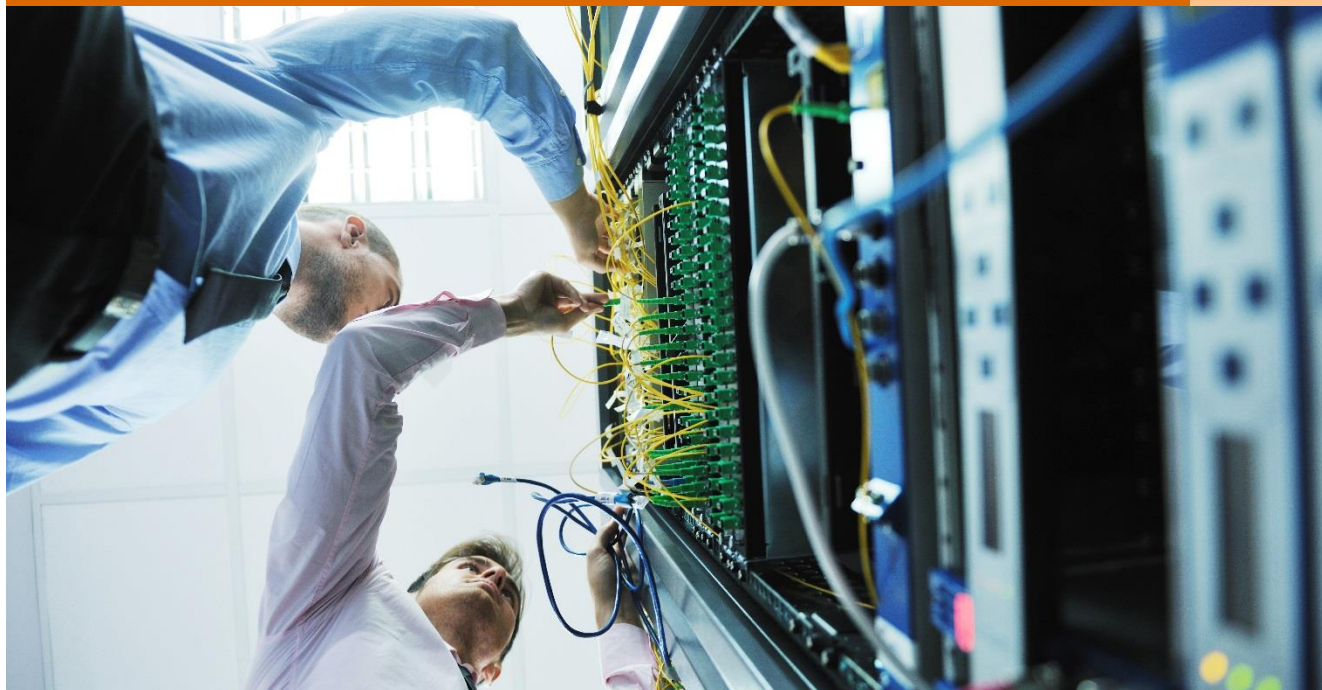


# *Ochrona biznesu w cyfrowej transformacji*

Prezentacja wyników 4. edycji badania „Stan bezpieczeństwa informacji w Polsce”

16 maja 2017 r.



## *Stan cyberbezpieczeństwa w Polsce wg raportu PwC*

**96%** dużych i średnich firm w Polsce doświadczyło ponad 50 incydentów na przestrzeni ostatniego roku

**55%** respondentów nie ma świadomości, jakie były efekty ataków na dane w ich organizacjach biznesowych

**52%** dużych i średnich firm w Polsce wydaje na kwestie związane z bezpieczeństwem mniej niż 1 milion złotych rocznie

**41%** firm przemysłowych obawia się ataków hakerskich, które mogą spowodować znaczące uszkodzenia infrastruktury

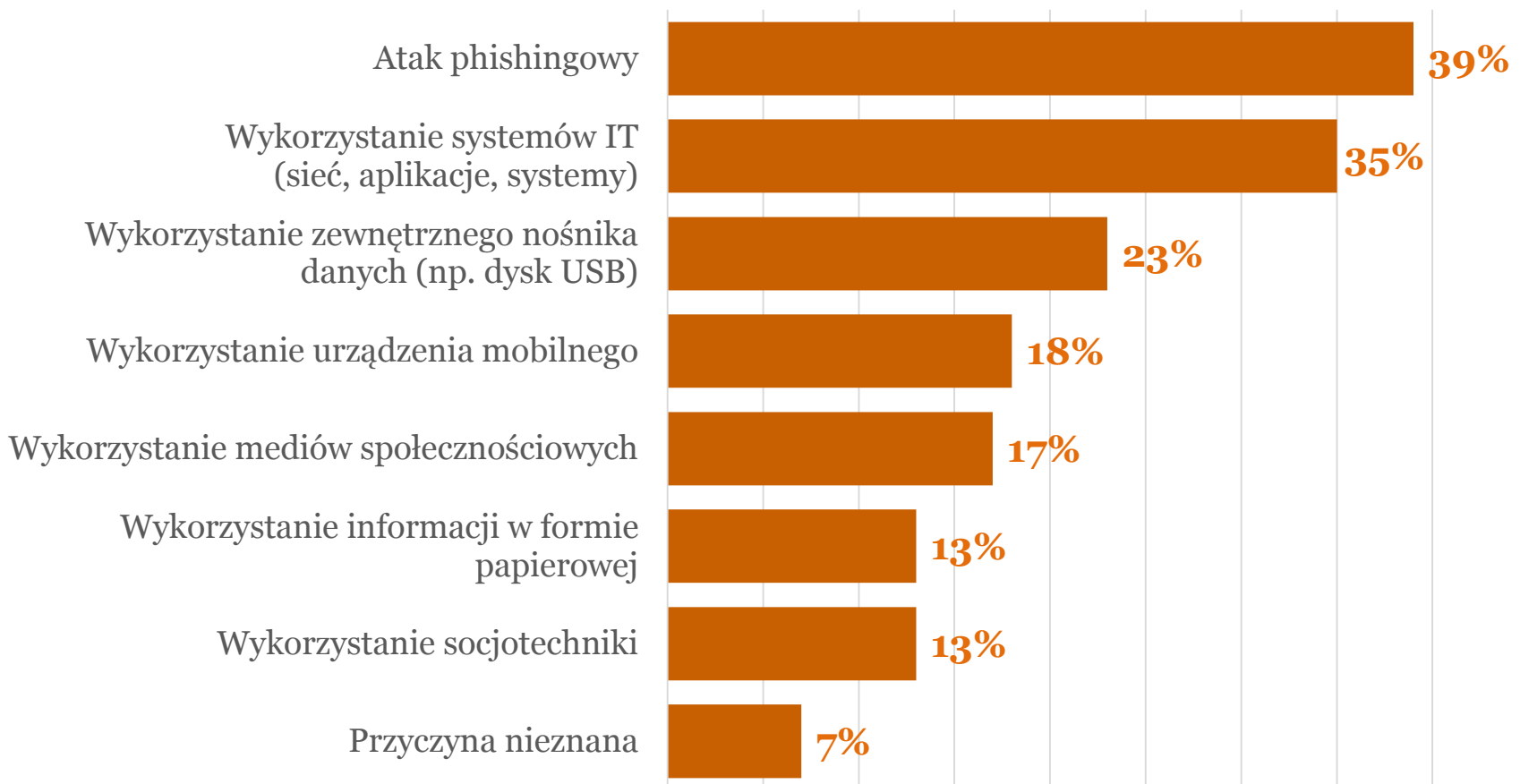
**Atak phishingowy** jest najczęściej wykorzystywaną metodą cyberataków na firmy w Polsce

Wiele polskich firm **nie jest gotowych** na wdrożenie europejskiego rozporządzenia o ochronie danych osobowych (**RODO**)

# *Stan cyberbezpieczeństwa w Polsce*

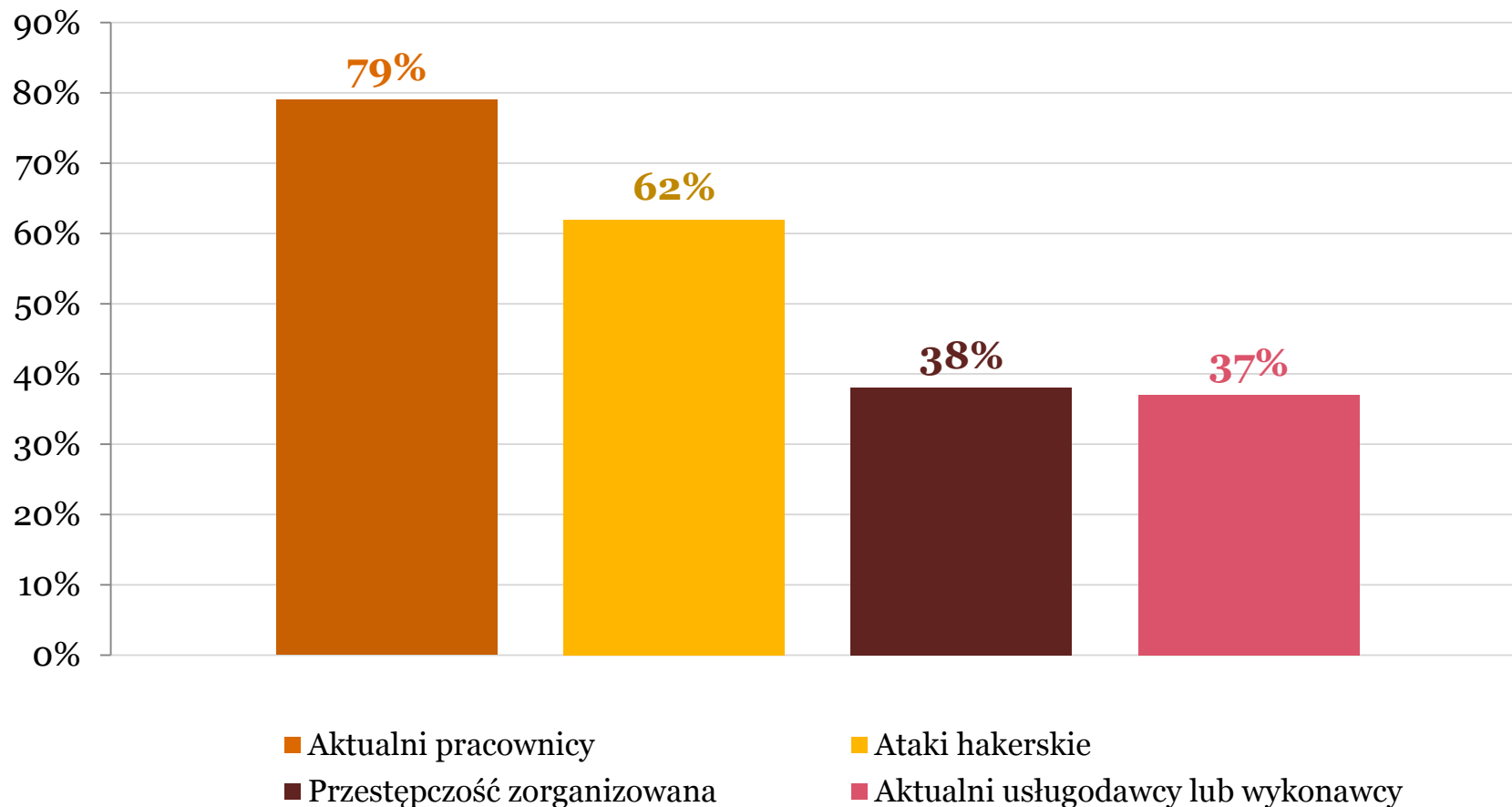
# ***96% dużych firm w Polsce w minionym roku doświadczyło ponad 50 incydentów związanych z cyberzagrożeniami***

## ***Jak dochodziło do incydentów naruszenia bezpieczeństwa?***



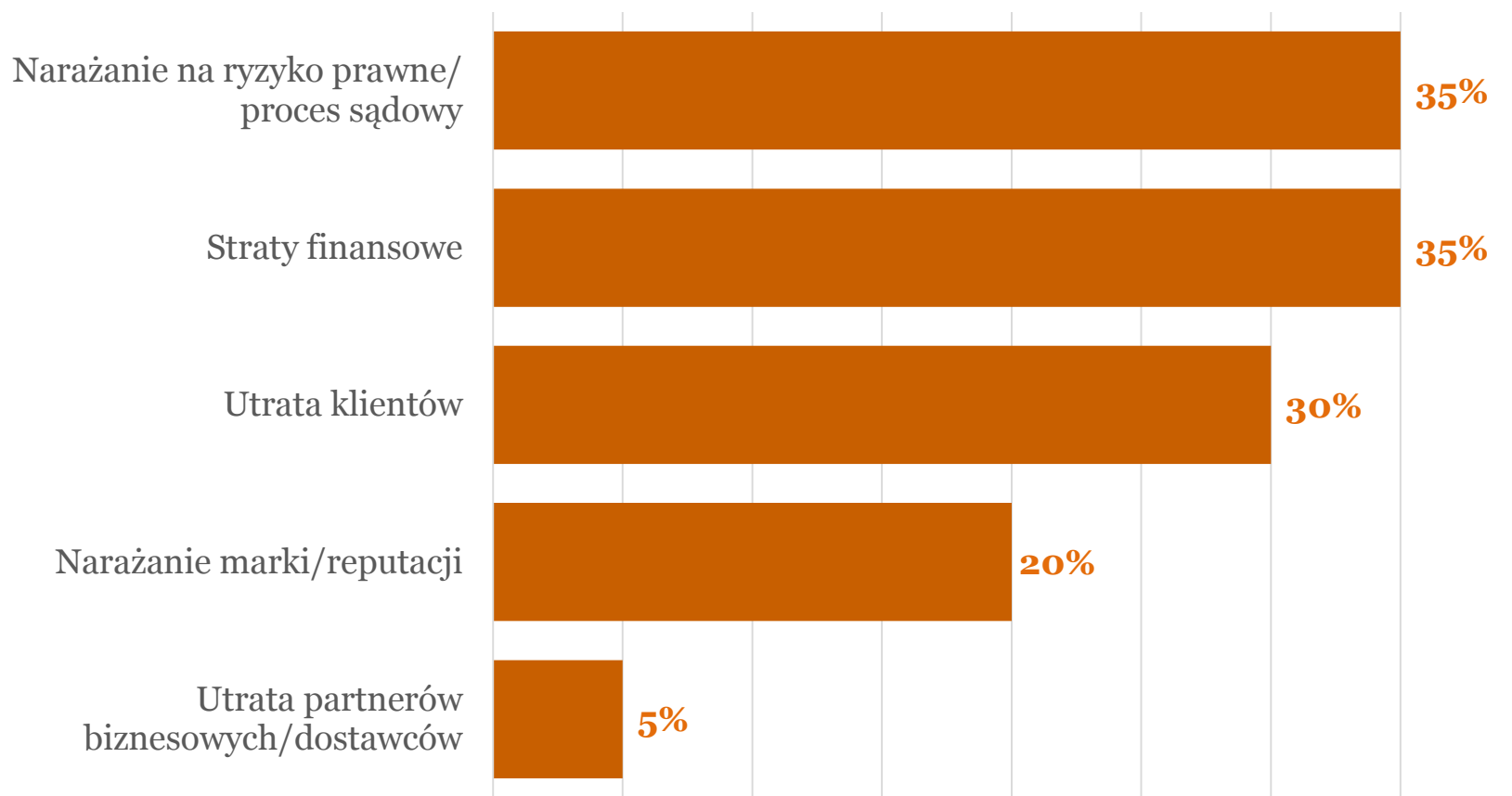
## Najczęstsze bezpośrednie lub pośrednie źródła zagrożeń

Jakie były źródła incydentów w obszarze bezpieczeństwa informacji lub systemów IT?



## Skutki zagrożeń cybernetycznych w firmach

*Jakie były skutki incydentów naruszenia bezpieczeństwa biorąc pod uwagę działalność firmy?*

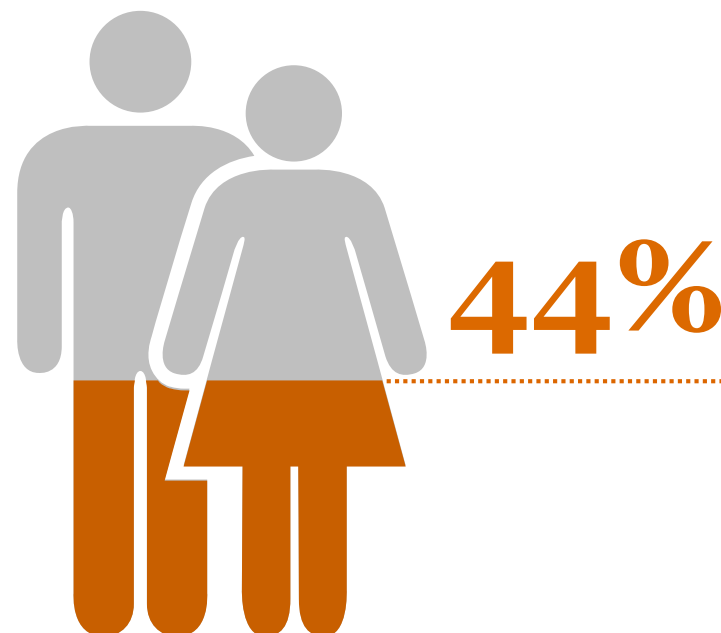


**55%** firm nie ma świadomości,  
jakie były efekty ataków  
cybernetycznych na dane w ich  
organizacjach biznesowych.

## Wydatki firm w Polsce na cyberbezpieczeństwo



dużych i średnich firm w Polsce wydaje na kwestie związane z bezpieczeństwem więcej niż 1 mln zł rocznie



przedstawiciele badanych firm zadeklarowała, że budżet przeznaczony na bezpieczeństwo IT i bezpieczeństwo informacji na 2016 rok mieścił się w przedziale od 500 tys. do 1 mln zł



## Bezpieczeństwo priorytetem dla firm, ale...

Jakie są najważniejsze priorytety w obszarze bezpieczeństwa na najbliższe 12 miesięcy?



**72%** firm nie prowadzi działań zmierzających do identyfikacji wrażliwych zasobów, a większość nie posiada szczegółowych strategii dot. mediów społecznościowych, urządzeń mobilnych czy chmury IT

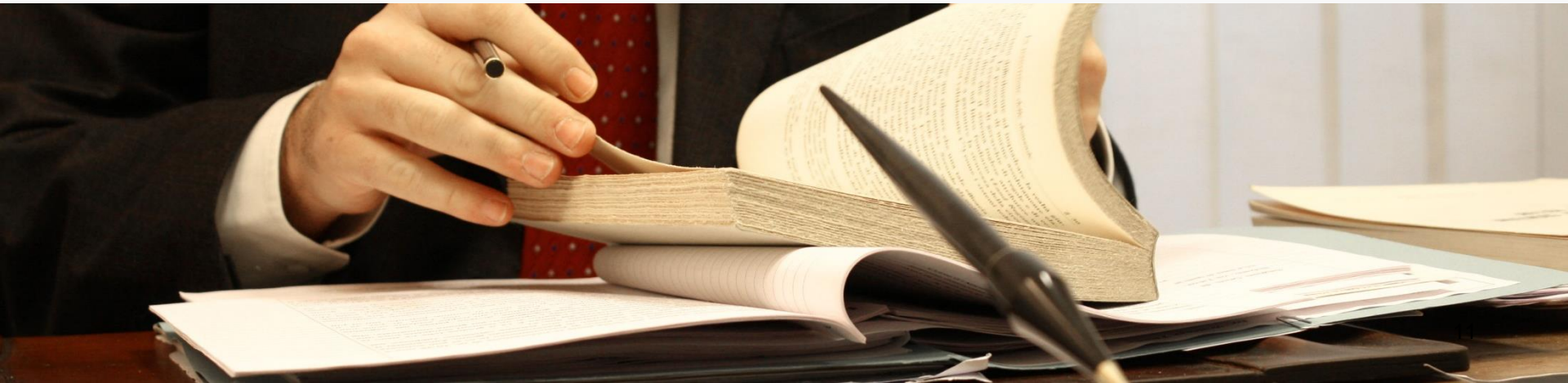
# *Rozporządzenie o ochronie danych osobowych (RODO) a cyberbezpieczeństwo*

## ***Co oznacza Rozporządzenie o Ochronie Danych Osobowych (RODO) dla firm?***

RODO będzie obowiązywało wszystkich przedsiębiorców od **25 maja 2018 r.** i zastąpi wszystkie krajowe przepisy w zakresie ochrony danych osobowych.

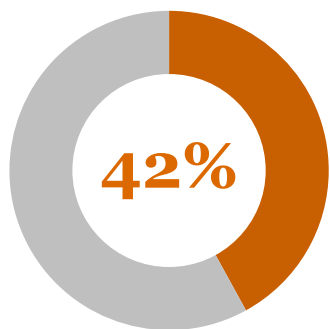
RODO wprowadza wiele istotnych zmian w podejściu do spełnienia wymagań zabezpieczania danych osobowych. Na przykład wszystkie incydenty związane z naruszeniem bezpieczeństwa danych osobowych będą musiały być zgłaszane w ciągu **72 godzin** do organu regulacyjnego.

Naruszenie przepisów będzie wiązać się z ryzykiem nałożenia na przedsiębiorstwa kary finansowej do **20.000.000 euro** lub **4%** wartości rocznego światowego obrotu przedsiębiorstwa.

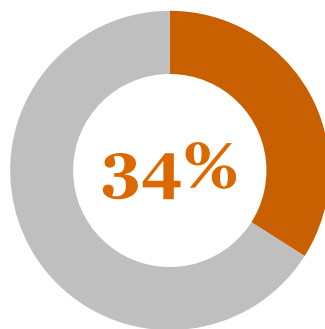


# *Polskie firmy nie są gotowe na RODO*

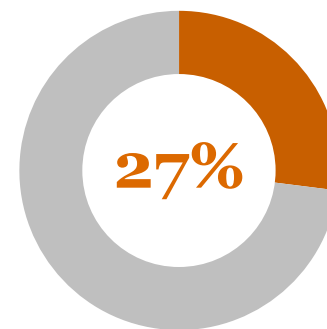
## *Stopień wdrożenia mechanizmów RODO*



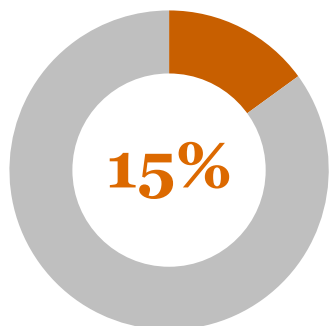
Uwzględnienie mechanizmów ochrony danych osobowych w nowych systemach IT



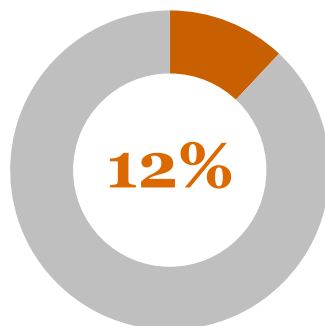
Zobowiązanie pracowników do okresowych szkoleń o polityce ochrony danych osobowych



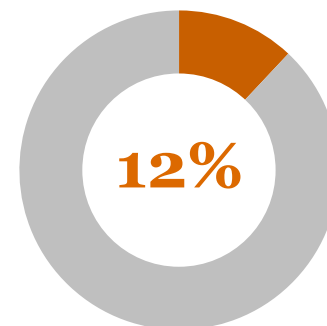
Wdrożenie zabezpieczeń w zakresie ochrony danych osobowych oraz audytu firm zewnętrznych obsługujących dane osobowe



Ocena skutków operacji przetwarzania



Ograniczenie liczby operacji przetwarzania do minimum koniecznego do osiągnięcia celu, dla którego zostały zebrane

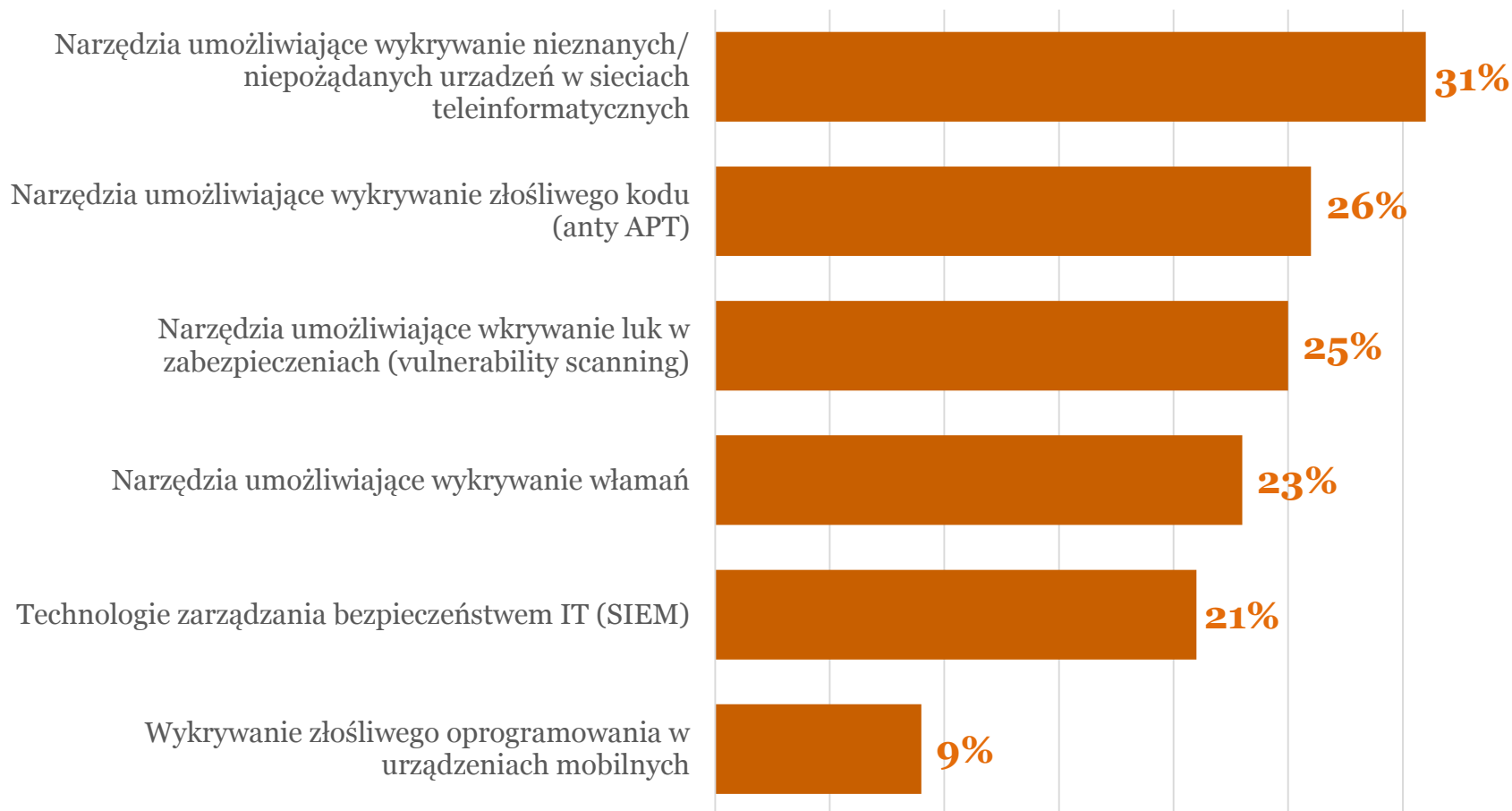


Utworzenie i aktualizacja rejestru operacji przetwarzania danych osobowych

# *Nowe technologie a cyberbezpieczeństwo*

# Luki w technologicznej architekturze bezpieczeństwa

## Technologie zabezpieczeń środowisk teleinformatycznych IT wdrożone w firmach



## ***Rośnie znaczenie bezpieczeństwa systemów przemysłowych (OT)***

***Jakich skutków związanych z cyberatakami obawiają się firmy?***



**Systemy OT odpowiadają za podtrzymanie kluczowych procesów technologicznych w firmach. Cyberataki na to środowisko mogą mieć poważne konsekwencje.**

## ***Wnioski z raportu - 4 kroki do bezpieczniejszej firmy***

**Zaufanie w centrum uwagi –  
przygotuj się do zmian**

**Świadomość przede wszystkim  
– miej pewność**

**Monitorowanie efektów –  
sprawdzaj skuteczność i  
wyciągaj wnioski**

**Analityka, automatyka,  
internet rzeczy –  
patrz szerzej**



## *Stan cyberbezpieczeństwa w Polsce wg raportu PwC*

**96%** dużych i średnich firm w Polsce doświadczyło ponad 50 incydentów na przestrzeni ostatniego roku

**55%** respondentów nie ma świadomości, jakie były efekty ataków na dane w ich organizacjach biznesowych

**52%** dużych i średnich firm w Polsce wydaje na kwestie związane z bezpieczeństwem mniej niż 1 milion złotych rocznie

**41%** firm przemysłowych obawia się ataków hakerskich, które mogą spowodować znaczące uszkodzenia infrastruktury

**Atak phishingowy** jest najczęściej wykorzystywaną metodą cyberataków na firmy w Polsce

Wiele polskich firm **nie jest gotowych** na wdrożenie rozporządzenia o ochronie danych osobowych (**RODO**)

## Kontakty



### **Tomasz Sawiak**

Wicedyrektor, zespół Cyber Security  
Technology Services  
Tel. 519 504 234  
E: [tomasz.sawiak@pl.pwc.com](mailto:tomasz.sawiak@pl.pwc.com)



### **Patryk Gęborys**

Wicedyrektor, zespół Cyber Security  
Technology Services  
Tel. 519 506 760  
E: [patryk.geborys@pl.pwc.com](mailto:patryk.geborys@pl.pwc.com)



### **Piotr Urban**

Partner, lider zespołu zarządzania  
ryzykiem w Polsce  
Tel. 502 184 157  
E: [piotr.urban@pl.pwc.com](mailto:piotr.urban@pl.pwc.com)



### **Jacek Sygutowski**

Dyrektor, zespół Cyber Security  
Technology Services  
Tel. 519 504 954  
E: [jacek.sygutowski@pl.pwc.com](mailto:jacek.sygutowski@pl.pwc.com)

*Dziękujemy za uwagę*