Strategic Themes

Strategising Mental Health: COVID-19's silver lining?

Vaccines: pathway to immunity littered with obstacles

All Change: Transport & Commuting

Preparedness: COVID-19 and pandemic modelling

WTC: The Future of Work

Cyber

London Work, Travel & Convene Coalition

Preparing for Future Systemic Cyber Risk

Overview Online report Download Report

Data points:

58%

58% of cyber attacks target SMEs (World Economic Forum)

336%

Cyber insurers reported a 336% jump in claims from the start of 2019 through to 2020. (Source: Aon's 2021 Cyber Risk Report)

486%

Ransomware was up 486% from Q3 2018 to Q4 2020 (source: Coverware Ransomware Report)

1/2

Only two in five organisations report they are prepared to navigate new exposures arising from rapid digital evolution (Source: Aon's 2021 Cyber Risk Report)

21%

21% of organisations report having baseline measures to oversee critical suppliers and vendors (Source: Aon's 2021 Cyber Risk Report)

"The whole landscape changed, and effectively we have considered the pandemic a 'zero-day' exploit globally. The biggest shift has been that threat-based approaches are no longer sufficient. We have to take a risk-based approach – non-traditional in today's cybersecurity industry — particularly because the increasingly connected landscape demands it."

Dr Jacqui Taylor, CEO of FlyingBinary, and Strategic Advisor to the UK Government

The COVID-19 catalyst

"Step aside CTO, CIO, and CFO. COVID-19 joined the C-suite in 2020, leading change as companies were forced to rapidly set up remote work environments and enable digital customer experiences. Any thought of a paced and strategic digital agenda was tossed aside in favour of survival. Perhaps your company rapidly transitioned to the cloud. Under time and cost pressures, you execute a 'lift and shift' approach, quickly moving existing architecture to a new cloud environment.

"You may now believe that this strategy, necessary as it was, brought considerable security disadvantages and perhaps offset the many benefits of the cloud. Or, your organisation weathered the pandemic, but the board is now calling for more innovation; maybe urging deployment of artificial intelligence (AI) to inform smarter decisions. Change seems constant, and it is."

Aon's 2021 Cyber Risk Report: Balancing Risk and Opportunity Through Better Decisions

It has been well over a year since the World Health Organisation declared COVID-19 a global pandemic. In March 2020, as we left the office, none of us knew that we would not be returning in any major capacity until at least mid-2021. Organisations were thrust into a state of emergency; working from home was the only option to keep the lights on – leaving many with little choice but prioritise digital change over everything else, including security.

While the world struggled against COVID-19's stranglehold, one sector was primed to captialise on the opportunity the pandemic posed. Cybercrime's exploitation of this rapid shift in the digital landscape can be evidenced by the sharp uptick in the volume and severity of cyberattacks, including ransomware incidents, coupled with supply chain and support vendor vulnerabilities. The current environment poses a real risk to the mid-market: "58% of the attacks that happen in terms of numbers actually target our SMEs, so they are a key risk. They're the engines of our future digital economies," Dr Jacqui Taylor says.

She continues, "The pandemic effectively brought an additional billion people online; the whole work-from-home movement meant that the one set of people who were prepared were the criminals. Across all of our digital economy, we had to handle that."

Preparedness has been an ongoing theme for the London Work, Travel, Convene Coalition, and organisations have shared their experiences of how they coped in the COVID-19 early days. Aon Programme and Change Manager Ted Winterbottom says, "Were we prepared for disaster recovery? Yes, we were very well prepared. Some protocols had been tested to a degree. In terms of working from home, the technology supported us well. We had been encouraging people to work agilely within parameters. However, no one anticipated a business continuity event as dramatic as it was."

With the global vaccination rollout now well underway, we must now prepare for a new phase of recovery. As organisations embark upon their Smart Working journey and return to the office in some capacity, many remain ill-prepared for the financial impact of a cyberattack, including crisis, defence, liability and regulatory expenses, and business interruption loss.

Nevertheless, the majority of the cyber threats organisations face are not new — connected devices, ransomware, and insider risk will be ever-present. But what is new is that COVID-19 has systemically altered how we conduct our businesses, and the zero-day event (that was the pandemic) has moved the level of risk forward exponentially.

Top 5 Cyber Risks

Aon's London Work, Travel, Convene Coalition talked to cyber experts to identify the top five risks that COVID-19 and Cyber present in 2021.

Sadie Creese
— Professor of Cyber Security in the Department of Computer Science at the University of Oxford

Dr Jacqui Taylor
– globally recognised as a Smart City Tzar, CEO of FlyingBinary, and Strategic Advisor to the UK Government

Eric Friedberg
— Co-President of Stroz Friedberg, LLC and Aon's Cyber Solutions

Geoff White
— Investigative Journalist, Author of 'Crime Dot Com' and creator of 'The Lazarus Heist' podcast at BBC

Top talent issues

1. Cybercrime as a Service
2. Known Vulnerabilities
3. Interdependencies
4. Agile Working
5. Insider Risk

Download the full report

London Work, Travel, Convene Coalition
Preparing for Future Systemic Cyber Risk
Aon

The Office Reimagined:
Smart Working towards a Resilient Future

Download PDF (3,456kb)

Next

Preparedness: COVID-19 and pandemic modelling