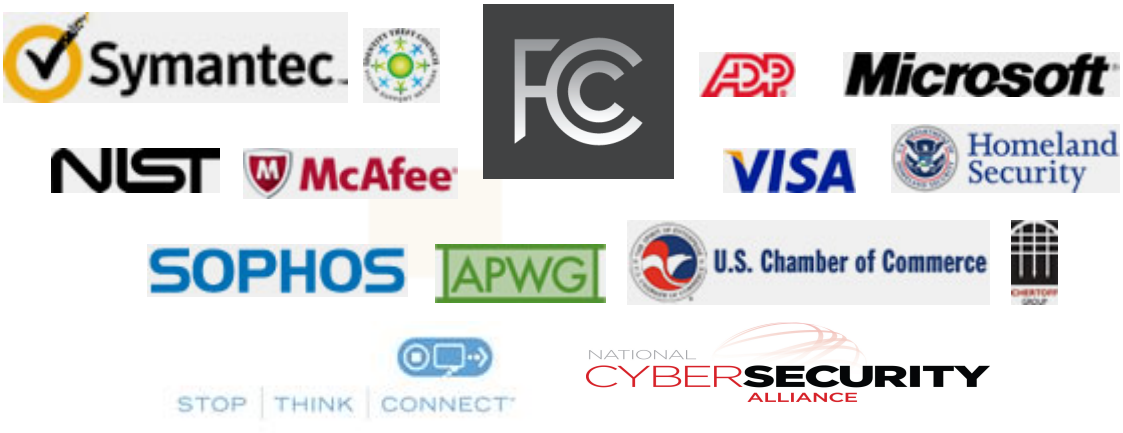
Federal
Communications
Commission



Incident Response

Even well-implemented cyber security structures and plans may not prevent all breaches of your business' data defenses, so be sure to have procedures in place to respond to security breaches when they occur.

Types of breaches

Physical breaches include real-world crimes such as burglaries and equipment theft, as well as any event when your company's equipment is misplaced or lost in transit. Unauthorized devices may be installed on a system or network, permitting further compromises of data confidentiality and integrity. Physical breaches can also result from reselling, donating or recycling old equipment that has not been properly cleansed of potentially sensitive information.

Network and system security breaches include events when computers become infected with malicious code, are accessed by unauthorized individuals remotely or are used by authorized individuals to perform malicious activity. This can also include breaches to network routers and firewalls, both within and outside your organization's boundary and control.

Data breaches, meaning the leakage or spillage of sensitive information into insecure channels, can result from any of the types of events described above. Data breaches can also occur if sensitive information is left improperly exposed by mistake.

Cyber Plan Action Items, if Breach Occurs:

1. Notify law enforcement if necessary

Depending on the type of breach and type of business, your company may be required to notify local law enforcement or other government authorities upon discovery of a data breach. In the event of exposure of customer information, you should notify the customer(s) of the incident, record the data that was lost or exposed and record the measures taken to ensure against future exposure.

2. Work cohesively across technical and leadership teams to limit the damage

Once your company becomes aware that a breach has occurred, technical personnel and business decision makers should work together to decide on the most practical and effective containment plan. Containment plans will vary from one set of circumstances to the next, and they may quickly become intensive in terms of time and resources from both the technological and business impact perspectives. In any case, the containment of data breaches should be focused on determining the extent of the compromise and preserving the confidentiality and integrity of sensitive data that has not yet been stolen or disclosed.

Other issues affecting the selection and execution of a containment plan include your company's reputation-risk management strategy and the decision on whether to request outside assistance – either from local or federal law enforcement, a private consulting firm or a computer incident response organization such as US-CERT.

3. Begin recovery effort

After a containment plan has been established and execution has begun, get started on eradication and recovery efforts. In the case of network and system security breaches, eradication usually means removing all instances of unauthorized software from the network and disabling all access privileges associated with users who have committed malicious activity.

Cleaning a network or system of all traces of malicious code can often entail having to completely wipe all storage media and perform a "clean install." Therefore, recovery from such a breach may be resource intensive and require careful restoration of data from backups. Bear in mind that backups may also contain malicious code and should be carefully checked for compromise; otherwise, the security breach will be perpetuated after the recovery phase.

Key Disaster Recovery Principles

- *Don't wait until it's too late* – Small businesses should not wait until after a disaster to think about what should have been done to protect their data. Not only is downtime costly from a financial perspective, but it could mean the complete demise of the business. Small businesses should map out disaster preparedness plans ahead of time, including the identification of key systems, data and other resources that are critical to running the business.

- *Protect information completely* – To reduce the risk of losing critical business information, small businesses must implement the appropriate security and backup solutions to archive important files, such as customer records and financial information for the long term. Natural disasters, theft and cyber attacks can all result in data and financial loss, so small businesses need to make sure important files are saved not only on an external hard drive and/or company network, but in a safe, off-site location.

- *Get employees involved* – Employees play a key role in helping to prevent downtime. They should be educated on computer security best practices and what to do if information is accidentally deleted or cannot easily be found in their files. Since small businesses often have limited resources, all employees should know how to retrieve the businesses' information in times of disaster.

- *Test frequently* – After a disaster hits is the worst time to learn that critical files were not backed up as planned. Regular disaster recovery testing is invaluable. Test your plan anytime anything changes in your environment.

- *Review your plan* – If frequent testing is not feasible due to resources and bandwidth, small businesses should at least review disaster preparedness plan on a quarterly basis.

- *Be prepared* – It is always better and less costly to invest in adequate security up-front rather than going through a costly incident response which could result in rebuilding your entire network infrastructure.

4. Hold a 'lessons learned' meeting

Lastly, your company should always perform a "lessons learned" meeting after the recovery phase has been successfully completed to discover, document and refine the knowledge gained during the incident handling process.