Case Study Set 1

**VIKRAMADITYA REDDY VARKALA**

**Z1973679**

**Case Study 1: Kraft and protecting personal data**

**Q2) How does Craft comply with EU data privacy regulations governing the protection of employee data?**

The EU directive requires **“appropriate technical and organizational controls”** to be in place to protect the confidentiality and integrity of personal data.

Kraft began to move towards these **standardized system platforms and architectures** as a means of improving data security. By 2003, all international HR systems at Kraft were converted to the SAP HR system

**Q3)The EU directive requires "appropriate technical and organizational controls" to be in place to protect the confidentiality and integrity of personal data. How can an organization determine whether its security controls are appropriate?**

* Information **security policies** were developed, including those pertaining to compliance with the Sarbanes-Oxley Act of 2002, business continuity and **disaster recovery planning, and backup and recovery processes.**
* Institute Risk mitigation initiatives, including threat and vulnerability analyses.
* Citicus ONE **risk management software** is used regularly to conduct risk assessments of individual systems, identify risk factors between systems, record risk remediation activities, monitor the risk status of critical applications, and ensure compliance with existing codes of practice
* Implementing stronger data security policies through out the organization.

**Q4)What user access controls are in place for the UPPS and SAP HR systems?**

Access to, and use of, the UPPS and SAP HR systems are restricted to those portions of the systems that are directly related to the employee's job responsibilities.

An Access Request Form must be completed by each individual requesting access to UPPS or SAP HR. The form requires the employee's name, identification number, title, function, and organizational dimension.

* The form must be signed by the employee, the employee's manager, the HR manager, and the Security Administrator at Kraft Foods Inc.
* If the employee requests access to data outside of his or her organizational dimension, a Security Access Exception Form also must be completed, in which the business reason for the additional access must be explained. This form must be signed by the employee, the employee's manager, the HR manager, the requisite Vice Presidents of all affected organizational dimensions, and the Security Administrator.

**Q5)How does Kraft implement the following access controls: need to know; least privilege; mandatory access control; and role-based access control?**

* Each user who has rights to employee data must sign a Human Resources Data privacy form in which user agrees to comply with Kraft’s Data privacy principles along with the respective authorities depending on the level of access required.
* HR data must be accessed only by **authorized users** who need to know the data to perform their jobs.
* Users are granted the **least** privilege necessary to perform authorized tasks.
* All access to HR **is restricted** to the fewest number of data fields possible, for the shortest time necessary, to carry out the job responsibilities.

**Q6)Identify at least ten examples of specific HR data that are considred sensitive at Kraft Foods Inc.**

Specific HR data that are considered sensitive are

* Social Security number
* Home address
* Home telephone number
* Age/birth date
* Salary grade/pay information
* Job performance ratings
* Race/ethnic origin
* Religion
* Gender/sexual orientation
* Criminal record or charges
* Benefit choices
* Photographic images
* Political opinions
* Trade union membership

**Q8)Why is Kraft moving away from the use of employee social security numbers for user identification on UPPS?**

On the SAP HR system, the employee ID is randomly generated where as on UPPS the employee ID is employee security number.

To protect the **employee rights to privacy** and to improve consistency between UPPS and SAP HR systems Kraft is in the process if changing its employee ID from social security number to randomly generated numbers .

**Q9)Through the UPPS, Kraft provides its employees online access to their own employee data. Why would Kraft do this?**

Through the UPPS, Kraft provides its employees web-based self-service was offered to salaried employees, including the ability to

* view their paychecks,
* confirm their personal information,
* access their credit union accounts,
* make travel arrangements,
* file expense reports.

**Case Study 2:Advo and physical security**

**Q1)Traditionally, managing IT security and physical security has treated as two separate domains. Why should they be integrated?**

The security management system integrates the company's security applications, including employee identification badges, visitor controls, parking permits, security tour controls, alarm systems, security cam- eras, and support measures for incident investigations. It also allows the

SCC to exercise centralized control of these applications at all locations.

* Employee identification badges are created in the SCC.
* Each badge includes an employee photograph.
* The badges are programmed for access control purposes and the data are stored in the security management system database
* Badge access is required to enter any facility, and to enter specific areas within a facility and SCC can observe all entries ,Reject access and modify access privileges.

They should be integrated because of following reasons:

* Organizations can eliminate redundancy and improve efficiency.
* IT security detect cyberattacks or any malware attacks where as physical security detect physical attacks. By integrating these a company will have an understanding of potential security threats.
* Allows comprehensive risk management approach.
* An integrated security system can lock down IT system and alert security during investigating an incident.

**﻿﻿﻿Q2)Why is top management's awareness and support essential for establishing and maintaining security?**

Top Management awareness and support essential for establishing and maintaining security because of the following reasons:

* They are responsible for the organization's strategic direction, policies, and procedures.
* They are responsible to hire consultants to address issues such as improving the data center at corporate headquarters, implementing stronger software countermeasures, physically protecting its computer systems, establishing tighter access controls for enterprise applications, monitoring network usage, and developing the company's disaster recovery plan.
* They determine employee access rights to all data and applications.
* Responsible for ensuring that all physical security measures were implemented and enforced at the corporate head quarters and all facilities.
* Responsible for conducting security audits

**Q3)﻿﻿﻿Why should those responsible for leading the organization’s security efforts be placed high in the organizational chart?**

Security is the top priority for the organization. Those responsible for leading the organization’s security efforts be placed high in the organizational chart because

* They ensure accountability, communication and accountability within the organization.
* They ensure that security considerations are taken into account when making important decisions that affect the organizations overall strategic direction.
* Placing them high in the organizational chart ensures they have authority to allocate resources to implement security measures effectively.
* Placing them high ensures that security issues are addressed at the highest levels of the organization.
* They ensure that all physical security measures were implemented and enforced at the corporate head quarters and all facilities.

**Q4)The first decision made by Advo's top management in the after math of the 9/11 attacks was to improve physical security. Why was attention focused on this particular aspect of security?**

The terrorist attacks elevated the importance of security within Advo. There was an abrupt and dramatic change in executive attitudes and physical security was given top priority. Advo's CEO ,in consultation with the Senior Vice President of Fulfillment, mandated that a real security presence be established at al locations. The Wackenhut Corporation was immediately hired to provide uniformed security officers on a 24-7 basis at Advo's corporate headquarters and at all mail processing facilities.

Less than two weeks after the 9/11 attacks, the first bioterrorism-related anthrax attack occurred.Public fears grew as media reports of anthrax-laced mail increased.Two postal workers had died from anthrax exposure which led to public to wide spread panic. The impact of the anthrax attacks was dramatic. To the general public, nothing seemed to be safe anymore, not even the mail.

The results of environmental anthrax testing caused USPS to temporarily close several postal facilities. For a company like Advo, whose business relies on the USPS and whose clients rely on people opening their mail, the anthrax attacks posed a significant threat to its existence.

**Q5)**

**a.What are the advantages and disadvantages of using consultants and third-party organizations to provide security-related services?**

The Director of IT Security and Enterprise Architecture was allowed to hire consultants when needed to address Advo's most critical IT concerns.

These concerns included improving the data center at corporate headquarters, implementing stronger software countermeasures, physically protecting its computer systems, establishing tighter access controls for enterprise applications, monitoring network usage, and developing the company's disaster recovery plan.

Advantages:

* Specialized expertise and knowledge in security related matters
* Cost effective
* Flexibility to adjust security measures based on changing business needs

Disadvantages:

* Lack of control over security measures implemented.
* Risk of data breaches.

**b.What reasons would a company have for hiring consultants to provide guidance for its security efforts?**

Because there was little in-house expertise to provide necessary guidance, consultants were hired. Kroll, Inc., was hired to do a risk analysis of the company's physical security, and Ernst &Young was hired to do a risk analysis of IT security. Their recommendations included the hiring of additional employees in IT and physical security.

**Q6) Why is it a good security practice to have few visitors in a reception area?**

Visitor controls are imposed through an extended application of the security management system.

* Employees can pre-register their visitors through the company's intranet, which reduces the number of unexpected visitors.
* Visitor badges can be printed in advance, resulting in shorter visitor waiting times and fewer visitors in the reception area.

**Q7) Identify the security risks involved in allowing networked systems to be used by large numbers of temporary employees who do not need to log in. What password guidelines should be implemented for stronger user authentication?**

User authentication is established by means of password entry during login.

User passwords must be :

* At least five characters long
* They must be changed at least once every ninety days.

There also are kiosk PCs located on the shop floor of every facility. The kiosk PCs are connected to the company's intranet and can be used to access the Internet. Currently ,no login is required for these systems, which can be used by more than **125 temporary employees** who work on the shop floor of each mail processing facility.

Security risks:

* Data Leakage
* Malware attacks
* Unauthorized access-difficult to track who has accessed the system and what actions were taken.
* Social Engineering attacks-Phishing ,pretexting

**Q8) How far away should a backup site be located from company head-quarters? What factors should be considered in determining the location of a backup site?**

Both the data center and the SSC have an on-site uninterruptible power supply provided by a diesel generator with a 250-gallon diesel tank. A backup site for the data center and the SCC was completed in September 2005. Located about four miles away from corporate headquarters in Windsor, Connecticut, the site provides complete system redundancy; it operates on its own power grid with separate backup power.

Backup site should be located far enough away from the primary site to avoid being affected by the same disaster but not so far away that it becomes difficult to access or transfer data

Factors in determining the location of a backup site:

* Risk assessment:Site should be far from disaster prone areas
* Connectivity for data transfer without delay
* Accessibility to company staff to reach the site
* Legal and regulatory requirements
* Cost of setting up and maintaining back up site.

**Q9) Advo believes that frequent audits help to ingrain a security mindset among the company's employees. What other benefits are there to performing frequent security audits?**

Advos’ security managers conducted a security audit at corporate headquarters in Windsor, Connecticut, and at each of the twenty-one mail processing facilities. The audit was designed to evaluate the controls implemented through the integrated security management system.

The audit covered twenty-one key areas: access controls, bomb threats, cleaning of equipment, dark hours,18 emergency action plan, fencing, identification badges, key control, laptop security, lighting, locking devices, mailroom, parking control, pre-employment screening, record access and retention, security cameras, security incident reporting, security officers and technicians, tour management system, utility security, and workplace violence

Advo now conducts **security audits semiannually.** The audit areas and specific audit points are reviewed each year and revised when needed to reflect the industry's best practices.

The company believes that frequent audits:

* reinforce the importance of security
* help to ingrain a security mindset throughout the organization.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*