THINKTANK

Cyberbezpieczeństwo

– zagrożenia dla przedsiębiorstw oraz wyzwania dla kadry zarządzającej

Tomasz Klekowski

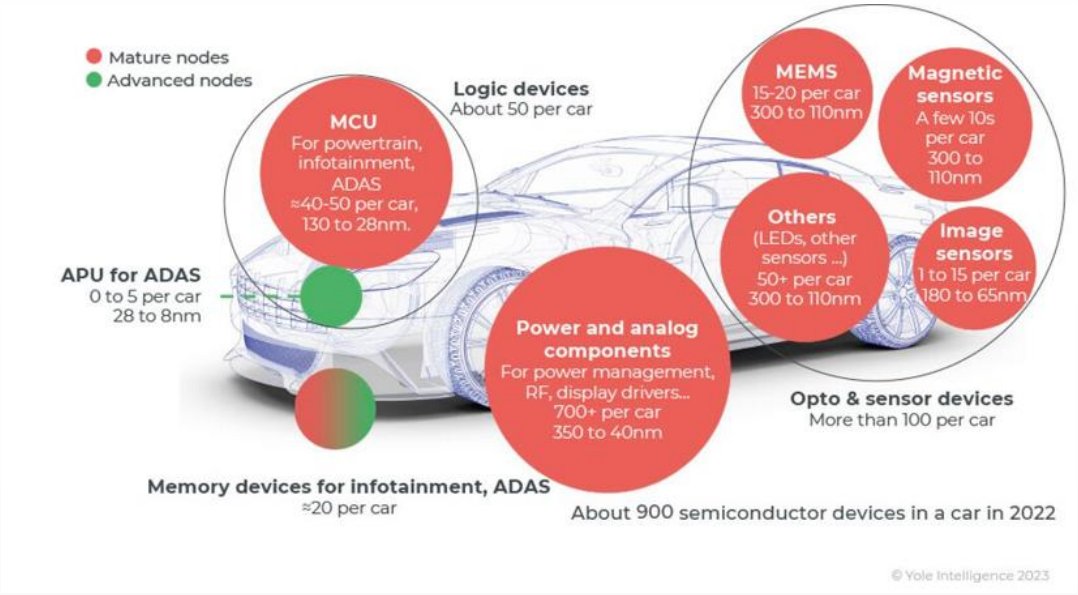
Trzy wymiary transformacji w przemyśle samochodowym

Transformacja produkcji	• Przemysł 4.0
Zmiana produktu	• Ewolucja pojazdu
Zmiana modelu biznesowego	• Ekosystem i infrastruktura

Ewolucja pojazdu

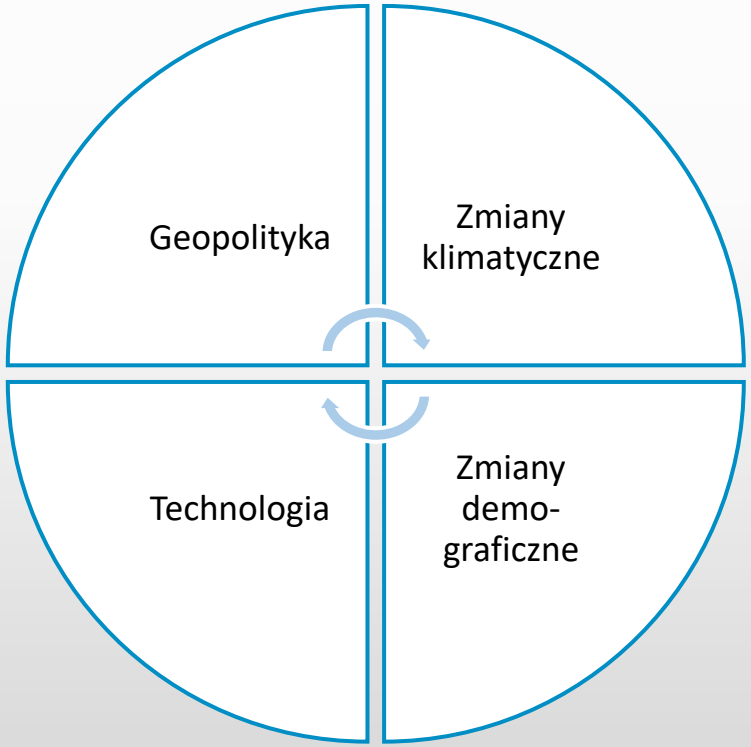
- Więcej układów i funkcji cyfrowych
- Wzrost integracji funkcji cyfrowych
- Ciągłe połączenie z infrastrukturą cyfrową
- Wzrost zależności od oprogramowania

Rosnące znaczenie cyberbezpieczeństwa

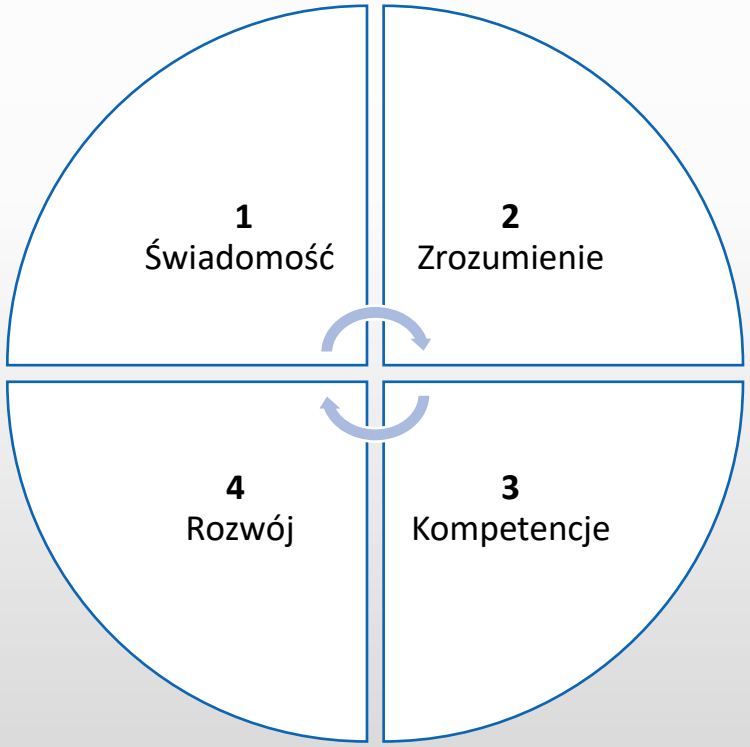


Jakie największe zmiany wpływają na nasz świat?

Tempo zmian



Znaczenie dla każdego z nas



Strategiczny kontekst cybersecurity

- Poziom świadomości zależności od technologii cyfrowych w poszczególnych obszarach działalności przedsiębiorstwa jest zróżnicowany
- Cybersecurity jest głównie widziane jako domena techniczna
  - Raport Trend Micro: głównie jako domena techniczna (41%),
  - Całkowicie jako domena techniczna (21%)
- Nie ma wystarczającego powiązania głównych inicjatyw biznesowych z wymaganiami cybersecurity
  - Tylko 23% firm deklaruje, że wymagania cybersecurity należą do głównych czynników podczas projektowania nowych inicjatyw biznesowych

Główne rekomendacje:

•Utworzyć rolę Business Information Security Officer (BISO) celem poprawy współpracy z funkcjami biznesowymi

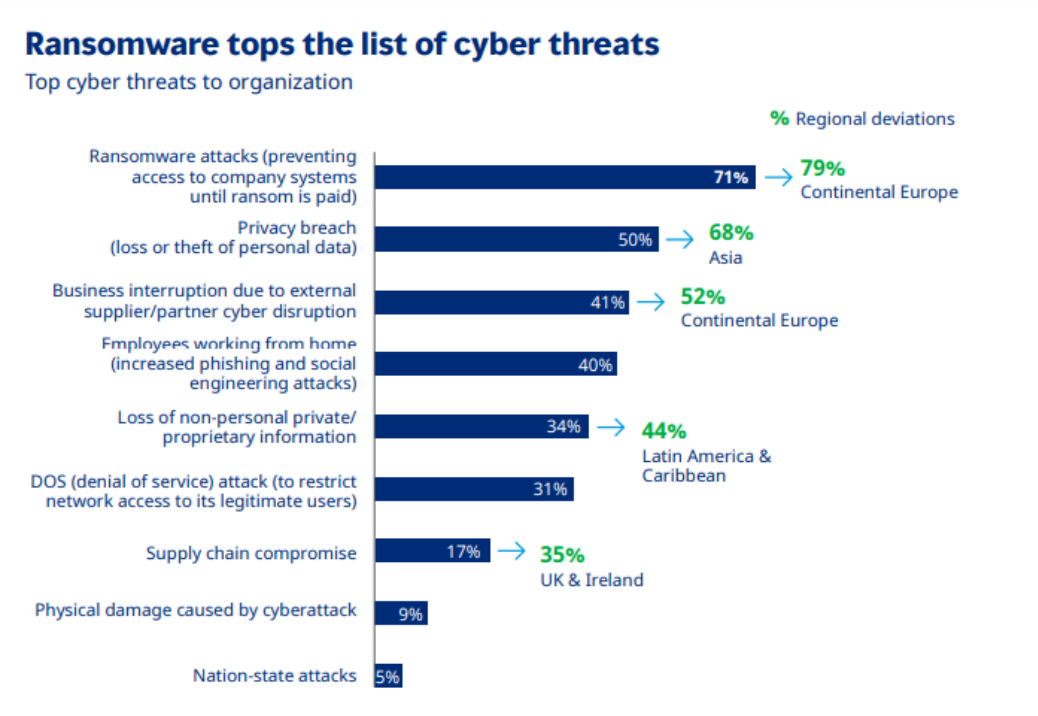
•Tworzyć całościowe programy zapewnianie bezpieczeństwa cybernetycznego, z mierzalnymi wskaźnikami, które mogą stanowić podstawę regularnych przeglądów z Zarządem.

• Zdefiniować rolę CISO jako bezpośredniego współpracownika CEO.

Źródło: https://www.helpnetsecurity.com/2021/02/01/board-members-cybersecurity/

Cybersecurity z perspektywy zarządczej

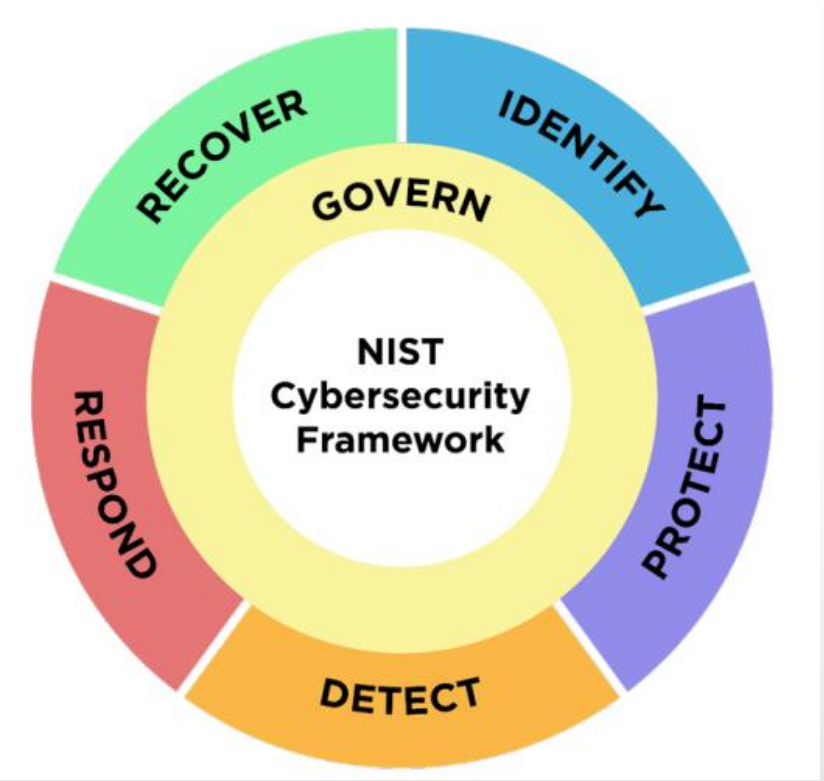
- 73% organizacji było obiektem cyberataku
- Tylko 41% organizacji angażuje w tworzenie planów oceny ryzyka cybernetycznego działy prawne, finansowe, operacyjne i zarządzania łańcuchem dostaw
- Tylko 26% respondentów stwierdziło, że ich organizacja stosuje mierniki finansowe w zakresie oceny ryzyka cybernetycznego
- 53% organizacji uważa, że największą barierą w ocenie ryzyka cybernetycznego jest brak odpowiednich pracowników/umiejętności, aby to zrobić



The state of cyber resilience 2022.
https://www.marsh.com/dk/en/services/cyber-risk/insights/the-state-of-cyber-resilience.html

Kamień węgielny organizacji procesów cybersecurity - Matryca NIST

- Spójny, powszechnie używany język opisu
- Obejmuje szeroki zakres technologii, sektorów, etapów rozwoju
- Oparty o ocenę ryzyka
- Oparta o międzynarodowe standardy
- Regularnie aktualizowana
- Wynik współpracy sektora publicznego, prywatnego i naukowego



The National Institute of Standards and Technology - https://www.nist.gov/cybersecurity

Zalecenia dla zarządów

- Edukacja zarządu i kierownictwa i zrozumienie skali zagrożeń i ryzyka
- Zrozumienie struktury wymagań dla cybersecurity – (NIST, ISO27001)
- Budowa wspólnego i spójnego systemu pojęć
- Przypisanie adekwatnej odpowiedzialności członkom zarządu kluczowych obszarów firmy
- Ustalenie wysokiego priorytetu dla cyberbezpieczeństwa, jako jedenego z kluczowych obszarów ryzyka
- Stworzenie struktury audytu ryzyka, okresowej oceny, testów i korekt
- Rozwój kultury Security by Design

Zarządy formułujące nadzór nad bezpieczeństwem cybernetycznym powinny wprowadzić te same procedury zarządzania w celu nadzorowania bezpieczeństwa cybernetycznego korporacji, które okazały się skuteczne i wystarczająco elastyczne, aby ocenić i zweryfikować dokładność i wiarygodność sprawozdań finansowych.

Harvard Business School: Cybersecurity: The SEC's Wake-up Call to Corporate Directors (harvard.edu) April 2018

https://www.ncsc.gov.uk/collection/board-toolkit/introduction-to-cyber-security-for-board-members#:~:text=Board%20members%20can%20ensure%20that,security%2C%20aligned%20to%20business%20risks

Dziękuję za uwagę

Tomasz Klekowski – tomasz.klekowski@insead.edu

- Partner: ThinkTank.pl
- Inicjator i kierownik kierunku: Biznes.ai – Technologia, Prawo, Zastosowania Sztucznej Inteligencji – Akademia Leona Koźmińskiego
- Founding member: Inteligent Leadership Hub
- Ekspert: Doradca Urzędu Regulacji Energetyki, Grupa Robocza AI przy KPRM (GRAI),
- Mentor i Inwestor: SMOK Ventures, Małopolska Agencja Rozwoju Regionalnego, Coachwise, AIESEC
- Rady: Sektorowa Rada ds. Kompetencji Informatyki, Sektorowa Rada ds. Kompetencji Telekomunikacji i Cyberbezpieczeństwa
- Wykładowca: Akademia Leona Koźmińskiego, Politechnika Śląska, Smart MBA
- Kolegia nagród: NEW@POLAND, PoLAND of IT Masters, Członek Rady Programowej Konkursu Fabryka Przyszłości
- Wybrany do grupy 100 osób o największym wpływie na rozwój kompetencji cyfrowych w Polsce – PTI TOP 100

- Doświadczenie:
- Intel, EMEA Director of Market Development Data Center and IoT
  - AI, Big Data Analytics, Cloud, Cybersecurity, IoT
  - Automotive, FSI, Manufacturing, Retail, Telecommunication
- Intel Central Eastern Europe General Manager
- Retail, enterprise, distribution, OEM,
- Interim management
- Wiceprezydent Konfederacji Lewiatan
- Rada Fundacji Platforma Przemysłu Przyszłości,

AKADEMIA LEONA KOŹMIŃSKIEGO

Sektorowa Rada ds. Kompetencji Informatyka

LISTA 100 '2019

Platforma Przemysłu Przyszłości

ZWIĄZEK PRACODAWCÓW TECHNOLOGII CYFROWYCH LEWIATAN

THINKTANK