


BackGround Software Inc. Computer Forensic, Security Breach Damage Assessment



minimize the impact of the security breach as well as determine the extent of the damages caused by it. It is not possible to predict accurately what the amount for such service would be, as it depends on the individual security breach nature and resources necessary to determine the extent of the damages. As a general rule of thumb, you can estimate that such an engagement would cost approximately \$20,000 per server involved.

What will you get for your money?

- All deliverables as described for Computer Forensic Service.
- Report on estimated cost of all system components that need to be verified, fixed, rebuilt or replaced (in terms of hardware, software and labor)
- Report on estimated cost of all compromised data resources (in terms of common market value of such data, third party and/or customer value and labor required to recover, fix, rebuild or replace such data)
- List of business services and time line of interruption
- Report on estimated cost of each disrupted business service for the time that it was unavailable.
- Report on estimated cost of all resources engaged in the Security Breach Damage Assessment activity.
- Our support throughout the process, including communication with the authorities and all the way up to the legal process to recover damages.

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.

Morning Discovery

It's an early morning. You have just put down your freshly brewed cup beside the keyboard. You try your email. It does not work. You try file server. It does not respond. You manage to log into the database server. Memory usage: very low. CPU usage: almost none. Check the file system. 98% available. The phone rings. You can hear other phones on the operations floor ringing at the same time. Then it hits you. You have been HACKED. Not just hacked, you have been taken to the cleaners. Everything is gone. Everything.

You've Been Hacked

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, admit to yourself that you will be a victim of cyber crime, if you have not been one already.
- 2) Then, do everything possible to make that experience as painless as possible.
- 3) 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.

So, what can you do when you find out?

Generally speaking, here are a few steps that you should follow in case of the security breach.

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. |

In the case that you are dealing with the already happened security breach, the steps 1 and 2 should be done as soon as possible, although it may seem that it is too late. You never know how far the intruder has managed to get, so the faster you disconnect the equipment the more of a chance you have to

save your data. You should start with the most important servers/storage first.

So, what can you do after the fact?

- Try to remember all the steps that you have done and document them in a time line.
- Communicate with the implicated business owners and proceed with the Business Resumption/Continuation Procedures (BRP/BCP) as outlined in your Disaster Recovery (DR) plan.
- Contact an independent consultant to arrange for the Computer Forensic service and Security Breach Damage Assessment to be done.

Computer Forensic Service

We will track the intruders and follow their network trail based on number of traces that they may have left. Even no network trace is a signature of the attacker in some way. Modus Operandi (MO) of certain individuals will be consistent and even lack of network trail of the attacker, in combination with the compromised system status and type of the organization being targeted, may be enough to profile the criminals and get the authorities on the right track.

How much will it cost?

The Computer Forensic service is Time & Materials (T&M) engagement where our consultants will work closely with your technical staff to analyze particular system for certain types of actions. In case of the security breach it will address all the actions that intruder might have performed in order to penetrate the organization security. As a general rule of thumb, you can estimate that Computer Forensic service related to the security breach would cost approximately \$8,000 per server involved.

What will you get for your money?

- Intruder entry path report (initial engagement)
- Intruder inside path report (security breach log)
- Intruder exit path report (disengagement)
- Analysis of the probable intruder target
- List of the resources touched
- List of the resources compromised

Security Breach Damage Assessment

We will do the following:

- 1) *Computer Forensic Service* as described above.
- 2) We will work with your business owners to determine the business impact of determined technical difficulties directly or indirectly caused by the security breach. For example, we will put a dollar amount to front desk customer service being unavailable while the servers were off-line due to the breach in security.
- 3) We will work with your legal counsel to determine the most appropriate approach to recover lost dollars, through a fixed, fact-based amount to be used as a claim for damages suffered.
- 4) We will assist your business owners in executing the damage control plan, to limit the impact of the compromised data (for example, compromised credit card numbers should be communicated immediately to the credit card company and the credit card owner).

How much will it cost?

The Security Breach Damage Assessment is Time & Materials (T&M) engagement where our consultants will work closely with your technical, business and legal staff to