



PREVENTING DATA BREACHES GUIDE

HOW TO PROTECT VALUABLE IDEAS AND ASSETS
FROM CYBER-HACKING

LOREDANA BOTEZATU, IOANA JELEA
E-THREATS ANALYSIS AND COMMUNICATION SPECIALISTS

SMALL AND MEDIUM ENTERPRISES



Table of contents

- Table of contents.....2
- What motivates a cyber-hack?3
- How does a cyber-hack happen?4
- What are the risks a cyber-hack poses?.....7
- How to stay protected8
- Employees and Security*8
- Physical Access to the Company Building*.....9
- Laptop vs. Desktop*10
- Encryption and Backup10
- Use of Network Resources*.....11
- Advanced Firewall11
- Application Control.....12
- Security Compliance*12
- Updates*13
- Removable Devices*13
- Mail Server*14
- Company's Web Site*15
- Physical Network Security*16
- Conclusion17

What motivates a cyber-hack?

Today's business environment can hardly be imagined as fully functional without a connection to the Web and indispensable applications such as e-mail, instant messaging, voice over IP, Web sites, and file servers.

Securing this type of communication must be a key concern for all companies, regardless of their size or main activity. Security incidents can occur pretty easily unless a few steps are taken in due time and the employees are properly instructed on the damage they may be causing while poorly handling the sensitive information of the company. Needless to say that when a company becomes the victim of an e-threat, its business partners will suffer as well.

Cybercrime has become a very prolific line of business and its practitioners fuel their high-impact efforts on very strong motivations.

Public recognition – This need drives cybercriminals to exploit the known vulnerabilities of various Content Management Systems (CMS) and to forcefully display their logo or screen name on the defaced web sites. This kind of attack is a moderate threat, which means that the affected Web site/organization would only lose credibility and some working hours in order to restore things to normal.

Money – Hackers will try to gain control over a specific Web site and exploit it for financial advantages by seizing the following resources:

a) Members' profiles stored in a CSV (Comma Separated Values) file. E-mail addresses are valuable commodities in the spam industry, while personal data (such as credit card credentials) will be used for identity theft and e-banking fraud.



b) FTP servers can host malware or carbon copies of banks' Web pages to be used in phishing schemes. Once on the server, cyber intruders may infringe upon the company's intellectual property by copying confidential code, binaries or even the Web site itself.

c) Access to the Web server allows hackers to send tremendous amounts of unsolicited messages without taking the ensuing legal liability. In the end it's all about cash and financial power, with the hacker on the winning side and the targeted company on the losing one.

d) Another compelling means of extortion is threatening businesses with DDOS attacks. This is how the blackmail scenario goes: unless the company pays a specified amount of money, its Web page will be automatically flooded with access requests which the Web server will be unable to answer and would cause it to collapse. In the meantime, the company loses potential customers and, implicitly, money.

Cyber-warfare – Various political, economic and religious organizations may recur to DDOS attacks, for instance, to reduce opponents to silence or to throw them off balance and, ultimately, to send a message to whomever may be at loggerheads with them.

How does a cyber-hack happen?

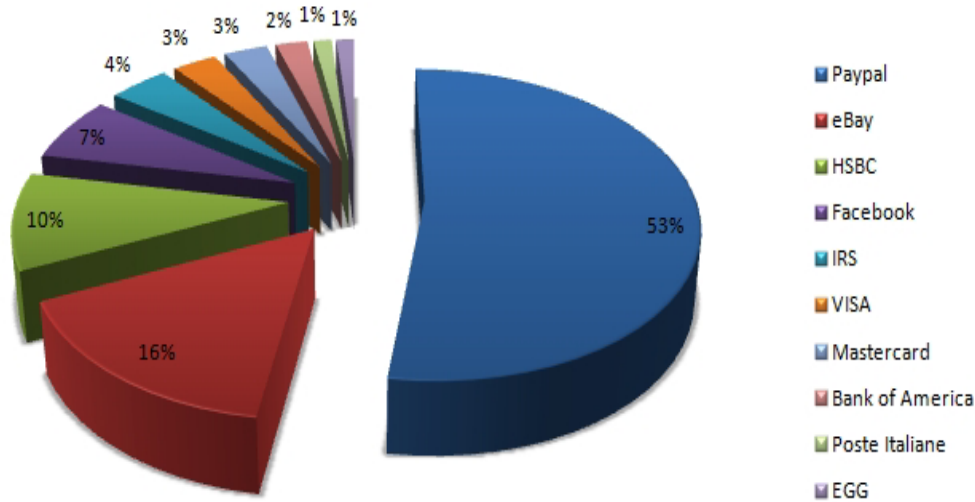
Depending on their identified source, cyber threats could be separated into two major categories:

1. Insider negligence – this accounts for roughly 78 % of the total number of data loss incidents. Two major subcategories fall under this heading:

- *Human error* – this is a multi-faceted e-plague:



- employees can lose or delete important information by mistake;
 - they can inadvertently give away sensitive data to people who can benefit from it;
 - they can leave the desk without locking their workstations and someone else can use a flash drive to steal important data or infect the system;
 - if employees use default passwords their exposure to illicit system accessing and data theft increases considerably;
 - something as simple as forgetting doors unlocked is also a hazard as anyone could enter the office and steal confidential data or even computer units;
 - open ports may grant unauthorized persons access to sensitive information;
 - involuntary malware infestation via removable drives or direct downloads from the Internet put the whole network at risk, especially if employees willingly or unwillingly disable the antivirus solution installed on their machines.
- **Hardware theft (or loss)** – several scenarios are possible:
- unsupervised equipment can be stolen from the company;
 - employees can misplace material goods such as back-up disks or external hard-drives which, as a rule, are not to be stored in public locations;
 - laptops and telephones can easily be stolen and lost along with all the sensitive data stored on them.



Top counterfeit identities exploited in phishing raids during the first half of 2010, according to BitDefender H1 2010 E-Threats Landscape Report.

2. Malware attacks represent a mere 6 % of the total data loss incidents. Even though the figure is not that impressive, targeted malware attack incidents can cause companies much more damage than hardware failure or human error.

Financial departments need to take great care when it comes to various online bank transactions in order to protect themselves from the infamous Banker Trojans, for instance. Unlike conventional keyloggers that are able to intercept and send each and every key the user presses while in front of a computer, Banker Trojans are especially written pieces of malware that have a sixth sense: they remain dormant most of the time and only wake up when users point their browsers to bank sites the malware is instructed to monitor. When they see it, they perform miscellaneous tricks to intercept the entered credentials and then report back to the base.

It is this extra level of stealth that makes the Banker Trojan awfully difficult to detect: it eliminates the amount of overhead a keylogger would place on the network card by constantly transmitting the intercepted data via Internet. Moreover, since it only collects a couple of bytes of data per session, it is able to send these credentials using post or get requests to the attacker’s Web site.

These malware design efforts are well justified given that they allow stealthily accessing and preying upon companies' financial resources. Phishing and spam opening the way for phishing are still going strong as well. According to the [BitDefender H1 E-Threats Landscape Report](#): “During the first half of the year, financial institutions were cyber-criminals’ preferred targets, with more than 70 percent of the global phishing messages.”

What are the risks a cyber-hack poses?



While hardware failure, human error and random notebook, HDD or computer theft would prevent the company/user from exploiting data and systems, targeted malicious attacks and insider sabotage would also impact on the company's image and backfire into a series of exorbitant lawsuits.

Fraud, identity theft, impersonation, unfair competition and sabotage (campaigns, new product launches) are only a few of the possible cyber wrongdoings a company might suffer from. As a rule, the cost of an incident is proportional to the value of the data proper plus the collateral damage, such as credibility loss, operational loss and even a class action lawsuit against the victim company.

Having customers' records stolen, for instance, can trigger a daisy-chain reaction where not only the company gets hurt, but also its past and current business partners. All the info present in a company file - client's contact details, a history of bank transactions - is enough for someone with a hidden agenda to take on a false identity and to cause great financial losses that may lead to the victim going bankrupt.

To give an example, in May 2008, a human resources and recruitment company fell victim to a burglary and lost its physical records that contained sensitive information on a major company's employees hired prior to 2006. Unfortunately, the HR company had not used encryption methods to secure the personal documentations of the candidates examined on behalf of various company clients, losing credibility, clients and money. Ultimately, the company went bankrupt and ceased its activity within three months of the incident.

How to stay protected



Employees and Security

There are two key elements in this equation: raising awareness among the employees about data security measures and making them aware of their individual responsibilities in the process of securing the company's computer-based operations against attacks. That is why it is mandatory for all employees to be trained at least once a few months by a security specialist.

In addition to that, employees' control over the antivirus settings should be limited, given the fact that they may be tempted to disable or uninstall the antivirus protection for better system speed or in order to gain access to a blocked, harmful resource.

Other resources that should be closely monitored are social networks and instant messaging services. Sometimes, classified information can be leaked unintentionally by employees through social network profiles or even through personal blogs. Some of the most frequent details that go public ahead of time are product launch dates, product screenshots or other branding elements such as logos and boxes. One of the means to mitigate this problem is for employees to be provided access to critical data on a need-to-know basis and for fragmentation of information to be encouraged.

Another simple thing that might save companies a lot of trouble is the requirement that each computer have a personal password, known only by one user and/or a biometric authentication module. Furthermore, this password should be changed regularly. The use of a token would be a good alternative in this particular situation.



Physical Access to the Company Building

The aspects covered in this section are the employees' e-mail accounts, work phone numbers, access badges, and passwords.

Access to the company building should be limited and directly supervised by qualified security staff. There are various stratagems some third party may resort to in order to trick an employee into letting him inside the building. One of the most common scenarios has the attacker hands full of boxes waiting for a so-called delivery. As soon as an employee swipes his/her badge over the access control device, the attacker would ask that employee to hold the door for him. In this way, the employee will let an unauthorized person inside the building without supervision. Within minutes, the attacker may leave with a mobile backup device, paper records or other classified information.

An employee's privileges ought to be terminated once that person no longer works for the company. This prevents former employees from communicating with a client or partner using the company logistics, and impersonating a current, well-intended member of staff.

If a former employee is still able to use the work telephone number, the work e-mail account, the access badge, he/she would have all the necessary means to send messages aiming at discrediting the former employer, stealing clients, sabotaging a campaign or causing any other harm fueled by frustration.

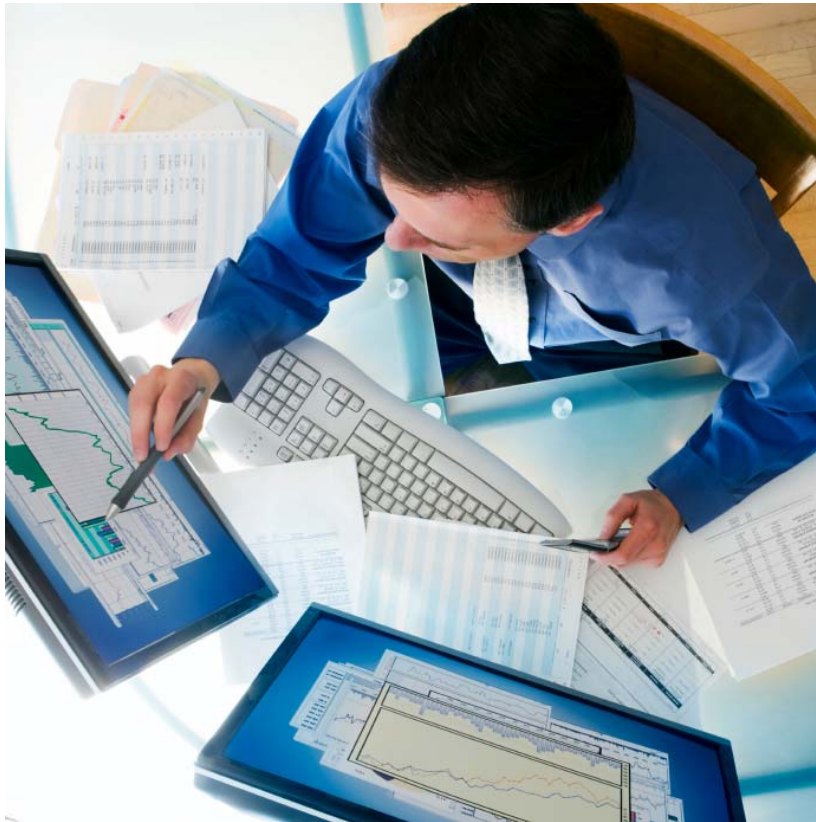
Laptop vs. Desktop

Encryption and Backup

As mobile stations are easy to move around and take home, chances are that they are lost or misplaced. Consequently, sensitive data may get in the wrong hands, especially since mid-range laptops and average ultra-mobile PCs may not have any built-in hardware encryption feature. That is why, whenever possible, these devices should be protected with a hardware level password preventing unauthorized access and use of the information stored on them.

Small businesses will most probably not have a full time IT specialist, so that it is recommended for them to hire an IT company to configure automated backups and regularly ensure that these operations were performed correctly.

In the case of very small networks, a possible security solution to this particular problem might be the use of **BitDefender Internet Security** or **BitDefender Total Security**, two data security solutions for individual computers that can be successfully used to protect workstations in any small office or home office (SOHO). What makes them especially efficient, in this context, is a new feature called *File Vault* – a location on the hard disk drive encrypted using military-grade standards, and able to accommodate as many files as the local hard-drive can store. The *Online Backup* feature stores these files on a remote, highly secured server, from which they can be retrieved by typing in a password. In this way, the files will be available even if the laptop has been stolen or destroyed by accident.





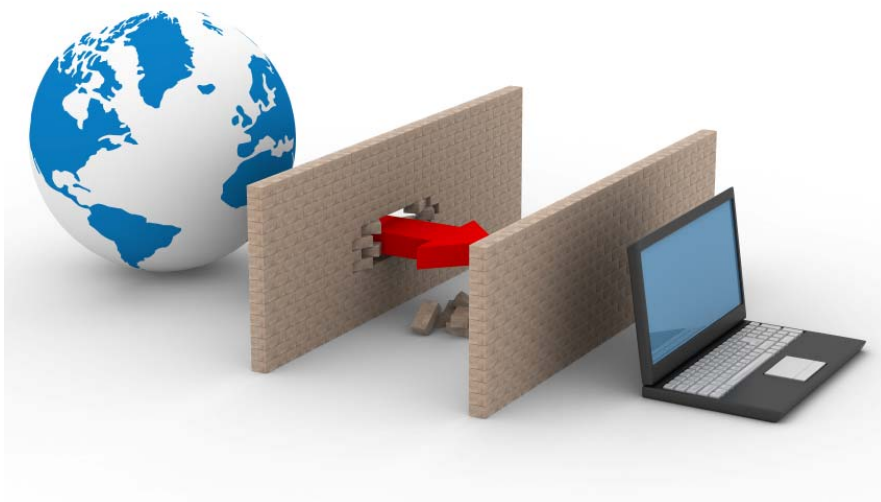
However, Small and Medium Businesses (SMBs) with over 10 workstations should establish their local backup procedure to ensure all critical user data can be accessed and recovered within the business premises. For such networks, *BitDefender Business Solutions* might be the answer. Their remotely configurable and automated backup features ensure that the selected user data will be backed up regularly to the centralized backup repository. These solutions allow managing networks and computers zones in order to identify the proper settings for trusted networks (such as the local area networks at the office), and to pinpoint unsecured wireless hotspots as posing a higher security risk.

Remote access to the organization's information resources or e-mail services can also be protected by using a cryptographic tunneling method known as Secure Virtual Private Networking (VPN). Secure VPN services ensure the confidentiality of business information and make it safe to use otherwise unsecured connections at home or public wireless hotspots.

Use of Network Resources

Advanced Firewall

Windows workstations are not set by default to prompt users to allow applications to connect to the Internet in order to transmit data to external servers. *BitDefender Client Security* enables full control over applications' access to Windows Registry, automated application start-ups, and the listing of applications allowed to use network connectivity. In this way, the applications generating the current network activity are easy to check in order to make sure that no malicious software is working in the background and transmitting sensitive data to external servers.



Application Control

Additional security features present in the BitDefender Business Solutions allow the remote monitoring and management of applications installed on workstations so as to prevent prohibited software (such as Peer-To-Peer file sharing) from running within business networks.

Further on the application control front, with the *BitDefender Endpoint Auditing and Management Scripts* network security reporting becomes more transparent as network administrators can remotely identify all installed applications as well as control, terminate or uninstall running applications. These features help save IT staff's time and prevent malicious code from entering companies' networks.

Security Compliance

As their name says it, mobile stations will frequently get in and out of the network, which might be problematic as far as compliance with the overall security policies is concerned. BitDefender Business Solutions provide system administrators with the possibility of setting and centrally managing security policies that will be automatically deployed on mobile stations once these stations are reconnected to the network. In this way, their freedom of movement is unhindered, while the same level of data security is maintained throughout the entire network.

Updates

The reliability of a security solution's updating system is a key element to be considered when SMBs choose how to protect their data and network. The BitDefender Business Security Solutions, for instance, not only rely on hourly updates with the latest virus signatures, but also enable network administrators to deploy updates and monitor the update status of the entire network easily, in a centralized way.

Removable Devices

The use of removable storage devices, such as hard-disk drives, flash drives, and memory cards is of great interest when approaching data security within company networks, as almost anyone has access to them. These devices need to be frequently scanned for malware, preferably each time they are connected to the computer, as they are known to be the main infection vector within business environments. To keep troubles pouring on, worms may open the door to other categories of malware, including Trojans and viruses which will spread throughout the company network and cause it to be exploited by third parties for commercial or financial gain.

To help prevent these security issues BitDefender automatically detects when a removable storage device is connected to the computer and offers to scan that device before the user accesses its files. With BitDefender Business Solutions removable device scanning policies can be remotely configured and enforced to ensure users will not skip the scanning either as an act of negligence or in the intent of saving some time. Some organizations may even want to disable auto-runs on removable devices or completely block removable USBs, two features that BitDefender supports through centralized management policies.



Mail Server

The company's mail server is one of the most sensitive links to "the outer world", including the customers. New business opportunities, accounts, sales reports, newsletters, and confidential attachments act like honeypots for cyber-criminals, who might force their way through poorly secured mail servers. Inefficient or inexistent antispam filters on the e-mail server might open the doors to significant amounts of unsolicited messages bundled with various e-threats. Moreover, outsiders might also use these servers to send spam on the company's behalf, which would dramatically impact on the company image and level of customer trust.

BitDefender offers award winning anti-spam and antimalware protection for the mail traffic passing through any Windows or UNIX-based mail servers. These solutions protect against directory harvesting attacks (DHA) and combine excellent core security features (antivirus, antispymware, antiphishing) with specific mail protection features (antispam, attachment and content filtering). Content filtering prevents data leakages by setting limits for e-mail attachment size. E-mails can be scanned based on a number of predefined rules or keywords to prevent sensitive information (such as credit card or account information, report names or client databases) from being transmitted outside the organization. The antiphishing features can recognize techniques redirecting users to a seemingly legitimate website in order to harvest sensitive company information. With all of these tools in store, the BitDefender data security solution dedicated to mail servers increases business productivity, reduces network traffic and prevents the loss of confidential data.





Company's Web Site

Since most small-scale businesses do not have a dedicated IT development team to build the company's Web site from scratch, they will rely on free, open-source content management systems, such as Wordpress®, Drupal® or Joomla®, to name only a few. The downside of using these systems is that everyone has access to the project's source code, which allows potential attackers to look for coding flaws and other vulnerabilities in the Web site's structure.

Amateur Webmasters usually fail to correctly deploy and patch their content management systems, which turns up to be extremely helpful to criminal entities set on breaking in and taking over.

Unlike the corporate environment, where system administrators check their infrastructures at least on a daily basis, average computer users having set up domains don't realize that their Web sites have been hacked into until their Webhosting providers notify them. This is usually a long process: Web-hosting providers are initially notified by tech-savvy computer users or by independent organizations such as StopBadware.org. As soon as they receive an official complaint about security incidents, Web-hosting providers would attempt to contact their affected customers before suspending their accounts. The process may take weeks or even months (assuming that these unwary offenders are spotted after all), and during this timeframe, criminals may keep exploiting the affected resources in their favor.



Cross-site scripting, code insertion and SQL injections are only a few of the threats associated with Web site hacking. While cross-site scripting and iFrame insertion would only impact on visitors, SQL injections might expose customer sensitive data such as their address, history of banking transactions (along with credit card information) and e-mail addresses. Should the Web site fall victim to a hacking attack, it is mandatory that the Webserver be taken down for further investigation and that all the exposed customers be announced about the potential dangers they are exposed to.

Physical Network Security

Physical network security is also a key element in protecting the company's proprietary information stored on systems and file-servers. For instance, routers and switches should never be placed in rooms that are accessible to everybody, since any unauthorized user may tap into open hardware ports and browse throughout the LAN (Local Area Network) shared resources.

Most SMBs have at least one wireless router deployed as a means of cutting down on network design and wiring costs. These routers and access points are delivered either completely unprotected, or protected by a default password, which would allow an attacker to sniff traffic or tap straight into the company's network without even having to breach the firewall. Enhanced protection with encryption algorithms, like Wi-Fi Protected Access (WPA/WPA2), must be enabled on the wireless routers and the default passwords must be changed.

Conclusion



To put it simply, data security within company networks should be taken very seriously. Leaving workstations, critical servers or networks unprotected equates leaving an open door to welcome anybody into your office and to the organization's confidential information.

The theft of companies' proprietary procedures and information is an extremely expensive risk and the ensuing losses could be irremediable. Unfortunately, most companies do not report data thefts in order to preserve their customers' trust. This is by far the most unproductive step to take since it gives the cyber criminals the time to exploit their leverage on the exposed customers as well.

Aside from proper reporting and cooperation with the competent authorities, one of the reasonable actions to be taken would be the setting up of data safety, risk management and loss recovery strategies so that contingencies are handled as rapidly and as efficiently as possible. A good start in what seems to be an elaborate company e-safety strategy is installing a reliable antivirus solution.

In the absence of these basic requirements for a safe operation in the virtual world, business strategies can be sabotaged, confidential information about new products may be posted on the Internet, clients and partners can be exposed to unnecessary risks, while information subject to professional secrecy can end up into the hands of the competition. Money, time and trust are lost all because important data safety elements have been overlooked. That is why they say that it is far better to prevent than to cure!

The information and data asserted in this document represent the current opinion of BitDefender® on the topics addressed as of the date of publication. This document and the information contained herein should not be interpreted in any way as a BitDefender's commitment or agreement of any kind.

Although every precaution has been taken in the preparation of this document, the publisher, authors and contributors assume no responsibility for errors and/or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein. In addition, the information in this document is subject to change without prior notice. BitDefender, the publisher, authors and contributors cannot guarantee further related document issuance or any possible postrelease information.

This document and the data contained herein are for information purposes only. BitDefender, the publisher, authors and contributors make no warranties, express, implied, or statutory, as to the information stated in this document.

The document content may not be suitable for every situation. If professional assistance is required, the services of a competent professional person should be sought. Neither BitDefender, the document publishers, authors nor the contributors shall be liable for damages arising here from.

The fact that an individual or organization, an individual or collective work, including printed materials, electronic documents, websites, etc., are referred in this document as a citation and/or source of current or further information does not imply that BitDefender, the document publisher, authors or contributors endorses the information or recommendations the individual, organization, independent or collective work, including printed materials, electronic documents, websites, etc. may provide. Readers should also be aware that BitDefender, the document publisher, authors or contributors cannot guarantee the accuracy of any information presented herein after the date of publication, including, but not limited to World Wide Web addresses and Internet links listed in this document which may have changed or disappeared between the time this work was written and released and the moment it is read.

The readers are entirely responsible to comply with all applicable international copyright laws arising from this document. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of BitDefender.

BitDefender may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from BitDefender, this document does not provide any license to these patents, trademarks, copyrights, or other intellectual property.

Copyright © 2010 BitDefender. All rights reserved.

All other product and company names mentioned herein are for identification purposes only and are the property of, and may be trademarks of, their respective owners.