
Kingston
TECHNOLOGY
The challenges of mobile workforce security – and how to solve them
#KingstonIsWithYou

The challenges of mobile workforce security – and how to solve them

Foreword

It's time your workforce paid more than just lip service to data security. You already know that remote working is a business enabler. But the challenges posed to your network security and compliance with GDPR are too big to ignore. Many businesses believe that it's an insurmountable challenge to keep demonstrative control over the IT ecosystem without significant expenditure. But it doesn't have to be that way. Cost cannot be an excuse.

The systems, services and products are out there – and they cost less than you may have thought. In fact, the reality is that the security challenge is not only financial or technical, but cultural. You can create the right IT environment for remote working with relative ease. But unless your staff adopt the right attitudes and behaviours towards security and data compliance, your business will struggle. And the potential costs of breaches are incredibly high.

The products are out there.
But education is everything.

Contents

This short ebook has been compiled by three experts in data security and remote working.

Rob Allen
@Rob_A_kingston

Rob is the **Director of Marketing & Technical Services at Kingston Technology**, and has been with the company since 1996. In his role, Rob is responsible for overseeing PR, Social Media, Channel Marketing with Digital Marketing Media and Creative for all Kingston brands and products.

Rafael Bloom
@rafibloom73

Rafael is the **Director of Salvatore ltd.** In this role he helps companies to manage the strategic, commercial and procedural challenges and opportunities created by technological and regulatory change.

Sarah Janes
@SarahkJanes

Sarah has been the **Managing Director of Layer 8 Ltd** since 2014. Their mission is to empower security managers to deliver and sustain effective cyber security culture change across whole organisations, from small businesses to large corporates.

The challenges of mobile workforce security – and how to solve them

Table of contents

Section 1 – The problem

Remote access is critical

The days of work being done exclusively in a central office location are long gone. Staff access work email on their personal smartphones. Your COO spends days working from home or their favourite café. The field sales team access mission-critical business data from client sites. Remote working is the new normal.

It boosts productivity and staff retention.[1] It reduces business overheads.[2] It's good for the environment.[3] Research suggests that **70% of professionals work remotely at least once per week**.[4]

However one person can compromise the security integrity of your entire organisation if they don't follow the necessary security protocols.

Compliance with GDPR is a must

Appropriate security should be non-negotiable, both for the integrity of your organisation and for preventing breaches to GDPR compliance. And GDPR is serious. The Information Commissioner's Office (ICO) recently handed out fines to British Airways and the Marriott hotel chain totalling almost £300 million for data breaches.[5]

What sort of businesses are at risk?

If you have staff members working remotely, or using their own devices to access business systems, then your business is at risk.

[1] **Inc.com: A 2-Year Stanford Study Shows the Astonishing Productivity Boost of Working From Home -** www.inc.com/scott-mautz/a-2-year-stanford-study-shows-astonishing-productivity-boost-of-working-from-home.html

[2] **PGi: What are the cost savings of telecommuting? -** www.pgi.com/blog/2013/03/what-are-the-cost-savings-of-telecommuting/

[3] **FlexJobs: 5 stats about telecommuting's environmental impact -** www.flexjobs.com/blog/post/telecommuting-sustainability-how-telecommuting-is-a-green-job/

[4] **CNBC: 70% of people globally work remotely at least once a week, study says -** www.cnbc.com/2018/05/30/70-percent-of-people-globally-work-remotely-at-least-once-a-week-iwg-study.html

[5] **The Guardian: GDPR fines: where will BA and Marriott's £300m go? -** www.theguardian.com/business/2019/jul/10/gdpr-fines-ba-british-airways-marriott-data-watchdog

70% of professionals work remotely at least once per week.[4]

Section 2 – The challenges of remote access

Remote working presents several security challenges.

They can be difficult to reconcile but must be taken seriously for the integrity of your organisation.

Businesses struggle to keep their internal systems and devices advancing at the pace that technology generally is developing.

Sarah Janes
@SarahkJanes

Managing Director
Layer 8 Ltd

"A major concern under the new GDPR legislation is for a business to have control over the personal data they hold. This is not possible if they don't know where that data is being stored."

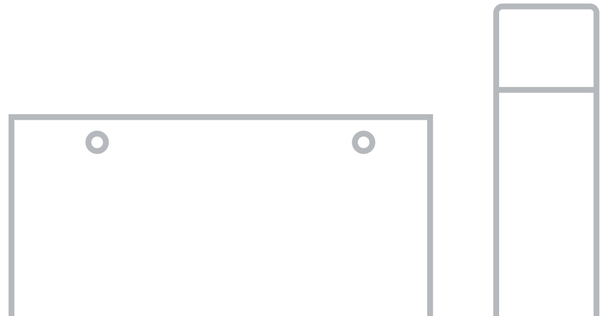
Indeed 38% of remote workers hired by SMEs feel that they do not have the technological support or expertise they need when working at home or in a public space.

This can lead to employees finding workarounds that – breach your data protection efforts and leave your business exposed to security threats. Unless your security protocols are designed around enabling efficiency for your staff, they will find workarounds – storing sensitive information in places like Slack, Dropbox, personal email or private USBs. Even worse you will instil a Them v Us culture between your IT security team and the rest of your workforce. Your business is at risk.

Rob Allen
@Rob_A_kingston

Director of Marketing & Technical Services, Kingston Technology

"In my experience, the larger the organisation the more restrictive and cumbersome it becomes for employees to work remotely – with lengthy login times and security measures to navigate."



Section 2 – The challenges of remote access

BYOD

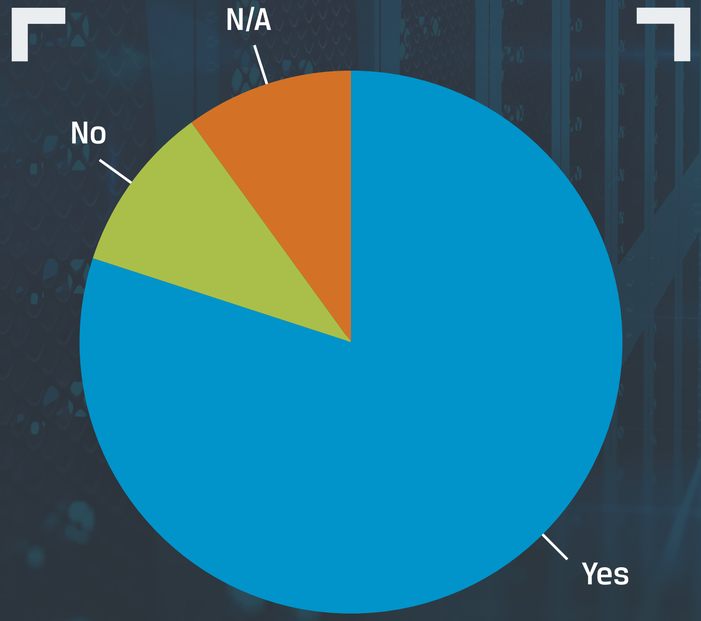
It's common for modern professionals to use their smartphones to read work email; to access your organisation's data from personal laptops and tablets. This poses dangers. Is your team transferring data out of the organisation? Is their hardware safe from harm and their software secure? These are questions that need to be answered.

Sarah Janes
@SarahkJanes

Managing Director
Layer 8 Ltd

"Businesses have a massive retrospective challenge just to understand where their data is being held."

Do you have any concerns that employees find unsuitable workarounds with enforced security measures?



Source: Kingston Survey 2019

Public WiFi networks

It's not all about working from home. What about the café crew, logging in with latte in hand? Public WiFi networks are a hacker's paradise. You must arm your workforce with the tools to mitigate the risk.

Cyber-attacks and sophisticated phishing

Phishing emails that target individual employees are increasingly sophisticated and convincing. Are your staff trained in how to identify them? What about the ever-evolving threat of malware and ransomware? Your devices – all of them – must be protected.

Section 3 – The infrastructure of remote access (and a note on mental mindset)

The technology exists to simplify the security challenges of remote working. And it doesn't have to cost a fortune.

Creating the right infrastructure

Employers must make sure their mobile workforce can easily and efficiently access the necessary tools and data to perform their daily tasks and be productive. It's not necessarily about adding new products but about making the right selection in the first place. For example, most companies will need computers or laptops. So, choose encrypted hard drives or solid state drives. That way if company data is lost or stolen, it's protected from getting into the wrong hands. Additionally, if there is a data breach, the ICO will look on you more favourably if you have taken demonstrable measures to protect your data.

Work with the right vendors

When it comes to IT security, there are countless manufacturers and vendors. Do your research. It's all about having a system in place that comes from a trusted solution provider with the specific expertise in enabling your mobile workforce.

VPNs

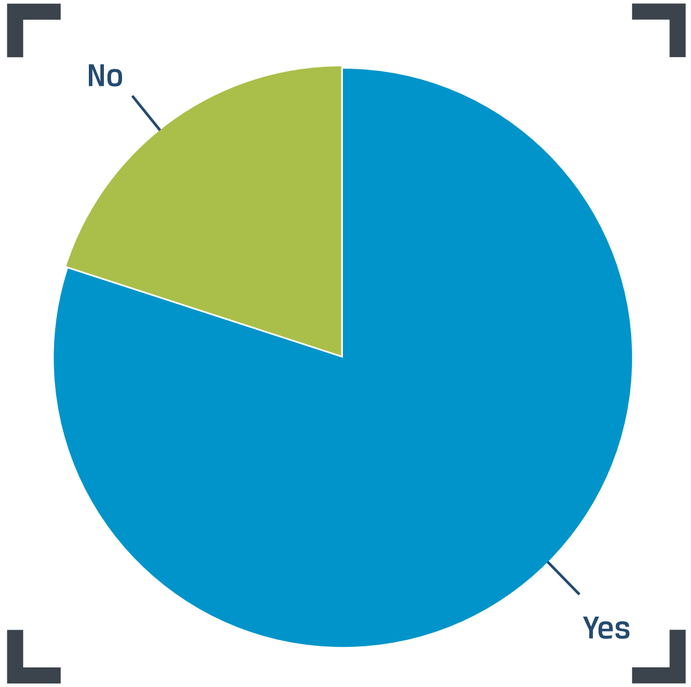
If protecting your organisation means using a virtual private network, then giving the right individuals the appropriate tools will significantly reduce your risks. VPNs are particularly salient for staff who are accessing business data over public WiFi networks.

DLP software

Nearly all DLP software suites offer the ability to restrict access to your network, while whitelisting certain devices like encrypted USBs that have been designed from the ground up to be uniquely identifiable. This comes at a minimal cost. (Take a look at Kingston's range of USB offerings, which are customisable to your organisation.)

Do/did you have to make significant changes to ensure that your business is GDPR compliant?

Source: Kingston Survey 2019



Section 3 – The infrastructure of remote access (and a note on mental mindset)

USBs and SSDs

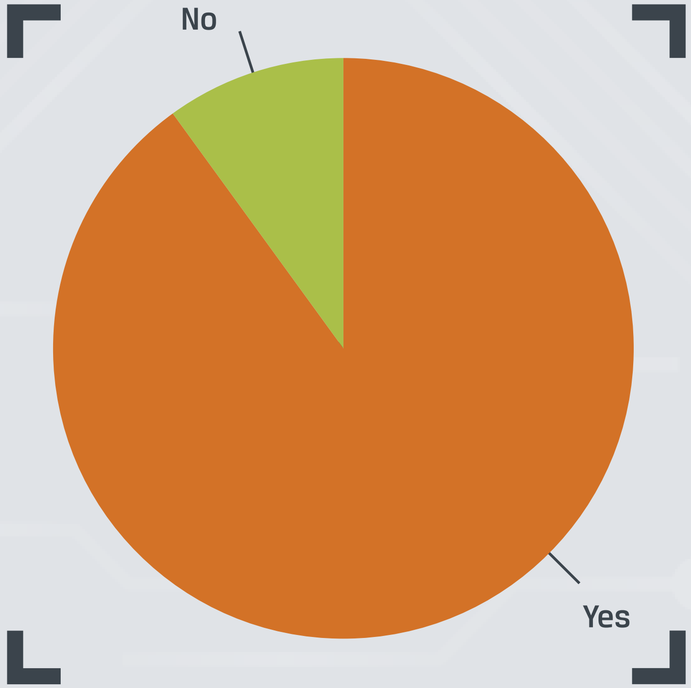
Deploying encrypted USBs and equipping your notebooks with hardware encrypted SSDs goes a long, long way to resolving the challenges of remote working. With an encrypted USB plus hardware encrypted SSD (WiFi or not) your data is protected and available anytime, anywhere. And if a device is lost or stolen, you can be confident no one will have access to the encrypted files. You can even remotely destroy lost USBs.

Always assume the worst

Sometimes an optimistic mindset is a thin veil for blind faith. As a security team it's always best – necessary, even – to assume the worst. Trust in your workforce and your security measures. But always hypothesise about worst case scenarios. You will do wonders for the integrity of your network security by assuming it can – and will – be breached.

Do you compliment endpoint security software with your workplace mobile devices? e.g USBs, notebooks etc.

Source: Kingston Survey 2019



Section 4 – Educating your staff is the only way

The right technology is only half of the battle. The real challenge is what happens to your staff when nobody is looking. It's why the security challenge is as much a question of workplace culture as a matter of technology. Without appropriate education, your workforce will never see things like GDPR, PECR and other 'rules' as anything more than a headache.

Here are some tips.

No rules without reason

"Don't go behind that tree."

"Don't go behind that tree because there's a lion."

Which is more memorable? Humans don't respond well to rules without reason. Help your employees to understand why rules are there in the first place.

Make it personal

Likewise, your workforce will better understand the security challenge when you make it relevant to their lives. Take GDPR, for example. To help your team appreciate that there's a person behind every data set, make them think about how they would feel if an organisation had a slapdash approach about personal data, they held on them. How would they feel if their details fell into the wrong hands?

"When you explain to an employee how important security and GDPR is for their own interests outside of working life, they begin to understand how an organisation is obliged to protect them."

Rafael Bloom
@rafibloom73
Director at Salvatore Ltd

"Ultimately the best method to enhance security awareness is to open up conversations with employees to find strategies that are both secure and productive."

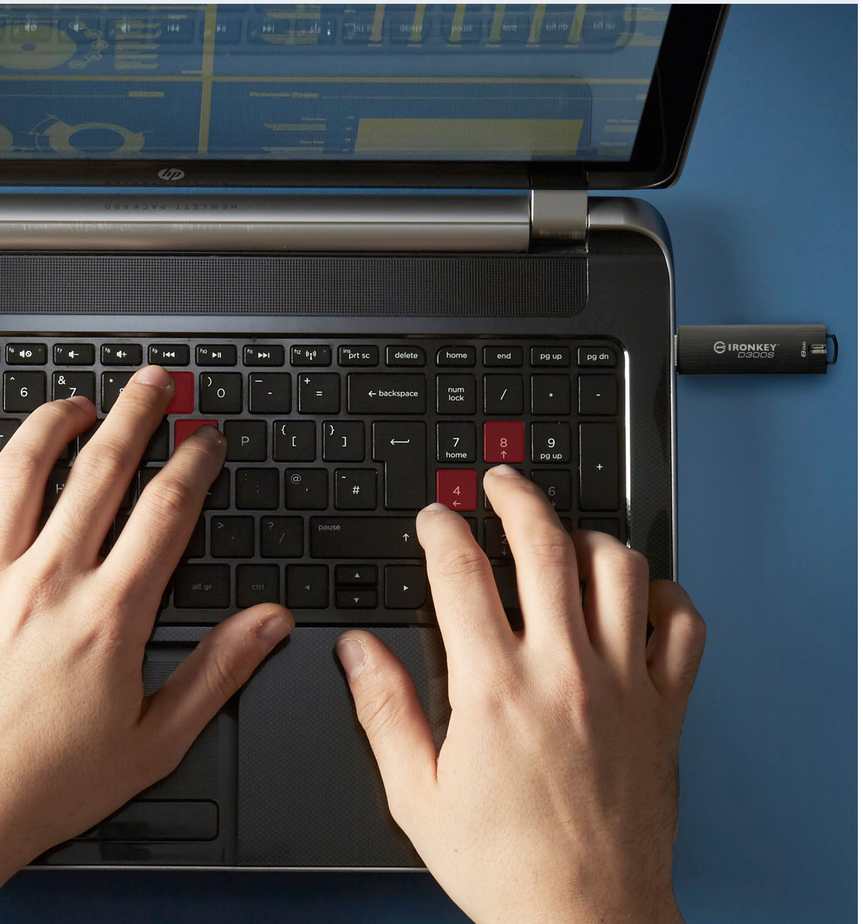
Sarah Janes
@SarahkJanes
Managing Director Layer 8 Ltd

Source: Kingston Survey 2019

Do you regularly audit your employees' external storage usage?

71%	11%	9%	9%
Yes	No	Not sure	N/A

Section 4 – Educating your staff is the only way



Education is the start, not the end

Because most organisations provide a lack of security training internally, businesses have stepped in to plug the gap. But beware false prophets. Education provided by external consultants is often skewed towards the compliance requirements of that business (because this is what they can get funding for), meaning your workforce won't get a full understanding and appreciation of cyber security. Insecure behaviours will persist.

Sarah Janes
@SarahkJanes

Managing Director
Layer 8 Ltd

"If organisations want to truly change behaviour, they need to be brave enough to step away from providing 'tick-box' security training. They need to think about providing education that gives the basics of understanding for security and cyber in general."

Likewise, training isn't a fig leaf. It's all too easy to think that because your staff have received training, they will automatically adopt secure behaviours and become compliant. That is dangerously naive. Success requires ongoing behavioural and cultural nurture.

Rafael Bloom
@rafibloom73

Director at
Salvatore Ltd

"I have experienced the sight of 'certified' companies that keep spreadsheets or notebooks of passwords, or that keep non-encrypted copies of their hard drives in employees' cars overnight. What use is certification when people don't understand the basics?"

Allocate responsibility at the grass roots

One strategy for driving the necessary cultural change within your business is to adopt Security Champions, who discuss security challenges and deliver security protocols to your workforce at the grass roots level.

Sarah Janes
@SarahkJanes

Managing Director
Layer 8 Ltd

"Champions having conversation to make security more relevant to each employee's working world – coupled with online training materials that can be used to facilitate the changes – is the best method to achieve adoption of secure behaviours."

Summary

Data protection and cyber security can feel like an onerous responsibility. The right tools however will make remote working easy, safe and secure – and they are inexpensive to implement. But be mindful that there must be cultural change within your organisation as well as the right security infrastructure if secure behaviours are to be adopted by your team.

Here's a quick summary.

- Remote working is here to stay and has many benefits – including productivity, staff loyalty and reduced overheads. However, remote working also raises a number of security challenges.
- Data breaches are a serious concern, with the ICO issuing big fines for flouting GDPR.
- BYOD, insecure hardware, software misuse and public WiFi networks are common security threats.
- A successful security infrastructure must enable – not inhibit – efficiency in your workforce. Otherwise staff will cut corners and search for workarounds.
- Research IT manufacturers and vendors choose those with a proven track record.
- Tools such as encrypted SSDs and USBs, VPNs and DLP software are easy to implement and don't have to be expensive.
- Success with data protection and security requires a cultural and behavioural shift within your organisation. Your staff must understand why the rules are there, instead of being instructed to follow the protocols blindly.
- External consultants can help with staff security training – but make sure the materials are suitable and beware that staff will not automatically adoptthe right behaviours just because they have been told to on a training course.
- Adopt Security Champions to discuss security challenges and guide good security behaviours at the grass roots level.

About Kingston

With 32 years of experience, Kingston has the knowledge to identify and resolve your remote working challenges – making it easy for your workforce to work securely from anywhere, without compromising your organisation.

#KingstonIsWithYou