Understanding the potential fall-out from the ongoing Microsoft Exchange attacks

Using CyberCube data to highlight industries and regions that are most at risk

CyberCube

www.cybcube.com

CyberCube has analyzed over 20 million companies within our Enterprise Intelligence Layer (EIL) to create heat maps highlighting the industries and geographies most at risk of exploitation in the ongoing cyber attacks targeting Microsoft Exchange servers around the world.

Attackers are actively exploiting four Microsoft Exchange server zero-day vulnerabilities in an attack chain known as ProxyLogon, to steal the contents of a target's emails, harvest credentials, and deploy web shells to gain access to target networks undetected and at will. Up to tens of thousands of Microsoft Exchange servers could have been infected with the malicious ChinaChopper web shell as part of this attack. Companies that have been infected with a web shell will have to forensically investigate their networks to ensure that attackers can not re-enter and wreak havoc, even after patching. (Re)insurers could be on the hook for third-party breach investigation and incident response claims from thousands of companies as they investigate for indicators of compromise and the presence of web shells.

The (re)insurance community is likely to see a long-tail of attritional claims resulting from this attack. We will see attackers sell backdoor access to enterprise networks that were originally compromised through a vulnerable Microsoft Exchange server. At the same time, there will be a relatively small (but not insignificant) number of unpatched Microsoft Exchange servers for the foreseeable future. Patching is not always as simple as pushing an update button. Nefarious actors will continue to seek out and exploit Microsoft Exchange servers if they are unpatched.

Large-scale cyber events that create risk aggregation issues for (re)insurers are becoming more familiar. From WannaCry and NotPetya in 2017, to SolarWinds in 2020, and now Microsoft Exchange in 2021, the potential for a single cyber attack to cause widespread and catastrophic damage is now undeniable.

The impact of the attack is still unfolding

The insurance industry is only beginning to understand the scope of possible damage. According to researchers at ESET, up to 10 different advanced persistent threat (APT) actors are now actively exploiting the web shells used in this attack in a variety of nefarious ways. The number of threat actors exploiting the web shells is likely to increase with others' successes.

Researchers from TrustedSec have observed attackers leveraging web shells on MS Exchange servers to install cryptocurrency mining malware. Microsoft has confirmed that ransomware known as DearCry is currently being installed in human-operated attacks on Microsoft Exchange servers. Researchers from MalwareTech caught a threat actor compromising a decoy Microsoft Exchange server to deploy what is known as Black Kingdom ransomware. One of the largest ransomware demands ever publicly disclosed is already being tied to a vulnerable Microsoft Exchange server at a multi-billion dollar computing company in Thailand.

The scope of this attack is still largely being determined by threat actors and their motivations. Microsoft and CISA have fought back with automated scanning tools that can help patch and detect indicators of compromise associated with this attack. These efforts are proving to be successful at reducing the number of unpatched Microsoft

Exchange servers. However, (re)insurers and their customers will be prudent to keep their guard up.

Insurance industry stakeholders can use the heat maps in this report to help prioritize your attention and to check your own footprint analysis against CyberCube's EIL.

Concierge service

The information in this report is a sampling of work that was originally delivered exclusively to CyberCube's customers as part of our Concierge cyber intelligence service. Through Concierge we offer access to emergency response briefings following cyber events, detailed attack-footprint analysis, and more.

Microsoft Exchange attack footprint takeaways for (re)insurers:

1. Large and medium insureds are vulnerable

Large and medium-sized insureds ($250 million-plus revenue) are more likely to be impacted by this attack than small or micro-sized insureds. These companies tended to have started hosting on-premises Microsoft Exchange servers before enterprise cloud computing became widely accepted.

2. Legacy infrastructure is a proxy for cyber risk

Insureds that rely on legacy infrastructure (using 2010, 2013, or 2016 versions of MS Exchange) in all markets are at risk. Underwriters should pay particular attention to organizations that operate on thin margins and have smaller budgets for IT resources and updates, newer versions and software patches.

3. Entire industries are impacted

Insureds operating in education, healthcare, and the public sector are at greater risk than insureds in other industries. These industries displayed the highest concentration of on-premises Microsoft Exchange servers globally, which means that attackers have more opportunities to compromise insureds that are operating in these industries.

4. Companies operating in North America are at greater risk than those in Europe

Large, medium, and small insureds in North America, are more at risk than their counterparts in Europe. Microsoft Exchange dependencies in CyberCube's EIL appear more frequently in North America than in Europe, with a high concentration in the US. A stand-out feature is that insureds operating in Germany are also particularly at risk given the number of dependencies.

5. Public sector insureds are at high risk

Underwriters should particularly focus on small and medium-sized public sector insureds running Microsoft Exchange servers in North America. They may be operating on thin margins (especially during COVID-19) and may lack resources to patch and scan for indicators of compromise in line with best practices.

6. Global connectivity affects us all

Insureds across the world are at risk. Our data takes a global look at tech dependencies in Africa, Australasia, and the Middle East. CyberCube has observed a relatively high share of Microsoft Exchange servers connected to the Internet in those regions as compared to the world.

What we know so far

A Chinese state-sponsored threat actor known as Hafnium (and others) are actively exploiting four zero-day vulnerabilities in Microsoft's Exchange servers' Outlook Web Access software.

On March 2, Microsoft released security patches for the four vulnerabilities across Exchange Server versions 2010, 2013 – 2019. Once security patches were issued the attackers ramped up their operations to take advantage of as many organizations as possible, by scanning the Internet to target unpatched Exchange Servers. The attackers indiscriminately compromised hundreds of thousands of organizations worldwide over a period of days using automated vulnerability-exploiting scripts, and exfiltrated sensitive email communications from a targeted number of organizations.

> **attackers indiscriminately compromised hundreds of thousands of organizations worldwide over a period of days**

The Chinese government is known for purposefully countering attempts at attribution. The attackers left clues when they attempted to maximize their exploits and hack as many systems as possible once they were discovered. This suggests the attack may be the work of a rogue threat actor or a change in strategy. It could also be a tactic to hide the attackers' digital tracks.

Overview

- Technical Detail: Exploit of four zero-day vulnerabilities in Microsoft Exchange server
- Incident Summary: 100k+ servers backdoored worldwide (60k+ in US)
- Revealed: March 2, 2021 (initial attack activity discovered January 3rd)
- Countries affected: Global

Who has been affected and how?

While the scope of the attack appears to be worldwide, sources have told cybersecurity reporter Brian Krebs that approximately 30,000 organizations in the US have been hacked so far. Bloomberg estimates put this figure at closer to 60,000, as of March 8.

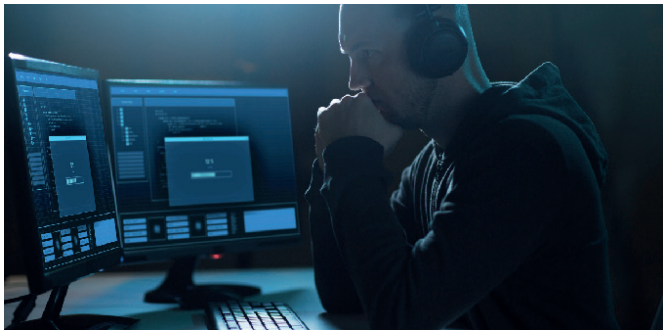
Regions around the world that exhibit the highest share of Microsoft Exchange dependencies include: Africa, Australasia, and the Middle East, followed by North America, and Europe, respectively.

Within Europe, German and Turkish insureds are more likely to be running vulnerable Microsoft Exchange servers compared to other countries in Europe. Within North America, US-based insureds are at risk. Top industries impacted across regions include education, healthcare and the public sector.

Individual entities impacted are widespread and range from national banking institutions to small or medium-sized businesses. Organizations that are running an on-premise Microsoft Exchange Server tend to be large and medium-size and are likely to have been in business for longer than there has been the option to use cloud computing for the provision of email and collaborative services.

Espionage vs. destruction

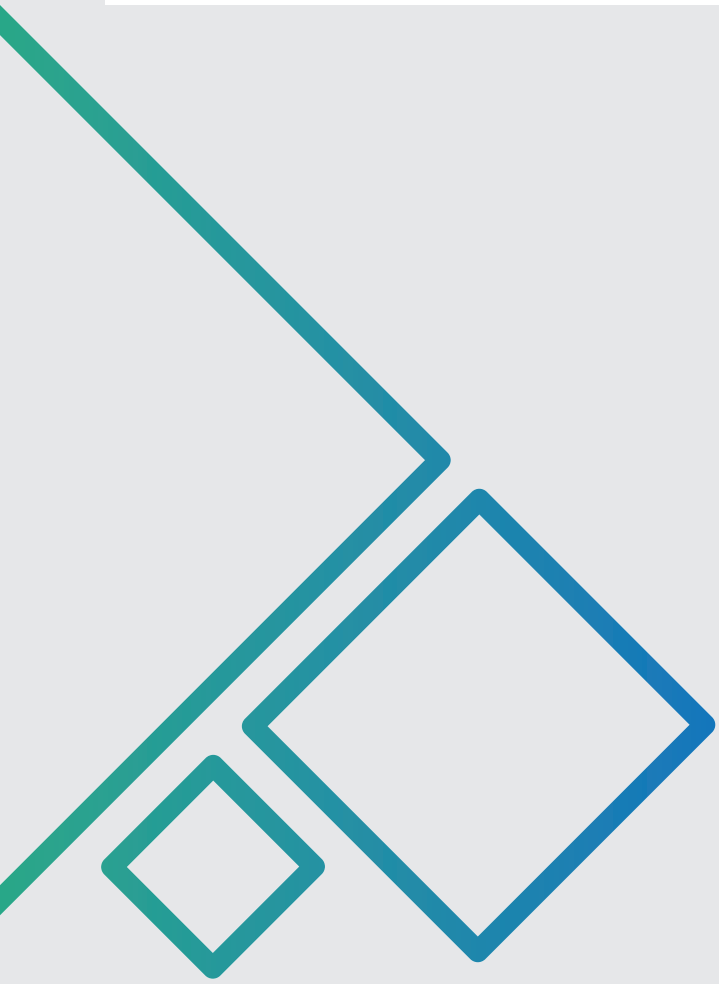
The initial attack campaign appears to have been motivated by espionage, with attackers focussed on casting a wide net before filtering targets to spy on and to steal data from. However, the widespread presence of the attacker's web shell and the continued existence of unpatched servers means destruction such as ransomware or wiper malware is still within reach.



The associated insurance claims are likely to be focused on legal, forensic, and clean-up costs. Installing the patches Microsoft issued will do nothing to clean

servers that have already been infected with the web shell. The web shell and any other malicious software that has been installed will persist until it is removed. This will lead to investigation costs and the need to potentially replace servers (or switch to the cloud) at a cost.

The types of data breaches that may result could encompass any sensitive information in an email, with consequences for personally identifiable information (PII), as well as intellectual property (IP). CyberCube expects claims from this incident to have a "long-tail". It is too early to calculate potential losses from the theft of a corporation's IP. These kinds of data breaches could have delayed, but long-lasting impacts on commercial competitiveness.



"An accumulation of loss could result in multiple (theoretically, tens of thousands) companies making insurance claims

An accumulation of loss could result in multiple (theoretically, tens of thousands) companies making insurance claims to cover investigation, legal, business interruption (through system maintenance) and possible regulatory fines (breach of PII). As noted above, there is still the ongoing possibility that even more attackers will launch ransomware or other types of destructive cyber attacks.

CyberCube's analysis

CyberCube has conducted analysis of the event and identified industries and geographies that are at greatest risk based on data from our EIL, which contains information on 746,000 on-premises MS Exchange server dependencies globally.

Defense in depth

Only Microsoft Exchange versions 2013 – 2019 are considered vulnerable to the four zero-day vulnerabilities associated with this ongoing attack. However, Microsoft is issuing patches for older versions of MS Exchange such as 2010, and has publicly stated that a "defence-in-depth" approach to cyber security necessitates inspecting all versions of MS Exchange.

Our analysis casts the widest net possible and includes all versions of on-premises MS Exchange servers. We also identified cloud-based versions of Microsoft Exchange in our EIL, although those dependencies are excluded from this analysis.

Insured sizes: (total annual revenue, $ USD)

- Large: $1 billion +
- Medium: $250 million – $1 billion
- Small: $10 million - $250 million
- Micro: $0 - $10 million

Reading the heat maps

The heat maps in this report are calculated by determining the number of entities using on-premises MS Exchange servers compared to the overall number of entities in the CyberCube EIL. Darker squares in each heat map represent a higher share of entities using on-premises MS Exchange servers, which means attackers have more opportunities to compromise insureds in those sectors.

As demonstrated in **Exhibit 1**, large and medium-sized insureds are more at risk compared to small and micro insureds. In particular, insurers should focus on advising their large insured clients in the Middle East, Africa, and Australasia.

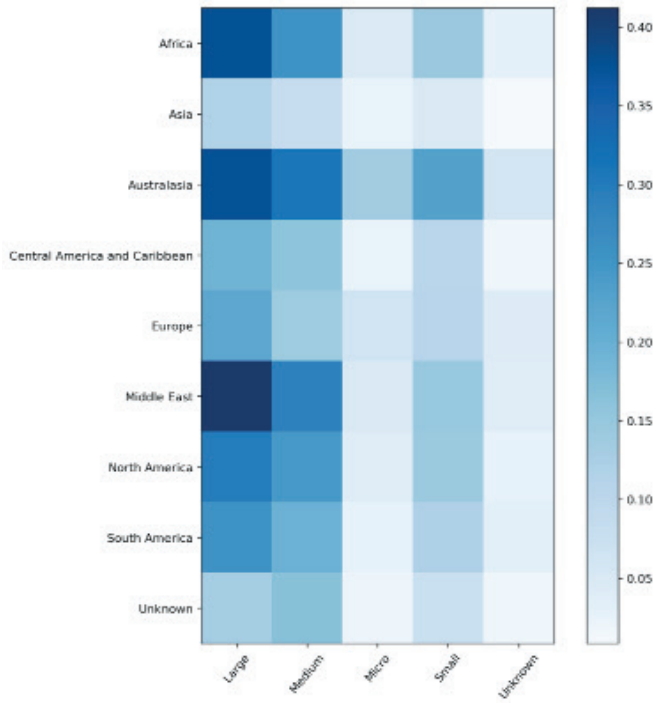


Exhibit 1: Region/Size heatmap

Meanwhile, large, medium, and small insureds in North America are at greater risk than their counterparts in Europe.

Insureds operating in the education, healthcare, and public sectors face greater risks than other industries (see **Exhibit 2**). Insureds operating in the education industry in Africa and Australasia are the most at risk, while those in aviation and banking are particularly vulnerable in the Middle East. Public sector entities are at risk in all regions, particularly in Africa, Australasia, and North America.

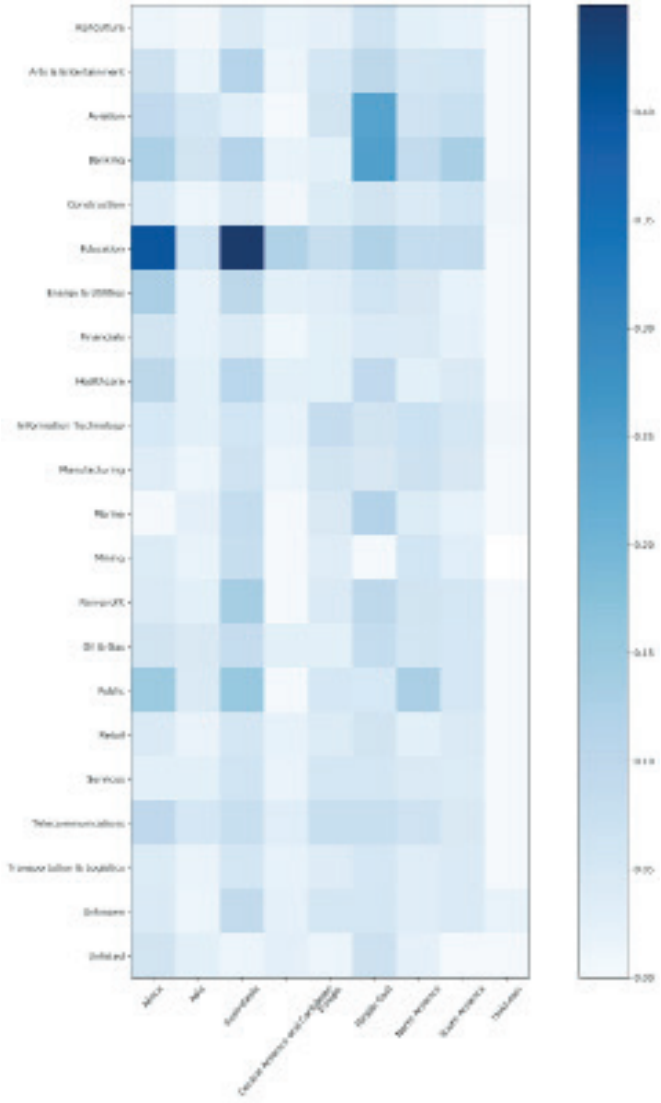


Exhibit 2: Industry/Region heatmap

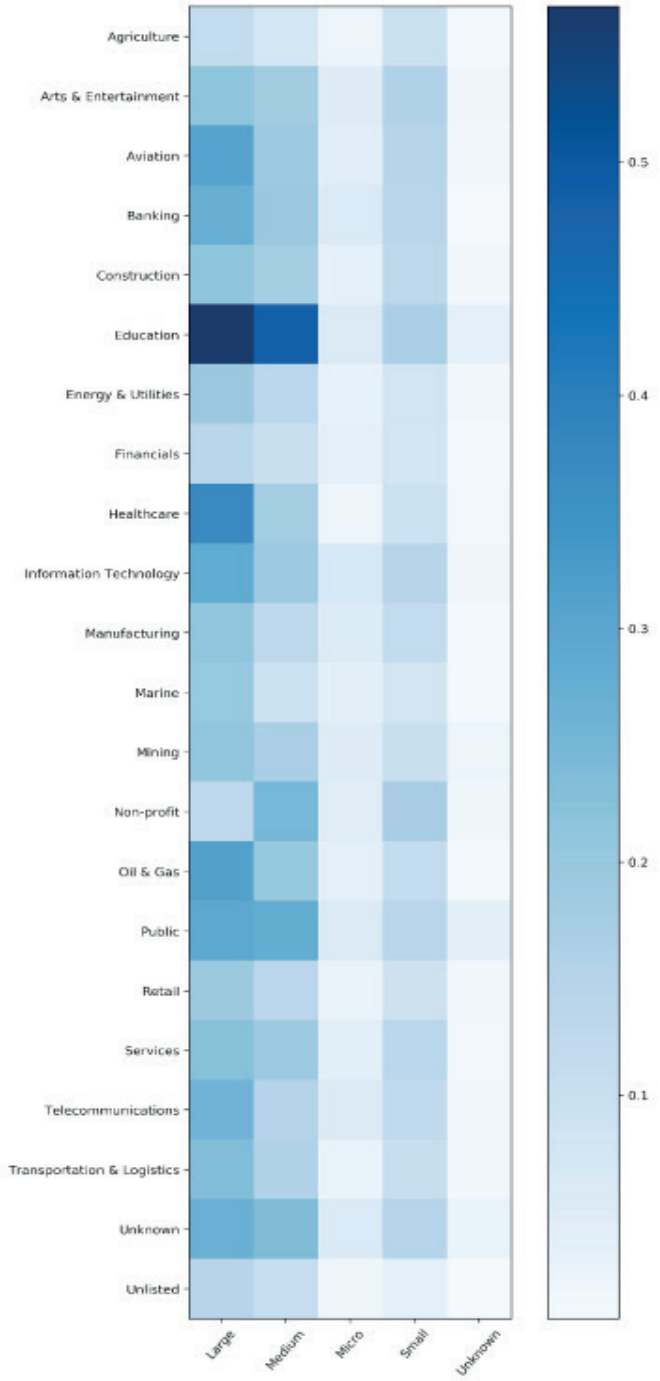


Exhibit 3: Industry/Size heatmap

Large and medium-sized insureds in the education industry are at risk (see **Exhibit 3**). Cyber risk practitioners may wish to prioritize attention for insureds operating in education, healthcare, the public sector, and telecommunications. Large insureds in aviation, banking, Information Technology, as well as oil and gas also face a number of exposures. Other priorities for cyber (re) insurers should include medium and small-size non-profit organizations as well as non-governmental organizations and think tanks.

Conclusion

Cyber attacks on SPOF can impact all of us

While roughly 80% of Microsoft Exchange customers are located in the US, CyberCube's analysis has also identified potential targets in seven additional countries. These are: Canada, Mexico, Belgium, Spain, the UK, Israel and the UAE.

The attack further underscores the need for international policy to help guide nation states towards acceptable behavior in cyberspace. Indiscriminate and automated targeting of single point of failure (SPOF) technologies ought to be branded as one of the worst offenses in cyberspace. A key lesson from the Microsoft Exchange attack is that the attacks that will surely follow it are increasingly likely to impact all of us.

(Re)insurers can prepare for tomorrow's biggest cyber attacks by integrating SPOF intelligence - such as where insureds are running Microsoft Exchange servers - into their underwriting and portfolio management workflows.

CyberCube has focused on SPOF, creating a database that can help (re) insurers develop an edge in cyber underwriting and portfolio management by obtaining insights on SPOF and their connectivity with risks in a portfolio. (Re)insurers can create new insurance products that have terms and conditions tied to SPOF, inform underwriting strategies by optimizing exposure to SPOF based on risk appetite, and quickly understand potential exposure and claims arising from catastrophic SPOF incidents such as the ongoing Microsoft Exchange attacks.

Authors

William Altman, Cyber Security Consultant

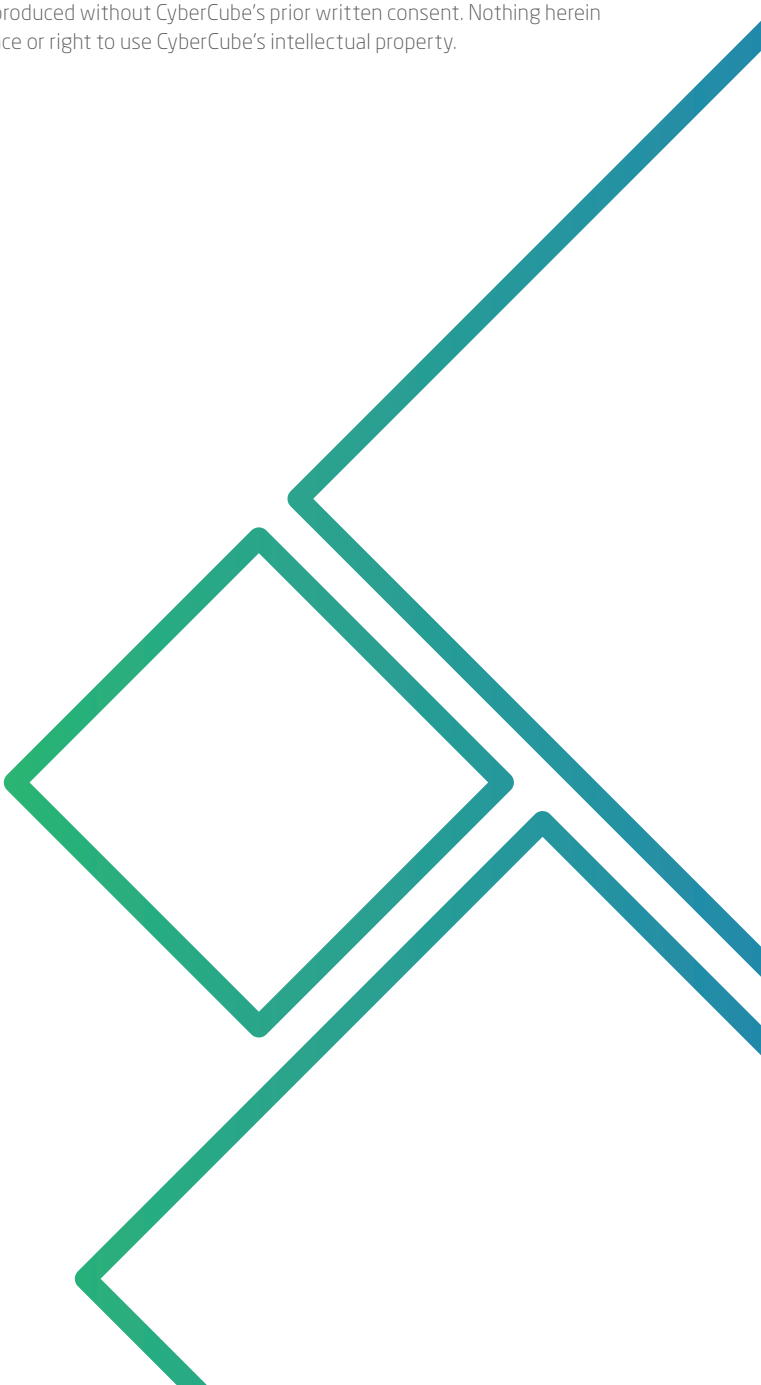
Darren Thomson, Head of Cyber Security Strategy

Data & Analytics

Mohammad Al Boni, Lead Data Scientist

Editorial Content

Yvette Essen, Head of Research & Communications



CyberCube

www.cybcube.com