

CYBERSECURITY TRENDS TO LOOK OUT FOR IN 2021

Presented to you by osDORO



OFFICE RENTAL MARKET IS EXPECTED TO INCREASE BY

10 TO 12%

This is due to the growing demand from Chinese tech giants as well as technology and media companies.

CONCERNING INCREASE IN SPEAR PHISHING ATTACKS DUE TO AUTOMATION

There are multiple tools available that automate elements of spear phishing allowing attackers to send more emails, thus increasing their success rate.

47%

OF IT EXECUTIVES SAY CYBERATTACKS HAVE INCREASED SINCE THE BEGINNING OF COVID-19

Businesses have begun automating business and IT processes by using tools such as AI and machine learning. 36% experienced an increase in security vulnerabilities. This is due to remote work as employees are taking cybersecurity timesaving methods for convenience such as using unsecured channels (personal email addresses, instant messaging applications and cloud-based document processes) and unsecure personal devices.

ENTERPRISE CYBERSECURITY SPENDING WILL GROW IN FOUR CORE INDUSTRIES

These industries include technology and media telecommunications, banking and financial, healthcare systems and services, and the public and social sectors.

HOWEVER, DEFENSIVE SECURITY FOCUSING ON DETECTING CYBER THREATS WILL BE AVAILABLE.

Due to innovation, in 2021 there will be an increase in use of Cloud SIEM (Security Information and Event Management), supported by machine learning-powered SIEM tools such as Azure Sentinel, which exposes attacks before they are able to access sensitive data. SOAR (Security Orchestration, Automation and Response) software programs allow companies to collect data about security threats and UEBA (User and Event Behaviour Analytics), which uses machine learning to collect data from users in corporate networks and detect any use of any cyber attacks or malicious behaviours.