

COVID-19: Cyber risk exposure calculator

COVID-19 has forced many workforces to work remotely. For many businesses, this shift would normally require long-term IT transformation efforts. But this has not been possible due to the pandemic's speed.

While many businesses are reconfiguring networks and systems to serve the needs of remote workforces, the transformation's success is often limited by less-than-optimal technology capabilities. Businesses IT infrastructure may be stressed by significantly increased demand, while cyber-threat actors actively seek to exploit weaknesses in newly implemented or temporary IT infrastructures.

Whatever the size of your business, you probably depend on electronic systems to help run it. It might be selling online, using office applications or email. In some cases, your whole business might be IT systems driven. When cyber-attacks occur, they can result in devastating damage, such as business disruptions, revenue loss, legal fees and a permanently tainted reputation.

Due to the impact of COVID-19 and the way businesses have rapidly adapted, you could be leaving your business exposed. Use our calculator to find out your businesses cyber exposure risk:

Instructions

Answer the statements below and give each response a numerical value depending on the answer:

- **Yes:** 0 points
- **No:** 5 points
- **Unsure:** 5 points

After completing all of the questions, total your score to determine your businesses level of cyber risk

- **Low risk:** 0-10
- **Moderate risk:** 15-25
- **High risk:** 30-50
- **Escalated risk:** 55-100

Exposure	Yes	No	Unsure	Score
1. Do you have a training programme for employees regarding data privacy and security?				
2. Are all employees working from home using company-owned devices? (EG: Not using any personal devices - Laptops, smartphones, iPad's)				
3. Is access to sensitive information limited to those employees that need it for their job?				
4. Is personal or sensitive data encrypted when at rest on your servers?				

Exposure	Yes	No	Unsure	Score
5. Do you have a formal password policy that explains good password hygiene for all systems used by employees?				
6. Do you use multi-factor authentication (MFA) for remote or working from home access?				
7. Do you use a virtual private network (VPN) connection?				
8. Have all employees been trained on how to spot phishing emails?				
9. Do you share any data with any third parties?				
10. Do you have a policy to ensure access is immediately revoked or amended for joiners, movers and leavers?				
11. Do you know the top cyber security concern that faces your business today?				
12. Are full system backups taken at least weekly and stored either off site or disconnected from your network?				
13. Is network security training for employees compulsory?				
14. Can employees update their computers or company-issued devices passwords regularly whilst working from home?				
15. Does your business or IT department update all systems including firewalls and anti-virus software at least every 30 days?				
16. Is there an individual in your business with assigned responsibility for information security?				
17. Do you outsource any of your information processing or operational systems?				
18. Does your business have a disaster and recovery plan in place?				
19. Has your business updated its processes and procedures to include processes for employees now working from home?				
20. Has your business reviewed its data security or cyber security policies and procedures in the last year?				
Total				

Companies cannot ignore the cyber challenges associated with a largely or entirely remote workforce. In the long term, changes made in response to the pandemic should be viewed through a resiliency lens, with an eye to building more flexible and secure business operations.

Get in touch with our expert cyber team to see how they can support you and your business through COVID-19 and beyond.

This is a marketing communication.

Marsh Commercial is a trading name of Jelf Insurance Brokers Ltd, which is authorised and regulated by the Financial Conduct Authority (FCA). Not all products and services offered are regulated by the FCA (for details see marshcommercial.co.uk/info/regulation). Registered in England and Wales number 0837227. Registered Office: 1 Tower Place West, London EC3R 5BU. FP.20.217