

WORKPLACE PRIVACY & ETHI

MODULE 4

Work place monitoring

- Keeping an eye on employees
- Monitoring will be done on quantity and quality of work produced by their employees
- Employees have some degree of privacy in workplace.
- Excessive, routine and unnecessary monitoring is a breach of data protection laws

Need of workplace monitoring

- Employee or customer safety
- Liability & investigations- harassments, the
- Network and system perf.: protection a virus, avoiding network slowdown etc
- Right to know for employers: legitimate pro
- To check the procedure are following
- To prevent or detect crime
- In the interest of national interest

Types of work place monitoring

- Hardware monitoring
- Software monitoring

Hardware monitoring

- Audio surveillance
- Video surveillance
- Infrared badges at work
- Mega stripe cards

Software monitoring

- Electronic surveillance
- Spyware
- Screen, data, idle time monitoring

Advantages

- Reduce mistake
- Employee safety
- Unbiased performance evaluation
- Violation of policies prevented

Disadvantages

- Prevents efficiency-being too intrusive
- Expensive instrument
- Devious employees
- Too much monitoring lead to high infidelity competition rather than team competition
- Too much monitoring lead discomfort of employee

Computer crime

- Type of fraud where computers are used
- It is a an act performed by a knowledgeable user.
 - Ex: unlawful use or access- hacking(with permission)
 - access for fraud
 - Data theft- use/ copy/damage/ alter info permission

Computer crime at workplace

- Computer crime is increasing in workplace
- Use of authorisation to get a sensitive data and change it or sell it to make more money
- Most fraud are not committed employees
-

Types of computer crimes at workplace

- Software theft - theft-unlicensed copying
- Hardware theft - microprocessors, laptop hard disk drives etc
- Hardware theft is most common fraud

Preventing computer crimes a workplace

- Tactic such as encryption, firewalls, employee training and awareness, routine audit, physical surveillance, appointing security personnel
- Reward system for employees for reporting employee initiated audit, updating computer virus program, ISO agreements etc

Workplace plagiarism

- Act of fraud
- Involves both stealing someone's work and lying about it afterward

Types of workplace plagiarism

- Using others' images & work
- Taking credit for an idea
- Failing to list a source
- Stealing blog content
- Reproducing an e-book

Effect of workplace plagiarism

- Personal integrity
- Legal consequences
- Company reputation
- Fairness to colleagues

Employee privacy and ethics (i

- Freedom for employee from unauthorised intrusion from employers
- Describes the context to which employers monitor and collect information on the activities, communication, and private lives of workers.

- A controversial and legal issue
- Employers are allowed
- Other pvt spaces- lockers/ drawers- e/rs should not violate worker's privacy
- Tough task-to decide how much monitor necessary?

No privacy but convenience

A debate...

- Would you like to have complete privacy workplace but accept the risk of potential abuse/ other problems??
- Are you ready to give away ur privacy for benefit of avoiding any problems?

Death of privacy

- Digital footprints- to track what employees do: delivery records, travel logs, expense reports, productivity reporting etc
- Electronic toll collection tags- to record passing time in vehicle without stopping the vehicle
- Cell phones- monthly bill can be reviewed
- Even location from where the calls were received could be traced- transmission towers
- GPS- should not track employee's location after work hours-unfair to do so. (global positioning system)

Use all the above with legitimate business reasons



HOW GPS WORKS



Defence of employee privacy ri

- employers not to intrude employees per life, choices, background, habits etc.
- Without considering the employees inte not to be disclose/discussed in public
- Ex.: pvt msgs in inbox, checking purses/w in public
- When employee not trusted he/she wou longer see any incentive in being produc /efficient

- Increased surveillance leaves no room for employee self control and self monitoring
- With data security and other organisational interests becoming paramount, the employee's rights for privacy and freedom is curtailed

Breaching employee privacy

- During recruitment process - confidential info like family background etc- if relevant but to be kept confidential in co records
- During performance tracking - to check work habits, client management to find causes for poor performance etc
- During electronic surveillance - necessary to keep check on the work space activities
- Electronically stored e/e data- getting access to people- personal and professional data must be confidential.

Guidelines to defend employee pr

- Let there be a clear policy- taking consent and making aware of what is pvt and what is not
- Only on legal grounds-no other utility of the monitoring tools
- Do not have unnecessary harsh policies- result in attrition
- No electronic harassment – offensive emails/direct messages take enough care
- Use of internet only for business
- Use of all electronic tools for business or professional purpose
- In-house privacy controller- for large orgtns can be a rep for data protection and use of techno in the org



"Johnson, I think you misunderstood our Casual Fridays dress code."

The elements of Invasion of Privacy

