European Commercial – August 2020

European Cybersecurity

Cyber investment to create new European office demand

Cyber-attacks : an introduction

The number of cyber-attacks has risen by 67% over the last five years, and the average cost of a cybercrime for a corporation has increased by 12% to $13 million (€11.6 million) in 2019, according to Accenture. Since GDPR was introduced in 2018, a number of multi-million euro fines have been imposed for breaches of personal data.

Covid-19 and cyber-attacks

Since lockdown, the European Union Agency for Cybersecurity (ENISA) has reported that an increased number of cyber-attacks are targeting ecommerce and online payment businesses, as well as the healthcare sector. In March 2020, the World Health Organisation (WHO) fell victim to "a sophisticated cyber-attack" and in May, a large European airline announced that nine million customers' details were revealed.

One of the concerns for employers during lockdown has been workers' rising use of personal electronic devices to access company data. Trustedsec report that cyber-attacks have increased by circa 500% during the course of lockdown, with a marked rise in those targeted at employees working from home. This stems from the fact that approximately one third of employees' bring-your-own-devices (BYOD) do not meet existing company cybersecurity guidance.

Savills Office FiT indicates that the proportion of homeworking will increase post COVID-19. Prior to lockdown, 32% of office workers reported that they worked remotely either one or two days per week, and once lockdown is lifted, 55% expect to work remotely one or two days per week as working practice becomes more agile. Companies will ultimately need to invest further in cybersecurity software to accommodate the growth of agile working and to avoid data breaches and fines from regulatory authorities.

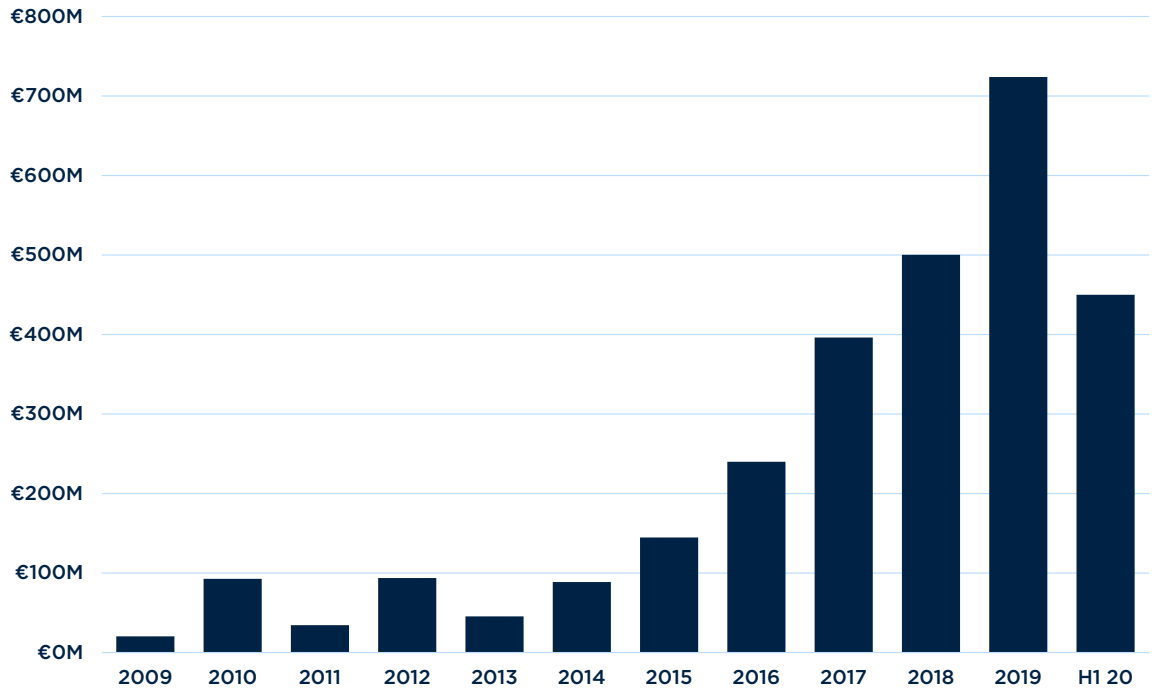
New funding to cybersecurity and office demand

Savills Research track corporate investment activity into the cybersecurity sector as a lead indicator of latent occupational demand within the sector. A growing number of European cyber-attacks has attracted €2.3bn of venture capital (VC) investment into European headquartered cybersecurity companies during the last five years, with a record level of €724m recorded in 2019. The UK accounted for €1.3bn of the five year total, although we are observing an increasing flow of capital into companies based in mainland Europe, led by France (€316m), Switzerland (€303m), Ireland (€70m), Germany (€68m) and Spain (€36m).

As well as corporate investment, increased public funding is targeting cybersecurity, as governments recognise the elevated need for data security. The European Commission adopted a new cybersecurity strategy in May 2020, allocating €49 million to boost EU cybersecurity innovation, encouraging the emergence of SMEs. Similarly, in June 2020, the UK Government announced £10 million (€11.1 million) of funding over the next four years to improve UK businesses' resilience to cyber-attacks and committed funding to the Cyber39, a cybersecurity accelerator in London's Canary Wharf, for startups to showcase new products to businesses.

Although many of the leading cyber companies' global headquarters are clustered in Silicon Valley, California, many US companies maintain a large European footprint- Palo Alto Networks, for example, currently occupies eight floors in Amsterdam's Oval Tower. Many of the larger European cybersecurity companies are London headquartered, although with regional offices across Europe. For

Chart 1: Venture capital investment to European headquartered cybersecurity companies €



Source Savills Research, company database

> **Increased cyber-attacks, GDPR regulation and increased home-working during lockdown are driving corporate investment into cybersecurity and creating new demand for office space across Europe.**

€1.3bn
of venture capital funding has been raised in the UK since 2016, with office leases signed by Mimecast, NCC Group, Darktrace and Intellicentrics.

€2.3bn
of venture capital investment into European cybersecurity companies over the last five years.

example, Mimecast opened their 79,000 sq ft (7,339 sq m) headquarters at One Finsbury Avenue, London during 2019, although satellite offices in Amsterdam and Munich service the local European regional markets. Darktrace also signed for 20,000 sq ft (1,858 sq m) in the Maurice Wilkes Building, Cambridge for their new HQ, which opened in 2018. As such, development plans for a Cyber Central UK, located next door to GCHQ, Cheltenham now indicate the realisation of a need for a dedicated park.

Securing cyber talent

Universities play a significant role in developing talent and influencing corporate occupier expansion across Europe. Avast signed for 15,000 sq m as their global headquarters in Prague after the acquisition of AVG in 2016, who later filed for an IPO in 2018. Accenture also work closely with universities around innovation and opened their Cyber Fusion Center in Prague to help customers protect themselves against cyber-attacks.

NCC Group signed for 60,000 sq ft (5,574 sq m) in The XYZ Building, Manchester following a number of corporate acquisitions and have formed a partnership with the University of Surrey to advance cybersecurity research in the space industry.

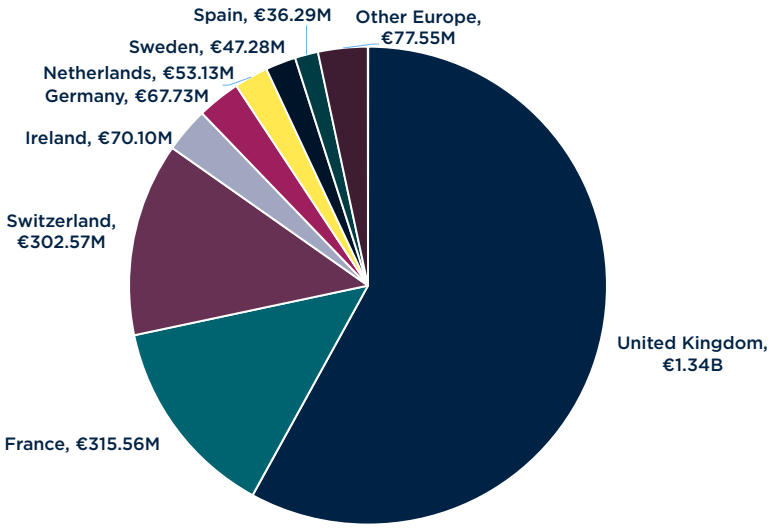
More industry networking events are driving demand across Europe. Spain is host to ENISE, an annual international conference on cybersecurity and has subsequently recorded office leasing deals from Sothis, Vector and GMV in Madrid over the past 12 months.

Outlook- what next for the cybersecurity sector?

A more agile working strategy post-COVID-19 will create new office demand for cyber services as companies mitigate risks of cyber-attacks. Following €724m of venture capital investment into European cybersecurity businesses in 2019, we anticipate further office demand targetting mainland Europe. We expect occupiers to expand in cities which attract higher levels of corporate funding including within the UK, France and Switzerland. Government funding targeting universities and startups will develop cyber talent and create business environments.

Increased data usage will require additional storage, creating new occupational demand for datacentres. Given that datacentres contain a company's business-critical data, having both the facility and equipment secured against breaches is essential.

Chart 2: VC investment to European headquartered cyber companies €, last five years



Source Savills Research

Savills team

Please contact us for further information

Jeremy Bates
EMEA Head of Occupational Markets
+44 (0) 207 409 8813
jbates@savills.com

Mike Barnes
European Research
+44 (0) 207 075 2864
mike.barnes@savills.com