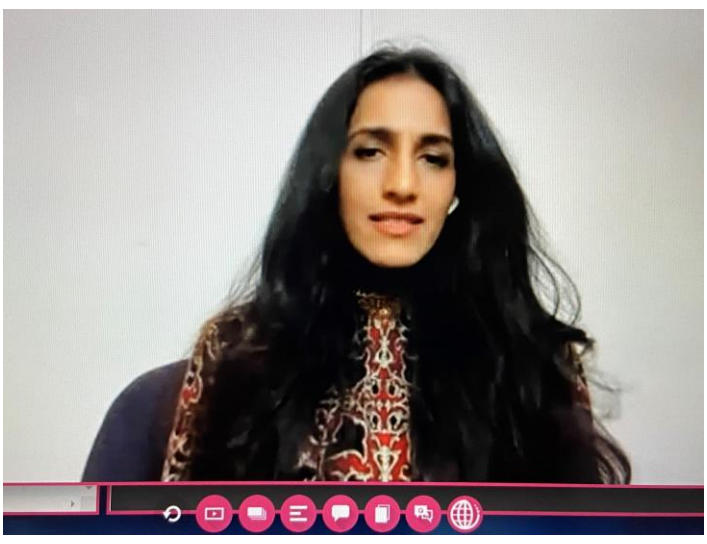
Dear Member,

New technologies such as artificial intelligence (AI), the Internet of Things (IoT), and robotics can offer urban businesses and citizens higher quality, more productive, and more sustainable lifestyles. Hackers – akin to a rouge destructive virus, are equally active and alive in this very same cyberworld. Cybersecurity must be adapted to counters such threats.

As the keynote speaker for day 3 on 16 June, Dr Ayesha Khanna, Co-founder and CEO of ADDO AI delivered a comprehensive assessment of case studies and best practices on how to effectively implement and be part of the Smart Cities 2.0 paradigm. Today, Keren Elazari, Senior Researcher at Tel Aviv University's Balvatnik Interdisciplinary Cyber Research Center and friendly hacker, spoke on the importance of hackers and how thinking of helpful hackers as the immune systems of the Internet can make security stronger and better prepare and secure the organisation's digital presence.

Smart Cities 2.0 by Dr Ayesha Khanna



According to Ayesha, more than half of the population now is part of the middle class. In fact, five people every second join the middle class, she said. In the near future, almost all of these people — at least 80% of them — are going to live in a city, she noted. Facing this reality, the future will be largely defined by how people live in these cities, and how to use the defining force of our times, data, to both live and work.

Taking this concept to the extreme, and inspired partially by the challenges recently seen during the pandemic, designers have developed the idea of a pandemic-proof "smart city," Ayesha explained. This concept revolves around the idea of people living in an area where everything one needs for a high-quality life is 15 minutes away. All food would be sustainably grown within the city walls using "vertical farming" methods aided by AI and immersive experiences such as going to the theatre or gym could be had within a person's home.

Ayesha said leveraging machine tools such as AI to enrich people's lives has great relevance in the present, both personally and professionally. For internal auditors, AI enables them to dig deeper into data than ever before and with much greater efficiency. Contracts can be viewed for suspicious activity and money laundering activity can be detected at levels previously unthinkable. AI can even be used to monitor employees to develop detailed root cause analysis of operational risks, she explained.

What professionals such as internal auditors bring to the table is their experience and expertise, which no AI can replicate. Over-reliance on AI comes with a multitude of risks, such as "coded bias" that can promote discriminatory practices, she noted. Such inherent risks must have a human element to counteract them.

"The future of cities and new technologies depends on us being responsible in how we use AI," Ayesha said. "Without ethics, you cannot have an AI discussion."

Building a Digital Immune System for the New Age by Keren Elazari

The development of cybersecurity is interwoven with the evolution of the hacker community. Keren said that the beauty of hackers is that they force people to evolve and improve. She shared this message that hackers can be helpful allies with a variety of different organisations and people.

In the past couple of years, more and more businesses are finding the value of working with the friendly hacker ecosystem. One way is through the "bug bounty programmes" which involve big companies actively inviting friendly hackers to look at their products to find vulnerabilities. When security flaws are discovered, the companies will reward the hackers for their efforts in the form of money paid in prepaid credit cards or debit cards. She explained that by creating these programmes, it allows friendly hackers a "pathway" to report their findings and help organisations get safer.

Cybersecurity threats are increasing with IoT and the proliferation of devices that are connected. Keren said "it is all about personal responsibility." As more people start to ask vendors who create these technologies and sell these products questions like, "What are your security protocols?", "What is your method of updating operating system for this device?" or "How can I change my passwords?", there will be a "more secure ecosystem."

There will be malicious individuals and organisations that will use technology for ill gains. "The friendly hacker community can help" and it is important to invest in "cybersecurity, education and awareness."

You can read more about the takeaways from the IIA 2021 International Conference **here**. Do follow us on our LinkedIn Page and Facebook to get updates of the event.

We hope members have found both the content and engagement rewarding.

Thank you.

Goh Puay Cheh, *CIA, CRMA*
Executive Director
The Institute of Internal Auditors Singapore

Brought to you by:

The Institute of Internal Auditors Singapore

Website | Our Facebook | Our LinkedIn | Contact Us