**Assess the Security Breach**

The first step you should take after a data breach is to determine which servers have been compromised and contain them as quickly as possible to ensure that other servers or devices won't also be infected. You'll need to determine the cause of the breach within your specific facility so you can work to help prevent the same kind of attack from happening again.

* Who has access to the servers that were infected?
* Which network connections were active when the breach occurred?
* How was the attack initiated?

You may be able to pinpoint how the breach was initiated by checking your security data logs through your firewall or email providers, your antivirus program, or your Intrusion Detection System.

**Contain the Cyber Security Breach**

You should change all affected or vulnerable passwords immediately. Create new, [strong passwords](https://amtrustfinancial.com/blog/small-business/5-tips-for-creating-strong-passwords) for each account, and refrain from reusing the same passwords on multiple accounts. That way, if a data breach happens again in the future, the damage may be limited.

* Disconnect your internet
* Disable remote access
* Maintain your firewall settings
* Install any pending security updates or patches
* Change passwords

**How to Improve Firewall Security:**

[1. Limit VPN Access](https://www.sunnyvalley.io/docs/network-security-tutorials/how-to-improve-your-firewall-security#1-limit-vpn-access)

[2. Monitor User Access](https://www.sunnyvalley.io/docs/network-security-tutorials/how-to-improve-your-firewall-security#2-monitor-user-access)

[3. Shut Off Unused Network Services](https://www.sunnyvalley.io/docs/network-security-tutorials/how-to-improve-your-firewall-security#3-shut-off-unused-network-services)

[4. Update Firewall Software](https://www.sunnyvalley.io/docs/network-security-tutorials/how-to-improve-your-firewall-security#4-update-firewall-software)

[5. Automate the process of firewall updating](https://www.sunnyvalley.io/docs/network-security-tutorials/how-to-improve-your-firewall-security#5-automate-the-process-of-firewall-updating)

[6. Buy New Security Hardware](https://www.sunnyvalley.io/docs/network-security-tutorials/how-to-improve-your-firewall-security#6-buy-new-security-hardware)

[7. Secure Wireless Access](https://www.sunnyvalley.io/docs/network-security-tutorials/how-to-improve-your-firewall-security#7-secure-wireless-access)

Steps to Recovery:

1. Don’t Improvise

* Identify Source ad Extent of Breach
* Addressing Legal and Ethical Obligations
* Answering Consumer Queries

1. Conduct a Data Breach Post-Mortem
2. Document Everything
3. Implement Robust Data Encryption Measures
4. Don’t Get Complacent