VansonBourne

Cybersecurity in response to COVID-19

COVID-19 has paved the way for financial, behavioural and cultural change – with organisations working from home at scale and evergrowing threats to cybersecurity. What do IT decision makers (ITDMs) think about this change and what needs to be done to mitigate the risks?

In the final quarter of 2020, we conducted a series of in-depth telephone interviews with eight UK ITDMs to gain a detailed understanding of the cybersecurity issues they're facing. We followed that with a wider quantitative study of 300 UK and US ITDMs to explore the topic further – below are the key highlights of what we discovered.

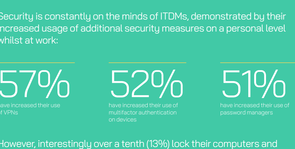
Cybersecurity risks are on the rise thanks to evolving work environments

Over half (52%) of IT decision makers believe that COVID-19 and the rise in home working environments has heightened cyberattack vulnerabilities within their organisation.

> *How can I check that nobody is looking over your shoulder whilst you're working at home?*
>
> ITDM from the healthcare products and tech sector

78% say that a cyberattack within their organisation is a question of when, not if.

Almost half rank malware (49%) and phishing (47%) in the top three attacks they are most worried about:



The foundation to cybersecurity risk starts from within, as 73% of ITDMs report that whilst external threats will always be a concern, internal errors and oversights are the bigger cybersecurity threat.

> *There are threats from outside of the organisation, but we do have potential threats from within too.*
>
> ITDM from the transport sector

Organisations need to rethink their training procedures

Security is constantly on the minds of ITDMs, demonstrated by their increased usage of additional security measures on a personal level whilst at work:

57% have increased their use of VPNs

52% have increased their use of multifactor authentication on devices

51% have increased their use of password managers

However, interestingly over a tenth (13%) lack their computers and devices less so than they did before the pandemic, suggesting a level of complacency as a result of the working environment shift.

> *COVID-19 makes it more lackadaisical because we're at home. You feel more comfortable, you tend not to put in the same protocols you would have if you were in a work environment - because you feel safe in a work environment.*
>
> ITDM from the telecoms sector

The vast majority report that their organisation conducts a range of cybersecurity training formats for employees:

92% computer based cybersecurity training

92% information sharing procedures training

82% corporation training events

80% live lectures training

Benefits to cybersecurity training centre mostly, and expectedly on making organisations more secure (66%) and over half (53%) reporting an increase in staff compliance.

And yet, many also see additional benefits such as long term cost savings (48%), protecting reputation and trust (48%) or improving culture and morale (33%).

> *It's important to make sure that executives are aware of the biggest risks that we face.*
>
> ITDM from the IT services sector

Whilst the widespread utilisation of cybersecurity training is encouraging, there are still improvements to be made and risks in not doing it right.

Over half (51%) believe that most of their organisation's employees consider cybersecurity training a hindrance, and not a help to their day to day jobs.

It is on decision makers to keep up to speed with threats and adapt training regimes accordingly in order to train employees in the most effective way.

> *Cybersecurity professionals like myself need to keep learning new things because it's never going to stay the same.*
>
> ITDM from the IT services sector

The future of cyber looks bright, but there are also evolving risks on the horizon

When it comes to the future of cyber and cybersecurity, a common perspective is that cybercriminals will become more sophisticated in their activities (55%).

But whilst this is the case, 54% of IT decision makers also believe that software and technology will become more advanced.

> *Hackers are getting a lot more sophisticated in terms of the processes that they have, but at the same time the measures that are being put in place to protect organisations are also keeping pace with these changes that are happening.*
>
> ITDM from the transport sector

As it is anticipated that technologies and the smart devices will become more connected (46%), it is essential that security measures are in place to patch up the current and future risks that come with these devices.

Lines are being blurred between what was once very much separated – the home and the workplace. These factors highlight vulnerabilities which are expected to intensify:

> *IoT opens your whole house to people looking at documentation – the way you act, what you do, the people of the household...*
>
> ITDM from the telecoms sector

> *You don't have control over the whole infrastructure that has now moved beyond the office.*
>
> ITDM from the healthcare products and tech sector

Cybersecurity is less about complacency, making assumptions and trusting current systems. It is becoming evermore about interrogating systems in place and how future threats can have an impact.

For more information:
enquiries@vansonbourne.com
vansonbourne.com