The murky world of cybercrime is inhabited by various actors that play by different rules from the rest of society and are driven by conflicting motivations. Identifying threat origination is key to predicting future attacks and protecting organizations against their tactics.

Nearly half (47%) of CISOs in the UAE perceive cybercriminals to present one of the biggest threats. Such concerns are underscored by the rise in ransomware and phishing attacks seen in the UAE over the past few months, as described in our recently released report on the ongoing 2020 ransomware campaigns, accentuated by the Covid-19 pandemic. This also includes advanced persistent threat (APT) groups WildPressure and Anonymous, which respectively are driving malware and doxing campaigns (“dropping dox” is an online attack in which hackers publish personal information and documents about an individual to expose on the internet the identities of people wishing to remain anonymous).

What cyber attack group do you believe is the biggest threat to your organization?

<table>
<thead>
<tr>
<th>Group</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber criminal</td>
<td>47%</td>
</tr>
<tr>
<td>Nation state</td>
<td>19%</td>
</tr>
<tr>
<td>Hacktivist</td>
<td>19%</td>
</tr>
<tr>
<td>Insider</td>
<td>16%</td>
</tr>
</tbody>
</table>

Of less – but still significant – concern are nation-state actors, hacktivists, and insiders. These segments are less motivated by monetary gain and more by disruption or exposure. They are also more likely to target individual organizations, increasing the need for sophisticated defense tactics.
Amongst the various types of attacks, phishing is considered the biggest threat (88%), followed by malware (56%) and ransomware (53%). Phishing campaigns have become progressively more widespread, with a significant number of cyber criminals leveraging the ongoing Covid-19 pandemic. APT groups, such as Mustang Panda (based in China) and others, have been exploiting pandemic themes as a lure. Phishing often serves as the first step in a well-organized attack chain, frequently followed by more sinister attacks, such as ransomware and data exfiltration.

Our recent report on 2020 ransomware campaigns finds an uptick in the deployment of ransomware, such as REvil/Sodinokibi and Defray. These are widely linked to ongoing malicious attacks in the oil & gas and healthcare sectors, as well as recent global attacks on the public sector. Wannacry is still active, largely due to the widespread use of legacy systems. There is no immediate solution, as cybercrime actors are well-coordinated and highly organized.

Cybersecurity is a board-level concern

Business leaders across the UAE increasingly find cybersecurity to be high on their agenda, with a majority of CISOs (66%) providing cybersecurity updates directly to their organization’s board. Greater board-level awareness may be a key factor in explaining increased cybersecurity budgets among local companies.

While the majority of boards view cybersecurity as an enabler for growth, the function is also viewed as a cost of doing business – particularly in a post-Covid-19 world. This equation may be key in future cost-cutting decisions. If boards continue to view cybersecurity as an enabler for growth, they may be inclined to sustain its funding and find other cost centers to trim. However, as the pandemic weighs on organizations’ financial well-being, many are faced with tough financial decisions.

System availability versus data protection

Our survey found a perceived divergence in cybersecurity-related concerns. According to CISOs, approximately one-third (39%) of boards in the UAE are primarily concerned about the impact of cyberattacks on the availability and integrity of critical customer—or citizen-facing systems, with 24% being concerned about the theft of customer data. Two-thirds of CISOs (67%) believe that managing and protecting customer data is as important as delivering a product or service.
Regulation on data protection backs the CISO agenda

According to this year’s survey, 77% of CISOs agreed they are accountable for protecting customer data, confirming that privacy sits within their remit.

Locally, we have seen the data protection regulatory regime shifting, as organizations strive to comply with requirements established by freezones, emirate and/or federal directives and at a global level. For instance, in the financial sector, Dubai International Financial Center (DIFC) and Abu Dhabi Global Market (ADGM) have issued data protection laws. The DIFC’s revised Data Protection Law 2020, ADGM’s Data Protection Law and the Federal Law No. 2 of 2019 are codifying and mandating the protection of personal data – steps that the majority of CISOs already agree are necessary.

Other recent legislation includes:

- National Electronic Security Authority (NESA) Information Assurance (IA) standards, relevant to the financial and oil & gas sectors
- Abu Dhabi Healthcare Information and Cybersecurity Standard (ADHICS), to ensure security in the healthcare sector
- Dubai Electronic Security Center (DESC), covering industrial control systems standards

The UAE is one of the Middle Eastern region’s largest trading partners with the European Union (EU); 40% of UAE-based organizations are subject to EU General Data Protection Regulation (GDPR).

If a local organization processes personal data of subjects located within Europe, not only do they have to comply with the conditions set out in the GDPR, they must also appoint an EU-based representative in order to comply with Article 27 of the regulation.

Global standards have shaped reforms, such as those implemented by the DIFC and the ADGM, and encouraged compatibility.

Thus far, it appears such reforms have had a positive impact, with the vast majority of CISOs (89%) stating their security posture has improved due to the advent of new cybersecurity regulations.

Has the roll-out of cyber security regulation affected your company’s security posture?

47% Yes our security posture is much better

42% Yes, our security posture is somewhat better

11% Not really, our security posture has stayed the same

11% Single response
Data protection principles such as transparency, individual rights and accountability have become key pillars within any effective data governance programme. The way in which your organisation manages, processes and shares personal data is likely governed by global data protection laws, privacy obligations or consumer expectations.

Sami Mohammed
Head of The Office of Data Protection, Abu Dhabi Global Market
Contacts

Tim Wood
Partner
Head of Cyber
KPMG in the UAE and Oman

T: +971 4 249 6525
E: timothywood@kpmg.com

Maliha Rashid
Director
Head of Data Privacy
Cyber Lead, Healthcare, Energy
KPMG in the UAE

E: mrashid5@kpmg.com
T: +971 50 608 2013