Cyber breaches and attacks on government and company computer systems have become regular news. Inadequate information security has dragged down organisations’ hard-fought reputations, customer confidence and CEO careers. Are information security leaders ready to take on the task of managing the ever-evolving threats and opportunities in today’s complex, digital world?

Raytheon surveyed over 1,000 chief information officers (CIOs), chief information security officers (CISOs) and information security leaders across the world, including 403 in Europe, to identify the overarching sources of cybersecurity risks and the major cyber trends over the next three years.

Here are the seven key European Cybersecurity Megatrends from the study:

1. Cybersecurity as a priority
Senior leaders and Boards of Directors are not involved in shaping the cybersecurity strategy — but they should be.

2. Insider threat risks
The impact of insider threat risks (from employee behaviours) is expected to decline. With improved insider threat technologies and increased emphasis on employee training, organisations expect the cybersecurity risk from employee behaviour to decline in the next three years.
3. Cyber crime
Cyber crime keeps information security leaders up at night. European information security leaders rated cyber crime as having the greatest impact on their organisations' level of cybersecurity, followed by enabling technologies and human factors.

The impact of factors on your organisation's cybersecurity

- Cyber crime: 25%
- Enabling technologies: 19%
- Human factors and employee behaviour: 16%
- Compliance costs: 15%
- Disruptive technologies: 6%
- Organisational factors: 6%

4. Internet of things
A surprising 70 per cent of European organisations are not prepared to deal with the potential risks resulting from the “Internet of Things,” an expanding network of billions of connected devices that could be vulnerable to hackers.

5. Talent gap
The cyber talent gap continues to be an issue. As technology advances, the education, recruitment and ongoing training of information security practitioners need to stay current with the ever-evolving cyber threats and technologies.

66% of respondents say their organisation needs more knowledgeable and experienced information security employees.

6. Technologies
Encryption, big data analytics, forensics and intelligence-based cyber solutions are creating big shifts in technology. Information security leaders expect less emphasis on anti-virus and anti-malware technologies in three years.

Not surprisingly, increased sophistication of the attacks is driving the technology shifts. According to information security leaders, the most prevalent types of attacks three years from now are expected to be zero-day attacks, cloud data leakage and database compromise.

7. Optimistic about their organisations' cyber future
Despite all the alarming cyber news in the media today and the dynamic nature of the threats, European information security leaders continue to be optimistic about their organisations' cyber future.

Future state of your organisation's security readiness in 3 years

- Will improve: 32%
- Will stay the same: 55%
- Will decline: 13%

Success in today’s virtual landscape requires more than just the application of the newest technologies. Success requires a deliberate blend of people, processes and technologies to ensure that governments and businesses can be resilient against all manner of cyber threats and reap the benefits of the global information environment.

Information security leaders need to partner closely with their senior leaders, and together they can drive the digital maturity of governments and businesses. In order to fully take advantage of the Internet of Things and manage the cyber risks that come with it, leaders must ensure the organisation has the right structure, talent and governance today and in the future.

In our digital future, the successful organisation adopts cybersecurity as a business imperative instead of looking at it as an information technology effort. The successful organisation will see cybersecurity for its potential to offer a competitive advantage and as a differentiator — not just a cost burden.