mailock

WHITEPAPER

Fighting Fatigue and Stress: How Maximising Remote Workers' Wellbeing Can Minimise Cyber Risk

beyondencryption.com

CONTENTS

An Overview

The Story So Far: Covid-19 and its Effect on Businesses

In 2020, the arrival of Covid-19 completely altered everyday life, rapidly transforming the business landscape and pushing the majority of commerce and communications online. This has impacted companies in several ways:

Turning the dial on digitisation

Businesses have dramatically accelerated the digitalisation of their supply chain and customer interactions, with McKinsey revealing that organisations are now 3 to 4 years ahead of their digital transformation projections. The study also reveals that 55% of global products and services are now partially or fully digitised, with 58% of customer interactions taking place digitally.

From the office to the kitchen table

During 2020 and the numerous UK lockdowns that took place, an estimated 46.6% of employed individuals experienced working from home in some capacity. Although remote working was thought to be a temporary solution, an initial Gartner survey reveals that it will have longer lasting impact, with an estimated 82% of companies stating they will continue to allow their employees to work remotely for at least one day a week.

As businesses establish more long-term plans for their hybrid and remote workforce, a key topic for consideration remains the security of maintaining a working-from-home approach. According to research, workers have already faced numerous IT challenges, including: →

44%

Poor connectivity

41%

Lack of IT support

30%

Difficulty with navigating technical problems

Source: Digit

FIGHTING FATIGUE AND STRESS

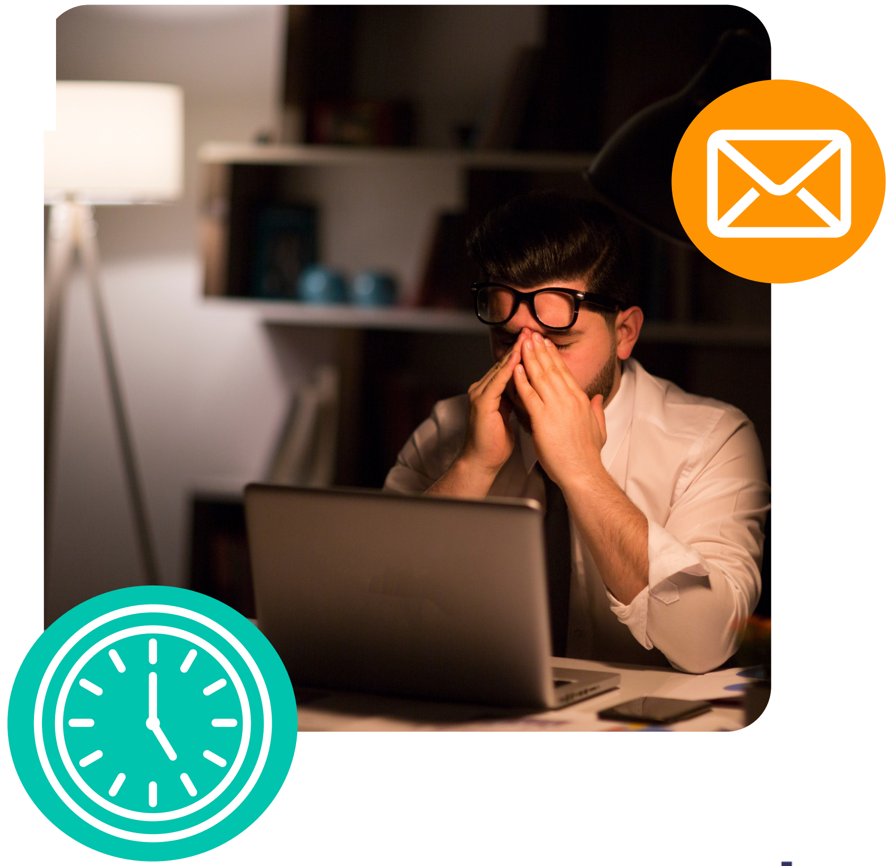
The Dangers of a Digital Approach

These combined issues have affected company efficiency, with 54% of employees stating they have suffered lost periods of productivity. In addition, concerns over security measures are at an all-time high, with 78% of senior IT believing their organisations lack sufficient protection and 20% of business leaders admitting that data breaches are their top cyber concern.

With employees working across different locations, the traditional 'castle and moat' approach is no longer viable, offering companies less direct control over cybersecurity. However, the potential negative impact from remote working stretches farther than IT. Studies are starting to explore the psychological impacts that remote working has on employees, how this affects a company's overall cybersecurity, and what business leaders can do to counteract this.

How has Remote Working Changed the Average Workday?

Let's take a look.



Longer hours
With remote working blurring the lines between home and the office, 56% of employees are finding it increasingly difficult to switch off after their working day. Coined the 'always on approach', remote employees are spending increasing amounts of time working, with a study by the Office of National Statistics revealing that they work an average of 5 hours a week more than someone who remains in the office.

Extended email use
Longer remote work hours have led to increased reliance on communication tech, with businesses seeing a 50% increase in overall email use. Employees now spend an average of 28% of their day reading and responding to emails, with 36% of home workers reporting that they constantly need to be at their computers to respond quickly to messages. This has caused the average workday to be extended by 48.5 minutes, with 92% of employees who work from home stating that they reply to emails outside of office hours.

When remote workers were asked how they felt about this elevated use of email, 89% revealed that it was one of the most unpleasant aspects of working remotely, with 54% stating that they would rather tackle a commute to work than have to keep organising their email and other message notifications.

Curious about how much time you spend on email? Check out this handy calculator.

Increased time in meetings
Email use is not the only form of communication that has increased. Company use of video chat has grown by 54% since Covid-19 started, with Microsoft revealing that time spent in weekly virtual meetings has grown 150% in the past year. However, although the number and duration of meetings have heightened, a study by Harvard Business School shows overall productivity in meetings has decreased. 1/3 workers feel that video calls are one of the most unpleasant parts of their day, with 44% wishing they had more meeting-free days.

CONSEQUENCES

The Impact of Working from Home on Employee Wellbeing

Although remote working has provided many benefits, the combination of extended hours and increased use of digital communication has had a profound effect on employee wellbeing, with an estimated 44.4% of remote employees experiencing a decline in their mental health since the start of the pandemic.

Research has also revealed that those working from home are 30% more likely to experience a decline in their mental health than employees who remain in the office, with fatigue and stress being common.

CONSEQUENCES

Employee Fatigue

Feeling high levels of fatigue has increasingly become the norm for those working from home, with 37% of employees experiencing disturbed sleep and 52% feeling that they are not getting enough rest overall.

According to SHRM research surrounding the impact of Covid-19 on employee mental health, this has led to:

- 35% feeling tired or having little energy.
- 41% feeling burned out from their work.
- 45% feeling emotionally drained from their work.
- 44% feeling used up at the end of a workday.

This lack of energy and motivation has been felt most strongly when encountering emails and video calls. London South Bank University has discovered that staff energy levels are depleted significantly faster when working from home and engaging in extensive online communication, with 'Email fatigue' predicted to be the main reason that 1/3 of office workers will eventually quit their jobs.

CONSEQUENCES

Employee Stress

In the UK alone, 800,000 people experienced work-related stress, anxiety or depression in 2020-21, with an estimated 17.9 million working days lost each year due to mental health-related absences. For staff that work from home, 41% consider themselves to be highly stressed, in comparison to 25% of employees who work on-site.

When considering the reasons behind this level of remote worker stress, email is seen as a major contributor. A study that involved monitoring employee heart rate during computer use has revealed that the longer one spends on email in an hour, the higher their stress is for that hour. Additionally, employees are reported to experience increased anxiety when frequently exposed to after hour emails, as they induce a feeling of 'anticipatory stress'.

Staff find themselves constantly alert and waiting for a message to come through, even when they are off the clock, negatively impacting time that should be restful and work free.

'Employees are reported to experience increased anxiety when frequently exposed to after hour emails.'

THE IMPACT

How does Low Employee Wellbeing Affect Company Cybersecurity?

From a cybersecurity perspective, we begin to see why an organisation may not be as secure as they think. Mistakes are often to blame for cyber risk and damage within an organisation, falling under the umbrella of 'human error'.

43% of employees have admitted to making mistakes that resulted in cybersecurity repercussions for their company. Wellbeing should then be a crucial part of any cybersecurity strategy, with human error being the no. 1 cause of data breaches in 2020, with 90% of all cases reported as such.

When considering how low mental health affects an employee's capacity to work, research has shown that:

40% of employees make more flawed decisions.

30% cannot concentrate on tasks as well as they should.

26% admit to being less productive throughout the day.

52% make more mistakes when they are stressed.

41% make more mistakes when they are tired.

STATISTIC SPOTLIGHT

Fatigue and Cybersecurity

Burned-out employees are:

3x as likely to feel that security rules and policies are not worth the effort.

Almost 2x as likely to pick easy passwords and reuse them for all their accounts.

(Source: 1Password)

When sending company emails:

58% of employees have sent an email to the wrong person.

44% of those workers cited fatigue as being the main contributing factor.

(Source: IFA Magazine)

STUDY IN FOCUS

Stress and Cybersecurity

Research has revealed that stress can deeply affect our short and long-term memory. When thinking of the implications this can have on cybersecurity, stressed individuals may be more likely to forget:

- Cybersecurity or compliance training they have completed.
- To check inbound messages for fraudulent links or files.
- To check outbound messages that include sensitive data are being sent to the right recipient.

CYBERSECURITY FOR BUSINESSES:

Why Should You Care?

Neglecting employee wellbeing can evidently have serious implications for cyber risk. So, what are the consequences for organisations that overlook this?

Cost: When considering the cost to citizens, businesses and the government, it is estimated that cybercrime costs the UK £27 billion per year.

Compliance: Failing to meet compliance measures can result in hefty fines from regulatory bodies, with UK GDPR breaches carrying a maximum fine of £17.5 million or 4% of annual global turnover.

Customer loss: Your organisation's reputation is put at risk when associated with a breach of client data, with 20% of companies losing customers as a result of mistakenly sending an email to the wrong person.

Company downtime: When experiencing a cyberattack, organisations often experience substantial periods of interruption, with the average downtime period currently set around 22 days.

beyondencryption.com

IN REALITY

How to Tackle Poor Employee Wellbeing: Company Culture

When considering how best to confront the rising issue of employee mental health, improving company culture and technology will play a significant role.

Managerial Support:

There is a worrying lack of help and resources available to those suffering from work-related mental health issues. In a recent survey, less than 1/6 employees felt that their mental health was being well supported, with 51% of respondents saying they feel the need to put on a brave face at work. In fact, 68% of workers would rather talk to a robot than their manager about any stress or anxiety they are experiencing.

More extensive help should be available to vulnerable workers. 78% of surveyed employees agree that their company should be doing more to listen to their needs.

of employees think their company should be doing more to listen to their needs.

IN REALITY

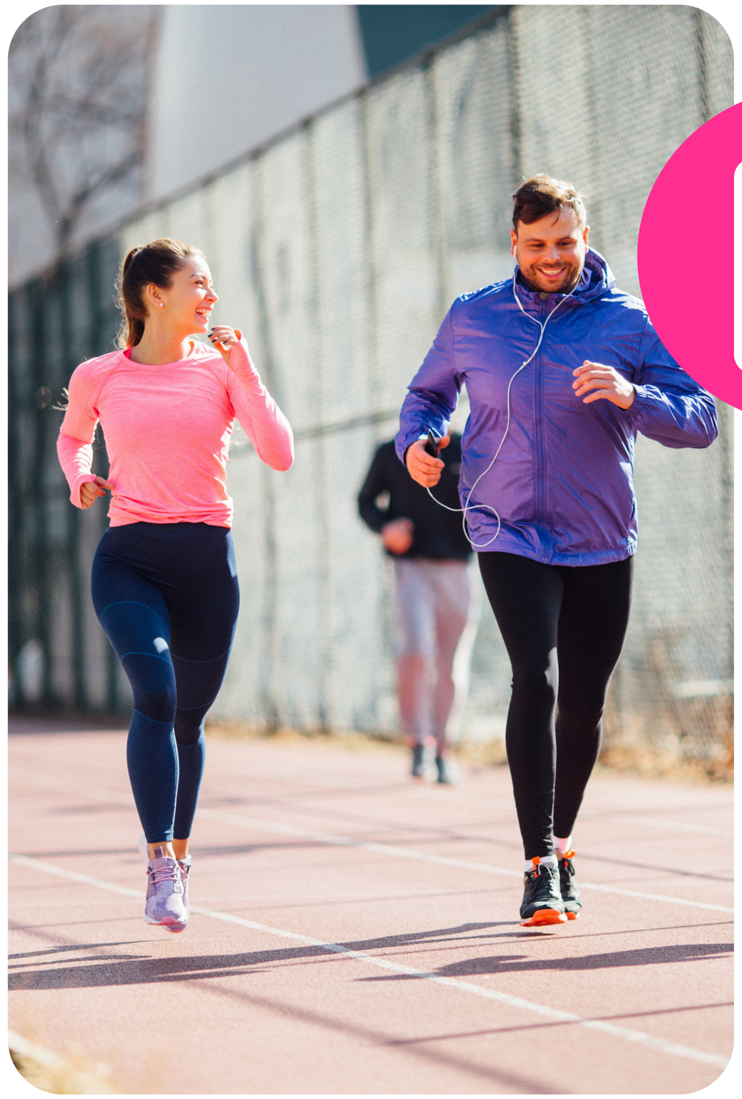
How to Tackle Poor Employee Wellbeing: Company Culture

Work-life balance:

With remote working, people lose crucial transition periods between work and home, leaving employees struggling to switch off from work and increasing feelings of fatigue.

In a survey, remote workers at SME's were asked what their companies could do to help prevent burnout. The responses all revolved around equalising the work-life balance, with the top suggestions including:

- Keep communication and work expectations within working hours - 59%
- Encourage fitness/wellness programs- 59%
- Organise regular 'fun breaks' with colleagues- 46%
- Reduce large workloads- 41%
- Be encouraged to take annual leave- 26%



How to Tackle Poor Employee Wellbeing: Technology

Cybersecurity Training:

Currently, 42% of UK working adults are scared of making a mistake at work that could affect their companies cybersecurity, with remote workers (63%) feeling more at risk from cyber threats than with on-site staff (51%). A key way to prepare and protect employees is to provide them with cybersecurity training, which businesses often fail to prioritise. At the beginning of the pandemic, 2/3 remote workers had not received any in 2020, with only 11% of businesses regularly providing security courses to non-cyber employees.

More recently, research has revealed that more remote staff (59%) are receiving necessary cyber training. However, when tested on basic cybersecurity knowledge, 61% of surveyed individuals failed. It's clear that businesses do not only need to increase the quantity of training they are providing, but the quality too, to ensure that employees retain the necessary knowledge to make training effective.

Security software:

One of the most important ways to ensure employee wellbeing and cyber safety is through security software. Tech is becoming a key component for empowering employees, helping them to nurture core skills. 45% of remote employees who don't follow their company's security policies say they would be more likely to do so if technology was used to help.

In 2020 an estimated 37% of companies increased spending on their data security, with funds contributing towards the deployment of one-time password technology (51%), biometric authentication (40%) and mobile identity verification (36%).

Mailock: A Technology Solution for Remote Working Challenges

OUTBOUND SECURE EMAIL

Mailock is Beyond Encryption's secure outbound email solution, providing employees and customers with a safe platform to send confidential messages and documents. Mailock gives employees peace-of-mind when dealing with client or company data, offering specialised features to prevent harmful data leaks:

Encryption- protect emails with military-grade, AES-256 encryption where not even we can gain access to your data.

Authentication- ensure messages are opened by intended recipients only with Q&A and SMS authentication.

Revoke- Send the wrong document to the right recipient? No problem, Mailock's revoke capabilities allow you to recall your email and attachments.

To find out more about Mailock's features and what Beyond Encryption can do for your business, get in touch.

Supporting your Business

MAILOCK ENABLES YOU TO...

MEET ESG GOALS

Strengthen your environmental, social, and governance proposition. Businesses with strong ESG goals achieve higher equity returns and reductions in bottom-line risk.

CUT OPERATIONAL COSTS

Over 9.5 billion* documents are sent in the UK each year, the vast majority by businesses. In the UK financial services industry alone, digitising print and post operations could save £1.3 billion**

PROTECT DATA

The most common cause of data exposure is sending an email to the wrong person. Protect your staff and any sensitive information you send with identity authentication and full revoke.

Sources:
*https://www.statista.com/statistics/1006816/royal-mail-volume-of-parcels-and-letters-delivered-uk/
**https://www.ns-businesshub.com/science/going-paperless-cost-savings-uk-financial/

MAILOCK HELPS YOU...

KNOW YOUR CUSTOMER

Digitise friction-inducing KYC, anti-money laundering, and ID Verification.

STRENGTHEN YOUR BRAND

Add company logos to secure emails. Show your business as a leader in data protection.

CUT POSTAGE BUDGETS

The financial services sector alone could save up to £1.3 billion by reducing its' paper output.

REDUCE DATA RISK

Emails sent to the wrong person are the #1 cause of data exposure. Prevent misfires.

BUILT TO COMPLY WITH LEGISLATION

✓ GDPR

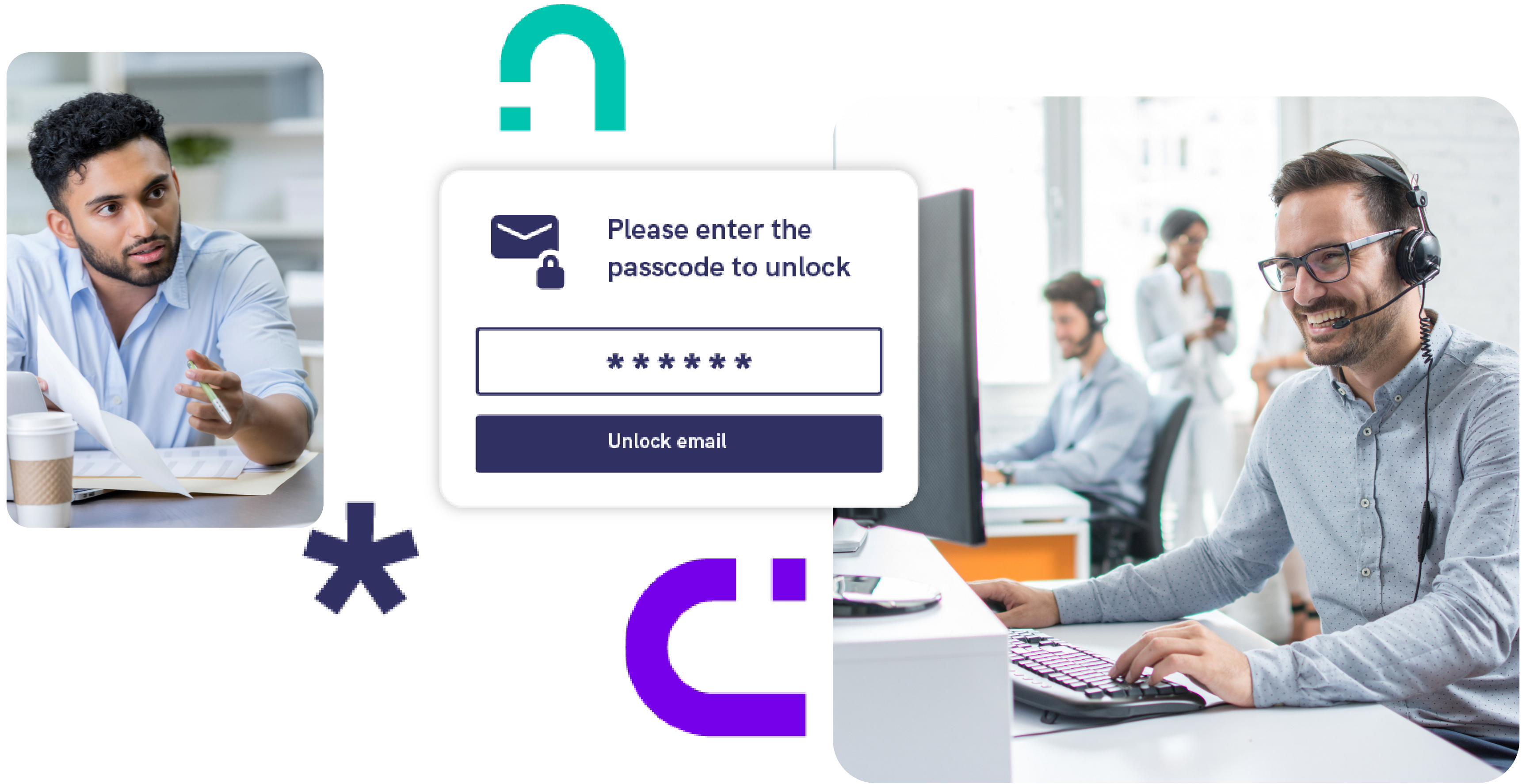
✓ MIFID II

✓ ISO 27001

beyondencryption.com

About Beyond Encryption

Beyond Encryption is a SaaS company based in Fareham, Hampshire. We are passionate about helping companies and individuals secure their data and online identity, all while remaining compliant, reducing costs, and improving operational efficiencies.



Please enter the passcode to unlock

******

CONTACT US

beyondencryption.com
sales@beyondencryption.com
Beyond Encryption, Gloster Court,
Whittle Avenue,Fareham, PO155SH

Beyond Encryption