Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Preparing For A Disaster: Determining the Essential Functions That Should Be Up First

Copyright SANS Institute
Author Retains Full Rights

AD

PREPARING FOR A DISASTER

DETERMINING THE ESSENTIAL FUNCTIONS THAT SHOULD BE UP FIRST

By: L. Barry Lyons IV, CISSP

How do you determine those services and functions that should be up first when a disaster strikes? A Business Impact Analysis (BIA) will verify the critical functions/processes (and their related dependencies) that are essential for your business to continue operating. The BIA will also discover vulnerabilities, present a risk mitigation strategy and determine financial loss over time along with the cost to recover.

The first step in the BIA process is to obtain a commitment by senior management that they support a BIA and will instruct all departments/divisions to cooperate. Obtaining useful information without senior management support is virtually impossible.

Once you have buy-in from senior management, the next step is to identify all business units within an organization. This can be confirmed by using an up-to-date, "certified" organization chart. You will need to clearly identify the business process/function owners.

Once this is accomplished, questionnaires are developed. You will be interviewing process owners along with the department heads and "C" level individuals. (Many times the department heads are also the process owners.) The questionnaire for the process owners will be more extensive than the "C" level questionnaire.

The "C" level questionnaire will focus on goals and their perception of an impact if a disaster occurs. Suggested questions:

- What are the goals of the organization?
- What would it cost the organization/company in dollars for every minute/hour/day you lost your ability to:
    - Process orders
    - Communicate with customers
    - Communicate with vendors
    - Communicate with investors and/or the press
    - Communicate with employees
    - Negotiate contracts
    - View/ retrieve vital records and information
- What would it cost, in dollars, reputation and "good will", if customer data was exploited, lost or stolen?
- What would it cost in dollars, reputation and "good will", if sensitive company data was exploited, lost or stolen?
- What are the three most important business functions that would cause severe damage to the organization if they were unavailable for 24, 48, or 72 hours?
- Of the three business functions identified above, is there one that can't be down for five minutes?
- If it can be down for longer than five minutes, what is the absolute *minimum* time you are willing to accept for this business function to be down? Here you are establishing the Recovery Time Objective (RTO). You will compare this with process owners RTOs.

© SANS Institute 2006, As part of the Information Security Reading Room Author retains full rights.

Don't be discouraged if the "C" level interviewee doesn't have precise answers to every question. Sometimes just by asking the questions, you have started a thought process that the "C" level hasn't even considered. This is a good thing.

Next you need to develop the process owner questionnaire. (Sample questionnaire is attached in Appendix B.) The goal from these interviews is to come away with a clear understanding of the systems they use and all system dependencies. You also want to dig up, from their perspective, how important their processes/functions are to the organization, obtaining their view of what it would cost if they were down for an hour, 4 hours, a day, a week, and even a month.

When you meet with the process owner it is always good to start with diagrams of the department's network and systems. Diagrams offer excellent interview reference points.

Sample process owner questions:

- What does your department provide?
- Describe its functions
- Who are your "customers"? (Name the departments/divisions and the people – you want the people's names as this will confirm you have the correct names on the organization chart.)
- What systems do you use? List Hardware, Software, be specific. Do they have custom software? Who supports it? How is it supported? Build a list of each piece of hardware and its associated software.
- What other department(s) do you depend on to complete your function/process? List each one and confirm that you understand the relationship between them.
- Are there other departments/processes that depend upon your functions/process? List each one and confirm that you understand the relationship between them.
- Do you have critical times of the day, week, month and/or year that you MUST be up and running? What do you produce/provide that is critical and/or time sensitive? Why? Who needs it? Do you believe senior management agrees with your assessment of this critical process? (Confirm this with the "C" level interview information.)
- Does your system/function/process have to meet any compliance laws, standards or initiatives?
- If your department went down, what would the potential effects be? (See chart below)

OUTAGE:	< 4 hours	4-8 hours	2-4 days	5-10 days	> 10 days
Have an effect on:					
Hard $$ Loss					
External Customers					
Internal Customers					
Operating Expanse ($$ spent while down)					
SLA impact					
Legal impact					
Functions dependant upon you					
Business Partners					
Company 'Good will'					

© SANS Institute 2006, As part of the Information Security Reading Room Author retains full rights.

Lastly:

- What is your Recovery Time Objective (RTO)?

Each function/process should be assigned a RTO based on its importance to the organization. It is essential to note that some individual process owners will feel their process/function is "the most important", but many times this isn't that case, especially if the particular process doesn't have an immediate negative financial impact on the organization.

On the other hand, some process owners will have a good idea what the RTO should be based on their importance to the overall business. At this juncture, you need to compare the senior management's perception of RTO with the process owner's perception. Are they aligned in their thinking, or are they a million miles apart? What you will find is that the better the communication between senior management and process owners, the closer they are in their perception of the RTO.

Each time an interview is concluded, you should write-up a summary and send it to the interviewee to confirm that what was said was what you heard and you didn't miss anything. Don't wait until you have concluded all the interviews; they will start to melt together. Validate each interview within 24 hours after the interview while thoughts are still fresh in everyone's mind.

Beside the questionnaire, you should also develop a list of Supply/Resource Items that each department needs in order to perform their function. This list should be completed while you are taking a walk through the process owners department. The reason you do this is because process owners don't always think about those things that are "around" them. The BIA has to take into account the costs associated with these items since they will need to be replaced too:

- ✓ Printers
- ✓ Special Purpose Printers
- ✓ Scanners
- ✓ Surge Protectors
- ✓ UPS
- ✓ Projectors
- ✓ White boards
- ✓ Copiers
- ✓ Copy paper
- ✓ Blank CDs
- ✓ Calculators
- ✓ Postage Meter
- ✓ Office supplies
- ✓ Shredder
- ✓ Desk, Computer and Conference room furniture
- ✓ Blank Back-up tapes
- ✓ Mobile phones
- ✓ Pagers
- ✓ Telephone systems

Pay particular attention to the network devices in a department. Often the individual process owners don't "own" the network devices, yet these devices are an integral part of the overall systems architecture. It is important that you determine who owns the network(s) and how they interact with the departments. Some organizations have a separate group that is responsible for "the network" and all its devices. They have to be factored into the equation when developing a BIA. Make sure you interview the network owner(s) too. Remember, the switches and routers will not "magically" appear at a recovery site. And very likely, network components will be essential to getting critical systems up first. There has to be a replacement plan in place for these devices, especially if they are not owned by process owners. This may seem blatantly obvious but BIA's have been developed that missed the network backbone components.

We are just about ready to write up our BIA Summary, but we aren't quite there yet. We need to perform a Risk Assessment. A BIA Risk Assessment is made up of three different assessments: The IT Risk Assessment, the Physical Assessment and the Management Disaster Awareness Assessment.

© SANS Institute 2006, As part of the Information Security Reading Room Author retains full rights.

The Management Disaster Awareness Assessment addresses the existing (if there is one) Disaster Recovery Plan from senior management's point of view. If a DRP doesn't exist, you then need to confirm the "Who, what, where, and how" of the senior management's disaster knowledge, asking, "If there is a disaster:

- *Who* is in charge? (Is there a Delegation of Authority list by department? Is there an Order of Succession list/plan in place?)
- Do you know exactly *what* you are supposed to do?
- Do you know *who* is supposed to do *what*, and *when* they are suppose to do it?
- Do you know *where* your management team is located and *how* to reach them at any time, day or night?
- Do you know *where* your backed-up vital records are stored and *how* to retrieve them?"

With the Management Disaster Awareness Assessment you are measuring the current state-of-affairs regarding management's knowledge and understanding of how to respond to a disaster. There is "risk" here if management is clueless, or only "thinks" they know what to do.

Concurrently, while you are performing your interviews, you should have a knowledgeable systems engineer perform network, operating systems, application, host and penetration scans and tests. These sans and tests address the IT portion of Risk Assessments. Keep in mind that prior to performing an IT Risk Assessment, careful consideration must be given to the types of scans/tests you will perform. (For a list of some currently used scan products, please see Appendix C.) Some organizations only want internal scans and do not desire a penetration test from the "outside". Others will require internal scans of everything in their IT infrastructure along with an outside-to-the-inside penetration test. It is recommended that you obtain senior management approval *prior* to commencing any penetration tests or scans. Furthermore, it is imperative that you have a written agreement between you and the organization, holding you harmless if a disaster occurs while you are scanning and/or performing penetration tests. Even if you are an employee of the organization, it is prudent to have written confirmation that you will not be held liable for any harmful incident due to scans and/or penetration tests.

Also part of a comprehensive Risk Assessment is reviewing the physical elements of an organization's location, especially the data center(s). Some questions to ask:

- Who is responsible for physical security?
- How is the data center secured? What access control methods are in place? Who is allowed access? Why? Is there an access audit trail? Is there more than one entrance/exit to the data center? Where are they?
- Is the data center built with fire-rated walls, floor and ceiling?
- Do the walls go all the way up to the building's ceiling or next floor, or stop at the false ceiling?
- Is the area below the raised floor monitored for excessive heat or moisture? Is it cleaned regularly?
- How is "after-hours" access accommodated? Is there an audit trail?
- What fire suppression system is in place in the data center? Are employees fully trained on how to activate the fire suppression system? If the fire suppression system fails, is there a back-up plan?
- Do employees know how to use a fire extinguisher?
- Is there a rapid shut-down system in place if the fire sprinkler system is accidentally activated?
- Are exit routes clearly marked? Do you have regular emergency fire drills? Do employees know where to meet outside the building?
- Are combustible materials stored in or near the data center?
- Does the fire department have a diagram of the building/data center?
- Is there excessive dry brush close to the building?

© SANS Institute 2006, As part of the Information Security Reading Room Author retains full rights.

- Can employees exit the data center easily and safely if there is a fire emergency?
- Are the air ducts equipped with power dampers that will automatically close in the event of a fire?
- How is the building(s) secured? Is there free access to every department/floor/room?
- Are the parking lots secured?
- Are there video cameras inside and outside? How is the data recorded and stored?
- What is the lighting situation around the building and the parking lot?
- Is the building in a flood plane area? Is the data center below or at ground level?
- What is the condition of the roof? Does it leak? Does water drain easily off the roof? Where does it go?
- Where are back-up tapes stored?
- Where are paper vital records stored?

These are just some of the questions you can ask. Think about everything and anything that has to do with the physical aspects of a building/data center. Note its location. Is it near a chemical plant, or railroad tracks? How does water drain around the building? Is it in an earthquake prone area? Is it susceptible to lightening strikes? All these things have an associated risk.

Before writing the BIA Summary, you will need to develop the Risk Assessment Summary as it will be included in the BIA. Remember that some risks are relative and change over time. For example, today Company "X" may have a 65% risk of its front-end order entry computers going down because they have not installed the latest operating system patch. Tomorrow, this risk may decrease considerably because patches were installed. On the other hand, the data center may be located in a 100 year flood plane. This should be accounted for especially if the data center is on the first floor. This may not change over time because the organization will not move the data center to a higher floor; the cost outweighs the risk mitigation benefit, therefore the risk remains the same over time.

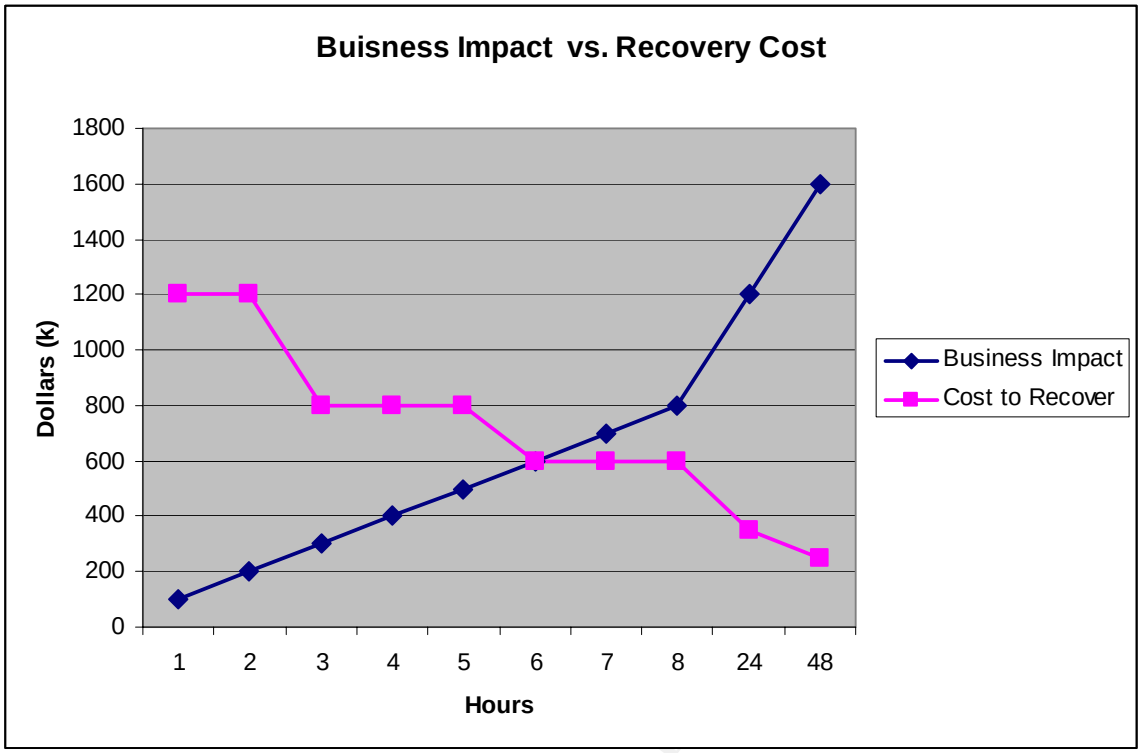
Risk Assessments are a "snapshot" in time of an organization's current risk position. Risk is constantly changing, especially in the IT arena. One IT risk assessment made during an initial BIA does not adequately serve an organization. Vigilant monitoring and routine vulnerability scanning should be performed. In fact, IT risk assessments should be performed at least once every six months by a competent, third-party IT Security Company. If the organization is not aggressive in keeping up with patches, or introduces new applications/servers/web interfaces on a regular basis, IT risk assessment should be performed every 3 to 4 months. It is also recommended that the organization seriously considers Configuration Management tools to pro-actively monitor changes made to the organization's information system.

The Risk Assessment Summary will be folded into the BIA Summary. The BIA Summary will document the facts gleaned from interviews, scan/tests, and walking tours. It will present an analysis of the information, listing risk mitigation recommendations, and pointing out serious deficiencies in areas that require prompt attention. But these factors alone won't address the Business Impact if a disaster occurs. You need to make clear the potential financial loss if a disaster transpires and present the cost for a disaster recovery solution. It will also clearly delineate those systems that should be up and running first. Let's look at an example:

The Lyons Group, a worldwide retail clothing company, processes $90,000 in on-line orders every hour. It was determined during the BIA study an additional $10,000 per hour in productivity also occurs; hence they will experience a financial loss of $100,000 per hour for every hour they are down. The BIA further revealed that there were multiple systems that supported the on-line order entry system.

The Disaster Recovery/Risk Mitigation solutions for their situation vary from $1,200,000 for 1-2 hour recovery to $250,000 for 48 hour recovery. They compared the business impact with the cost-of-recovery.

© SANS Institute 2006, As part of the Information Security Reading Room Author retains full rights.



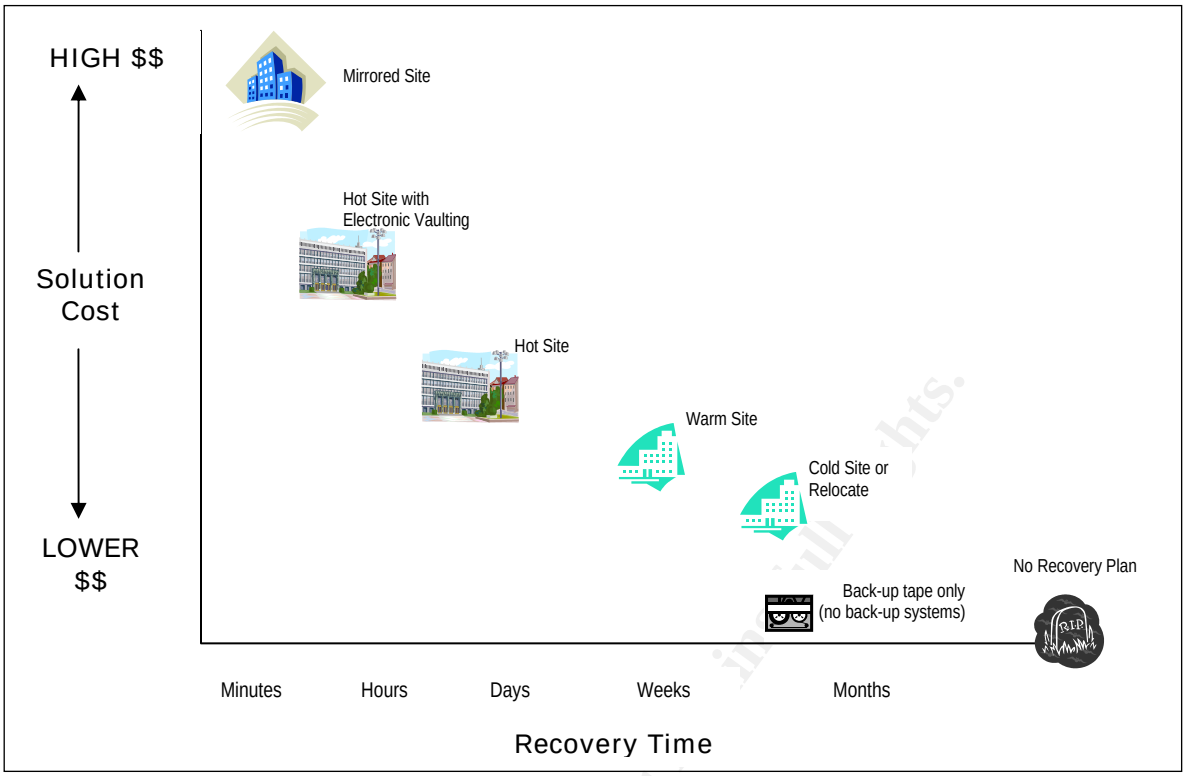
The CEO did not want to lose even 1 hour of revenue, but realized that they couldn't afford to spend $1,200,000 to protect a potential loss of $200,000. She realized that spending $600,000 to protect a potential loss of $600,000 to $800,000 was a better investment. (Note: Spending $600,000 to protect the potential loss of $600,000 to $800,000 is based on just one disaster occurring. If they have two outages in one year, the $600,000 expenditure will protect $1,200,000 to $1,600,000 in potential loss.)

Keep in mind that there are organizations that are willing to spend $1,200,000 because they feel the intangible "good will" loss would be greater than the tangible loss of $200,000.

Plotting a chart like the one above offers decision makers a view of the financial impact in relationship to the cost-to-recover and helps cost justify a recovery solution.

Remember too that the cost-to-recover is directly related to the TYPE of recovery desired. The faster the recovery, the higher the cost:

© SANS Institute 2006, As part of the Information Security Reading Room Author retains full rights.



Not only does the BIA outline Business Impact and cost to recover, it will determine those functions/processes that should be up first. This is provided by a Critical Impact table:

CRITICAL IMPACT TABLE

Department	6 hours Outage	2 - 5 days	6 - 10 days	> 10 days
Sales	On-line orders	Customer Support / Marketing & Investor relations	Mail-in orders	Sales Reports
Procurement			Ordering products for resale	
Shipping		Product delivery		
Financial			Payroll/ Accounts receivable	Accounts Payable
Information Systems	Telecom/Internet/IS support for on-line orders	E-mail/ order tracking	Financial Operations Support	All other applications
Legal				Regulatory items

The table above identifies the relative criticality of an item and its associated recovery time frame. This dramatically delineates those systems that should be up first by virtue of their business impact. In the Lyons Group study, the BIA findings documented three separate systems that must be up to support on-line orders. The Critical Impact Table is an essential component of the BIA Summary.

© SANS Institute 2006, As part of the Information Security Reading Room Author retains full rights.

The BIA Summary includes:

- A Management Summary and Background
- Project scope and assumptions
- Project Objectives
- Risk Assessment Objectives
- Project Actions (that were completed)
- Findings (Include a chart that outlines Threats, Consequences, Preventive Measures/Mitigation and Likelihood of Occurrence Sample Chart in Appendix A.)
- Critical dependencies
- Existing Strengths / Problem areas
- Existing budget to address Problem areas (and where it may fall short)
- Existing Insurance Coverage
- Final Analysis and Recommendations

Don't be surprised if management doesn't accept the recommendations. Your job is to present the facts uncovered during your interviews and assessments, the recommendations and their associated cost, along with outlining the consequences of not performing recommended corrections. It is important to offer multiple recovery solutions and their associated cost to assist management make an intelligent decision when comparing these costs with the Business Impact.

An accepted recovery solution depends on an organization's policies, goals and financial resources. A comprehensive BIA is a proven tool in guiding an organization on a correct disaster recovery course and determining those functions that should be up first when a disaster occurs.

Attachments:

Appendix A: Sample Consequence Chart

Appendix A: Sample Process Owner Questionnaire

Appendix A: List of IT Scanning Tools (Fortrex Technologies)

© SANS Institute 2006, Author retains full rights.

© SANS Institute 2006, As part of the Information Security Reading Room Author retains full rights.

APPENDIX A – Sample Consequence Chart

THREAT	CONSEQUENCES	PREVENTATIVE MEASURES	LIKELIHOOD
Sever Storm	Flooding	• Vital Records & IS systems are above first floor • Plastic bags are available to protect paper & magnetic tape • Roof, windows and outside doors are in excellent condition and have been tested for leakage • Moisture sensors are located between real floor and raise floor • Vital records and back-up tapes are located off-site in a professional off-site storage facility	Low to Moderate
	Power Outage	• Back up generator is on site and tested monthly • Sufficient fuel is on site for back up generator • Fuel supply vendors have been pre-contracted to deliver fuel • Mobile back-up generators have been pre-contracted for delivery	Moderate
	Structural Damage	• Hot site/Warm site is in place • Telecommuting is available and supported • Construction Contractors have been pre-contracted • Budget is set aside for immediate emergency construction • Building is up to code and checked regularly for deficiencies • Data Center is constructed with concrete walls, ceiling and floor. • Work-space trailers have been pre-contracted	Low

© SANS Institute 2006, As part of the Information Security Reading Room Author retains full rights.

THREAT	CONSEQUENCES	PREVENTATIVE MEASURES	LIKELIHOOD
Sever Storm (con't)	Voice/data Communications outage	• Telecommuting is available and supported • Alternate communications paths into the building are in place • Optical Fiber is used, all connection points to copper are above ground • Non-digital telephones are available with direct dial copper lines to local exchange switching center	Moderate
	Loss of Physical access	• Hot site/Warm site is in place • Telecommuting is available and supported • Construction Contractors have been pre-contracted • Work-space trailers have been pre-contracted	Low to Moderate
	Employees can't get to work	• Telecommuting is available and supported	Low to Moderate
Computer Virus / Worm	• Critical processes crash • Orders can't be processed • Company sued for being a vicious "launching site" of virus/worm/malware • Frustrated employees • Angry customers • Loss of investor confidence • Negative Press	• Consistent nightly updates of latest virus / worm / Spyware signature files • Run nightly virus scans • Use Multiple virus vendors • Incorporate SPAM protection devices/software • Restrict/Block the opening of incoming file attachments – pre-scan in holding "area" • Restrict/Block the use of personal email accounts on work computers • Restrict Web use and build a Web site whitelist/blacklist • Restrict/Block s/w installation on individual computers • Block Peer-to-Peer connectivity • Set-up auto virus scan on any media inserted into computers • Train employees on computer use company policy • Delay mirrored back up communication by "X" minutes to stop virus to mirrored site	High

© SANS Institute 2006, As part of the Information Security Reading Room Author retains full rights.

APPENDIX B – Sample Process Owner Questionnaire

BIA PROCESS OWNER INTERVIEW SHEET **Page 1 of 2**

Department: _____

Process Owner: _____

Interview Date: _____

What does your department provide? _____

Are there other departments that depend on your process? NO ☐ YES ☐

Department: _____

What they do: _____

Process Owner / Contact number: _____

Do you depend upon other departments to complete your process? NO ☐ YES ☐

Department: _____

What they do: _____

Process Owner / Contact number: _____

Who are your primary customers? _____

Do you have a critical time of the day / week / month / year that your process must be completed?
(Circle all that apply.)

What do you produce that is critical? _____

Why is it so critical? _____

Who is it produced for? _____

What computer systems do you use?

Hardware	Software

© SANS Institute 2006, As part of the Information Security Reading Room Author retains full rights.

BIA PROCESS OWNER INTERVIEW SHEET **Page 2 of 2**

Department: _____

Process Owner: _____

Interview Date: _____

How long could your department operate manually without computer support? _____

How long could you sustain an outage before your department would have a critical impact on the organization?

< 2 hours ☐ 4 hours ☐ 8 hours ☐ 2 days ☐ 3 - 5 days ☐ 6 - 10 days ☐

Other: _____

Describe the impact it would have: _____

How do you currently back-up your systems? Tape ☐ Mirrored site ☐ Don't know ☐

Other: _____

How often? _____ Where are tapes stored? _____

How long would it take you to retrieve your back-up tapes? _____

Each time you perform a tape back-up, do you run 1 or 2 back-ups? 1 ☐ 2 ☐

How do you currently protect your systems from Virus/Worms/Spyware? _____

How do you currently protect your systems from insider threats? _____

Has your department ever experienced a disaster? NO ☐ YES ☐

If YES, what type and how did you recover? _____

What is your Recovery Time Objective (RTO)? _____

Why? _____

© SANS Institute 2006, Author retains full rights.

© SANS Institute 2006, As part of the Information Security Reading Room Author retains full rights.

APPENDIX C – List of IT Scanning Tools

List provided by Fortrex Technologies, www.fortrex.com
1-877-FORTREX (367-8739)

- QualysGuard – Commercial network vulnerability assessment tool with a comprehensive vulnerability knowledgebase that incorporates 4,700+ unique checks. QualysGuard provides network discovery and mapping, asset prioritization, centralized reporting, and remediation workflow and verification.
- Sam Spade - A network query tool that performs many useful operations, including DNS lookups, whois lookups, website crawling and mail relay testing.
- Nmap - A powerful and flexible port scanning tool that employs numerous techniques for discovering open ports on target systems.
- Amap - An open-source tool that remotely identifies application versions.
- Netcat - A networking utility that reads and writes data across network connections using the TCP/IP protocol.
- Internet Scanner (ISS) - A leading commercially available vulnerability scanner.
- Nessus - A tool used to detect a broad range of vulnerabilities related to network services.
- Nikto - A scanning tool that focuses on web-related vulnerabilities; commonly referred to as a CGI scanner.
- Paros - A desktop web proxy that allows the user to intercept and manipulate web traffic before sending it to its destination. This is very useful for web-based attacks.
- THC-Hydra - An open-source tool that performs brute force login attacks against numerous well-known network services.
- Metasploit - An extremely useful tool that provides a framework for developing and executing buffer overflow exploits.
- Burp Suite - An integrated platform for attacking web applications. It contains the entire set of burp tools (proxy, spider, intruder and repeater) with numerous interfaces between them designed to facilitate and speed the process of attacking a web application.
- Socat - A relay for bidirectional data transfer between two independent data channels.
- SMTPscan - An SMTP server scanner used to identify SMTP server software and versions.
- ExploitTree - A categorized collection of ALL available exploit code.
- WebScarab - A framework for analyzing applications that communicate using the HTTP and HTTPS protocols.
- LdapMiner - A tool used to collect information from different LDAP server implementations.
- Cisco Audit Tool - A tool used to audit Cisco devices and the IOS operating system.

© SANS Institute 2006, As part of the Information Security Reading Room Author retains full rights.

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**