

Data Breach

RESPONSE & PREVENTION CHECKLIST

24 Hours After A Breach

- Document When Breach Was Discovered
- Notify The Response Team
- Isolate Breach If Possible
- Notify Law Enforcement If Advised By Response Team
- Document The Investigation Of The Breach
- Freeze Financial Data (If Applicable)

First Week After A Breach

- Document The Breach Investigation
- Coordinate With Response Team to Resume Normal Operations
- Notify Any Clients Who May Have Been Affected By The Breach
- Document Breach Remediation Efforts
- Use Dark Web Monitoring Tools To Monitor For Affected Credentials
- Work With Your Response Team To Create A Disaster Recovery Plan

First Month After A Breach

- Implement Employee Security Training Measures
- Enable Multi-Factor Authentication
- Use Automation And/Or Assistance From Your Response Team To Perform Regular Patching Of Devices
- Invest In Advanced End Point Protection Or Retain The Services Of A Response Team Who Provides It

First Year After A Breach

- Have An Annual CyberSecurity Assessment Performed
- Review CyberSecurity Preparedness Review And Update Your Disaster Recovery Plan
- Invest In CyberSecurity Insurance
- Continue Regular CyberSecurity Monitoring Efforts & Improvements
- Insure Backup Procedures Are In Place & Are Multi-Layered