Benjamin Cox and Micah Leslie

Assignment 3, CSC 321

Kanthi Narukonda

3/4/2024

“We certify that this assignment is our own work.”



CB Solutions

# Introduction

“Just as oil powered the industrial revolution, data is powering the digital revolution, “(Jooste 24). Our company name is CB (Cloud Based) Solutions, and we are an IT company situated in Boise, Idaho with other locations in Idaho and Montana. We currently employ over 1200 employees across all our branches. We offer general IT solutions for small-midrange companies with a strong commitment to data security and integrity. The following policy will be an issue specific security policy focused on the company’s response in the event of a suspected data breach. This aligns with the company’s goals of providing secure data storage to its customers and will help safeguard the company from legal trouble if breaches occur.

# Organizational Chart

(Inspired by Whitman and Mattord 2016)

A diagram of a company

Description automatically generated

# Role Descriptions:

**CEO:** Manages all operations of a company.

**CFO:** Manages all aspects of finance and resources within a company.

**COO:** Manages all daily operations within a company

**Sales Manager:** Manages the sales staff in charge of partnering with new businesses.

**Human Resources Manager:** Manages employees to create a good work environment to have good employee retention.

**Legal Department Manager:** Controls and advises departments about certain legal requirements for certain data and audit information.

**Legal Team:** Our legal team focuses on making sure we follow all rules and legal regulations with data storage, access, and protection.

**Accounting Manager**: Manages business finance to ensure profitability and stability.

**The Accounting Department** includes roles such as Payroll, Risk and Insurance, and general finances.

**Research and Design Manager:** Pushes us forward by employing research to improve our operations and push the boundary in security and efficiency.

**Security Team Manager:** Manages our physical security team for our employees and our data servers.

**Business Services Manager:** Manages the customer facing part of our business with business IT help and maintenance.

**Business Support helpdesk**: Offers 24/7 business support for products and calls the technicians based off their needs.

**Printing Technician:** Travels to businesses to fix and set-up printers.

**Server Technician:** Travels to businesses on-site to do server maintenance and fix problems when they arise.

**Hardware Technician:** Set employees up with Virtual Desktops with thin clients and updates/fixes hardware when needed.

**Information Security Manager:** Manages the back end of our business with protecting data and our systems from attack.

**Database Administrator:** make sure only the correct employees have access to certain databases and the database runs efficiently. Also creates new databases as needed for a company.

**Network Administrator:** Makes sure all aspects of our network are running and alerting businesses of any outages.

**Emergency Response Team:** Specific team members in multiple departments with training in what to do in response to cyber-attacks and leaks as mentioned in our Policy Statements

**Cyber Offence Team:** Checks our system for vulnerabilities constantly by trying to find innovative ways to infiltrate our system.

**Cyber Defense Team:** In conjunction with the cyber offence team, protects our systems from any vulnerabilities they find and tries to predict and stop future attacks.

**Cyber Security Engineer:** Part of the Cyber Defense team dedicated to building firewalls and systems to stop users trying to gain access.

**IT security auditor:** A sub-department of our legal and tech team to review changes and audit our information.

# Data Breach Response Policy

**1. Purpose**

This policy establishes the goals that are to be met during the breach response process. This policy defines who it applies to and when and includes the definition of breaches, staff roles, responsibilities, standards, reporting, remediation, and feedback mechanisms. This policy must be publicized and made accessible to all employees related to data services and those whose work involves data privacy and security.

CB Solutions’ InfoSec’s intentions for this policy are to give focus on data security, specifically on how breaches are to be handled and how CB Solutions is focused on trust and integrity for its clients. InfoSec at CB Solutions is committed to protecting CB Solutions employees, sponsors, and the company from any damaging actions by knowing or unknowing individuals, (SANS 2024).

**1.1 Background**

The Data Breach Response Policy mandates that anyone suspecting that a theft, breach, or exposure of CB Solutions data has occurred is required to immediately provide a description of the suspected breach over email to Helpdesk@CBSolutions.org through the helpdesk reporting page on the company website. The email address, and website, are monitored by the Information Security Administration Team at CB Solutions. In the event of a suspected event the team will further investigate to confirm that the theft, breach, or exposure has occurred. If one of the events has occurred, the InfoSec Administration team will then follow the appropriate procedures set forth in this policy, (SANS 2024).

**2.0 Scope**

The policy is intended to apply to anyone who collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or handle protected information used at CB Solutions or information of its members. Any agreements with supporting suppliers will also contain language that protects the organization, (SANS 2024).

**3.0 Policy Confirmed theft, breach, or exposure of CB Solutions data**

In the event a breach, theft, or exposure is confirmed a team will be made including members from:

* The IT Department
* Finance (if applicable)
* Legal
* Administrations
* Human Resources
* The department where the breach occurred or the department that works with the involved data
* Additional departments based on the current COO/CFO’s discretion.

The CEO shall be notified of the event, along with the designated team, who will analyze the breach or exposure in attempting to determine the root cause. When an event occurs, all access to data related to the breach will be restricted to only this team until the event is resolved, (SANS 2024).

**3.1 External forensics and Communication plan**

Depending on the extent of the theft, breach, or exposure the team described above may determine the need for an external forensics team and plan appropriately. In either case of needing an external team or not, the team should work with CB Solutions communications, legal, and HR departments to decide on how to communicate the breach to; a) internal employees, b) the public, and c) those affected by the breach, (SANS 2024).

**3.2 Ownership and Responsibilities**

* Sponsors – Sponsors are members of CB Solutions’ community whose responsibility is to maintain any information resource. Sponsors may be selected by any Executive at CB Solutions within their administrative responsibilities.
* Users include all members of CB Solutions, ‘external users’ implies customers who use CB Solutions.
* The response team shall be chaired by executives of the following departments: IT, Communications, Legal, Management, Financial, HR, and InfoSec

**4.0 Enforcement**

Any CB Solutions employees that violate this policy may be subjected to disciplinary action, up to and including termination. Any third-party partner companies found in violation will have their connections to CB Solutions terminated, (SANS 2024).

**5.0 Definitions**

Third Party Company: An outside company providing services to CB Solutions

**6.0 Revision History**

Current Version: 1.0, Date of Release: 3/4/2024, Description: Initial Version  
Next Planned Review: 6/4/2024.

# Conclusion

During the planning and creation of this data breach policy, we further learned how companies are structured, including more specific definitions of the many roles in an IT company. We found out that we wanted to do a data breach issue specific policy since it fit how our company was based on providing cloud storage and IT services. During research for an example policy, we found the general response to a suspected data breach is to first contain it, investigate its origins, and then decide if it qualifies as a breach before responding, (NYU 2016).

References

**(NYU 2016)**

NYU Web Communications. (2016). *IT Security Information Breach Notification Policy and Plan*. Nyu.edu. https://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/it-security-info-breach-notification.html

**‌(SANS 2024)**

*Information Security Policy Templates | SANS Institute*. (2024). Sans.org. <https://www.sans.org/information-security-policy/?page=2>

**(Whitman and Mattord, 2016)**

Michael E. Whitman; Herbert J. Mattord, (2016), Management of Information Security (PG 234 Figure 5-5). *Cengage Learning*

\*Used for general outline of info for organizational chart.

**(Indeed 2024)**

*Flexible Information Technology Jobs | Indeed.com*. (2024). Indeed.com. https://www.indeed.com/jobs?q=information+technology&l=&vjk=3c0612ec3c7e6f22

‌\*Used for some of the job position titles and general research into IT jobs and what other businesses hire\*

**(Jooste 2024)**

*LinkedIn*. (2024). Linkedin.com. https://www.linkedin.com/pulse/unlocking-power-data-understanding-why-oil-21st-century-jooste/

‌

‌