What did you do?

In preparation of establishing my ransomware recovery strategy, I reviewed the Dzimiela and Jennex case study and coupled that with my personal research from a few notable publications like IBM and Dell. During my research I found that many of the publications are very consistent in the steps that one should take on how to prioritize their most vital assets in the event of a ransomware attack. I think it's important to note, especially if this is a plan for a business, that although one should prioritize the recovery of network assets and protect sensitive information as quickly as possible, but one should also consider how to complete this process simultaneously while focusing on business continuity as well. Based on the research, I used the information below a general guideline on how to prioritize my assets in establishing my recovery plan.

1. Critical Assets – Identify and prioritize the recovery of critical systems that are essential to the organizations day-to-day operations. These might include email servers, customer relationship management (CRM) systems, financial systems, and any other platforms crucial for conducting business.

2. Data Repositories - Focus on recovering databases and file servers that contain critical data such as customer information, financial records, intellectual property, and any other sensitive data vital for the organization's operations.

3. Backup Systems - Ensure that backup systems are recovered early in the process so that data restoration can begin promptly. This includes both on-site and off-site backups.

4. User Workstations - Depending on the scale and scope of the attack, recovering user workstations may be necessary to restore productivity across the organization. Prioritize systems used by key personnel or teams critical for business operations.

5. Network Infrastructure - Restore network infrastructure such as routers, switches, and firewalls to ensure stable connectivity and security across the organization's network.

6. Communications Systems - Restore communication platforms such as VoIP systems, video conferencing tools, and instant messaging services to facilitate collaboration and communication among employees.

7. Security Systems - Ensure that security systems such as intrusion detection/prevention systems (IDS/IPS), antivirus software, and security information and event management (SIEM) systems are restored to mitigate the risk of future attacks and monitor for any suspicious activity.

8. Public-Facing Systems - If the organization provides services or interacts with customers through public-facing systems such as websites or applications, prioritize the recovery of these systems to minimize the impact on customer experience and reputation.

9. Regulatory Compliance Systems - If the organization is subject to regulatory requirements such as GDPR, HIPAA, or PCI DSS, prioritize the recovery of systems and data necessary to maintain compliance with these regulations.

10. Third-Party Dependencies - Consider any third-party dependencies or interconnected systems that may have been affected by the ransomware attack and prioritize their recovery accordingly.

After establishing a sufficient guide to start my recovery plan, I revisited the output from Research Assignment #1 to gather the equipment needed to build my network and thus prioritized them all. In addition to listing out all the equipment in assignment #1, I also referenced a small diagram built for the first assignment and shows how the equipment is connected and designates if it's a hardwired, cloud, wireless, or Bluetooth connection. This diagram helped to ensure nothing was missed and that there is a plan for each component.

I then revisited Research Assignment #2 and #3 to identify my devices using Zenmap (NMAP) that need to be updated through discovering open ports and services, thus detecting any vulnerabilities that need attention; and also the results from Wireshark, used to capture network packets and analyze the real-time traffic. I used my home network for assignments #2 and #3 and didn't have many things that needed to be addressed from a vulnerability perspective, but I understand that performing the scans on a business network would contain much more information and potentially more threats to address.

Much like the process for identifying which network assets need to be prioritized during ransomware recovery, the process for identifying passwords that need to be backed up is practically identical and involves understanding which passwords and are crucial for restoring access to various systems, applications, and data within the organization. I compiled a list of the roles and/or applications that should be prioritized for password recovery:

- System Administrator Accounts
- Database Credentials, including database management systems
- Application Accounts, including ERP and CRM
- User Account Credentials, including individual workstations
- Email Account Credentials
- Cloud Service Credentials
- Backup and Recovery System Credentials

What are the results?

To prioritize the **list of components for recovery** and specifically identify which assets are vital and must be recovered first based on my network design from Assignment #1, I compiled the guide below:

Data Recovery: Since data is one of the most imperative components to prioritize for recovery, my plan would be to first mitigate any further exposing or loss of it. This includes databases that contain sensitive business and customer information that's needed for day-to-day business to activities. Since the purpose of most ransomware attacks involves obtaining personal information for financial gain, I would want to prioritize protecting my Cloud Services that houses most of that information. This includes my CRM, ERP for financial data, and my email server. Recovering this data quickly will allow the business to resume normal activities and maintain continuity.

System Infrastructure: My plan would then focus on recovering the physical system infrastructure, including workstations, POS stations, and storage systems. Quickly restoring these physical components will ensure that the necessary resources are available to support data recovery.

User Access: After identifying an attack and implanting the recovery plan, we would restore user access to critical systems, applications, and data to enable employees to resume their roles and responsibilities. This may involve resetting passwords, provisioning temporary access, or restoring user profiles to ensure uninterrupted workflow.

Communication Channels: Restore communication channels such as email, messaging platforms, and collaboration tools to facilitate internal and external communication during the recovery process.

Security Controls: Reestablish security controls and measures to protect recovered systems and data from future attacks. This includes deploying security patches, updating antivirus software, and implementing intrusion detection/prevention systems to prevent reinfection.

Business Applications: Recover critical business applications and software necessary for day-to-day operations. This may involve reinstalling applications, restoring application data, and ensuring compatibility with recovered systems and infrastructure.

External Services: Restore access to external services and dependencies, such as cloud platforms, third-party vendors, and hosted services. Ensuring connectivity to external resources is essential for resuming normal business activities and maintaining service levels.

Regulatory Compliance: Address any regulatory compliance requirements and obligations during the recovery process. Ensure that recovered systems and data remain compliant with relevant regulations and industry standards to avoid penalties and legal consequences.

Documentation and Reporting: Document recovery efforts, actions taken, and lessons learned for post-incident analysis and reporting. Ensuring that you maintain documentation helps improve future response strategies and ensures accountability for recovery activities.

List of Backups

Data Backups: The benefit of my critical systems being mainly Cloud systems is that they are usually very secure, and the stored information is usually in real-time and constantly backed up and easily recoverable if there is a ransomware attack. To ensure these systems and data are recoverable, it's important to understand the policies for the vendors, what their recovery process is, and what security measures they have in place to continuously protect your information. Regularly backing up all critical data stored on servers, workstations, and other devices will ensure that you recovery quickly in the event of an attack.

System Backups: Backing up entire system images of servers and workstations, including the operating system, installed applications, and system configurations. System backups enable quick restoration of entire systems in the event of a ransomware attack. These system backups can be large and can take some time, but to mitigate this, I think it's important to dedicate uninterrupted system backup time to ensure that we have the most updated information if we need to revert to a backup after an attack.

Cloud Backups: Many cloud services such as Microsoft 365, Google Workspace, or other cloud storage providers, ensure that data stored in the cloud is regularly backed up, as mentioned in the data backup section. Many cloud services offer built-in backup solutions or other third-party backup providers can be used to protect cloud data.

By implementing a comprehensive backup strategy that encompasses multiple backup types and storage locations, organizations can mitigate the risk of data loss and disruption caused by an attack. It's important to regularly review and update backup processes to adapt to evolving threats.

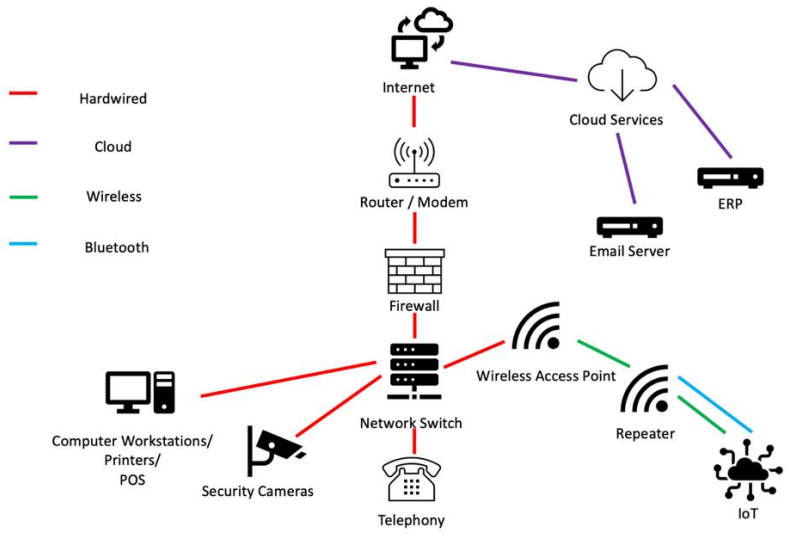
List of Passwords to be backed-up

Identifying passwords that need to be backed up during ransomware recovery involves understanding which ones are most crucial for restoring access to all your important systems. I believe that the only roles that need access to backup and recovery passwords would be those that are aligned to the IT organization. Mainly because they'd be the parties responsible for implementing the recovery plan.

The passwords for the IT team and/or system administrator accounts would include those for the operating system, network infrastructure devices (routers, switches, firewalls), and server management, Cloud services, etc.

List of devices that need to be updated

In Research Assignment #1, I listed the physical components needed to build a network for a small café and drew a small diagram to visually represent the equipment.



The physical devices that would need to be updated are:

- Router/modem
- Firewall
- Network Switch
- VoIP Telephony system
- Security system
- IoT devices
- Computer Workstations/ POS

Inventory of network devices

The inventory of the network devices listed out in Assignment #1 are:

Modem – AT&T BGW320-500 Wireless Voice Gateway (Fiber) (LAN)

Router – Meraki GO GX20

Firewall – Cisco Firepower 1120

Switch – Cisco Business 220

Access Point – Cisco Business 200 Series

Repeater – Cisco Business 100 Series

What did you learn?

It still amazes me that organizations must go through this grueling amount of planning to mitigate potential ransomware attacks and must be on guard 24/7, but all it takes is an attacker one time to “get it right” and exploit the entire system. Given that attacks are becoming more apparent and even affecting some of the biggest and most trusted brands, I think it’s important to know that it can happen to anyone, thus the reason organizations should have a well thought out plan in case an unfortunate event happens. My biggest take away from this assignment is that having a recovery plan isn’t just to recover data and get back to status quo, but these plans must consider that business must still go on as well and can’t simply stop just because there’s a recovery attempt in process. Having a plan in place ensures that an organization can accomplish both. I don’t work in an IT capacity now, but this information is very helpful, especially as I plan to open a business of my own in the future. So having this knowledge helps me understand that for every system or process I have in place to run my business, I also must have a recovery plan for each one in case of an attack.