

Security Services

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. There are two types of corporations today. The ones that have already fallen victim to cyber criminals and the others that will soon.

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.

Car or Computer Accidents Happen

The concept is pretty much simple.

Cars = Computers.

Just like that. In the beginning, there were a few cars on the roads. The accidents were few and far apart. It really was not a problem. It was hard to believe that anyone could really get hurt at the speeds of 10 miles per hour, when there was a single engine powered cart in the whole county. But, as with any genial concept as that, the progress took its toll. The people soon developed, bigger, better, faster cars. Lots of them. All of a sudden, people started killing each other with the weapon of choice. Car.

Same thing happened to another technological miracle. Computer. There were only a handful of systems connected to a university network in the beginning. Good guys only.

But then, corporations outside universities picked up the trend. Then the common folk got the magic box. Computer became the piece of furniture as standard as a telephone. Then those people hooked up in a nuclear-catastrophe-survivable-network called Internet. All of a sudden, as with the cars, people started attacking each other with newest weapon of choice. Computer.

Now, since the automotive industry has had a bit of a head start, we should look for valuable experiences to learn from them. How did the society react to a new threat created by production of new, lethal weapon, such as a motor vehicle?

Cars: Managing the Risk

Simple. Society has managed the risk. The cars are far too valuable to abandon the concept over the risks that they bring. We have simply learned to live with it. Although, some adjustments were necessary:

- 1) Every year, car manufacturers work hard on producing safer vehicles through introduction of seat belts, air bags, rigid body cages and crumple zones.
- 2) Learning process was introduced to educate, test and license drivers.
- 3) New laws were introduced to make the wearing of seatbelts mandatory.
- 4) Road builders have introduced new road geometry and surfaces to accommodate safety at higher speeds.
- 5) Insurance of both vehicles and passengers is mandatory almost everywhere in the world.

Joint effort has resulted in acceptably safer, but not fool proof system. Car accidents still happen. We all accept it, knowing that everyone has done the most that they could to prevent the fatal outcome.

Computers on the Internet: How Do We Manage That?

So, let's learn something from this example and make living with Internet, an acceptable risk.

What do we, as a society, need to do, is similar to our car example:





- 1) Every year, computer manufacturers should work hard on producing safer systems through introduction of secure operating systems, thoroughly tested and bug-free software and compatible, manageable components.
- 2) Learning process must be introduced to educate, test and license system administrators of any computer system that is attached to a public network.
- 3) New laws should be introduced to make the computer security mandatory for all public and private corporations as well as government agencies.
- 4) Network equipment manufacturers must introduce products that accommodate safety as well as throughput of network traffic.
- 5) Insurance of both computer systems as well as data that resides on them should be mandatory for all the systems that are attached to the public network.

So, what can you do?

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 the 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.



Security Services



<i>Car Accident Steps</i>	<i>Computer Security Incident Steps</i>
1) Stay calm and stay in your vehicle until you determine that you have not been injured. Turn engine off.	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 fire, evacuate all passengers as quickly as possible.	2) If there is a potentially malicious code running, disconnect media devices as quickly as possible (i.e. disks, SAN, NAS).
3) In case of anyone being injured, call the ambulance immediately.	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.	4) Report the accident to the police and insurance company as soon as possible.
5) Do not move vehicles before the police surveys the scene	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 other driver(s) and vehicle(s) involved, witnesses, insurance policy numbers, weather conditions, location, etc.	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 vehicle be towed into the shop to either be fixed (if it is a minor accident) or replaced by a loaner for time being.	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.	8) Go on with your life.

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
 EMail: sales@bgdsoftware.com
 WWW: <http://www.bgdsoftware.com>
 November 2002, © All Rights Reserved.