



Your Business Secure

**Back to Network Basics:
Prepare before the disaster occurs**

Submitted by: Marcia Mealy

Date: September 5, 2005

Table of Contents

Abstract	2
Introduction.....	2
Action Plan for Businesses	4
Communication.....	4
Creating a Disaster Recovery Plan	5
Securing Data and Utilities	5
Protecting Your Assets	5
Conclusion	6
Works Cited	7

Abstract

Symantec's Internet Security Threat Report shows that attacks are rising. Making sure that your networks are guarded against the above "Perceived Threats", and other threats, such as crackers and Cyberattacks, can help ward off un-natural disasters such as lawsuits, loss of integrity, loss of revenue, loss of market share and information thief.

Prepare before the disaster occurs, which should include a disaster recovery plan that is customized to include your unique situation. This paper is directed more so to small businesses. Many businesses today depend on their network and the Internet to conduct business. Therefore, it is very important that Network Professionals keep the system up during a disaster. If you have not done so before, create a disaster recovery plan.

Back up your critical information, using the Grandfather/ Father/ Son method, which consist of one daily backup (Son), one weekly backup (Father) and one monthly backup (Grandfather). Electricity is absolutely essential to your office network. Without it, (electricity and / or your network), your company may be permanently out of business. Protect your networks systems investments, by making, sure that you carry disaster insurance to cover your losses. You should also carry business interruption and service interruption insurance, for instances when your system is down for a long period of time. A good business interruption policy would include contingent business interruption, extra expense coverage, and service interruption coverage. Furthermore, make sure that the policy covers blackouts and cyberterrorism attacks.

Introduction

In response to a possible threat of terrorism, the US Naval War College and Gartner, Inc of Stamford, Connecticut, conducted an exercise "War Game" in July of 2002, to determine if a cyber-terrorist attack could successfully bring down the Internet. They concluded that a successful "Cyberattack" could occur, but it was unlikely, due to the expense (\$200 million) and the length of time to organize the attack (5 years) and the fact that it would have to be sponsored in a hostile country. Moreover, it would take a core team of 20 individuals, who would have to recruit and orchestrate the entire operation that would devastate the four critical infrastructures, telecommunications, the Internet, electrical facilities and financial services.

In addition, Information Technology professionals at manufacturing, service, technology and other industries responded to a survey in which 55% believed that there would be a major cyber attack against the four critical infrastructures within the near future.

Symantec's Internet Security Threat Report for 2002 shows that attacks on Power and Energy companies are rising. Moreover, moderate and high severity threats are

becoming the most prevalent of the new vulnerabilities. Furthermore, the report makes the following disturbing statements on Security trends:

Cyber Attack Trends¹

- Eighty-five percent of all attacks reported during the past six months were classified as pre-attack reconnaissance, while the remaining 15 percent were classified as various forms of exploitation attempts.
- Companies averaged 30 attacks per company per week over the past six months, as compared to 32 attacks per company per week during the prior six-month period.
- Power and Energy companies show the highest rate of both attack activity and severe event incidence. In addition, the Financial Services sector experienced an elevation in overall attack volume and severe event incidence.
- As a country's Internet usage grows, the potential for compromise grows; this is illustrated by the rise in incidents from countries like South Korea, where incident reports grew 62 percent over the previous six-month period.

Vulnerabilities Trends

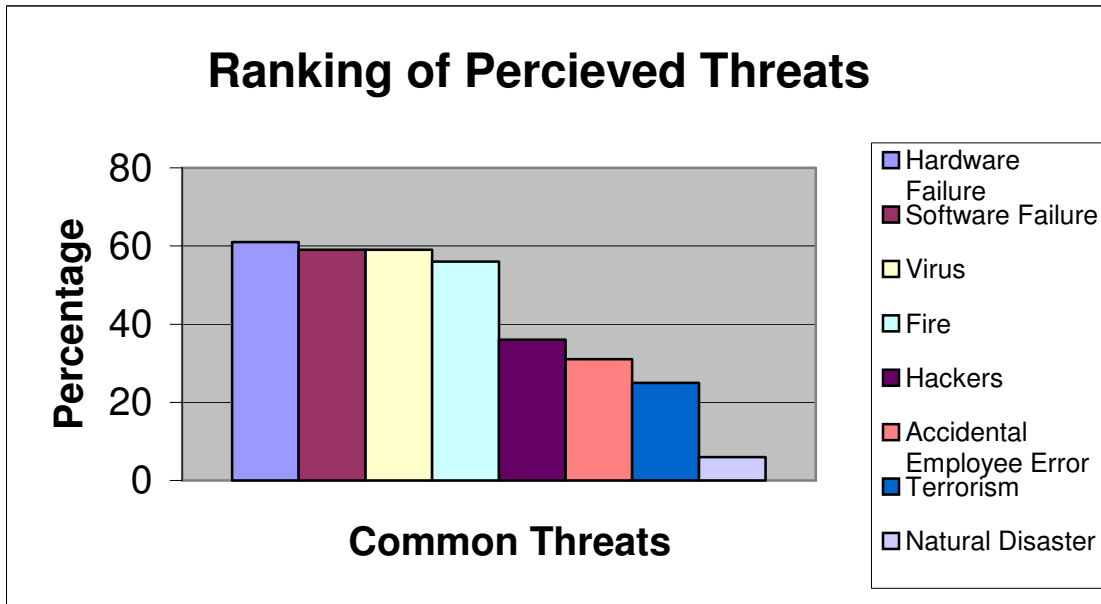
- Moderate and high severity threats drove the growth of new vulnerabilities.
- The relative ease with which attackers are able to exploit new vulnerabilities remained unchanged over the past year. Approximately 60 percent of all new vulnerabilities could be easily exploited either because the vulnerability did not require the use of exploit code or because the required exploit code was widely available. However, of the subset of vulnerabilities that required the use of exploit code, only 23.7 percent actually had exploit code available in 2002, as compared with 30 percent in 2001.

Malicious Code Trends

- Blended threats, continued to constitute the most frequently reported threat. Blended threats combine the characteristics of viruses, worms, Trojan horses, and malicious code with server and Internet vulnerabilities to initiate, transmit, and spread an attack.
- Eighty percent of all malicious code submissions were caused by only three blended threats: Klez, Opaserv, and Bugbear. Further, 78 percent of all cyber attack activity detected by Symantec was related to both old and recent blended threats.

With the emergence of new more malicious and vulnerable tendencies, there is an increased probability that more business networks will be affected in the near future. However, per a survey of 877 IT managers conducted by Dynamic Markets Ltd in 2003, Cyberterrorism (terrorism) did not rank high on their list of common threats. The following graph shows results of how the IT managers ranked perceived threats on the survey. Software failure and viruses ranked at least twice as high as Cyberterrorism. Businesses do not seem to connect the link between securing their entire Information system for more than viruses as a means to fight Cyberterrorism.

¹ [Symantec Internet Security Threat Report Sees Sharp Increase in Reported Vulnerabilities but Drop in Overall Attack](#). (Symantec Corp. 2003)



Making sure that your networks are guarded against the above “Perceived Threats”, and other threats, such as crackers and Cyberattacks, can help ward off un-natural disasters such as lawsuits, loss of integrity, loss of revenue, loss of market share and information thief.

Action Plan for Businesses

In order to avoid a major impact from common threats to your business, you need to go back to basics: Preparation.

Prepare before the disaster occurs, which should include a disaster recovery plan that is customized to include your unique situation. This paper is directed more so to small businesses. However, mediums and large businesses can use this paper as a basis for their recovery plan. Moreover, due to the length of this paper, it will only cover some of the basic essentials that should be a part of any disaster plan, which are communication, creation of a disaster recovery plan, securing data and utilities, and protecting your assets.

Communication

One of the most essential items, during any disaster, is making sure that you can communicate with the outside world. Many businesses today depend on their network and the Internet to conduct business. Therefore, it is very important that Network Professionals keep the system up during a disaster. If you have not done so before, create a disaster recovery plan.

Creating a Disaster Recovery Plan

After the September 11th event, many small businesses in Downtown New York found themselves without telephone and network service, due to Verizon Communication, Inc.'s network being down. Other businesses were un-able to physically access their offices, due to the emergency situation. Part of the disaster recovery plan, should included a hardcopy manual or a online document that is not on your network, that contains a listing of your network equipment suppliers or service representatives, along with a contact name, phone number and a description of the type of service that they will supply to you.

Securing Data and Utilities

If your data is very critical to your business, not only do you need to protect it from hackers, crackers, viruses, etc, you need to back it up and store it off-site. You should keep at least two backup copies of data on disk, even if you have a backup to the server, in the event that your servers are damaged or erased. Take one of the copies home and bring the other copy to work each day, so that you can restore data from the day before. If both of the tapes are kept on site, you risk the loss of all of your data, in case of an emergency in which you cannot access your office, such as fire or flood. Some businesses use the Grandfather/ Father/ Son method, which consist of one daily backup (Son), one weekly backup (Father) and one monthly backup (Grandfather). As, I mentioned before, all backups should be kept offsite, especially if you have to setup your office in a temporary location. If you cannot afford to lose your data then back it up and store it appropriately.

Electricity is absolutely essential to your office network. Without it, (electricity and / or your network), your company may be permanently out of business. Therefore, to make sure that you will have electricity, buy a generator and test it to make sure that it runs.² Several companies have run into problems during emergencies because they did not test their equipment and it failed. Also, make sure that you buy a generator that is large enough to handle your needs. You should try to determine the minimum number of systems (lights, computers, servers, air conditioners, etc.) that you will need to run during an emergency and purchase a generator to handle it. Furthermore, make sure that you have enough gasoline, to last for at least a week. Remember that the Gasoline Stations have to use electricity to pump the gasoline. During the "War Game", the participants found out that most companies only carried about 72 hours of fuel for their backup generators. Make sure that your electricity will be there when a disaster strikes.

Protecting Your Assets

Protect your networks systems investments, by making, sure that you carry disaster insurance to cover your losses. During the blackout several small groceries and

² J. Peter Lark,. "Michigan Public Service Commission: Report on August 14th [2003] Blackout." Michigan Public Service Commission. November 2003: 101-103.

restaurants loss all of their perishables and were not able to recoup the costs. You should also carry business interruption and service interruption insurance, for instances when your system is down for a long period of time. Check your policy because service interruption insurance was drop from most policies several years ago. A good business interruption policy would include contingent business interruption, extra expense coverage, and service interruption coverage. Furthermore, make sure that the policy covers blackouts and cyberterrorism attacks. Check with your local chambers of Commerce for possible insurers or contact your current insurance agent for coverage information.

In a severe disaster (fire or a natural disaster, etc.), in which one or all of your employer's business or offices may be closed, you need to communicate with your department's management or another area of the company to determine what is the contingency plan if the office is down for an extended period of time. For example, if there are alternate work locations, are they up-to-date with the same PC, workstations, server equipment, version of software, etc. or will it have just minimal equipment and software needed to access records, etc. A disaster recovery test should be conducted at least once a year to assess how long it will take to get the alternate work location systems up and running. Furthermore, the assessment should include testing of the applications to make sure that they can be used as replacement systems. You do not want to find out when a disaster occurs that all of your data is in a version or format that cannot be assessed or read by your backup systems. This part may be easier for a medium or large business that man be stretched across greater distances, since the likely hood of all of the networks going down is slim.

Conclusion

In this day and age of increasing threats to networks, Information Technology, Security and Network professionals must diligently strive to stop or lessen the impact to their networks, information and physical structures. Knowing that you have a disaster recovery plan should help to elevate some of the panic and uncertainty that a disaster can cause.

Works Cited

- "Blackouts, Threats of Terrorism Spur Disaster Recovery Planning." Veritas Software. September 3, 2003. Retrieved 02/13/2004. <<http://www.veritas.com/news/press/PressRelease.jhtml?NewsID=60519>>.
- "Detroit Regional Chamber Determines Blackout Losses to Region Will Top \$220 Million." Transmission & Distribution World. October 2003. Retrieved 02/01/2004. <http://tdworld.com/ar/power_detroit_regional_chamber_2/index.htm>.
- "Disaster Checklist from Are you ready? A guide to Citizen Preparedness by the Federal Emergency Management Agency (2002)." ASIS International. Retrieved 02/13/2004. <<http://www.asisonline.org/newsroom/crisisResponse/disasterChecklist.xml>>.
- "Economists compare blackout to a blizzard." InfoTrac OneFile. Adams Business Media. October 2003. Retrieved 01/31/2004. <http://proxy01.academic.walshcollege.edu:2098/itw/infomark/613/170/42840205w7/purl=rc1_ITOF_0_A110813990&dyn=6!xrn_2_0_A110813990?sw_aep=lom_walshcoll>.
- "Food and Water in an Emergency." American Red Cross. November 1994. Retrieved 01/31/2004. <http://www.redcross.org/static/file_cont39-lang0_24.pdf>.
- Berinato, Scott. "The future of security." ComputerWorld. December 30, 2003. <<http://www.computerworld.com/printthis/2003/0,4814,88646,00.html>>.
- Bittar, Christine, and Reyes, Sonia, and Greenberg, Karl, Brand. "Retail, Auto Sectors Attempt to Reboot." EBSCOhost: Business Source Elite. eWeek. August 18, 2003. Retrieved 01/27/2004. <http://proxy01.academic.walshcollege.edu:2189/citation.asp?tb=1&_ug=dbs+afh+sid+3B147B44%2D7683%2D40D6%2D923E%2DEAB271CE354E%40sessionmgr5+FBDC&_us=dstb+ES+fh+0+hd+0+hs+0+or+Date+ri+KAAACBUC00075341+sl+%2D1+sm+ES+ss+SO+580F&_uso=db%5B0+%2Dafh+ex%5B2+%2Dthesaurus+ex%5B1+%2Dproximity+ex%5B0+%2Dfulltext+hd+0+op%5B0+%2D+st%5B0+%2DAN++10716609+tg%5B0+%2D+38D8&cf=1&fn=1&rn=1>.
- Booth, Mason. "Blackout Puts the Spotlight on Preparedness." American Red Cross. August 18, 2003. Retrieved 01/31/2004. <http://www.redcross.org/article/0,1072,0_333_1022,00.html>.
- Caldwell, F., and Hunter, R., and Bace, J. "'Digital Pearl Harbor' War Game Explores Cyberterrorism." Gartner, Inc. August 7, 2002. Retrieved 02/1/2004. <www.gartner.com>.
- Garvey, Martin. "Disaster recovery isn't just for big business." OCLC FirstSearch. Information Week. April 1, 2002. Retrieved 02/01/2004. <http://proxy01.academic.walshcollege.edu:2102/WebZ/FTFETCH?sessionid=sp01sw01-33913-dqpvvzo7-ubh1in:enttypagenum=12:0:rule=990:fetchtype=fulltext:dbname=ABI_INFORM_FT:recno=2:resultset=5:ftformat=ASCII:format=T:isbillable=TRUE:numrecs=1:isdirectarticle=FALSE:entityemailfullrecno=2:entityemailfullresultset=5:entityemailftfrom=ABI_INFORM_FT:>>.
- Johnson, Jim. "Spoiled food costs markets, restaurants." Info Trac OneFile. Crain Communications, Inc. September 1, 2003. Retrieved 01/31/2004. <http://proxy01.academic.walshcollege.edu:2100/itw/infomark/267/952/46697190w2/purl=rc1_ITOF_0_A107240077&dyn=3!xrn_1_0_A107240077?sw_aep=lom_walshcoll>.
- Lark, J. Peter. "Michigan Public Service Commission: Report on August 14th [2003] Blackout." Michigan Public Service Commission. November 2003. Retrieved 01/31/2004. <http://www.michigan.gov/documents/mpsc_blackout_77423_7.pdf>.
- Long, Cindy. "Red Cross Responds to Blackout, Reminds Communities to Prepare." American Red Cross. August 14, 2003. Retrieved 01/31/2004. <http://www.redcross.org/article/0,1072,0_333_1071,00.html>.
- Mazur, John, and Crowles, Ron. "Terrorists could Hijack the Internet." Gartner, Inc. September 30, 2002. Retrieved 01/31/2004. <www.gartner.com>.
- Mogull, Rich, and Caldwell, French, and Hunter, Richard. "Cyberattacks and Cyberterrorism: What Private Business Must Know." Gartner/G2. September 2002. Retrieved 01/31/2004. <<http://www.gartner2.com/qa/qa-0902-0091.asp>>.
- Mogull, Rich. "The Security Quake: A Call to Action or Continued Ignorance." GartnerG2. January 2002. Retrieved 01/31/2004. <<http://www.gartner2.com/rpt/rpt-0102-0009.asp>>.
- Nobel, Carmen, and Carlson, Caron. "Blackout makes communication difficult." EBSCOhost: Business Source Elite. eWeek. August 25, 2003. Retrieved 01/27/2004.

<http://proxy01.academic.walshcollege.edu:2189/citation.asp?tb=1&_ug=dbs+afh+sid+3B147B44%2D7683%2D40D6%2D923E%2DEAB271CE354E%40sessionmgr5+FBDC&_us=dstb+ES+fh+0+hd+0+hs+0+or+Date+ri+KAAACBUC00074799+sl+%2D1+sm+ES+ss+SO+B4C2&_uso=cli%5B3+%2DSO+cli%5B2+%2DFT+cli%5B1+%2DDT1+cli%5B0+%2DPZ6+clv%5B3+%2DeWeek+clv%5B2+%2DY+clv%5B1+%2D20030800%2D20030900+clv%5B0+%2DArticle+db%5B0+%2Dafh+ex%5B2+%2Dthesaurus+ex%5B1+%2Dproximity+ex%5B0+%2Dfulltext+hd+0+op%5B0+%2D+st%5B0+%2Dblackout+tg%5B0+%2D+5A18&fn=1&rn=5>.

Pipkin, Donald L. Information Security: Protecting the Global Enterprise. New Jersey: Prentice Hall PTR, 2000.
“Symantec Internet Security Threat Report Sees Sharp Increase in Reported Vulnerabilities but Drop in Overall Attack Activity.” Symantec Corporation. February 3, 2003. Retrieved 01/27/2004.
<<http://www.symantec.com/press/2003/n030203.html>>.