DMCC Cyber Security Seminar

8:30 am on 23 February 2017
Eng. Ahmed Hassan Mohamed Noor, Director of Compliance, DMCC

Introduction and Biography

Ladies and gentlemen, distinguished guests, good morning, and welcome to the first DMCC Cyber Security Seminar of 2017, and the latest edition of our Knowledge Series, a really valuable resource in which we bring together the entire DMCC member community to share our collective experience and expertise for the benefit of us all.

Thank you for joining us today.

For those of you who do not know me, my name is Ahmed Hassan Mohamed Noor, and I am the Director of Compliance here at DMCC.

Today, cyber security is a big part of that, and it has been at the core of my professional experience for more than 12 years.

Prior to joining DMCC, I was Director of Risk Management and Compliance at du Telecom, leading the organisation's Information Security and Operations Risks strategies as well as its Compliance programmes.

I was also at the Telecommunications Regulatory Authority (TRA), where I led the Threat Intelligence Operations Center, Infrastructure and the Research & Analysis section for its UAE Computer Emergency Response Team. In the past I also headed Etisalat's Enterprise Network Security function.

So, as you can see, cyber security is a passion for me.

To begin with today, I'd like to ask you all a question.

In today's online world, in which we are all connected to one another by unseen digital networks, we must ask ourselves, how secure is it in reality?

The answer, fortunately for us all, is that we take our cyber security here at DMCC just as seriously as our physical security.

The Cyber Security Market

When looking at Cyber Security, it is helpful to understand that the challenges faced by business in this regard are so acute that solving them has become big businesses in itself.

And it is getting bigger by the day.

The global cyber security market is estimated to grow from a value of USD 122.45 Billion in 2016 to USD 202.36 Billion by 2021, at a Compound Annual Growth Rate of 10.6%, according to US research company Markets and Markets.

45 per cent of Middle East, Turkey and Africa based organisations reported cyber security incidents in the first quarter of 2016, according to Kapersky Lab.

As a result, the Middle East cyber security market is expected to reach around US$10 billion by 2019, double the US$5 billion it was worth in 2014 (Markets and Markets).

In 2016, Dubai launched a US$270 million Future Accelerators programme designed to transform the city into an innovation hub, and the Gulf Cooperation Council (GCC) is predicted to spend up to US$1 billion on cyber security by 2018.

And the reason there is so much budget to be spent in this area is because there is so much at stake.

Cybersecurity Ventures predicts cybercrime will continue rising and cost businesses globally more than $6 trillion a year by 2021.

The cybercrime cost prediction includes damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm.

Cyber Security Trends for 2017

So, the biggest companies operating in this market, the likes of Root9B, Herjavec, IBM Security and Palo Alto Networks, are helping us to guard our businesses against a barrage of online attacks.

We have all heard of so-called computer viruses - we may even know some of them by name such as Shamoon and Shamoon 2 that struck with disastrous effect in Saudi Arabia back in 2012 and, it seems, again just last month.

Getting more technical, some of you may have come across events such as a Denial of Service attack, or DoS, whereby groups of individuals use bots and other AI to bombard the website of a particular business with countless requests at the same time leading the website to shut down.

But, there are at least three types of attack that are perhaps less well known that most industry observers agree are among the biggest areas of cyber security concern for businesses in 2017.

1) Ransomware

Ransomware is software that infiltrates computer networks or systems and encrypts data or denies access until a ransom has been paid, and was the fastest-growing cybersecurity threat globally during 2016. IN the United States more than 4,000 ransomwear attacks were reported a day last year with the healthcare sector particularly vulnerable. The software often arrives in a familiar looking “phishing” email with a file attached that the receiver activates with a simple click.

2) The Cloud

As we use collective data storage solutions more and more, we are opening ourselves up to potential cyber security threats on an almost uncontrollable level. If a Cloud user has weak security protocols such as poor passwords or unmonitored access, hackers can gain access to that user’s system as then use it as a means of accessing the cloud, where it can do real damage across the networks of thousands of other users by the backdoor.

3) The Internet of Things

It is predicted that 20.8 billion “connected things” will be in use by 2020 - from your coffee maker to the environmental management system of an entire building. Security is falling way behind in this sector, however, leaving hackers and criminals an easy path into your business or residence. Last year when Twitter, Reddit and Netflix suffered damaging shutdowns of service it emerged that hackers had gained control of the websites by “taking over” Internet of Things connected security cameras.

These trends are as fascinating as they are frightening, and I am sure we will be discussing them at greater length today and well into the future.

Understanding the Dark Web

Also, key among the facets of cyber security we will be discussing today is understanding the so-called Dark Web which refers to secretive hidden corners of the internet largely used by criminals or those who do not want their online activities to be tracked.

Intellectual Property Theft and Misuse

A recent study by Deloitte claimed that digital intellectual property theft had become the number one concern for the majority of businesses in operation today.

And this is why it is so important for us all to improve security, and protect our organisations from these new threats as they continue to evolve.

Conclusion

Cyber security is no longer a specialist niche market.

We live connected lives that require connected security because cyber security impacts life at every level.

I would like to thank you all again for attending this fascinating Knowledge Series event, and all of us at DMCC very much look forward to continuing this discussion for the remainder of the session.

Thank You.