El estado del ransomware 2021

SOPHOS

Datos demográficos: 5400 responsables de TI de 30 países

País	N.º de encuestados	País	N.º de encuestados	País	N.º de encuestados
Australia	250	India	300	Arabia Saudita	100
Austria	100	Israel	100	Singapur	150
Bélgica	100	Italia	200	Sudáfrica	200
Brasil	200	Japón	300	España	150
Canadá	200	Malasia	150	Suecia	100
Chile	200	México	200	Suiza	100
Colombia	200	Países Bajos	150	Turquía	100
República Checa	100	Nigeria	100	EAU	100
Francia	200	Filipinas	150	Reino Unido	300
Alemania	300	Polonia	100	EE. UU.	500

VansonBourne

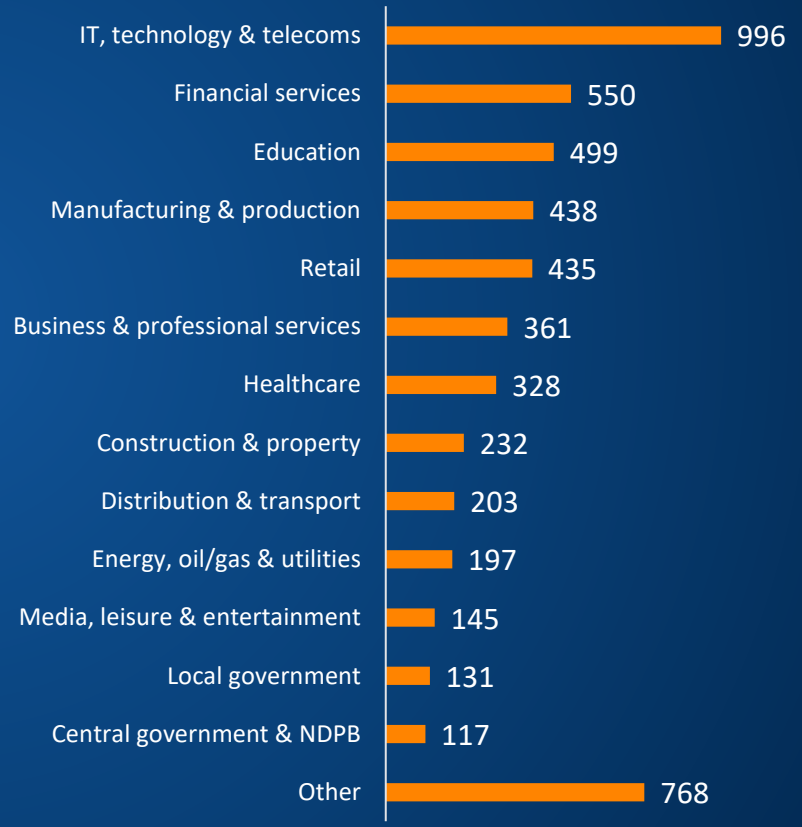
SOPHOS

División demográfica…

…por número de empleados

¿Cuántos empleados tiene su empresa en todo mundo? [5400]

…por sector



¿A qué sector pertenece su empresa? [5400]

Principales conclusiones

El 37 %

de las empresas encuestadas se vieron **afectadas por el ransomware en el último año**

El 54 %

de las empresas afectadas por el ransomware afirmaron que **los ciberdelincuentes consiguieron cifrar sus datos**

El 96 %

de las empresas cuyos datos se cifraron **recuperaron datos**

170 000 USD

fue el **rescate medio pagado** en 2020

El 65 %

de los datos cifrados se restauraron de media después de pagar el rescate

1,85 M USD

fue la **factura de recuperación media por un ataque de ransomware**, teniendo en cuenta el tiempo de inactividad, las horas del personal, el coste de los dispositivos, el coste de las redes, las oportunidades perdidas, el rescate pagado, etc.

La prevalencia del ransomware

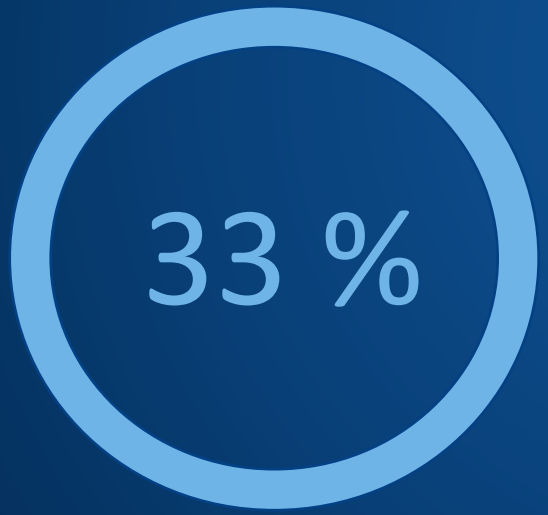
SOPHOS

El ransomware sigue siendo una importante amenaza

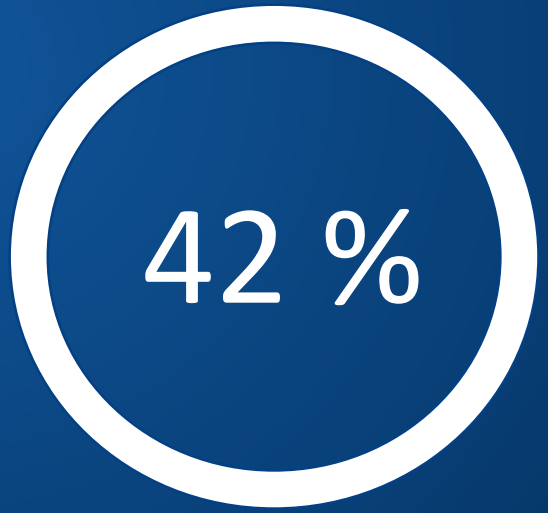
En el último año, ¿se ha visto afectada por el ransomware su empresa? Sí [2021=5400; 2020=5000; 2017=2700], omitiendo algunas opciones de respuesta, divididas por año

Las empresas grandes tienen más posibilidades de sufrir ataques

100 - 1000 empleados



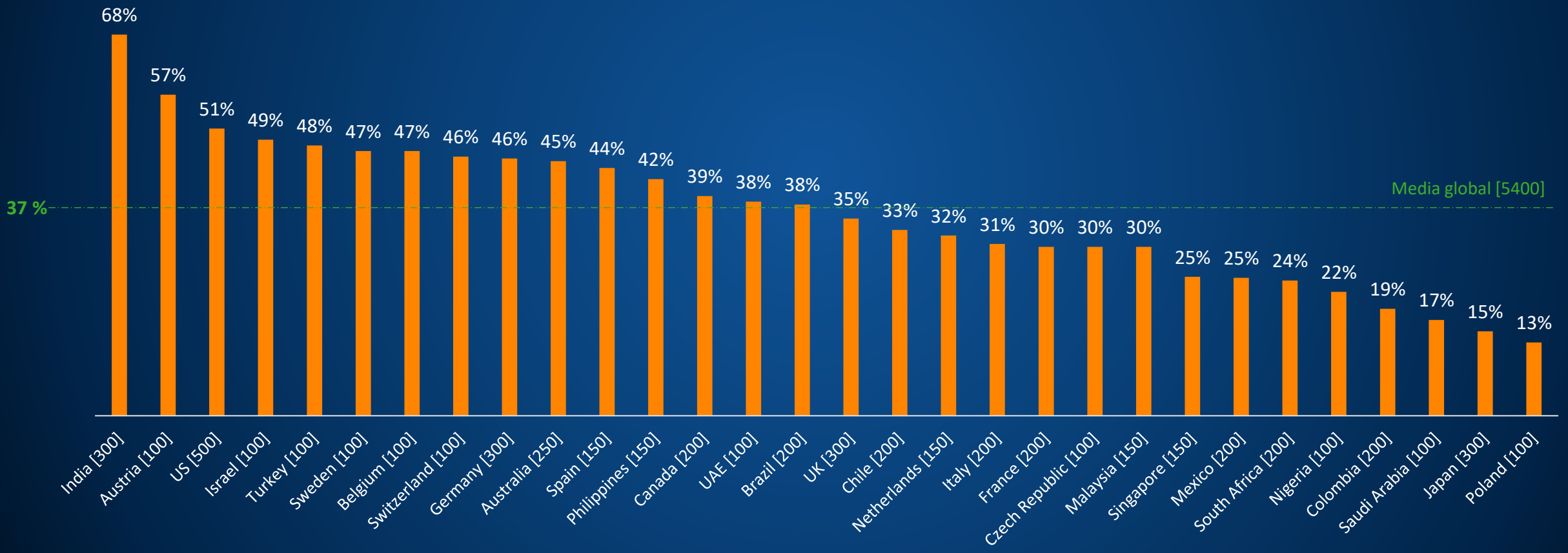
1001 - 5000 empleados



En el último año, ¿se ha visto afectada por el ransomware su empresa? Sí [5400], omitiendo algunas opciones de respuesta, divididas por tipo de empresa

Los niveles de ataque varían en todo el mundo

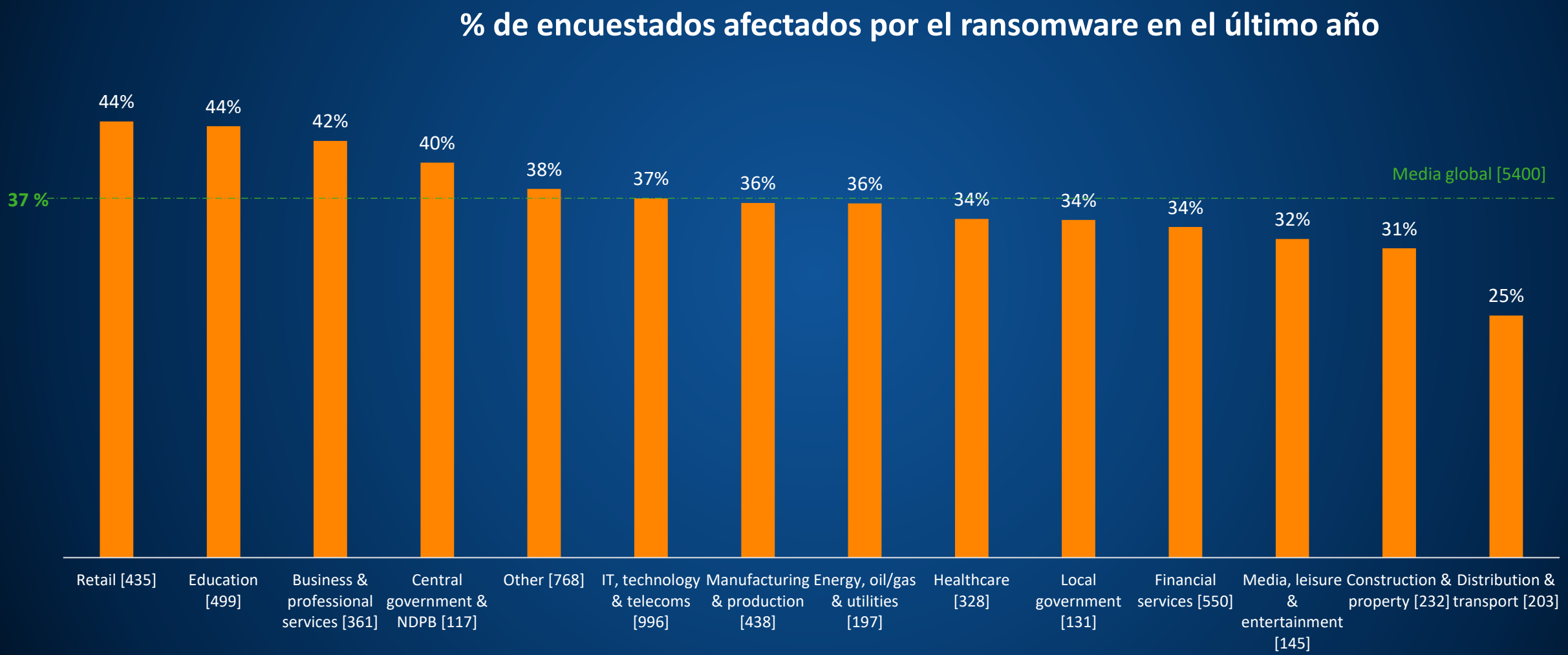
% de encuestados afectados por el ransomware en el último año



En el último año, ¿se ha visto afectada por el ransomware su empresa? Sí [números base en el gráfico], omitiendo algunas opciones de respuesta, divididas por país

SOPHOS

Comercio minorista y educación son los más atacados por el ransomware

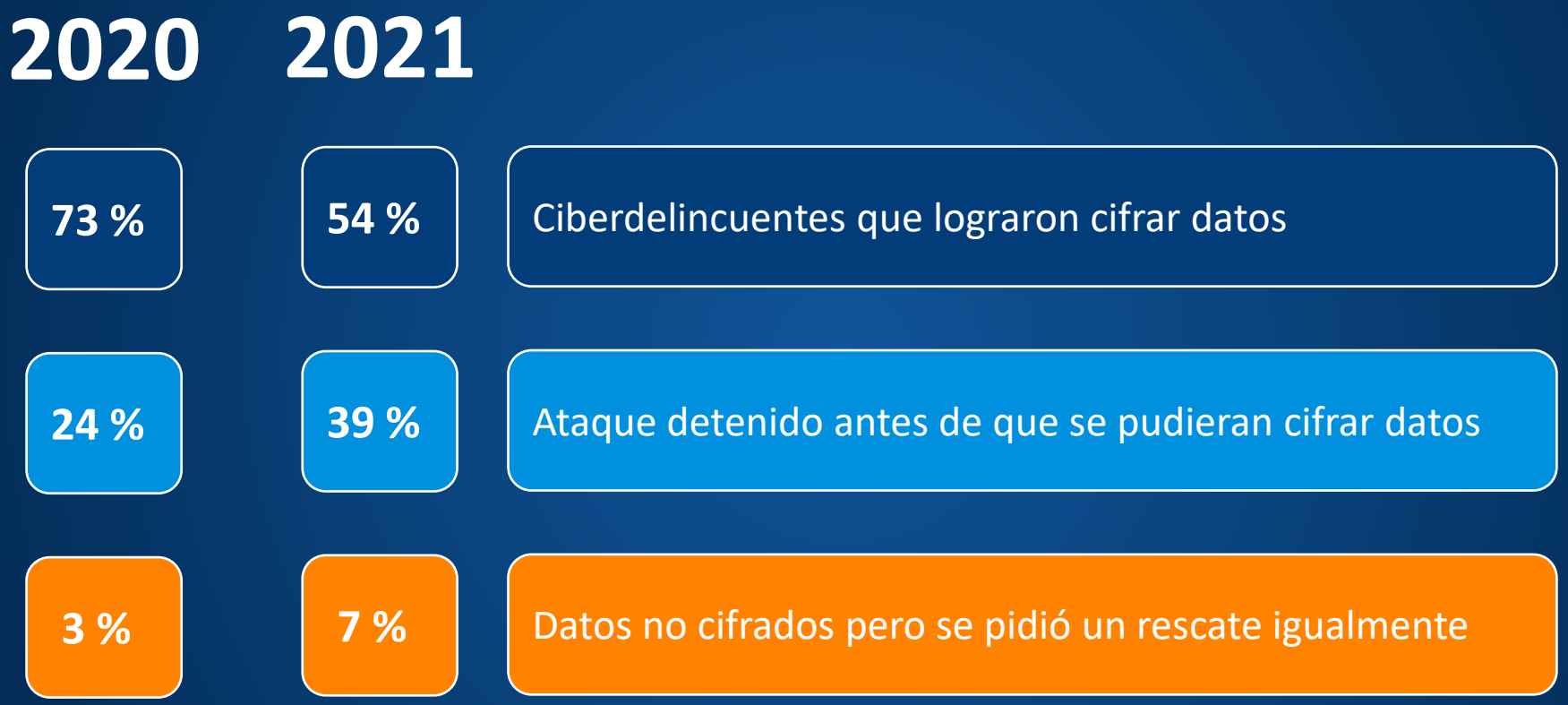


En el último año, ¿se ha visto afectada por el ransomware su empresa?
Sí [números base en el gráfico], omitiendo algunas opciones de respuesta, divididas por sector

El impacto del ransomware

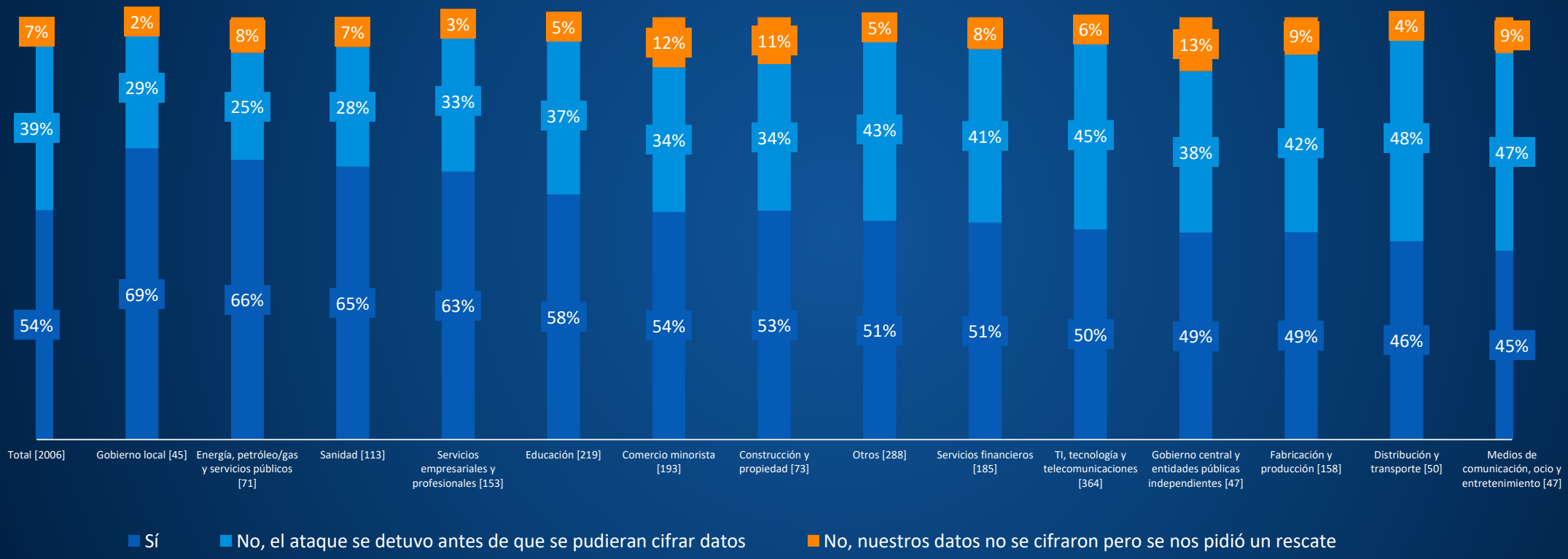
SOPHOS

El cifrado va en descenso. La extorsión va en aumento.



¿Consiguieron los ciberdelincuentes cifrar los datos de su organización en el ataque de ransomware más importante? [2021=2006; 2020=2538] empresas que se han visto afectadas por el ransomware en el último año, omitiendo algunas opciones de respuesta, divididas por año

La capacidad de detener el cifrado varía enormemente según el sector



¿Consiguieron los ciberdelincuentes cifrar los datos de su organización en el ataque de ransomware más importante? [números base en el gráfico] empresas que se han visto afectadas por el ransomware en el último año, omitiendo algunas opciones de respuesta, divididas por sector

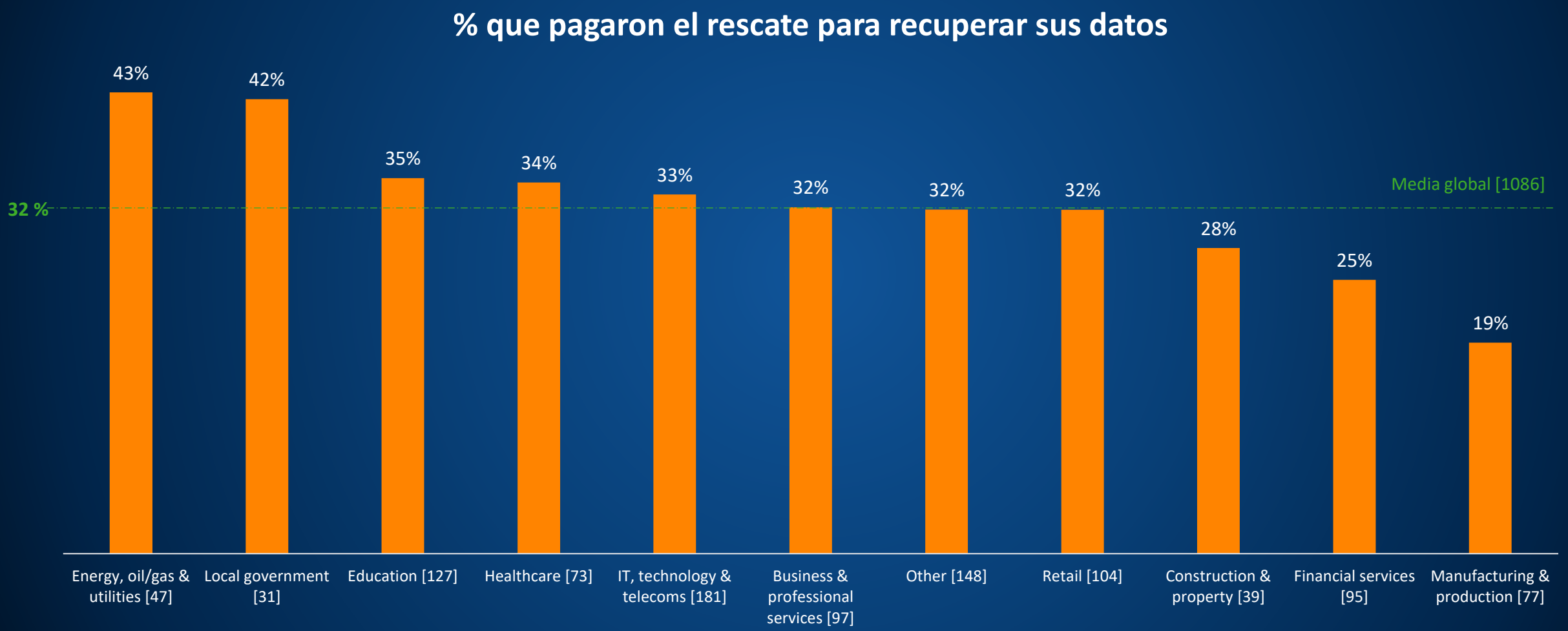
Más víctimas están pagando el rescate

2020	2021	
26 %	32 %	Pagaron el rescate
56 %	57 %	Usaron copias de seguridad
12 %	8 %	Usaron otros medios
94 %	96 %	Total que recuperó sus datos

¿Su empresa recuperó los datos en el ataque de ransomware más importante? [1086 empresas cuyos datos habían sido cifrados]

SOPHOS

La predisposición a pagar varía por sector



¿Su empresa recuperó los datos en el ataque de ransomware más importante? Sí, pagamos el rescate; [número base en el gráfico] empresas en que los ciberdelincuentes lograron cifrar sus datos en el ataque de ransomware más importante, omitiendo algunas opciones de respuesta, divididas por sector

Pagar el rescate solo permite recuperar parte de los datos

29 %

recuperaron hasta la mitad de sus datos después de pagar

8 %

recuperaron todos los datos después de pagar el rescate

Cantidad media de datos que recuperaron las empresas en el ataque de ransomware más importante; [344] empresas que pagaron el rescate para recuperar sus datos

El coste del ransomware

SOPHOS

Los pagos de rescates varían enormemente

10 000 USD

Pago de rescate más común (USD)

170 404 USD

Pago de rescate medio (USD)

3,2 M USD

Pago de rescate más alto (USD)

107 694 USD

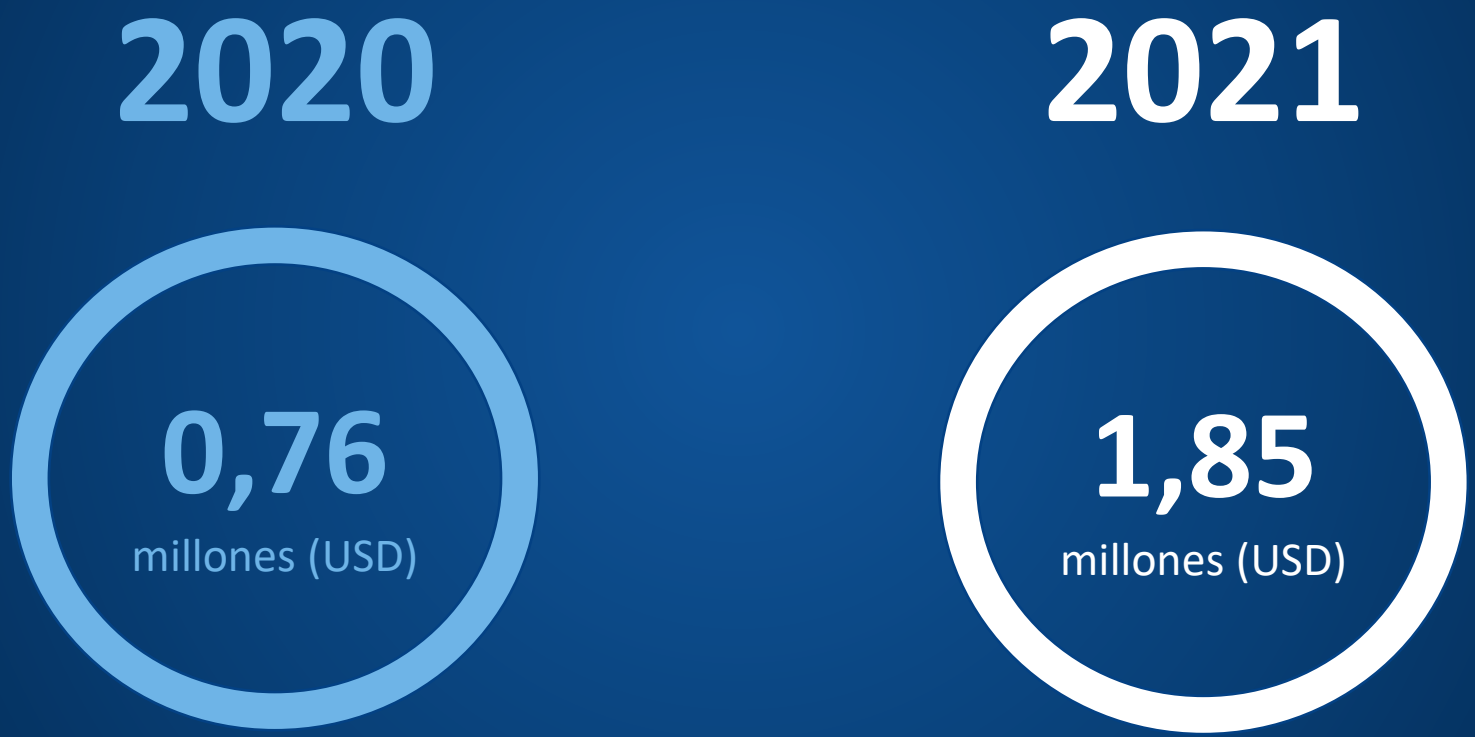
Pago de rescate medio (USD)
100 - 1000 empleados

225 588 USD

Pago de rescate medio (USD)
1001 - 5000 empleados

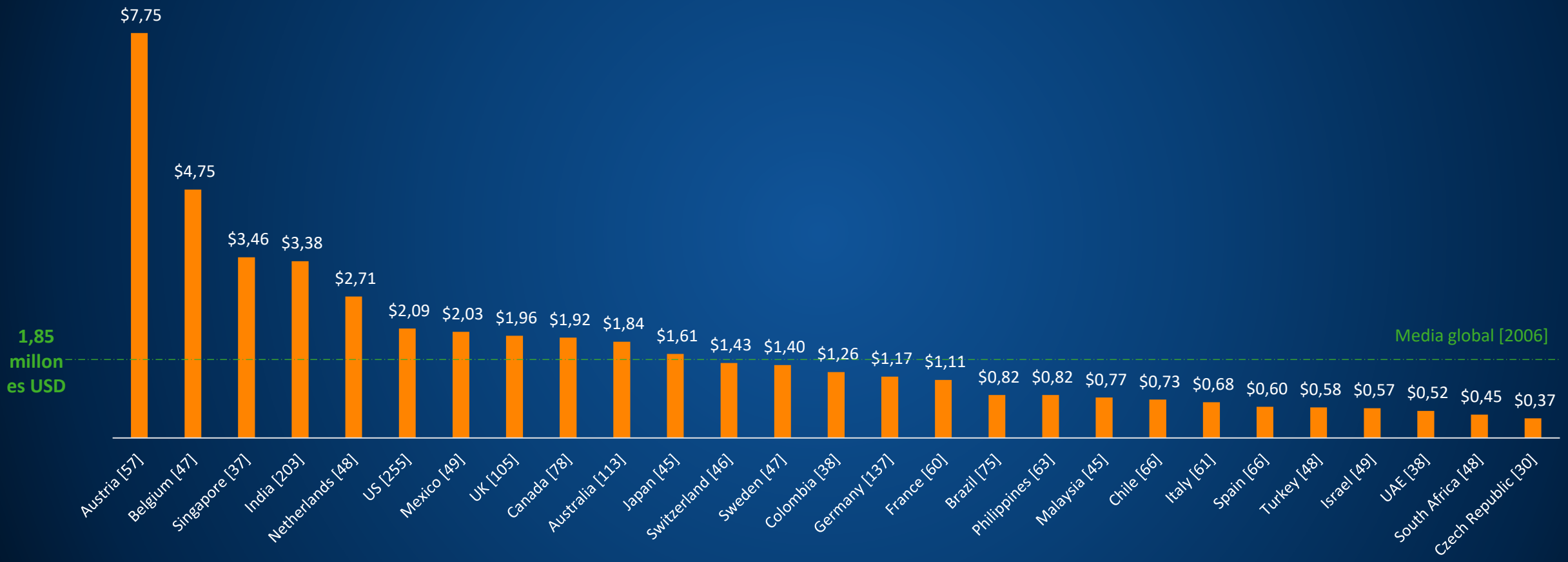
Pago de rescate medio que pagaron las empresas en el ataque de ransomware más importante y el encuestado conocía la suma pagada; [282] empresas que pagaron el rescate para recuperar sus datos o pagaron el rescate pero no recuperaron sus datos

El coste de recuperación del ransomware se ha más que duplicado



Coste medio aproximado para las empresas de rectificar las consecuencias del ataque de ransomware más reciente (considerando el tiempo de inactividad, las horas del personal, el coste de los dispositivos, el coste de las redes, las oportunidades perdidas, el rescate pagado, etc.); [2006] encuestados cuya empresa se ha visto afectada por el ransomware en el último año, divididas por año

Los costes de recuperación del ransomware varían por ubicación



Coste medio aproximado para las empresas de rectificar las consecuencias del ataque de ransomware más reciente (considerando el tiempo de inactividad, las horas del personal, el coste de los dispositivos, el coste de las redes, las oportunidades perdidas, el rescate pagado, etc.); [números base en el gráfico] encuestados cuya empresa se ha visto afectada por el ransomware en el último año, divididas por país

El futuro

SOPHOS

Las expectativas futuras varían

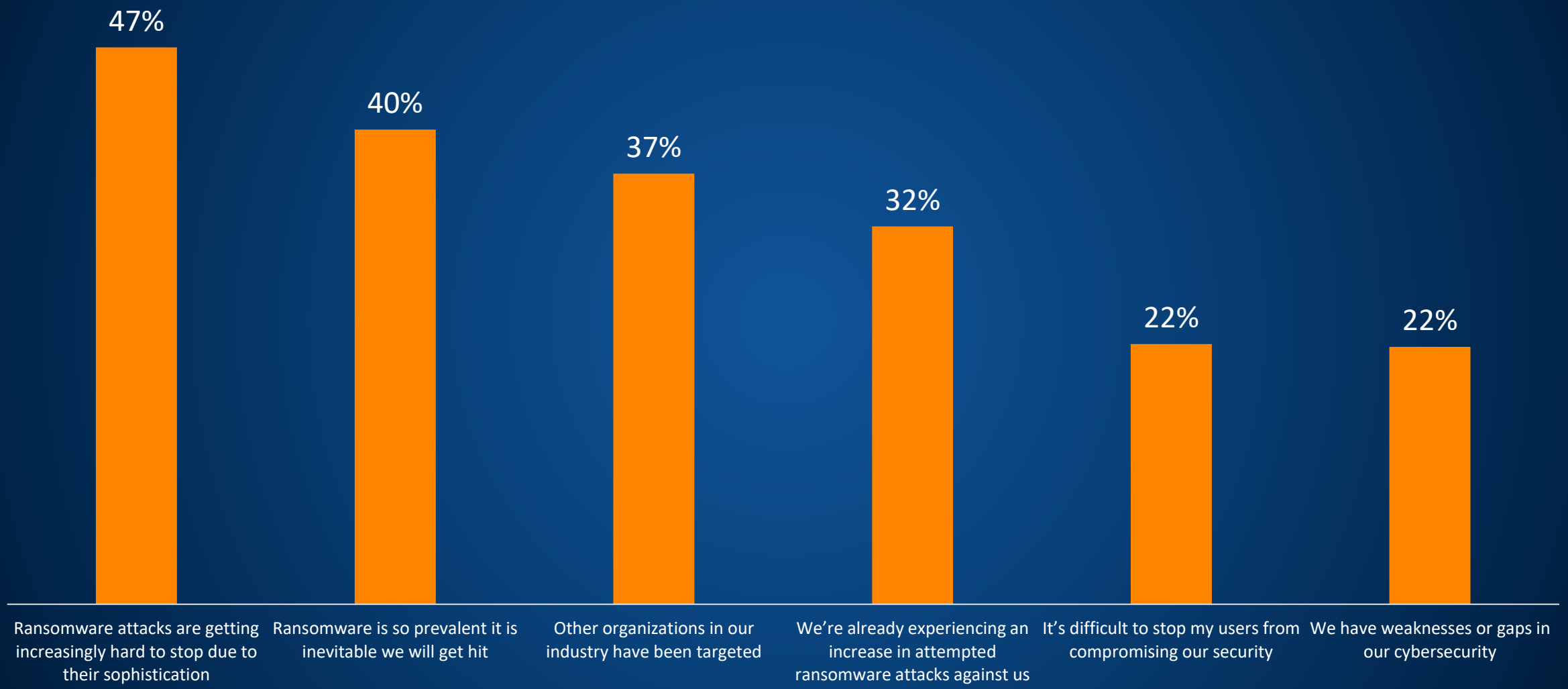
Esperan ataques en el futuro

No esperan ataques en el futuro

Encuestados que contestaron "No" a la pregunta "En el último año, ¿se ha visto afectada por el ransomware su empresa?" [3353]

SOPHOS

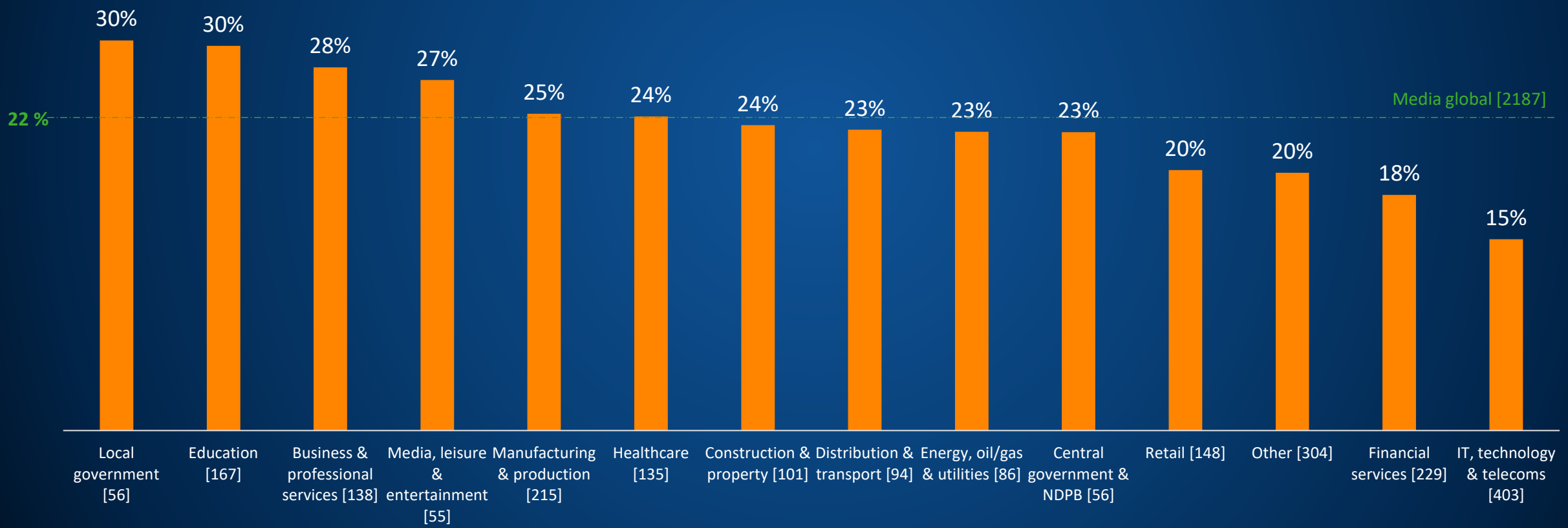
Por qué esperan ataques de ransomware las empresas



¿Por qué espera que su empresa sea atacada por el ransomware en el futuro? [2187] empresas que no han sido atacadas por el ransomware pero que esperan serlo en el futuro, omitiendo algunas opciones de respuesta

El gobierno local es el que tiene más probabilidades de tener carencias de seguridad

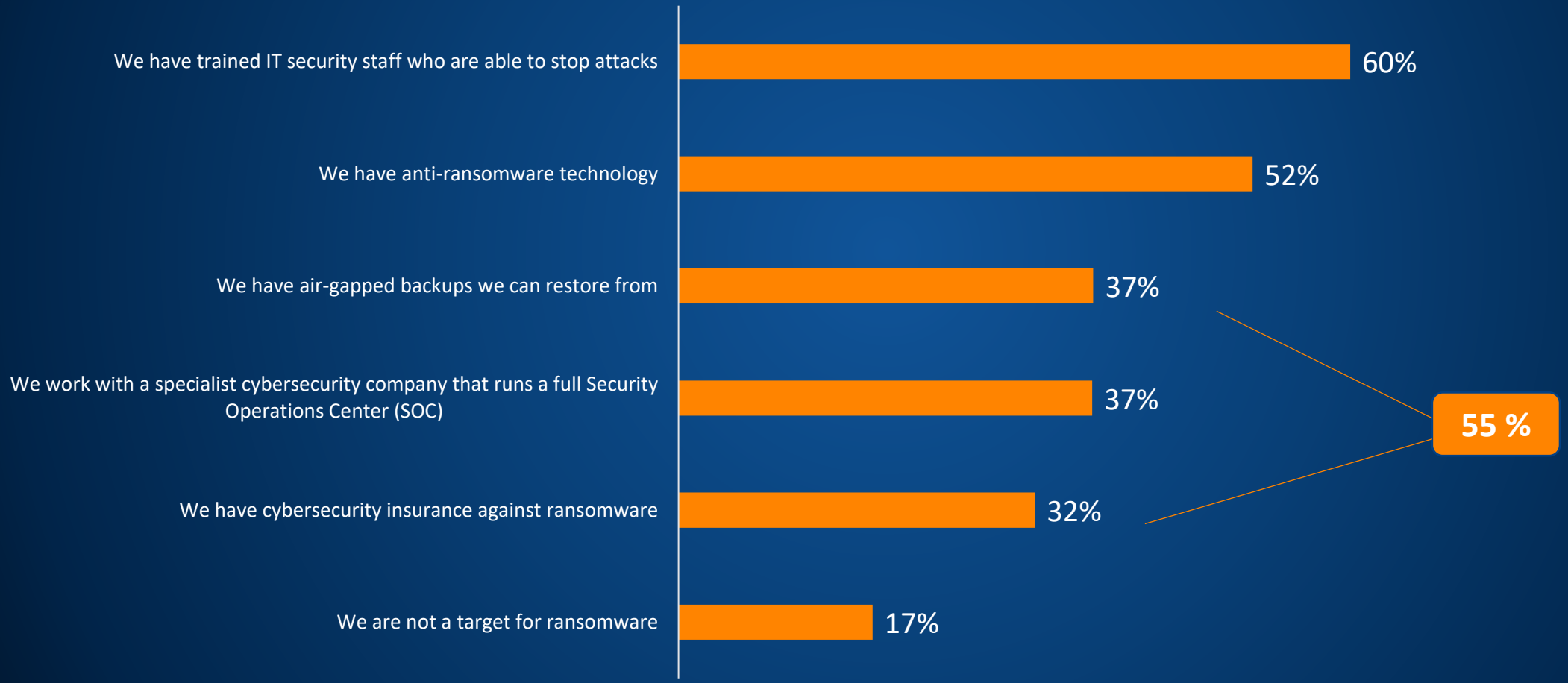
% que esperan sufrir ataques en el futuro y admiten tener deficiencias en su ciberseguridad



¿Por qué espera que su empresa sea atacada por el ransomware en el futuro? Tenemos puntos débiles o carencias en nuestra ciberseguridad; [números base en el gráfico] empresas que no han sido atacadas por el ransomware pero que esperan serlo en el futuro, omitiendo algunas opciones de respuesta, divididas por sector

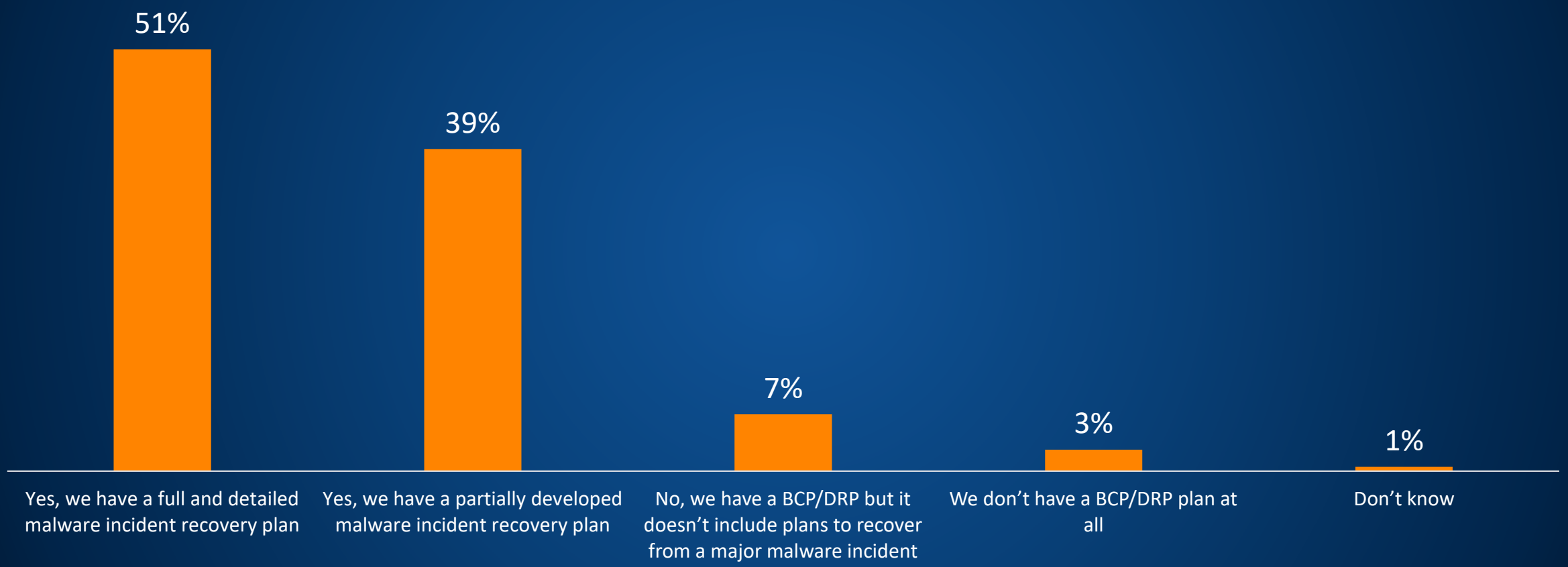
El personal de TI formado da confianza frente al ransomware

Por qué los encuestados no esperan sufrir ataques de ransomware en el futuro



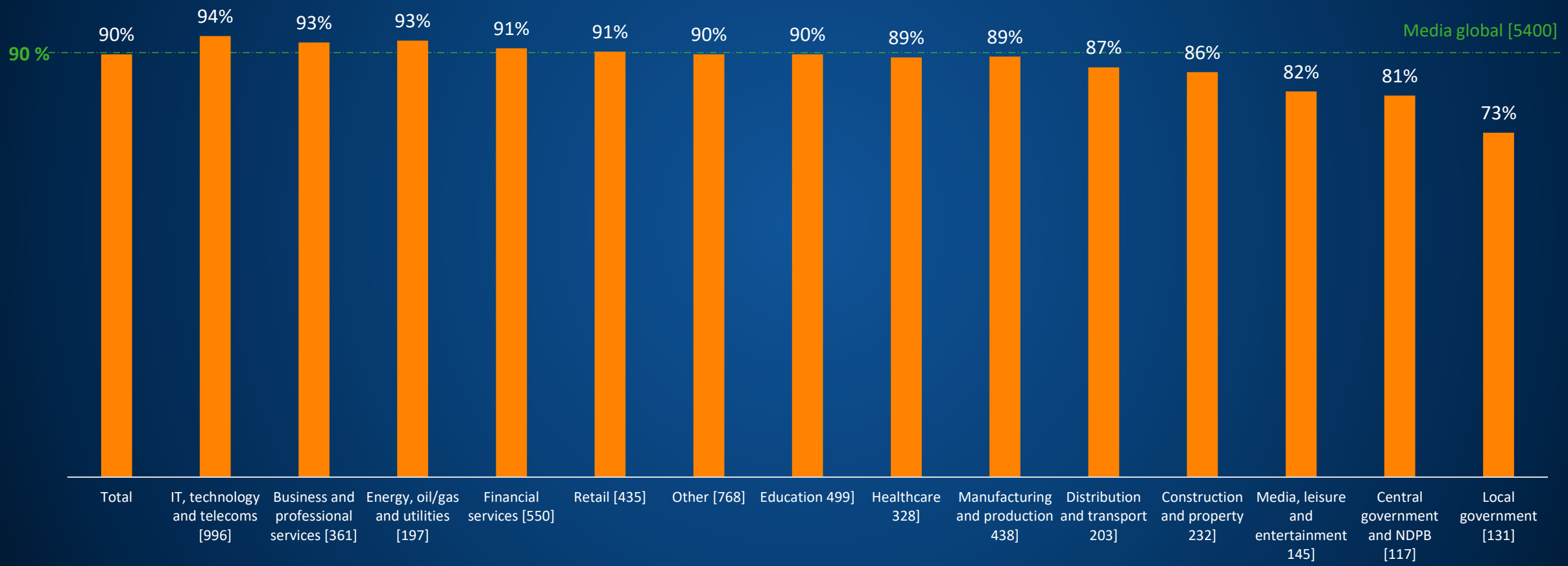
¿Por qué no espera que su empresa sea atacada por el ransomware en el futuro? [1166] empresas que no han sido atacadas por el ransomware ni esperan serlo en el futuro, omitiendo algunas opciones de respuesta

Los planes de recuperación ante incidentes de malware son la norma



¿El plan de continuidad empresarial o plan de recuperación de desastres de su empresa incluye planes para recuperarse de un incidente de malware importante? [5400]

Las organizaciones gubernamentales son las menos preparadas



¿El plan de continuidad empresarial o plan de recuperación de desastres de su empresa incluye planes para recuperarse de un incidente de malware importante? Sí, tenemos un plan de recuperación de incidentes de malware completo y detallado, y Sí, tenemos un plan de recuperación de incidentes de malware parcialmente desarrollado; [números base en el gráfico], omitiendo algunas opciones de respuesta, divididas por sector

Recomendaciones

SOPHOS

Recomendaciones

Dé por hecho que sufrirá un ataque

Planifique su estrategia de seguridad partiendo de este supuesto

Realice copias de seguridad

Son clave para recuperar sus datos

Despliegue una protección por capas

Detenga a los atacantes en cada punto

No pague el rescate

No conseguirá recuperar todos sus datos

Utilice personas y tecnología

La tecnología avanzada y los profesionales humanos son su mejor defensa

Tenga un plan de recuperación del malware

Sepa qué hacer de antemano

¿Cómo os podemos ayudar desde SOPHOS?

SOPHOS

Evolución de las Amenazas

"Living off the Land" techniques to evade detection

"Automated Active Adversaries" combine automation and manual steering

Covertly modifying security controls to evade or prolong detection

Exploiting third-party vendors in the supply chain

Security Program Objective

Protect

Prevent attacks and proactively secure known vulnerabilities

Detect

Detect active attacks and identify potentially malicious behaviors

Respond

Rapidly investigate and remediate incidents to minimize impact

Sophos: Ecosistema de Cibersecuridad Adaptativo (ACE)

Sophos Central
Security management and
SecOps threat hunting

SOFTWARE

XDR Endpoint EDR Mobile Server Email Encryption Firewall WiFi Cloud

HARDWARE

Firewall Switch RED AP

SERVICES

MTR Rapid Response Professional Services

Open APIs

- Industry/Developer
- Service Provider
- Administrator
- Security Operations

THREAT INTELLIGENCE

SOPHOS ARTIFICIAL INTELLIGENCE

SOPHOS LABS

SOPHOS SECURITY OPERATIONS

Data Lake

SOPHOS

Servicio MTR

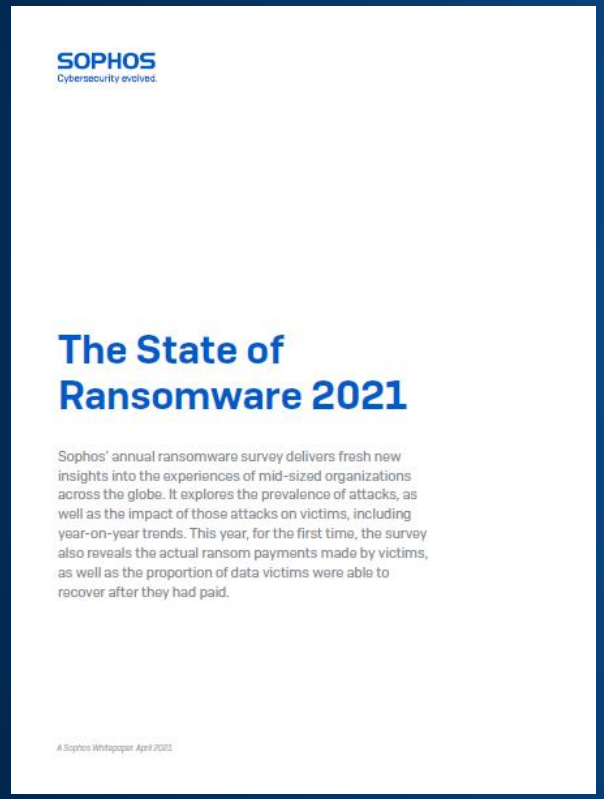
- 24/7 human-led threat hunting.
- We investigate suspicious activity, not just detections.
- Others Stop at Notification. We Take Action.

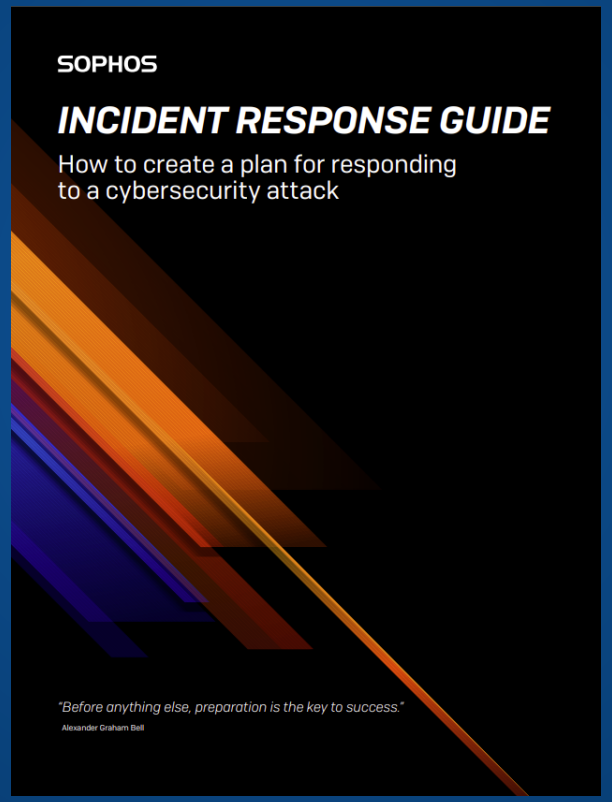
Analyst-Led Threat Hunting and Response

Targeted Actions to Neutralize Threats

Complete Transparency and Control

Más recursos





SOPHOS

Cybersecurity evolved.