Company Name: Brain Trust NSTA

Actions that would be taken after the Data breach

Handling a data breach requires a swift and effective response to minimize the damage caused. Here are some steps you can take to handle a data breach:

1. Don’t Panic
2. Disable (do not delete) remote access capability and wireless access points. Change all account passwords and disable (not delete) non-critical accounts.
3. Prevent the spreading of attack to other users, which would cause further damage, by isolating compromised endpoints and assets.
4. Contain the breach: The first step is to isolate the affected systems and prevent the breach from spreading. This may involve shutting down affected servers, disconnecting affected devices from the network, and closing off any vulnerabilities that were exploited.
5. Assess the damage: Once the breach has been contained, assess the extent of the damage. Determine what data was compromised, how it was accessed, and whether any sensitive information was exposed.
6. Notify affected parties: Depending on the nature of the breach, you may need to notify affected individuals or organizations. This may involve sending out notifications via email or mail, posting a notice on your website, or working with law enforcement agencies.
7. Investigate the cause: Determine how the breach occurred and identify any vulnerabilities that need to be addressed to prevent future breaches. This may involve working with forensic experts to analyze system logs and other data.
8. Implement remediation measures: Once you have identified the cause of the breach and any vulnerabilities that need to be addressed, take steps to remediate the situation. This may involve implementing security patches, upgrading systems, or reconfiguring access controls.
9. Review and improve security policies: Review your existing security policies and procedures and identify areas for improvement. Implement new policies and procedures to ensure that the same or similar breaches do not occur in the future.
10. Communicate with stakeholders: Keep all stakeholders informed throughout the process, including employees, customers, and partners. Be transparent about what happened, what is being done to address the situation, and what steps are being taken to prevent future breaches.

Handling a data breach can be a complex and challenging process, but taking swift and effective action can help minimize the damage caused and protect your organization's reputation.

**INCIDENT REPORT: COMPUTER NETWORK BREACH AFFECTING FINANCIAL AND EMPLOYMENT RECORDS**  
**Date of Incident**: [17/03/2023]  
**Time of Incident**: [11:55PM]  
  
**Summary of Incident**:

On 17/03/2023, Brain Trust NSTA experienced a computer network breach that affected their financial and employment records. The breach was detected at 11:55PM when our IT team noticed unusual activity on our network.  
  
**Nature of Incident:**  
The investigation revealed that an unauthorized party gained access to our network through a phishing email. The attacker was able to bypass our security measures and gain access to sensitive financial and employment records.  
  
**The attacker was able to access the following information:**  
  
Names and personal information of employees  
Social Security numbers and tax identification numbers  
Salary and compensation details  
Bank account information  
Other financial and employment records

**Response to Incident:**

Upon discovery of the breach, our IT team immediately took action to isolate the affected systems and limit the damage. We also engaged an external cybersecurity firm to assist in the investigation and remediation efforts.  
  
We have notified all affected employees and provided them with guidance on how to protect themselves from identity theft and other potential consequences of the breach. We have also implemented additional security measures to prevent similar incidents from occurring in the future.  
  
**Conclusion:**The security of our organization and the information of our employees is of the utmost importance to us. We deeply regret any harm or inconvenience caused by this incident and are committed to taking all necessary steps to protect our network and prevent future breaches. We will continue to monitor the situation closely and provide updates as necessary.