Contingency Planning

Blueberry IT Consulting

Blueberry IT Consulting
Magnus Øverbø, Robin Stenvi, Lasse T. Johansen
090832 100232 090749

Security planning and incident management
IMT 3521

Department of Computer Science and Media Technology
Gjøvik University College 2012

Avdeling for
informatikk og medieteknikk
Høgskolen i Gjøvik
Postboks 191
2802 Gjøvik

Department of Computer Science
and Media Technology
Gjøvik University College
Box 191
N-2802 Gjøvik
Norway

Contingency Planning

Blueberry IT Consulting

2012/05/15

Executive summary

The purpose of this document is for Blueberry IT Consulting to be qualified to respond to the scenarios we have discovered and developed plans for during the course of our project. These plans will ensure that a scenario is handled efficiently without endangering human life, business function, classified information or compromising potential evidence. Though, for this to be the case it will require full cooperation of the entire staff, spearheaded by the leaders. Without sufficient backing from the leaders of Blueberry IT these plans would potentially do more harm than good, which is why we emphasize this part of the implementation process.

We started out by mapping Blueberry ITs business functions, procedures, existing policies and guidelines before we analyzed our findings and documented all threats and business functions related to Blueberry ITs business processes. This continued with weighting and analyzing Blueberry ITs business functions and each threats impact on the business. These two analysis is correlated and prioritized in the ”Scenario Priority Document” which is used to decide which scenarios is to be developed further.

Then we performed a deep analysis of each of the top ten scenarios from the ”Scenario Priority Document”, which led to the development of the plans according to the subordinate plan classification, section 3.6.

Due to Blueberry ITs organizational size we set on developing the top ten scenarios from the ”Scenario Priority Document”. This would secure Blueberry IT from the ten most important scenarios in addition to avoid overwhelming them with plans which needs training and maintenance.

The plans is a result of careful consideration of Blueberry ITs internal and external business functions and policies. This ended up with an external document which is left out of the BCP document since it could cause conflicts during an incident.

We have finished developing plans for three of the ten different scenarios, due to the time limitations of the project. This means there is still seven scenarios left which it has to be developed plans for.

The plans we have developed so far is described in the ”subordinate plan classification”, section 3.6; ”Unauthorized installation of software”, ”Flood” and ”Phishing attack”. Within these plans we have made incident and disaster response plans for ’Unauthorized installation of software” and ”Flood”, for the ”Phishing Attack” we only developed a incident response plan since this particular scenario would after an incident cross over to becoming a different scenario.

The result of this document will help Blueberry IT Consulting with responding to incidents and disaster way more efficiently than before. This plan will also ensure that Blueberry IT Consulting will withstand serious blows to their business functions and still be able to resume business functions in a relatively short time. Much due to the mutual agreement with Strawberry Inc. in case one of them loose their main working facilities.

Of course all of this depends on proper management, initiative and implementation of the developed plans.

Contents

1 Business Description

Blueberry IT Consulting was founded in April of 2005 by 10 students exiting from GUC and is a small company specializing in risk assessment of small and medium business'. The founders of Blueberry IT Consulting exited from GUC with their primary fields within IT, ranging from Information Security to Network Administration.

1.1 Business overview

In the beginning Blueberry consulted small businesses in the local area, and assisted newly founded businesses to establish security policies, guidelines and procedures. In addition Blueberry also provided services for installation and revision of the existing IT-systems in these businesses .

After three years of managing small businesses in Oppland, Buskerud and Hedmark, Blueberry stated a new vision to expand their marketplace in 2008. The vision was and still is to "Help the business in need of technical or organizational help". To comply with this vision Blueberry expanded their staff, and today it consists of over 30 employees which include receptionists and third party contractors. After the change Blueberry saw the opportunity to undertake projects in the centralized parts of Norway and Sweden, and as a result of this they expanded their geographical marketplace as well. An overview of their current employee hierarchy is displayed in figure 1.

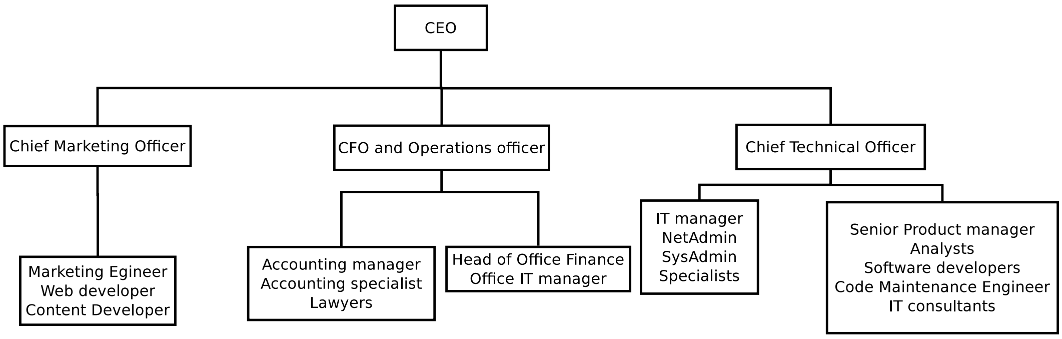

Figure 1: Organizational hierarchy

Blueberry's primary focus is set on the organizational aspects of the financial and service categories where they perform risk assessments of both the technical and HR aspect. The work information Blueberry ITs employees produce is stored and processed on Blueberry's in-house IT-systems since they have adequate security in place to maintain confidentiality, integrity and availability(CIA).

Blueberry's headquarter is located by the waterfront in Gjøvik's prime real estate area. They work in the building along with several other firms, but they lease the entire 2nd floor for themselves. The other personnel in the building stems from several small local business firms, which shares the third floor, the 4th floor is occupied by a telecommunications branch from Telenor AS. In addition the 1st floor serves as a public area with several conference rooms.

During business hours the facility is controlled by a security guard which controls the public access for any visitors. The outside perimeter is monitored by CCTV cameras running on a 7 day loop before they're deleted. The camera feed is in addition continuously streamed to the guards monitoring station inside the building, along with the recording station which is placed in a secure location on site. The access control system is integrated throughout the entire building and requires a security card along with a six digit, personal passkey.

1.2 Assets

Blueberry IT maintain their own in-house IT-system and file storage so they can personally secure their clients information and provide online services to their employees. Their assets include both internal and external assets, in-house server farm, applications and hardware, emergency generator, renovation and printer service.

The external security service is provided by Securitas, which consists of CCTV-surveillance, security guard, access control and alarm system. Blueberry also has other external assets which is data and telecommunication services from Telenor, renovation, cleaning, power and food delivery.

The ISP provides the necessary and redundant communication lines for Internet and telephone service. It is also a public renovation service for water, sewage and trash, which results in an increased risk of throwing out confidential information. The cleaning crew which is hired from reliable firms and recommended by others companies, cleans the entire building for all companies located there. The power company supplies the entire building with a single electrical feed. Since the building doesn't have a redundant power supply it is critical that they have an emergency generator for running the critical systems.

Information: Database information, employee contracts, consulting contracts, documentation, manuals, procedures, incident response plans, business continuity plans, client data and information, personal information, employee records, finance records, software licenses and other physical media.

Software: Applications, software, development and in-house software.

Physical property: Laptops, smartphones, server farm, UPS, access point, physical inventory, file cabinets, office supplies and other equipment.

Services: Data and communication services and client consultation.

Employees: Services, experience, information and knowledge.

Reputation: Blueberry ITs reputation in the public domain, the clients reputation.

External services: Third party contractors, electric power supplier, emergency generator, Internet service provider, security service, CCTV, access control system, food delivery, renovation service, external data storage, external physical storage and printer service.

1.3 Business procedures and processes

With many different aspects of information security as their daily job, it is expected that Blueberry has a good security culture for maintaining the basic principles of CIA. The section that follows describes Blueberry's main procedures, including their basic safety procedures.

1.3.1 Risk management process

Blueberry's risk management process is based on the books ”Principles of Incident Response and Disaster Recovery”[1] and ”Principles of Information Security”[2]. Blueberry IT also relies on certain guides and standards like NSM-ROS, [3], and ISO 27005, [4]. This divides Blueberry's process into two main parts; identification and control.

Establishing project

When Blueberry get a project they have a brief overview meeting with the business to estimate the capacity, time and settlements needed to complete the task in hand. When the parts settles on a project the consultant from Blueberry and the business signs a contract for the work to be done. This also dictates the rules, the consequences and the scope of the project. In addition to put an estimate for total fee for the entire project Blueberry charges a start-up fee for the project until they reach the presentation of the security breach report. The finance services is handled by the accountant at Blueberry ITs office, which involves processing and storing the information on the local finance systems.

After this Blueberry establishes a repository on their in-house systems which acts like a dossier for the project. This is where all documentation, log-files, information and reports is stored during and after the project is complete. After this in-house procedure the consultant gathers the necessary employees of the business to participate in the the project. Then they hold a meeting where they gather the current business information corresponding to the the projects scope. Dependent on the contract, the business' information will be temporary stored on Blueberry's SVN server for easy access to the consultant.

Discovering security breaches

At the information gathering meeting they establish a timeline for the project which contains the outline of the project, including tasks, deadlines and milestones. After this meeting they categorise and document their findings and future tasks on the Blueberry server. Even though the consultant from Blueberry does the most work and has the responsibility for the project, the whole team is part of the process of risk control and decision-making processes. The next step after the initial meeting is to continue digging deeper into each part of the project, which means getting access to even more information. After each part of the project the team documents their findings according to the scope of their project and have a brief meeting internally with the team.

Security breach report

When they are done reviewing the current state of the business they create a final report of their findings and present the findings for the business' board of directors. Depending on the projects scope, the job might be finished or the team might have to develop countermeasures for their findings. The next part of this is to develop and implement solutions to the discovered security breaches. At this stage Blueberry IT charges the client for the work done this far.

Developing solutions

This stage involves in-depth interviews with employees to gain knowledge about each function of the business. These interviews are meant to discover the business' assets and their related classification, but also to identify the threats related to the assets. All these procedures boils down to being able to implement the correct solutions in the right order.

Solution report

At this point the team has developed the necessary solutions and ordered them by the factor of criticality to the business' functions. They then document and present their findings to the board of directors so it can be decided which countermeasures to implement. When Blueberry has presented the solution report they charge the client for the work done so far.

Implementation

Depending on the contract Blueberry might not be a part of this. The implementation procedures is divided into two parts, implementation and testing. The first part is to implement the solution according to the policy, guidelines and technical demands set by the business, followed by testing the solutions durability and resilience. After the tests are run they evaluate the solutions effect and plan accordingly.

Hand-over

The final stage after testing the solutions effect is to train and pass the systems on to the business. If this is a technical solution employees must be instructed and trained to use it correctly. If it instead is an organizational aspect employees must be informed, and properly trained to act accordingly to the new policies, guidelines and procedures.

All training and guides is documented and placed on the servers at Blueberry for safekeeping and easy access in case it is needed at a later date. In addition to the guides, etc., all needed documentation is handed over from Blueberry to the business.

After this final stage in the business process they charge the employer for their total outstanding fee and hands over the work.

Clean-up

After a project is done the cleanup procedure takes effect. This involves removing access rights to Blueberry's network, securely removing all files stated in the contract, securely removing all hard copies and storage devices, and making sure all access rights to the clients information systems is severed.

In the light of this it is clear that Blueberry ITs most important business functions is their ability to manage the project management system and their ability to manage invoicing. The different departments dependencies of Blueberry IT is shown in figure 2. This shows that the consulting department depends on several business functions described in table 2

1.3.2 Internal Procedures

Visitors: Visitation to Blueberry ITs offices is only allowed by appointment and upon entry and exit they have to sign the visitor protocol in the guard booth at the first floor. Then when a visitor is on the premises he/she should always be escorted around the premises due to security reasons.

Callers: All calls to Blueberry is in general answered and forwarded by the receptionist. It is the receptionists job, among else, to keep track of meetings, visitors and calls. All calls are registered in a call log.

Customer management: Blueberry IT gives their customers superb support through their help-

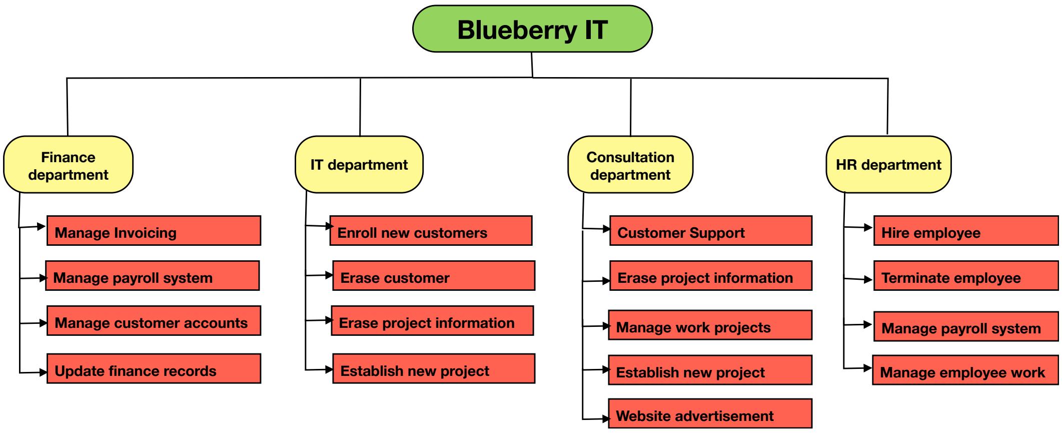

Figure 2: Dependencies between business functions and the different departments.

desk and analysts since it is imperative to keep a professional relationship with the customer. This involves full helpdesk support during normal business hours and access to all documentation during and after the project is ended.

Managing invoices: After each finished project stage the accountant is informed of the current outstanding payment. The accountant then creates an invoice and sends it to the customer. The accountant is also responsible for overseeing Blueberry ITs taxes, finances and expenditures.

Destruction/removal of information: All restricted and confidential information, see section 1.3.4, should be securely deleted from the system. If the information generated from one medium is to be archived it should be securely transferred to the archive and then permanently deleted from the medium. When private or confidential information is transferred between two points, it is by policy required to use a secure form for transmission. Management of public information that in large quantities can be perceived as private or confidential information should be treated as such.

1.3.3 External Procedures

Visitors and delivery Visitors and deliveries arrive first to the security guard on the first floor, which is then met or picked up by an employee from Blueberry.

Guard The guard is serviced by Securitas, which is a well known security provider for businesses and home-owners. They provide 24/7 CCTV, daytime guard-service and full shell security. The guard has access to the entire place except the server room, even at night time.

Janitor/cleaning services The janitor/cleaning services is hired from reliable sources and provide the necessary maintenance of the building. The janitor oversee everything from the generator to the plumbing in the building. This means he has access to every floor in the building excluding the server room, because of their employee status they have access only during business hours.

1.3.4 Asset classifications

Public: Information and assets which is legally distributed/available and otherwise non-threatening to the company or its customers. This is for example information distributed through Blueberry ITs website and information used in PR-campaigns.

Restricted: This is information and assets which is not critically threatening to the business, but is not meant to be available for public viewing. Disclosure of this information will yield minimal impact on the company's daily operations, but will result in a breach of trust either with the public or customers. This involves work schedules, superficial business information and other non-sensitive materials.

Confidential: Information and assets which is sensitive, business critical or otherwise legally obliged to be held confidential. Disclosure of this information will impact Blueberry IT in a way which disrupts or or threatens the company's daily operations. This involves, among else, information related to the privacy act, business procedures, and client information.

1.4 Network and security

Blueberry IT is a big target for crackers and espionage, this drove Blueberry ITs to the decision of hosting their own in-house information system, excluding the secure off-site back-up solution. Due to this they're now able to promise their customers a secure storage of information in compliance with the principles of confidentiality, integrity and availability(CIA).

1.4.1 Network

The company hosts their own web services inside the building. Maintenance of these services and the rest of the network is the responsibility of Blueberry's own IT department. The company network is divided in two parts; the internal network, and the Demilitarized Zone(DMZ). Connection between the two zones is at a minimum, and connections should always be initiated from the internal network which is handled by the network firewall.

To detect suspicious traffic, an NIDS(Network Intrusion Detection System) is placed on the internal network before the internal firewall. That way they will be able to log traffic in the sensitive area, and not be overwhelmed by traffic in the DMZ(Demilitarized Zone).

The internal network consists of a database server where information about customers and projects is stored. The network also has a VPN server because a lot of the consultants is working away from the office. The rest of the network consists of work machines, and a wireless network. The database server is only accessible from the cabled and not the wireless internal network. The internal network also consists of a file server which is used as a subversion repository, when the consultants work together on a project.

Blueberry IT have placed the web-server, DNS-server and the e-mail server in the DMZ. A simple overview of the network topology is presented in figure 3.

The database server contains a lot of information about customers and saved projects. This is highly sensitive information and access is based on a "need to know" basis. For example the receptionist has access to name, phone numbers etc, but not specific detail about what kind of tests was run against a specific business.

The VPN server is the only way into the internal network from the outside, and it has to be properly secured. Only the people who absolutely need it will have access to VPN. So all the consultants who work away from the office will have access, but accountants for example will not have access unless it is during special circumstances.

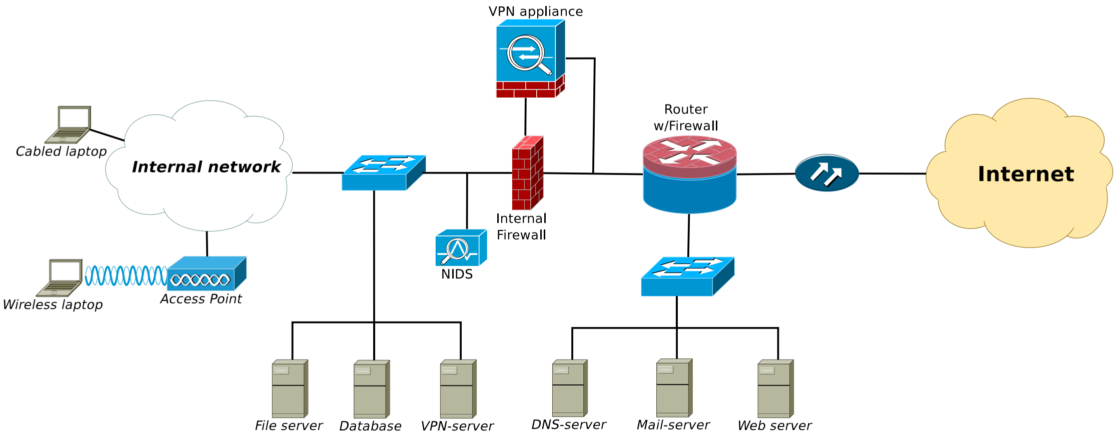

Figure 3: Simple overview of the network topology

1.4.2 Rules and regulations

The company have strict routines for mobile devices. Smart phones or tablets should never contain restricted or confidential information. Laptops is used a lot in the job, which means they contain restricted and confidential information. For this reason, the whole laptop is set up with full disk encryption by the IT department before the employee receives the computer.

USB sticks are a vital part of Blueberry ITs daily business and because these sticks are small and easy too loose, the same procedure applies to these as with laptops. Because of this it is the IT-departments job to set up and distribute USB-stick to the employees, and keep track of them. Personal USB sticks are allowed to be used, but not to store any business information. The only place employees can store business information is on media approved by the Blueberry ITs IT-department.

All employees is required to properly secure their work equipment as a part of the employee contract they have signed with the company. In return the company promises to give adequate education on how to secure their equipment. This kind of security measures includes anti-virus, secure communication, physical security, clear-desk policy and other relevant topics. These rules is set by the Blueberry ITs security policy and guidelines.

Blueberry IT have an incremental daily backup strategy and a complete back-up each Friday night. These back-ups is stored both on site and off site. The off site storage facility is at a secure third party service provider, which complies with the same policies and legislative demands as Blueberry IT.

1.4.3 Physical security

As said previously, the place is divided in two parts, the first floor which is shared amongst other companies and the second floor which contains the offices and server room. Figure 4 shows the overview of how the second floor floor plan looks like.

Physical access to the the premises is, like everything else, based on a ”need to know” basis. The figure is color coded where yellow means an open area where customer and other may be. Green is restricted to the employees of the company. Pink is restricted to some employees. Most

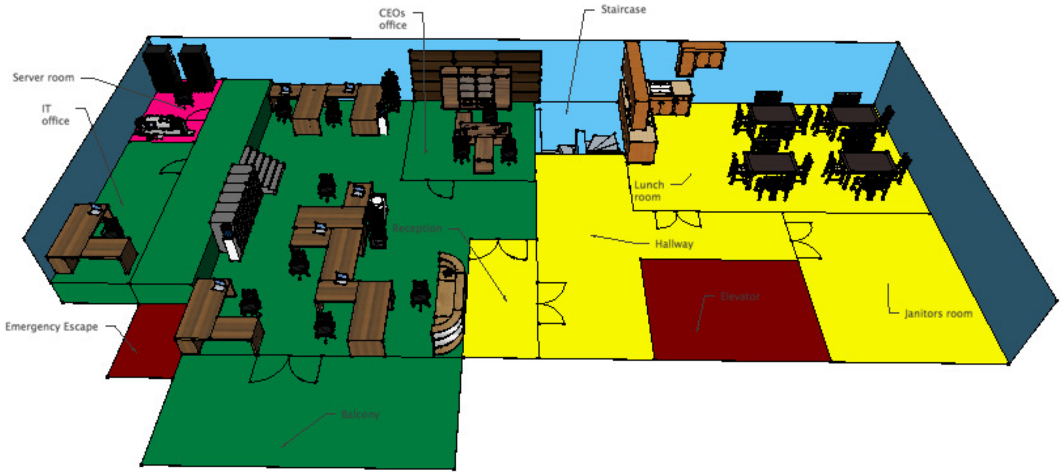

Figure 4: Schematic of the office space

of the office is very open, except the server-room, so people can walk around. The server room is only accessible by Blueberry ITs IT-department.

2 Business Contingency Planning Policy

Purpose

The purpose of this policy is to set the tasks Blueberry IT Consulting is required to perform. This is in order for Blueberry to be in compliance with both legislative and ethical demands. In addition this policy sets the framework for fronting the development, maintenance and training of business continuity plans.

Scope

The scope of this policy applies to all planning committees within Blueberry IT and other parties involved in the Business Contingency Planning procedures. The policy dictates the main guidelines for performing, delegating and initiating the contingency planning within each department of Blueberry IT as well as Blueberry ITs centralized contingency planning committee. The policy is a part of Blueberry ITs main information security policy and is distributed along with that. The Info.sec policy is classified as an internal document and is freely distributed amongst Blueberry IT Consulting employees.

Funding

- Blueberry IT is required to set aside 25% of their profits to Business Continuity development and training.
- The business continuity budget is divided as follows:

  20%: is set aside in a separate account as an emergency fund in case of a disaster strikes.
  30%: is used for revision of the current plans
  50%: is used for business continuity training.

- The task of delegating this money is the responsibility of the CFO

Organization

- The CEO is responsible for electing the Chief Business Continuity Planning Officer(CBCPO), from the following employees; Senior Prod. Manager, IT Consultants, IT Manager, SysAdmin, Chief Tech. Officer
- The CBCPO is the leader for the contingency planning management committee(CPMC)
- The CBCPOs is responsible for leading, monitoring and fronting the development of the Business Contingency Planning.
- The CBCPO is required to elect a BCP leader within each of the company's departments.
- The department BCP leader is a part of the main CPMC.
- The department BCP leader is in charge of its incident, disaster and business continuity planning committees.
- The department BCP leader is responsible for establishing the different planning committees within the department

- The CBCPO is responsible for supervising all departments development and maintenance of business continuity plans.

Training

- The Chief Management Officer(CMO) is required to implement measures to ensure user awareness in compliance with business contingency plans.
- The CMO is required to annually hold a mandatory in-house security seminar.
- During the security seminar all employees is guided through the different incident detection plans.
- The Chief Technical Officer(CTO) is required to send out a weekly e-mail regarding information security and contingency planning.
- The CBCPO is required to perform a structured walk-through or simulation for each scenario which endangers human life.
- The CBCPO is required to perform a structured walk-through or simulation for each of the ten incident response plans.
- All other contingency plans is to be annually executed as a ”chalk talk” by the departments planning committee and supervised by by the departments BCP leader.
- Special procedures during an incident is required to be executed as a training scenarios at certain intervals by the BCPO.
  - Every 6 months: Fire drill and emergency evacuation drills
  - Annually: Emergency shutdown of IT-systems
  - Each quarter: Test of information back-up system

Revision and development

- The CBCPO is responsible for developing and maintaining the Business Contingency Planning Policy
- The CBCPO is responsible for developing and maintaining the external *”Scenario Priority Document”*
- All attacks which has reasonable chance to endanger human life is automatically prioritized highest in the *”Scenario Priority Document”*
- The CPMC is responsible for developing and maintaining the business impact analysis.
- The department BCP leader is responsible for leading the development and maintenance of the contingency plans
- The department BCP leader is responsible for annually leading the revision of business contingency plans.
- Business continuity plans is required to be revised annually by the departments corresponding planning committee.
- The Business Impact Analysis is required to be revised annually by the CPMC.
- The ”Business Continuity Planning Policy” is required to be revised annually by the CPMC.
- The CEO is responsible for the annually revision of the ”salvage priority list”.
- The CFO/Operations Office is responsible for the quarterly revision of the telephone register and equipment placement register.

3 Business Impact Analysis

The business impact analysis(BIA) is divided into six parts, where the first part is the analysis of the risk each threat poses to Blueberry IT. This is followed by the Business Unit Analysis(BUA) which indicates how the business would suffer under the loss of a business function. The following table, table 1, is an overview of the different attack scenarios from the weighted business risk analysis(WBRA), followed by a detailed description of our weighting. The next table, table 3.2, is an overview of the different business functions Blueberry IT provide and how it would impact if it is lost. This is followed by a description of our weighting.

When this analysis is done we developed an external document which correlates the information from the WBRA and WBUA and gives a list of the scenarios of the highest priority. The top ten scenarios, from the ”Scenario Priority Document”, is then listed in this document depicting the reasons for choosing them and if they've been fully developed.

This section is followed by a detailed examination of the scenarios impact on Blueberry's functions and assets, before their ”worst”, ”best” and ”most likely” scenario to occur is described. Finally it is decided which plans to develop for each of the scenarios in section 3.6.

3.1 Weighted Business Risk Analysis

The WBRA describes each scenario which was discovered during the risk assessment. The two main categories are weighted equally with a 50-50 split between ”probability” and ”consequence”, though the ”consequence” is subdivided into ”damage cost” and ”repair cost” with a total weight of 50%. The ”repair cost” is weighted at 30% since the repair cost involves larger sums since it will involve upgrading equipment and future expenses. The ”damage cost” is weighted at 20% since the damage cost is one single blow to the economy, but since it is all part of the consequence will the difference not be larger than 20%. Each threat scenario is followed by a short description which describes the weights it's been given. Prioritization of each scenario is covered in the appendix and is base upon which resources is most valuable to the company. This means that preservation of human life is prioritized above any other scenario. The template which is utilized for the WBRA is extrapolated from table 2-2[5] in the book ”Principles of Incident Response and Disaster Recovery”.

Weighted Risk Analysis				
Threat	**Probability**	**Damage cost**	**Repair cost**	**Total**
Weighted score:	**0.5**	**0.2**	**0.3**	**1.0**
Information leakage	0,5	0,7	0,8	0,63
	High damage high risk. It also have a high cost because it is difficult to discover and repair.			

Continuing on next page

Weighted Risk Analysis ...continued				
	Probability (0.5)	Damage cost (0.2)	Repair cost (0.3)	Total (1.0)
Social engineering attack via e-mail	0,8	0,4	0,3	0,57
	Very likely that some phishing e-mails will go through the spam-filter, but it would most likely cause minimal damage because of routines.			
Destruction of project management system	0,2	0,8	0,9	0,53
	The likelihood of someone destroying the project management system is low, though in the case of such an incident the damage cost is high. The repair cost of this incident is extreme due to the fact they have to repair, replace and restore their systems.			
Flood	0,5	0,6	0,5	0,52
	The chances for a flood to occur is moderate, and the damage cost to business for inability to properly function is moderate. The repair cost is low since the flood doesn't directly affect them on the second floor.			
Unauthorized software installation	0,6	0,5	0,4	0,52
	The probability for this act is low, but it will usually take time and resources to repair.			
Loss of information	0,5	0,4	0,5	0,48
	This is not uncommon since information is often transported by portable storage mediums and on paper. The damage cost is moderate since storage mediums is encrypted and papers doesn't contain sensitive information. Repair cost is moderate since Blueberry must initiate an investigation and then implement proper counter measures.			
Lightning	0,3	0,7	0,6	0,47
	The chances for this incident to occur is low due to in-place countermeasures. The damage cost is high because all of Blueberry ITs IT-systems is connected to the infrastructure. Repair cost is also high since they need to repair and restore their systems.			
Worm on the internal network	0,3	0,7	0,6	0,47
	With strict access routines and well educated staff, the likelihood is small, the damage however could be very severe. It would take a moderate amount of time and resources to fix the network.			
Water leakage	0,3	0,7	0,6	0,47
	This happens rarely but can be costly and inconvenient when it does happen. Both in external costs and resources wasted handling the incident.			

Continuing on next page

Weighted Risk Analysis ...continued				
	Probability (0.5)	Damage cost (0.2)	Repair cost (0.3)	Total (1.0)
Destruction of the buildings structure	0,4	0,5	0,5	0,45
	This is a probable attack which may occur, and the costs of the damage is moderate since it will result in lost work time and business functionality. The repair cost is also moderate due to the fact it results in higher rent, along with a split repair cost.			
Unauthorized access to wireless network	0,5	0,4	0,4	0,45
	A basic WPA2 encrypted network is moderately easy to crack, but the network is very little used and would probably be detected early.			
Destruction of finance system	0,2	0,7	0,7	0,45
	Destroying the finance system will nearly never happen, but when it occurs the damage is high due to loss of customers accounts and billing information. The cost of repairing this system is also significantly high due to the restoration and improving of the system.			
Loss of user equipment	0,6	0,3	0,3	0,45
	This is not uncommon since users might break or loose their equipment. The damage cost is moderate since its only the equipment which is lost, the repair cost is also moderate since one has to replace the equipment.			
Fire	0,1	0,9	0,7	0,44
	The likelihood for a fire to occur is extremely low, but the damage cost is extreme. The repair cost is real high, but not extreme since the office is rented and the landlord is responsible for repairs.			
Unauthorized access to work laptop	0,4	0,6	0,4	0,44
	All laptops are encrypted so the most likely attack vector is via malware. It does contain sensitive information and could be used to further attacks so the damage could be large.			
Accidental deletion of data	0,7	0,3	0,1	0,44
	It is a high probability for that this error will occur, though usually this will not make a big difference to the organization mainly because of backups and subversion systems.			
Sabotage of access control equipment	0,5	0,4	0,3	0,42
	Sabotaging the access control system is probable since there is many able to access it. The damage cost is moderate, and the repair cost is low since it is an external service.			
Sabotage of project and finance system	0,3	0,3	0,7	0,42

Continuing on next page

Weighted Risk Analysis ...continued

	Probability (0.5)	Damage cost (0.2)	Repair cost (0.3)	Total (1.0)
	The chances of sabotaging either system is not very likely. The damage cost is low since the systems is properly secured and monitored. The repair cost is high due to the work needed to restore and improve the security, along with pursuing the incident.			
Hard-disk on backup server crashes	0,4	0,3	0,5	0,41
	The backup procedures are redundant which make sure that there are more than one copy. Most losses are based on time and resources spent.			
Unauthorized access to file server	0,3	0,7	0,4	0,41
	The file server is placed securely on the internal network and access to it would be hard. It does contain sensitive information that could be severe if it falls in the wrong hands. Backups would make it easy to restore.			
Functional bugs in 3rd party software	0,6	0,2	0,2	0,40
	These kind of bugs might have a slight impact on the business, but it will most likely be corrected fast and it will be barely noticeable.			
Theft of finances	0,3	0,6	0,4	0,39
	This incident happens rarely, but may happen either by error or deliberately. The damage cost of this is high since it will result in loss of finances and possibility of large faults in the accounting and loss of employees. The repair cost is moderate since it will result in a complete revision of the accounting and lawsuits.			
Sabotage of physical documents	0,4	0,3	0,4	0,38
	The chances of sabotaging physical documents is moderate since they are stored in a secured file cabinet in the office. The damage cost for sabotaging the documents are low, but the repair cost is moderate since it has to be done a complete check of the inventory.			
Unauthorized access to database	0,3	0,7	0,3	0,38
	The database is well secured on the internal network. Compromise could cause severe damage to reputation, but backups would mean that it is relatively easy to restore.			
Unauthorized access to VPN account	0,3	0,4	0,5	0,38
	The biggest attack vector here is weak passwords which there are strict routines against. This is an intermediate attack which an attacker could use to further compromise assets.			
Web site defacement	0,3	0,5	0,4	0,37

Continuing on next page

Weighted Risk Analysis ...continued				
	Probability (0.5)	Damage cost (0.2)	Repair cost (0.3)	Total (1.0)
	Unlikely since the web site is very static, but would cause severe damage to reputation because the company is in security. The cost to repair would be small because of extensive backups.			
Accidental removal of critical equipment	0,3	0,5	0,4	0,37
	The probability that this error will occur is low, but mistakes do happen. The impact of this will be moderate because critical equipment or information storage devices will be unaccounted for, but only temporary lost and not stolen.			
Unauthorized physical access to restricted areas	0,2	0,6	0,5	0,37
	These areas has enhanced security, which in return makes the cost of repairing and replacing the access control system higher.			
Unauthorized physical access to Blueberry's internal facilities	0,2	0,6	0,5	0,37
	The areas within Blueberry's office is also secured with enhanced security and the damage cost is covered by other threats. The repair cost will be the same as over.			
Filing error	0,5	0,1	0,3	0,36
	This happens from time to time, but no information is lost.			
Earthquake	0,1	0,5	0,7	0,36
	It is not likely for an earthquake to occur because of the location. The damage cost is moderate since it's only the inventory which will cost Blueberry and the repair costs is high since it is necessary to replace and restore their systems.			
Social engineering attack via phone	0,5	0,1	0,3	0,36
	It is moderately likely that because the numbers are freely available at the web site. The damage however would likely be small because of procedures against exactly this kind of incidents.			
Hard-disk on laptop crashes	0,4	0,3	0,3	0,35
	All employees are required to do backups regularly so most costs are directed at time lost replacing and configuring the new work environment.			
Hard-disk on file server crashes	0,4	0,3	0,3	0,35
	This would cause problems with the daily operation very fast, but good backup routines ensures that very little data will be lost.			
Hard-disk on database server crashes	0,4	0,3	0,3	0,35
				Continuing on next page

Weighted Risk Analysis ...continued				
	Probability (0.5)	Damage cost (0.2)	Repair cost (0.3)	Total (1.0)
	Good backup routines will make sure we do not loose a lot of data, but it still takes time recovering and that is work time lost.			
Hard-disk on web server crashes	0,4	0,3	0,3	0,35
	A backup server is in place so there will be very little downtime, most costs are directed towards setting the environment to the previous standards.			
Vendor stops supporting software	0,2	0,5	0,5	0,35
	Vendors rarely stop security updates to a product suddenly, if they do it might take considerable resources to update our systems.			
Loss of access credentials	0,6	0,1	0,1	0,35
	Loss of access credentials is not uncommon because of its regular use. The damage is not significant since employees is trained to report loss and it's used in combination with a six digit PIN. The repair cost is low since it is only a matter of disabling and issuing a new ID and PIN.			
Unauthorized physical access to the premises	0,3	0,4	0,4	0,35
	It is implemented good physical security, the damage is covered by other threats. The damage cost and repair cost is for covering repair and replacement of the access control system.			
Theft of information	0,3	0,2	0,5	0,34
	This occur rarely, but is not uncommon either. Even though the damage cost is low since the information is encrypted and physical information is not to be of a sensitive nature. Repair cost is moderate since Blueberry must initiate an investigation and then implement proper counter measures.			
Security bugs in 3rd party software	0,5	0,1	0,2	0,33
	There are strict procedures for updating when a security bug is found, so it will probably have very little impact on the business.			
Denial of service against assets	0,3	0,4	0,3	0,32
	It is unlikely that this would happen, competitors might use this to limit resources or to discredit us. This would cause moderately small damage because of an IT-department that would limit this attack immediately.			
Destruction of access control system	0,3	0,2	0,4	0,31
				Continuing on next page

Weighted Risk Analysis ...continued				
	Probability (0.5)	Damage cost (0.2)	Repair cost (0.3)	Total (1.0)
	The destruction of the access control system is not likely, but probable due to the fact of its exposed placements. The damage cost is low since it is leased by an external service provider. The repair cost is somewhat higher due to the process of restoring and enhancing the system.			
Destruction of emergency systems	0,3	0,2	0,4	0,31
	This is not likely, but still possible due to its natural placement and implementation. The damage cost is low since it is the landlords task to maintain it. The repair cost is moderate since it requires additional testing and repair work before its functional and up to code again.			
Theft of user equipment	0,2	0,3	0,4	0,28
	This incident happens rarely. When this incident occurs is the damage cost moderate since it contains information and access to the business secured network, though the entire system is encrypted and will wipe it self in case of theft. The repair cost is moderate since one need to replace the equipment and implement mitigating controls for the incident.			
Power outage	0,4	0,2	0,1	0,27
	This happens rarely and is usually very short when it does happen.			
Theft of access credentials	0,3	0,2	0,1	0,22
	This incident happens rarely, but when it occurs the damage is not severe since employees are trained to report this type of incident. The repair cost is low since it only involves disabling and issuing a new ID-card with a new PIN.			
Strong winds	0,3	0,1	0,1	0,20
	Strong winds occur, but will almost never cause any damage. The damage cost is low due to the fact Blueberry does not have any assets exposed other than it may be temporary loss of third party services. The repair cost is also low since it is the landlords responsibility to repair building damage and the service providers responsibility to repair damage beyond the demarcation point.			
Internet outage	0,2	0,1	0,1	0,15
	The ISP has a guarantee against downtime so the likelihood that this would happen is small. Downtime would likely be small so damage is minimal.			
Power brownout	0,2	0,1	0,1	0,15
	This will have very little impact on the operation because they still have some power.			

3.2 Weighted Business Unit Analysis

The WBUA describes the impact Blueberry IT will endure when a certain business function is unable to function properly. The table below is extrapolated from table 2.3[6] in the book ”Principles of Incident Response and Disaster Recovery". The weights are modified to into three separate factors with modified weights. The impact on profitability describes this functions ability for Blueberry to actually make money, because of the importance is why the weight is set to 60%. The impact on the public image is set to 20% since it is not as important as the ability to make money, neither is the impact on internal operations which is also set to 20%.

Function prioritization				
Business function	**Impact on profitability**	**Impact on public image**	**Impact on internal operation**	**Total**
Weighted score:	**0.6**	**0.2**	**0.2**	**1.0**
Establish new project	0,9	0,7	0,9	0,86
	Inability to establish new projects will result in severe profit loss since they can't start to work until they have a project area on the IT system. This will also impact the public image since they can't do any work on the project. The internal procedures will be extremely affected since they can't correlate and perform their work tasks.			
Manage invoicing	1,0	0,7	0,3	0,8
	This will impact the profit extremely and make the business unable to receive any money for their work. This will also severely impact the public image since it might seem like they are working on the black market. The internal functions will not be affected in any big way since they still can do their work.			
Customer support	0,9	0,9	0,3	0,78
	In the lack of having customer support will expose the business profit and public image for extreme damage. This is because it is a significant for upholding the public relations and function as a business. The internal operations will not be severely affected since they still will be able to work on their projects.			
Manage customer accounts	0,8	0,9	0,5	0,76
	Inability to properly manage customer accounts will result in loss of profit since this means they are unable to handle the customers accounting, information and history. This will as a result in a huge impact on the public image. The internal operations will be impacted, since Blueberry will be unable to properly maintain the customer accounts.			
Enroll new customers	0,8	0,2	0,9	0,7
	If they are unable to enroll new customers it will result in a severe problem for the profit and internal operations. The public image will not be affected in a severe way since it is possible to engage in the preliminary business functions anyway.			
Manage payroll system	0,5	0,8	0,7	0,6
	In lack of managing payroll system will the profitability receive a severe impact since employee morale will drop. This will in return result in disgruntled employees which will impact the public image. The internal operations will not function as usual since employees will strike, reduce their work effort and so on.			
Manage work projects	0,5	0,5	0,9	0,58

Continuing on next page

Function prioritization ...continued				
	Profitability (0.6)	Reputation (0.2)	Internal Operation (0.2)	Total (1.0)
	Lack of managing work projects will result in a sever impact on the internal operations since they will not be able to manage the area and CIA to where the work projects are stored. The profit will be impacted and since there will be pauses in the work. The public image will as a result of pauses and downtime be severely affected.			
Manage employee work	0,5	0,6	0,7	0,56
	If Blueberry can't correlate their employees work schedules it will result in a severe impact on business profit since they might miss meetings, double book an employee. This results in severe loss of public image due to the fact that management is not functioning properly. The internal operations will also be severely impacted since some employees will be in disarray and have a low work morale.			
PR campaigns	0,8	0,1	0,1	0,52
	Inability to hold PR campaigns will severely reduce their income since other businesses will not know of their existence. The public image will not be affected, though it will not grow either. The internal operations will also not be affected.			
Terminate employee	0,5	0,5	0,6	0,52
	If Blueberry is unable to terminate an employee from its position is the resulting loss in profit severe since they have to pay for an employee which should have been fired. This results in a sever impact on the public image since they can't fire employees which is bad for business. The resulting internal operations is affected by this since the work morale is lowered.			
Website advertisement	0,3	0,8	0,1	0,36
	Lack of advertisement through their website does not severely impact the profitability, but will severely affect the public image since they are an IT-based company. The impact on internal procedures is also minimal, though it will result in some extra work for the IT-service.			
Erase project information	0,2	0,5	0,2	0,26
	The inability to erase project information will not cause any severe problems for the internal operations and profits. This will result in a severe impact on the public image since they can't erase sensitive information or information which does not belong to Blueberry IT.			
Terminate project	0,2	0,5	0,2	0,26
	If Blueberry can't terminate a project it will not impact their profit in a severe way. It will however affect the public image since they customer will not have their project terminated as of contract agreements. It will not have any significant impact on the internal procedures since they will continue as usual.			
Erase customer	0,1	0,6	0,2	0,22

Continuing on next page

Function prioritization ...continued				
	Profitability (0.6)	Reputation (0.2)	Internal Operation (0.2)	Total (1.0)
	This is will not impact the profitability at all, but will impact the public image since they won't be able to erase sensitive materials which does not belong to them.			
Update finance records	0,2	0,2	0,3	0,22
	Inability to update finance records will not result in any significant profit loss and public image since it is not based on the actual service Blueberry provides. It will however result in a loss of internal operations since it means they will not be able to properly manage the accounting history.			
Hiring employees	0,2	0,1	0,2	0,18
	If Blueberry IT lacks the ability to hire new employees it will not affect the public image, though it will have a little impact on the profit and the internal procedures, since one will not be able to replace employees when needed.			

3.3 Incident Prioritization

Based on the risk analysis and business unit analysis we've have decided to develop plans for the scenarios depicted in table 3. This table shows the top ten scenarios from the external *"Scenario Priority Document"* which is maintained separately from the business contingency planning document to avoid confusion during an incident. **This list of scenarios is prioritized and applies to both incident and disaster scenarios. A disaster scenario will take precedence over an incident scenario. A scenario which threatens human life will always take precedence over any other scenario**. This means that in case there is multiple attacks on Blueberry IT Consulting, occurring at the same time, the attack-scenario highest on this list is to be dealt with. There is some exceptions to this, as described above. In addition to those points one might respond to several incidents if there is enough manpower to sufficiently respond to several attacks.

The prioritization is based on the weighting of the attacks impact on business functions, but due to statements in the policy will preservation of human life always take precedence over all other attacks.

Incident prioritization		
#	**Scenario**	**Description**
1	Fire	Since this attack endangers the life of the employees and its potentially devastating impact it is of the highest priority. This attack could potentially destroy Blueberry ITs HQ and all assets could be destroyed beyond the point of recovery. Due to off-site back-up routines will very little information be lost. **It has not been developed any plans for this attack, due to time limitations and should be developed within the next six months.**
		Continuing on next page

Incident prioritization ...continued		
#	Scenario	Description
2	Flood	This attack has a smaller chance of endangering human life, but can still occur with such severity. In addition to the factor of human life there is factor of damage to Blueberry ITs HQ which depending of the severity can create huge structural damage. This would involve construction work and downtime of information systems. **This attack is fully developed and has three separate plans; incident notification, incident response, disaster and continuity as described in the subordinate plan addendum.**
3	Sabotage of project and finance system	Sabotage of either system is an immediate danger to Blueberry IT Consulting due to the systems highly sensitive classification. This attack could result in severe loss of profit, embezzlement, and extreme loss or corruption of information. The reason why this takes precedence over so many incident is because of the potential ramifications it has towards the customers. **It has not been developed any plans for this attack, due to time limitations and should be developed within the next six months.**
4	Destruction of project management system	Destruction of the project management system is very important due to its sensitive nature and potential loss towards the business. A potential loss of this asset will render the business unable to give customer support or effectively work on a project in a secure environment. Though it is not a very likely scenario it will still have a big impact on Blueberry IT as a company. **It has not been developed any plans for this attack, due to time limitations and should be developed within the next six months.**
5	Destruction of finance system	Destruction of the finance system is not as severe as the destruction of project management system, but since this will render Blueberry IT unable to receive, distribute or maintain a financial history it is very important. During such an attack employees will not be able to receive paychecks, Blueberry IT can't distribute invoices etc. which in turn will make employees gradually reduce their work effort. Though it is not a very likely scenario it will still have an extreme impact on Blueberry IT as a company. **It has not been developed any plans for this attack, due to time limitations and should be developed within the next six months.**
6	Installation of Unauthorized Software	This attack is very likely to happen due to the wast amount of software available on the Internet. Installation of such software could potentially compromise or destroy the entire information system at Blueberry ITs HQ. **This attack is fully developed and consists of; incident notification, incident response, disaster response and continuity plan.**

Continuing on next page

Incident prioritization ...continued		
#	Scenario	Description
7	Unauthorized access to file server	This attack will occur do to many people have access to the server and access credentials could be left open due to management error. The severity of this attack is of such proportions that any malicious intent will result in a severe loss for Blueberry IT. **It has not been developed any plans for this attack, due to time limitations and should be developed within the next six months.**
8	Functional bugs in 3rd party software	This attack could result in loss of information either on the off-site back-up or the internal information system, or have a huge impact on the overall business performance due to problems with payroll or other software solutions. **It has not been developed any plans for this attack, due to time limitations and should be developed within the next six months.**
9	Accidental deletion of data	This scenario is bound to happen in all degrees of severity, though it is most often a trivial incident. Even though it is mostly trivial it also got the potential to become catastrophic if one accidentally deletes finance information or back-up tapes and other sensitive materials. Because of its probability rate and its potential to cause an extreme impact on Blueberry IT it has to be a response plan for it. **It has not been developed any plans for this attack, due to time limitations and should be developed within the next six months.**
10	Social engineering attack via e-mail	Due to todays many ways to perform social engineering it is bound to happen, either because the attacker wants information about Blueberry ITs customers or to gain access to Blueberry IT itself. This attack alone will not have serious consequences, but can lead to more serious attacks. **This attack is fully developed and consists of; an incident notification and response plan.**

Table 3: Top ten scenarios

3.4 Attack success scenario development

This section describes the scenarios details. This involves describing which assets are at risk, what damage the assets are exposed to, and which threat agents and vulnerabilities is involved. The template is extracted from the book ”Principles of Information Security and Disaster Recovery”[7]. The purpose of this is to outline each threat scenarios damage extent when it succeeds, before continuing with its corresponding ”potential damage assessment”.

Installation of Unauthorized Software	
Date of analysis:	March 2, 2012
Attack name/description:	Installation of unauthorized software as a result of human error
Threat agents:	User carelessness/awareness

Continuing on next page

Installation of Unauthorized Software ...continued	
Known or possible vulnerabilities:	• Poorly revised user permissions • Poorly training of user awareness • Poorly security culture focus, carelessness
Likely precursor activities or indicators:	Change in system behaviour
Information assets at risk from this attack:	All information systems
Damage or loss to information assets likely from this attack:	• Information system(s) • Stored information • Organization reputation
Other assets at risk from this attack:	In worst case scenario: Partner(s) assets
Damage or loss to other assets likely from this attack:	None likely
Immediate actions indicated when this attack is under way:	Isolate system(s), revoke user permissions
Follow-up actions after this attack was successfully executed:	Debrief, user awareness training
Comments	None

Flood	
Date of analysis:	27.02.2012
Attack name/description:	Flood impacting Blueberry IT Cons. HQ
Threat agents:	• Spring flood from the mountains during late late April/early May. • Flood during a heavy rain season • Faulty storm drain system
Known or possible vulnerabilities:	• The building is located in an area where flood water may cut off the access to the area • Parts of the electrical system may need to be disabled, due to security reasons. • The generator will not be operational if it is water in the machine room
Likely precursor activities or indicators:	• Heavy rain fall in a short period of time • Announcements from weather reports and local authorities • Rapid increase of the water levels • Rapid melting of ice in mountains • Unusual behaviour of storm drains • Reports of faulty storm drains
Information assets at risk from this attack:	• Infrastructure and servers • Physical and digital media • User equipment • Employees
	Continuing on next page

Flood ...continued	
Damage or loss to information assets likely from this attack:	• May result in temporary loss of infrastructure and servers • Will result in downtime for the emergency generator • May result in temporary loss of employees
Other assets at risk from this attack:	• Office spaces • Building structure • External services
Damage or loss to other assets likely from this attack:	• May result in temporary loss of access to the office • May result in permanent/temporary damage to the building • May result in loss of external services
Immediate actions indicated when this attack is under way:	• Shut down all unnecessary systems • Back up the entire system to a secure facility • Evacuate equipment and set up an external business facility
Follow-up actions after this attack was successfully executed:	• Review the performance of the incident response handling • Perform recovery of the damage done to the building • Move the hardware back to the main office • Shut down the external facility
Comments	None at this time

Social Engineering Attack	
Date of analysis:	March 1, 2012
Attack description:	Social engineering attack via e-mail or phone
Threat agents:	• Competitor • Hackers • Organized crime
Known or possible vulnerabilities:	• Easy to spoof an e-mail address • E-mail addresses available online • Phone numbers available online
Likely precursor activities or indicators:	Possibly announcement from security firms
Information assets at risk from this attack:	• Information about infrastructure • Sensitive information about employees
Damage or loss to information assets likely from this attack:	Personal information about employees
Other assets at risk from this attack:	None likely
Damage or loss to other assets likely from this attack:	None likely
Immediate actions indicated when this attack is under way:	• Alert all employees • Start investigating who is responsible • Discover if it was successful

Continuing on next page

Social Engineering Attack ...continued	
Follow-up actions after this attack was successfully executed:	• Investigate what the perpetrator wanted. • Investigate what the information was used for. • Review procedures and make appropriate changes. • Review staff involved and consider additional training.
Comments	None at this time

3.5 Potential Damage Assessment

The following describes the best, worst and most likely scenarios in great detail. The template which been used is extracted from the book ”Principles of Incident Response and Disaster Recovery”[8]. The three different scenarios is detailed in four steps each. It starts with a detailed description of the incident and how the attack and countermeasures would behave. This is followed by a weight and a text describing the scenarios risk. The weight is of an arbitrary value like; *”none”, ”low”, ”moderate” or ”high”*. The ”Scenario Risk” is followed by the ”scenarios cost to the organization”, which starts with an arbitrary weight followed by a description of the cost. The last part of the scenario description is the ”probability for the attack scenario to continue and spread”, which starts with an arbitrary weight followed by a description of the probability.

Installation of Unauthorized Software: addendum	
Date of analysis	03.03.2012
Attack name/description	Installation of unauthorized software
Comments	None at this time
Best case scenario for this attack	
Description: The best case scenario is when an employee understands that this is an illegal activity and calls the IT-support to get an authorization to install it. Then the software is investigated and authorized or banned. **Scenario risk:** Low, in a firm like Blueberry employees are trained not to install such software on their job computers. **Scenario cost to organization:** Low, the employee training can be done relatively easy and the extra work caused by the incident would at most require an hour of work to clean up. **Scenario probability of attack continuing and spreading:** Very low, depends on the software installed also, but in a best case scenario there will be no probability of spreading malware.	
Worst case scenario for this attack	
Description: When unauthorized harmful software is installed, and it gains root-access to critical systems. Due to network segmentation and good password policy only one area of the company network can be compromised, but that may be enough to gain access to organization critical information. Assets value and integrity might be at stake. **Scenario risk:** Low, since Blueberry have mostly has employees with willingness to have a good security culture and mindset. **Scenario cost to organization:** High, in worst case customers and website visitors might be attacked as well. **Scenario probability of attack continuing and spreading:** High, if gone unnoticed this will continue to spread across the entire network until it is cleaned from all systems.	
Most likely case scenario for this attack	

Continuing on next page

Installation of Unauthorized Software ...continued
Description: The most likely scenario is that the employee installs a software program, but does not infect the system or network. Though this means extra work for the IT-service for performing cleaning and repairing the system. **Scenario risk:** Moderate, due to human error this scenario might spread around the business. Even though the software does not contain any malware it might expose vulnerabilities which will not be patched by the IT-service. **Scenario cost to organization:** Low; a few extra hours of work for cleaning and restoring the system to its original state. **Scenario probability of attack continuing and spreading:** High; if gone unnoticed and it does not impact service or performance this attack will continue. Depending on the popularity of the software, employees might spread it throughout the business.

Flood: addendum	
Date of analysis	03.03.2012
Attack name/description	Flood of property
Comments	None at this time
Best case scenario for this attack	
Description: The best case scenario is when it is a small and short flood, and the in place drainage systems is able to divert the flood water away from the property. The current drainage system outside is able to divert the normal spring flood occurring around April/may, but not the extreme cases of flood. **Scenario risk:** Moderate; the assets for mitigating these threats is mostly out of Blueberry's control. Since the sewer and water systems is publicly owned and maintained, it is up to the local government to perform maintenance work and upgrades. **Scenario cost to organization:** Very low; the cost of this scenario is insignificant to the organization due to the fact that it does not affect the business. **Scenario probability of attack continuing and spreading:** Very low, the flood will not spread, and it will not continue since it is a short flood.	
Worst case scenario for this attack	
Description: The worst case scenario is that the mitigating controls fails and the entire property is flooded, including the basement levels and 1st floor. This involves severe damage to the buildings structural integrity and hindering of employees to access the building, in addition it would mean that the power generator is unable to function. In the case that Blueberry doesn't have an alternate business site, the cost of downtime and repositioning is significantly high. **Scenario risk:** High; the only way to mitigate this attack is by move the entire business, to a less exposed environment or perform serious construction work to the building to properly divert the water stream. **Scenario cost to organization:** Moderate; even though the cost of repairing the damages and draining the water out of the facility is high it is not a severe cost to Blueberry since they are renting offices from the landlord. Though, while the renovation and repairs is ongoing the cost of downtime and set-up of alternate location is moderate. **Scenario probability of attack continuing and spreading:** Moderate, because of the placement of Blueberry's facilities the spreading of flood is not significant, but the flood will continue for a prolonged time until it dissipates.	
Most likely case scenario for this attack	

Continuing on next page

Flood ...continued
Description: The most like scenario is that there will not be any internal flooding of the building, but the employees will be unable or experience trouble gaining access to the premises. This is due to flooding of the outside premises and the storm drains inability to properly divert the flood water. **Scenario risk:** Low; the risk of this scenario is low since there is no danger to the business assets, other than the inability to work at the office. Since the project management system, and all supporting IT-systems, is up and running the employees will be able to work on their current projects. **Scenario cost to organization:** Moderate; the cost of this scenario depends on the length and severity of the flood, but a flood that usually lasts two days and is making it hard or impossible to access the premises. This makes the cost moderate since it means some lost work hours, and inability to properly maintain business procedures. **Scenario probability of attack continuing and spreading:** Moderate; the attack will not spread, but it will continue until it dissipates, which is most likely between 1 to 5 days.

Social Engineering Attack: addendum	
Date of analysis	05.03.2012
Attack description	Social engineering attack targeted at the organization
Comments	None at this time
Best case scenario for this attack	
Description: The best case for this attack would that the target understands that a phishing attack is happening and the target follows protocol and warn her superiors. **Scenario risk:** Low; minimal time and resources will be spent. **Scenario cost to organization:** Low; the organization has to spend time training the employees, but it does not take up much time each year. **Scenario probability of attack continuing and spreading:** Very low.	
Worst case scenario for this attack	
Description: The worst case happens if user has forgotten his training and the attacker gets access to company assets. This can lead to further attack. **Scenario risk:** High; this attack would most likely lead to further attacks and compromise of several other systems. **Scenario cost to organization:** High; highly sensitive information can go astray this way and the amount of resources cleaning up after a big attack could possibly be massive. **Scenario probability of attack continuing and spreading:** Very high.	
Most likely case scenario for this attack	
Description: The most likely case for this scenario is that the target might supply the attacker with some information about employees, but nothing that is highly sensitive. This can happen in a phone call where the attacker pretend to be someone else, then it is easy for an attacker to obtain some information, but the employee will most likely remember his training and not give up any sensitive information **Scenario risk:** Low; the information the attacker has obtained will have low value. It might be slightly useful as information gathering, but nothing else. **Scenario cost to organization:** Low; The only cost is slight loss of time. **Scenario probability of attack continuing and spreading:** Low; although information is lost, it is not sensitive and unlikely that it can be used in further attacks.	

3.6 Subordinate Plan Classification

The last part of the BIA is the Subordinate Plan Classification which dictates what plans is to be made for the corresponding attack scenario and who it is passed on to. This template used is taken from the book ”Principles of Incident Response and Disaster Recovery”[9].

Install. of Unauth. Software: subordinate plan classification	
Date of analysis	07.03.2012
Attack name/description	Installation of unauthorized software
Threat agents	User carelessness/awareness
Known or possible vulnerabilities	• Poorly revised user permissions • Poorly training of user awareness • Poorly security culture focus, carelessness
Subordinate plan classification	
Description: This attack is passed to the incident response planning team for developing incident response plans for the attack. After the incident response plans are finished, they, along with this document shall be passed on to the disaster recovery planning team. They will then develop disaster recovery plans in case of escalation of the initial incident. This incident will require a business continuity plan to be developed. This plan must dictate how to temporary replace and restore the original IT-systems when a disaster has occurred. At both levels the mitigating actions should specified along with current policies and guidelines for properly removing software and contaminated systems. In addition it should be specified guidelines for properly upholding sanctions for breach of policy.	

Flood: subordinate plan classification	
Date of analysis	06.03.2012
Attack name/description	Flood
Threat agents	• Spring flood from the mountains during late late April/early May. • Flash flood during a heavy rain season • Faulty storm drain system
Known or possible vulnerabilities	• The building is located in an area where flood water may cut off the access to the area • Parts of the electrical system may need to be disabled, due to security reasons. • The generator will not be operational if it is water in the machine room
Subordinate plan classification	
Description: This attack is passed to the incident response planning team for developing incident response plans for the attack. After the incident response plans are finished, they, along with this document shall be passed on to the disaster recovery planning team. They will then develop disaster recovery plans in case of escalation of the initial incident. This plan also requires a business continuity plan for relocating to a temporary location and back to a permanent location. At both levels the mitigating actions should specified along with blueprints of the storm drains and current building structure.	

Social Engineering Attack: subordinate plan classification	
Date of analysis	March 6, 2012
Attack name/description	Targeted social engineering attack via phone or e-mail.
Threat agents	• Competitor • Hackers • Organized crime
Known or possible vulnerabilities	• Easy to spoof an e-mail address • E-mail addresses are available online • Phone numbers available online
Subordinate plan classification	
Description: This case is passed to the incident response planning committee for developing an incident response plan for this attack. Mitigating actions should be specified, including user awareness and review of protocols.	

4 Incident response plan

All attack scenarios dictated, by the ”*subordinate plan classification addendum to end case*”, to create an incident response plan is added to this chapter. The template used for all incident response plans is taken from the ”Principles of Incident Response and Disaster Recovery”[10]. This details each action to be taken during an incident, when the incident is declared over, what actions to be taken when the incident is over, when the restoration process is over and which actions is to be taken in advance to an incident.

In addition to the incident response plan it is added a shortened incident response plan which describes the notification response corresponding to the incident. This describes how the person which discovered the attack and which action they should take when notifying the correct personnel.

4.1 Installation of Unauthorized Software

Installation of Unauthorized Software	
Incident Detection Plan	
Attack type:	Unauthorized installation of software
Trigger:	Suspicious of a co-worker.
Reaction force and lead:	IT-department Employee executive
Notification method:	Phone E-mail Direct contact
Response time:	10 minutes
Actions to be taken during this response:	
1: Notify the IT-department by phone, e-mail or direct contact.	
2: The IT-department decides whether the incident is real or not and executes the incident response plan.	
Incident is ended and actions cease when:	
- The IT manager has determined if the incident is real or not and has taken control over the incident.	
Preparation actions to be integrated into IR plans before incident response plan is needed:	
1: Awareness training for employees	

Installation of Unauthorized Software	
Incident Response Plan	
Attack type:	Unauthorized installation of software.

Continuing on next page

Installation of Unauthorized Software ...continued	
Incident Response Plan	
Trigger:	Alert from employee. Review of system logs.
Reaction force and lead:	Lead is IT-department employee on duty, reaction force is dynamically allocated of the company dependent on the scale of the incident. If needed CEO and IT-manager are called in to assist.
Notification method:	Phone Direct contact E-mail
Response time:	2 hours
Actions to be taken during this response:	
1: Debrief the employee that owns the system which the software is detected on and find out the following: - Its origin - How it was installed - Other systems which its been installed on - Other employees which may have the software	
2: Isolate the system.	
3: Examine if the software is a potential malware.	
4a: If malware; perform in-depth analysis of the system to check for damage.	
4b: If not malware; isolate the infected systems from the internal network.	
5a: If the damage of the malware has gained access to one of the following assets, the incident is escalated to disaster: - The project management system - The customer database - The finance system - Security systems, like firewalls, routers or NIDS - The public website	
5b: Uninstall software and secure the systems.	
6: Review systems after uninstallation of software.	
Incident is ended and actions cease when:	
- All infected assets has been cleaned and are ready to be placed back into the network. - The incident has been escalated to a disaster.	
Actions to be taken after incident response is ended:	
1: Review current rules and regulations and change if necessary.	
2: Interview the people responsible for the incident and issue an official reprimand if it is nessecary.	
3: Create a incident report and distribute it to the CEO and all other parties involved.	
4: If not malware; analyse if the software could be usefull to business procedures.	
Incident follow-up is ended and actions after the incident is complete when:	
- Reports are finished. - Managers are briefed on the incident. - Regulations has been changed where necessary. - Official reprimands has been issued.	
Continuing on next page	

Installation of Unauthorized Software ...continued
Incident Response Plan
Preparation actions to be integrated into IR plans before incident response plan is needed:
1: Develop rules to use company equipment.
2: Create user awareness of the risks.

4.2 Flood

Flood	
Incident Detection Plan	
Attack type:	Flood
Trigger:	Rapidly rising water level Local weather reports Notice of evacuation or flood warning from local authority Reports from employees
Reaction force and lead:	IT-manager, back-up CEO
Notification method:	Verbal communication by telephone, physical interaction or physical.
Response time:	Maximum 12 hours from detection to notifying Helpdesk and maximum 24 hours from being notified until an incident is discarded and relayed to incident response task force.
Actions to be taken during this response:	
1: Notify the current IT-manager by phone, text or physical verbal communication and explain the situation	
2: The IT-manager performs an initial assessment of the reported incident	
3: The IT-manager decides if the incident is to be relayed to the incident response task force or not.	
4: The IT manager notifies the incident task force leader; CEO.	
Incident is ended and actions cease when:	
- The incident is discarded. - The responsibility of the incident is shifted on to the task force leader: CEO	
Preparation actions to be integrated into IR plans before incident response plan is needed:	
1: Training the IT-managers to correctly assess a flood scenario.	
2: Training the employees in how to notify	
3: Exercise routines for the call roster.	

Flood	
Incident Response Plan	
Attack type:	Flood
Trigger:	Report of incident from Helpdesk
Reaction force and lead:	Leader: Chief Executive Officer, back-up CEO Force: Chief Technical Officer, back-up CFO This incident can seize as much manpower as needed depending on the incident.

Continuing on next page

Flood ...continued	
Incident Response Plan	
Notification method:	Verbal interaction either by VoIP, telephone or physical interaction.
Response time:	Maximum 24 hours
Actions to be taken during this response:	
1: Perform an assessment of the reported incident to achieve an overview of the situation.	
2: Mobilize the incident response team.	
3: Gather all employees in main office and perform a head count of all employees	
4: If there's missing any employees, confirm their whereabouts or search the building for them.	
5: Evacuate all unnecessary personnel from the premises	
6: Notify the landlord and building manager, if they weren't the notifiers.	
7: Notify the local authority, if they weren't the notifiers.	
8: Inspect the sub-levels for flooding	
9a: If flooding inside building or the severity escalates; escalate to disaster.	
9b: If not; engage back-up procedures of finances and project management systems.	
10: If needed, request help from the local authority to help with mitigating the incident.	
Incident is ended and actions cease when:	
- All employees is evacuated from the premises - All infrastructure is properly secured - The incident is properly mitigated	
Actions to be taken after incident response is ended:	
1: Assess the damage level	
2: If data was lost, recover the most recent back-ups.	
3: Restore the most essential business functions to normal operation.	
4: Restore the rest of the business functions to normal operation	
5: Assess all costs the incident caused.	
6: File claim to insurance company	
7: Hold an AAR-meeting.	
Incident follow-up is ended and actions after the incident is complete when:	
- Fully operational business management is restored at at primary or secondary location	
Preparation actions to be integrated into IR plans before incident response plan is needed:	
1: Training for performing an emergency evacuation of the premises	
2: Training for performing a correct emergency back-up procedure	
3: Training the CSO to perform a correct assessment of a flood situation.	
4: Periodic review of the incident response plan.	

4.3 Social engineering attack

Social Engineering Attack	
Incident Detection Plan	
Attack type:	Social engineering attack
Trigger:	Suspicious e-mail, phone call or visitor.
Reaction force and lead:	All employees.

Continuing on next page

Social Engineering Attack ...continued	
Incident Detection Plan	
Notification method:	E-mail, phone or verbal communication.
Response time:	5 min.
Actions to be taken during this response:	
1: Determine if the attack is real.	
2: Alert the IT department by phone.	
Incident is ended and actions cease when:	
- The IT-department has been alerted.	
Preparation actions to be integrated into IR plans before incident response plan is needed:	
1: Awareness training for employees	

Social Engineering Attack	
Incident Response Plan	
Attack type:	Social engineering
Trigger:	One or more of the following: ● Employee alerts according to their IR plan. ● Suspicious e-mail. ● Suspicious phone call. ● Suspicious visitor.
Reaction force and lead:	IT manager is in charge of the IR plan. The IT manager is also in charge of delegating tasks as he see fit over other employees in the IT department.
Notification method:	E-mail, phone or verbal communication.
Response time:	20 min.
Actions to be taken during this response:	
1: Determine which employees have been targeted.	
2: Determine what kind of information was lost.	
3: Make sure the attack has stopped by alerting the appropriate employees.	
4: Protect any assets which security might have been weakened by the information lost.	
Incident is ended and actions cease when:	
- When employees have been alerted and the attack has stopped.	
Actions to be taken after incident response is ended:	
1: If sensitive information about employees or customers have been lost, alert the affected parties.	
2: Document the timeline and patterns of the attack.	
3: Determine if protocols were followed.	
4: Determine if more training is required.	
5: Determine if a change in protocol is needed.	
Incident follow-up is ended and actions after the incident is complete when:	
- All affected parties have been notified. - The reason the attack was successful/unsuccessful has been found.	
Preparation actions to be integrated into IR plans before incident response plan is needed:	
1: Define clear policy and procedures as to what the employees should do.	
Continuing on next page	

Social Engineering Attack ...continued
Incident Response Plan
2: Define clear policy and procedures as to what the IT department should do.
3: Perform a walk-through on different incident at least once a year. The Chief Technical Officer is in charge of this walk-through.
4: Perform a simulation at least once a year. This simulation will be started by the Chief Technical Officer and should come as a surprise to all other parties involved.
5: Review policy at least once a year regardless of incidents.

5 Disaster response plan

The disaster response plan describes the actions to be taken by the disaster response team during an escalated incident scenario or disaster scenario. The template is extracted from ”Principles of Information Security and Disaster Recovery”[11] and describes the response plan step by step. First it describes the same as incident planning of the organizational aspect before the instruction set is shown. Then it describes the steps to take during the disaster, before stating when a disaster is officially ended. Then it might be over or it might escalate and the business continuity plan needs to be invoked. The plans also covers recovery on the primary site regardless of the business continuity plan.

5.1 Installation of Unauthorized Software

Installation of Unauthorized Software	
Disaster Response Plan	
Disaster type:	Unauthorized installation of software
Trigger:	System behavior Employee notification Confidential information available in public domain
Team lead:	CTO and System Administrator. Backup is IT-manager and CEO.
Notification method:	Calling Direct contact Email
Response time:	Should be initiated within 10 minutes
Actions during disaster:	
1: Notify everybody on the DR-notification list	
2: Prevent spread out of Blueberry ITs LAN by severing the hardlines.	
3: Determine the spread of the attack in correspondence with proper procedure for handling potential evidence	
4: Isolate the infected systems in correspondence with proper procedure for handling potential evidence	
5: Take down the infected machines in correspondence with proper procedure for handling potential evidence	
Actions during disaster are complete when:	
- The disaster is properly mitigated - Infected systems is taken offline and isolated	
Actions after disaster:	
1: If IT-systems was taken down, assess the need for replacement	
2: If replacement is needed; invoke the corresponding BCP for replacing the IT-systems	
3: Determine where the attack originated, if a targeted attack on Blueberry IT engage the local authority.	

Continuing on next page

Installation of Unauthorized Software ...continued
Disaster Response Plan
4: Notify the system distributor/owner of the vulnerability
5: Close the vulnerability
6: Determine the extent of the damage
7: Correlate and recover lost or damaged information
8: Properly clean and restore the IT-system
9: Restore proper business function to the original IT-systems
10: Close the case with a formal report and debrief all involved parties
11: Hold an AAR-meeting
Actions after disaster are complete when:
- The original or new IT-system is restored to normal business functionality
Actions before disaster:
1: User awareness training
2: IT-department training within response and digital forensic
3: Walkthrough of the IR/DR-plans

5.2 Flood

Flood	
Disaster Response Plan	
Disaster type:	Flood
Trigger:	Escalating incident which threatens structural integrity Internal flooding Severe flood Notice of evacuation from local authority
Team lead:	CEO, back-up Chief Technical Officer IT manager, back-up CFO Team lead may seize as much manpower as needed.
Notification method:	Verbal communications either by telephone or physical interaction.
Response time:	Maximum 5 hours before initiating the disaster response plan
Actions during disaster:	
1: Assess the situation with internal flooding and flood severity in mind.	
2: Perform emergency shut down of all IT infrastructure	
3: If possible; evacuate all employees from the premises	
4: If not possible; notify local emergency personnel to help out with the evacuation	
5: Notify local authority to help out with performing activities to mitigate the incident.	
6: Restrict access to the premises	
Actions during disaster are complete when:	
- IT-systems is securely shut down - Employees is successfully evacuated from the premises - The disaster is successfully mitigated	
Actions after disaster:	
1: Notify everybody on the DR-notification list	
2: Assess the damage level and time to restore it to its pre-disaster state.	

Continuing on next page

Flood ...continued
Disaster Response Plan
3: If there is water inside the building: Hire an external contractor to pump out the remaining water.
4: If business relocation or replacement of IT-system is needed invoke the corresponding Business Contingency Plan
5: Restore functionality to the IT-system
6: Correlate information and restore any lost information.
7: Perform damage assessment and file claim to insurance company
8: Restore normal business function at primary location.
9: Hold an AAR-meeting to review the actions taken during the incident.
10: Resume normal business functionality.
Actions after disaster are complete when:
- Full business functionality is restored at primary or secondary location
Actions before disaster:
1: Review the disaster response plan as instructed by the policy
2: Training for emergency evacuation as instructed by the policy
3: Review systems for diverting floods
4: Set up a contractual agreement with a business for renting submersible water pumps for the aftermath.
5: Maintaining mutual relocation agreement with Strawberry Inc.

6 Business Continuity Plan

The BCP dictates how Blueberry IT is to transition from a fixed state to a temporary state, before transitioning back again. So in this case we have developed two possible situations where business continuity is needed. One is when the IT systems are down and the company has to set up a new temporary IT system. Another scenario is when the whole company has to relocate for some period of time. In the case of flood, it might be necessary to implement both plans.

6.1 IT-system replacement

Replacement of the IT-system
Business Continuity Plan
Prerequisites:
The IT-system is partially down and needs temporary replacement. The IT-system is completely down and needs temporary replacement.
Actions during BCP:
1: Determine what system is lost
2: Prioritize the recovery process
3: Obtain suitable replacement system
4: Recover lost data from backup
5: Restore function to the system
Business Continuity actions is ended when
- The IT systems business functionality is properly restored.
Relocating back to primary systems:
1: Ensure that the original system is properly cleaned and secure
2: Restore the system to its proper state
3: Schedule the recovery process to happen during the weekend or night.
4: Restore the current information to the system from the backups
5: Replace temporary system with the original system
6: Recover proper business functionality to the IT-system
7: Properly clean all information from the temporary system.
Relocation actions is ended when:
- The IT-system is fully restored - Proper business function is restored at primary or secondary location

6.2 Business Relocation

Business Relocation
Business Continuity Plan
Prerequisites:
Continuing on next page

Business Relocation ...continued
Business Continuity Plan
a: More than one week of repair is needed and all systems is down. **b:** More than one week of repair is needed, but IT-systems is able to function
Actions during BCP:
1: Invoke the mutual temporary workplace agreement with Strawberry Inc.
2a: Invoke the BCP for replacement of IT-systems
2b: Secure the primary locations IT-system and run the essential systems on generators.
3: Establish essential business procedures at secondary location(IT, finance and management).
4: Correlate information and restore lost information.
5: Set up home-offices for all consultants, specialists and other which primarily is working at outside Blueberry ITs HQ.
6: Hold an AAR-meeting to review the actions taken during the incident.
7: Restore business procedures.
8: If it is impossible to relocate to primary location, begin searching for a new primary location
Business Continuity actions is ended when
- Business procedures is up and running at the temporary locations
Relocating back to primary site:
1: Plan and schedule the move during a weekend followed by a slow week.
2: Perform a complete backup of all IT-systems
3: Move the less important IT-systems during the evening of week days.
4: Move critical infrastructure during the weekend
5: Restore Infrastructure at primary location
6: Restore backups
7: Move all inventory to the primary location
8: If needed obtain missing assets
9: Move all personnel to primary location
10: Restore full business functionality at the primary location.
Relocation actions is ended when:
- Business functionality is fully restored at the previous or new primary location.

7 Appendix: A (Basic information)

Table 23, 24 and 25 are based on templates from the book Principles of incident response and disaster recovery[12] which was collected from Texas State library[13]

Emergency call sheet		
Service:	**Contact person:**	**Number:**
Ambulance	Hans Hansen	11 22 33 44
Electrician	Petter Pettersen	22 33 44 55
Plumber	Karl Karlsen	33 44 55 66

Table 23: An example over how an Emergency call sheet might look like, some sample emergencies are included.

Location of emergency equipment	
Emergency:	**Placement:**
Fire extinguisher	At help desk
Electricity	Basement

Table 24: An example of how to enumerate all emergency equipment, should be placed on map.

Equipment outside the company		
Item:	**Contact/company:**	**Number:**
Sprinkler system	Building janitor	99 88 77 66
Backup web server	Evry	88 77 66 55

Table 25: An example of how to enumerate all equipment not in company care, and how to reach a contact employee.

The numbers in table 26 are based on the following criteria. The rating is inspired by the book Principles of incident response and disaster recovery[14].

1: Salvage at all costs.

2: Salvage if time allows it.

3: Dispose of as part of general cleanup.

Salvage priority list		
Item:	**Location:**	**Priority:**
Backups	2. floor IT department	3

Salvage priority list *continued*		
Item:	**Location:**	**Priority:**
Personal computers	At personal desk	2
Database server	2. floor IT department server room	2
File server	2. floor IT department server room	2
Other servers	2. floor IT department	2
Non-storage equipment over 10.000NOK	2. floor	2
Non-storage equipment below 10.000NOK	2. floor	1

Table 26: List of all assets in priority human lives are not in the list, but always have top priority. This list shall be followed when several assets are at risk from one or several incidents at the same time.

8 Appendix: B (Inter-company Contact Info)

Company Call sheet				
Position:	**1. phone:**	**2. phone:**	**E-mail:**	**Address:**
Chief Executive Officer	555-1234	555-4321	ceo@blueberry.no	Strandgata 19, 2819 Gjøvik
Chief Marketing Officer	555-2345	555-5432	cmo@blueberry.no	Industrigata 1, 2819 Gjøvik
Chief Financial Officer	555-3456	555-6543	cfo@blueberry.no	Bedriftgata 20, 2819 Gjøvik
Chief Technical Officer	555-4567	555-7654	cto@blueberry.no	Gjøvikgata 5, 2819 Gjøvik
IT manager	555-5678	555-5678	itm@blueberry.no	itveien 1, 2819 Gjøvik
Network administrator	555-6789	555-9876	netadmin@blueberry.no	Nettverksgata 21, 2819 Gjøvik
System Administrator	555-1122	555-2211	sysadmin@blueberry.no	Systemveien 7, 2819 Gjøvik
Accounting manager	555-2233	555-3322	accountman@bluebery.no	Økonomiveien 9, 2819 Gjøvik
Senior Product manager	555-3344	555-4433	spm@blueberry.no	Produktveien 6, 2819 Gjøvik

Table 27: Call sheet for leader positions that are responsible for handling an incident.

9 Appendix: C (Evaluation of contingency plan)

Executive summary

The executive summary clearly sums up what we found out during the course of developing the business contingency plan. It briefly describe our process and whats left. It also depicts the importance of proper implementation. We've focused on keeping it short and concise so it would be easy to read and understand our findings.

It might be missing bit deeper insight to some of the issues we found, but by adding this would make far too long to be a functional summary.

Contingency planning policy

The policy encourages continuity training, and this covers the activities described in the report as well. The scope of continuity planning activities is set by the time intervals for revision in the policy. The different responsibilities, though not very precise, is stated in the policy along with whom is responsible for the development of the different plans.

The policy also states how the funding for business contingency planning is to be divided and used.

Quality of the writing

The quality is generally clear and concise, though there are some places where it could benefit from a better language structure. When the reader reads this entire report he/she might be able to distinguish the different authors of the report.

Since we've been using templates from the book it has a good quality of its structure which gives a good quality of the text.

Report structure

The report is logically structured and divided into chapters and sections, with the result that one can intuitively access the different areas of the report without reading the whole document. The structure of the report is built so it is easy to access the incident and disaster response plans during the annually revision. Though in an incident/disaster response scenario this report structure is not adequate, but could be solved by separating and placing the response plans in a separate folder.

In ”Appendix: A”, chapter 7, it is added collection of information documents which is meant to help during an incident. This appendix contains the salvage priority list, number register, and equipment location register for when it is needed to call plumbers, employees or find equipment around the premises. In ”Appendix: B” we have added the call list for all employees in case of an emergency.

We've purposely left out the ”Scenario Priority Document” due to it would possibly confuse employees during an incident. Instead we have added the top ten of scenarios in the BIA.

Comprehensiveness

Because we chose a fictional company to review it was important to create a comprehensive ”Business Description”. We used a lot of time getting the business description right since it would later on make it easier to analyze and develop the different attack scenarios. We’ve described Blueberry ITs assets, network topology and the physical layout of their office in the Business description, though we have mainly focused on their network topology and business functions.

The analysis in the ”Business Impact Analysis” and ”Business Unit Analysis” is comprehensive and describes all the threats and business functions related to Blueberry IT, though some of the threat descriptions might be vague. During the development of ”attack success scenarios” we decided to narrow our scope and took out three scenarios from the ”Incident Prioritization”-section to focus on. The scenarios we chose where ”unauth. installation of software”, ”flood” and ”phishing” attacks.

When we developed the incident and response plans we focused on the same scenarios as we did in the ”Potential Damage Assessment”. We struggled with finding the correct structure for this section, so after checking out existing plans we landed on our own structure which is divided into two parts; a short incident detection plan and an incident response plan. This way we could have a short plan which all employees can use and a plan which is meant for the incident response team. This is followed by our disaster response plan which handle the escalated incident or pure disaster incident.

The last part, part 6, contains the ”Business Continuity Plans” which describes how Blueberry is to perform a partial or full relocation of the business, and how they would recover from a partial or full loss of their IT-systems. This structure was developed by us by using a similar template as the IR/DR-plans.

The other reason why we only developed plans for three scenarios is because of the time limitations and the fact that Blueberry IT is a small company which doesn’t have the time or resources to properly train or respond to every incident, though they could be developed. Since this project had a time sensitive schedule it meant we had to hold a rather narrow scope on hour report.

Implementable

We’ve taken into consideration that Blueberry IT is a small company with only thirty employees and therefor focused on limiting the scenarios which they have train and focus their resources on. Because of their size we’ve in the policy stated that Blueberry IT is required to annually hold a security seminar. In this seminar all employees will participate in the learning of how to properly notify people during an incident and of the current risk in relation to Blueberry ITs business functions.

The policy also dictates the revision and training intervals for the different attack scenarios. We’ve here set the training exercises to occur on different intervals since some of them are more critical. In example: testing the ”Emergency Backup”-procedure is done each quarter since it is imperative that it functions properly and the testing does not affect the business procedures. On the other side, testing the ”Emergency Shutdown of IT-system”-procedure is performed annually due to its critical due to its severe effect on the business function.

In the we decided on setting a limit of ten for how many scenarios Blueberry IT is supposed to arrange training sessions on during the course of a year.

Team roles

The report clearly states who has the different responsibilities and roles within the company, but it does not clearly states who has the authority to make decision. Though its stated that during an incident that the task force leader has the authority during an incident/disaster.

Incident prioritization

Incident prioritization is based on which assets is at risk from the incident. Based on this will the incidents be prioritized by the salvage priority list, in table 26. This means that if two scenarios would at the same time and threaten the same assets it is up to the task force to make the judgement call on which to pursue.

Reporting procedures

As a part of the incident response plan we have developed another set of plans which we’ve called incident detection plans. They clearly state what the incident is and where/whom to report it to along with the instructions for what the recipient is to do. If the detected incident is regarded to be real it will trigger the incident response plan.

Formal aspects and references

We’ve been using LaTeX for this project in cooperation with the ”guc-master-thesis” style for hour project. Since we’ve been working across country lines during this project we used LaTeX in addition with the IT-departments project management system, their Subversion system. During our start up sessions we developed a group contract and set up our development environment. During our project we’ve had meetings twice a week over Skype on Mondays and Thursdays in the beginning and then later on on Mondays and Fridays, due to changes in our schedules. During our project we have continuously added references to the books, figures, tables and resources we’ve used in an orderly fashion in our report.

Bibliography

[1] Michael E. Whitman and Herbert J.Mattford. *Principles of Incident Response and Disaster Recovery*. Course Technology, 2007.

[2] Michael E. Whitman and Herbert J.Mattford. *Principles of Information Security*. Course Technology, 3rd international edition edition, 2009.

[3] NSM. Ros-2004. Technical report, NSM, April 2004.

[4] BSI. Iso-standard. Technical Report 27005, BSI, 2007.

[5] Michael E. Whitman and Herbert J.Mattford. *Principles of Incident Response and Disaster Recovery*, chapter 2, pages 60–61. Course Technology, 2007. Table 2-2.

[6] Michael E. Whitman and Herbert J.Mattford. *Principles of Incident Response and Disaster Recovery*, chapter 2, page 62. Course Technology, 2007. Table 2-3.

[7] Michael E. Whitman and Herbert J.Mattford. *Principles of Incident Response and Disaster Recovery*, chapter 2, page 63. Course Technology, 2007. Example of A Malicious Code Attack Scenario.

[8] Michael E. Whitman and Herbert J.Mattford. *Principles of Incident Response and Disaster Recovery*, chapter 2, pages 67–68. Course Technology, 2007. Malicious Code Attack Scenario Addendum.

[9] Michael E. Whitman and Herbert J.Mattford. *Principles of Incident Response and Disaster Recovery*, chapter 2, page 69. Course Technology, 2007. Subordinate Plan Classification Addendum to End Case.

[10] Michael E. Whitman and Herbert J.Mattford. *Principles of Incident Response and Disaster Recovery*, chapter 3, page 111. Course Technology, 2007. Incident Response Plan Addendums to Attack Success End Case.

[11] Michael E. Whitman and Herbert J.Mattford. *Principles of Incident Response and Disaster Recovery*, chapter 7, page 278. Course Technology, 2007. Figure 7-1: Disaster Respnse plan addendums to disaster scenario end case.

[12] Michael E. Whitman and Herbert J.Mattford. *Principles of Incident Response and Disaster Recovery*, chapter 9, pages 289–290. Course Technology, 2007.

[13] Texas state library and archives. Example disaster recovery plan. Resource not found.

[14] Michael E. Whitman and Herbert J.Mattford. *Principles of Incident Response and Disaster Recovery*, chapter 9, page 293. Course Technology, 2007.