

BackGround Software Inc. Security Services



How Can We Help You?

We can help you make the experience of being a victim of cyber crime as painless as possible through following services:

- **Security Assessment Service** will help you prepare and minimize potential damages.
- We will help you determine the magnitude of impact through our **Security Breach Damage Assessment Service**. This should help you put a dollar amount to the damages that you have suffered due to the security breach.
- We will provide you with all recoverable information about the intruding party to facilitate corporate, legal and criminal prosecution of the cyber criminals through our **Computer Forensic Service**.

For more information on these services, please see the service bulletins describing each one in detail. Service bulletins can be obtained from our web site as outlined below.

Ready to start?

Please contact us to discuss your needs and how we can help you. Your security is our business.

For more information, please contact:

BackGround (BGD) Software Inc.
900 Steeles Ave West, Suite 608
Thornhill, ON L4J 8C2 CANADA
Tel: (416) 917-0130
Toll-Free: (888) 230-8320
E-Mail: sales@bgdsoftware.com
WWW: <http://www.bgdsoftware.com>
November 2002, © All Rights Reserved.

You've Been Hacked

No, do not laugh. It will happen to you, too. There is nothing to speculate about. It is a fact. You **will** be subject of cyber crime. Regardless of how good you are. Regardless of how careful you are. Regardless of anything that you may or may not do, it will happen to you.

Most organizations are not willing to even discuss the topic, let alone face the fact that they will lose their assets due to the illegal computer activities. So, one may argue that "resistance is futile" and that it may be cheaper not to do anything as opposed to try and fail. Wrong on all counts. Let's lay down some facts.

- 1) First, you need to admit to yourself that you will be a victim of cyber crime, if you have not been one already.
- 2) Then you have to do everything possible to make that experience as painless as possible.
- 3) After all that can be done is done, brace for impact.

If you accept the three outlined steps as reality, you stand a good chance to survive in the cyber space. On the other hand, should you choose to ignore these truths, you are in for the rude awakening.





Computers on the Internet: How Do We Manage That?

Let's examine options that you have:

- 1) Buy computer equipment from the computer manufacturers that consistently address security issues in their products. Good indication is to always put ear to the ground on many newsgroups for comments on a specific hardware or software product. Do not talk. Just listen for a while what others are saying and you will soon have a much clearer picture about the certain product. For brand new products, usually (unlike mutual funds) past performance of the manufacturer is a clear indication of future expectations.
- 2) Carefully choose, educate, test and license system administrators that are going to be managing and maintaining your computer systems that will be attached to a public network. The best car with an average driver will still go off the road in a first dangerous curve.
- 3) Lobby your government to introduce new laws that would make the computer security mandatory for all public and private corporations as well as government agencies. It should be a direct responsibility of the board of directors to ensure computer security for their electronic assets, the same way that it is mandatory to wear a seat belt when driving a car. It could be anyone in the vehicle that does not wear a seat belt, still the driver gets a ticket, if stopped by

the police. Hence, if the board of directors and CEO were personally liable for their corporate security mishaps, they'd make pretty sure that their corporations are secure.

- 4) Buy network equipment and services from the manufacturers and suppliers that make products that accommodate safety as well as throughput of network traffic. Lobby all your business partners to do the same. The link between you and your electronically-connected partners is as secure as the weakest link between you. Network.
- 5) Insure both computer systems and data that resides on them for all the systems that have a potential exposure to the public network. Make sure that you know what both are worth to you and your customers and partners, so that you can buy insurance in adequate quantity.

Well, technically speaking, that's it. But in reality, there is a bit more to it. You should also get ready to experience the inevitable. That sour, "We've been hacked" feeling.

The preparation for it will help you enormously. The same way you fare better in a car accident, due to the improved quality and technology used to make the vehicle that you are driving, the use of seat belts, air bags, active crumple zones, your driver training, road surface that slows you down faster and insurance to cover the expenses.

If you prepare carefully, you will have less things to worry about, and chances are that when you do experience the inevitable mishap, you will be able to survive it, be up and running in no time and remember it as an anecdote for a while.

Anecdote or not, when the disaster happens, you need to always remember some elementary steps that need to be taken.

Computer Security Incident Steps	
1)	Stay calm and stay in your data center until you determine the impact of the security breach. Disconnect your server(s) from the network.
2)	If there is a potentially malicious code running, disconnect media devices as quickly as possible (i.e. disks, SAN, NAS).
3)	In case that data has been compromised, call the data owner to start data verification and execution of business contingency plan. Also business damage containment, if applicable (for example if the credit card numbers have been stolen)
4)	Report the accident to the police and insurance company as soon as possible.
5)	Do not touch anything on the systems that have been attacked until the computer forensic experts have examined them.
6)	Get as much as possible information on parties that may have been implicated with the security breach, network provider logs, system logs, firewall logs, intrusion detection system logs, etc.
7)	Let your server(s) either be fixed (if it is a minor incident) or replaced by a loaner for time being.
8)	Go on with your life.

