State of Play for Middle East Cybersecurity Leaders

In collaboration with Synack

Cybersecurity risk management is a distinct practice for every organization, depending on its size, business vertical, staff composition, technology environment, and more. The best practices for one company sometimes don't apply to another, and the top priorities for different cyber risk teams are often not the same.

Nevertheless, there are certain commonalities across sectors, regions, company sizes, and other characteristics. This paper distills the findings of the Middle East Institute panel "State of Play for Middle East Cybersecurity Leaders," a discussion held in September 2020 about the unique threats, best practices, and corporate landscape in the Middle East and North Africa region.

The common issues and dynamics for cyber risk managers in the Middle East specifically fall into three categories: the threat environment, business environment, and talent environment.

THREAT ENVIRONMENT

The threat environment in the Middle East is severe — there are 10 percent more attacks on organizations in the region than the global average, according to Maya Horowitz, the director of threat intelligence at Check Point Software Technologies. This may be because the penetration of web technology is relatively high in the Middle East, but the market is not yet mature enough for security technology and awareness to be fully endemic.

The two most common forms of threats in the region are ransomware via tools like Emotet and information theft attacks, according to the panelists. Both of these are also common forms of attack worldwide, especially given the vertiginous rise of ransomware attacks globally in recent years.

Something more particular to the region is the origin of these attacks — as a hotbed of geopolitical instability, the volume of nation-state attacks is significantly pronounced. This includes governments spying on their own citizens, governments spying on foreign citizens, and globally prominent governments like China and Russia targeting individuals or organizations in the region. The threat of nation-state attacks prompts the issue of risk tolerance for cyber risk management professionals in the Middle East: governments have functionally limitless resources to carry out attacks, so a higher degree of risk acceptance — in particular the risk of cyber espionage — is an inevitable cost of doing business in the region.

BUSINESS ENVIRONMENT

The business environment in the Middle East is not dramatically different from that of the world more broadly, although the heavier reliance on industrial control systems (ICS) for resource extraction and critical infrastructure processes like water desalination poses its own challenges. These systems require their own distinct security solutions, as they do anywhere. However, they again underscore the issue of risk acceptance: ICS systems are an attractive target for nation states due to their pronounced importance to national security, and for government hackers, an oil extraction site or water desalination plant is targeted effortfully, not opportunistically.

The broader Middle East business environment incorporates network technology at similar levels to the rest of the world, but security technology and practices are not yet as diffuse as in Western Europe or North America (where there is still a great deal of progress to be made). This security immaturity is known to cyber criminals, and it makes Middle East organizations more attractive targets for phishing and other commercially motivated attacks.

A critical solution to this problem is investing in employee security training. Cybersecurity is not just a line-item or a box to check, it is a continuous process that requires the participation of all team members. Cyber criminals expect Middle Eastern targets to be vulnerable to phishing attempts, and the single best way to thwart them — although it is difficult, asymmetric, and even Sisyphean — is to defy their expectations.

TALENT ENVIRONMENT

The Middle East, like the rest of the world faces a talent shortage for cybersecurity professionals. Cybersecurity is a complicated and variegated field, and there is no degree or training program that can be expected to produce the right quotas of specialists in cryptography, information technology, geopolitics, forensics, malware analysis, regulatory compliance, and policy management.

Israel is commonly touted for having solved this problem, with a flourishing technology and cybersecurity sector, thanks in large part to its national service requirement and in particular the training of recruits to Unit 8200 (the Israeli equivalent of the U.S. National Security Agency). For governments, a national military or public service requirement can be a powerful pipeline for training and producing skilled workers with practical, hands-on work experience — also a common barrier for young cybersecurity professionals.

For companies and practicing cyber risk management professionals in the Middle East, who obviously cannot establish universal government service programs, a helpful solution may be to identify and promulgate free or paid training resources from websites like Coursera, edX, and Udemy. These online classes can be made available following mandatory employee trainings in cyber hygiene, and can be paired with opportunities to train and work with existing, experienced cybersecurity staff.

CONCLUSION

The cyber threat landscape may be more dangerous in the Middle East than elsewhere, but it is not overwhelmingly so — the higher risk level is only a matter of degrees. It is both possible and imperative that companies and cybersecurity specialists in the region acclimate to the threat environment to prevent serious and potentially catastrophic attacks. This will only become more salient over time as the world adopts and adjusts to new, web-connected technology like 5G, automated machinery, driverless cars, the internet of things, and more.

This panel discussion was sponsored by Synack, a cybersecurity company that combines AI and machine learning-enabled security software with a crowdsourced network of white-hat hackers to help keep its customers secure. To view Synack reports, webinars, datasheets, and other resources, click here.

MEI Cyber Program Research Assistant Mneera Abdullah contributed to development of this white paper.