Cyberodporność w akcji

Testy porównawcze globalnej gotowości przedsiębiorstwa
w zakresie bezpieczeństwa / wykrywania / odzyskiwania sprawności
Dyskusja na temat analizy
styczeń 2026 r.

DELL Technologies

Agenda

- Cele i firmografia
- Luka w cyberodporności
- Zabezpieczenia
- Wykrywanie
- Odzyskiwanie
- Złożoność, kultura i przyszłość

Cele biznesowe

- Pozycjonowanie firmy Dell jako wiodącego eksperta i strategicznego partnera w zakresie cyberodporności
- Potwierdzenie decyzji o przejściu z określenia „ochrona danych” na „cyberodporność”

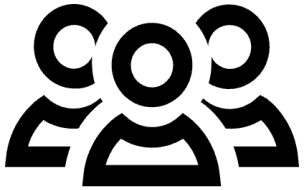
Cele badań

- Ocena dojrzałości i integracji strategii cyberodporności
- Ocena skuteczności praktyk w zakresie bezpieczeństwa, wykrywania i odzyskiwania sprawności w organizacjach
- Zrozumienie przeszkód w procesie podnoszenia cyberodporności, takich jak niewystarczające umiejętności, ograniczenia budżetowe i złożoność
- Dowiedz się w jaki sposób organizacje zabezpieczają swoje środowisko IT i chronią dane przed zagrożeniami ransomware

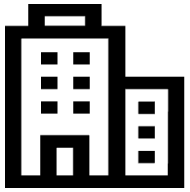
Z kim rozmawialiśmy?

Wywiady
z respondentami
przeprowadzono w lipcu
i październiku 2025 r.

850 decydentów IT
z globalnych organizacji



Organizacje zatrudniające
ponad 1000 pracowników



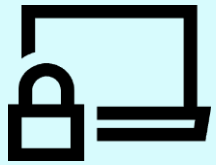
Organizacje działające
w różnych branżach sektora
publicznego i prywatnego

Respondentami są:
Członkowie zarządu;
menedżerowie średniego
szczebla i kierownictwo
najwyższego szczebla

Najważniejsze ustalenia

O 39%

organizacji ma w pełni ugruntowaną i stale optymalizowaną strategię cyberodporności



Kluczowa jest ciągła optymalizacja — bez niej strategie mogą szybko stać się przestarzałe w obliczu zmieniających się zagrożeń, co naraża organizacje na większe ryzyko

O 46%

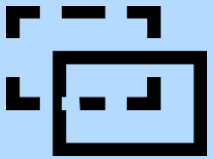
wiedzę, że dane w kopiach zapasowych nie są tak dobrze chronione, jak powinny

Wzmocnienie ochrony kopii zapasowych ma kluczowe znaczenie umożliwienia odzyskania sprawności w przypadku naruszenia głównych systemów.

Bezpieczeństwo

O 30%

używa kompleksowej platformy do wykrywania zagrożeń powiązanych z siecią, kopiami zapasowymi i głównymi pamięciami masowymi



Bez zintegrowanego wykrywania widoczność zagrożeń i czasy reakcji mogą być dłuższe, co zwiększa ryzyko braku wykrycia naruszeń bezpieczeństwa.

Wykrywanie

O 55%

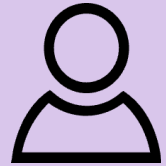
osób, które przeprowadzały symulowane cyberataki co najmniej raz w miesiącu, z powodzeniem odzyskało sprawność po ćwiczeniach / incydencie cybernetycznym

Częste testy pomagają zespołom przygotować się do rzeczywistych sytuacji. Zespoły, które nie są przygotowane, ryzykują opóźnienia w procesach reagowania i przywracania sprawności w krytycznych momentach.

Odzyskiwanie

O 63%

uważa, że kierownictwo przecenia gotowość swojej organizacji na ważne zdarzenie cybernetyczne



Nadmierna pewność siebie może powodować wstrzymywanie inwestycji, zaniedbywanie odpowiednio szybkiego planowania reakcji i pozostawianie krytycznych luk w zabezpieczeniach bez wprowadzania rozwiązań.

Rozdział 1: Luka w cyberodporności

Zrozumienie problemu i pilnej potrzeby rozwoju

Ciągłe optymalizowanie strategii odporności zapewnia lepsze odzyskiwanie sprawności, ale sukces nie jest gwarantowany

O 99,5%

posiada pewną formę strategii cyberodporności

O 39%

uważa się za organizację w pełni rozwiniętą i stale optymalizowaną (dojrzała strategia)

O 57%

nie zdołało skutecznie ochronić i odzyskać sprawności podczas ostatniego testu lub incydentu

W organizacjach z dojrzałymi strategiami cyberodporności pomyślne odzyskiwanie sprawności jest **2,6-krotnie bardziej skuteczne**

O 65% w porównaniu z **O 25-proc.**

O 63%

uważa, że **kierownictwo przecenia swoją gotowość** na ważne zdarzenie cybernetyczne

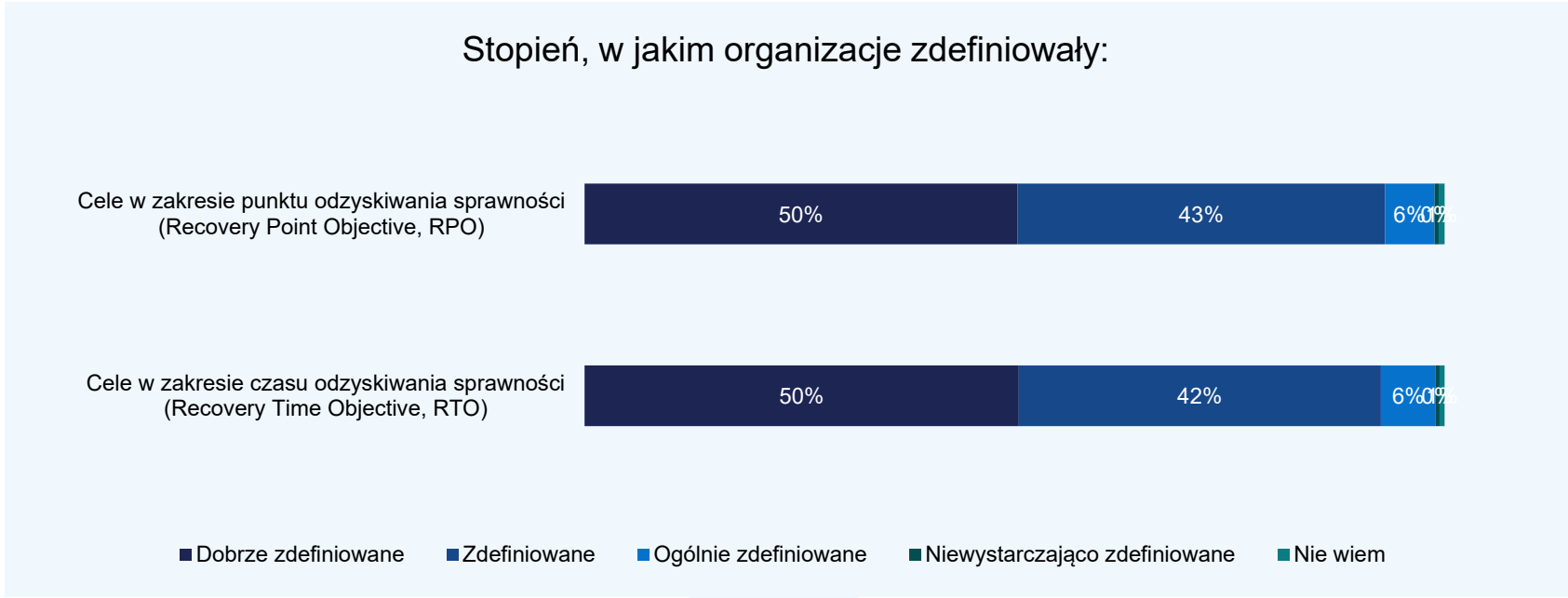
Dlaczego to ma znaczenie teraz

O 97%

Zgadza się, że ich organizacja musi stale wzmacniać bezpieczeństwo w miarę rozwoju zagrożeń

O 78%

uważa, że ich organizacja koncentruje się bardziej na zapobieganiu atakom, niż na przygotowaniu się do odzyskania sprawności po ataku



O 32%

Oba obszary powinny być dobrze zdefiniowane

Organizacji mających dojrzałą strategię cyberodporności

O 58%

Mają dobrze zdefiniowane RTO i RPO

Sekcja 2: Bezpieczeństwo

Zapobieganie atakom i wzmacnianie zasobów cyfrowych

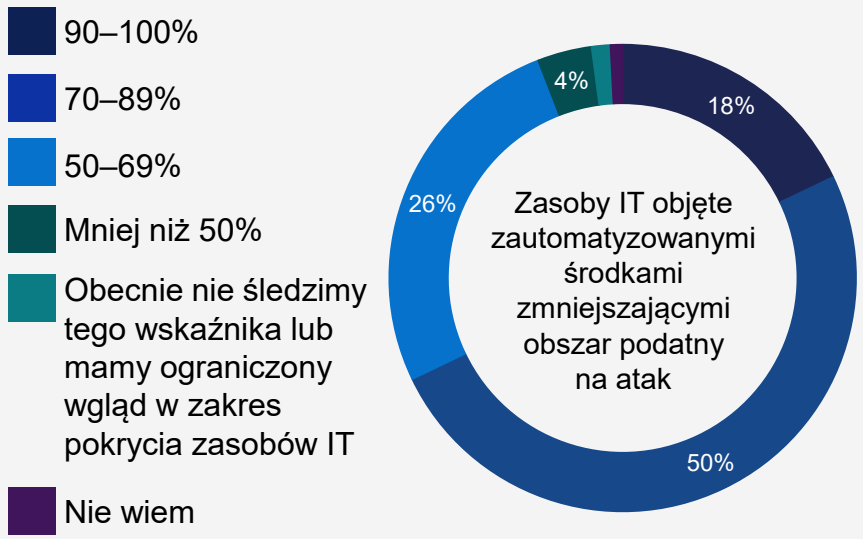
Luki w widoczności i braki w ochronie

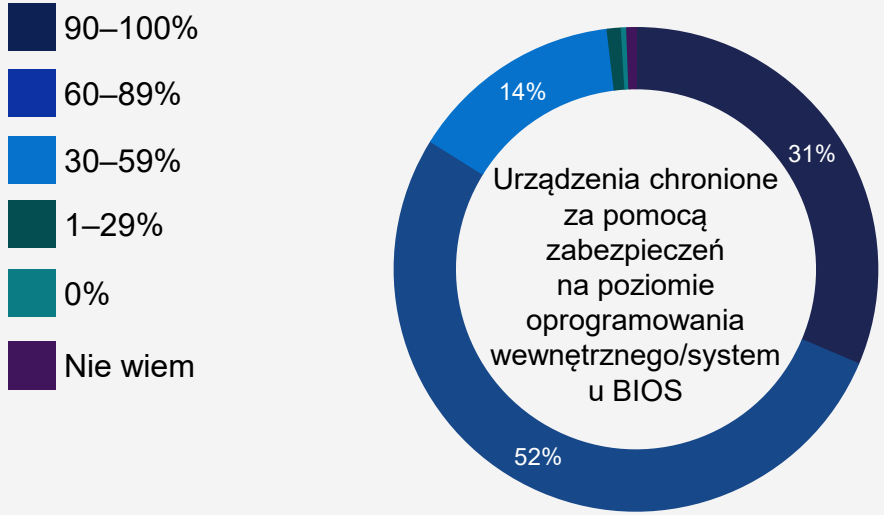
O 46%

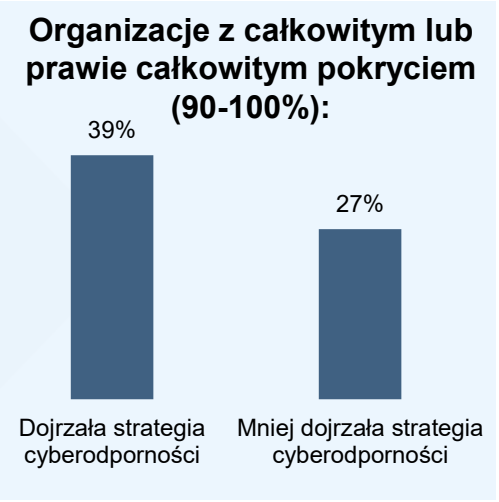
przyznaje, że dane w kopiach zapasowych nie są tak dobrze chronione, jak powinny

Niedostępne	**O 59%**
Europa, Bliski Wschód i Afryka	**O 43%**
Ameryka Łacińska	**O 41%**
APJ	**O 39%**

Ciągłe doskonalenie nie eliminuje luk w zabezpieczeniach, ale zapewnia organizacjom krytyczną przewagę w zakresie odporności na zagrożenia







Od integralności przed wdrożeniem po odzyskiwanie sprawności po ataku: wzmocnij bezpieczeństwo na każdym etapie

Procesy/metody stosowane przez organizacje w celu zapewnienia integralności sprzętu/oprogramowania IT

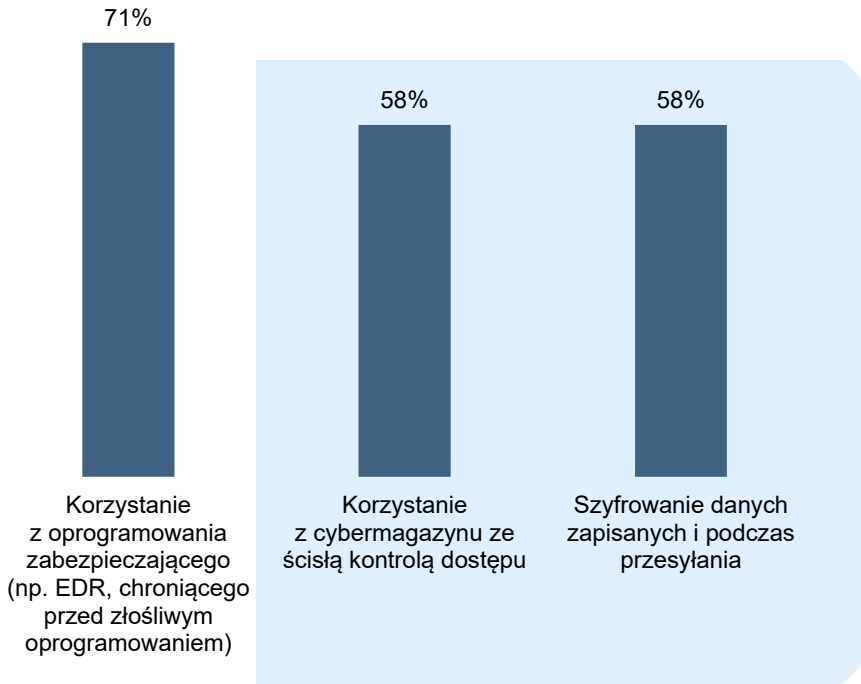
O 72%

opiera się na dostawcach w zakresie certyfikatów i atestów oraz na systemach z wbudowanymi narzędziami weryfikującymi integralność komponentów

O 64%

przeprowadza audyty wewnętrzne lub ręczne przeglądy podczas wdrażania

Metody stosowane przez organizacje do ochrony krytycznych danych przed atakami ransomware



Organizacje z dojrzałymi strategiami odporności na awarie częściej wykorzystują:

- **Szyfrowanie danych (O 59% vs O 57%)**
- **Magazyny cybernetyczne (O 63% vs O 55%)**

niż organizacje z mniej dojrzałymi strategiami odporności

Sekcja 3: Wykrywanie

Wykrywanie zagrożeń i reagowanie na nie przed ich wpływem

Wykorzystanie sztucznej inteligencji i automatyzacji może umożliwić wykrycie zagrożeń, zanim zagrożone będzie bezpieczeństwo kopii zapasowych

O 38%

organizacji korzysta z narzędzi opartych na AI/ML wraz z proaktywnymi procedurami ograniczania ryzyka i reagowania

organizacji z dojrzałą strategią cyberodporności **3,1 x** częściej używa tego rozwiązania

O 65% w porównaniu z **O 21%**

O 48%

organizacji **intensywnie używa sztucznej inteligencji i uczenia maszynowego do skanowania danych w kopiach zapasowych** w poszukiwaniu oznak naruszenia bezpieczeństwa

Szerokie wykorzystanie sztucznej inteligencji/uczenia maszynowego jest **2,3 x częściej stosowane w organizacjach z dojrzałą strategią cyberodporności**

O 72% w porównaniu z **O 32%**

O 83%

uważa, że cyberprzestępcy **coraz częściej atakują kopie zapasowe** podczas ataków typu ransomware

62-proc. traktuje priorytetowo inwestycje w automatyzację i wykrywanie zagrożeń za pomocą sztucznej inteligencji i uczenia maszynowego

Niekompletna widoczność zwiększa ryzyko

O 54%

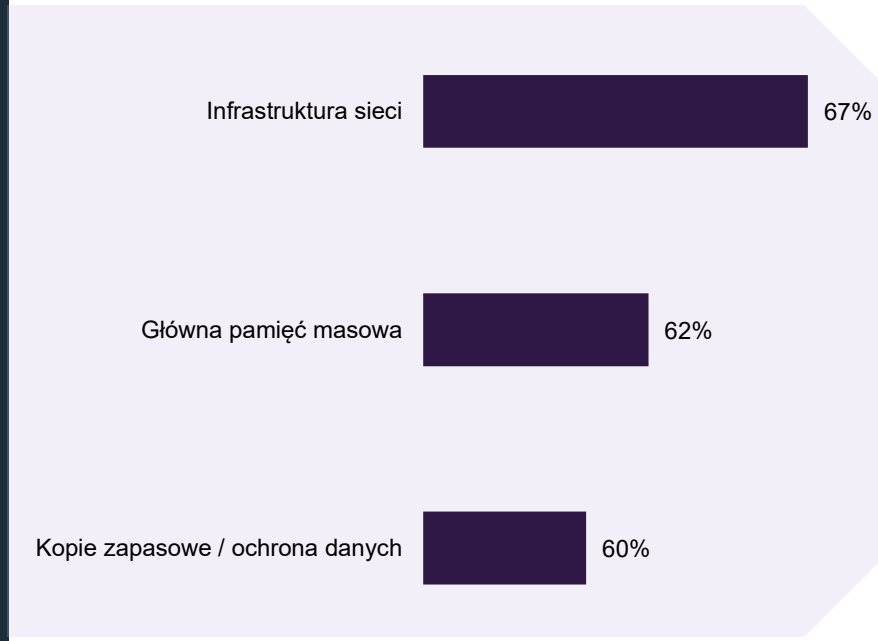
twierdzi, że ma pełny wgląd w podejrzane aktywności lub naruszone dane w swoich systemach tworzenia kopii zapasowych

O 74% Organizacje z dojrzałą strategią cyberodporności

w porównaniu z

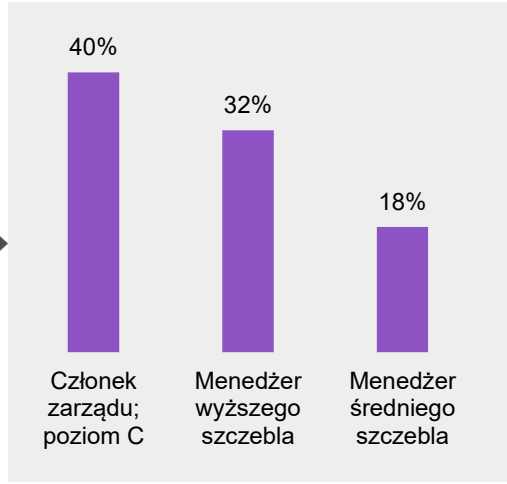
O 42% organizacji o mniej dojrzałej strategii cyberodporności

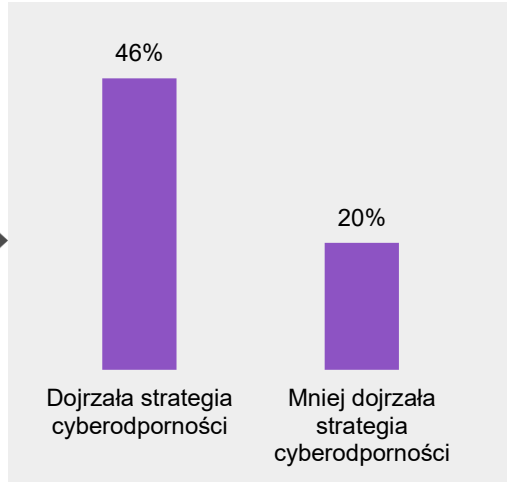
Organizacje z rozwiniętą platformą do wykrywania zagrożeń w następujących obszarach



O 30%

Kompleksowa platforma **we wszystkich 3 obszarach**





Sekcja 4: Odzyskiwanie

Szybkie wznowienie działalności zgodnie z oczekiwaniami SLA

Stan odzyskiwania: wiele organizacji osiąga wyznaczone cele, ale dalsze doskonalenie jest kluczowe, aby nadążyć za zmieniającym się krajobrazem zagrożeń

O 40%

z powodzeniem opanowano zagrożenie i odzyskano sprawność przy minimalnych szkodach

Członkowie zarządu (O 53%) częściej o tym mówią niż **menedżerowie średniego szczebla (O 30%)**

O 54%

Organizacje osiągnęły swoje **cele w zakresie RTO/RPO**

Według stanowiska: członkowie zarządu (O 45%), natomiast kierownictwo średniego szczebla (O 66%)

Nr 4

Głównym czynnikiem wpływającym na inwestycje w cyberodporność jest **niedawny incydent cybernetyczny lub sytuacja potencjalnego zagrożenia** w organizacji

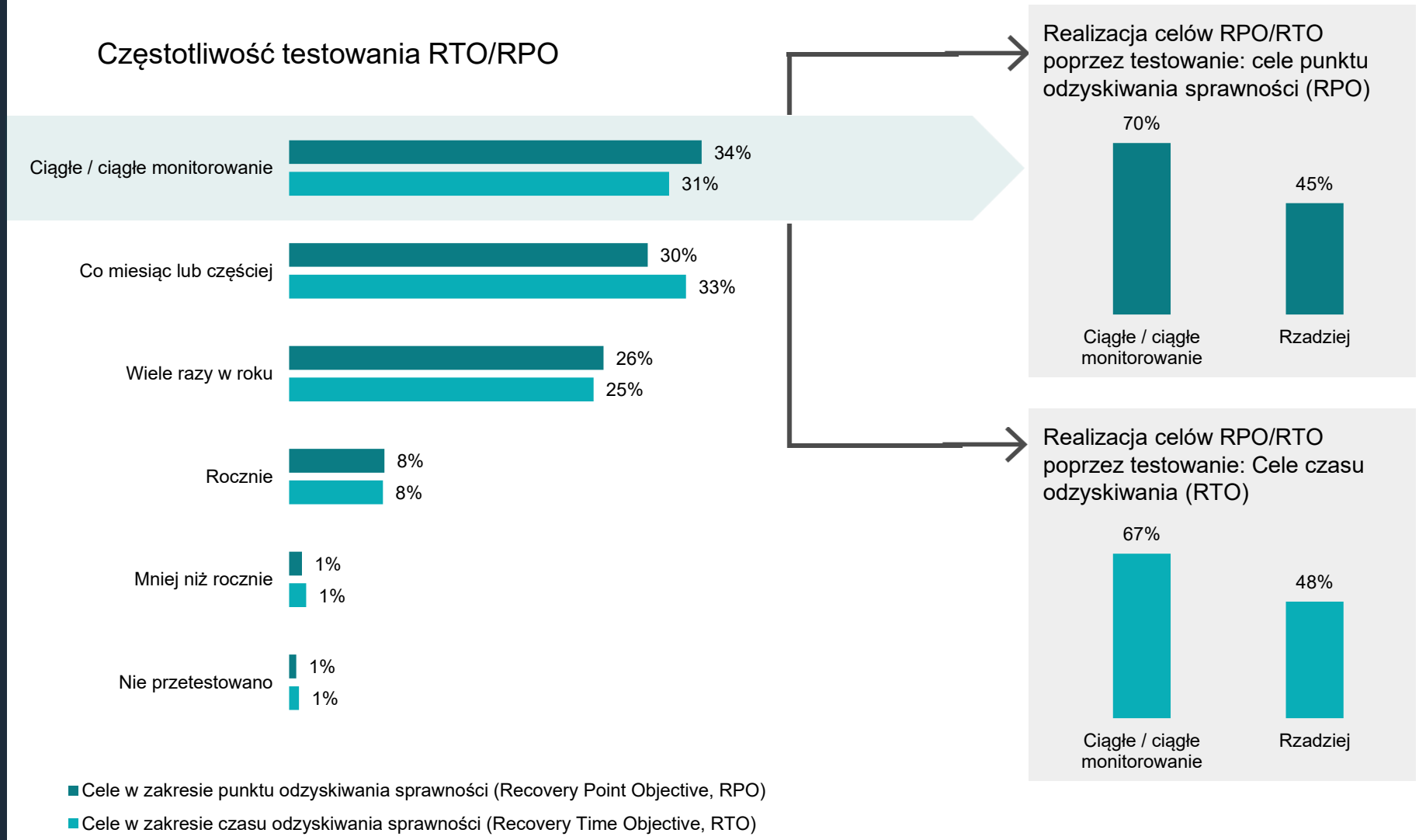
O 57% zwiększa odporność na awarie w celu **spełnienia wymagań regulacyjnych lub zgodności z przepisami**

Częste testy mogą zapewnić lepsze odzyskiwanie sprawności

Ostatecznie kultura czujności i ciągłego doskonalenia jest tym, co buduje odporność.

Menedżer wyższego szczebla, organizacja ds. usług konsumenckich, Brazylia

Testowanie ma kluczowe znaczenie dla odporności, dając organizacjom większe szanse na odzyskanie sprawności



Testowanie ma fundamentalne znaczenie dla odporności na awarie

O 48%

Stwierdzono, że testy cyberodporności ich organizacji nie symulują realistycznie nowoczesnych technik ataków

O 53% członków zarządu najwyższego szczebla

w porównaniu z

O 48% menedżerów średniego szczebla

Regularne ćwiczenia są kluczem do poprawy zdolności odzyskiwania sprawności, ale organizacje powinny stale tworzyć nowe plany, ponieważ zagrożenia nieustanie się zmieniają

Średnio razy w roku organizacja przeprowadza symulowane cyberataki

O 55%

osób, które przeprowadzały symulowane cyberataki **co najmniej raz w miesiącu, z powodzeniem odzyskało sprawność** po ćwiczeniach / incydencie cybernetycznym

O 35%

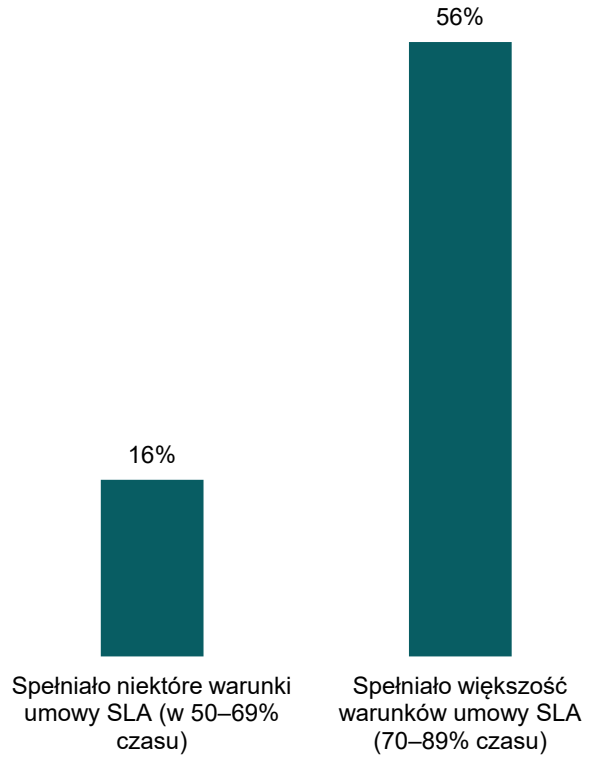
spośród tych, którzy przeprowadzali symulowane ataki cybernetyczne **rzadziej niż co miesiąc, tylko niewielki odsetek był w stanie skutecznie odzyskać sprawność** po ćwiczeniu/incydencie cybernetycznym

> *Potrzeba kompleksowego testowania i oceny wszystkich potencjalnych zagrożeń, zamiast skupiania się na punktowym testowaniu.*
>
> Menedżer wyższego szczebla, dział technologii IT i telekomunikacji, Wielka Brytania

> *Cyberataki przypominają nam, jak ważne jest regularne przeprowadzanie ćwiczeń z zakresu bezpieczeństwa.*
>
> *Rozbudowano szkolenia z zakresu świadomości bezpieczeństwa, umożliwiając każdemu pracownikowi identyfikowanie potencjalnych zagrożeń.*
>
> Członek Zarządu, Budownictwo i Nieruchomości, Australia

Umowy SLA są dowodem: organizacje z dojrzałymi strategiami dotrzymują obietnic odzyskiwania sprawności

Częstotliwość realizacji przez organizacje umów SLA dotyczących krytycznego odzyskiwania sprawności

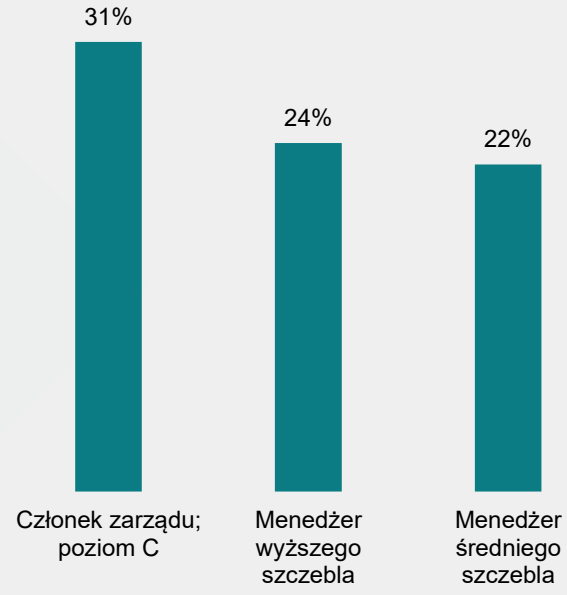


2 razy większy

organizacji z dojrzałymi strategiami cyberodporności będzie prawdopodobnie częściej konsekwentnie realizować swoje umowy SLA

O 36% w porównaniu z **O 18%**

Według pozycji:



Sekcja 5: Złożoność, kultura i przyszłość

Bariery organizacyjne i przyszłe plany inwestycyjne

Złożoność, braki w kompetencjach i nadmierna pewność siebie zagrażają cyberodporności, ale sztuczna inteligencja i szkolenia mogą pomóc

Najważniejsze wyzwania:

Złożone środowisko IT	O 49%
Ograniczenia budżetowe	O 42%
Brak wykwalifikowanego personelu	O 39%
Fragmentacja dostawcy/ narzędzia	O 38%
Niskie priorytety kierownictwa	O 23%

Większe organizacje częściej mierzą się z tym problemem:

- O 50% Co najmniej 5 000 pracowników
- O 50% 3 000–4 999 pracowników
- O 46% 1 000–2 999 pracowników

O 63%

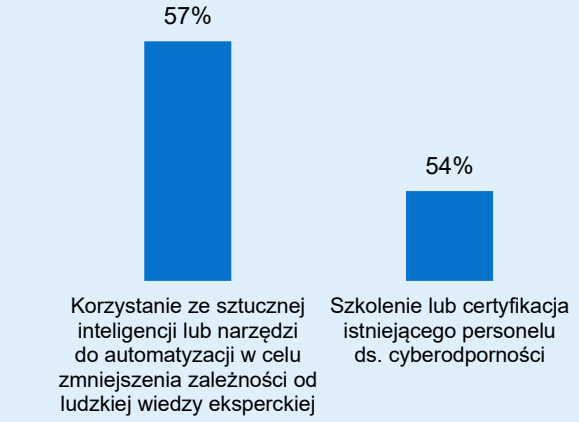
uważa, że kierownictwo przecenia gotowość swojej organizacji na ważne zdarzenie cybernetyczne

O 96%

Potwierdzenie, że mają braki w umiejętnościach lub wiedzy eksperckiej w zakresie cyberodporności

ALE…

Organizacje działają poprzez:



Z myślą o inwestycjach

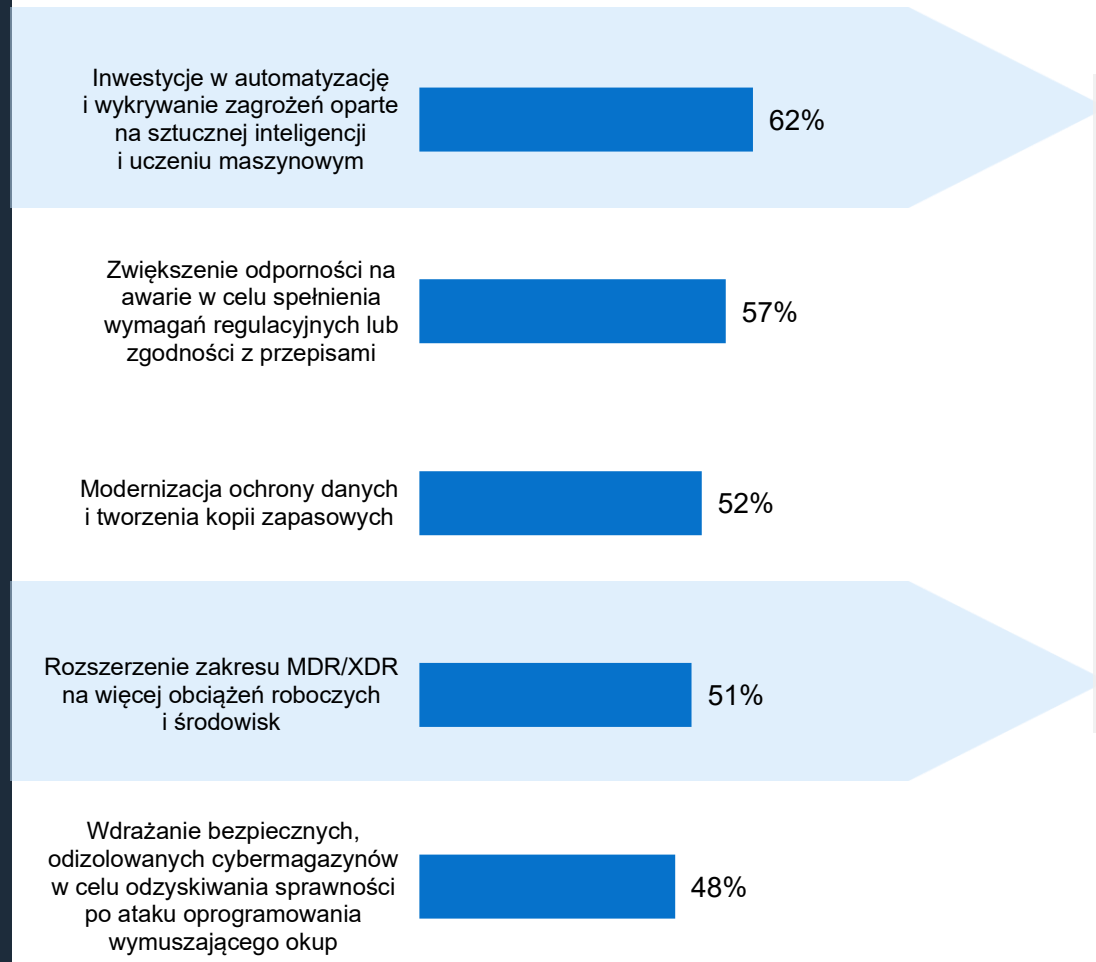
Ryzyko nr 1

Motorem inwestycji jest ewoluujący krajobraz zagrożeń

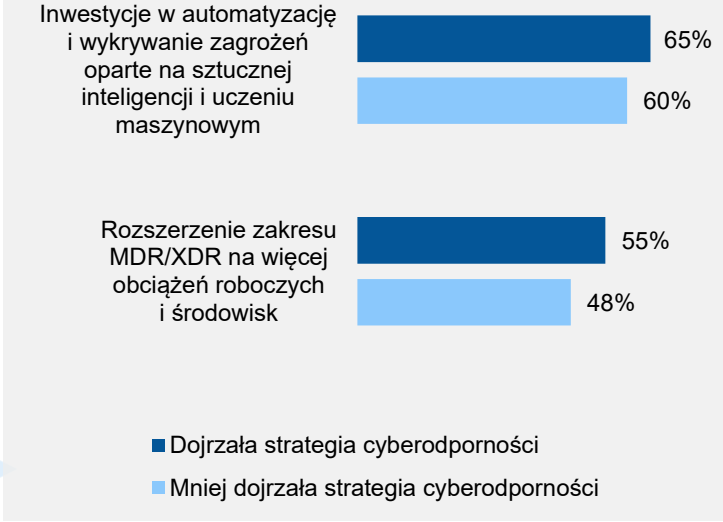
> „O 97% Moja organizacja musi stale wzmacniać swoje bezpieczeństwo w miarę rozwoju zagrożeń”

Aby zachować dojrzałą postawę, należy nieustannie inwestować i optymalizować działania

Priorytetowe inwestycje w cyberodporność w ciągu najbliższych 12 miesięcy



Dojrzałe organizacje odporne na cyberataki nieustannie inwestują

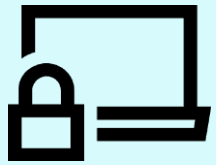


Najważniejsze wnioski

Najważniejsze ustalenia

O 39%

organizacji ma w pełni ugruntowaną i stale optymalizowaną strategię cyberodporności



Kluczowa jest ciągła optymalizacja — bez niej strategie mogą szybko stać się przestarzałe w obliczu zmieniających się zagrożeń, co naraża organizacje na większe ryzyko

O 46%

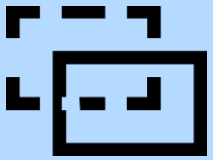
wiedzę, że dane w kopiach zapasowych nie są tak dobrze chronione, jak powinny

Wzmocnienie ochrony kopii zapasowych ma kluczowe znaczenie umożliwienia odzyskania sprawności w przypadku naruszenia głównych systemów.

Bezpieczeństwo

O 30%

używa kompleksowej platformy do wykrywania zagrożeń powiązanych z siecią, kopiami zapasowymi i głównymi pamięciami masowymi



Bez zintegrowanego wykrywania widoczność zagrożeń i czasy reakcji mogą być dłuższe, co zwiększa ryzyko braku wykrycia naruszeń bezpieczeństwa.

Wykrywanie

O 55%

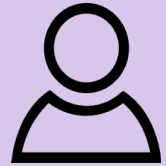
osób, które przeprowadzały symulowane cyberataki co najmniej raz w miesiącu, z powodzeniem odzyskało sprawność po ćwiczeniach / incydencie cybernetycznym

Częste testy pomagają zespołom przygotować się do rzeczywistych sytuacji. Zespoły, które nie są przygotowane, ryzykują opóźnienia w procesach reagowania i przywracania sprawności w krytycznych momentach.

Odzyskiwanie

O 63%

uważa, że kierownictwo przecenia gotowość swojej organizacji na ważne zdarzenie cybernetyczne



Nadmierna pewność siebie może powodować wstrzymywanie inwestycji, zaniedbywanie odpowiednio szybkiego planowania reakcji i pozostawianie krytycznych luk w zabezpieczeniach bez wprowadzania rozwiązań.