Status Ransomware 2020

Damian Przygodzki
System Engineer

3.06.2020

SOPHOS

Sophos Snapshot

1985
Rok Założenia
OXFORD, UK

$760 million
W liczbach
(FY19)

3,500+
Pracowników
(APPX.)

Główna Siedziba
ABINGDON, UK

350,000+
Klienci

100M+
Użytkownicy

47,000+
Partnerzy

Sophos HQ, Abingdon, UK

SOPHOS

Sophos History

Ewolucja do pełnego bezpieczeństwa

- Corporate
- Enduser Protection
- Network Protection

1985 — Founded in Abingdon (Oxford), UK

Peter Lammer
1985

Jan Hruska
1985

1988 — First checksum-based antivirus software

1989 — First signature-based antivirus software

2003 — ActiveState acquisition

2008 — Utimaco Safeware AG acquisition

2011 — Astaro acquisition

2012 — Dialogs acquisition

2014 — IPO London Stock Exchange

2014 — Cyberoam acquisition

2014 — Mojave acquisition

2015 — Reflexion acquisition

2015 — Surfright acquisition

2016 — Phish Threat acquisition

2016 — Barricade acquisition

2017 — Invincea acquisition

2019 — AVID Secure acquisition

2019 — Dark Bytes acquisition

2019 — Rook Security acquisition

SOPHOS

Sophos: Network Visionary + Endpoint Leader

Only Visionary in UTM M.Q. + Leader in Endpoint Protection Platforms M.Q.

Gartner

Gartner Magic Quadrant NETWORK FIREWALLS

Magic Quadrant for Network Firewalls
Rajpreet Kaur, Adam Hils, Jeremy D'Hoinne, John Watts
17 September 2019

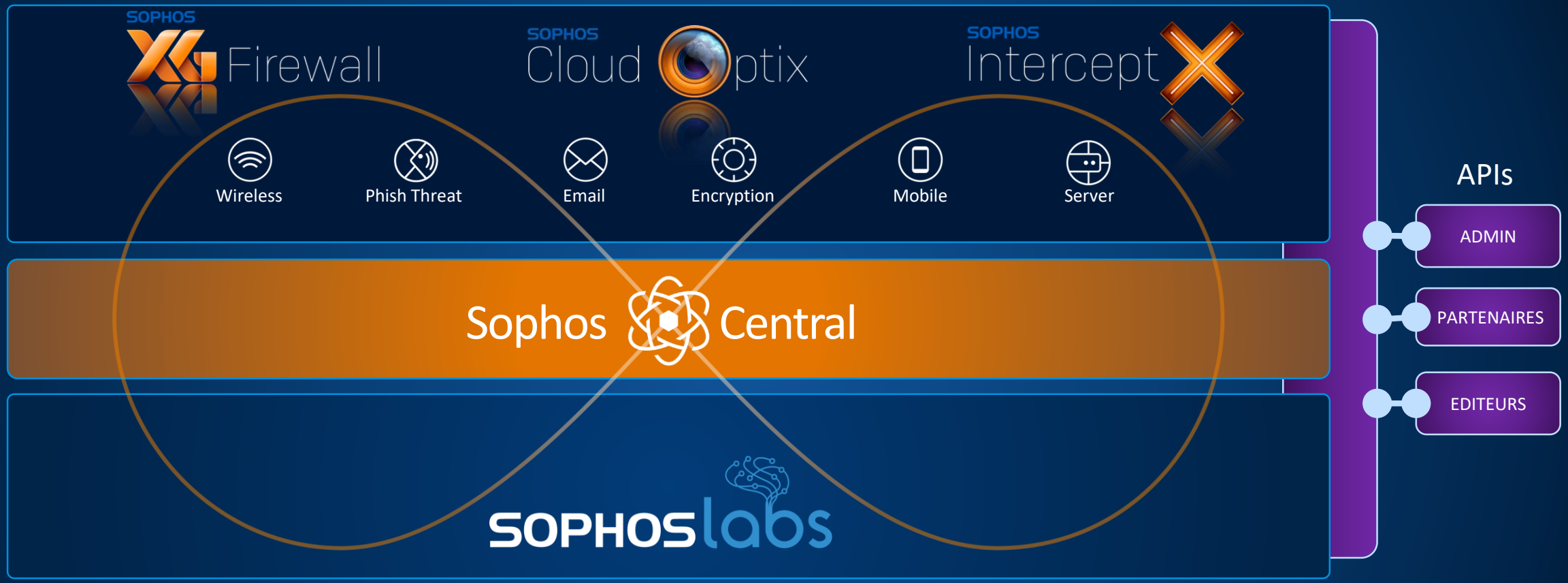
Gartner Magic Quadrant ENDPOINT PROTECTION PLATFORMS

Magic Quadrant for Endpoint Protection Platforms
Peter Firstbrook, Dionisio Zumerle, Prateek Bhajanka, Lawrence Pingree, Paul Webber
20 August 2019

SOPHOS

Platforma Sophos Synchronized Security

Najbardziej zaawansowana i kompleksowa zsynchronizowana platforma bezpieczeństwa



2015	2016	2017	2018	2019
• Endpoint + Firewall • Security Heartbeat ™ • Automatic Isolation	• Endpoint + Chiffrement • Heartbeat ™ Destination • Missing Heartbeat ™	• Synchronized App. Control • Heartbeat ™ for Linux • Heartbeat ™ for Mac OS	• Endpoint & Mobile + WiFi • PhishThreat + Endpoint • Lateral Movement Prevention	• XG SFOS 18 • Endpoint + Firewall Deep Interaction

SOPHOS

Status

Ransomware

5,000 Respondentów z 26 Krajów

Kraj	# Respondentów	Kraj	# Respondentów	Kraj	# Respondentów
Australia	200	India	300	Singapore	200
Belgium	100	Italy	200	South Africa	200
Brazil	200	Japan	200	Spain	200
Canada	200	Malaysia	100	Sweden	100
China	200	Mexico	200	Turkey	100
Colombia	200	Netherlands	200	UAE	100
Czech Republic	100	Nigeria	100	UK	300
France	300	Philippines	100	U.S.	500
Germany	300	Poland	100		

VansonBourne

Respondenci z Organizacji 100m 5,000 Użytkowników

50%
100 – 1,000 zatrudnionych

50%
1,001 – 5,000 zatrudnionych

VansonBourne

Respondenci z wielu Sektorów

Sektor	# respondentów	% respondentów
IT, technology and telecoms	979	20%
Retail, distribution and transport	666	13%
Manufacturing and production	648	13%
Financial services	547	11%
Public sector	498	10%
Business and professional services	480	10%
Construction and property	272	5%
Energy, oil/gas and utilities	204	4%
Media, leisure and entertainment	164	3%
Other	542	11%

VansonBourne

Polska

28%
Dotkniętych przez ransomware w ostatnim roku

50%
Ofiar zatrzymało atak przed zaszyfrowaniem danych

0%*
Odzyskało dane po zapłaceniu okupu

Średni koszt odzyskania danych
500,000 zl

71%
Posiadało polisę cyberbezpieczeństwa

44%
Polisa obejmowała atak ransomware

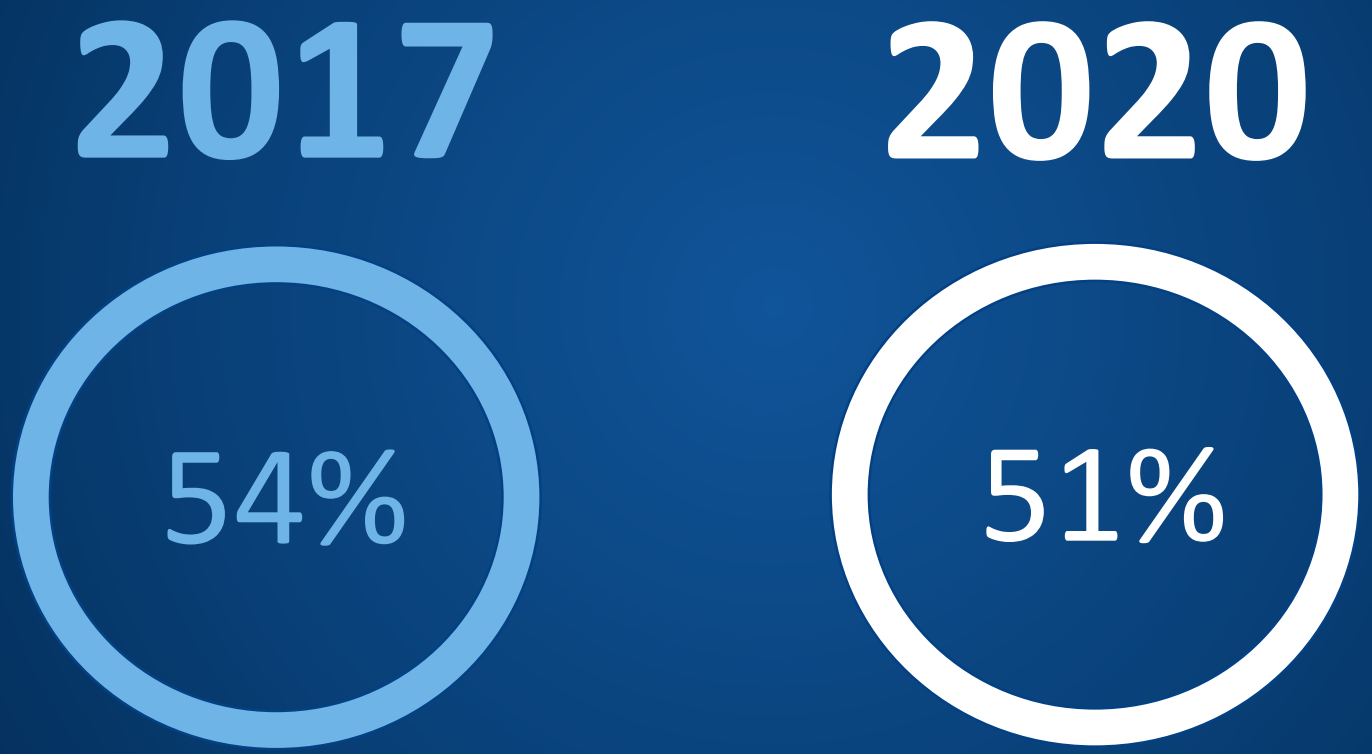
Monthly Business Update

** ilość odpowiedzi zbyt niska dla prawidłowej oceny*

Rozpowszechnienie Ransomware

SOPHOS

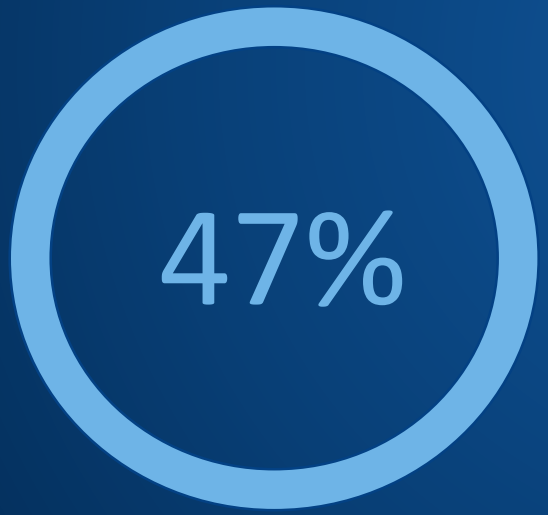
1 na 2 Organizacje Została dotknięta Ransomware w ostatnim roku



Czy w ostatnim roku Twoja organizacja została zainfekowana ransomware? Base 5,000 (2020), 1,700 (2017).

Rozmiar nie ma znaczenia

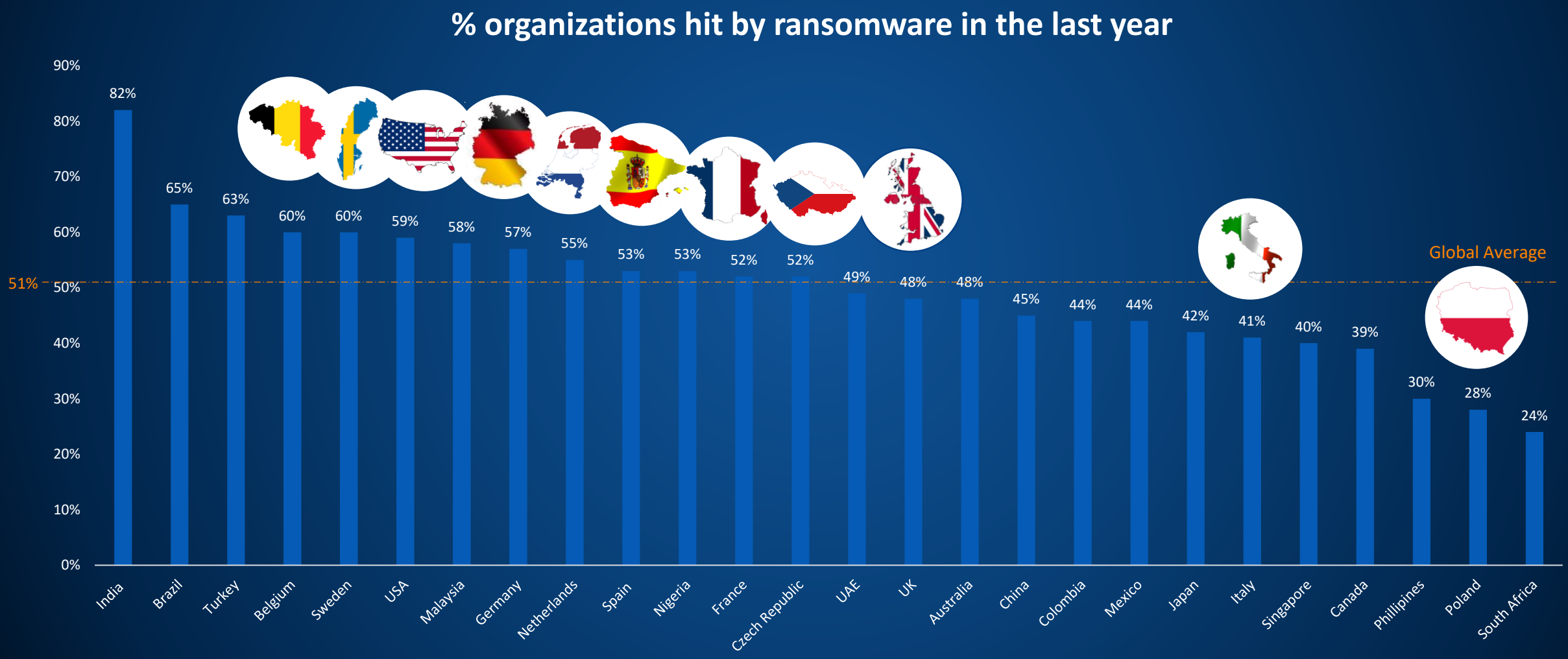
100-1,000 pracowników



1,001-5,000 Pracowniów

Czy w ostatnim roku Twoja organizacja została zainfekowana ransomware?? Base 5,000

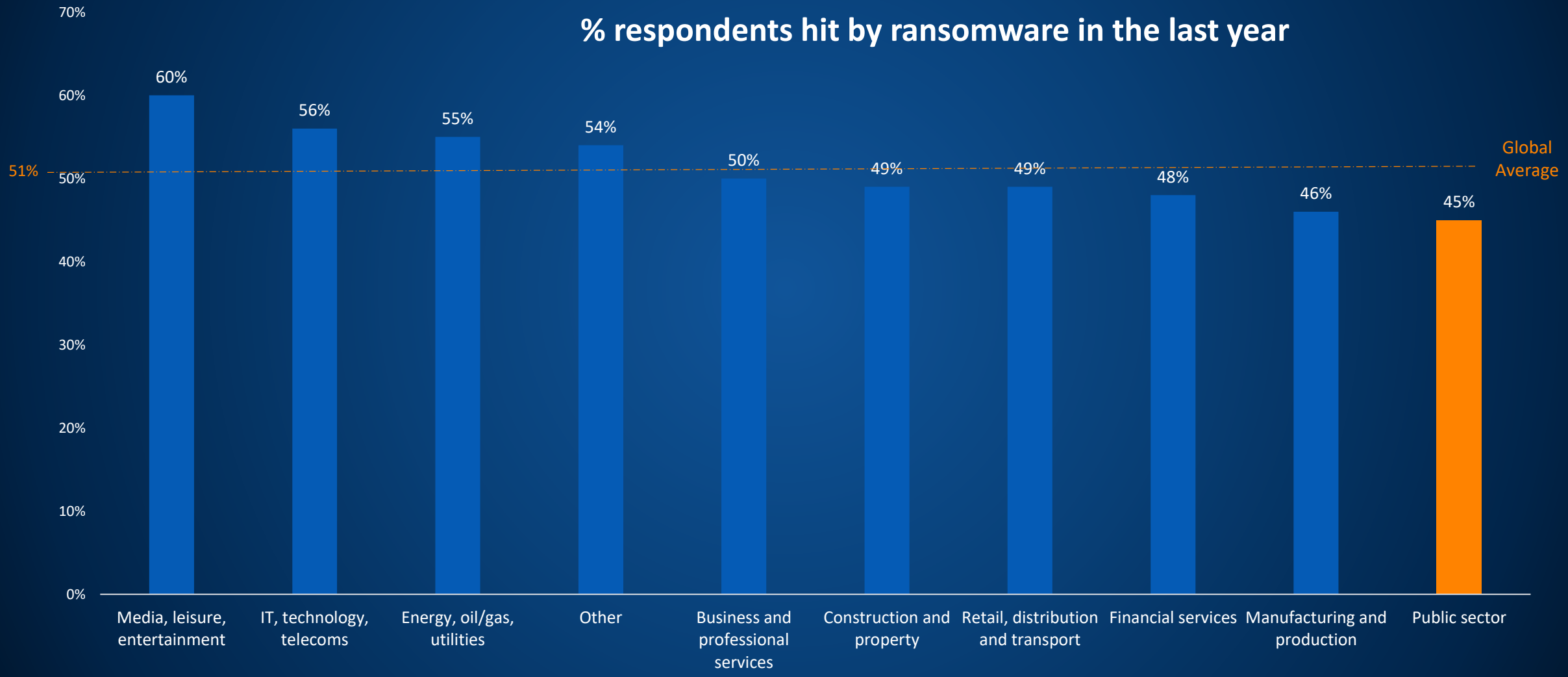
Poziomy Ataku Różnią się na całym świecie



Czy w ostatnim roku Twoja organizacja została zainfekowana ransomware?? Base 5,000

SOPHOS

Sektor publiczny Cierpi Najmniej na Ataki Ransomware



Czy w ostatnim roku Twoja organizacja została zainfekowana ransomware?? Base 5,000

SOPHOS

Wpływ Ransomware

SOPHOS

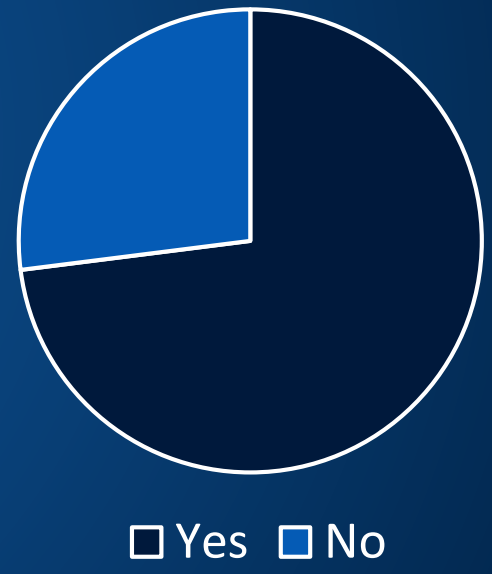
Przestępcom udaje się Zaszyfrować Dane w 3 na 4 Atakach

73% Przestępcom udaje się **zaszyfrować** danea

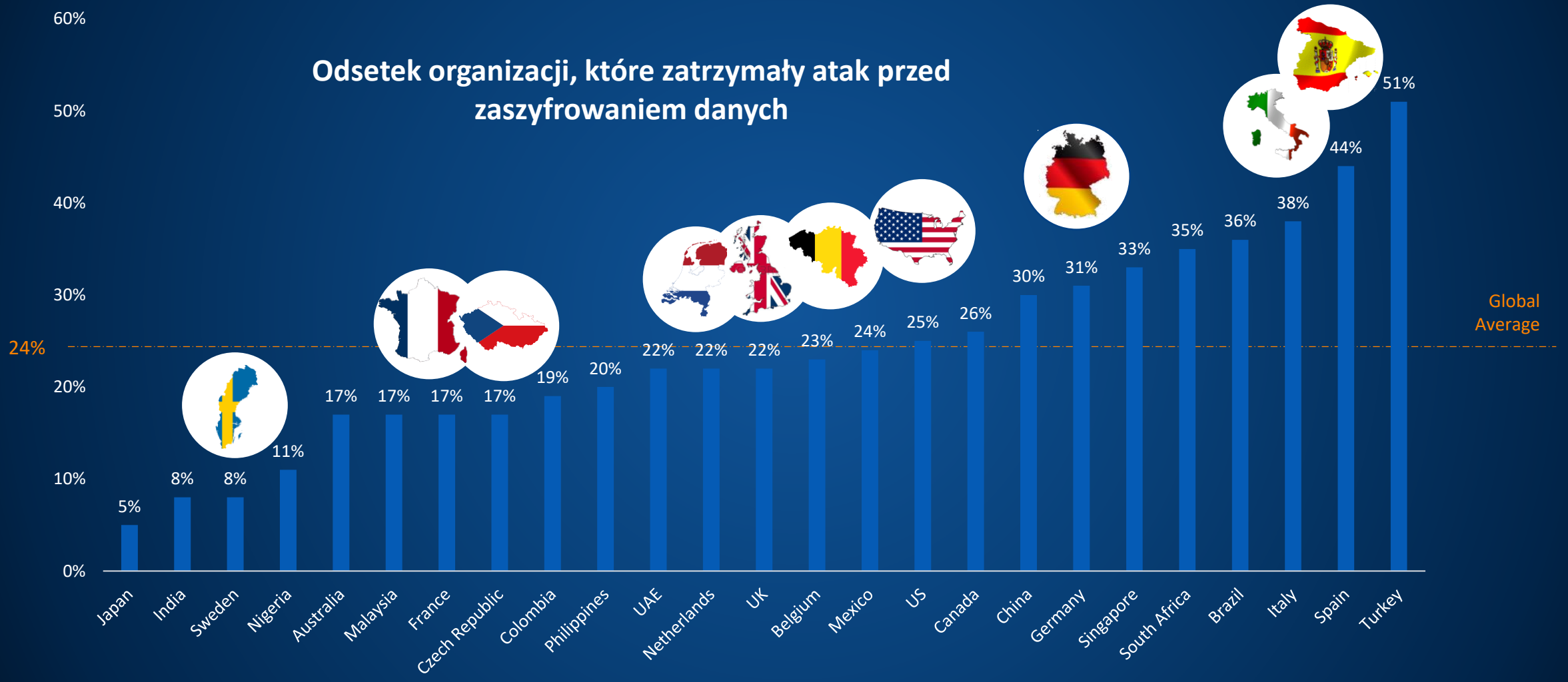
24% Atak został **zatrzymany,** zanim dane mogły zostać zaszyfrowane

3% Dane **nie zaszyfrowane** ale ofiara wciąż przetrzymywana w celu okupu

Czy cyberprzestępcom udało się zaszyfrować dane organizacji w najbardziej znaczącym ataku ransomware?



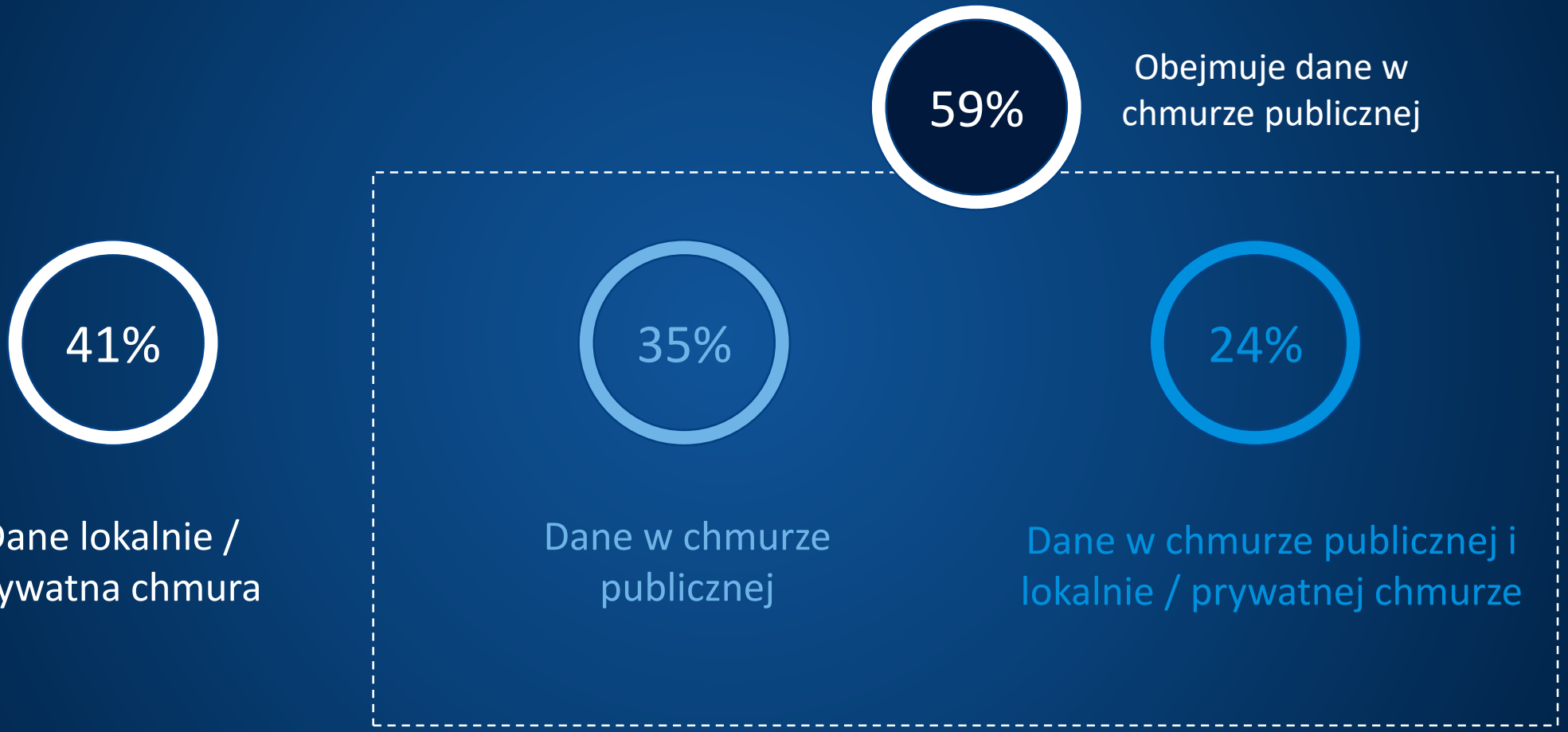
Ataki, które Najprawdopodobniej mogły się udać w Japonii



Percentage of respondents that answered 'No, the attack was stopped before the data could be encrypted' to: Did the cybercriminals succeed in encrypting your organization's data in the most significant ransomware attack? Base 2,538.

SOPHOS

Dane w Publicznej Chmurze są głównym celem ataków



Odsetek respondentów, którzy odpowiedzieli „Nie, atak został zatrzymany, zanim dane mogły zostać zaszyfrowane”, Czy cyberprzestępcom udało się zaszyfrować dane organizacji podczas najbardziej znaczącego ataku ransomware? Base 1,849

Jedna na Cztery Ofiary Płaciła okup by odzyskać Dane

26%

Zapłaciło okup

Czy Twoja organizacja odzyskała dane z ataku ransomware? Pytanie zadawane tylko przez respondentów, których organizacja miała atak ransomware, w którym dane były szyfrowane. Base 1,849

SOPHOS

Indie i Szwecja najczęściej Płaciły okup

Odsetek respondentów, którzy odpowiedzieli „Tak, zapłaciliśmy okup", Czy Twoja organizacja odzyskała dane w przypadku ataku ransomware? Pytanie zadawane tylko do respondentów, których organizacja miała atak ransomware, w którym dane były szyfrowane. Base 1,849.

Prawie wszyscy odzywskują swoje Dane

73%

Ataków kończy się zaszyfrowaniem danych

94%

Odzyskuje swoje dane

56%

Wykorzystało kopie zapasowe do odzyskania danych

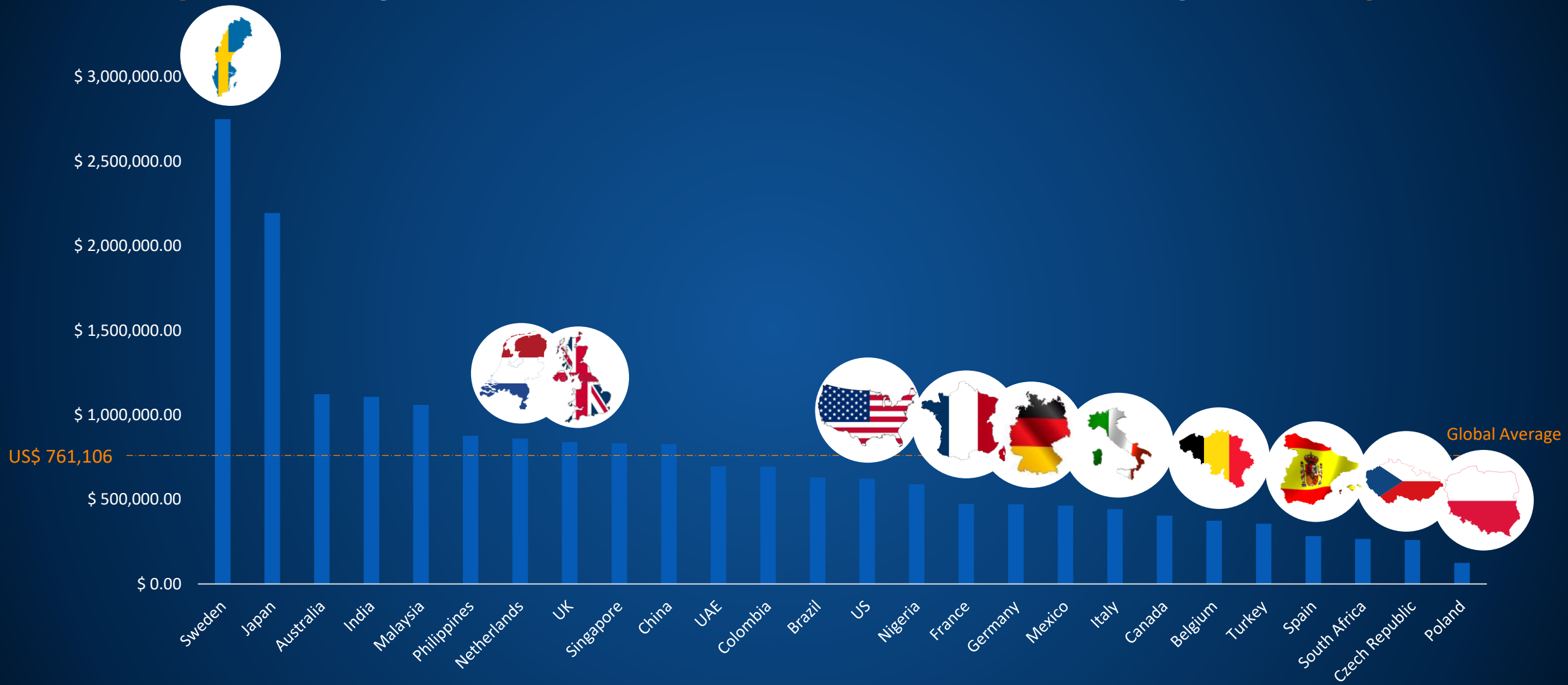
Czy Twoja organizacja odzyskała dane z ataku ransomware? Base 1,849

SOPHOS

koszty przywrócenia Różnią się w zależności od wielkości

Jaki był przybliżony koszt dla Twojej organizacji w celu skorygowania skutków ostatniego ataku ransomware (biorąc pod uwagę czas przestoju, czas ludzi, koszt urządzenia, koszt sieci, utraconą oportunicję, zapłacony okup itp.)? Pytanie zadawane tylko przez respondentów, których organizacja została dotknięta oprogramowaniem ransomware w ostatnim roku. Base 2,538

Koszty usunięcia Ransomware uzależnione per Kraj



Jaki był przybliżony koszt dla Twojej organizacji w celu skorygowania skutków ostatniego ataku ransomware (biorąc pod uwagę czas przestoju, czas ludzi, koszt urządzenia, koszt sieci, utraconą szansę, zapłacony okup itp.)? Pytanie zadawane tylko przez respondentów, których organizacja została dotknięta oprogramowaniem ransomware w ostatnim roku. Base 2,538

Płacenie Okupu Podwaja koszty

Did your organization get the data back in the most significant ransomware attack? Base 1,849. ***Paid the ransom*** *combines responses "Yes, we paid the ransom" and "No, even though we paid the ransom".* ***Didn't pay the ransom*** *combines responses "Yes, we used backups to restore the data", "Yes, we used other means to get our data back" and "No, we didn't pay the ransom".*

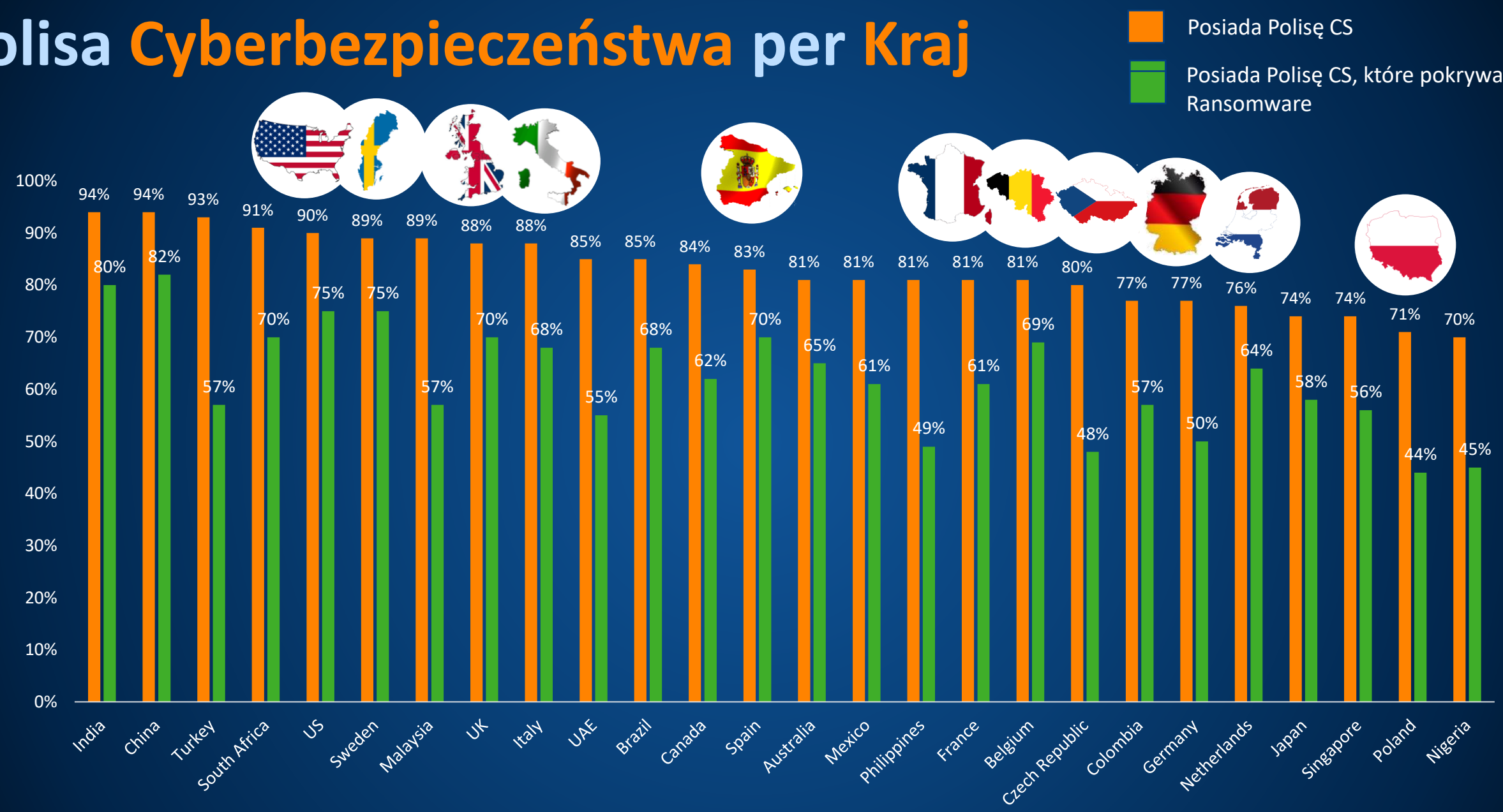
Rola Ubezpieczenia/Polisy

SOPHOS

1 na 5 Posiada Niejednolitą Polisę Cyberbezpieczeństwa

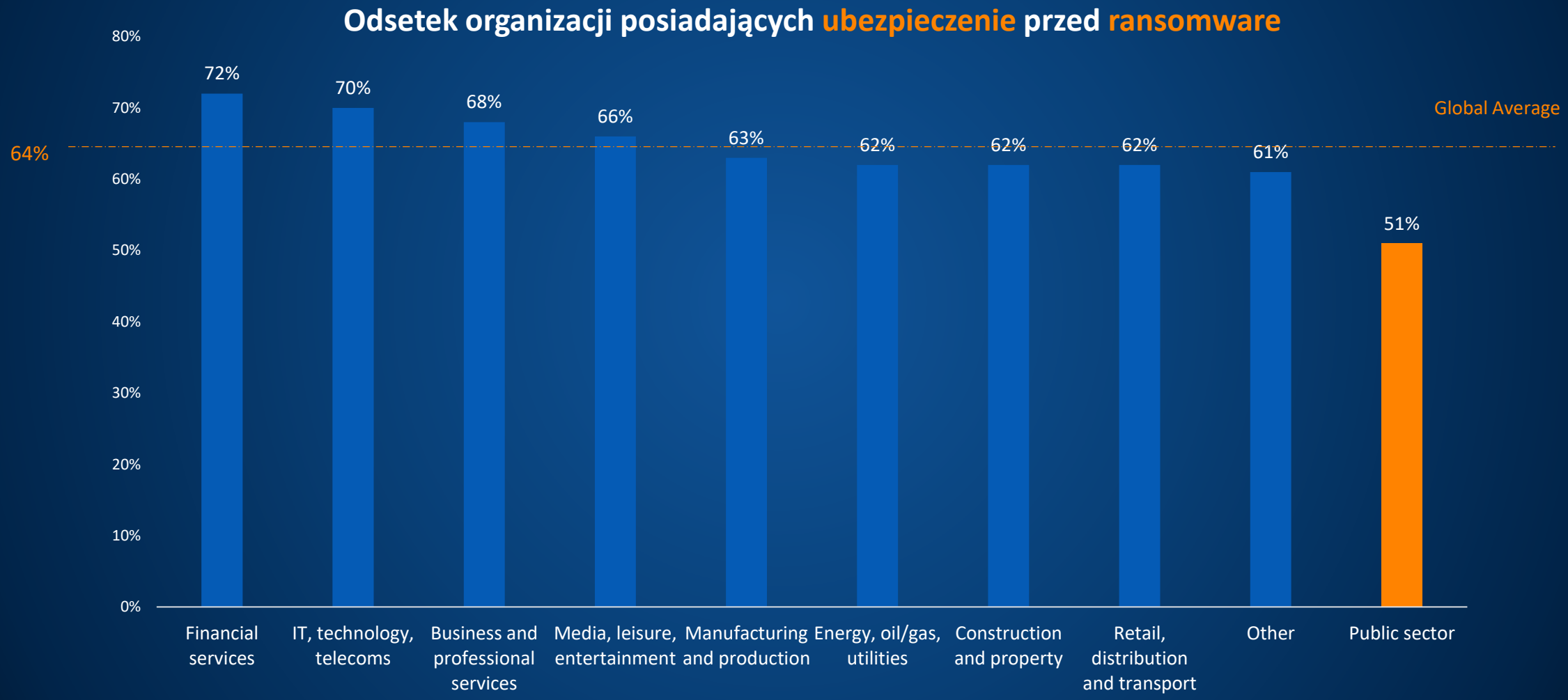
Czy Twoja organizacja ma Polisę cyberbezpieczeństwa, które obejmuje zainfekowane oprogramowaniem ransomware? Base 5,000

Polisa Cyberbezpieczeństwa per Kraj



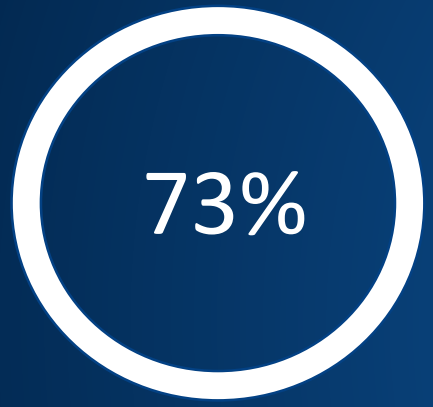
Czy Twoja organizacja ma Polisę cyberbezpieczeństwa, które obejmuje zainfekowane oprogramowaniem ransomware? Base 5,000

Sektor Publiczny jest Najbardziej Narażony na Koszty związane z Ransomware



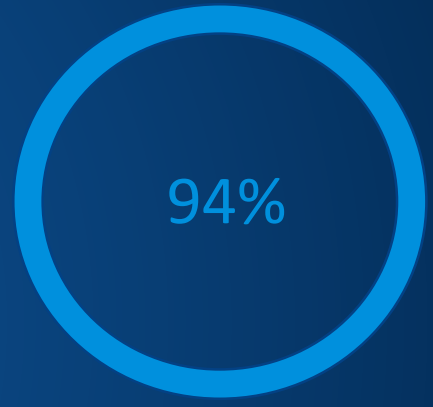
Czy Twoja organizacja ma Polisę cyberbezpieczeństwa, które obejmuje zainfekowane oprogramowaniem ransomware? Base 5,000

Czy Polisa Cyberbezpieczeństwa podsyca płacenie Okupu?



Ataki Ransomware spowodowały **zaszyfrowanie** danych

Organizacje, których dane zostały zaszyfrowane **zapłaciły okup**



Orgnizacje, które zapłaciły, zadeklarowały, że **Ubezpieczenie** spłaciło okup

Odsetek respondentów, którzy wybrali „Tak, zapłaciliśmy okup” i potwierdzili, że zapłacono okup w ramach Polisy cyberbezpieczeństwa..

Techniki Ataku Ransomware

SOPHOS

Atakujący wykorzystują Wiele Taktyk aby przełamać obronę

Jak ransomware dostał się do organizacji	#	%
poprzez pobrany plik/email ze złośliwym linkiem	741	29%
poprzez zdalny atak na serwer	543	21%
poprzez email ze złośliwym załącznikiem	401	16%
Błędne skonfigurowanie instancji chmury publicznej	233	9%
poprzez Protokół Zdalnego Pulpitu (RDP)	221	9%
za pośrednictwem dostawcy	218	9%
poprzez USB/wymienne urządzenie/nośnik danych	172	7%
Inne	0	0%
Nie wiem	9	0%
Total	**2,538**	**100%**

W jaki sposób atak ransomware dostał się do Twojej organizacji? Pytanie zadawane respondentom, których organizacja została dotknięta oprogramowaniem ransomware w ostatnim roku. Base 2,538

Trendy w Atakach

SOPHOS

Od Masowej Dystrybucji … Po Ataki Ukierunkowane

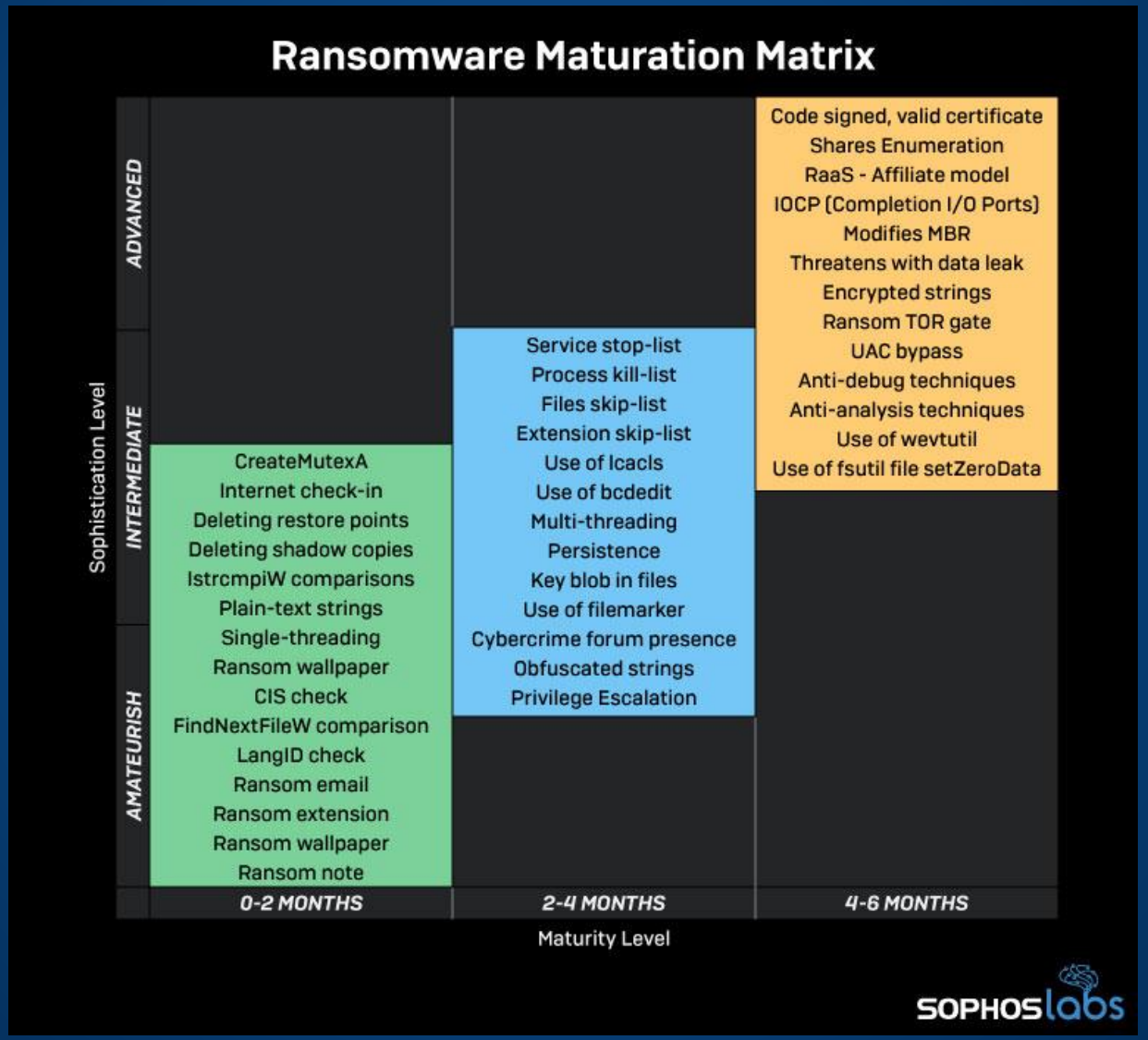
WannaCry, NotPetya etc …		Ryuk, GandCrab, Maze …
Explozywna Dystrybucja		Kilka Atakow Dziennie
Ataki Masowe	**vs.**	Ataki ukierunkowane
Kilka Tygodni		Przez Lata

Starożytne i Prosperujące Rodziny

	BitPaymer	SamSam	Ryuk	Dharma	GandCrab
First Appearance	2017	2015	2018	2016	2018
Type	Targeted	Targeted	Targeted	Targeted	RaaS
Deployment	RDP	RDP	RDP	RDP	RDP/Email/Exploit Kits
Targets	Medium/large organizations	Medium/large organizations	Medium/large organizations	Small organizations	Any
Typical ransom demand	$50,000-$1M+	$40,000	$100,000	$5,000	$1,000-$8,000+
Frequency of attacks	Multiple a week	1+ a day	Multiple a week	Multiple a day	Frequency is unknown due to anyone being able to use the kit, however it is very popular
Desired damage	All servers	All servers and endpoints	All servers	Critical servers	Any
Regions affected	Global	Global with highest % in US	Global	Global	Global
Can be decrypted without paying	No	No	No	No	Some variants but mostly not
Payment method	Bitcoin arranged via email, sometimes dark web onion site	Bitcoin arranged via dark web onion site	Bitcoin arranged via email	Bitcoin arranged via email	Bitcoin arranged via dark web onion site
Additional insights	Spends time to ensure all backups are deleted before the attack	Has a history of targeting healthcare	Spends time to ensure all backups are deleted before the attack; attempts to disable antivirus	Manually attempts to disable antivirus before attacking	Regular updates and support from the developers; recently released all the encryption keys for Syrian victims of GandCrab and said Syria would not be targeted anymore

SophosLabs 2019 Threat Repors
15th November 2018

Ransomwares Maturation Matrix



Więcej informacji…

SOPHOSlabs

Sophos **News**

Maze ransomware: extorting victims for 1 year and counting

SophosLabs Uncut · Maze ransomware

Evolved from "simple" ransomware, Maze has made waves with its public extortion of "customers".

12 MAY 2020

By Sophos

It's been a year since the Maze ransomware gang began its rise to notoriety. Previously identified as "ChaCha ransomware" (a name taken from stream cipher used by the malware to encrypt files, the Maze "brand" was first affixed to the ransomware in May of 2019.

Initial samples of Maze were tied to fake websites loaded with exploit kits. Since then, Maze has been delivered by multiple means: exploit kits, spam emails, and—as the group's operations have become more targeted—Remote Desktop Protocol attacks and other network exploitation.

But aside from the gang's adjustments in initial compromise approaches, the Maze group has risen in prominence largely because of its extortion tactics: following through on threats of public exposure of victims' data in public "dumps" of victims' stolen data, and offering victim data on cybercrime forums if no payment is made.

While Maze did not invent the data-theft/extortion racket, it was among the first ransomware operations to use data theft as a way of twisting the arms of victims to pay up. The Maze gang has made public exposure central to their "brand" identity, and actively seeks attention from press and researchers to promote their brand—and make it easy for victims who might hesitate to pay them to find out their reputation.

Stepping into the spotlight

news.sophos.com/en-us/2020/05/12/maze-ransomware-1-year-counting/

Sophos **News**

LockBit ransomware borrows tricks to keep up with REvil and Maze

SophosLabs Uncut · data breach · exfiltration · I/O Completion Ports · IOCP · LockBit Ransomware · UAC Bypass · User Account Control

Recently-adopted techniques advance LockBit to a major ransomware player...for now.

24 APRIL 2020

By Albert Zsigovits

Ransomware operators are always on the lookout for a way to take their ransomware to the next level. That's particularly true of the gang behind LockBit. Following the lead of the Maze and REvil ransomware crime rings, LockBit's operators are now threatening to leak the data of their victims in order to extort payment. And the ransomware itself also includes a number of technical improvements that show LockBit's developers are climbing the ransomware learning curve—and have developed an interesting technique to circumvent Windows' User Account Control (UAC).

Because of recent dynamics in the ransomware world, we suspect that this privilege-escalation technique will pop up in other ransomware families in the future. We've seen a surge in "imposter" ransomware that are essentially rebranded variants of already-existing ransomware. Not a single day goes by where a new brand of ransomware does not come out. It has become surprisingly easy to clone ransomware and release it, with small modifications, under a different umbrella.

The Ransomware Learning Curve

news.sophos.com/en-us/2020/04/24/lockbit-ransomware-borrows-tricks-to-keep-up-with-revil-and-maze/

Rekomendacje

SOPHOS

Podsumowując...

Ransomware jest **prawdziwym zagrożeniem**

Jedna na cztery ofiary **zatrzymuj** atak

Dane w **publicznej chmurze** są zagrożone

Kopie danych działają

Uważaj na **niejednolite cyber ubezpieczenia**

Atakujący **próbują i próbóją** ponownie

Załóż, **że będziesz** celem ataku

Zainwestuj w technologię **anti-ransomware**

Chroń dane **niezależnie** gdzie są

trzymaj je **poza siedzibą** i **offline**

Zabezpiecz się przed **ransomware**

Wdróż **wielowarstwową** ochronę

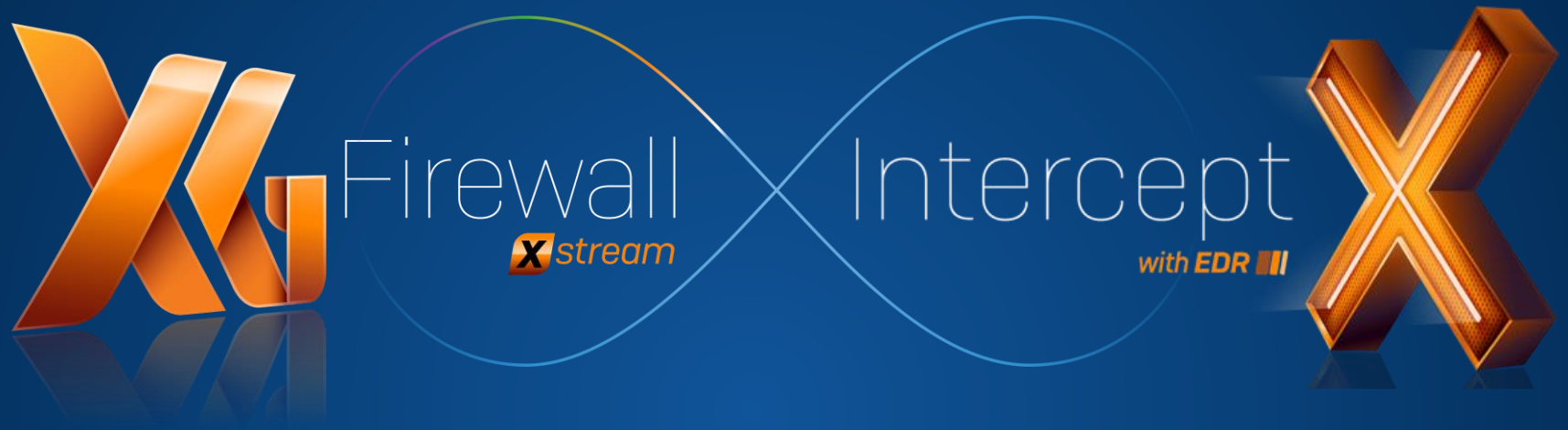
Jak Sophos może Ci pomóc

SOPHOS

Wdróż Intercept X

29%	21%	16%	9%	9%	9%	7%
File download/email with malicious link	Remote attack on server	Email with malicious attachment	Remote Desktop Protocol	Misconfigured public cloud instances	Supplier	USB/ Removable media

Wdróż Intercept X + XG Firewall



29%	21%	16%	9%	9%	9%	7%
File download/email with malicious link	Remote attack on server	Email with malicious attachment	Remote Desktop Protocol	Misconfigured public cloud instances	Supplier	USB/ Removable media

Zabezpiecz Publiczną Chmurę z Sophos

aws Google Cloud Azure

Cloud Storage & Databases

Cloud Virtual Machines

Containers & Serverless

Cloud Optix

SOPHOS Intercept X For Server with EDR

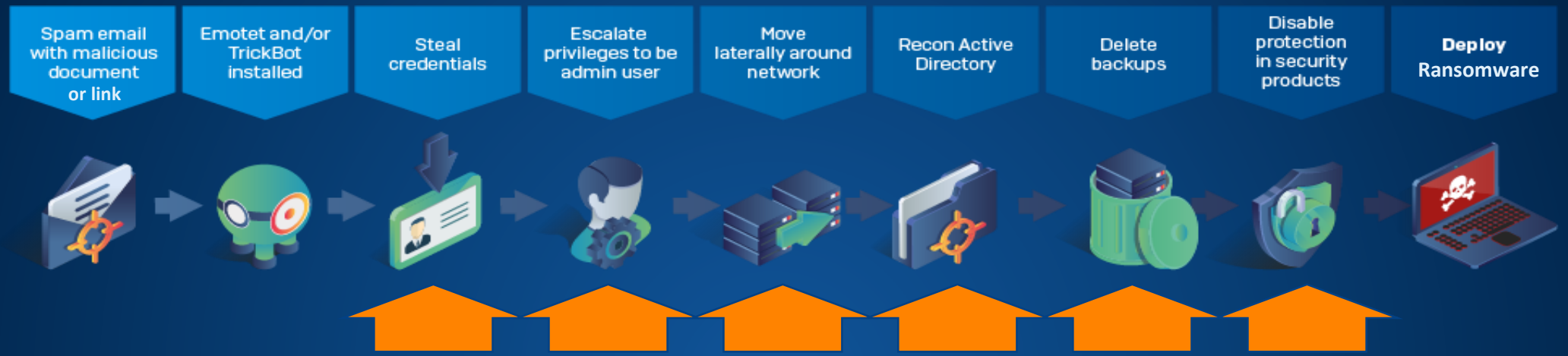
XG Firewall Xstream

Vulnerability Analysis | Identity Security | Workload Protection | Network Firewalling

SOPHOS

Zablokuj Big Game Hunting z Intercept X i EDR

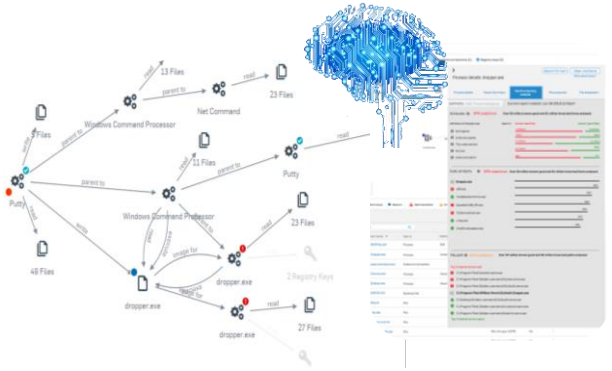
Intercept X with EDR



Deploy protections against active attacks

- IDENTITY THEFT
- PROCESS PRIVILEGE ESCALATION
- MALICIOUS PROCESS MIGRATION
- REGISTRY BASE MODIFICATION
- APC VIOLATION ATOM BOMBING
- CODE CAVE
- MAN-IN-THE-BROWSER
- POWERSHELL OR MALICIOUS MACROS
- LATERAL MOVEMENT

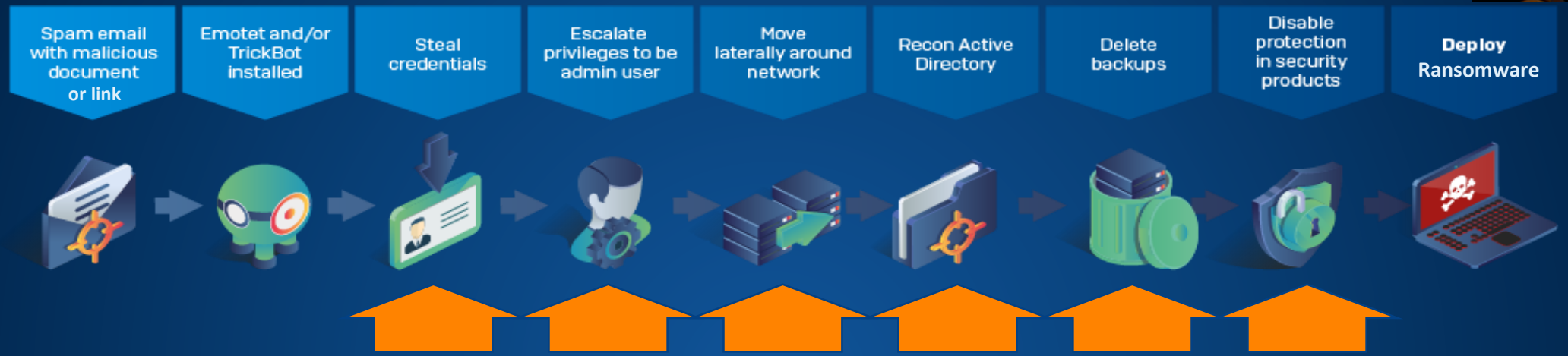
- Deploy **EDR**
- Put active monitoring and response in place (**SOC**)



SOPHOS

Zablokuj Big Game Hunting z usługą Sophos MTR

SOPHOS Managed Threat Response



VansonBourne

8 out of 10

experience difficulties in hiring and retaining experts

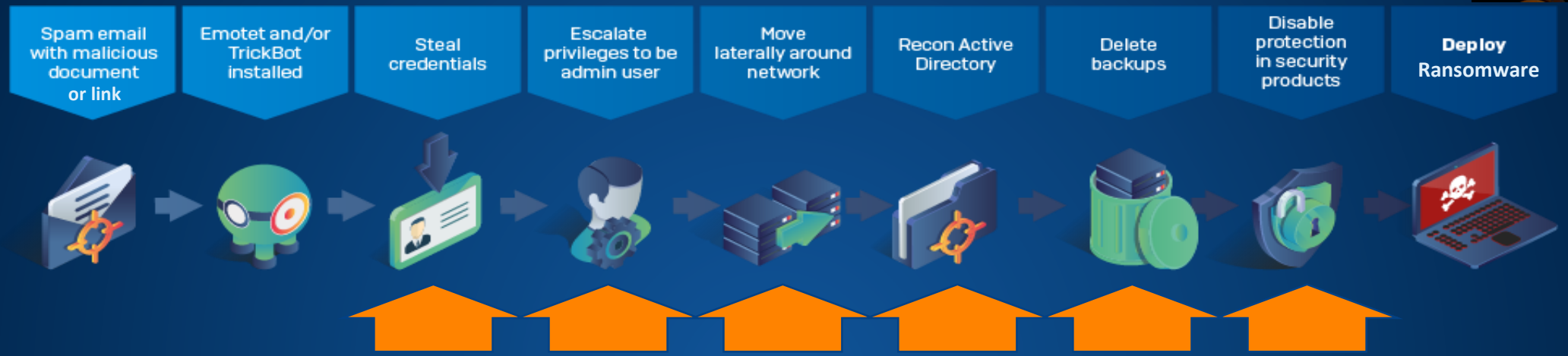
Not to mention week-end…

…and night shifts!

SOPHOS

Zablokuj Big Game Hunting with usługą Sophos MTR

SOPHOS Managed Threat Response



VansonBourne

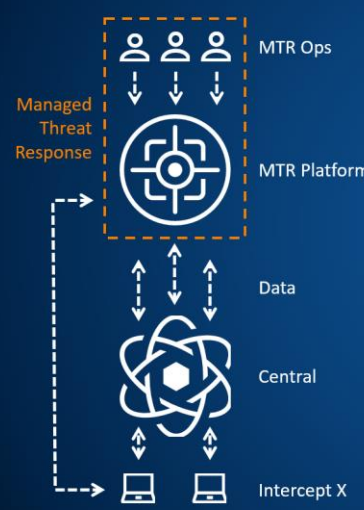
8 out of 10

experience difficulties in hiring and retaining experts

Not to mention week-end…

…and night shifts!

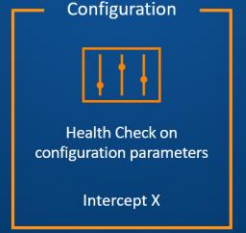
Active Threat Hunting 24x7 + 365 days a year



Intercept X with EDR + MTR advanced IoCs

IPS Events + ATP Events

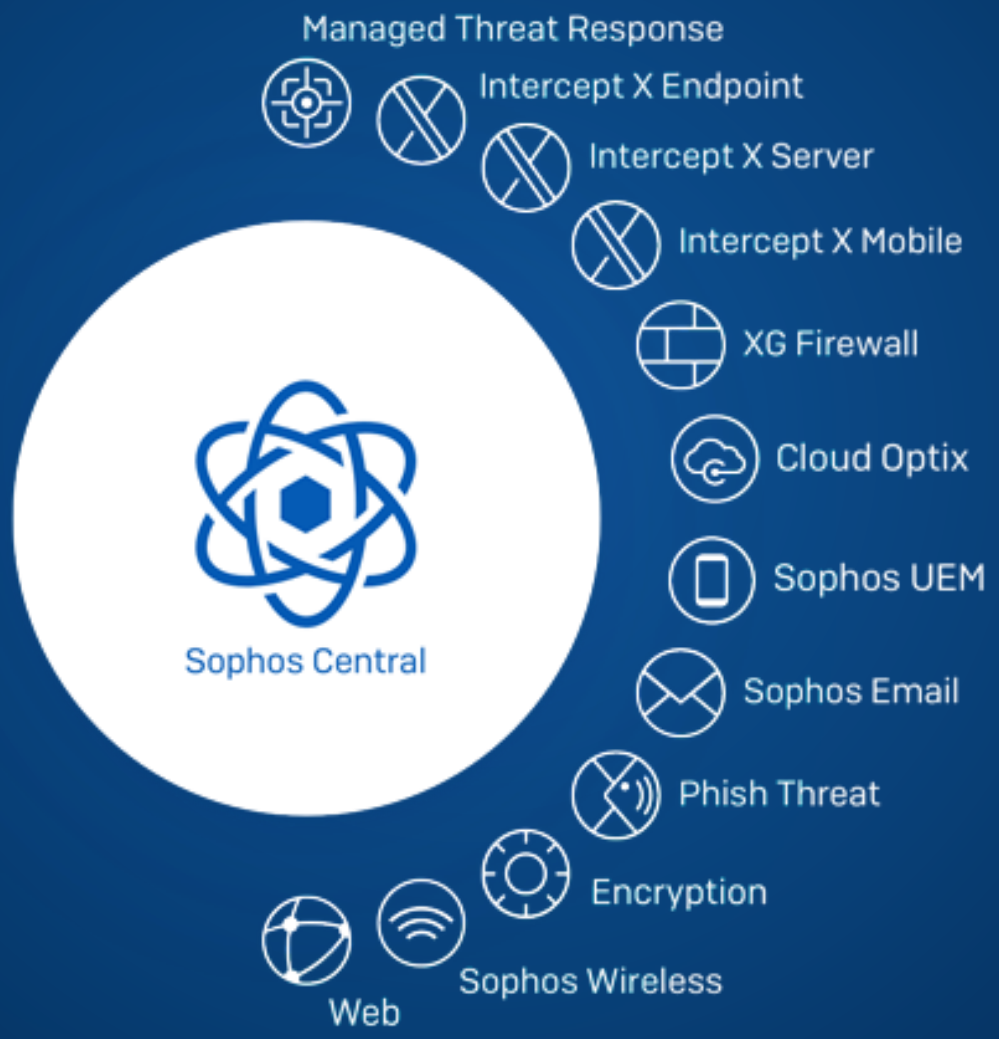
Cloud Optix Anomalies *(login, outgoing traffic …)* + Amazon GuardDuty *(CloudTrail, VPC Flow, DNS logs)*

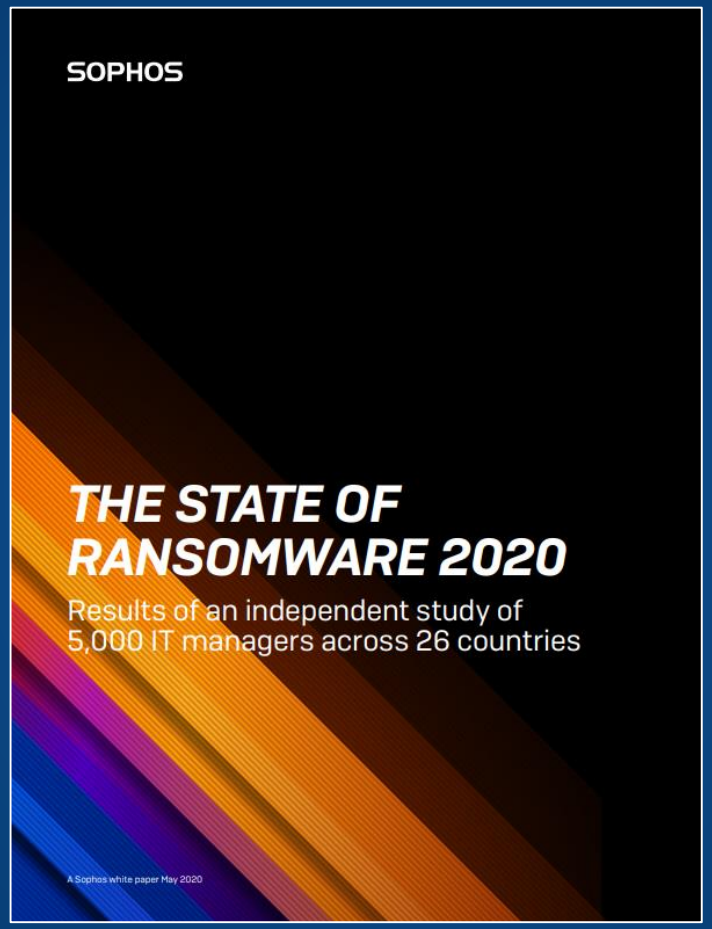


SOPHOS

SOPHOS

Ujednolicone zarządzanie z Sophos Central





www.sophos.com/ransomware2020

Pytania ?

SOPHOS

SOPHOS

Cybersecurity evolved.