Legal issues

Technology, Internet

Security Awareness and Training Program (for Nancy Johnson and other similarly situated employees)

Nancy Johnson and other employees were terminated from their jobs by the administrator of the company, US Bancorp Comprehensive Welfare Benefit Plan Committee. The “ Cause” of Johnson’s termination of employment is “ willful and gross misconduct”; when Johnson accessed the files of her supervisor containing the 2002 performance level of the company’s employees.

When Johnson was denied the severance payment (she was able to access a file that contains the proposed merging of US Bancorp with another company – some employees would be terminated with severance payment, except those who were involved in gross misconduct), she requested for a summary judgment to the district court. The district court favored Johnson arguing that the company did not establish a security information system that would prevent employees from accessing the files of the company. The committee though wrote an appeal to the circuit court arguing that the court erred in its interpretation of the provisions of the plan. The circuit court agreed to the arguments of the committee, arguing that since no official interpretation as to the use of the terms “ willful and gross misconduct”, the administrator of the plan can apply these terms to similar situations. The severance payment to Johnson was therefore denied.

Information security awareness and training programs then should be designed based on the so-called Computer Fraud and Abuse Act of1984. The statute “ criminalizes unauthorized access to a ‘ protected computer’ with

the intent to obtain information, defraud, obtain anything of value or cause damage to a computer” (Security Awareness Laws, http://www. massachusetts. edu/lawsfaq/faq. cfm#7). The so-called ‘ protected computer’ is a computer used for foreign orcommunicationpurposes (as in the case of the plaintiff) and for interstate interaction. Without authorization from the Department of Defense or the Foreign Affairs, accessing information from said institutions is deemed illegal.

Also read: Explain Legal Issues, Policies and Procedures Relevant to Assessment

Sharing of passwords, computer fraud, and damage of essential federal information are also deemed illegal. The law was extended to include private computers. In the case of the defendant (the corporation), it must institute narrower definitions as to the terms “ willful and gross misconduct.” This will definitely also narrow the options for employees who are accessing important information from the company’s database. The employees must be first acquainted (by memorandum) of the sites allowed to use during office work.

Security Awareness and Training Program (for Scott Moulton)

The plaintiff, Scott Moulton accused the defendant of probing the former’s network of clients. Defendant claims statements from Moulton concerning the defendant were defamatory. First is the statement made by Moulton to C. J. Johns, information systems manager for the Cherokee County’s Sheriff’s Office (December 19, 1999) that defendant had created security risks and

that defendants network employees were stupid. The second is the statements made by Moulton that the way defendant planned to connect the Police Department to two systems created a security risk from the internet. Lastly, statements from the plaintiff said that defendant’s network had created a security risk.

The plaintiff though argued that these statements were merely opinions. People may agree or disagree with the statements made. The court though granted the defendant summary judgment for thefailureof the plaintiff to run a put test in the project. The plaintiff was also granted a summary judgment for the failure of the defendant to reduce the security risks.

The US Congress passed a bill on July 2004, stating that internet probing of contractors to government websites (contractors duly approved to negotiate for the construction of website connections between government offices) can only be legal on three counts: 1) probing does not in any way create security risks for the government office involved, 2) the probing would not result to malversation of any public information, and 3) such probing must be requested by the client government office, with approval from its head office. Though the case was a posteriori since the bill was passed before the case was filed, it would be good for government offices to follow the guidelines of the law on internet probing of intergovernmental offices. Hence, law analysts saw the law as the “ most Balearic” safeguard of the government from hackers.

Security Awareness and Training Program (for Dewey Watkins)

The plaintiff, Dewey Watkins requested the district court to cancel a computer access code that had been assigned to him and was being used (with the supervisor's approval) by another authorized employee. The code provided access to confidential records maintained for Tennessee's Medicaid Program. The plaintiff argued that the action of the supervisor violated the confidentiality provision of the state law. The plaintiff also accused EDS of terminating his employment when the former refused to participate in the " illegal" conduct. The circuit court however affirmed the decision of the district court to grant summary judgment in favor of EDS, for the reason that Tennessee law does not conflict with the general provision of the Confidentiality Law.

There was no proof that other employees also use the computer access code, and if there was such a case, it would be legal. It is noteworthy that the same law discussed in case 1 also applies in this case. Sharing of passwords to access public documents is clearly prohibited by law. Nonetheless, although the terms " public information" was the focus of the case, it should be noted that public information are information that have direct link to the public in general. This constitutes government programs, strategic social and economic planning, and of course interstate activities. Security awareness programs must be based on the definition of public information in order to vindicate any instances of sharing passwords or revealing information from government-locked and secured database.

References

Nancy J. Johnson v. US Bancorp … United States Court of Appeals for the Eight Circuit. Appeal from the United States District Court of the District of Minnesota. September 9, 2005.

Security Awareness Laws. 2006. University of Massachusetts. Retrieved September 14, 2007.

Scott Allen Moulton and Network Installation Computer Services, Inc., Plaintiffs v. VC3, Defendant. United States District Court, Atlanta Division.

Watkins v. EDS. NO. 1: 00-CV-434-TWT. United States Court of Appeals No. 03-6353. United states Court of Appeals for the Sixth Circuit. November 2, 2004.