**CSG 3309 IT Security Management**

**Part-1: Essay on the ethics of trading privacy for security**

**Privacy vs. monitoring of an organization’s staff**

Contents

[**Executive summary** 3](#_Toc32092408)

[**Introduction** 3](#_Toc32092409)

[**Reasons** 3](#_Toc32092410)

[Insider threats 3](#_Toc32092411)

[Example of insider threat 4](#_Toc32092412)

[Easy target 4](#_Toc32092413)

[In terms of productivity 4](#_Toc32092414)

[**References** 6](#_Toc32092415)

# **Executive summary**

For this scenario, I support **organizations should** monitor their employee’s email, web usage, and online activities if the security of an organization can be improved. In this, I started with an introduction then continued to reason then progressed to advantages and ends with a conclusion.

# **Introduction**

Employee monitoring is generally surveying employee activities with the help of a software or using any other mediums. There is always a clash between monitoring vs privacy at the workplace. Some support it and some do not. But when considering organizations in this cyber/digital era it’s better to support it because without proper monitoring we cannot proceed further our business. What if an employee turns around his/her employer and decided to misuse his privileges then definitely it will cause a severe impact on the organization? And what if the same employee decided to leak your organization’s critical information resources? Or what if the threat comes within the organization which usually won’t be in risk analysis/mitigation strategies.

# **Reasons**

There are several reasons why an organization should monitor its employee’s activities such as their emails, web usage. The primary reason is to protect the organization against legal problems. When we look at the current digital workplaces majority of the organizations equipped with the required resources to connect with the internet and their employees have access to them. So, in this case, if an employee uses the provided resources for illegal activities such as online bullying then the organization will get affect and face legal, and as well as reputation damages.

## Insider threats

Insider threat is basically the threat that raises from within the organization. The successful insider threat attacks are due to non-adequate monitoring. According to Verizon’s 2019 Annual threat report (Verizon, 2019) , 34% of all the security breaches occurred in 2018 are due to insider threats and the percentage is 6% higher than 2017 and 9% higher than 2016.

According to Accenture & Ponemon’s research (Accenture/Ponemon Institute, 2019) on the cost of cybercrime research 2019 reveals that the average cost of an insider threat is 1,621,075 USD in 2019 which is 15% higher than compared with 2018.

## Example of insider threat

One of the examples for this insider threat is Anthem Medicare Insurance which took place in 2017. According to reports (espellman, 2017) , it’s been found that one of the employees emailed a file that consists the personal information of 18500 anthem members such as their Medicare ID numbers, including Social Security numbers, Health Plan ID numbers, names and dates of enrolment. This breach resulted in Anthem to pay 115 Million USD to settle the lawsuit. This entire thing happened due to an employee which teaches the importance of employee monitoring.

Another incident that happened in 2003 is Bae Systems vs CAAT. In which Bae system used a private detective to spy on CAAT and Where the key players got into CAAT by posing as employees and passed all the information to Bae systems (High Court of Justice Queen's bench division, 2007).

## Easy target

Presently when we look at most of the cybercrimes, they are not targeting an organization’s executive/board members rather they’re targeting low-level employees. Recently in the USA (Lindsey, 2020), it has been found that hackers are targeting the potential employees to spread malware on the organization’s system. Usually, most of the organizations send their employees to proper cybersecurity awareness training but still, employees fail in this at some point especially in business email compromise and/or phishing scams. Sometimes, the failures lead to ransomware attacks also.

## In terms of productivity

Apart from the above-stated reasons productivity also involves the need for employee monitoring. A survey conducted in 2012 (Salary.com staff, 2012) particularly highlighted that 64% of employees use non-work related sites (especially Facebook, Twitter, etc..) on a regular basis. Every hour they spent on this directly impacts the financial, and resource consumptions (Budget on IT services like equipment, internet).

**Advantages**

* As stated, before the primary advantage would be the organization would be safe. Apart from that we can spot the mistakes and can resolve the issues in an easy manner.
* This also helps to identify the effective employee in the organization.
* Also, this helps the organization to save a solid portion of the fund on their infrastructure resources.

**Conclusion**

Finally, to conclude this, for these reasons I support employee monitoring. Also, from an employee perspective, I must say that these are valid points. Apart from this, each county has its own laws that justify the monitoring. For example in Australia, Workplace Surveillance Act 2005 No 47 (Workplace Surveillance, 2017) justifies employee monitoring under the certain term and conditions which are fair.

# **References**

Accenture/Ponemon Institute. (2019). Accenture/Ponemon Institute: The Cost of Cybercrime. *Network Security*, *2019*. doi: 10.1016/s1353-4858(19)30032-7

espellman. (2017). Anthem suffers data breach…again - IT Governance USA Blog. Retrieved 8 February 2020, from https://www.itgovernanceusa.com/blog/anthem-suffers-data-breachagain

High Court of Justice Queen's bench division. (2007). Retrieved from https://www.5rb.com/wp-content/uploads/2013/10/CAAT-v-BAE-QBD-26-Feb-2007.pdf

Lindsey, O. (2020). Iranian Hackers Target U.S. Gov. Vendor With Malware. Retrieved from <https://threatpost.com/iran-hackers-us-gov-malware/152452/>

NSW Parliamentary Counsel’s Office. Workplace Surveillance (2017). [www.legislation.nsw.gov.au](http://www.legislation.nsw.gov.au).

Salary.com staff. (2012). Wasting Time at Work 2012 | Salary.com. Retrieved from <https://www.salary.com/chronicles/wasting-time-at-work-2012/>

Verizon. (2019). Verizon: 2019 Data Breach Investigations Report. *Computer Fraud & Security*, *2019*(6). doi: 10.1016/s1361-3723(19)30060-0