IQPC
International Quality & Productivity Center

MIDDLE EAST CYBER SECURITY LANDSCAPE

CYBER SECURITY FOR ENERGY & UTILITIES

Produced by IQPC Middle East in association with the MENA Rail Operational Readiness Summit in January 2016 in Doha, Qatar.

68% of organisations in the Middle East lack the internal capabilities to protect themselves against sophisticated cyber attacks.

"Organisations need to get a handle on securing virtual environments. There's a growing awareness of the risks, but there's still inertia and a lack of understanding of the specific factors involved in protecting virtualised systems." – Kaspersky Labs, Global IT Security Risks Survey 2015

As the internet continues to grow in size, scale and complexity, companies and service providers across every industry are able to develop more innovative and convenient methods of serving and communicating with their target audience. However, new risks and challenges go hand-in-hand with these new opportunities and arguably the most worrying emerging threat is cybercrime.

Cybercriminals come in a wide range of varieties: from thrill-seeking juveniles to politically motivated "hacktivists" and economically motivated data thieves. Regardless of their background and motivations, cybercriminals across the world are developing increasingly severe and sophisticated means of penetrating target companies' ICT security networks in order to steal their valuable data, halt or hamper their operations and even cause lasting infrastructural damage.

Unfortunately, while general awareness of overall threat of cybercrime is increasing, 68% of organisations in the Middle East lack the internal capabilities to protect themselves against sophisticated cyber attacks. Meanwhile, 70% of regional IT decision makers lack complete confidence in their company's cyber security policies and capabilities to adequately defend them against emerging threats.[1]

In order to protect their operations and key data from the predations of cybercriminals, it is essential for ME company leadership members and ICT decision makers to understand the nature of the diversifying threat landscape that they face.

Examples of High-Profile Attacks in the Middle East

March 2015: Trojan.Laziok: Last year, this virus specifically targeted energy companies around the world with a focus on the Middle East. The attack started through the use of spam emails loaded with malicious command code attachments which were executed if the recipient opened the email attachment. Trojan.Laziok then made a comprehensive search of the infected hard drive infected, looking for anti-software details, CPU capabilities, GPU details and more. This information was sent to the attackers who then infected the host with additional malware designed to steal further useful data.[2]

December 2014: Operation Cleaver: Over 50 entities in 16 countries were victims of a concerted cyber attack campaign thought to have originated in Iran. Most worryingly, security systems at airports in Pakistan, Saudi Arabia and South Korea were compromised along with airlines in the US, United Arab Emirates, South Korea, Pakistan and Qatar. The hackers gained complete access to airport security gates and their control systems, potentially allowing them to fake passenger details and flight gate credentials, leading to all manner of security vulnerabilities.[3]

---

[1] *Gulf Business, Cyber war: Is the Middle East prepared?*
[2] *Khaleej Times, Oil and gas platforms at risk of cyber attack, 26/06/2015*
[3] *IB Times, Operation Cleaver: Iran's state-sponsored hackers infiltrate airport and airline security, 03/12/2014*

August 2012: Saudi Aramco: The computer network of Saudi Aramco was struck by a self-replicating virus that infected as many as 30,000 of its workstations, wiping data indiscriminately from their hard drives. Operations halted and the company took almost two weeks to recover and regain full operational capabilities.[4]

Threat Trends Affecting ME Companies

Denial of Service attacks (DoS/DDos)

DoS attacks are the fastest growing type of cyber attack being experienced globally and are quickly becoming one of the most common threat types. They rely on flooding the connections between the internet and the target business with vast amounts of traffic in order to overload the network's servers to the point of inoperability, resulting in denial of service.

More sophisticated DoS attacks utilise multiple nodes in concert to send even greater volumes of malicious traffic to a site in distributed denial of service (DDoS) which increases the severity of the attack while making its source more difficult to locate.

Unfortunately, the tools for initiating DoS/DDoS attacks are readily available and easily understood, meaning that a wide range of hackers are capable of utilising them.

Potential damage factors:

Revenue losses: No trading, selling, communicating etc can be performed during service outage.

Reputational losses: Loss of customer satisfaction and perceived inability for the company to protect itself.

Overall, IDG Research suggests that for a large business enterprise the average DDoS attack can cause $100,000 worth of associated damages for each hour of network outage.[5] Even SMEs or smaller MNCs can suffer $10,000 to $50,000 in losses per day.

Loss of continuity of services: Interrupting operational continuity will affect any business enterprise or government service department. For this reason, 25% of companies in the Gulf region consider DDoS attacks one of their top three business threats.[6]

Data Theft Attacks

The damaging impact of successful DDoS attacks cannot be overstated in terms of immediate losses and interruption of business operations. However, data theft attacks can be equally devastating should they allow an intelligent and motivated hacker to access particularly valuable data assets.

As with DDoS, businesses are facing a widening range of data theft threat types, most of which are designed to take advantage of inherent vulnerabilities at the web application level. Data thieves bypass traditional network-layer security tools through the generation of application traffic which appears in the form of genuine requests to fool detection systems and allow the hacker to inject commands into the compromised application. The hacker then subverts the application to for their own uses, such as allowing them to discover and extract sensitive internal data.

Overall, IDG Research suggests that for a large business enterprise the average DDoS attack can cause $100,000 worth of associated damages for each hour of network outage.

[4] *IISS, The Cyber Attack on Saudi Aramco, 01/04/2013*
[5] *IDG Research Services, A DDoS Attack Could Cost $1 Million Before Mitigation Even Starts, 24/10/2013*
[6] *Kaspersky Lab, Global IT Security Risks Survey 2015*

60% of businesses that suffer a data breach find their ability to function severely impaired

Potential damage factors:

- **Intellectual property theft:** Hackers performing complex data theft attacks are usually highly skilled and motivated, meaning that they will be aiming to extract intellectual property and other high value data.
- **Loss of commercial competitiveness:** Data theft can ultimately leave the target in a state where their ability to compete is compromised as key operational and/or intellectual data is illegally shared or subverted.
- **Ongoing ICT vulnerabilities:** Many data theft attacks are sophisticated enough to leave the target unaware of the breach and subsequent theft. If the breach remains undetected, the perpetrator can gain entry once again at a later date to steal more information.
- Reputational and financial losses: Public knowledge of data breaches can cause significant reputational losses that then lead to lost business opportunities and damaged customer relations.
- Overall, the average cost of a data breach for SMBs and Enterprises stands at $38k and $551k respectively. Large enterprises can suffer losses amounting to millions of dollars. 60% of businesses that suffer a data breach find their ability to function severely impaired.[7]

Malware and Ransomware

Malware is a malicious form of code used by hackers to input their desired commands into a target's ICT infrastructure in order to subvert, damage or control it. Ransomware is a specific malware tactic designed to lock out the rightful owners from their command and control systems in order to hold them to ransom.[8]

Hackers will often trick the target entity's employees into activating their malware by getting them to click on links or email attachments. Once enabled, malware infects the target's network and can log key information, disrupt operations and cause a wide range of persistent problems.

Potential damage factors:

Compromised operational effectiveness: Malware can slow or entirely halt operational processes via malicious commands.

Financial losses from ransoms: The specific tactic of ransomware can cost target companies tens of thousands of dollars if they choose to pay the ransom, not to mention the lost revenue from the downtime incurred.

---

[7] Kaspersky Lab, Global IT Security Risks Survey 2015
[8] The National, Cyber attacks on the rise across the Middle East and North Africa, 22/05/2015

Future Threat Landscape: Pitfalls and Protection

"With smart cities and IoT, the more places you have access to and the more dependent you get on those things or devices, the more prone to cyber attacks you become. In smart cities, traffic, transportation, rail, all these things are connected so there is a huge amount of information that is produced." – Mahir Nayfeh, Senior VP, Booz Allen Hamilton

As significant as the emerging threat landscape is now, cybercriminals are always looking to develop the next hack, attack pattern or exploit in order to breach their target's ICT infrastructure. As many of the Middle East's respective countries move towards achieving their smart city ambitions, the potential for cybercrime to inflict lasting economic or even physical damage to citizens and infrastructure will rise even further.

Each of the following smart city components and systems represent a high value target for both politically and economically motivated hackers:

Smart utilities: In the smart cities of the near future, urban utilities providers will merge their monitoring and metering systems to improve service delivery. Manipulating these systems could cause untold economic harm by causing service disruption, inaccurate billing and even infrastructural damage.

Smart policing and emergency response: Law enforcement and medical institutions will come to share greater quantities of personal information in the future and successful data theft attacks will both impair the authorities' efforts and could jeopardise citizens' safety and wellbeing.

Smart transport systems and driverless cars: Manipulating interconnected public transport systems has the potential to cause massive delays, disruption and confusion or, in a worst case scenario, destruction of infrastructure and loss of life.

Leading ME Companies are Preparing to Protect Themselves

"What we have traditionally seen in the Middle East is that people like to have their own little areas of structure. What really and truly needs to happen is for everybody to embrace IoT (Internet of Things) and not look for empire building in any shape or form. That's the whole thing about private-public partnership. Getting people to work together for the greater good is going to be the hardest thing," – Paul Black, DC MEA and Turkey Director - Telecoms and Media

"The answer lies in collective action. Cyber security is no single person, organisation or industry's problem - it is everyone's. Just as the risks are shared, so should the responsibility for addressing them. Through an alliance of pooled expertise, resources and budgets, we can begin to give the cyber security challenge the attention it demands." – McConnell, Senior Executive Advisor, Booz Allen Hamilton

Despite the rising frequency and severity of attacks being experienced by ME companies (particularly those in the energy, utilities and oil & gas sectors), there are two key issues that are holding back the overall improvement of cybersecurity in the region.

"With smart cities and IoT, the more places you have access to and the more dependent you get on those things or devices, the more prone to cyber attacks you become. In smart cities, traffic, transportation, rail, all these things are connected so there is a huge amount of information that is produced."

Mahir Nayfeh, Senior VP, Booz Allen Hamilton

1. The majority of companies are being reactive rather than proactive. Until recently, cybersecurity has been a low priority and most companies will wait until they experience an attack, endure the damage it causes and then develop a solution in order to prevent it from happening again.
2. Too many companies are unwilling to share cybersecurity best practices with one another and collaborate on building better industry-wide defences. This is due to their entrenched position of competition with one another and an inherent hesitance to reveal any vulnerabilities or security challenges that they are facing, in case this shared knowledge is exploited for commercial gain.

These two issues are being experienced globally and are in no way unique to the Middle East. However, they must be overcome in order for ME governments and companies to work together towards a future where they are better protected from cybercrime. Fortunately, ME business sectors have been waking up to the growing threat and today far fewer enterprises are willing to simply stick their heads in the sand and hope that the hackers will pass them by. Instead, they are going to greater lengths than ever before to protect themselves, a goal that respective ME governments are keen to help them achieve.

Too many companies are unwilling to share cybersecurity best practices with one another and collaborate on building better industry-wide defences.

Ensuring best practices through regulation: ME governments are looking to encourage key sectors like energy and utilities to adhere to international best practice with regards to cybersecurity. For example, the UAE National Electronic Security Authority (NESA) draws on a number of guidelines from the internationally recognised ISO 27001 standards and insists that many companies in key sectors will have to adhere to these principles by end of 2016.[9]

The ISO Code of Practice for Information Security Management (ISO 27001/27002) is a security management framework. It outlines a set of high-level organisational policies, procedures and technical standards that a company needs to follow, based on the specific risks it faces, in order to properly analyse and manage its ICT security risks.[10]

Currently, some organisations will simply choose to implement the standard of ISO 27001 in order to benefit from the best practice it contains, while others decide they also want to get certified to reassure customers and clients that its recommendations have been followed.[11] However, it seems that more ME governments are moving towards an obligatory model where companies in certain key industries will have to follow such guidelines in order to remain eligible for government contracts.

Increased official support: ME governments are investing more in national cybersecurity solutions in combination with implementing new regulatory measures. For example, over the course of the next 10 years the UAE will be more than doubling its homeland security budget to over $10 billion with a sizeable proportion being allocated to cybersecurity through NESA.[12] Similarly, in December 2014 Egypt established the High Council for Cyber-Security (HCC) which is tasked with securing vital national infrastructure and utilities networks against cyber attacks.[13]

Increased spending on holistic cybersecurity solutions: More companies in vulnerable industries such as energy, utilities and oil & gas are realising that their own in-house ICT security capabilities may well be insufficient to protect them from the heightened threat landscape that is currently emerging.

---

[9] MWR, NESA – The New Standard of Information Security in the UAE, 06/04/2015
[10] Bloomberg BNA, An Overview of the Different Standards U.S. Government Agencies and Other Entities Are Developing to Regulate Cybersecurity, 07/12/2015
[11] ISO.org, ISO/IEC 27001 - Information security management
[12] Defence News, UAE to Double Security Budget, Focus on Cyber, 24/02/2014
[13] Al Monitor, Egypt's cybersecurity council prompts privacy concerns, 22/01/2015

Recent research suggests that worldwide spending on cybersecurity for oil and gas infrastructure will reach $1.9 billion by 2018.[14] As one of the most highly targeted regions worldwide, the Middle Eastern energy sector has leading companies that are investing in the latest cybersecurity technologies in order to achieve a holistic, multi-layer approach to the defence of its assets and data centres.

For example, more companies in the oil and gas sector are investing in the next-generation firewall (NGFW) that is more adaptive and predictive than previous generation firewalls. NGFWs are designed to provide the full contextual awareness and dynamic controls needed to automatically assess threats, correlate intelligence, and optimise a company's cyber defences against incoming attacks.[15] It utilises a suite of analytics programs to provide detection, blocking, tracking, analysis, and remediation capabilities to protect against the full spectrum of attacks.

This exemplary approach to cybersecurity preparation is of very important in encouraging best practice throughout the region and may pave the way for increased collaboration – not just between companies and security solution providers, but also between competing companies themselves. By adopting such a collaborative approach, companies are in a better position to improve their own online security strategies and create a safer, more secure operational environment.

Innovating for a Safer, more Secure Virtual Business Environment

Cyber threats are here to stay and growing awareness in the Middle East of their severity must be matched with increased investment in cybersecurity capabilities. Cybercriminals will continue to evolve new and more insidious methods of attacking their targets so their efforts must be met in kind with continuous innovation and evolution of new defences and best practice.

In order to avoid financial and reputational losses, and stave off even more catastrophic damage types, businesses need to commit themselves to continuous education on the emerging threat landscape. Subsequently, knowledge of the threat must be paired with investment in neutralising it. This needs to be understood and encouraged from the top leadership down, not merely implemented as an afterthought.

By making these necessary changes, the key industries of the Middle East can avoid ongoing losses, confusion and hesitancy, while encouraging others to follow their example and even collaborate in further strengthening their respective security networks.

For example, more companies in the oil and gas sector are investing in the next-generation firewall (NGFW) that is more adaptive and predictive than previous generation firewalls.

[14] *Bloomberg, Hackers Target Oil Companies for Mayhem, 11/06/2015*
[15] *Cisco, Omani Organizations Must Deploy Security Solutions to Protect Against Highest-Ever Threat Landscape, 09/02/2015*

Sources:

http://www.bna.com/making-sense-morass-n57982064484/

http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

https://www.iiss.org/en/publications/survival/sections/2013-94b0/survival--global-politics-and-strategy-april-may-2013-b2cc/55-2-08-bronk-and-tikk-ringas-e272

http://archive.defensenews.com/article/20140224/DEFREG04/302240015/UAE-Double-Security-Budget-Focus-Cyber

http://www.khaleejtimes.com/nation/general/oil-and-gas-platforms-at-risk-of-cyber-attack

http://www.bloomberg.com/news/articles/2015-06-10/hackers-favorite-target-big-oil

http://www.al-monitor.com/pulse/originals/2015/01/egypt-cyber-security-council-privacy.html

http://www.cisco.com/web/ME/about/news/2015/090215.html

http://www.strategyand.pwc.com/reports/cyber-security-middle-east

http://www.gulfbusiness.com/articles/insights/what-should-the-middle-east-do-to-enforce-cyber-security/

http://www.livetradingnews.com/smart-city-plans-is-dubai-future-proofed-123385.htm

http://gulfnews.com/business/sectors/energy/cyber-attacks-an-increasing-threat-for-mideast-oil-and-gas-1.1399982

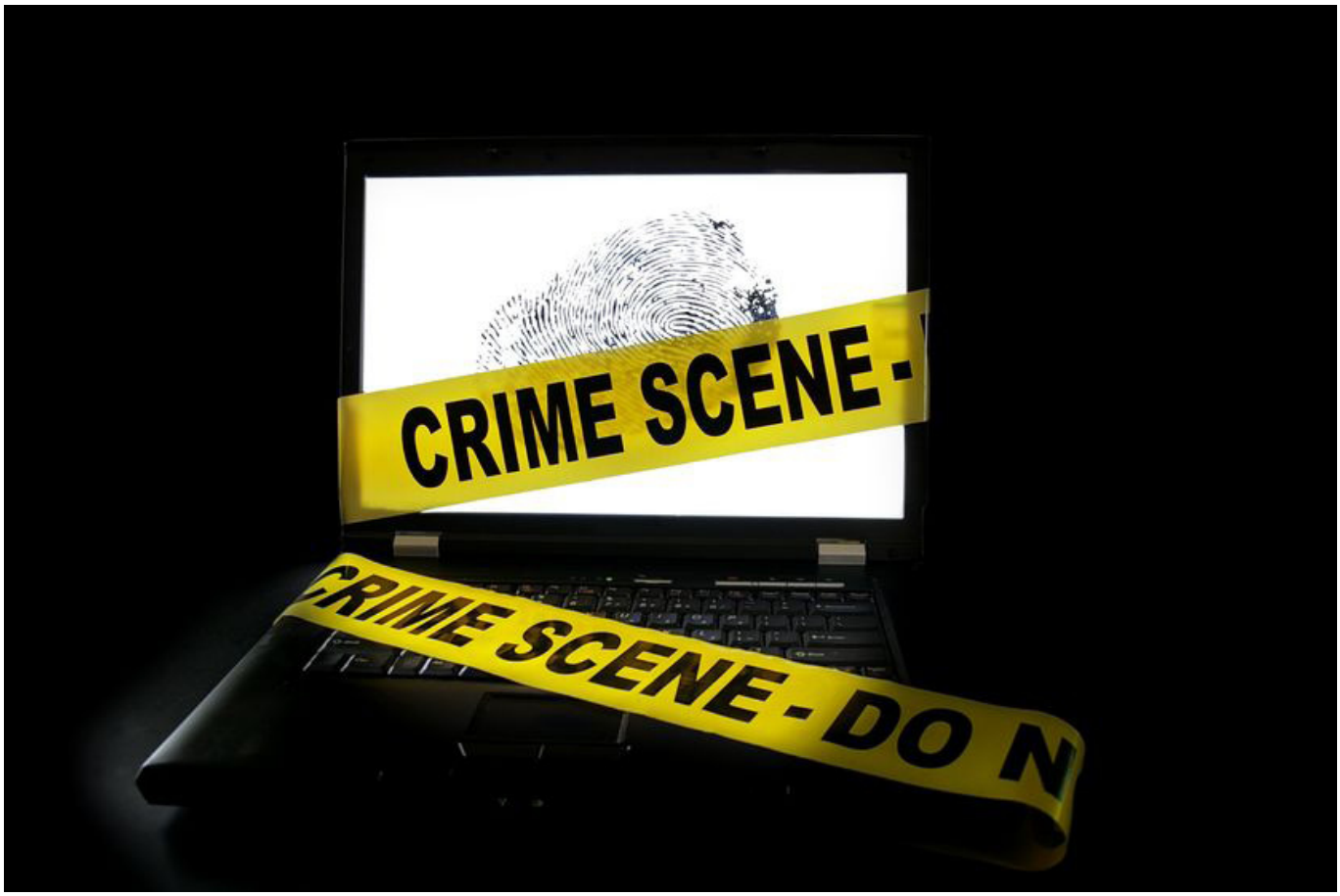
https://www.mwrinfosecurity.com/articles/nesa-the-new-standard-of-information-security-in-the-uae/

http://globalriskinsights.com/2015/09/how-strong-are-the-middle-easts-cybersecurity-networks/

http://media.kaspersky.com/en/business-security/it-security-risks-survey-2015.pdf

http://www.arabiangazette.com/cyber-security-awareness-increases-middle-east-20130131/

http://www.cbronline.com/news/cybersecurity/data/trojan-laziok-targets-global-energy-sector-4543988



Publisher contact details: Shrutika Shetty | IQPC Middle East | enquiry@iqpc.ae