Embracing Technology and Data, and Future Crimes 2025

Benjamin Mossé
MD, Mossé Security

The next 20 years are going to make the last 20 look like we accomplished nothing in technology. (Ray Kurzweil)

By 2025, the Internet population is expected to double. The average number of Internet-connected devices per household will increase from 10 devices today to 50. Advances in artificial intelligence and global data are going to entirely re-invent the world around us. Comparing the size and impact of today's technology to 2025 is like comparing a basketball to the sun.

2025: Opportunities vs. Threats

Whilst those advances will offer incredible opportunities to business leaders, so will the threats of cyber crime continue to grow, as well as the risks of cyber warfare and significant increases in regulations and compliance requirements for IT.

Power once came from controlling the sea lanes.
In the future, power will come from controlling the information lanes of cyber space.

Power once came from controlling the sea-lanes. But in the future, it will come from controlling the information lanes of cyber space (Joe Nye).

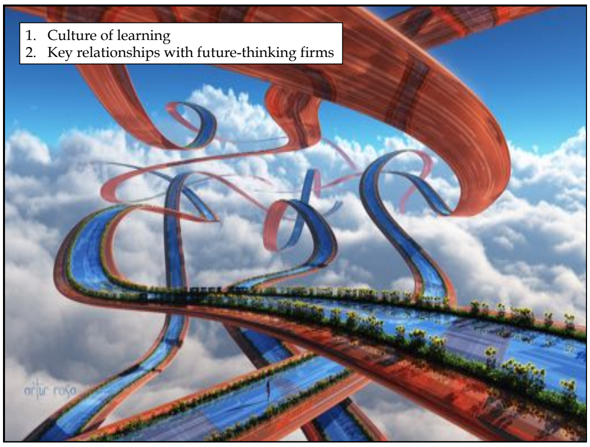
For the construction industry, that may mean potential attacks against core city infrastructure as well as smaller devices and systems connected to the Internet.

Attack Surface 2025

Think of future trucks, farms, smart houses, public transport and drones as the targets for attacks.

A realistic scenario is that many future devices will be built using the same software. A critical vulnerability discovered in that software could, overnight, affect millions of devices across multiple countries, cities and lands. Threat actors located on the other side of the world may render entire sections of devices unavailable for days at a time. Future crimes in your industry may impact public safety, public privacy, and even generate tensions between countries. One sure prediction is that cyber attacks will continue to increase the cost of doing business.

So how can business leaders achieve a



1. Culture of learning
2. Key relationships with future-thinking firms

First, and, most important is Learning and implementing a culture of learning within the enterprise. The leaders of tomorrow will be technologists and security experts. The best way is to foster a culture of on going learning amongst employees regarding security to keep up with new and emerging threats. That means adopting learning programmes on IT security and sharing knowledge from one person to the next to create an IT security common sense across the organization. This is becoming a world trend amongst top businesses.

And finally, as you are embracing technology and data, establish key partnerships with future-thinking firms focused on solving the problems of tomorrow rather than repeating the used-ideas of the past.

Thank you.

Thank you.

benmosse@mosse-security.com