

Computer Breach Emergency Checklist

In case you experience a breach or other cybersecurity incident, be prepared to act quickly with this **Computer Breach Emergency Checklist**.

You should print this checklist and keep it with your other emergency plans.

If you suspect that your firm has been breached:

1. Disconnect your network from the internet and, while someone does that, call your cybersecurity insurer if you have one. **Do this immediately!**
2. Disconnect any infected computers from your local network. If not sure, disconnect all your computers. You can do that by disconnecting cables at your network switch and powering off any WiFi hotspots.
3. If you have insurance, check with the insurer and connect with an approved cybersecurity incident response company and an expert cybersecurity attorney. Ask for **immediate advice** about what to do and what not to do. For example, your IT support person might want to reformat and reinstall infected computers. If you allow that, you may risk destroying evidence of what sensitive information may have been stolen and who stole it.
4. If you do not have insurance, you still need to call a cybersecurity company. Don't proceed without the go-ahead from a cybersecurity specialist. Three expert companies are suggested, below.
5. You have various legal responsibilities in the event of a potential breach of client information. Consult an expert cybersecurity attorney, not a general practitioner unless for a reference.
6. Reset every single password used by anyone in your firm. Since your computers are disconnected from the internet, you could use mobile phones to do so. Another option is to use a mobile phone as a hotspot that any uninfected laptops could connect to in order to make the changes.
7. Enable multi-factor authentication (MFA) for all internet accounts and remote control accounts such as LogMeIn, GoToMyPC, Spashtop, or my favorite, [DWService.net](https://www.dwservice.net), if you have not already done so.
8. Close any backdoors. It may not be enough to remove all the malware that is installed on your computers. Hackers may have left secret backdoors into your network. Your cybersecurity experts can track those down and eliminate them.

9. Follow the advice of your cybersecurity attorney. The attorney-client privilege can protect your consultation. The advice may include:

1. Preserving evidence of the break-in on original or cloned hard drives.
2. Notifying law enforcement authorities of the breach.
3. Contacting clients and others to warn of potential adverse effects and precautions relating to the break-in.
4. Educating your people about safe practices and warning signs.
5. Implementing better cybersecurity practices and defenses.
6. Managing the public relations and reputational aspects of the incident.
7. Take a deep breath! You will get through this with experienced providers.

For expert assistance with cybersecurity breaches and incidents, you could contact:

Procircular (procircular.com), 600 Nicollet Avenue, Suite 260
Minneapolis, MN 55402, Tel: 844/957-3287

LMG Security (LMGsecurity.com), 145 W Front Street, Missoula, Montana 59802, Tel: 406/830-3165

Sensei Enterprises, Inc. (senseient.com), 3975 University Dr., Suite 225, Fairfax, VA 22030, Tel: 703/359-0700

Note: Make sure you have a **paper copy** of the checklist or link to this post on your phone. The checklist won't do you any good if it is only on a server that's down!

Author:

Wells H. Anderson, JD, CEO, SecureMyFirm. Originally published in GPSolo eReport; Solo, Small Firm and General Practice Division; American Bar Association.