization's security policies. By signing, workers agree to respect the regulations of the company and prove that they understand them.

a) Acceptable Use Policy (AUP)

Employees need to know what they need to do to use business computers and other IT systems. This policy also tells you how to use email, the internet, and data correctly, as well as what you should and shouldn't do while you're managing sensitive data. The guideline on what employees can and can't do will include a list of vital items that everyone must do. People need to be attentive and responsible when they use all of the organization's IT resources, first and foremost. These resources need to be respected and kept in good working order for the business to run smoothly.

The policy also makes it clear that you can't use the organization's IT resources for your own gain. You should only use all of your equipment and systems for business purposes. Employees need to let the company's engineers know about any faults or malfunctions very away so that repairs or other measures can be made right away. Employees need to tell the company's engineers right soon if something goes wrong or there is a technical problem so that repairs or other actions can be made right away. This keeps the work flow going smoothly and makes sure that IT resources are safe.

Lastly, the policy makes it clear that employees are not allowed to access data for any reason other than their official duties. Employees need to be aware that these kinds of actions are against the rules and could get them in trouble. All of these standards work together to produce a safe, productive, and morally responsible workplace. We'll keep an eye on this policy by inspecting the IT assets on a regular basis. Anyone who breaks it will have to pay a big fine, which will come out of their income or benefits. Every two years, the IT officer will look over the policy.

b) Policy for Training and Raising Security Awareness

In order for a company's IT security plan to operate, it must make sure that its employees are well-trained [18]. The major goal of this policy is to make sure that everyone who uses the system understands how what they do potentially influence the organization's privacy and security. The purpose of the policy is to keep staff informed so that they are more responsible and alert. This will reduce the risk of security breaches and protect crucial business information. All personnel will have to go through required security awareness training to help reach this aim. The objective of this training is to teach employees how to conduct their jobs well while simultaneously keeping company data private, safe, and accessible.

Also, every month all employees will have to go to a lecture about being aware. Some of the main topics that will be covered in these talks are how to take care of workstations, how to keep your computer safe, and how to obey the regulations for email and internet access. The company wants all of its employees to be aware of security issues and to keep up good practices through frequent training. There will be a strict attendance list for every training session, and everyone who doesn't show up will have to pay a fine. Every three months, the person in charge of training employees will look at it.

c) Policy for Dealing with Change

This policy tells you how to change the way the organisation does IT and security. The goal of this policy is to make sure that all modifications are logged, watched, and given the green light. There are a lot of reasons why people often upgrade or change systems and software. Updates or adjustments could pose problems if there isn't a plan for managing them. This policy is aimed to decrease the chances of system failures and interruptions while making sure that the needs of the organisation are always met. Setting clear regulations is the policy's way of keeping IT resources steady and dependable. This will make sure that the business can keep running without any problems.

To do this, all changes to IT must be made in a planned and organised fashion. This organised way of doing things decreases the likelihood of mistakes and makes sure that updates and changes happen fast and without issues. Users of Phoenix business computers are not authorised to install or update new operating systems or application software. This regulation is there to protect the organization's IT infrastructure and bar anyone from making changes that could make the system less safe or less effective.

Users can alter their personal settings in permitted software packages, but the rules for change control will be carefully enforced. It's permissible to make changes like changing the fonts in a word processor or arranging email message folders in the right order. These concessions help workers make their workstations more comfortable without putting the organization's IT infrastructure at risk of being less secure or stable. We will keep an eye on this policy by regularly checking the operating system. If someone smashes it, they will have to buy a new computer. The chief of IT operations will check the policy every month.

d) Rules for Making and Keeping Passwords

This policy is aimed to teach employees how crucial it is to develop and retain strong, unique passwords. It shows you how to set up passwords and highlights how important it is to keep them safe at all times. Following these standards will help keep the company's digital assets safe and decrease the risk of unauthorised access. Employees are particularly crucial in this. People who use the service must choose passwords that are hard for others to guess. All fixed passwords must be at least eight characters long, and systems should automatically enforce this minimum requirement whenever they can. Users should also make their passwords harder to guess and safer by using both letters and numbers.

Once you've chosen a password, you can't use it again or recycle it. If you use the same password over and over again, this keeps security flaws from building up. Users must change their password the first time they use it, and systems that allow it must change their passwords every 120 days. If users fear someone else could know their password, they should update it straight away.

Everyone has to keep their passwords safe. No one, not even managers, support technicians, or coworkers, is authorised to give out passwords to anybody else. If you break this rule, you put critical information at risk and make the organization's security weaker. A centralised digital check will be utilised to actively watch the rule and discover anyone who break it. If you break these password guidelines, you won't be able to use IT resources for seven business days. Every three months, the IT officer will assess to see how well this monitoring and enforcement system is operating and make any necessary changes to deal with new security issues as they arise.

e) Rules for Accessing Remotely

More and more individuals are working from home, which makes business owners more nervous about how safe their data is when people access it from outside the workplace. This policy is aimed to make it less likely that the firm will have to pay for any damage that occurred because someone uses its assets without permission or in an illegal way. Setting clear expectations and procedures in the policy protects both company resources and employees from possible legal and financial concerns. Remote workers can only use their remote access for business objectives that are lawful and approved. They can't do anything against the law, and they can't let those who aren't supposed to use their work gear. This makes sure that company property is always safe and used the right way.

It is really hard to get to work computers from outside the workplace. People will only be able to access the internet from outside the office if they can establish that they really need to. This strategy makes it less likely that there will be security vulnerabilities, which helps keep the organization's IT infrastructure safe. Users should also take steps to protect the equipment used in information systems. If equipment isn't housed in a closed environment, you need to use anti-theft methods like locking wires. These actions make it less likely that someone will take or use sensitive equipment without permission.

Lastly, you shouldn't save passwords, user IDs, or any other information that lets you get into a computer on a portable or remote computer. If you don't keep this kind of information protected, it can be easy for someone to get to it

without permission. This could put both personal and corporate data at risk. Following these standards can help employees keep the organization's information and assets safe. The IT officer will make sure that this policy is followed, and anyone who breaks it will lose their employment. Every six months, the policy will also be checked anew.

f) Third-Party Policy

People who are not part of the organisation but can use the system should sign contracts that say they will keep the organization's information private and respect it. Security tools will keep an eye on this policy, and anyone who breaks it will be dealt with correctly.

C. Net Work Security

The organization's network is a well-planned, decentralised peer-to-peer network. Peer-to-peer (P2P) is a set of software that lets computers share resources directly with each other across a network [6]. A peer-to-peer (P2P) system intends to collect all the resources that are out there on the Internet and make them available to everyone. People on the Internet utilise P2P file sharing to distribute and receive information in a new way. They are more dependable, scalable, and fault-tolerant than most client-server systems, which makes resources easier to get to [23].

P2P networks can be either centralised or decentralised, even if they don't have a central server. In a decentralised paradigm, resources can be found and moved anywhere [8]. There are two kinds of decentralised P2P topologies: structured and unstructured. In structured networks, there are a lot of ways that the way things are laid out and the network design are limited. Network topologies don't affect how material is shared in unstructured P2P networks, on the other hand. According to Kent (2008), unstructured P2P networks usually operate better than organised ones when there is a lot going on.

They do, however, need to know how to search well and cope with challenges like spreading bogus content, getting something for nothing, covering up bad things, and search that doesn't scale [28]. You can't tell what a peer would upload to a network because P2P programs are open and anonymous. Bad peers often use these networks to spread bad software like malware or viruses and toxic content [25].

a) Network Design

The network of the Organisation is shaped like a star. A star topology has a device in the middle that connects everything. The physical topology of the network connects all of its hosts to the main connecting device using a network cable. Soni et al. (2019) argue that it might work as a ring or bus topology due of the way the protocols work. The central connecting device will deliver the data whenever one host wants to send it to another host. The main connected device then copies the data and sends it to the proper host.

The networking standard we use tells a central connecting device what to do. Some devices will copy that data and send it to all hosts (Hub) [23]. Next, each host will check the data to see if it is valuable to them. If the packet isn't meant for that host, it will be thrown away. The information within the box can only be read by the person who is supposed to recieve it. Other technologies for networking will work differently. Switch will remember which host is linked to which port on the central device. The main device knows which host is linked to which port, so the data will travel to the proper receiver [29].

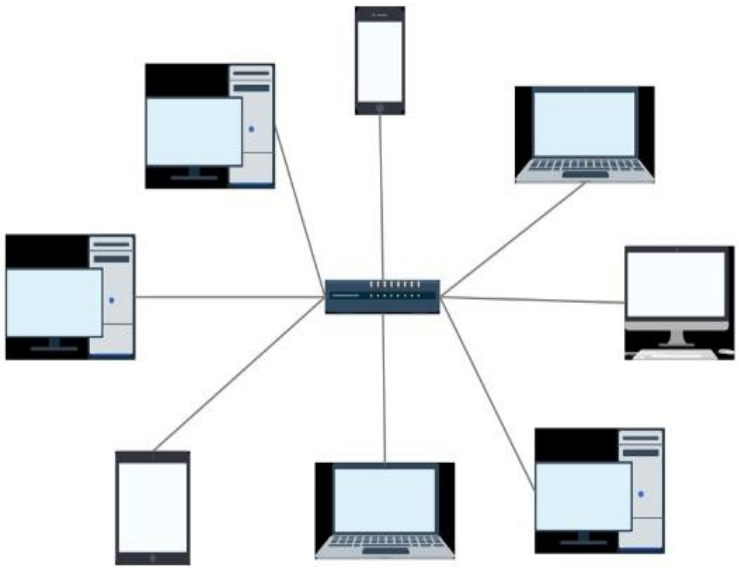

Figure 1 : The Star Network Topology (Wikipedia)

b) Allowed Protocol

The Dynamic Host Configuration Protocol (DHCP) lets each machine on a TCP/IP network receive an IP address, which is a number that tells the network who it is. On the other hand, it would take a long time and be a pain to give hundreds of workstations IP addresses by hand [25]. One risk of this is that someone could manually issue IP addresses and end up with duplicate ones, subnet masks that are erroneous, or TCP/IP setup parameters that are improper. The Dynamic Host Configuration Protocol (DHCP) automates the following procedures to make it easier for network administrators to handle IP addresses in TCP/IP networks [8]: Before DHCP, setting up TCP/IP was primarily a manual job. Bellovin (2009) states that one main problem with giving hundreds of devices their own IP addresses by hand is that they might not be unique. Every computer on a TCP/IP network needs its own IP address so that it may be uniquely identified.

Soni (2019), on the other hand, says that the Bootstrap Protocol (BOOTP) is what the DHCP protocol came from. BOOTP enables clients start up from the network instead of the hard drive. After that, the DHCP server gives DHCP clients IP addresses from a pool of IP addresses. The DHCP server and client normally send each other four messages during the negotiation process. The DHCP server and the client each send two messages.

c) How to Set Up and Use Routers

Routers tell different types of networks to maintain the best transmission channels open on their highways, which is like enforcing network traffic. If the router is the heart of the network, then the network should be the heart of the router. There was a constant stream of new types of routers that came out to fulfil the needs of clients of various sizes [12]. The group connects over a WIFI hotspot. A WiFi hotspot is a wireless local area network (WLAN) that connects to the Internet through a router [3]. WiFi technology lets any electrical device that needs the internet connect to hotspots and share data wirelessly.

d) Firewalls

Firewalls are security tools that keep an eye on network traffic and "curate" it according to a set of rules. They keep the internet from getting into your private internal network. Dahiya et al. (2018) say that both software and hardware can be used as firewalls and other ways to protect a network. Before letting any messages into the private network, the firewall verifies them all [30].

- A hardware firewall is a distinct piece of equipment. Every firewall has at least four ports that it utilises to talk to other devices on the network. Larger businesses may use more expensive firewalls with more ports and better security features[6].
- A firewall is a set of programs that are installed on a computer to protect data. You can alter the settings to help you set up a firewall that works best for you. The program keeps track of every packet that moves to and from the internet [23].

e) Anti-Virus

An antivirus tool can discover and remove malware and other programs that could be bad for your computer. Before, antivirus software could only stop viruses. Now, it can also stop worms, trojans, ransomware, and spyware, among other things [31].

f) Tools for Filtering Content

Content filtering devices block online information that could be harmful or rude. This includes emails, spam that comes in a lot, and even online sites. As the name suggests, these devices evaluate web material for safety by running it through a list of banned words [12]. Some CFDs can also recall and alert you about spam sites and email addresses that are well-known before you click on them. If someone tries to read unverified or perhaps dangerous content on these devices, they get a message that says "Access Denied." This network security device's default setting prohibits pornographic or hostile content [30]. A firm can also stop spam and other unwanted mail from trying to sell things. The security tools above operate well, but an intrusion detection system will make them work even better.

g) Systems that Find Invasions

Intrusion Detection Systems, or IDS, are tools that keep an eye on a network for undesirable behaviour, log in, and try to stop it if they can [8]. At the very least, an IDS will tell you what's going on on the company's network. The business might use these reports to make the network safer. Active intrusion detection systems (IDPs) sound alarms, drop harmful network packets, and restart the network channel connection to keep the network from blocking all future, legal network traffic [29]. We will use the SolarWinds Network Performance Monitor, which is the best network monitoring system on the market, to keep an eye on the security device. It uses SNMP to check on the condition of network devices. This monitoring tool has an auto-discovery capability that makes a map of the network's topology and a list of its assets automatically.

Figure 2 shows the current network diagram, and Figure 3 shows a proposed network that has an Active Intrusion Detection System for network security that connects to each network. The system will be watched by SolarWinds Network Performance Monitor. This software is great for that.

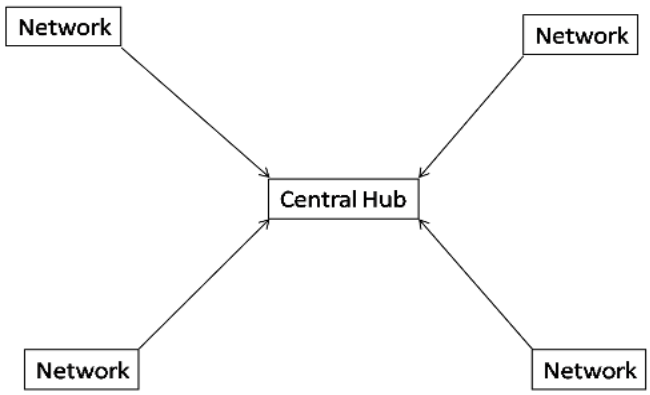

Figure 2 : Existing Network Diagram

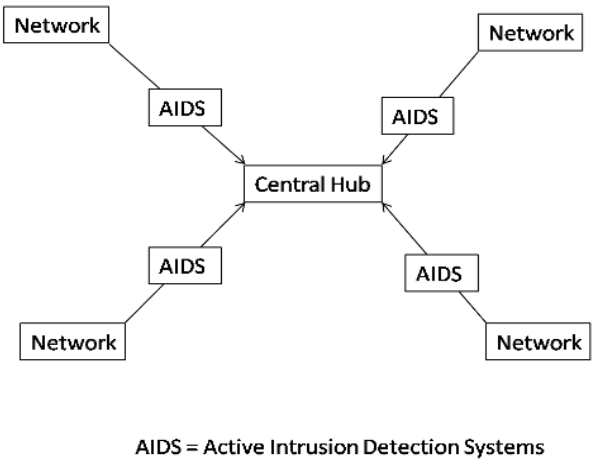

Figure 3 : Proposed Network Diagram

D. Plan for Business Continuity, Incident Response, and Disaster Recovery

Arean (2013) argued that both natural disasters (such floods, earthquakes, and wildfires) and man-made disasters (like riots, terrorist attacks, and war) can mess up how businesses work. Theft and equipment failures, which happen all the time, can make it hard for a firm to keep going. A BCP is the process of figuring out which apps, customers (both internal and external), and locations a business needs to use and enforce to keep things running smoothly. Pardon (2018) said that both disruptive events and failover strategies can be quite essential. A BCP plan should usually show how all of its pieces, like its technology, software, physical location, staff, and applications, work together. Gandecha (2022) mentioned that the BCP plan should be a quick and effective technique to get the firm back up and operating. It should include a business impact evaluation that figures out how much time can be lost before the value of the business starts to drop significantly. The process of making a BCP strategy includes suggestions for continuing testing, training, raising awareness, and maintenance. The BCP plan should make it obvious what needs to be done before, during, and after a disaster [24].

The BCP makes sure that Adler Consulting can keep conducting business at least a little bit. Disaster recovery plans are detailed plans that show you how to get systems, data, and network connections back up and running after a disaster and how to get ready for the worst. In case of an emergency, these plans include measures for cutting off entrance to the building and clear instructions for what to do when information resources are not available. They also think about the chance of losing key people who do significant work and make sure the business can keep going without these key personnel.

Making a list of people to call in case of an emergency is a vital step in getting back on your feet after a calamity. This guide shows what to do straight soon after an incident and makes it easy to get in touch with the proper people. The first things that happen following an incident are to preserve the company's assets and keep them safe. This keeps them from being harmed or lost in the future. To make sure their business can remain functioning, companies set up recovery, backup, or other locations. The offices are set up so that they can all back each other up, and the sites are chosen such that the working conditions are similar. These facilities are linked via LAN networks and backup leased lines, which makes it easier for centres to move between them and work together [32].

The corporation might have to buy new equipment if resources can't be swiftly recovered. Vendors are highly vital to the recovery process since they give out replacements. The organisation may also have to use emergency procurement procedures to get things like software, equipment, supplies, and other essentials. The recovery centre puts together old and new parts that have been saved. Recovery personnel make alterations at the last minute if vendors can't get them particular pieces of equipment. After putting the equipment back together, the next thing to do is to figure out how to retrieve the data back.

The Executive Management Team, which is made up of people from the BCP Committee and the Recovery Management Committee, is in charge of leading the recovery process. This group is responsible for putting together the recovery organisation based on the best information they have about how awful and big the outage was. The Recovery

Management Coordinator (RMC) is in control of the full recovery process. All the recovery teams report to the RMC. Different groups with different skills are helping people get better. The IT Recovery Group is in responsible of fixing computers, connecting to networks inside and outside the firm, and processing data. The Logistics Recovery Group handles the paperwork and logistics, as well as the indirect work that needs to be done to bring the company's procedures back on track. The Corporate Communication Group makes sure that all TSL employees and clients are aware of the recovery efforts. This helps maintain things honest and open when things are hard.

a) Teaching

The corporation needs to perform regular training sessions and run public awareness initiatives to teach management and senior personnel about business continuity. These programs help make sure that everyone realises how crucial it is for a firm to keep going and is ready to act fast if something goes wrong. The training program is for managers and personnel who are in charge of maintaining the Business Continuity Plan up to date. The organisation gives the right personnel targeted training so that they have the information and skills they need to keep the plan up to date and useful.

Also, the workers and management who are in charge of different sections of the strategy during a crisis would get more training. This strategy makes sure that all staff members are ready to fulfil their roles and obligations, which helps the reaction be organised and successful when it is most needed.

b) Testing and Reviewing

Every time something dangerous happens, people check to make sure the organisation can follow through on its recovery plans. Some of the most typical danger assessments are normal corporate procedures, while others are tests or drills. In these cases, a disaster is recreated, and team members "walk through" the recovery steps to uncover any faults or things that were missed. The test scenario will involve the Recovery Management Coordinator and people from a number of recovery teams. The people in charge of making the strategy will first meet with the internal technology team, the application team, and the network administrators to figure out what has to be done. This entails looking at resources from both inside and outside the company, as well as resources from other companies. Senior management in the IT department should always be kept up to date so that everyone is on the same page and supports the process.

The team will get all the relevant papers for the network infrastructure, such as network diagrams, equipment settings, and database settings. If they exist, you should get copies of the most recent IT and network disaster recovery plans to look at. The team will then look at the risks that IT infrastructure management thinks are the most important, like fire, human error, power outages, and system failures. They will also look at what management thinks are the most critical weaknesses, like not having backup power or having old copies of the database.

A look at the company's past experiences with outages and interruptions, including how they were handled, will give us useful information. The team will find out what IT asset management thinks are the most crucial things, such as call centres, server farms, and internet access. After that, they will figure out how long management can go without these essential assets. The team will look into how big interruptions are now handled and check to see when they were last checked to make sure they still work. For any severe IT infrastructure difficulties, the emergency response teams will be found, and their level of training with essential systems, especially during crises, will be checked.

All of the evaluation data will be put together to make a complete gap analysis report. This research will look at how things are done today and how they should be done. It will also point out areas that need work and provide suggestions on how to get ready for the required level of preparedness, along with the expenses that are expected. Management will study the report and approve it, deciding what has to be done next. The last thing the team will do is build an IT disaster recovery plan (or plans) for essential networks and systems. Testing will reveal how well the plan works, and any changes or improvements made during this step will be shown in all disaster recovery documentation.

E. Protection for Systems and Apps

a) Protection for Workstations and Apps

Every day, people with diverse degrees of technical and security understanding use desktops to communicate and transact business all over the world [21]. Workstations are very crucial for company these days, but they also offer a huge security risk, especially for persons who work in IT [1].

Follow these regulations at workstations

- Require encryption on workstations: According to our encryption policy, data is encrypted when it is not being used. BitLocker can encrypt the complete disc on Windows machines, while FileVault does the same thing [15].
- Make it a habit to keep workstations safe: A company's password policy can help keep workstations from being hacked, but it's not a strong security culture if employees don't lock their workstations when they leave their desks

[2]. System administrators can set up configurations that will automatically turn off the workstation if it hasn't been used in a specific amount of time. This is helpful for when workers neglect to do it on their own. A good technique to control who may access workstations and other information systems, including network servers, is to set up a password-protected screen saver or primary screen lock.

- Make it clear which workstations are only for work. Because they spend so much time at their desks, employees may think of office equipment as their own. They might start playing games, watching films and listening to music online, or saving and sharing files with other individuals. They show people how to use the company's property for work. You can see, edit, or delete any activities or data that are stored on the device at any time. Some businesses even stop people from using their wireless networks so that workstations may only connect to access points that support encryption.
- Users need clear instructions and a person or department to report the problem and correct it when a workstation or other company equipment is lost or stolen. We will add language that lets clients know that dealing with these kinds of situations may take a long time. For example, "Please report missing gadgets as soon as possible so IT can wipe the item." It also protects the company's data, reputation, and integrity.
- Make sure that every month, endpoints get patches for third-party software like Adobe, Java, Flash, and browsers. Updating third-party software is another important aspect of a healthy desktop setup. When we update the operating system, we can't just patch everything at once. We need to know all the apps on our network and which versions should stay the same. Some web-based apps might demand a certain version of Java, and if we upgrade the workstations to the newest version, the web app would not operate for users.

b) Managing Vulnerabilities and Patches

Oreilly and Ebad (2018) said that companies should form a patch and vulnerability group (PVG) to make it easier to locate and share patches within the firm. The PVG should make a program for the complete firm to manage patches and vulnerabilities. This program should encompass patching and upgrading the OS and applications.

c) The Group Should do These Tings

Using automated patch management solutions to speed up the deployment of patches to systems: As the number of patches that need to be installed grows and attackers identify and exploit code more quickly, manually patching machines becomes less effective [1]. It may seem hard to patch and keep an eye on vulnerabilities, but a validated and integrated patching plan that makes the most of automatic patching technology can help make sure that an organization's vulnerabilities are corrected.

Using a staged approach to roll out corporate patch management tools: Patch management systems can be rolled out in stages, fixing process and user communication problems with a limited group before the patch application is made available to everyone. Patch management technologies are often used to make sure that desktop PCs and single-platform server farms have the same settings at first [16]. Then we will work on the harder task of bringing together machines with different operating systems, nonstandard desktop systems, older PCs, and machines with strange setups.

Finding and minimising the hazards of employing corporate patch management solutions: These tools can assist minimise risk, but they can also make an organisation more vulnerable to security threats [21]. For example, an attacker may break into the main patch management computer and utilise the corporate patch management program to swiftly propagate malware that could be quite harmful.

III. CONCLUSION

This case study has meticulously put out a thorough plan for making Adler Consulting's digital systems security stronger and more proactive, so they can better protect themselves against the ever-changing cyber threat scenario. Adler Consulting is set to substantially improve its security posture by resolving recognised gaps and making smart changes to policy, network architecture, and incident response. Adler Consulting has the skills it needs to keep an eye on threats and construct a robust defence by setting up a Security Operations Centre (SOC) with a CISO in charge and hiring security experts. The suggested security policies, which include Acceptable Use, Security Awareness, Change Management, Password Management, Remote Access, and Third-Party Engagement, are important for making security a part of the culture and making sure everyone knows how to do their job.

The planned upgrades to network security, such putting in IDS/IDPS and keeping an eye on network performance on a regular basis, are aimed to make the decentralised network architecture stronger and make it easier to discover and stop attacks. Strong issue Response and Business Continuity Plans are also highly vital for keeping the organisation strong and functioning after a security issue. Adler Consulting will not only protect its valuable assets and client data by putting these

integrated measures into action in a planned way, but it will also improve its reputation as a secure and reliable global IT solutions provider. This will ensure long-term operational integrity and business growth.

IV. REFERENCES

[1] Ahmed, U., Bhuiya, I. and Rahman, M., (2017). A secure enterprise architecture focused on security and technology-transformation (SEAST), The 12th International Conference for Internet Technology and Secured Transactions, (ICITST-2017), Cambridge, UK, 11–4/12/2017.

[2] Alanazi, T., Anbar, M., Ebad, A., Karuppayah, S., and Al-Ani, A. (2020). Theory-based model and prediction analysis of information security compliance behavior in the Saudi healthcare sector. Symmetry, 12(9), 1544. DOI: 10.3390/sym12091544

[3] Ali, S. S., & Singh, Y. (2018). On Opportunistic Routing in Wireless Sensor Networks. International Journal of Computer Sciences and Engineering, 06(03), 21–25. https://doi.org/10.26438/ijcse/v6si3.2125

[4] Arean, O. (2013). Disaster recovery in the cloud. Network Security, 2013(9), 5–7. https://doi.org/10.1016/s1353-4858(13)70101-6

[5] Bejtlich, R. (2012). The Importance of Security Awareness, Threat Research Blog. FireEye.

[6] Bellovin, S. M. (2009). Security problems in the TCP/IP protocol suite. ACM SIGCOMM Computer Communication Review, 19(2), 32–48. https://doi.org/10.1145/378444.378449

[7] Bishop, M. (2005). Policy and Mechanism | An Overview of Computer Security, Inform IT Informit.com.

[8] Chandran, M., and Vinothramkumar, B. (2018). Crime Intelligent Security Control Robot Investigation System. International Journal of Computer Sciences and Engineering, 06(08), 114–124. https://doi.org/10.26438/ijcse/v6si8.114124

[9] Chapple, M. (2016). Can ISO 27002 be used as a standalone guide for security management? Search Security.

[10] Cohn, S., and Simon, C. (2019). Britain's Phoenix to buy Swiss Re's ReAssure business for $4.1 billion. Reuters – via www.reuters.com.

[11] Dahiya, B. P., Rani, S., & Singh, P. (2018). Performance Analysis of Swarm Intelligence Techniques to improve lifetime of Wireless Sensor Networks. International Journal of Computer Sciences and Engineering, 6(9), 885–895. https://doi.org/10.26438/ijcse/v6i9.885895

[12] Dandotiya, N., Singh Dandotiya, A., & Gupta, S. (2019). Impact of Software Defined Networking for Wireless Sensor Networks. International Journal of Computer Science and Engineering, 6(4). https://doi.org/10.14445/23488387/ijcse-v6i4p102

[13] Danchev, D. (2003). Building and Implementing a Successful Information Security Policy. WindowSecurity.com

[14] Dhillon, G. & Backhouse, J. (2001) “Current directions in IS security research: towards socio-organisational perspectives”, Information Systems Journal, 11, pp 127-153.

[15] Ebad, S. (2018). The influencing causes of software unavailability: A case study from the industry. Software Practice and Experience, 48(5), 1056–76. DOI: 10.1002/spe.2569.

[16] Ebad, S. (2018). An exploratory study of ICT projects failure in emerging markets. Journal of Global Information Technology Management, 21(2), 139–60. DOI: 10.1080/1097198X.2018.1462071

[17] Esa, F.; Yusof, Y. (2016). Implementing overall equipment effectiveness (OEE) and sustainable competitive advantage: A case study of hicom diecastings SDN. BHD. (HDSB). ARPN J. Eng. Appl. Sci.

[18] Fulford, H. and Doherty, N. (2003). The application of information security policies in large UK-based organizations: an exploratory investigation. Info Mngmnt& Comp Security, 11(3), pp.106-114.

[19] Gandecha, D. T. (2022). A Review on Cloud Computing Technology, Cloud Deployment, and Service Delivery Models. International Journal for Research in Applied Science and Engineering Technology, 10(1), 1238–1245. https://doi.org/10.22214/erased.2022.40022

[20] Gupta, A. and Hammond, R. (2005). Information systems security issues and decisions for small businesses. Info Mngmnt& Comp Security, 13(4), pp.297-310.

[21] Hashizume, K., Rosado, G., Fernández-Medina, E., and Fernandez, B. (2013). An analysis of security issues for cloud computing. Journal of Internet Services and Applications, 4(5), n/a. DOI: 10.1186/1869-0238-4-5.

[22] Ibrahim, R.; Jamal, M., Esmaeel, I., Zakuan, N, Mohd, N. (2018). C Trade-off Costing models for capacity optimization between used capacity and operational efficiency of business performance from the perspective manufacturing strategies: ScienceDirect

[23] Jewliya, S. (2017). Analysis of Web Application Security. International Journal of Computer Sciences and Engineering, 5(9). https://doi.org/10.26438/ijcse/v5i9.215220

[24] Ju, H. (2014). Intelligent disaster recovery structure and mechanism for cloud computing network. International Journal of Sensor Networks, 16(2), 70. https://doi.org/10.1504/ isn’t.2014.065860

[25] Kent, S. (2008). Comments on “security problems in the TCP/IP protocol suite.” ACM SIGCOMM Computer Communication Review, 19(3), 10–19. https://doi.org/10.1145/74674.74675

[26] Pardon, G., Pautasso, C., and Zimmermann, O. (2018). Consistent Disaster Recovery for Microservices: the BAC Theorem. IEEE Cloud Computing, 5(1), 49–59. https://doi.org/10.1109/mcc.2018.011791714

[27] Sustainable Manufacturing: Metrics, Standards, and Infrastructure—Workshop summary. Proceedings of the 2010 IEEE International Conference on Automation Science and Engineering, Toronto, ON, Canada.

[28] Sayeed, R., Miller, R., and Sayeed, Z. (2016). Throughput Prediction Across Heterogeneous Boundaries in Wireless Communications. Journal of Cyber Security and Mobility, 4(4), 233–258. https://doi.org/10.13052/jcsm2245-1439.441

[29] Schaefer, R. (2014). A usenet for a new age. ACM SIGSOFT Software Engineering Notes, 39(1), 7. https://doi.org/10.1145/2557833.2557863

[30] Singh, R. (2018). Evaluation of Energy Saving Medium Access Control Protocol for Wireless Sensor Networks. International Journal of Computer Sciences and Engineering, 6(6), 514–520. https://doi.org/10.26438/ijcse/v6i6.514520

[31] Soni, M., Singh, D., & Kumar, S. (2019). Wireless Sensor Network Performance with Energy-Efficient Approaches: A Review. International Journal of Computer Sciences and Engineering, 7(5), 1532–1537. https://doi.org/10.26438/ijcse/v7i5.15321537

[32] Upendra, Kanuru. (2025). Enterprise Security Strategy Framework for Electronic Health Record Organizations. *International Journal of Advanced Research in Computer and Communication Engineering,* 14(5), 1-8. https://doi.org/10.17148/IJARCCE.2025.14501