Cyber Attack Response Checklist

for Small Business

Resilience
Cybersecurity & Data Privacy

THE LAW OFFICES OF
BRIAN C. FOCHT
CYBER SECURITY | CIVIL LITIGATION

Cyber Attack Response Checklist
for Small Business

Phase 1

Detection

Whenever anyone in your organization learns of or suspects a cyber attack against your company, your cyber attack response begins. Phase 1 of your response begins the moment you learn about a suspected cyber attack ("Incident"):

☐ Designate/Activate your Cyber Attack Response Manager

In addition to managing your organization's response to the potential cyber attack, as detailed below, your Cyber Attack Response Manager will be responsible for maintaining "The Book," which is a record of all actions taken in response to the cyber attack.

☐ Activate/Retain IT Support (Technical Team)

Whether it's your in-house IT employees or third party vendor, you need people who specialize in containing and eliminating malicious activity and infections. While I recommend a different vendor than the one who provides any managed services to your organization, immediate availability is of utmost importance.

☐ Designate/Retain Communication Specialists (Communications Team)

In the event of a cyber attack, you are going to need people who are able to communicate effectively and responsibly with a wide-variety of external groups, from law enforcement to potentially irate customers or clients. Depending on the size of your organization, retaining an outside PR firm may be the best choice.

Now that your team is in place, it's time to get to work!

(Continue to Phase 2)

Cyber Attack Response Checklist
for Small Business

Phase 2

Phase 2 determines whether the suspicious behavior or information is a Cybersecurity Incident. In the event it is determined that no actual penetration of your security occurred, your inquiry may end here.

Investigation

- [ ] Investigate to determine if an "Incident" occurred
  An "Incident" is any confirmed attempt to penetrate your organization's systems and does not necessarily mean there was an actual breach.

If an Incident occurred:

- [ ] Determine whether the attack penetrated your system's security
- [ ] Identify the systems that were compromised/infected
- [ ] Identify all data that was accessed, including the nature of the data and the form it was kept

Analysis

- [ ] Review all data that was accessed and categorize based on type of data and your notice obligations under applicable law

(Continue to Phase 3)

Cyber Attack Response Checklist
for Small Business

Phase 3

Phase 3 is where your teams stop the proverbial bleeding, lay the groundwork for securely eliminating any threat from your systems, and establish contact with critical individuals and organizations.

Containment

- [ ] Determine if compromise/infection can be isolated in system

If isolation possible:

- [ ] Isolate affected systems
- [ ] Back up all critical data in non-affected systems
- [ ] Create full copies of all compromised systems for future forensic analysis
- [ ] Determine whether to monitor compromise/infection to determine full scope/source
- [ ] Remove all malware from infected systems

Triage

- [ ] Notify all essential contacts within the company of the Incident and status of response
- [ ] Contact appropriate law enforcement agency/agencies to report the breach

(Phase 3 – Triage Cont. on next page)

Phase 3 (cont.)

Triage (cont.)

- [ ] File claim with all applicable insurance carriers
- [ ] Contact financial institutions to freeze transactions and/or establish method to confirm all transactions going forward

(Continue to Phase 4)

Cyber Attack Response Checklist
for Small Business

Phase 4

Phase 4 involves both the removal of threats, and all associated vulnerabilities, from your your system, as well as the critical work of notifying potentially affected persons or entities pursuant to legal and contractual obligations.

Eradication

- [ ] Determine level of intrusion, including whether intruders gained system-level access
- [ ] Eliminate all malicious activity
- [ ] Perform all processes to eliminate the infection/threat
- [ ] Review all systems and software to ensure most recent patches and updates installed
- [ ] Re-configure any systems/applications as necessary
- [ ] Identify and close all potential points of entry into the system
- [ ] Identify any new defenses necessary to protect system from further compromise

Notice

- [ ] Review all compromised data
- [ ] Determine whether any data that was or may have been accessed triggers any notification obligation under applicable law or contractual obligation

(Phase 4 – Notice Cont. on next page)

Cyber Attack Response Checklist
for Small Business

Phase 4

Notice (cont.)

- [ ] Classify all compromised data based on type of information and source of notification obligation
- [ ] Create and implement system for notifying affected persons/entities pursuant to applicable notification obligations
- [ ] Follow-up with law enforcement agencies investigating the incident
- [ ] Obtain final report of investigation
- [ ] Contact any regulatory agency with jurisdiction over your company or as required by law

(Continue to Phase 5)

Cyber Attack Response Checklist
for Small Business

Phase 5

Phase 5 is the final elimination of the compromise/infection of your systems, and return to full operations.

Recovery

- [ ] Restore system where necessary with most recent non-compromised backup
- [ ] Restore system operations, prioritizing critical operations, per pre-determined order of importance
- [ ] Initiate continuous tests on previously infected systems to monitor for re-introduction of infection
- [ ] Identify and remove all vulnerabilities exploited in the breach and/or identified during investigation

Continuity

- [ ] Establish system to maintain notice and information system as required by law
- [ ] Continue correspondence with regulatory and/or law enforcement agencies as needed

(Continue to Post-Breach Activities)

Cyber Attack Response Checklist
for Small Business

Post-Breach Activities

Once the breach has been eliminated and all parties have been notified of the breach as required by law or contractual obligation, it is necessary to both assess your organization's response, as well as determine whethe

Follow-Up

- [ ] Remain Vigilant – monitor for new attempts to attack systems
- [ ] Determine whether notice requirements or reputation damage necessitate long-term PR assets
- [ ] Review status with stakeholders, including likelihood of litigation and possible need to retain outside counsel
- [ ] Prepare analysis of organization's response to attack
  - [ ] Review response to determine needs for future attacks
  - [ ] Understand what failed, how intrusion occurred, and the steps taken in response
  - [ ] Detail new security measures in place to prevent similar incidents in future
- [ ] Conduct "Lessons Learned" Meeting with Stakeholders and Staff

Cyber Attack Response Checklist
for Small Business

There is no guarantee that any security system will ever be enough to completely protect your organization from a cyber attack. How you respond to an attack, however, is at the very core of Resilience. By following this checklist, you will help put your organization, and your clients and customers, in the best position to both survive and learn from an attack.

Resilience
Cybersecurity & Data Privacy

THE LAW OFFICES OF
BRIAN C. FOCHT
CYBER SECURITY | CIVIL LITIGATION

For Further Information Check out:

Resilience

Cybersecurity & Data Privacy

www.resiliencecybersecurity.com

Or Click Here to sign up for free cybersecurity updates.

The material educational and informational purposes only and is not intended and should not be construed as legal advice.
This communication is considered advertising under applicable state laws.
Downloading or use of this checklist does not establish an attorney-client relationship