VansonBourne

# Cybersecurity
## in response to COVID-19
Snapshot report

## Cybersecurity has been at the forefront of organisations' minds for a while, but it is clear that both the advancements in technology and consequently the growing sophistication of hackers, has meant that cyber risk is becoming evermore prevalent in today's world.

Technology certainly proves to be a double edged sword; on one hand giving us the ability to enhance global connectivity and on the other, trying to keep up with advancements of hackers and their future potential.

Vanson Bourne have conducted both qualitative and quantitive research with IT decision makers to delve into the thoughts and approaches to cybersecurity within organisations. From this, we uncovered that the pandemic has played a pivotal role in growing cybersecurity threats and the worries that come with this.

Mass shifts to home working have exposed organisations to further security risks. Given the majority (78%) of ITDMs are aware of a need to redefine cybersecurity requirements within their organisation due to this shift to remote working at scale, they could be susceptible to attack.

## Cybersecurity risks are on the rise thanks to evolving work environments

Over half (52%) of respondents believe that COVID-19 and the rise in home working environments has heightened cyberattack vulnerabilities, thus increasing demand to mitigate them.

With predominant perceptions of cyberattacks also being a matter of when, not if (76%), it is clear that organisations are having to think about their cybersecurity processes now more than ever.

Almost half of ITDMs rank malware (49%) and phishing (47%) in the top three attacks they are most worried about; phishing is considered a threat due to its growing ability to fit into a genuine corporate environment. Nearly two thirds (64%) have either personally experienced/been impacted by a cyberattack at their place of work or have experienced cybersecurity threats which were intercepted beforehand, proving the extent to which organisations are battling risks every day. When it comes to the consequences of cyberattacks that respondents are most concerned about, these centre on both data losses (62%) and company reputational damage (59%) which would prove a detriment to organisations impacted by these attacks.

> **There's so much going on that your chances of escaping a cyberattack are quite low.**
>
> ITDM from the retail sector

## Organisations need to rethink their training procedures

In terms of what ITDMs do to mitigate cyber security risks, around three fifths (62%) already use firewalls on devices, as well as a VPN (59%). In fact, over half also reset their passwords periodically (55%), use different passwords for different accounts at work (55%) or lock computers/devices when left unattended (55%).

Nearly six in ten (57%) have increased their use of VPNs compared to before COVID-19, which makes sense in the context of the rise in home working environments. The use of multifactor authentication on devices (52%) and password managers (51%) have also increased during the pandemic, whilst using different passwords for different accounts and using firewalls on devices have been behaviours which were predominantly in place before the pandemic.

Interestingly, over a tenth (13%) lock their computers and devices when left unattended less so than they did before the pandemic, suggesting a level of complacency as a result of the working environment shift. It is clear that ITDMs may feel as though this is not as essential when working away from the office. Is this, however, a lax behaviour that should be discouraged within organisations? Perhaps a discussion point that needs covering during training procedures.

The sheer amount of organisations who have experienced some sort of threat and concern centring from the increase of home work environments proves that decision makers need to further develop training processes for their employees. Such training should aim to address and minimise internal errors and oversight, which almost three quarters (73%) see as a bigger cybersecurity threat to their organisation versus external threats.

Most (92%) organisations conduct computer based cybersecurity training, as well as information sharing procedures training (92%) and corporation training events (82%). From this, it is evident that a majority of organisations are conducting cybersecurity training of some sort. However, IT decision makers believe that the effects of cybersecurity training are dependant on both coverage and the attitudes of those who take them, with those who have not directly experienced cyberattacks to treat training as more of a tick box exercise than those who have felt the consequences first-hand.

What better way then, to incorporate live scenario training by replicating a 'real life' cybersecurity threat in the workplace. Four fifths (80%) of organisations are already doing this, with almost two thirds (68%) reaping the benefits. This type of training being conducted mostly in the form of fake phishing emails is a great way to test the eye of employees and flag key things to look for when faced with these scenarios in the workplace.

**57%**

**of ITDMs have increased their use of VPNs compared to before COVID-19**

**52%**

**have increased their use of multifactor authentication**

**51%**

**have increased their use of password managers**

> **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

Organisations have the ability to check whether employees click on falsified suspicious links and monitor how efficiently they report these to the relevant parties within their organisation. Interestingly however, more than a tenth (12%) of those who already utilise this type of training, believe that there are no benefits to this, suggesting there is still in part some progress to be made. On the flip side and more positively, the same amount (12%) who do not currently conduct this type of training within their organisation believe that there would be benefits in doing so, so there is certainly also potential for this type of training, if done right.

In terms of the benefits that come from cybersecurity training, it makes sense that security proves top of mind for organisations, with two thirds (66%) claiming the largest benefit is making their organisation more secure and over half (53%) reporting an increase in staff compliance. Almost half (48%) link cybersecurity training with long term cost savings by minimising cybersecurity risks, as well as protecting their reputation and trust as an organisation – both of which could have detrimental impacts on organisations affected.

51% **believe that most of their employees consider cybersecurity training a hindrance, and not a help to their day to day jobs**

It is clear that whilst the majority of organisations are already conducting training, there are still some improvements to be made.

Over half (51%) believe that most of their employees consider cybersecurity training a hindrance, and not a help to their day to day jobs. Perhaps training that is renewed, current and impactful has more potential to resonate with employees at scale. The impact of this training sits with decision makers and their awareness of current, as well as future, risks.

> **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%). However, whilst this is the case, 54% also believe that software and technology will become more advanced.

It is clear there are both positive and negative associations with the world of cyber and cybersecurity. Over two fifths (45%) believe that the Internet of Things will become increasingly prone to cyber threats, in part due to embedded security risks with these connected devices.

> **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

Ensuring that these devices are secure is vital, particularly in a future where the lines of cyber will be blurred in terms of privacy. Positively, almost half (47%) believe that there will be an increase in endpoint security and whilst a similar number of respondents (46%) also think that technologies and smart devices will become more connected, more robust security measures should help to patch up the risks that come with these devices.

One evident outcome from the pandemic is that cybersecurity awareness is evolving, and the future demand for cybersecurity professionals to increase awareness is evermore growing. Cybersecurity is less about complacency, making assumptions and trusting in devices, employees and their behaviours. Cybersecurity is becoming more about interrogating systems in place and how future threats can have an impact. Over two thirds (69%) of ITDMs agree that the increasing amount and sophistication of cyberattacks means that their focus should be more on nullifying their impact, rather than totally preventing their occurrence – proving further the growing difficulty in preventing cyberattacks themselves and a shift in priorities based on curtailing the impact when they do occur.

## Conclusion

COVID-19 and the growth in home working has allowed many organisations to maintain productivity and continue with business as usual. However, with this comes heightened cybersecurity vulnerabilities and the sad reality now is that organisations seem to expect threats of some sort and at some point during their operations.

In terms of mitigation, organisations seem to have had processes in place before the pandemic, but it's clear that priorities have needed to change, and fast. An increased use of VPNs, password managers and multifactor authentication are all evidence that organisations are also making changes on a individual level as well as at scale. Interestingly, whilst external threats are expected, it's internal complacency that poses bigger issues for organisations, proving a demand for impactful training and communication that resonates with employees.

Training is widely utilised within organisations and proves beneficial for the most part but with the world of cyber constantly changing, organisations will need to keep on top of new and upcoming types of threats and communicate these effectively to build necessary awareness. Practical based training that replicates real life scenarios has potential and is perhaps the path to simulating natural responses from audiences, responses of which can have positive impacts.

The future looks bright for cyber and cybersecurity, with a perceived expectation that security methods will become more advanced and in touch with changing demand. Connected devices and innovative technologies will also pave the way for a new means of life. With more connectivity comes a need to sacrifice a level of digital privacy and organisations must ensure to keep on top of risks to minimise the impacts they face.

# Recommendations

The rise in home working means that organisations have lesser control and visibility over the work landscape and should rethink their current cybersecurity procedures in order to minimise their potential impact. Organisations must get a full view of their now physically disperse infrastructure and conducting further research with individual organisations in mind can do exactly that. It is crucial to understand how exactly to finetune organisational processes in the best way.

The ownership and responsibility for IT security should sit with every employee and as a start, organisations should keep on top of cyber threats and ensure to effectively communicate these with employees through training and other comms where necessary.

Training rolled out to employees should be engaging and resonate in order to shift common perceptions of training being a hindrance rather than a help to their day-to-day roles. It is clear that there is currently a level of complacency and a replica of real life scenario training has the potential to foster necessary awareness amongst employees.

The current threats we face now will evolve in the future, and whilst technologies will become more advanced in dealing with these threats, the core foundation to minimising impacts starts internally and on an employee level.

**Methodology:** Vanson Bourne conducted both qualitative and quantitative research on cybersecurity. The qualitative element was conducted in November 2020 consisting of 8 in-depth interviews with UK IT decision makers from within organisations of 1000+ employees, across a range of sectors. The quantitative study was with 300 IT decision makers, 100 from the UK and 200 from US based organisations with 1000+ employees, across a range of sectors.

All interviews were conducted using a rigorous multi-level screening process to ensure that only suitable candidates were given opportunity to participate.

VansonBourne

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