From "Mr. No" towards enthusiastic agile business supporter? Quo vadis cyber security?

Tomáš Kudělka
Director, KPMG

—

17th February 2022

Cost of CyberCrime will increase

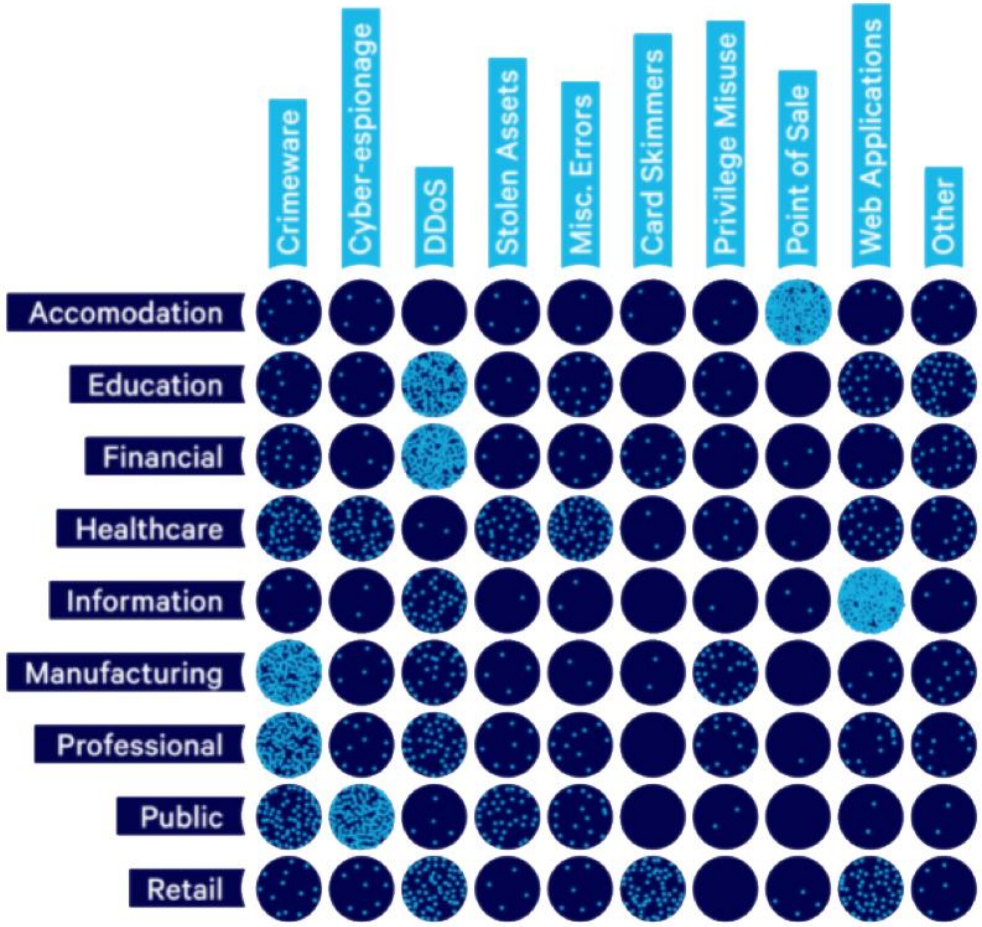
Cybercrime will cost companies worldwide an estimated **$10.5 trillion annually by 2025, up from $3 trillion in 2015.** At a growth rate of 15 percent year over year — Cybersecurity Ventures also reports that **cybercrime represents the greatest transfer of economic wealth in history**.

source: 2021 Must-Know Cyber Attack Statistics and Trends - Embroker

Burdens on CISOs shoulders

Some industries are more vulnerable to cyber attacks than others, simply due to the nature of their business. While any industry could be subject to a data breach, those **most at risk are businesses that are closely involved with people's daily lives.**

On the right side, we can see a matrix that shows which cyberattack method affects which industry the most.



source: 2021 Must-Know Cyber Attack Statistics and Trends - Embroker

There are upcoming more regulations which will require addition security controls to be implemented:

- ISO/IEC 27001 revision
- EU directives: NIS2, DSA, DMA
- Industry specific regulations: PCI DSS, Tisax, etc.

And business is more and more agile and fast moving. **What business men dream of today they want to see in production tomorrow.**

KPMG's annual Cyber security considerations report identifies eight considerations that leaders should prioritize to help mitigate and minimize the impact of cyber-attacks while protecting customers, data and sustainability in a digital world.

Eight key cyber security considerations for 2022

Expanding the strategic security conversation
Change the conversation from cost and speed to effective security to help deliver enhanced business value and user experience.

Achieving the x-factor: Critical talent and skillsets
Transform the posture of CISOs and their teams from cyber security enforcers to influencers.

Adapting security for the cloud
Enhance cloud security through automation — from deployment and monitoring to remediation.

Placing identity at the heart of zero trust
Put IAM and zero trust to work in today's hyperconnected workplace.

Exploiting security automation
Use smart deployment of security automation to help realize business value and gain a competitive advantage.

Protecting the privacy frontier
Move to a multidisciplinary approach to privacy risk management that embeds privacy and security by design.

Securing beyond the boundaries
Transform supply chain security approaches — from manual and time consuming to automated and collaborative.

Reframing the cyber resilience conversation
Broaden the ability to sustain operations, recover rapidly and mitigate the consequences when a cyberattack occurs.

source: Cyber security considerations 2022 - KPMG United Kingdom (home.kpmg)

The modern CISO should think in multiple dimensions: technologist, evangelist, investigator, psychologist, investor and negotiator. They need to align security with business strategy, approach incidents as opportunities and re-frame the way their team works.

Akhilesh Tuteja
Global Cyber Security Leader
KPMG International

Thank you

Tomáš Kudělka
Director, Head of Cyber Security
and Technology

T +420 222 123 197
M +420 724 244 944
tkudelka@kpmg.cz