



Digital shift has broadened the cyber-attack surface

December 1, 2020

Whilst managing crisis it is essential to keep sight of the risks on the horizon in order to build resilience. With this in mind, the COVID-19 pandemic has taught us all many lessons.

Falling consumer demand is only one trend contributing to the 'new normal' created by the COVID-19 crisis - companies need to be aware of the growth of e-commerce and remote contact with consumers; increased cost of raw materials and services; and home working. All of these trends are likely to influence customer base and business operations - for worse or in some cases for better

This site uses cookies. [Read our policy here...](#)

risk transfer accordingly. Where operating models have changed, so in turn will risk profiles and appetites.

In this article we take a look at cyber threats, one of the 5 big risks that can affect all businesses (Pandemic, Brexit, Climate Change, Flooding and Cyber), that we've covered in our latest [Resilience eBook](#).

The digital shift

The digital shift undertaken by both companies and consumers during lockdown has broadened the cyber-attack surface.

During lockdown, many companies redeployed staff to home working with little to no change to cyber security policies; in fact, best practices were harder to enforce in this environment. Poor IT systems and inadequate security led to significant vulnerabilities.

Couple this with increased remote contact with customers, suppliers, and stakeholders, and you opportunity presented to cyber criminals is vastly increased.

As such, attacks are increasing in both volume and sophistication.

There has been a significant increase in social engineering attacks during the pandemic, which is where individuals are manipulated into performing actions or divulging information. Both fake news in the form of COVID-19 updates and malicious emails are being used in these phishing schemes.

Hackers are using growing fears to capitalise on those seeking up to date information and guidance, leading to a growth in malicious online activity.

The following has been seen:

- Emails claiming to be from the World Health Organisation (WHO) - asking users to click on links and provide login credentials.

- Malware campaigns purporting to provide Coronavirus updates - asking for people to open files and click on links.

- Increased remote working providing gateways to hackers.

Weak passwords that are changed infrequently.

Cyber security

Companies have accepted that cyber-attacks are an inevitability, with more than 1 in 5 experiencing a breach of some sort in a 12 month period.

But Hiscox outlines that globally nearly four out of five small companies (those with one to nine employees) are “cyber novices”, with nearly half having no defined cyber security role.

According to the latest UK Government figures eight out of ten UK companies say cyber security is a high priority for senior management.

While this is an essential investment, it needs to be supported by cyber-resilient processes and practices. Two areas in particular will require additional attention due to the current climate created by the COVID-19 crisis: a resilience culture, and insurance provision.

If you found this interesting and would like to know more about the key risks on the horizon, [download our 2020 Resilience eBook](#). Our eBook explains how these risks have been impacted by COVID-19 crisis and we help you to understand how you make your business more resilient in a challenging market.

Tags

- COVID-19
- Data and Cyber Risks
- cyber security
- Commercial Insurance
- brexit

Building resilience

Keeping sight of key risks on the horizon, and understanding how these risks have been impacted by COVID-19 crisis, is key for building your businesses’ resilience. Discover more in our latest Resilience eBook.



Read our latest articles

Seven cyber risks facing the transport and logistics industry

April 27, 2021

Here are some of the most prominent cyber risks facing the transport and logistics industry today.

[View](#)

Top five supply chain management tips for Manufacturers

April 23, 2021

Top five tips for helping to manage and mitigate the most likely causes of manufacturers'

[This site uses cookies. Read our policy here...](#)

Say hello to helpful.

Sign up to our newsletter for updates to your inbox.

<input type="text" value="Email address"/>	<input type="submit" value="Submit"/>
--	---------------------------------------

What are you looking for?

[Articles & events](#)

[Private Clients](#)

[Local offices](#)

[Regulatory](#)

[Cookies](#)

[Making a complaint](#)

[Modern Slavery Statement](#)

[Commercial Clients](#)

[Claims](#)

[About](#)

[Terms of use](#)

[Privacy Policy](#)

[Transparency](#)

[Insurance Distribution Directive](#)

