Kompetencje cyfrowe. Dlaczego warto postawić na cyberbezpieczeństwo?

NIKOLA BOCHYŃSKA,
DIGITAL EU AMBASSADOR,
REDAKTOR NACZELNA
CYBERDEFENCE24.PL

KOMPETENCJE CYFROWE

W 2018 r. Rada Europejska: kompetencje cyfrowe jako obejmujące "pewne, krytyczne i odpowiedzialne korzystanie z technologii cyfrowych i interesowanie się nimi do celów uczenia się, pracy i udziału w społeczeństwie".

Umiejętność korzystania z informacji i danych, komunikowania się i współpracy, korzystania z mediów, tworzenia treści cyfrowych, w tym programowania, znajomości zagadnień bezpieczeństwa cyfrowego czy własności intelektualnej

Dostosowanie się do szybko zmieniającego się świata

FUNDAMENTALNE UMIEJĘTNOŚCI

Wiedza + umiejętności cyfrowe

Kompetencje cyfrowe to jedna z fundamentalnych umiejętności współczesnego człowieka. Niezbędna w pracy, do np. kontaktu z bankiem, urzędem czy w relacjach z bliskimi

Trwa „technologiczny wyścig zbrojeń" - kompetencje odgrywają równie ważną rolę jak sama technologia – kluczowy jest CZŁOWIEK

DLACZEGO SĄ WAŻNE?

Niezbędne w codziennej pracy, procesu uczenia się, w rozwoju społecznym, ale i zawodowym

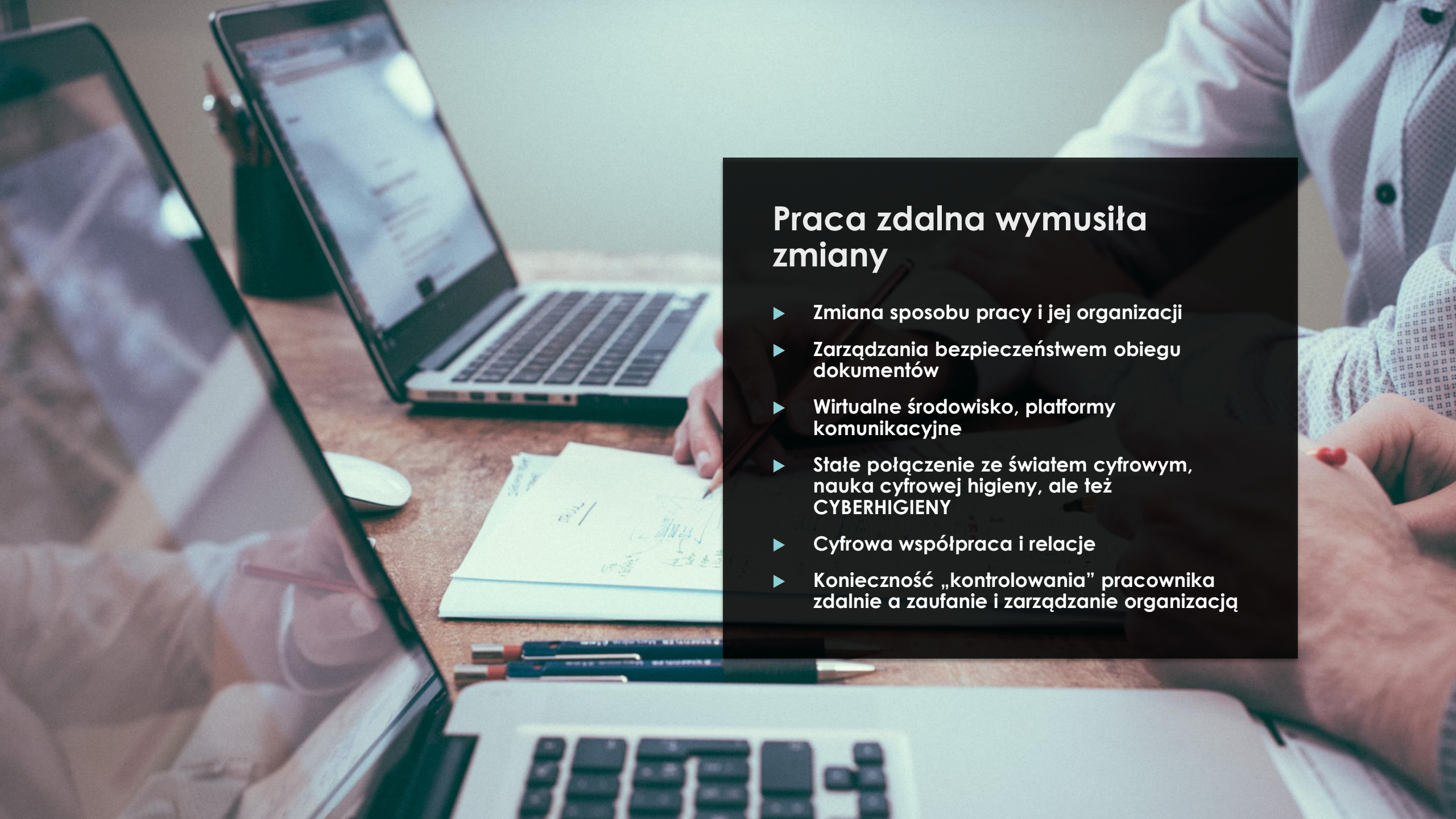
Poziom kompetencji cyfrowych wpłynie na konkurencyjność, efektywność, a także na innowacyjność organizacji/instytucji/firm

Technologie cyfrowe mają coraz większy wpływ na rynek pracy

W coraz większym stopniu wpływają na relacje społeczne

Do 2030 roku: automatyzacja wpłynie na nawet do 49 proc. czasu pracy w Polsce

9 na 10 współczesnych zawodów wymaga podstawowych kompetencji cyfrowych (dane: Agencja Rozwoju Przemysłu)



Praca zdalna wymusiła zmiany

- Zmiana sposobu pracy i jej organizacji
- Zarządzania bezpieczeństwem obiegu dokumentów
- Wirtualne środowisko, platformy komunikacyjne
- Stałe połączenie ze światem cyfrowym, nauka cyfrowej higieny, ale też CYBERHIGIENY
- Cyfrowa współpraca i relacje
- Konieczność „kontrolowania” pracownika zdalnie a zaufanie i zarządzanie organizacją

CYFROWY KOMPAS, CZYLI DOKĄD ZMIERZAMY?

W 2021 roku Komisja Europejska przedstawiła tzw. Cyfrowy kompas – wizję rozwoju w UE pod względem transformacji cyfrowej.

Założenie: do początku kolejnej dekady podstawowe umiejętności cyfrowe mieć będzie przynajmniej 80 proc. ludności, liczba wykwalifikowanych specjalistów cyfrowych do 2030 roku wzrośnie z ponad 8 mln do 20 mln, zwiększy się w tym sektorze równowaga płci.

Dlaczego? Ponieważ dla ponad 2/3 europejskich firm przeszkodą w rozwoju jest brak personelu o odpowiednich umiejętnościach cyfrowych oraz świadomość

Europa wciąż boryka się z niedoborem ekspertów ds. cyber, obszaru cyfryzacji & tech.

- W 2019 roku 1/3 dorosłych pracujących lub poszukujących pracy w UE – łącznie ponad 75 mln ludzi – nie posiadała żadnych umiejętności cyfrowych

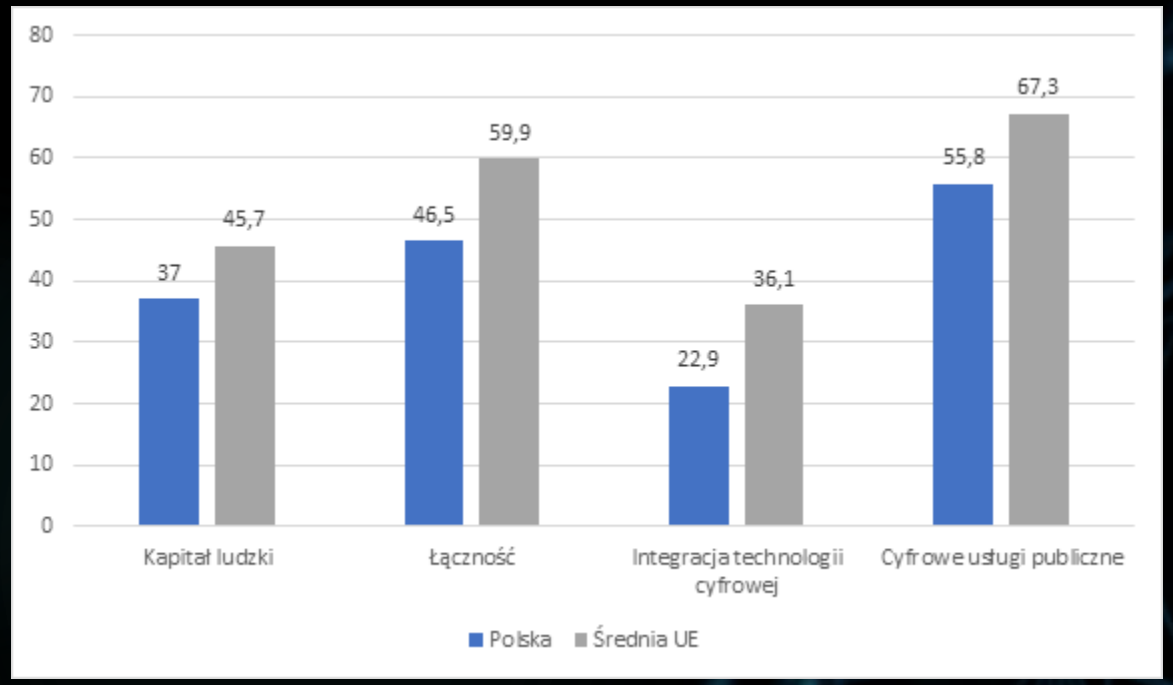
PRZEWAGĘ ZDOBYWAJĄ FIRMY/ORGANIZACJE, KTÓRYCH PRACOWNICY…

- … mają kompetencje **kluczowe, kompetencje 4.0 i kompetencje przyszłości**
  - **kluczowe**:(Rada UE: kompetencje w zakresie rozumienia i tworzenia informacji; technologii i inżynierii; **cyfrowe**, w zakresie uczenia się
  - **Kompetencje 4.0**: przydatne w przemyśle 4.0 czyli np. chmura obliczeniowa, sztuczna inteligencja, Big Data, Internet Rzeczy (IoT)
  - **Kompetencje przyszłości**: kreatywność, rozwiązywanie złożonych problemów, analizowanie danych czy współpraca w zespole

JAKIE UMIEJĘTNOŚCI WARTO ROZWIJAĆ?

- Odporność cyfrowa
- Płynność, biegłość cyfrowa
- Cyfrowy sposób myślenia (digital mindset) – świadomość możliwości, ale też zagrożeń i ograniczeń, jakie niosą ze sobą technologie
- Kreatywność do działania w cyfrowej rzeczywistości pomaga w radzeniu sobie w szybko zmieniającym się świecie
- Chęć stałego uczenia się i rozwoju, podnoszenia swoich kompetencji

KOMPETENCJE CYFROWE



Polska na świecie

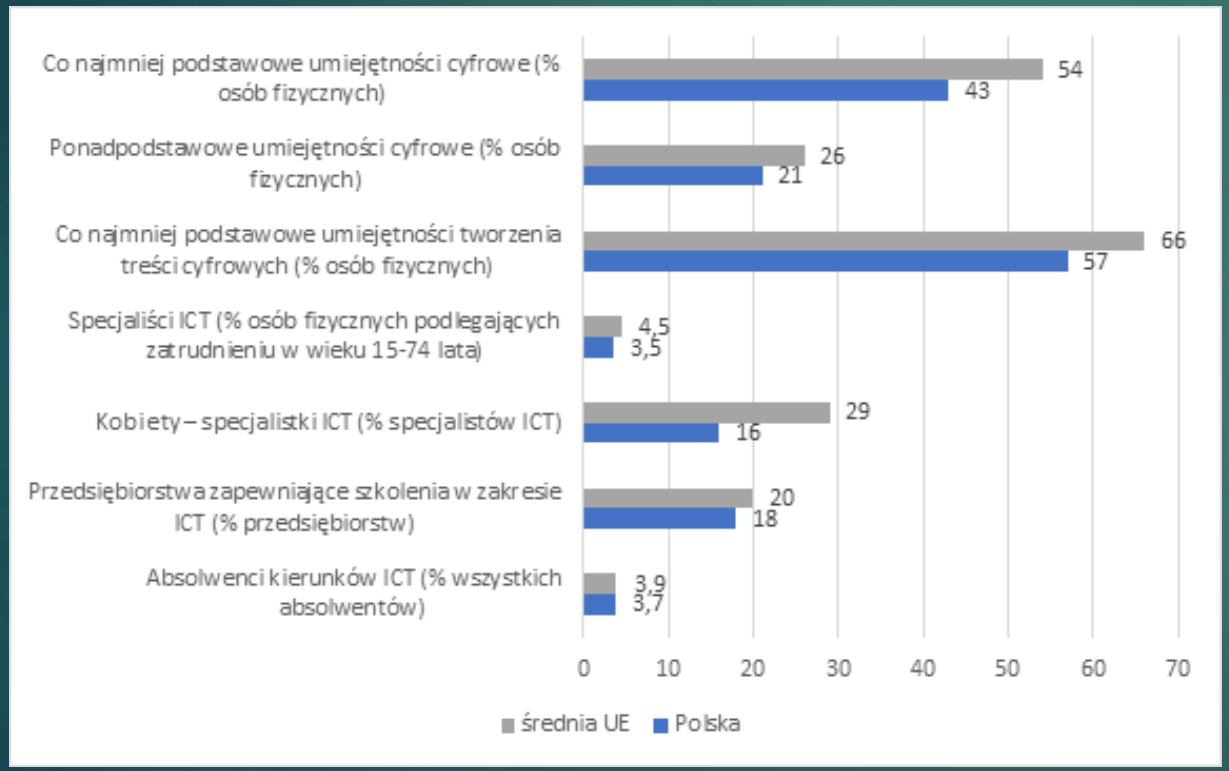
Komisja Europejska w rankingu DESI (Digital Economy and Society Index_ sprawdza cztery obszary: kapitał ludzki, łączność, integrację technologii cyfrowej oraz cyfrowe usługi publiczne.

Polska osiągnęła w tym roku ogólny wynik 40.5, podczas gdy średnia europejska wynosi 52.

KE: konieczne są dalsze działania, w szczególności ukierunkowane na zwiększenie liczby specjalistów ICT i podnoszenie poziomu kompetencji cyfrowych społeczeństwa polskiego.

Kapitał ludzki, czyli CZŁOWIEK

Dane za 2022 dla Polski w obszarze kapitału ludzkiego:



- Powyższe dane pokazują, że w zakresie kapitału ludzkiego w tegorocznym rankingu, Polska plasuje się poniżej średniej w każdym z badanych obszarów.
- **Pozostaje również na 24. miejscu wśród 27 państw Unii.**

KOMPETENCJE CYFROWE KSZTAŁTUJEMY OD NAJMŁODSZYCH LAT

IT Fitness TEST

W ostatnich miesiącach w krajach Grupy Wyszehradzkiej, w tym w Polsce, przeprowadzano IT Fitness Test.

Sprawdzenie umiejętności cyfrowych uczniów i nauczycieli.

Na tle pozostałych państw zajęliśmy trzecie miejsce pod względem kompetencji cyfrowych.

Najlepiej w polskich szkołach poradzono sobie z pytaniami z zakresu cyberbezpieczeństwa.

- W szkołach podstawowych test wypełniło 14 715 osób i średni wynik wyniósł 45,32 proc.
- Natomiast w szkołach ponadpodstawowych test wypełniło 15 676 uczestników (średni wynik był znacznie gorszy i wyniósł 41,12 proc.
- Najgorzej z narzędzi biurowych oraz umiejętności posługiwania się social mediami.

KOMPETENCJE PRZYSZŁOŚCI

Prognozy – ilu zawodów nie będzie?

Według raportu Światowego Forum Ekonomicznego "The Future of Jobs Report 2020", do 2025 roku automatyzacja i nowy podział pracy między ludzi i maszyny skutkować będą likwidacją nawet 85 mln miejsc pracy.

Jednocześnie, ze względu na rozwój nowych technologii, pojawi się blisko 100 mln nowych miejsc pracy.

Zapotrzebowanie kontra braki kadrowe

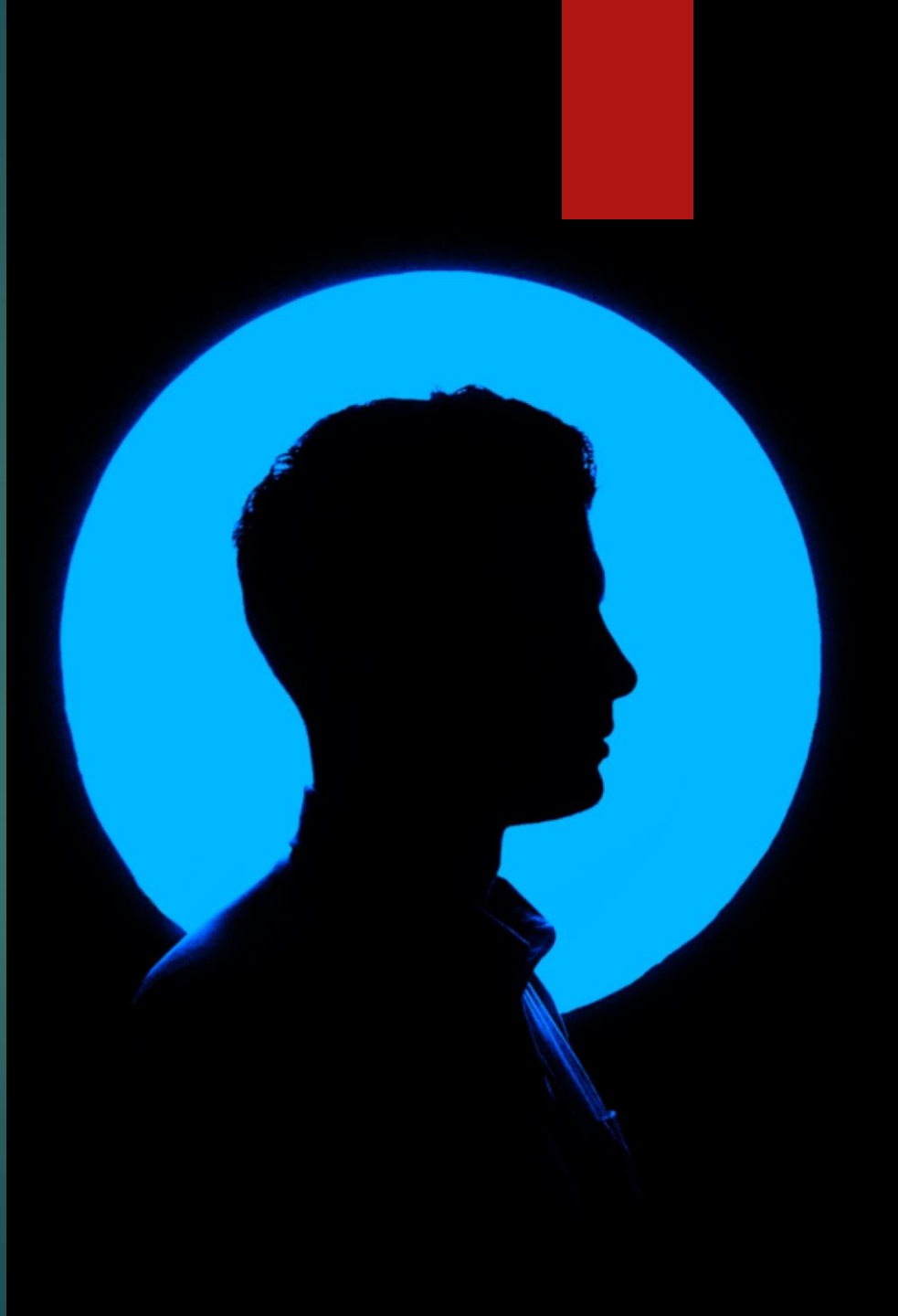
JAKI ROZWÓJ KOMPETENCJI CYFROWYCH?

Z JEDNEJ STRONY: ZAPOTRZEBOWANIE NA KOMPETENCJE CYFROWE STALE ROŚNIE, A PORUSZANIE SIĘ W CYFROWEJ RZECZYWISTOŚCI STAJE SIĘ TAK SAMO WAŻNE JAK UMIEJĘTNOŚĆ CZYTANIA I PISANIA

Z DRUGIEJ STRONY: DEFICYTY KOMPETENCJI CYFROWYCH MOŻNA ZNALEŹĆ W PRAKTYCZNIE KAŻDEJ GRUPIE ZAWODOWEJ + BRAKI KADROWE NA RYNKU PRACY

KLUCZOWE KOMPETENCJE, BO KLUCZOWY JEST CZŁOWIEK

- Wyzwaniem jest stałe nadążanie za technologią
  - Liczą się chęci, ale i predyspozycje
- Rozwijają się te organizacje, których szefowie są otwarci na wdrażanie nowych narzędzi i reagują na światowe trendy + dodatkowo kwestia oferowania produktu i usługi



Kompetencje cyfrowe możesz rozwijać sam/a

- rozwijanie podstawowych umiejętności korzystania z informacji i danych, niezbędnych przy wyszukiwaniu, przeglądaniu i filtrowaniu w sieci informacji, na przykład o towarach i usługach
- rozwijanie umiejętności korzystania z wyszukiwarek
- strategie zdobywania informacji
- krytyczna ocena jakości i wiarygodności źródeł
- korzystanie z aplikacji odpowiednich do rodzaju wykonywanej pracy
- obsługa baz danych i arkuszy kalkulacyjnych
- umiejętność pracy online i współpraca z innymi

STAŁY ROZWÓJ TO DZIŚ KONIECZNOŚĆ

- Najnowszy raport Google: większość Polaków nie chce się szkolić - tylko niecała ¼ bierze udział w spotkaniach edukacyjnych z tego zakresu


KOMPETENCJE
CYFROWE
A CYBER-
BEZPIECZEŃSTWO

FINANSOWANIE

Pieniądze na cyberbezpieczeństwo w samorządach

Projekt ustawy o szczególnych rozwiązaniach służących realizacji ustawy budżetowej na rok 2023 przewiduje wsparcie finansowe jednostek samorządu terytorialnego w związku z realizacją przez nie zadań i celów dotyczących cyberbezpieczeństwa

Był program „Cyfrowa Gmina", w 2023 roku ma być program „Cyfrowy Samorząd"

1) W 2023 roku NASK-PIB może utworzyć ze środków funduszu rezerwowego, w wysokości do 10 proc. tego funduszu za poprzedni rok obrotowy - **Fundusz wsparcia jednostek samorządu terytorialnego**

2) Minister odpowiedzialny za obszar informatyzacji „może przekazać z części budżetu państwa, której jest dysponentem, jednostce samorządu terytorialnego środki na realizację zadań z zakresu cyberbezpieczeństwa". Ustawa mówi wprost: przekazanie pieniędzy odbywa się w formie **dotacji celowej.**

ZNAMY TE INCYDENTY...

- Incydent w gminie Kościerzyna przed Bożym Narodzeniem w 2019 roku (Dane urzędu zostały zaszyfrowane. Za odszyfrowanie plików przestępcy żądali okupu)

- Zaszyfrowanie serwerów samorządowych powiatu oświęcimskiego w 2020 roku

- Na początku 2021 roku - urząd marszałkowski województwa małopolskiego (zaszyfrowanie danych)

URZĄD MARSZAŁKOWSKI WOJEWÓDZTWA MAZOWIECKIEGO W WARSZAWIE

- **Incydent** został stwierdzony **5 grudnia 2022 r.** polegał na **ataku złośliwego oprogramowania** szyfrującego pliki (**ransomware**)
- „Co ważne jednak, atak **nie ma wpływu na funkcjonowanie** samego **UMWM**. **Może mieć** jednak **wpływ** na funkcjonowanie **jednostek samorządu terytorialnego**, które korzystają z systemów informatycznych, dostarczanych w ramach projektów” – podawano w komunikacie.

KONIECZNOŚĆ ZGŁASZANIA INCYDENTÓW

Jakie obowiązki na podmioty publiczne nakłada ustawa o krajowym systemie cyberbezpieczeństwa?

Zgłoszenie osób do kontaktu z właściwym zespołem CSIRT poziomu krajowego

Zgłaszanie incydentu - najpóźniej w terminie do 24 godzin od jego wykrycia - do właściwego zespołu CSIRT

Zapewnienie obsługi incydentu

Gdzie samorządy powinny zgłaszać incydenty?

Właściwym zespołem CSIRT dla jednostek samorządu terytorialnego jest zespół CSIRT NASK

KONSEKWENCJE ATAKÓW

DLACZEGO WARTO POSTAWIĆ NA CYBERBEZPIECZEŃSTWO?

WZROST LICZBY CYBERATAKÓW

Liczba cyberataków w III kw. 2022 wzrosła w porównaniu do III kw. 2021 **o 28 proc**. W przypadku Polski wzrost wynosił 22 proc.

Średnia liczba ataków na przeciętną polską organizację wzrosła i wynosi niemal 1100 tygodniowo. Najgorzej sytuacja wyglądała na przełomie września i października. Wówczas odnotowywano nawet 1370 ataków w ciągu tygodnia.

Jeśli chodzi o Polskę, tu dominują **ataki na sektor użyteczności publicznej** (ponad 1300 incydentów).

[Analiza Check Point Research]

„CYBERWOJNA” TRWA?

- Aż 83 proc. firm ankietowanych w najnowszym raporcie ESET Digital Security Sentiment ocenia, że „cyberwojna jest bardzo realnym zagrożeniem, które może dotknąć każdego”, co sugeruje, że stale rosnące zagrożenia znacząco wpływają na nastroje wśród przedstawicieli MŚP.
- Jak wskazuje ESET, ocena wyników badania cyberbezpieczeństwa firm w 2022 roku wskazuje na **brak skutecznej strategii cyberbezpieczeństwa**, która zlikwiduje niedociągnięcia i zwiększy poziom odporności na cyberataki.

CO NA TO FIRMY?

- RAPORT ESET: Nawet **74 proc. małych i średnich firm** w Europie i Ameryce Północnej uważa, że są bardziej podatne na cyberataki niż duże przedsiębiorstwa.
- Co jest przyczyną tych obaw? Zaskakującą informacją może być to, że MŚP widzą główną przyczynę **w braku wiedzy ich pracowników z zakresu cyberbezpieczeństwa.**

REALNE RYZYKO DLA BIZNESU

2/3 respondentów potwierdziło, że cyberzagrożenia są dla nich jednym z trzech najważniejszych ryzyk, a prawie 80 proc. badanych stwierdziło, że bez dostępu do usług IT nie są w stanie kontynuować prowadzonej przez siebie działalności.

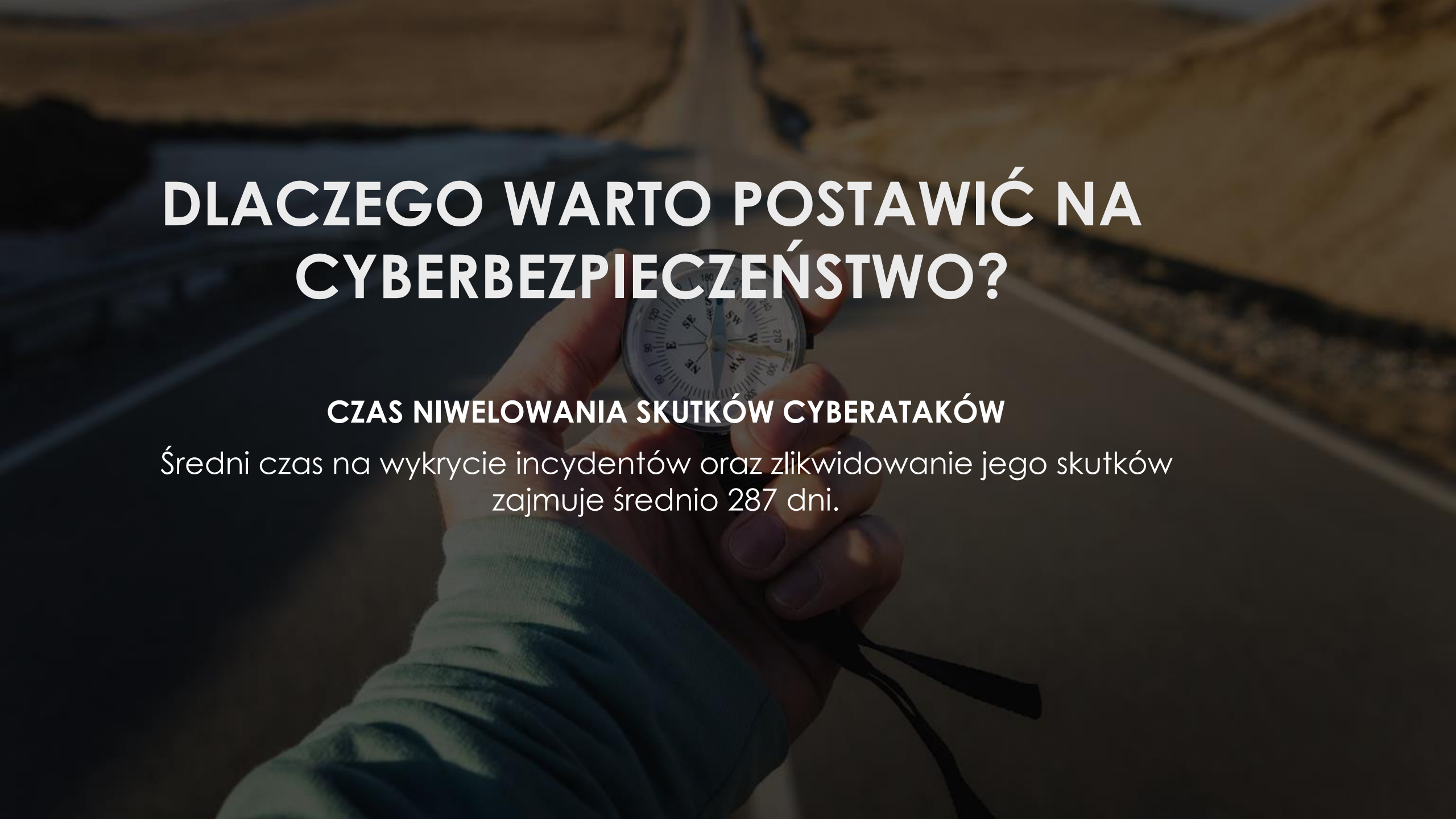
Raport potwierdził także powszechność cyberataków. **70 proc. badanych firm odnotowało incydenty z zakresu cyberbezpieczeństwa.** To ze 30 proc. respondentów incydentów takich nie odnotowało, nie oznacza wcale, ze nie padły one ofiarami takich ataków.

[Wspólny raport Kancelarii DGTL Kibil Piecuch i Wspólnicy i portalu CyberDefence24.pl „Zwarci, silni, gotowi? Polskie firmy w obliczu cyberzagrożeń.”]

DLACZEGO WARTO POSTAWIĆ NA CYBERBEZPIECZEŃSTWO?

KOSZTY CYBERATAKÓW

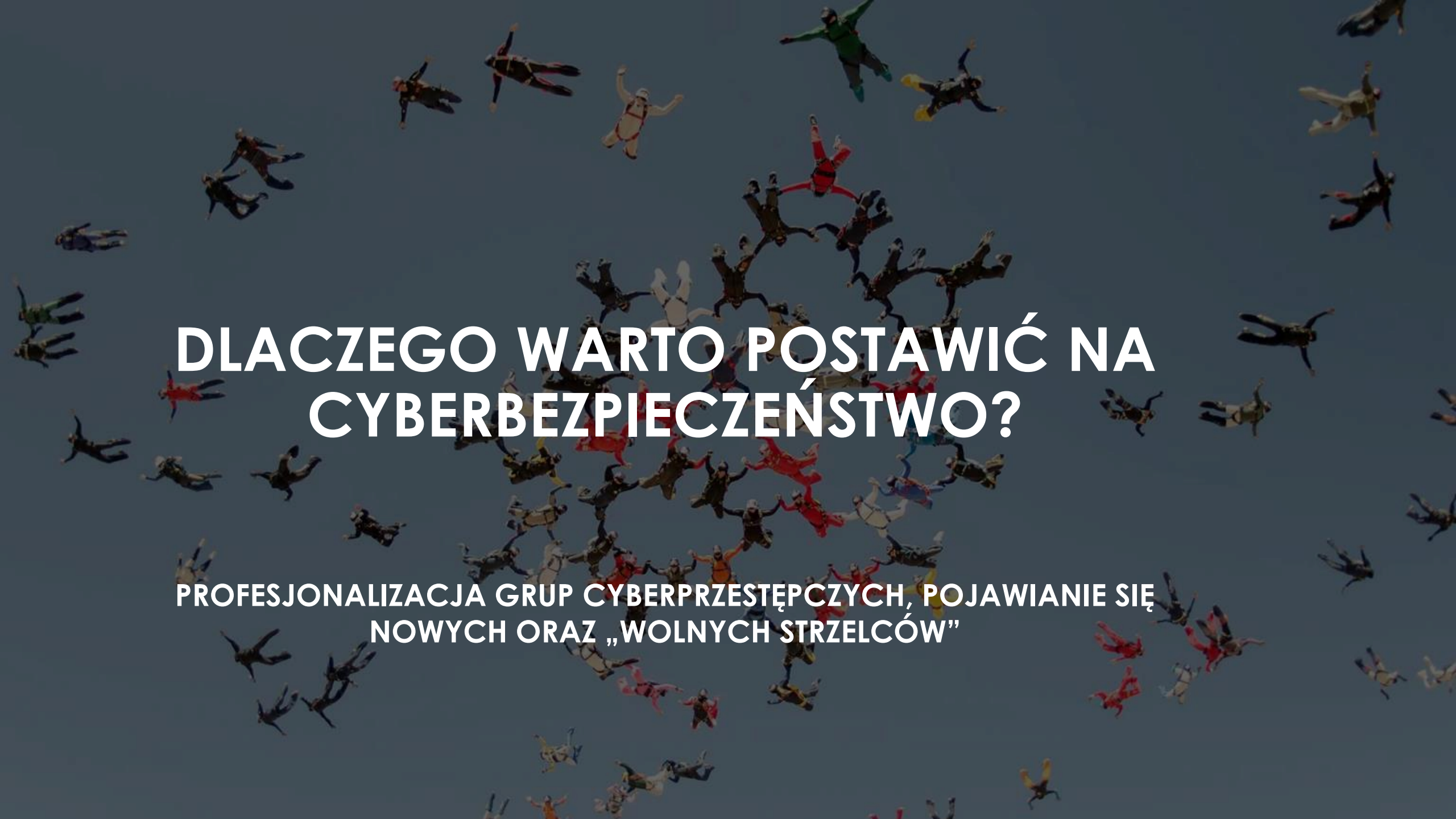
Ponad 2/3 z 1200 pytanych firm (w tym 59 proc. polskich) doświadczyło w ciągu ostatniego roku incydentu związanego z bezpieczeństwem IT. Jego średni szacunkowy koszt wyniósł niemal 220 tys. euro, czyli ponad 1 mln złotych - wynika z raportu ESET na temat bezpieczeństwa cyfrowego MŚP.



DLACZEGO WARTO POSTAWIĆ NA CYBERBEZPIECZEŃSTWO?

CZAS NIWELOWANIA SKUTKÓW CYBERATAKÓW

Średni czas na wykrycie incydentów oraz zlikwidowanie jego skutków zajmuje średnio 287 dni.

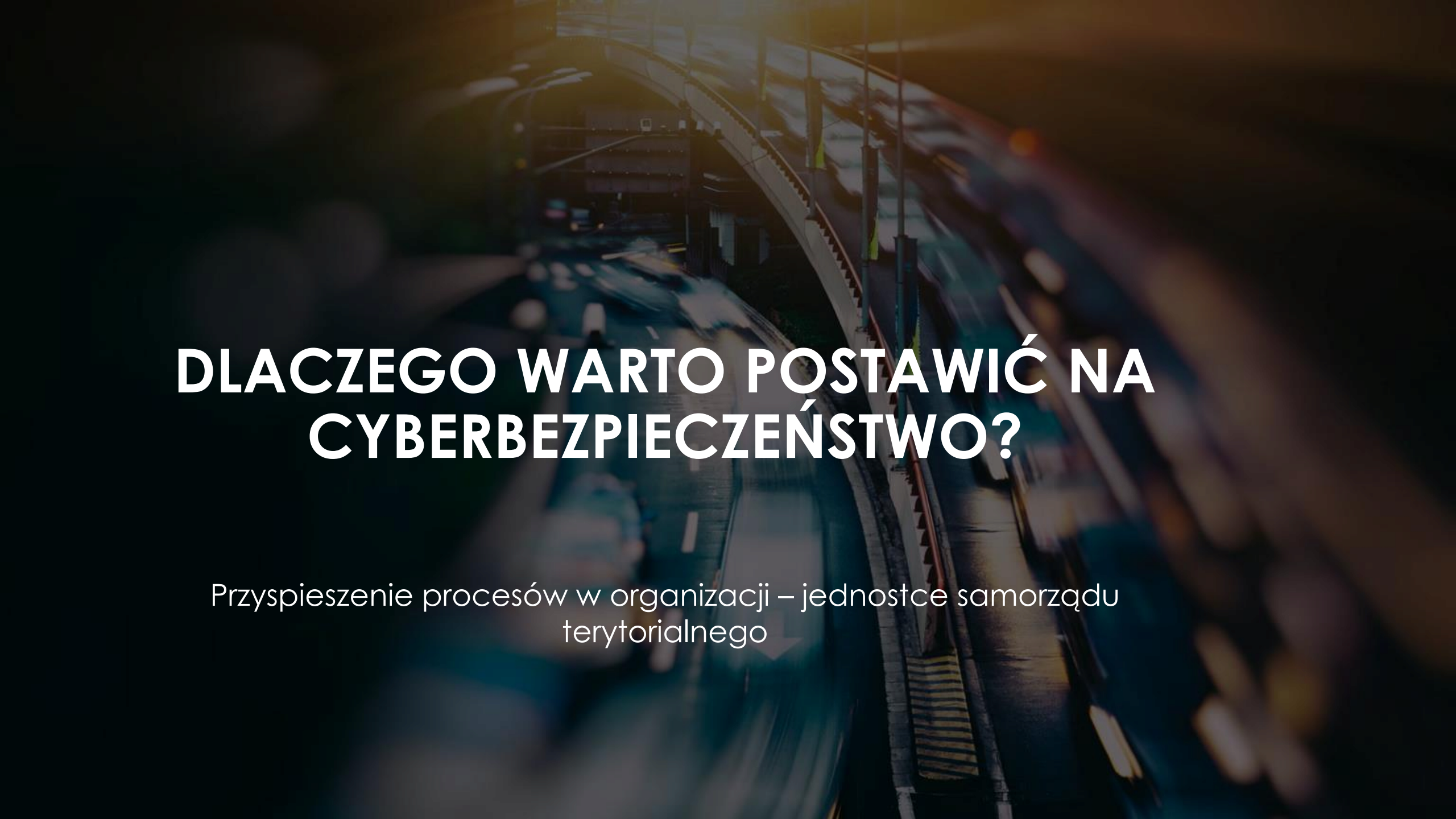


DLACZEGO WARTO POSTAWIĆ NA CYBERBEZPIECZEŃSTWO?

PROFESJONALIZACJA GRUP CYBERPRZESTĘPCZYCH, POJAWIANIE SIĘ NOWYCH ORAZ „WOLNYCH STRZELCÓW”

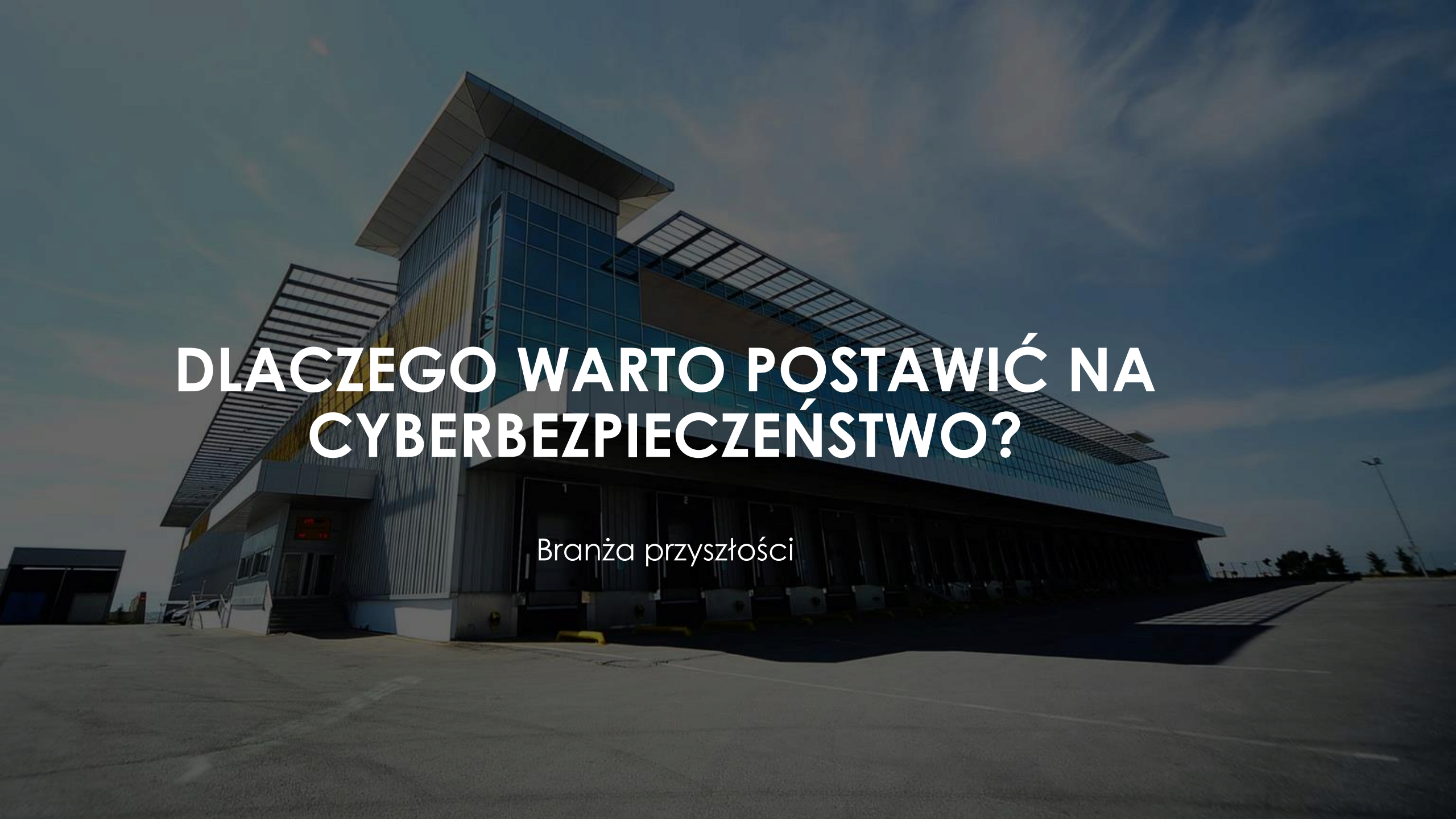
DLACZEGO WARTO POSTAWIĆ NA CYBERBEZPIECZEŃSTWO?

- Utrzymujący się wysoki poziom zagrożenia w cyberprzestrzeni – w Polsce obowiązujący trzeci stopień alarmowy CHARLIE-CRP



DLACZEGO WARTO POSTAWIĆ NA CYBERBEZPIECZEŃSTWO?

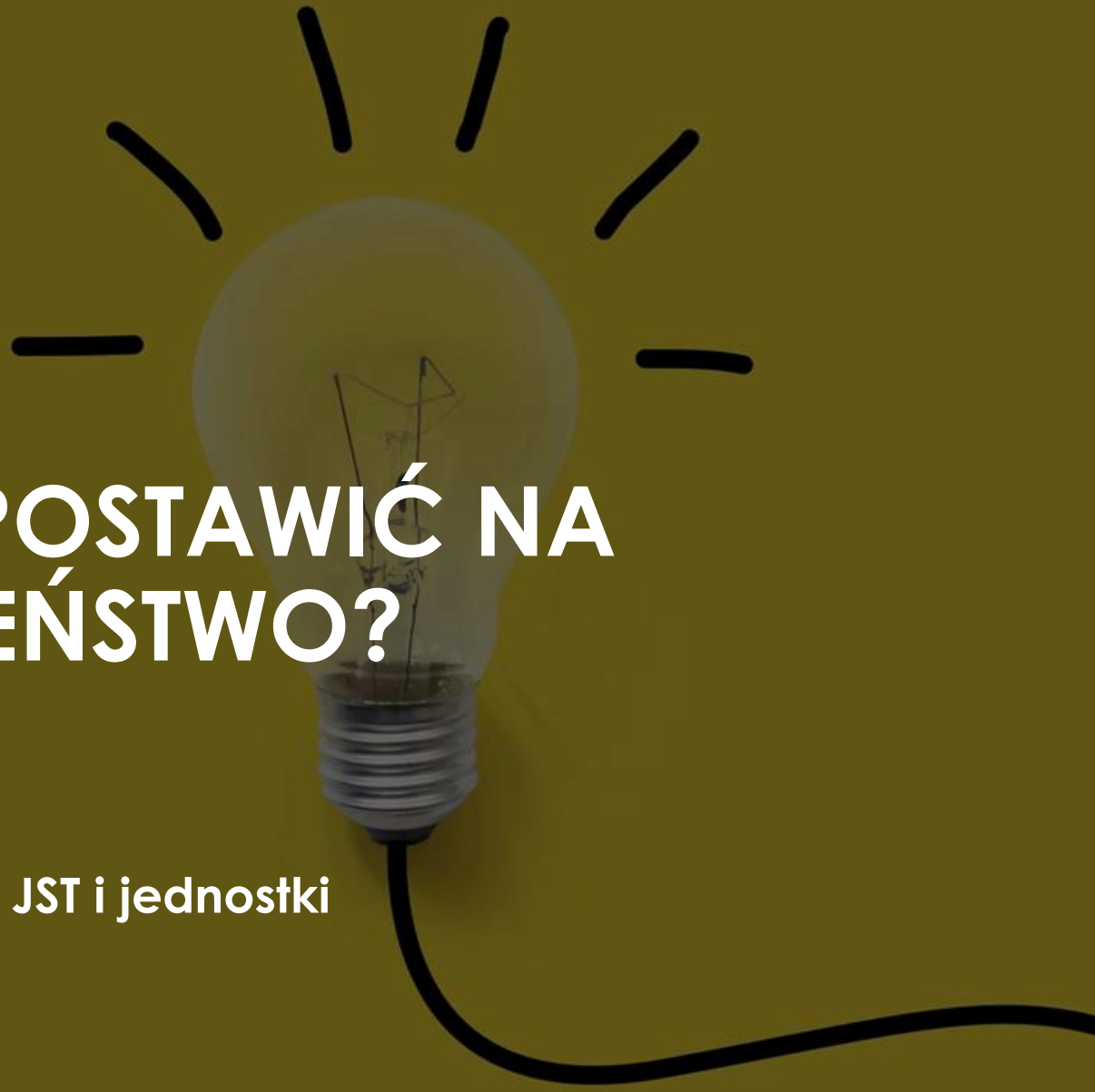
Przyspieszenie procesów w organizacji – jednostce samorządu terytorialnego



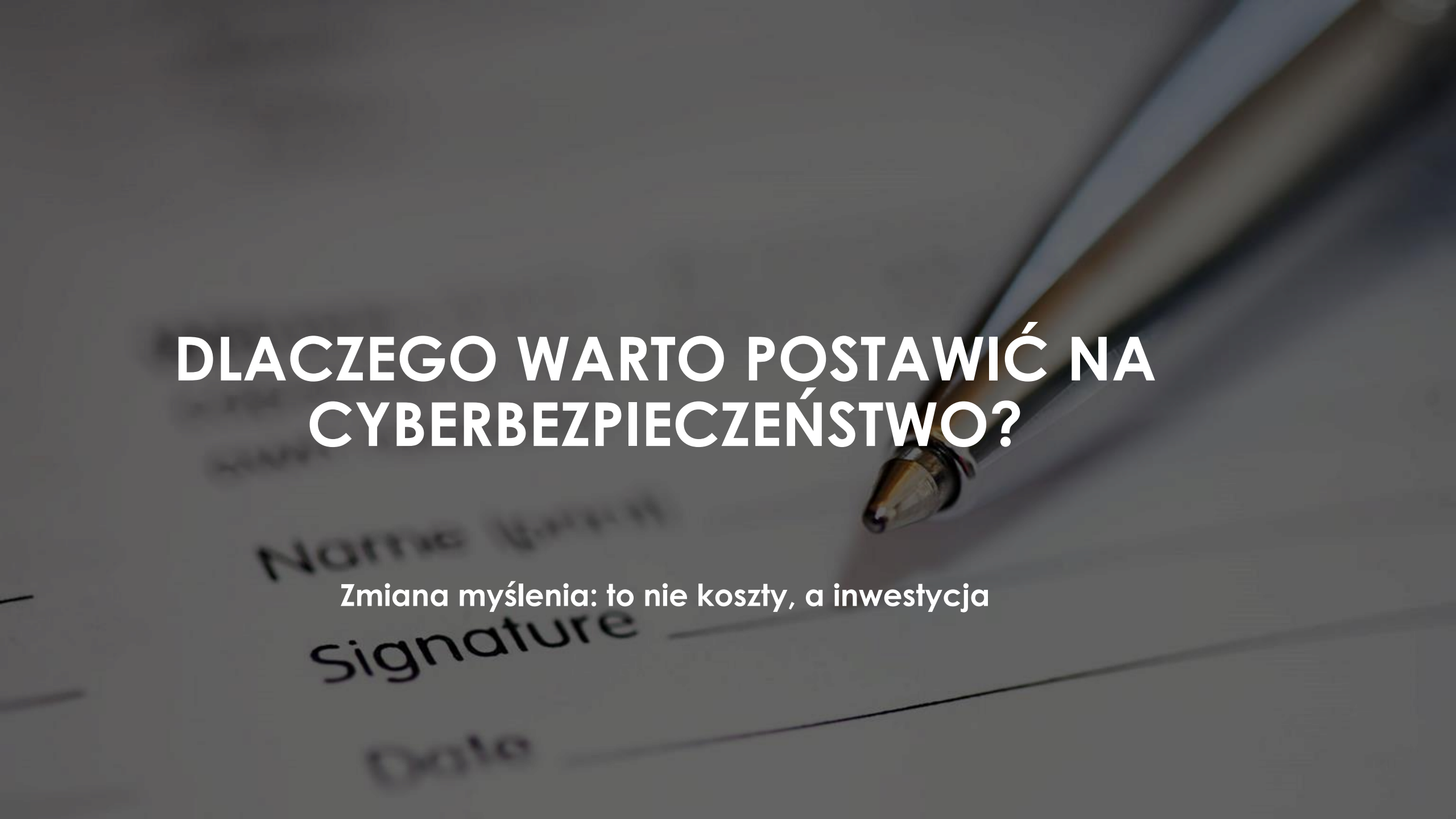
DLACZEGO WARTO POSTAWIĆ NA CYBERBEZPIECZEŃSTWO?

Branża przyszłości

DLACZEGO WARTO POSTAWIĆ NA CYBERBEZPIECZEŃSTWO?



Możliwość stałego rozwoju – JST i jednostki

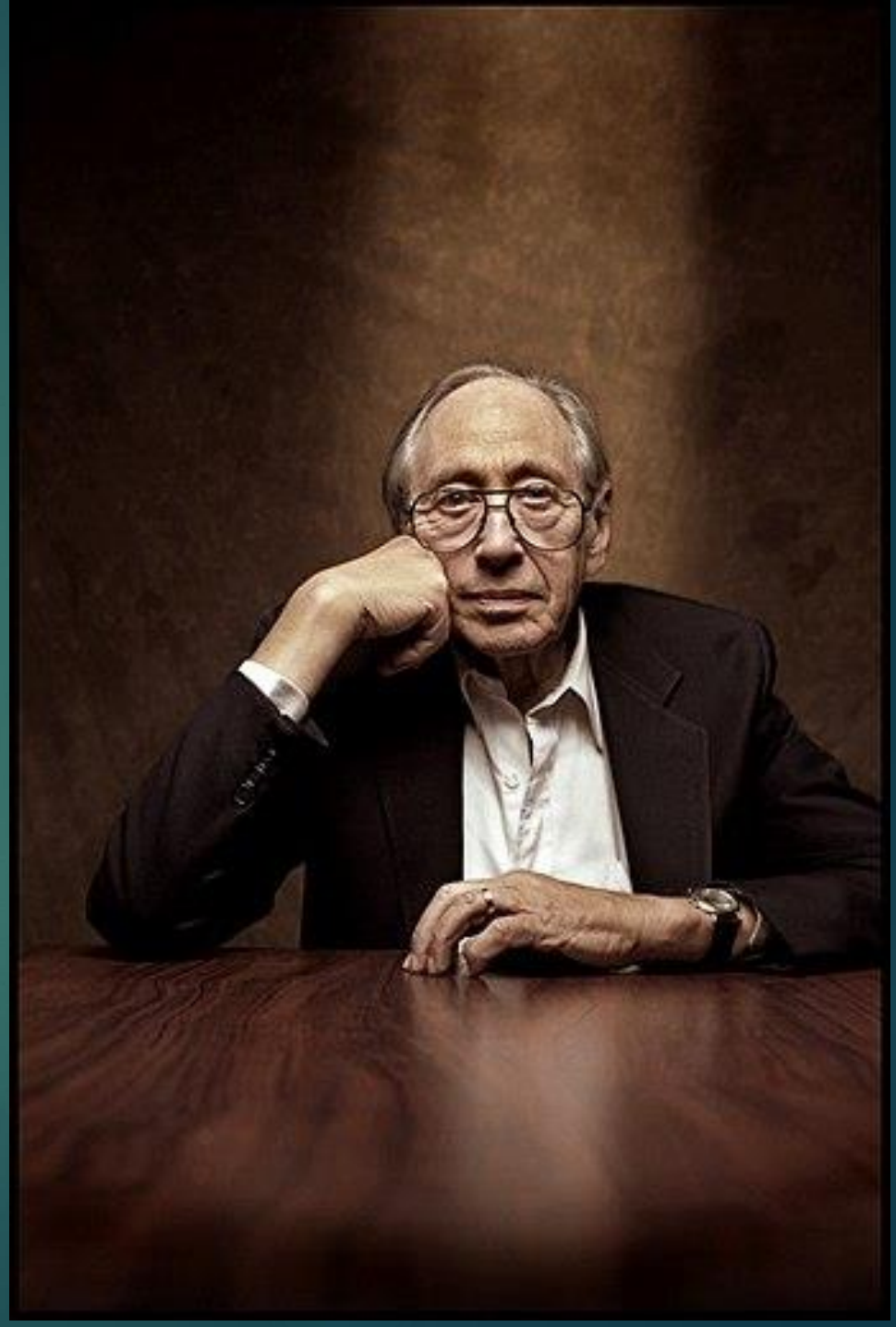


DLACZEGO WARTO POSTAWIĆ NA CYBERBEZPIECZEŃSTWO?

Zmiana myślenia: to nie koszty, a inwestycja

- **Analfabetą XXI w. nie będzie już ten, kto nie potrafi czytać ani pisać. Analfabetą będzie ten, kto nie potrafi się uczyć, potem oduczać, a następnie znowu uczyć.**

Autor: Alvin Toffler w książce „Szok przyszłości”

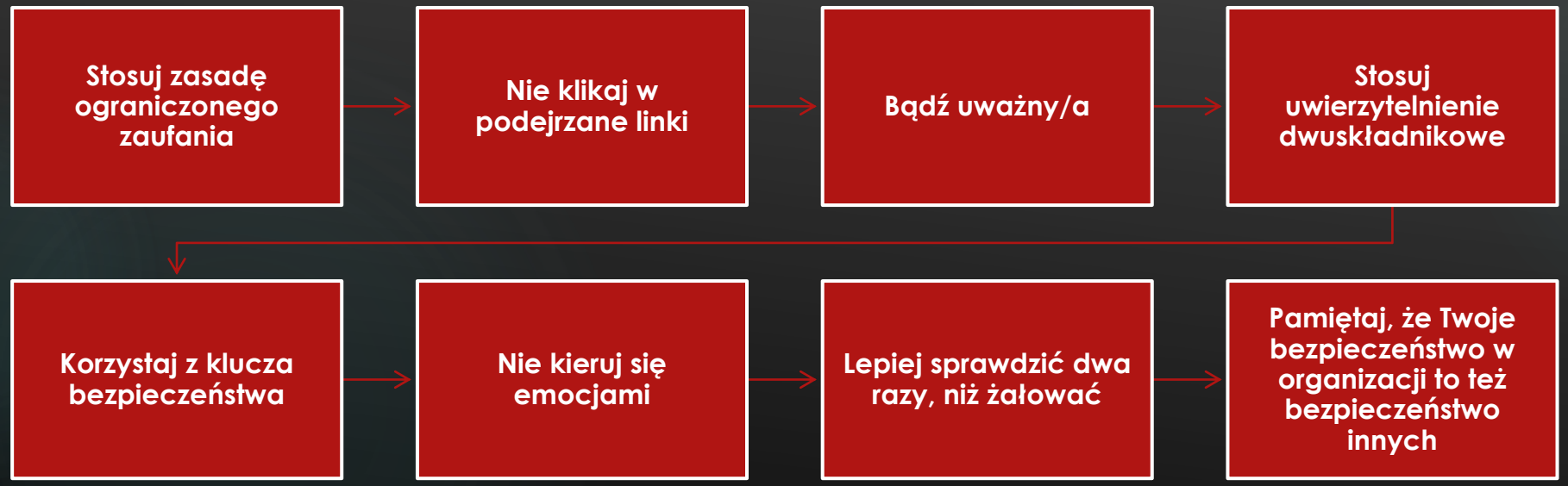



TO, CO ZROBISZ DZISIAJ –
PRZYNIESIE EFEKT W PRZYSZŁOŚCI

JAK ZADBAĆ O BEZPIECZEŃSTWO ORGANIZACJI?

- Nie podłączaj komputera do nieznanych urządzeń, nie korzystaj z nieznanych sieci
- Używaj sprzętu firmowego do celów związanych z pracą
- Nie otwieraj podejrzanych załączników
- Nie ujawniaj danych wrażliwych swoich i organizacji
- Korzystaj z VPN (wirtualnej sieci prywatnej)
- Nie ściągaj oprogramowania/plików/załączników pochodzących z nieznanych źródeł

JAK ZADBAĆ O WŁASNE CYBERBEZPIECZEŃSTWO?



DZIĘKUJĘ ZA UWAGĘ

- Mail: n.bochynska@defence24.pl
- Twitter: @BochynskaNikola
- LinkedIN
- Redakcja CyberDefence24.pl: kanały Twitter, Facebook, LinkedIN, YouTube (kanał Defence24)