STAFF TIMER

Real Time Monitoring - A data breach prevention tool

2020

Contents

01 Data Breach

Businesses, big or small, need to protect their data from potential theft, deletion, improper access and use, all the time. The reason why companies need real time monitoring tools in order to monitor, detect and stop any inappropriate usage of company sensitive data and also still be able to increase productivity and task collaboration. As we all know during remote work you can not ' go CCTV' every employee which makes it difficult to know how your employees are using your data.

Defining Data Breach

A data breach is defined as a breach in the system that discloses sensitive and confidential information to an unauthorized person, who has no authority to access protected information. The documents and/or files breached are shared without any consent or permission of the authorized party and without their knowledge.

Who is Responsible for Data Breach?

It is always assumed that a data breach is initiated by an outside hacker, the assumption is true but not always. They can also be caused by:

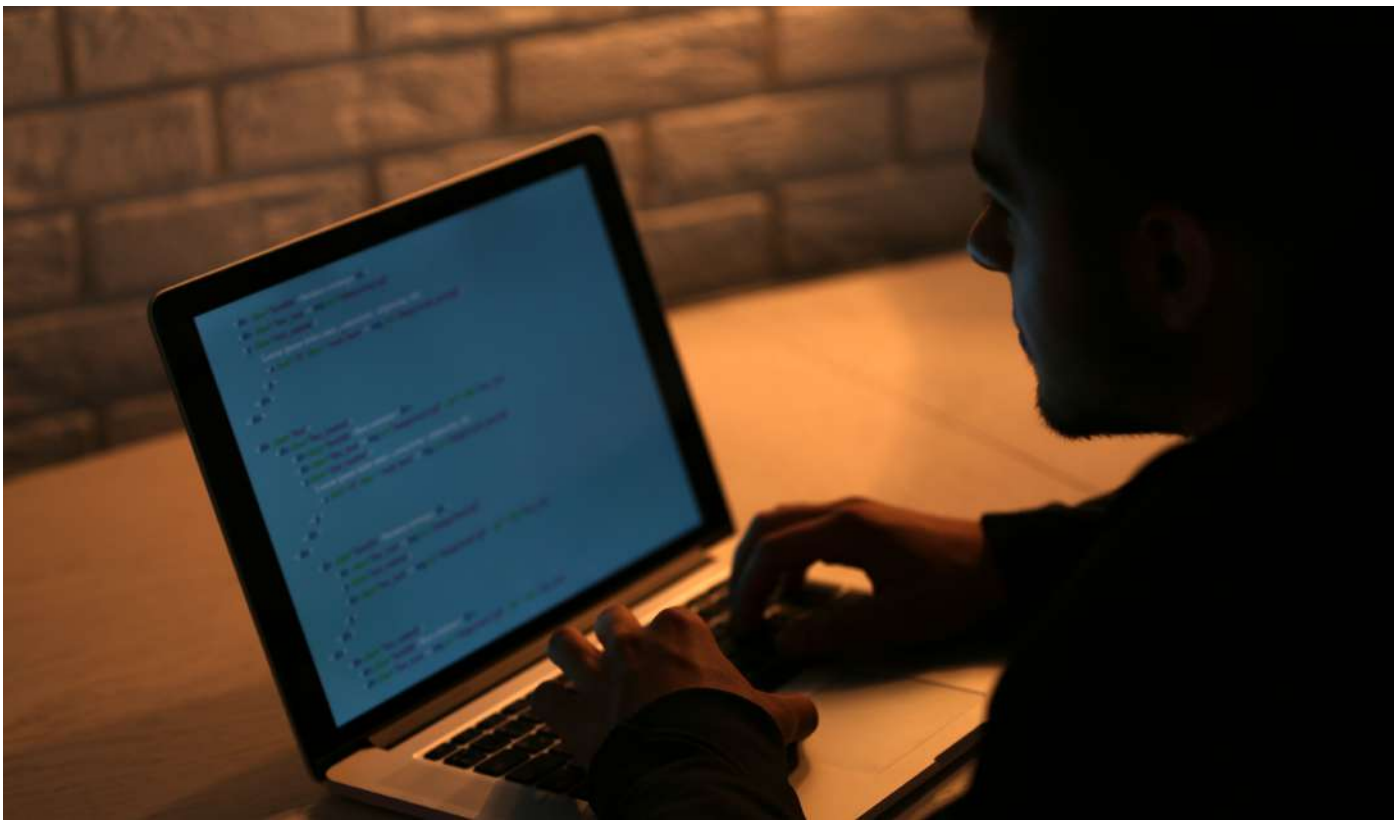
An ‘unintentional’ insider:

In this scenario, say for example, an employee is accessing their co-workers' work computer to read or check some files without having the permissions from the authorized person or the laptop owner. Even though in some cases it is harmless without any malicious intentions because no information is shared.

But however since it was viewed by an unauthorised person without having the permission, it will be considered a data breach.

A Malicious Insider:

Unlike accidental insiders, this individual accesses the data with bad intentions and in order to bring harm to the company. The malicious insider can have the authority to access the data but not only he shares the data but also uses it in heinous ways.



Data breach through stolen Devices:

This can be caused when an unlocked laptop or external device containing sensitive data, unencrypted, gets stolen or goes missing from inside the company.

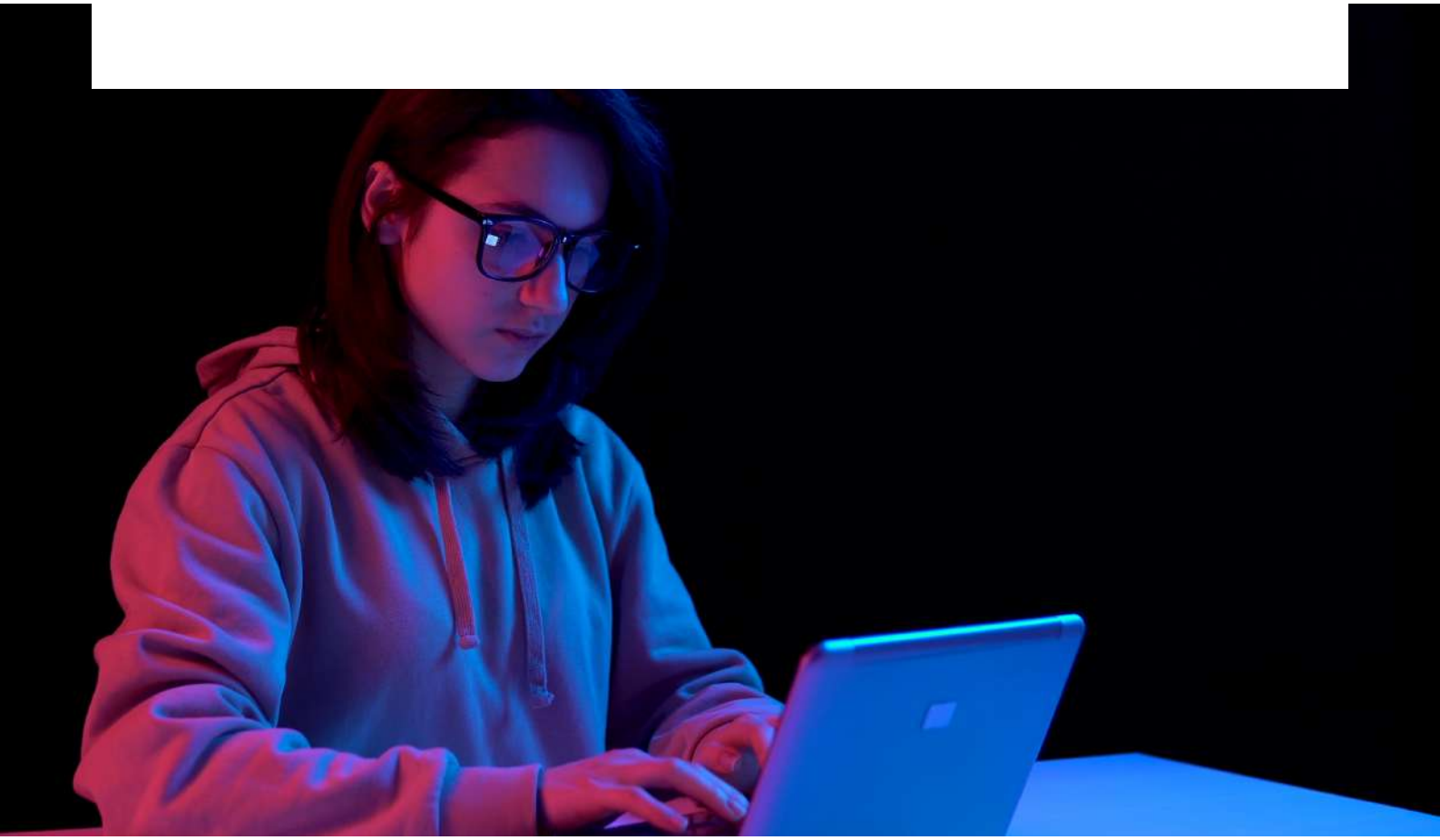
Outside hackers:

Now these are hackers who use various attacks to obtain information from a network or an individual.

Even though companies should trust their employees because they have hired them in the first place. Proper background screening is advised. But still there can be people who enter the organization with bad intentions and at that point you are unable to identify because they are good at hiding their schemes.

Real damage to the businesses happens when that person steals the company sensitive information with the intention to sell it for financial gain or to cause harm.

If such actors are inside the company, they spend a good amount of time learning the vulnerabilities in the system that makes it easier for them to plan. Once they make themselves aware of your weak points, that's when they attack. Either they copy and steal information directly from the devices issued to them via a USB or they let you download malware which makes their job easier. Once malicious actors are inside your system, they can get any data they want because they have lots of time. And on average it takes almost 5 months to detect a data breach, give or take.



02 Common attack methods used inside the company:

- The majority of data breaches happen because of weak credentials and system passwords. In companies, mostly the same password is shared by many and on various platforms which makes it easier for them to access or steal it.

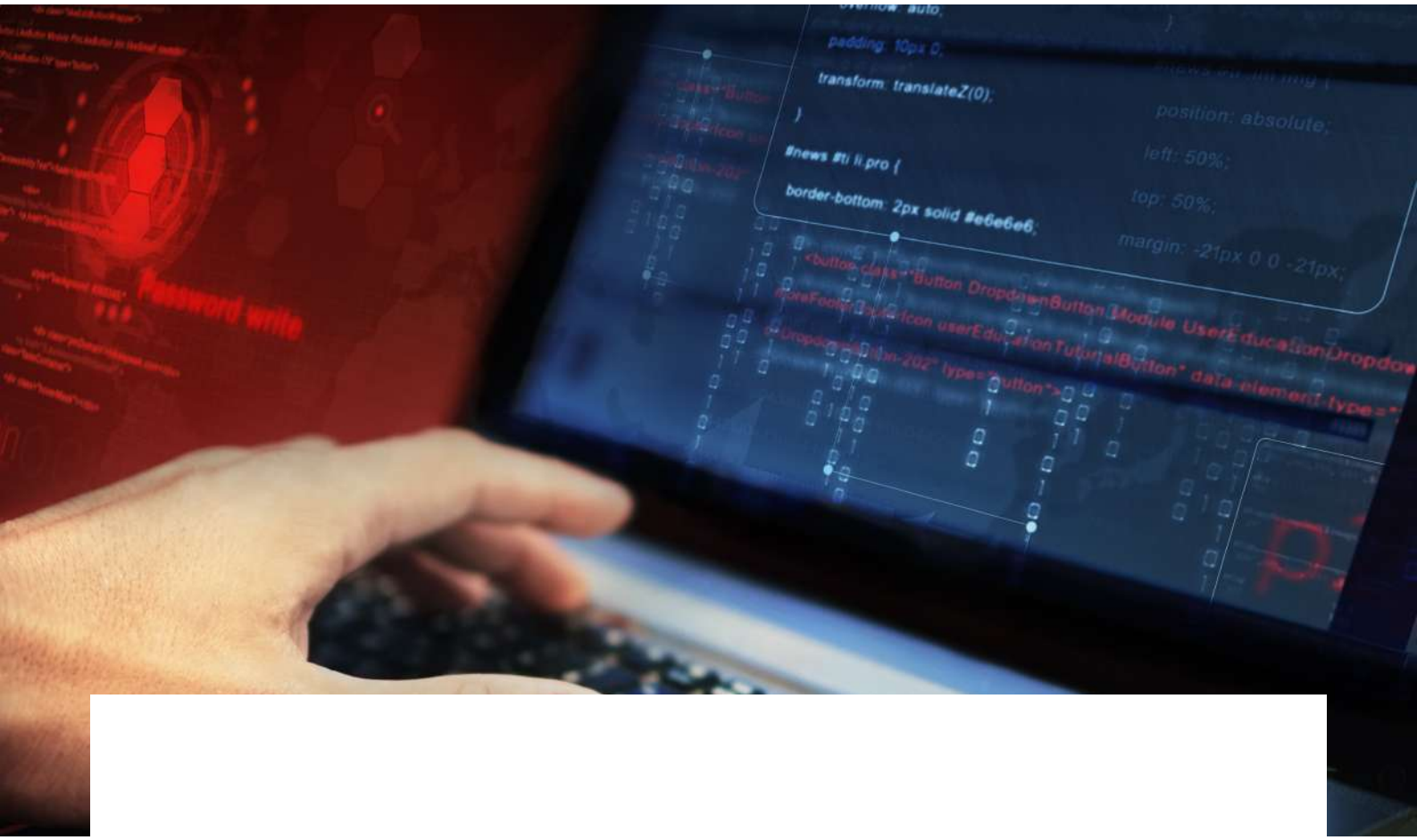
- Weak authentication and security protocols taken by the main admin to protect the computer.

- Unauthorized use of external devices to steal the data without any trace. Such as copying data to the USB.

- Third party access to your system and data. Malicious actors can get into your system through third parties.

- When employees are allowed to bring their own devices into the workplace, it's easy for those insecure devices to download apps that give hackers access to data stored on the device such as work emails or important files.

03 After effects of a Data Breach



A data breach can have devastating effects not only on your organization's reputation but finances as well.

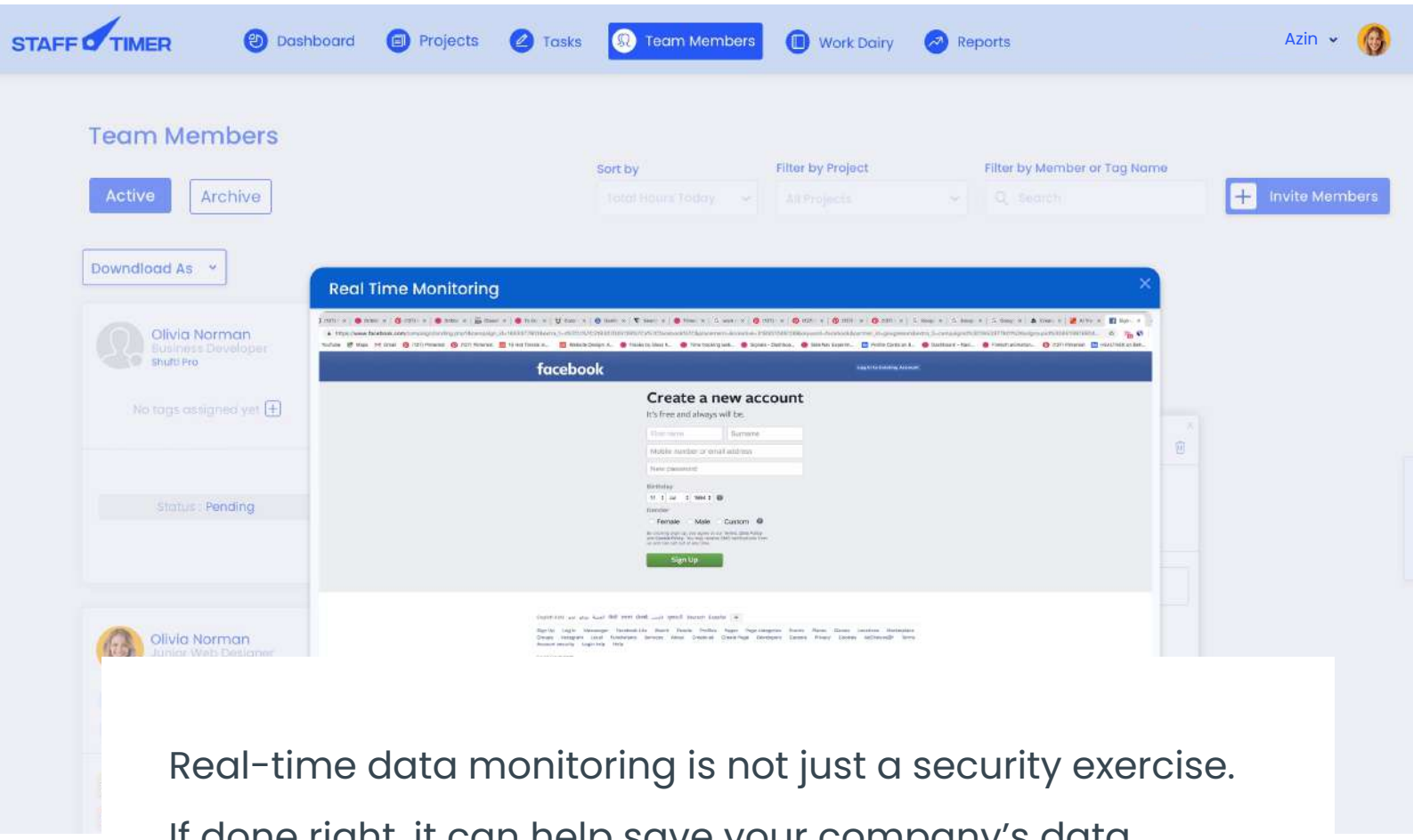
Financial and Reputation consequences:

A Lot of financial problems can arise due to the nature of the breach. Victim organizations may have to deal with the security costs that are incurred as a result of the breach. As some organizations deal with sensitive customer data, they somehow might have to compensate them for putting their privacy in danger. Their share value and trust may also decrease.

Operational and legal consequences:

Data breach also impacts the business operations. In some cases, important data can be lost forever and in some cases it takes months for the victims to recover the data and some organizations may have to shut down unless they find a proper solution on how to deal with it. Either way it is bad for business operations. And let's not talk about the legal consequences it might bring. Customers can sue you for losing and putting their data in jeopardy to begin with.

04 Real-time monitoring - A Prevention tool



Real-time data monitoring is not just a security exercise. If done right, it can help save your company's data. Tracking what's happening on your employees screens in real time is crucial to ensure proper data security. Real time screen monitoring does not mean espionage which by the way a lot of employees resist. Real time screen monitoring helps organizations watch over how their data is being used and how to manage data access. Here I will mention how staff timer app can help you protect your data at all costs.

Complete visibility of your employees:

Staff timer app's Real time screen monitoring via live screen sharing gives you complete visibility of your employees' screens and how they are using the network and company's data. You can easily identify and focus if something critical is about to happen, beforehand.

Keep an eye on user activities:

Through this tool, you can keep an eye on user activities and who is doing what, where and when. With the Staff timer app, you can address any or all insider threats at the spot.

Staff-Timer is extremely concerned about your data. Our security features save your data in encrypted form (ssl encryption) which only you can access. Staff timer LTD. itself has caught and addressed such issues recently where an employee is trying to steal data by copying it to a USB device. We hear many similar case studies and stories from our clients as well everyday.

05 You can also protect your assets through Staff timer app by

- Gaining more visibility into user activities
- Identifying threats on the spot before they cause damage
- Monitoring whether the data provided has been used properly

06 Stafftimer app Introduction

Staff Timer app is an AI-enabled software that effectively tracks employee work hours using key features like real-time monitoring and intelligent reporting.Stafftimer App is Time Tracking solution for teams dispersed globally powered by Staff Timer Ltd.

It is the perfect tool for employers who are managing remote teams and distributed teams. It not only gives you the exact billable and non-billable hours but the ability to remotely monitor the team members through

- Real time screen monitoring
- Minute by minute screenshots
- Review work through daily work videos
- Measure keyboard and mouse activity
- Monitor screens in real time
- Audio clips for task assignment
- Time sheet

STAY FOCUSED!

Questions for us ?

Email us

sales@stafftimerapp.com

Skype

support_60876

Call us

+44 1622 370838

For live demo

https://calendly.com/harri-st