White Paper

Sold Down the River by Moonlight

Protecting Your Business with Productivity Monitoring Software

02070936000
talk@htl.uk.com
www.htl.london

Introduction

Reduced Productivity and Insider Threats

Every boss or line manager is likely to have come across 'private jobs' which employees may try to weave into their working day. A kid's birthday party invite being designed on screen... Or a bit of watercooler gossip about the discovery of the latest chapter of so-and-so's novel on the printer... Someone on their mobile overheard discussing a project that's not going through the books - at least of your company, anyway.

Employees may get up to a variety of things in the workplace on company time that are not related to the firm's business. Some might be low-level, lunch hour 'personal projects', a certain amount of which, in more relaxed and unregulated businesses, may be treated with a blind eye. However, even if it is tolerated, the question remains - how much do these activities distract employees and divert resources away from the core business?

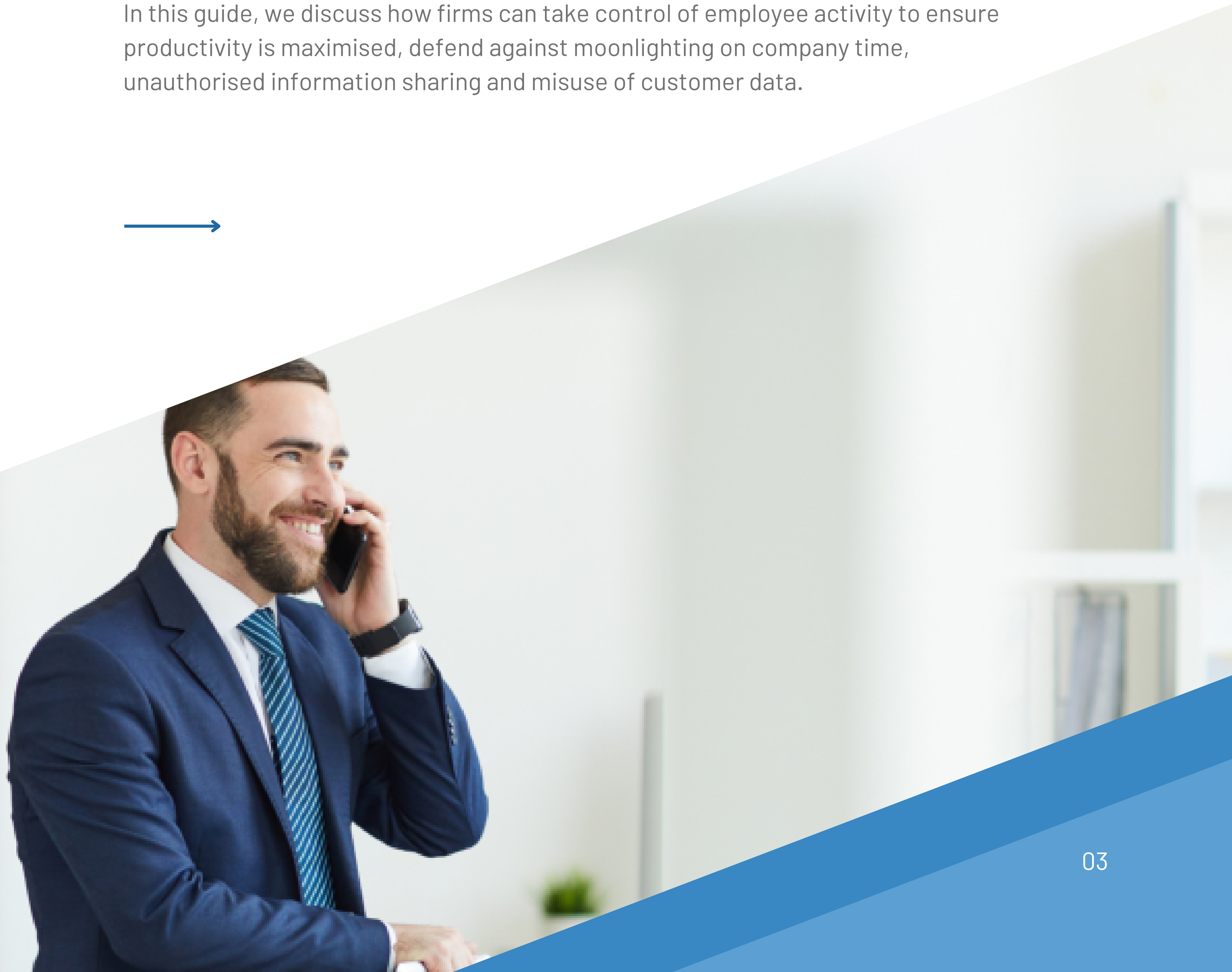
Moonlighters working on their own projects is one thing. Being 'sold down the river' by a disgruntled employee who decides that their grievance is best redressed by selling on your database to a competitor, is quite another.

The insider threats like this that are most likely to pose a risk to your business depend on the core activities of the firm. If it creates and owns IP, then employees could copy valuable data onto USB sticks and walk off with it. If it holds personally identifiable information (PII), then employees might be tempted to misuse the data fraudulently.

Generally, such activities may be collectively termed breaches of IT security. Whether such actions form part of a premeditated plan, or are a spur of the moment impulse that the employee instantly regrets, it only takes moments to attach a database file or a confidential commercial document to an email and send it.

In centralised office environments, moonlighting and insider threat activity may be relatively easy for management to pick up on. However, for home-based and remote workers, where people are out of close supervisory reach, it is harder to directly detect with just the eyes and ears.

In this guide, we discuss how firms can take control of employee activity to ensure productivity is maximised, defend against moonlighting on company time, unauthorised information sharing and misuse of customer data.



Employee Productivity Monitoring

Productivity monitoring software (PMS) is a class of technology tools that support information security by providing the capability to scrutinise computer usage. This may be deployed across a network of office computers to ascertain the activities of workers.

PMS captures the actions that each user performs on a computing device. This includes application usage, folder windows opened and directories viewed. Text entered and edited, URLs of web pages visited, and practically every on-screen event may be recorded.

This protects data by ensuring that employees and contractors stick to their assigned tasks, and pose no risk to the business. As a consequence of protecting data, it produces an audit trail of activity which can be used to determine the productivity of each user. The practice is more formally termed User Activity Monitoring (UAM).

Identifying the Insider Threat Groups

For the purposes of assessing risk from insider threats, three core groups of computer users may be identified:

- Full-time employees
- Contract, temporary or freelance staff
- IT management and support staff

Full-time Employees

Full-time, permanent employees are a significant risk because they have high trust levels. In a Microsoft Windows network, Active Directory (AD) Groups enable Users to inherit the identical access privileges defined for members of the same AD Group. This is convenient for configuring generalised access to network resources, but it may be difficult to restrict access to some without causing inconvenience that may slow productivity. Survey data shows 70% of this class of users has access to more data than necessary.

Contract, Temporary or Freelance Staff

Contractors, temps and freelancers also pose a significant risk and have the lowest trust levels. Often moving from competing firms in the same sector, this class of workers is more likely to have the means, motive and opportunity to be responsible for an information security breach.

IT Management and Support Staff

As system administrators, IT managers and support workers have a greater degree of access to systems and data than any other group of users. This level of responsibility means they have a very high level of trust, but also means they pose a considerable risk. They are fewer in number, but have the opportunity to do more damage in terms of a security breach.

In Office, Mobile, and Remote

All of these user groups may be monitored to record their computing activities. This determines their productivity as well as providing the audit trail to identify any information security issues raised by their actions. This can be implemented for each user whether in the office, when mobile or working remotely from a satellite office, over 3/4G or public Wi-Fi, from a customer location or a home office.

Capturing Activity with Productivity Monitoring

Capturing User Activity

PMS collects user data on worker activities, recording use and access of applications, web pages, internal systems and databases. This functionality works across all user groups, regardless of access privileges, and over any connection method to the network.

User Activity Logs

PMS software generates logs from the user activity that is observed. Typically logs are lists of events in chronological order. Log data may identify applications and filenames that have been opened, list URLs of web pages opened, record text actions such as typing, editing, copy & paste, and file actions such as delete and copy.

Screen Video Recording

PMS may employ screen recording of individual user actions. This provides a video record of onscreen activity which may be played back and linked with a corresponding log file of user actions. This provides a written record in the form of the log and the ability to view the actions as they unfolded through video playback.

Applying Productivity Monitoring Software Data

There are three key ways in which PMS may be applied to reduce the risk of information security breaches and to ensure users are fully productive on company activities. Firstly, visual forensics provides for examination of activity after the user session is completed. Secondly, activity alerting enables real-time monitoring and notification of undesired or suspicious user actions. Thirdly, behaviour analytics monitors user behaviour to identify high risk users and red flag their activities.

Visual Forensics

After a user has completed a session, as at the end of the work day for example, both a visual record and a written one in plain English is created, summarising the activities of each user. Should a security event occur which warrants investigation, the software provides the firm with the capability to search for the relevant actions, identify the user responsible for the event, and look at all the other activity of the person in question. Visual forensic data is considered legally permissible evidence.

Activity Alerting

PMS may be used to define and alert the firm of any user activity about which they wish to be notified. Real-time user activity alerting enables immediate responses to any undesired activity. Whether it is searching a database, copying confidential files or opening an application for which the user has no legitimate business use, the firm is able to assess the imminent risk and act appropriately. Alerts may be consolidated over time to build a risk profile for a user; alerts may combine rules to define multiple conditions under which alerts are raised.

Behavioural Analytics

Behaviour analytics lets the firm utilise user behaviour to help determine their risk to the business. Identifying behaviour which is of potential threat to the company and aggregating such actions over time, enables better management of an employee's future risk to the firm. In conjunction with real-time alerts that flags high-risk activity such as copying customer data, analytics lets a firm develop an understanding of each user's patterns of computer usage and productivity, as well as understanding the information security risk attached to each user.

What Does Productivity Monitoring Software Mean for Regulated Businesses?

Productivity monitoring software offers significant advantages for audit and compliance purposes, helping to lessen the burden of increased regulation. PMS achieves compliance with regulatory codes across the globe, including ISO 27001, the internationally recognised standard for information security. PMS enables audit requests for information relating to user activity to be met quickly, accelerating the process of post security incident investigations.

What Are the Implications of Productivity Monitoring Software for Privacy and Policy?

Productivity monitoring of employees by wholesale data collection of every user action raises questions of privacy for every company and each employee involved. Those in highly regulated businesses have to accept that this is now standard operating practice. However, there is enormous potential for people to object to such an approach in sectors where regulatory considerations are reduced or are absent.

Summary

The ability for a worker to be as productive when home or remote working as they are when in the office is one of the great enablers of business flexibility.

- However, whether in or out of the office, firms need to ensure that they have the ability to determine what work is being carried out on company time.

Whatever the KPIs of a business, setting realistic targets and hitting them consistently means there is a need for dependable prediction of the productivity levels of workers.

- To maximise the productivity of workers, firms need to ensure company resources are directed toward the core business and not private employee projects.

There is a need to defend the business against insider threats such as unauthorised information sharing and misuse of customer data.

- Such activity has a significant potential to undermine business performance by compromising commercial advantage and, for regulated businesses,
- it may constitute compliance failure.

Productivity monitoring software enables firms to monitor user activity to address these business issues.

Why is HTL Support a Preferred Technology Support Provider

HTL provides a range of services to support the use of technology in today's businesses. Whether it is infrastructure and user support, internet connectivity or voice communications, we provide the high degree of personalised service.

We are very proud to be able to say that we offer impartial advice because we are independent of suppliers, vendors and manufacturers. Ultimately this enables clients to obtain more value from business technology.

The cloud enables businesses to maximise the benefits of home working while enabling the associated risks to be mitigated.

About HTL Support

HTL Support was initially founded in 2009 by Managing Director Justin Dean, to provide specialist IT support and IT consultancy services to financial services sector clients. Since its launch, HTL has rapidly evolved to offer a full range of cutting-edge, integrated and flexible products and services to a worldwide client base across all industries. Our experience and professionalism has been endorsed both by our clients and by many of the world's leading hardware and software manufacturers.

All companies need to know that their IT support provider is not going to let them down when it comes to important projects. We will always find the right solution and are equally happy either functioning as project managers for your internal IT department or providing an experienced team to work under your own IT Director or project leader.

Further Reading

HTL Support
5 business advantages of cloud-enabled working practices
https://www.htl.london/white-paper/5-advantages-of-cloud-enabled-business

HTL Support
The CSat KPI: A buyer’s guide to identifying the best value IT support services
https://www.htl.london/white-paper/identifying-the-best-it-support-services

Thank You for Downloading Our White Paper

02070936000
talk@htl.uk.com
www.htl.london

30 Churchill Place,
London, E14 5RE