**Cybersecurity Case Study Final Report**

Sergey Dmitriev  
Cybersecurity  
May 13, 2025  
CyberProtect Inc. Data Breach Analysis

**Table of Contents**

1. Introduction
2. Summary of the Breach
3. Evidence Summary  
     • Login Logs  
     • Email Records  
     • Network Logs  
     • Incident Reports  
     • Threat Email
4. Email Breakdown  
     • Email 1: Phishing Message  
     • Email 2: Internal Cover-up  
     • Email 3: Hacker’s Ransom Demand
5. System Log Analysis  
     • Unauthorized Login Attempts  
     • Unusual Successful Login  
     • Data Transfer Event
6. Damage Assessment  
     • Type of Data Lost  
     • Financial and Reputational Impact
7. Fixing the Problem  
     • Technical Solutions  
       – Multi-Factor Authentication (MFA)  
       – Intrusion Detection System (IDS)  
       – Modern Encryption (AES)  
     • Non-Technical Solutions  
       – Employee Education  
       – Stronger Policies and Access Control  
       – Password Policy
8. Technical Exercises  
     • Caesar Cipher Demonstration  
     • Modern Encryption Comparison
9. Ethical Considerations  
     • Public Disclosure  
     • Conflict of Interest  
     • Stakeholder Impact
10. Conclusion

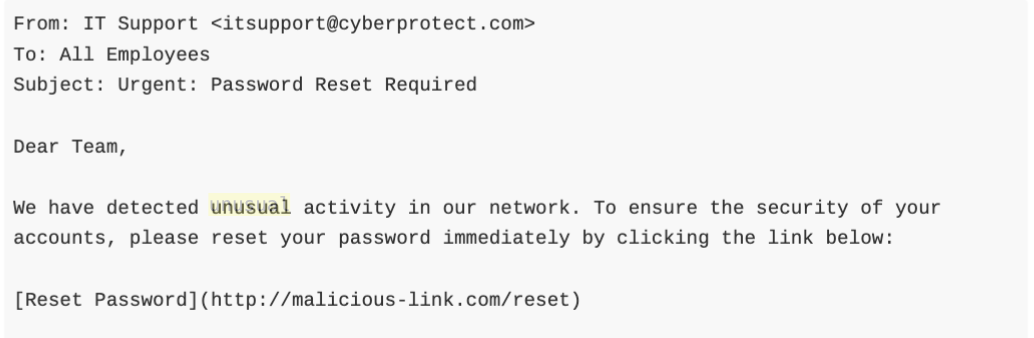
**Introduction**

This case study analyzes a cybersecurity incident at CyberProtect Inc., a company responsible for safeguarding sensitive client and employee data. The breach originated from a phishing attack in which employees were tricked into revealing login credentials, which the attackers then used to compromise credentials. The attackers gained unauthorized access to internal systems, extracted confidential data, and attempted to extort the company.

In this study, I will trace how the attack unfolded, identify the overlooked vulnerabilities that enabled it, and offer both technical and non-technical recommendations for remediation and prevention. Supporting evidence, such as system logs, email communications, and IP addresses, is presented to reconstruct the attack and justify the recommendations.

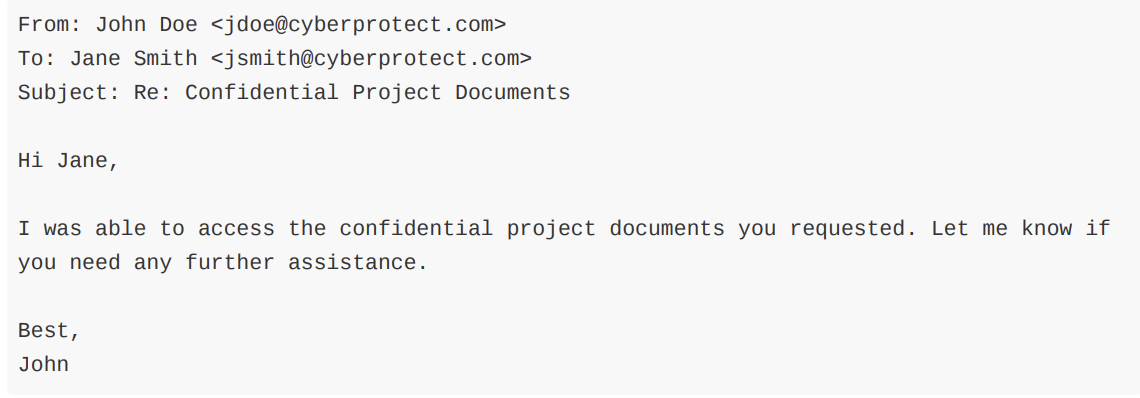
**Email Breakdown**

**Email 1: Phishing Message**

This email falsely alerted users to suspicious activity and urged a password reset through a malicious link. The link led to a fake login page where user credentials were harvested. Multiple employees, including Jane Smith and John Doe, were compromised.  
A close-up of a white background

AI-generated content may be incorrect.

**Email 2: Internal Cover-up**

An email sent between the two compromised accounts (Jane and John) appeared routine but was crafted to make the 500 MB data transfer look legitimate. This tactic was used to bypass suspicion during security log reviews.  


**Email 3: Hacker’s Ransom Demand**

Following the data extraction, the attacker reached out to the IT admin. The message threatened to release the data publicly unless a ransom was paid. This highlights the attacker's intent to monetize the breach through extortion.

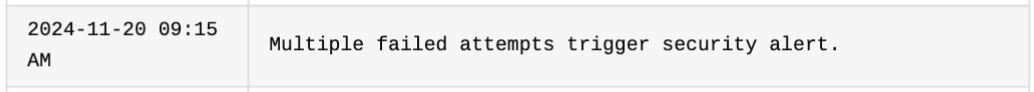
A white background with black text

AI-generated content may be incorrect. **A white background with a black and white flag

AI-generated content may be incorrect.**

**System Log Analysis**

**1. Unauthorized Login Attempts**



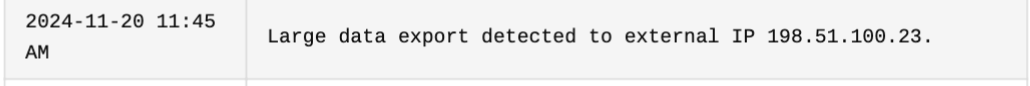
This suggests brute-force attempts or credential stuffing from a local machine.

**2. Unusual Successful Login**

****

Jane had no prior travel history, making this login highly suspicious.

**3. Data Transfer**

****

This marks the data exfiltration event that solidified the breach.

**Damage Assessment**

**What Was Taken (Stolen or Accessed):**

* **Confidential HR records**  
  (Private employee documents used by Human Resources)
* **Employee Social Security numbers**  
  (Important personal ID numbers used for taxes and employment)
* **Employee PII (Personally Identifiable Information)**  
  (Such as names, addresses, phone numbers, and other private details)
* **Internal company documents**  
  (Work files, memos, or plans that are not meant to be public)
* **Project files**  
  (Work-in-progress documents about company projects, possibly including future products or strategies)
* **Strategic plan for 2024–2026**  
  (Company goals for developing encryption and using machine learning for security)
* **About 500 MB of data was stolen**

-----------

* **Large financial costs**, including:
  + Hiring cybersecurity experts (forensic analysis)
  + Legal consultations
  + Upgrading security systems
  + Paying possible fines for breaking data protection laws
* **Reputation damage**  
  (Customers and employees may lose trust in the company)
* **Legal trouble**  
  (Because sensitive data was not properly protected, the company may face lawsuits or penalties)

**Fixing the Problem**

**Technical Solutions**

**1. Multi-Factor Authentication (MFA)**

**MFA adds an extra layer of security. It means that even if someone steals a password, they still can’t log in without a second code. That code might come from a phone app like Google Authenticator.**

**How to Use It:  
CyberProtect should make employees and users set up 2-factor authentication (2FA) using apps like** [**Google Authenticator**](https://apps.apple.com/us/app/google-authenticator/id388497605)**.  
More info:** [**Google Authenticator – Wikipedia**](https://en.wikipedia.org/wiki/Google_Authenticator)

**2. Intrusion Detection System (IDS)**

**An IDS watches the network to catch strange behavior. It can spot suspicious activity like logins at weird times or huge amounts of data leaving the network, and send out alerts before serious damage happens.**

**How to Use It:  
CyberProtect should install IDS tools like** [**Snort**](https://en.wikipedia.org/wiki/Snort_(software)) **or** [**Zeek**](https://en.wikipedia.org/wiki/Zeek) **to monitor traffic in real-time and find threats faster.**

**3. Modern Encryption (AES)**

**Encryption turns information into unreadable code unless you have the right key. This keeps data safe if it’s stolen.**

**Example:  
Instead of using a Caesar cipher (which is very easy to break), we can use AES (Advanced Encryption Standard), which is used by banks, apps, and governments.  
Encryption/Decryption Example (AES)  
Plaintext: Will tomorrow be Wednesday?  
Encrypted (AES): 6f4a13b8e9c832ac94d3abf4...  
Decrypted: Will tomorrow be Wednesday?  
This can’t be read unless you have the correct key. AES is much safer and used in real life.**

**Non-Technical Solutions**

**1. Employee Education**

**Many attacks happen because someone clicks a fake link or opens a bad email. Teaching employees how to spot phishing and what not to click can stop attacks before they happen.**

**How to Use It:  
Host monthly training sessions and run fake phishing email tests to see how well employees do.**

**2. Access Rules and Stronger Policies**

**CyberProtect should create strong rules about passwords, access, and file permissions. Only the right people should see important files, and passwords should be strong and updated often.**

**Password Policy Example:**

* **At least 10 characters**
* **1 uppercase letter (A–Z)**
* **1 lowercase letter (a–z)**
* **1 number (0–9)**
* **1 special character (!@#$%^&\*)**

**Strength test:  
"password123": cracked in 0 seconds  
"** **CyberProtect1!(protect)": estimated time to crack = 774 years  
This proves the need for complex passwords as described in our policy.**

**3. Enforce Cyber Rules with Access Control**

**Make cybersecurity training required. If someone doesn’t finish it, they should lose access to company systems until they do. That way, everyone stays alert and responsible.**

**Ethical Considerations**

**Should CyberProtect Inc. Disclose the Breach?**

Yes, CyberProtect Inc. should tell people about the breach. Even though this might hurt the company’s reputation, it’s the right thing to do. People whose private information was stolen—like social security numbers or addresses—need to know so they can protect themselves. Hiding the breach could lead to even more problems later, like lawsuits or customers losing trust.

Telling the truth follows ethical values like honesty, responsibility, and respect. Also, in many states, companies are required by law to report data breaches. Being honest now can help the company rebuild trust in the future. Trying to cover it up could make things worse if the truth comes out later.

**How the Breach Affects Different People (Stakeholders)**

There are three main groups of people who are affected by this breach, and each group has different needs and worries:

1. **Employees:**  
   The employees at CyberProtect had their personal information stolen. That includes things like social security numbers, addresses, and maybe even bank info. They are scared their identities could be stolen or misused. They need to be told right away so they can take action, like freezing their credit or watching for fraud. The company owes them honesty and support.
2. **Customers and Clients:**  
   Customers trust CyberProtect Inc. to keep their data safe. This breach damages that trust. If the company doesn’t tell them what happened, customers might leave and never come back. They deserve to know what information was exposed and what the company is doing to fix it. Being honest with customers is part of being a responsible business.
3. **The Company and Its Leaders:**  
   The people who run CyberProtect may want to keep the breach a secret to protect the company’s image and stock value. They might worry that public news about the hack will cause panic or financial loss. But hiding the truth is risky. If people find out later, the company could face bigger problems like legal action or government fines. The best long-term decision is to be honest and take responsibility now.

**Conclusion**

This case study shows how one fake email (a phishing scam) can lead to a major data breach. After getting some employees’ login info, the hacker used that access to steal private information. CyberProtect Inc. needs to take strong action by using two-step logins (MFA), teaching employees about safety, updating company rules, and using tools to watch for attacks.

In the end, this situation is a clear reminder that even strong computer systems can be broken if people aren’t careful. Being prepared is the best way to stay safe.