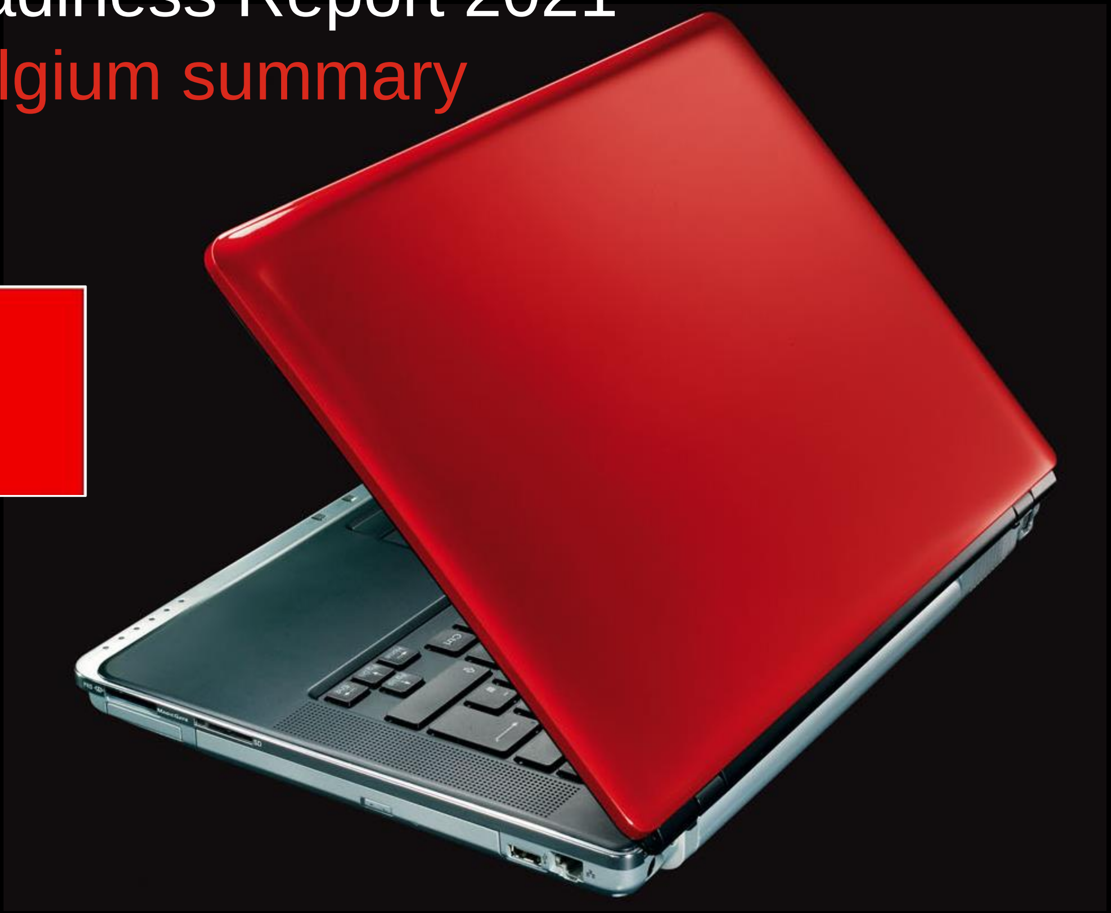
HISCOX

Cyber Readiness Report 2021
Hiscox Belgium summary



Global overview

Key findings

- **More firms targeted**
  The proportion of firms attacked rose from 38% to 43%. Many suffered multiple attacks.

- **Frightening range of outcomes**
  Cost of attacks varies widely. One in six firms attacked says its survival was threatened.

- **IT budgets reorient to cyber**
  The average firm now devotes more than a fifth (21%) of its IT budget to cyber, a jump of 63%.

- **Ransomware now commonplace**
  Around one in six of those attacked were hit with a ransom and 58% of them paid a ransom. Phishing emails were the main starting point.

- **Experts fared better**
  Firms qualifying as experts had fewer ransomware attacks, were less likely to pay up and recovered more quickly.

- **People, process, technology**
  Our cyber readiness model shows people scores are lower than for the other two areas.

- **Insurance take-up slow**
  Take-up of standalone cover creeps up from 26% to 27%; adoption highest among experts/big companies.

- **Big country variations**
  US firms top table of experts, Spanish firms are most heavily targeted, Germans pay heaviest price.

Hiscox Belgium overview

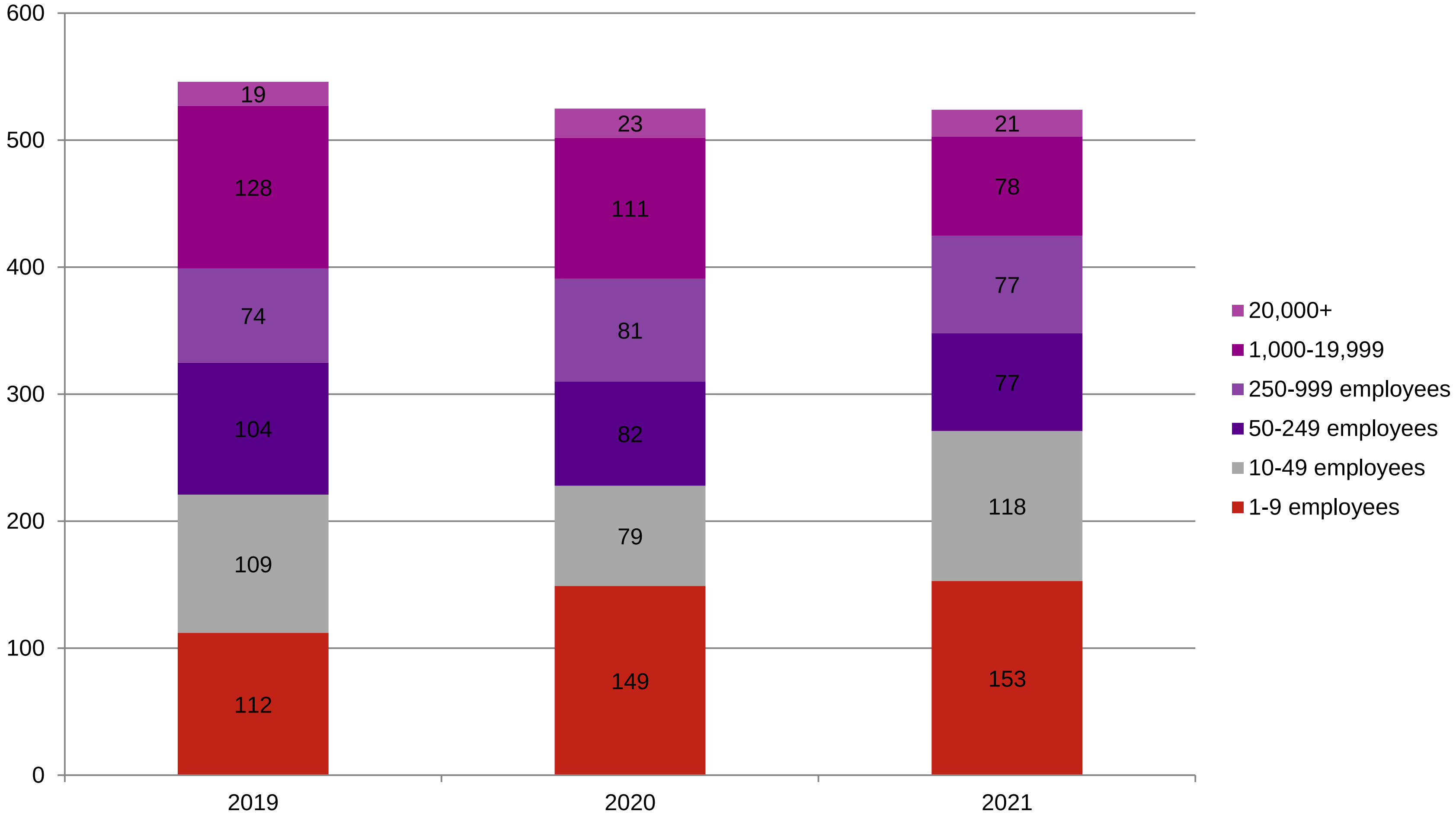
Key findings

- Belgian and German firms were most likely to have had ransomware attacks (19%), and Dutch firms were least likely (13%)
- On average, German firms spent the most on cyber security ($5.5m) while Belgian firms spent the least ($1.8m)
- US (33%) and Belgian (30%) firms are most likely to have a standalone cyber insurance policy

Reminder:
We've gone back to the prior question regarding 'cyber attacks' rather than cutting them up between incidents and breaches. Because of distribution, we're still using median, except for IT/cyber spend. We have a specific way of talking about overall breaches and costs for the Group that you should follow when referencing for your BU.

Hiscox Belgium demographics

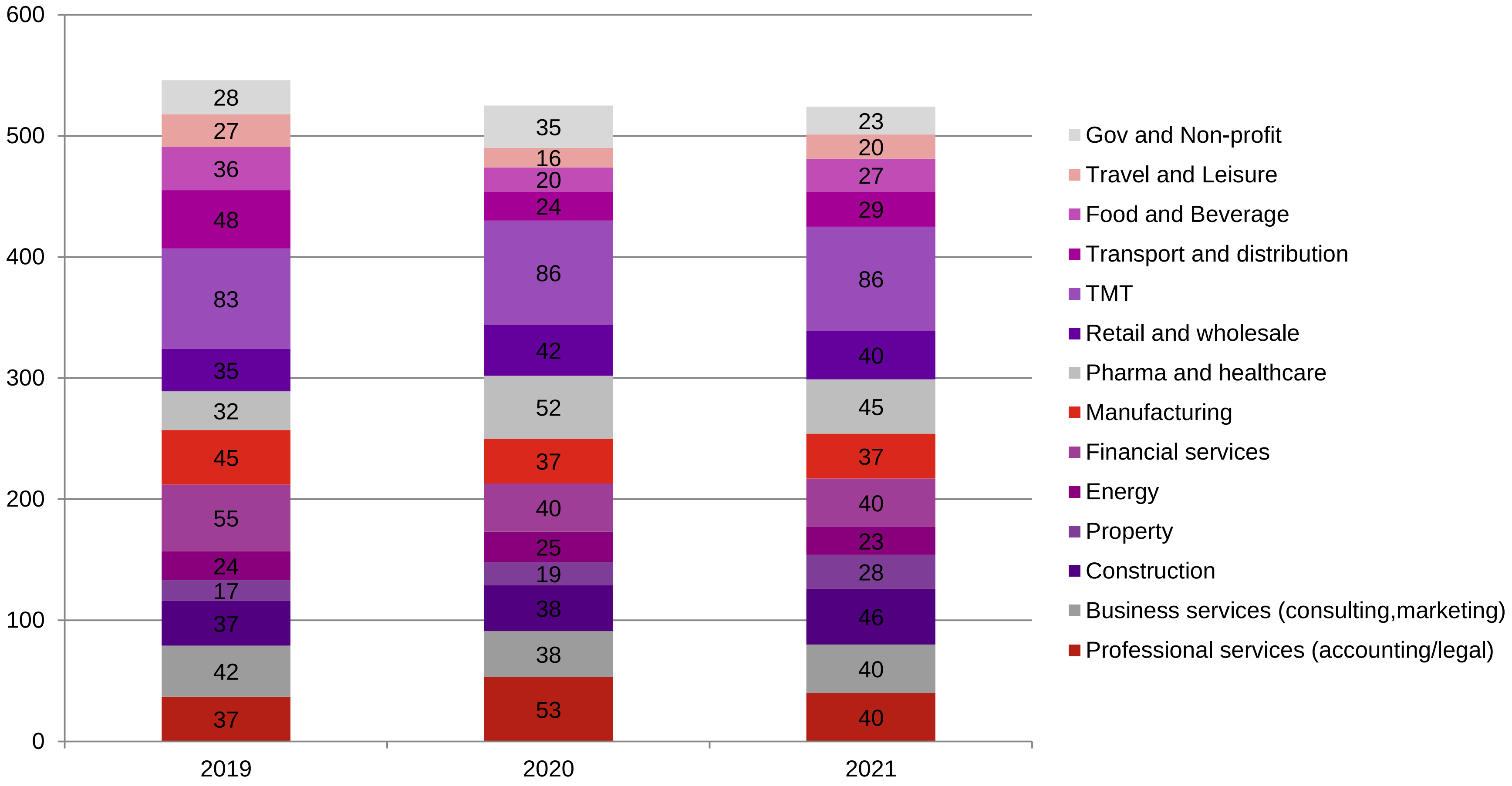
Audience breakdown stayed consistent between 2020 and 2021 report.



Belgium response base ;2019 – 546; 2020 – 525; 2021 - 524

Hiscox Belgium demographics

Industry stays relatively consistent YOY.



Belgium response base ;2019 – 546; 2020 – 525; 2021 - 524

SIZE OF THE PROBLEM

Hiscox Belgium IT Spending

Overall IT spend decreased slightly from 2020, but the % spent on cyber security increased drastically since last year.

Total IT spending:

Year	Total average	Belgium
2021	$15.4m	$10.6m
2020	$15.7m	$11.9m
2019	$14.7m	$15.3m

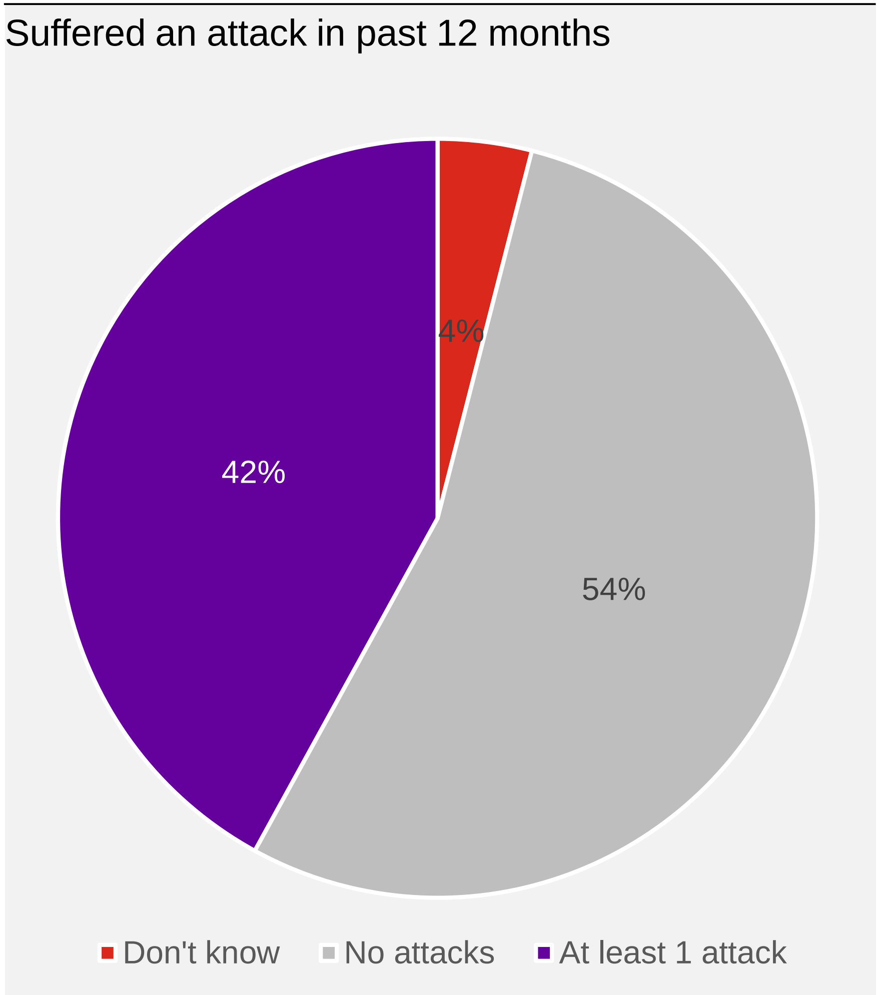
Cyber security as % of IT spend:

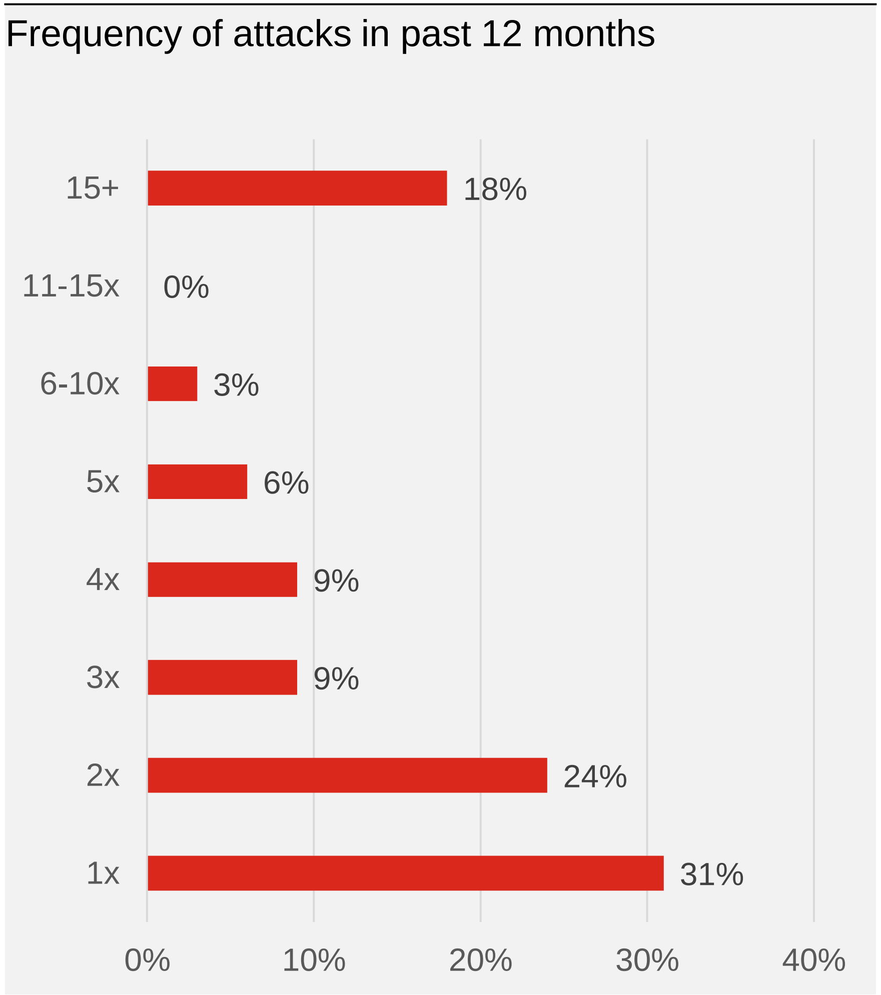
Year	Total average	Belgium
2021	21%	21%
2020	13%	13%
2019	10%	12%

Belgium response base: 2019 –329 ; 2020 – 416; 2021 - 349

Hiscox Belgium cyber attacks

Slightly fewer companies suffered attacks this year, but many suffered more than one.

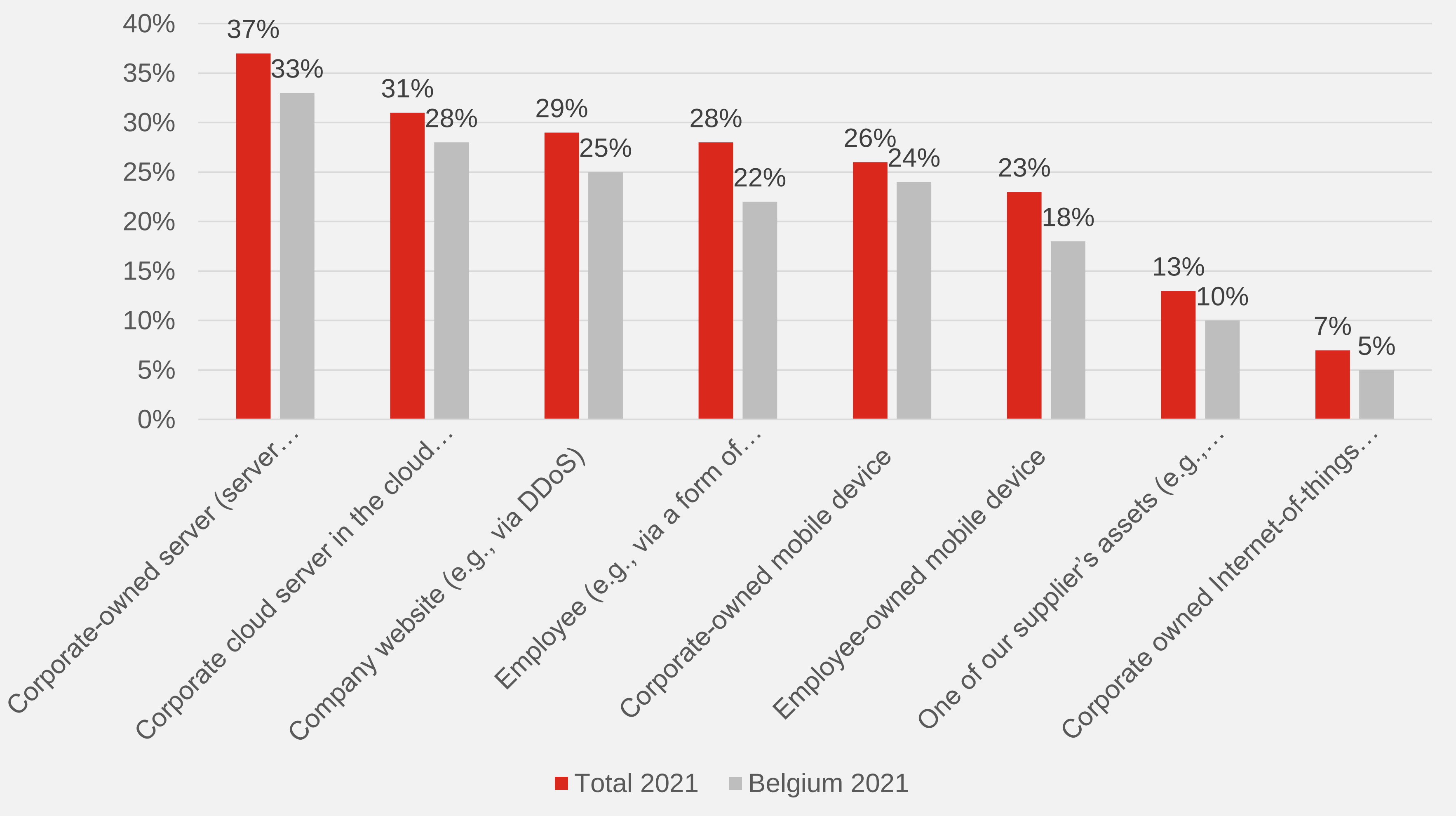




Total response base 6,042
Belgium response base: 524

Hiscox Belgium - First points of entry

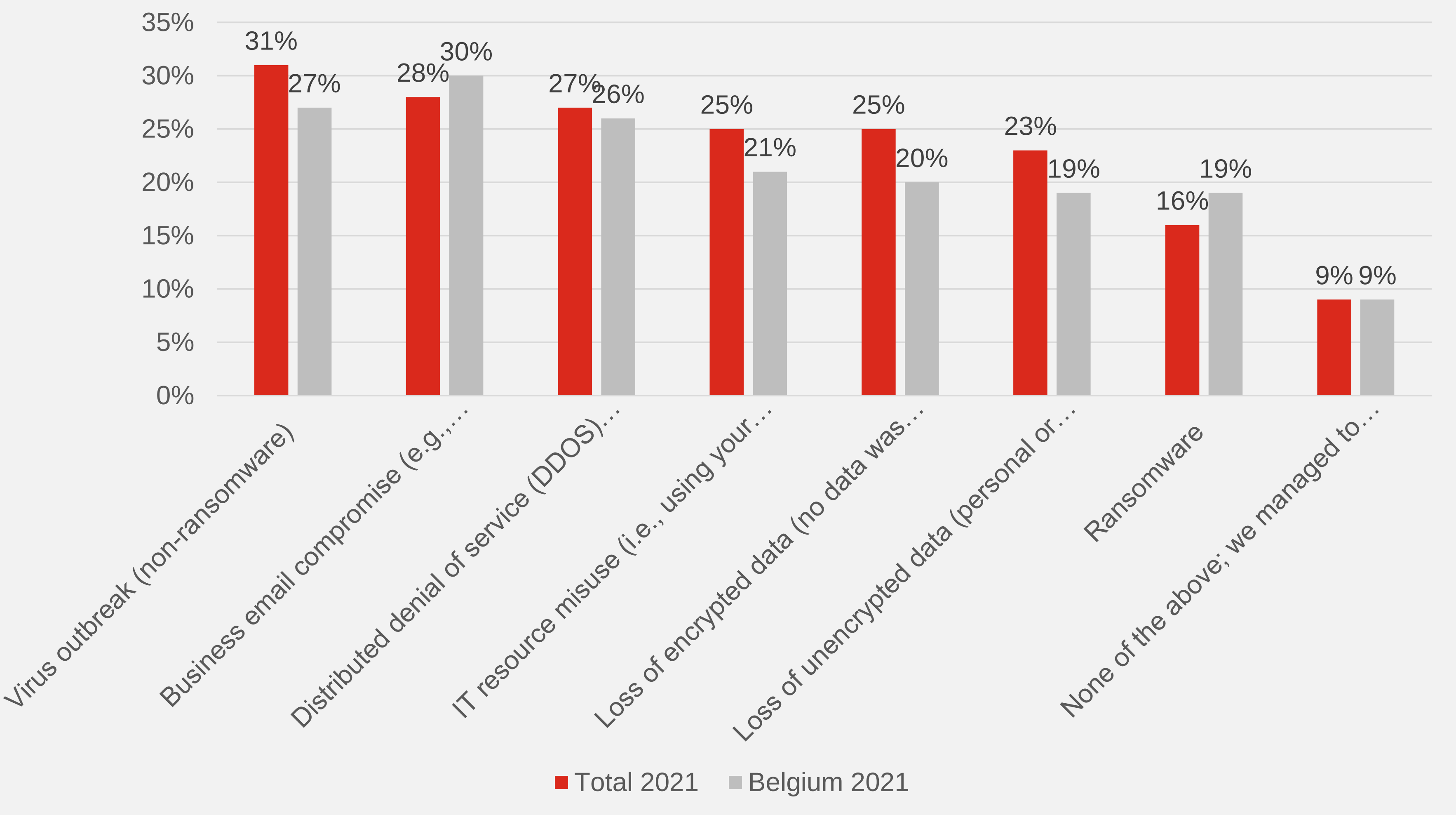
Belgium scored below total averages for how attacks occurred. Corporate-owned servers, cloud servers, and company websites were still top.



Total attacked response base 2,617
Belgium attacked response base: 218

Hiscox Belgium - Results/outcomes of cyber attacks

Belgium outpaced the overall average for business email compromise attacks and ransomware.



Total attacked response base 2,617
Belgium attacked response base: 218

Hiscox Belgium - costs

If one only looks at average or median figures the financial impact may appear containable. But behind those figures is a range of outcomes, some orders of magnitude higher.

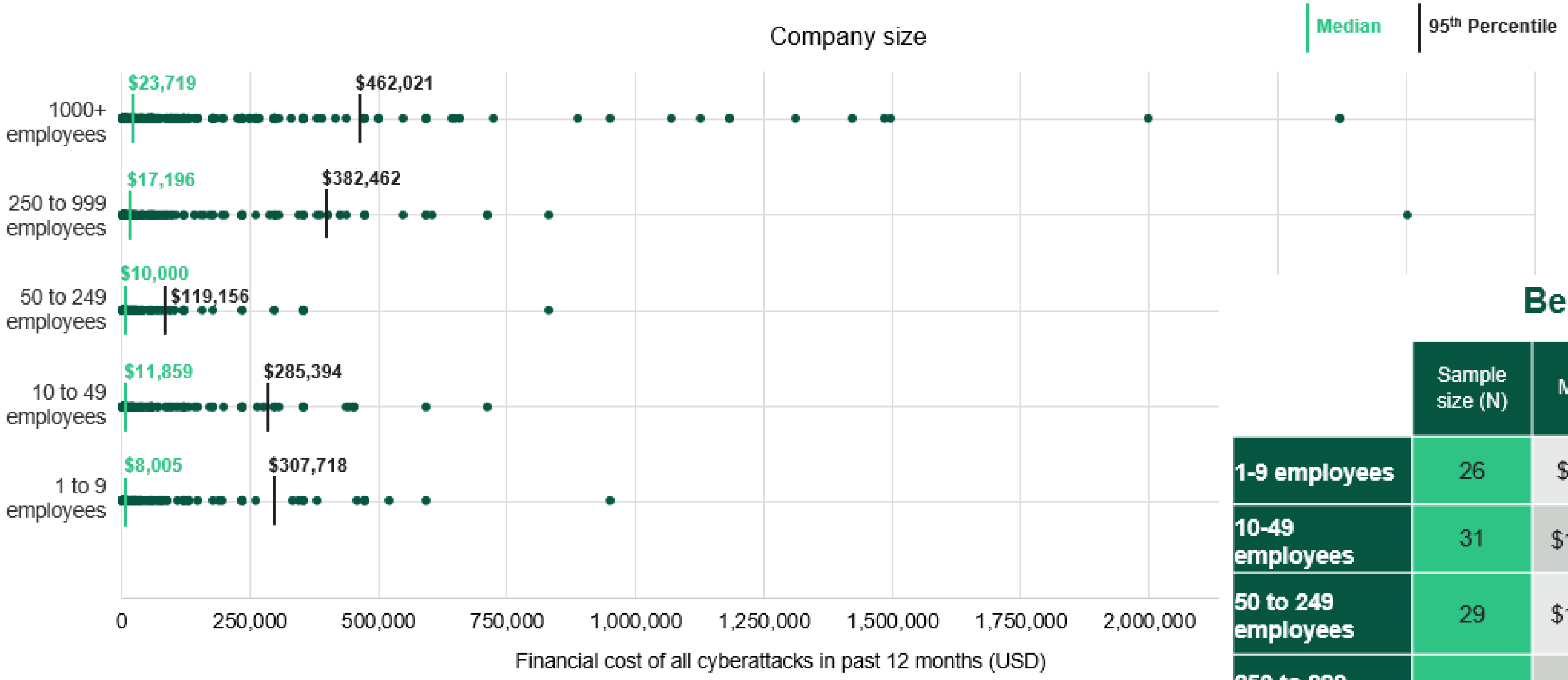
	2021	2020	2019
Belgium median cost of incident / breach	$11,859	$60,000	$5,000
Total median cost incident / breach	$13,126	$56,570	$10,000

	2021	2020	2019
Belgium cost single largest incidents / breach	$592,965	$825,000	$20,000,000
Total cost single largest incident / breach	$5,099,499	$15,800,000	$32,000,000

Total response base: 2021- 17092020 - 1,971; 2019 – 2,257
Belgium response base: 2021 – 149; 2020 – 247; 2019 - 276

Hiscox Belgium – costs by company size (excluding outliers)

Overall view compared to Belgian-specific shows the wide range of potential costs.



Base: 1709 professionals responsible for or involved in their company's cyber security strategy at companies that tracked the financial cost of cyberattacks
Source: A commissioned study conducted by Forrester Consulting on behalf of Hiscox, December 2020

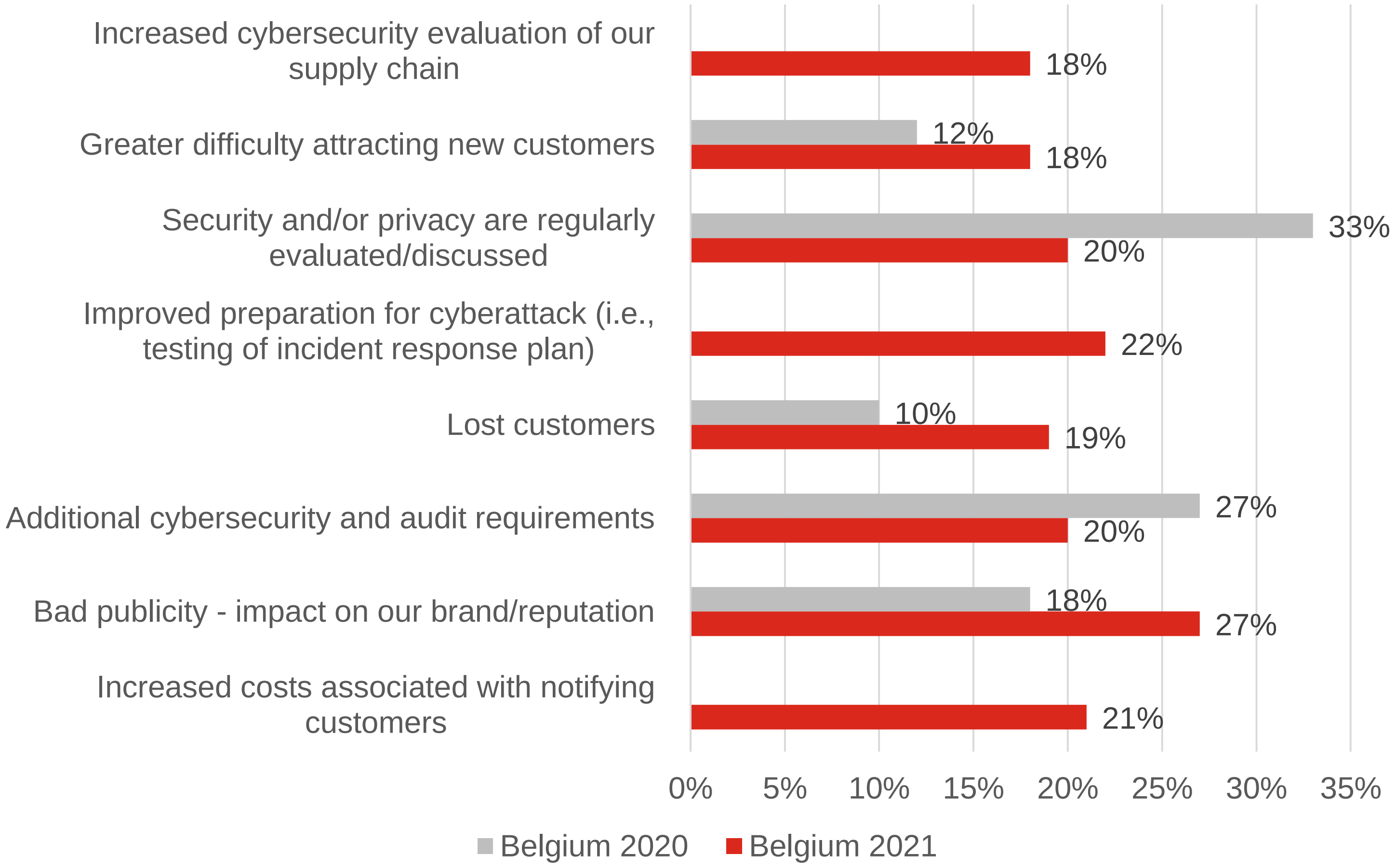
Belgium

	Sample size (N)	Median	95th Percentile
1-9 employees	26	$5,930	$106,734
10-49 employees	31	$11,859	$309,528
50 to 249 employees	29	$11,859	$49,572
250 to 999 employees	23	$8,302	$115,035
1000+ employees	36	$23,719	$391,357
Total	145	$11,859	$266,123

Careful when sample size below 50. Should only be used for internal reference. Use total otherwise.

Hiscox Belgium - impact and/or response to cyber attacks

Though some new options were added, top scores in 2021 included bad publicity from attacks and increased costs associated with notifying customers.



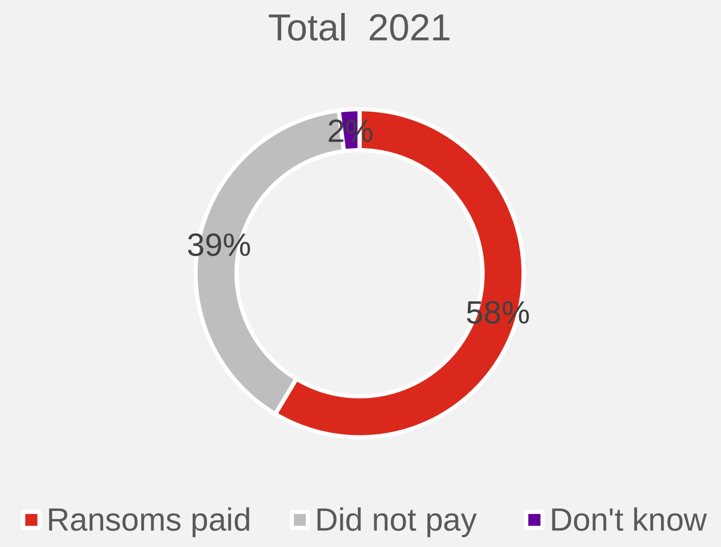
Belgium response base 2021: 218; 2020: 259

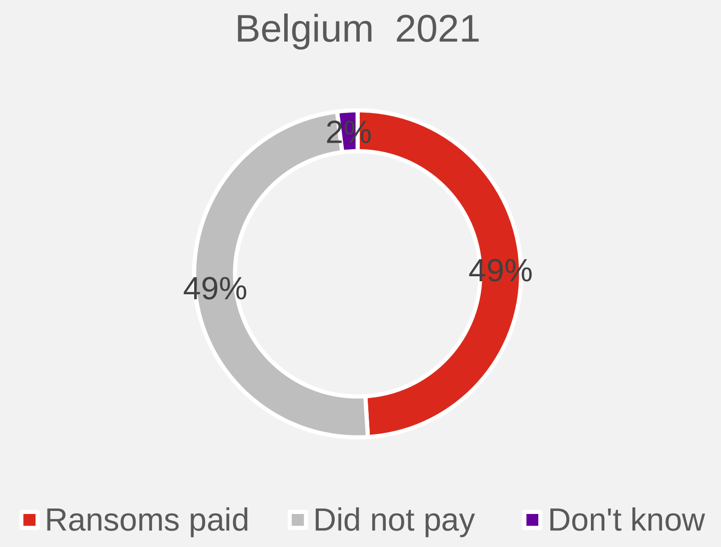
Hiscox Belgium ransomware impact

Belgium had slightly more ransomware attacks than the total but paid slightly less often.

Ransoms paid	Total 2021	Belgium 2021
Experienced ransomware attack	16%	19%
Total respondents	2617	220

Single largest ransom paid in Belgium 2021: $17,789

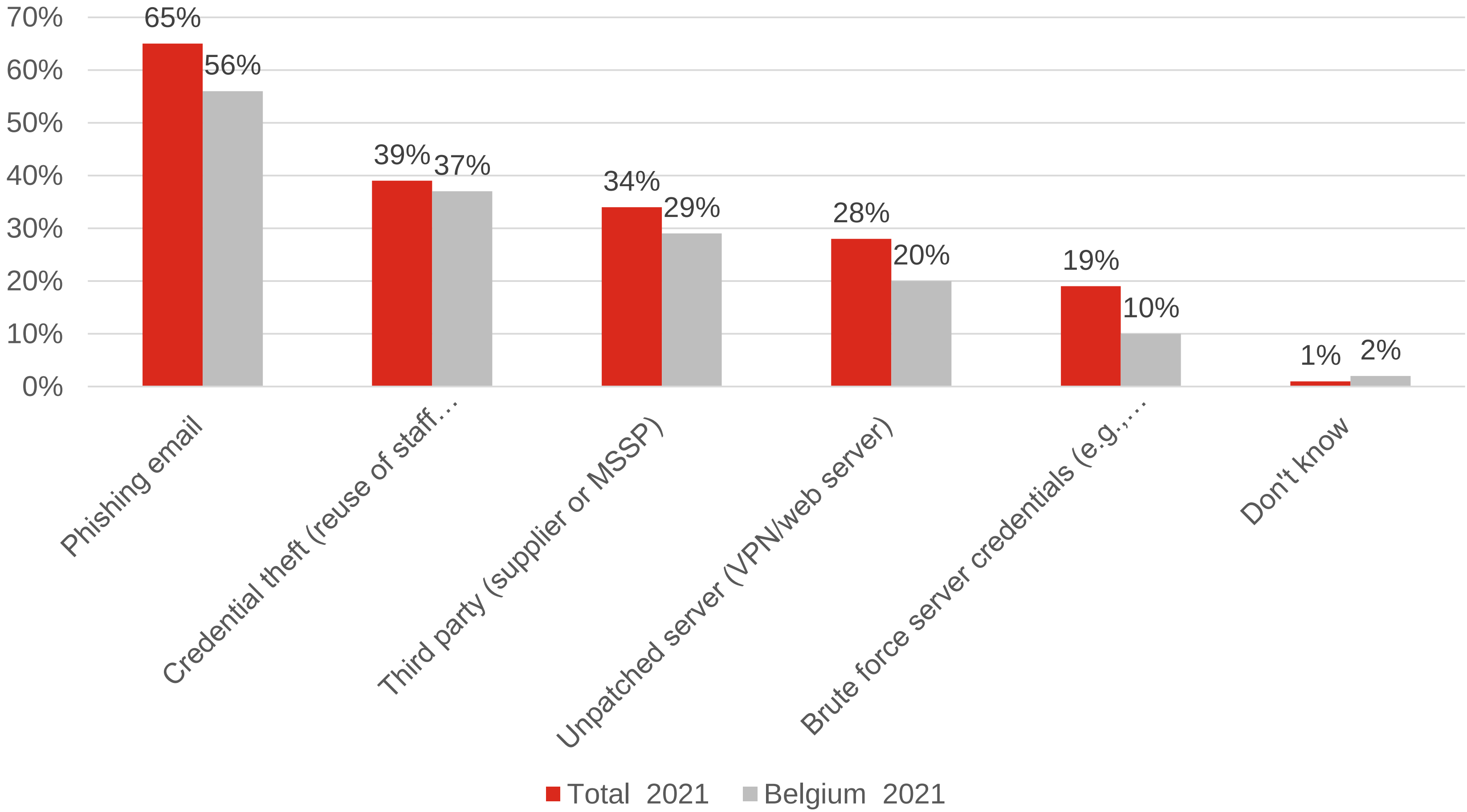




Response base: Total 2021 – 413; Total Belgium: 41

Hiscox Belgium – Ransomware method of entry

Phishing was the main point of entry in the Belgium for ransomware, followed by credential theft, both of which can be managed with better employee training.



Response base: Total 2021 – 413; Total Belgium 2021 - 41

READINESS MODEL

Hiscox Maturity Model background

Our readiness model is based on a capability-oriented architecture, encompassing the people, processes and technology needed to create an effective cyber security management system.

OVERALL (N=6,042)	People	Process	Technology	Total
Business Resilience Management	3.12	3.13	3.10	**3.12**
Cryptography and Key Management	2.93	2.90	2.94	**2.93**
Identity and Access Management	3.05	2.95	2.94	**2.97**
Security Information and Event Management	2.93	3.10	2.99	**2.99**
Threat and Vulnerability Management	3.00	3.12	3.28	**3.13**
Trust Management	3.07	3.05	3.09	**3.07**
Total	**3.02**	**3.04**	**3.06**	**3.03**

- It assesses a firm's maturity in six different areas of capability (domains) using the COBIT measurement framework. The six domains make up all the elements required to install, run, manage and govern an effective security system.

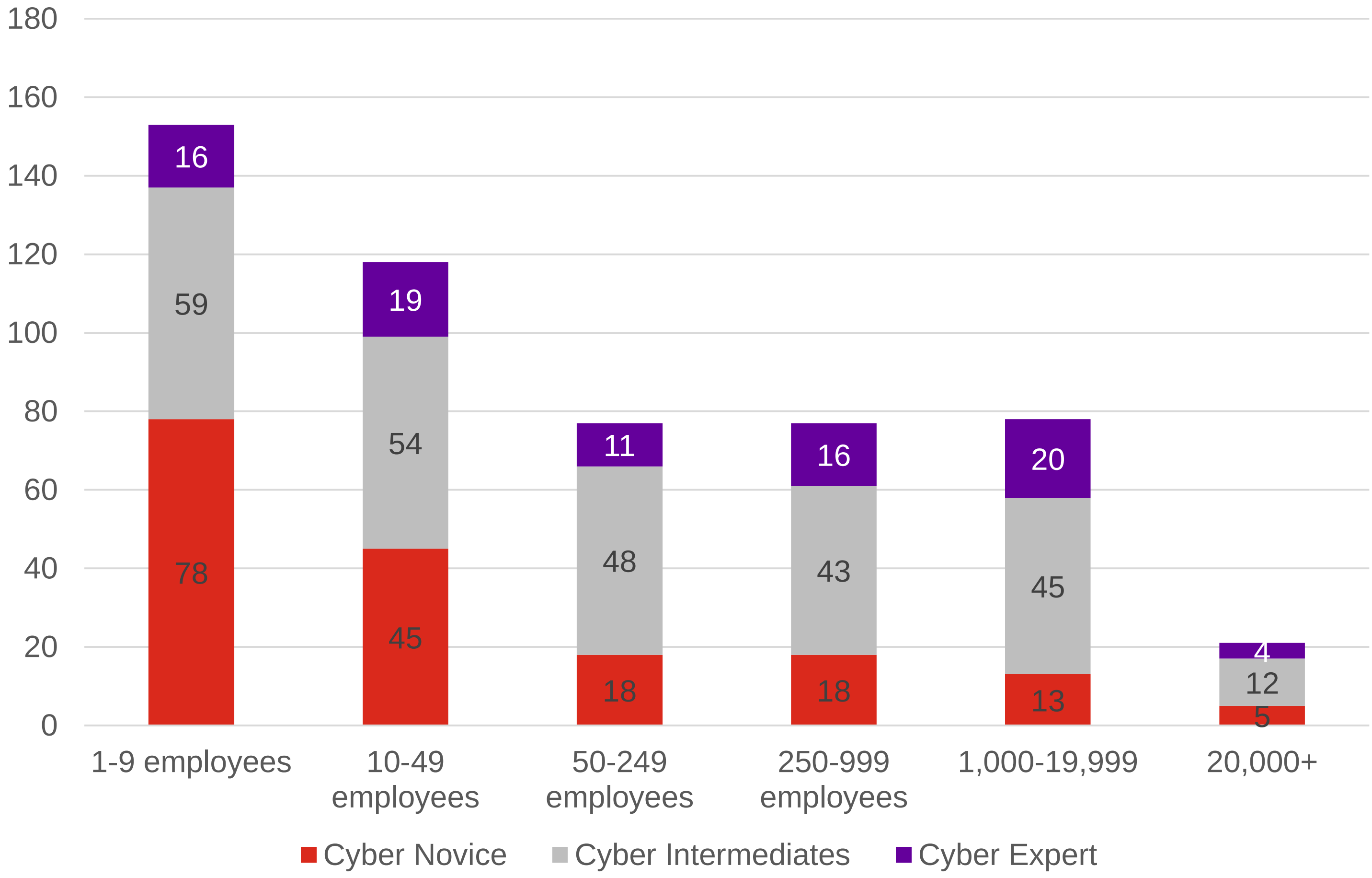
- Each domain is measured against three different attributes – people process and technology

- The scoring system marks each attribute according to how well developed it is – from non-existent or ad hoc at one end of the scale to optimised at the other.

- Firms can not only measure the effectiveness of their security controls but better understand the gaps the model reveals.

Hiscox Belgium - readiness model

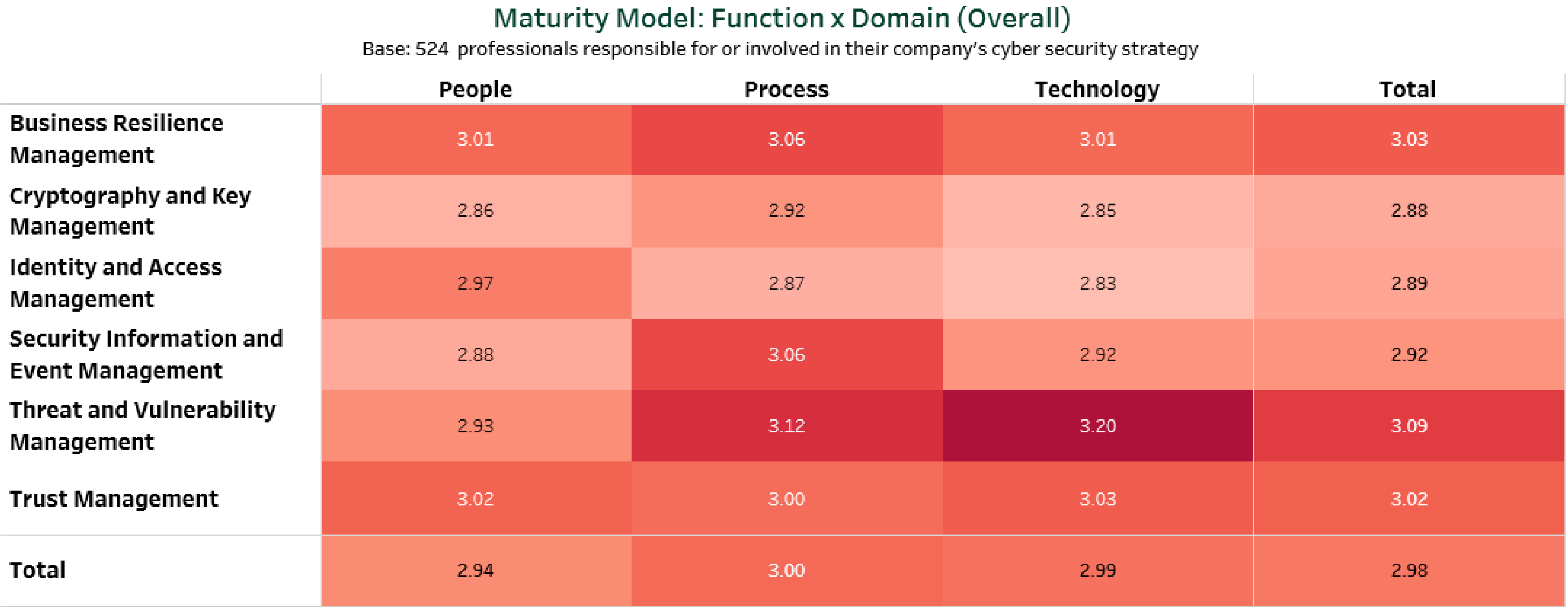
New model doesn't allow us to compare exactly to last year, though cyber experts have decreased slightly in Belgium and many novices are now intermediates.



Response base: Belgium 2021- 524

Hiscox Belgium - readiness model

Top performing area is Threat Mgmt Tech. Biggest areas of improvement are also in Tech for Cryptography and Identity access domains.



Maturity Model: Function x Domain (Overall)

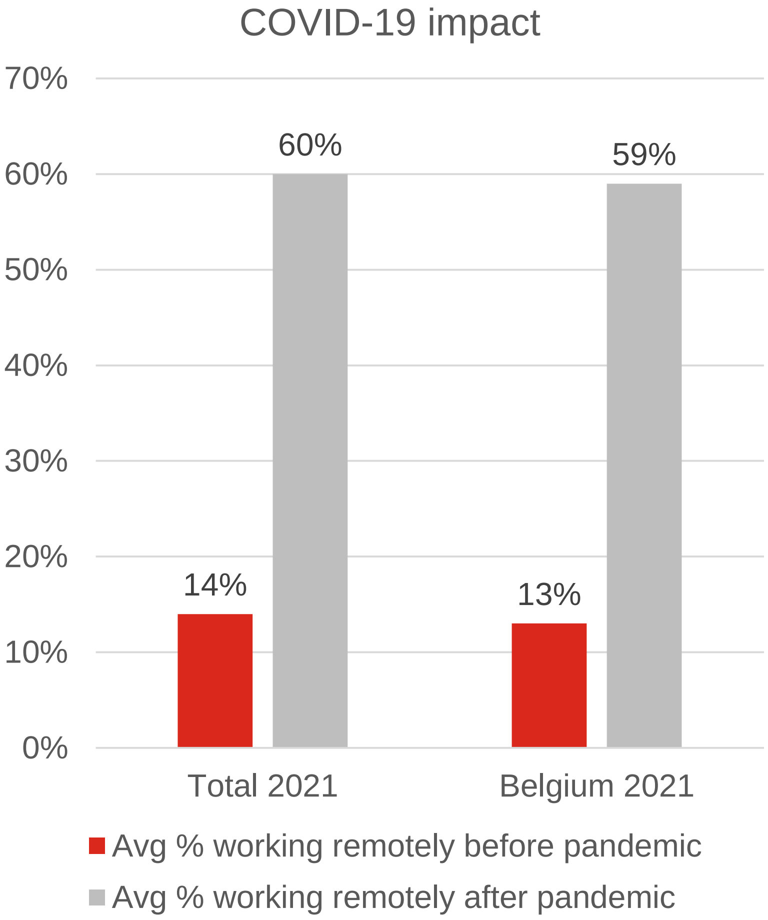
Base: 524 professionals responsible for or involved in their company's cyber security strategy

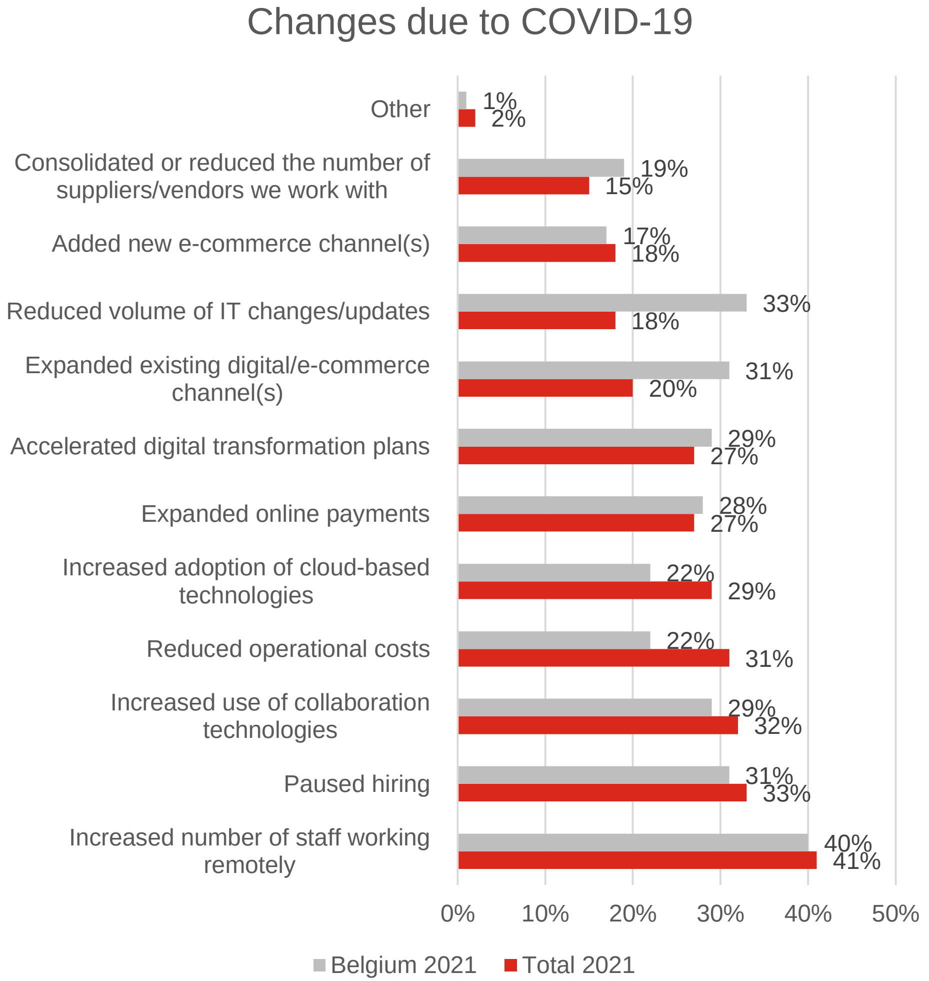
	People	Process	Technology	Total
Business Resilience Management	3.01	3.06	3.01	3.03
Cryptography and Key Management	2.86	2.92	2.85	2.88
Identity and Access Management	2.97	2.87	2.83	2.89
Security Information and Event Management	2.88	3.06	2.92	2.92
Threat and Vulnerability Management	2.93	3.12	3.20	3.09
Trust Management	3.02	3.00	3.03	3.02
Total	2.94	3.00	2.99	2.98

BUILDING RESILIENCE

Hiscox Belgium COVID-19 impact

COVID caused a definite increase in remote working, causing a reduction in the volume of IT changes and expanded digital commerce channels.

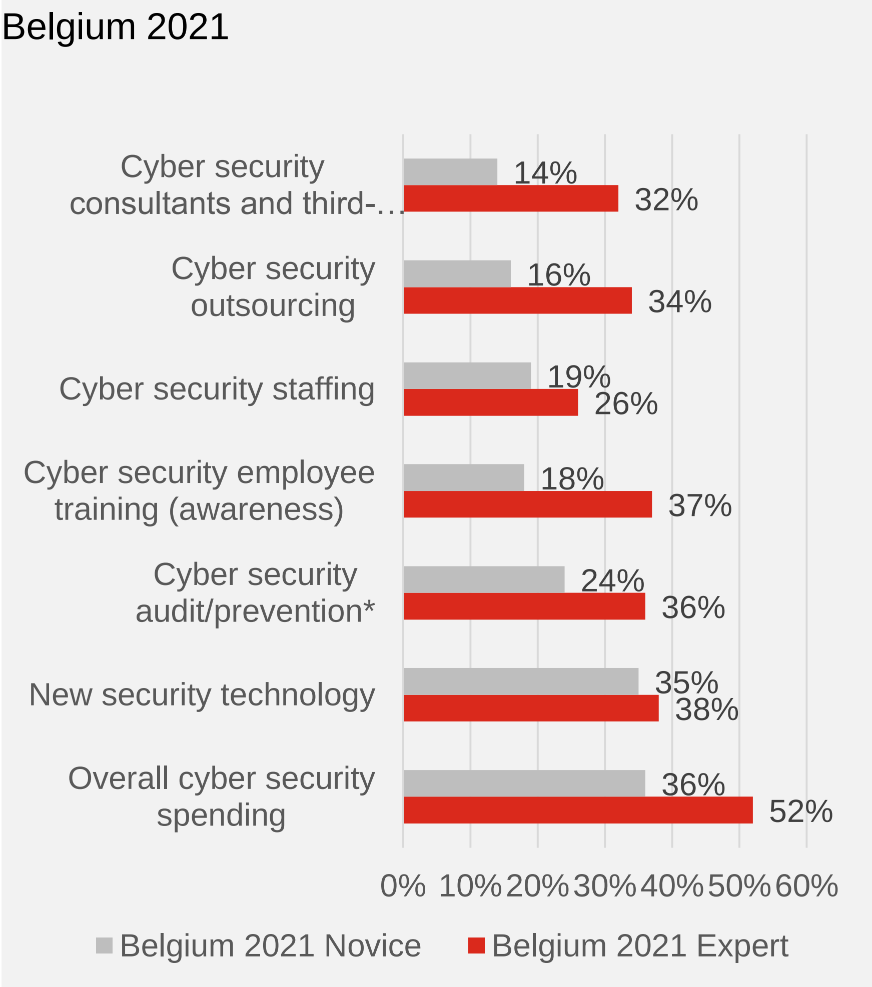


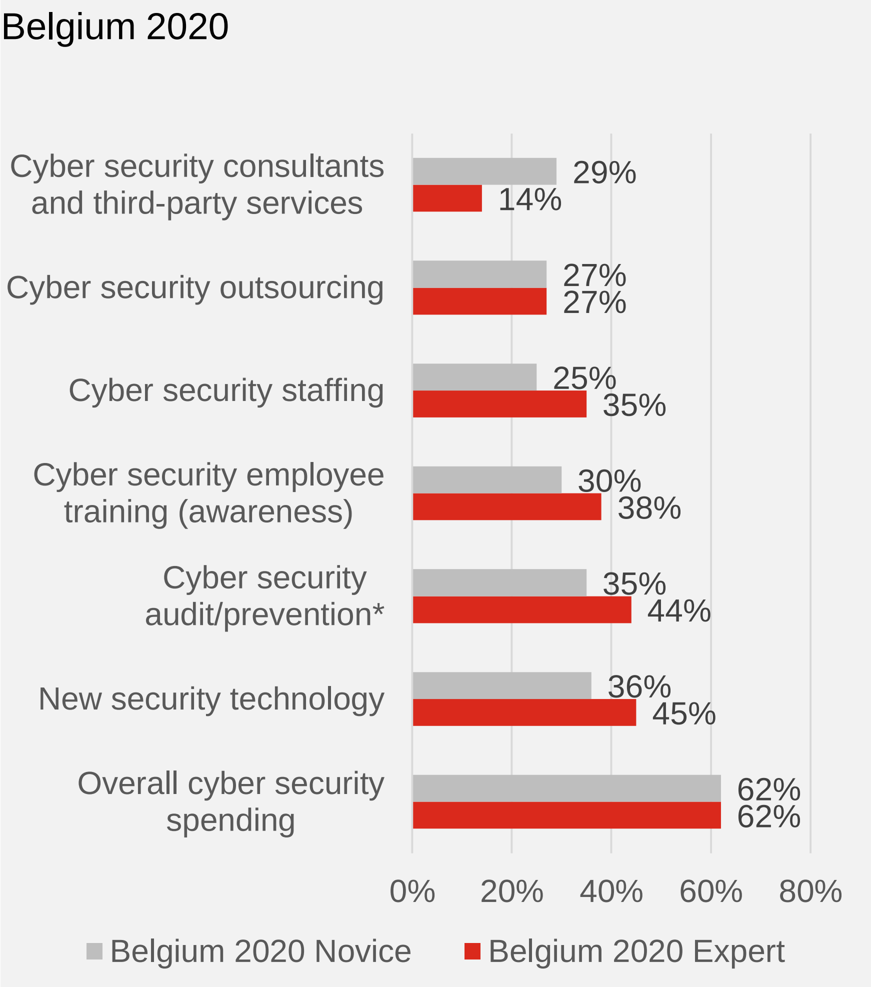


Response base: Total 2021 – 6042; Belgium 2021 - 524

Hiscox Belgium - cyber spending

Experts planning to increase new tech, employee training and audit/prevention measures. A larger difference now between novices and experts.

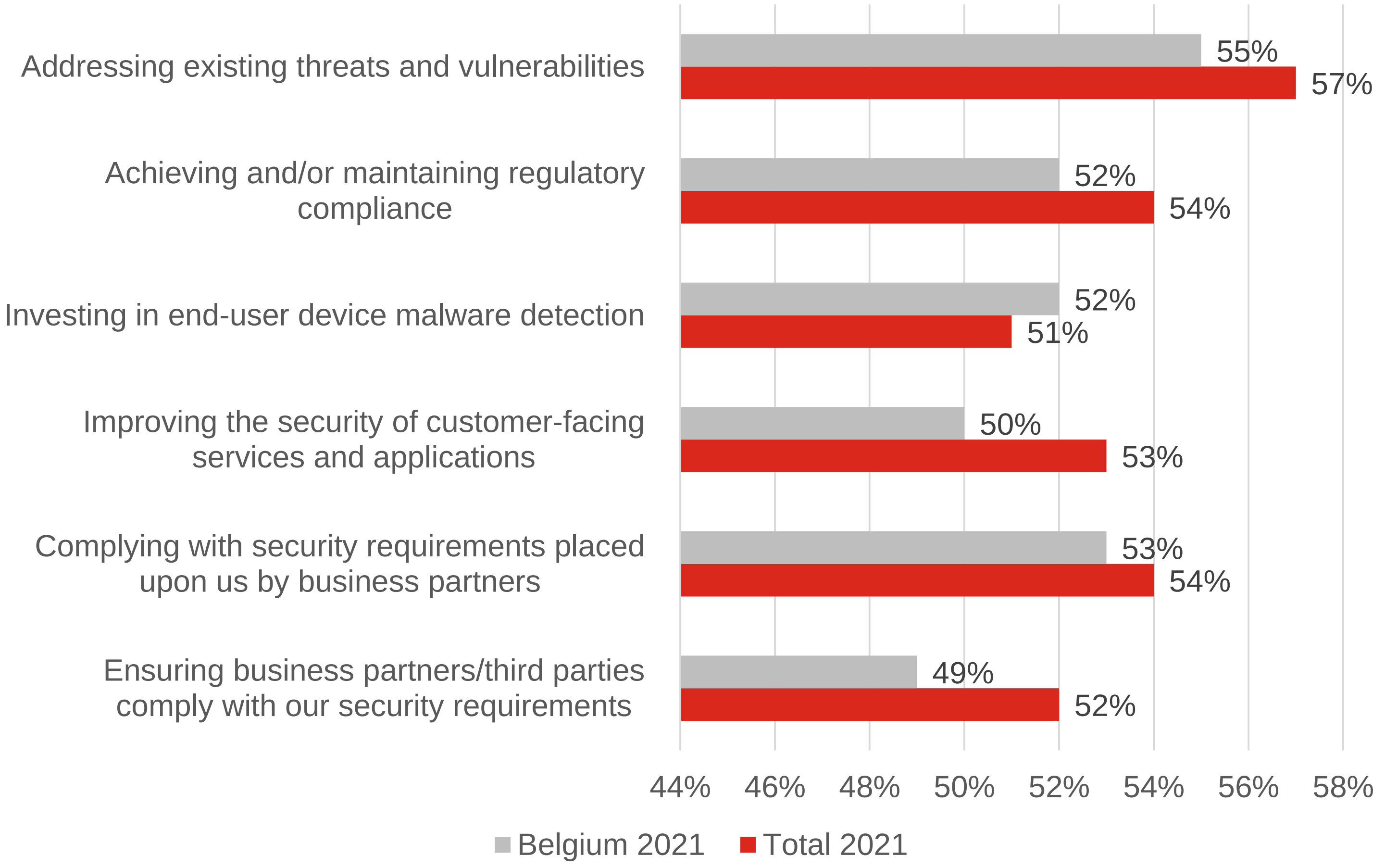




Belgium 2021 response base: 180
Belgium 2020 response base: 416

Hiscox Belgium – top cyber spending priorities

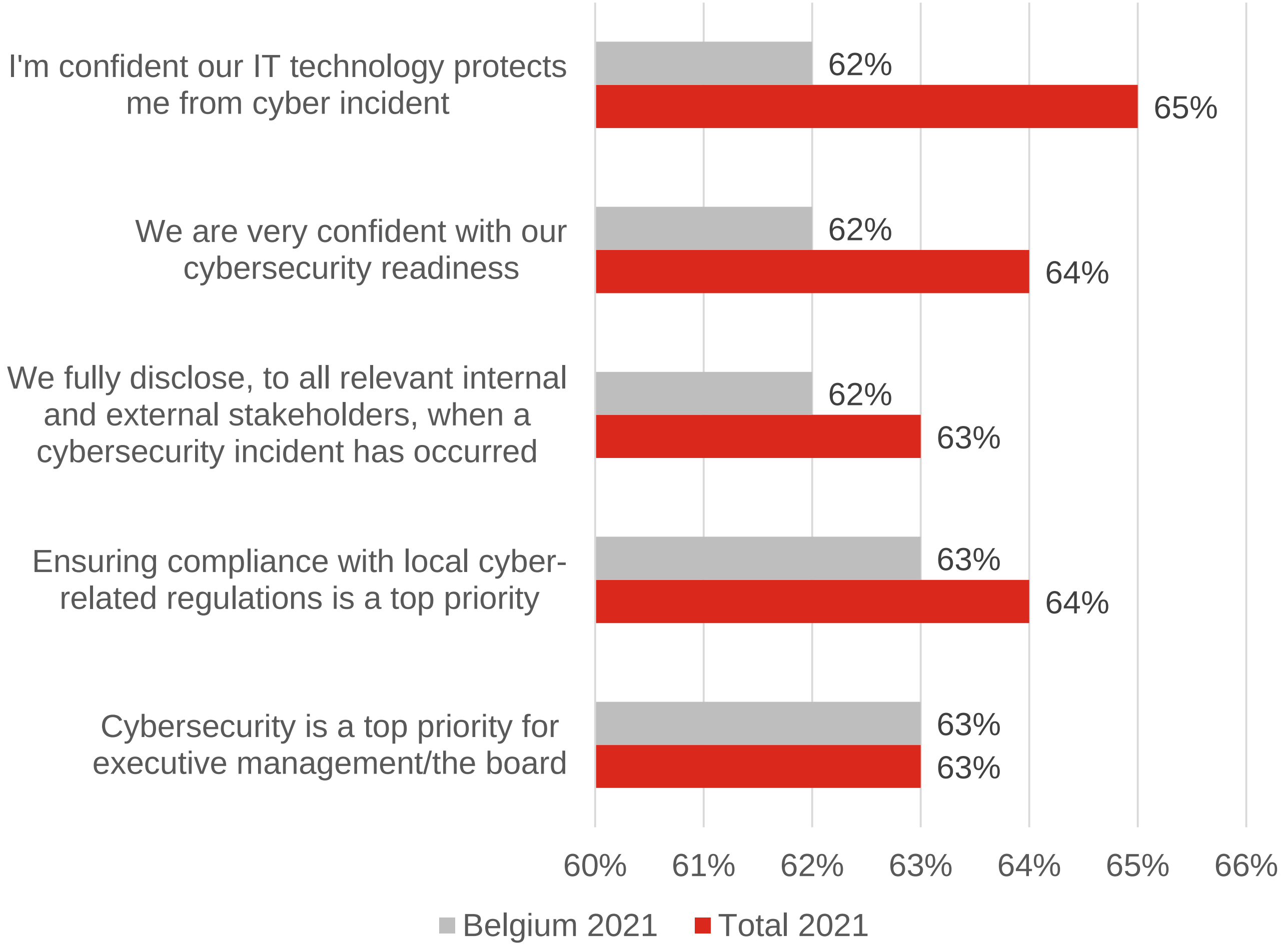
Addressing existing threats became a major area of importance, as well as complying with security requirements put on by business partners and improving security for customer-facing services.



Base response: Belgium 2021 – 524; Total 2021 - 6043

Hiscox Belgium– cyber security confidence

Top areas of confidence in 2021 or lack there included cyber security being a top priority for management and ensuring compliance with regulations.



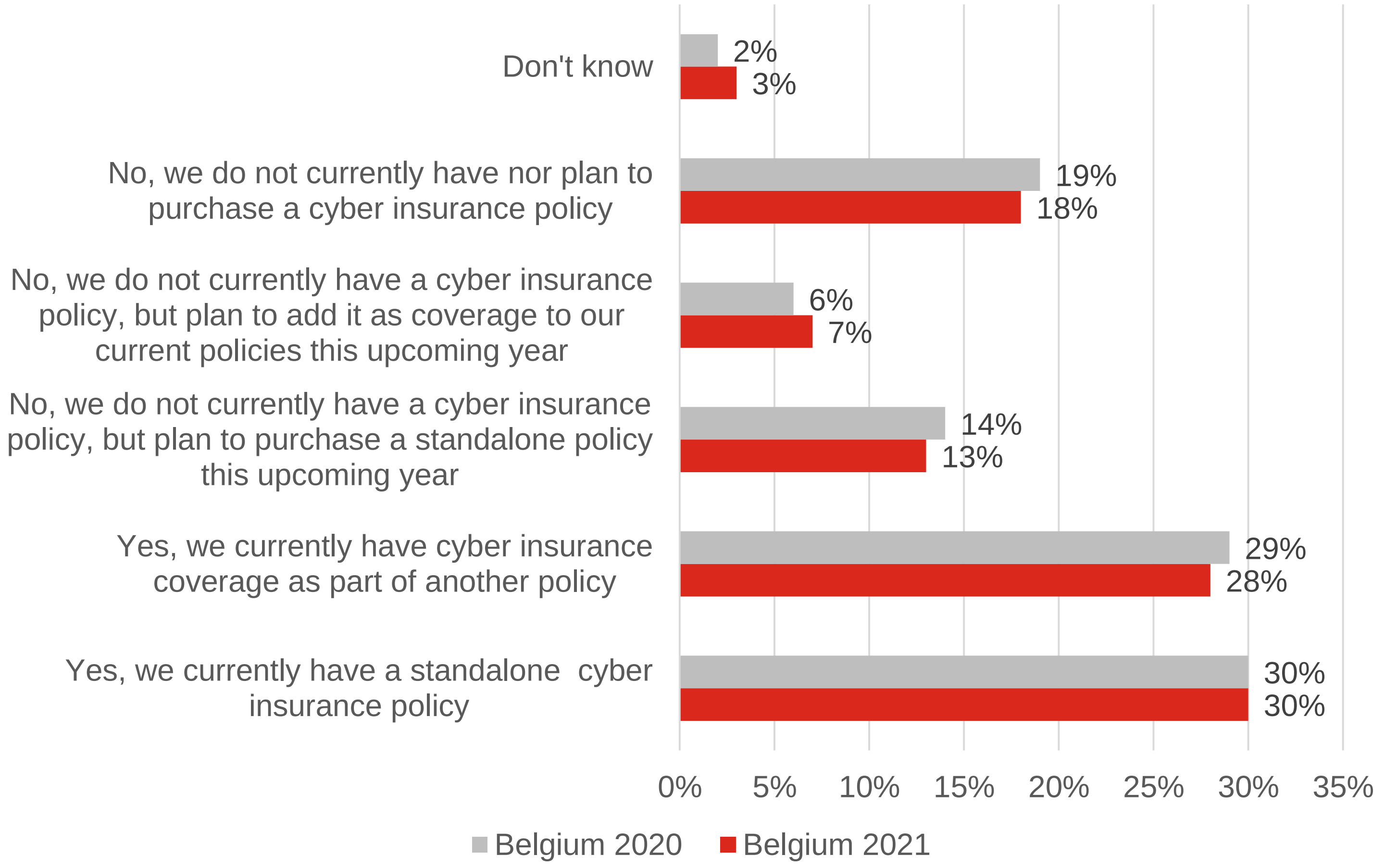
New questions asked in 2021 highlighted perception around COVID and cyber security for Belgium:

- My organisation has been more vulnerable to cyberattacks since the start of the coronavirus pandemic – 44%
- Because more employees are working from home, my organisation is more vulnerable to cyberattacks – 54%
- My organisation has increased my cyber defenses because of the coronavirus pandemic – 52%

Base response: Belgium 2021 – 524; Total 2021 - 6043

Hiscox Belgium - insurance purchase activity

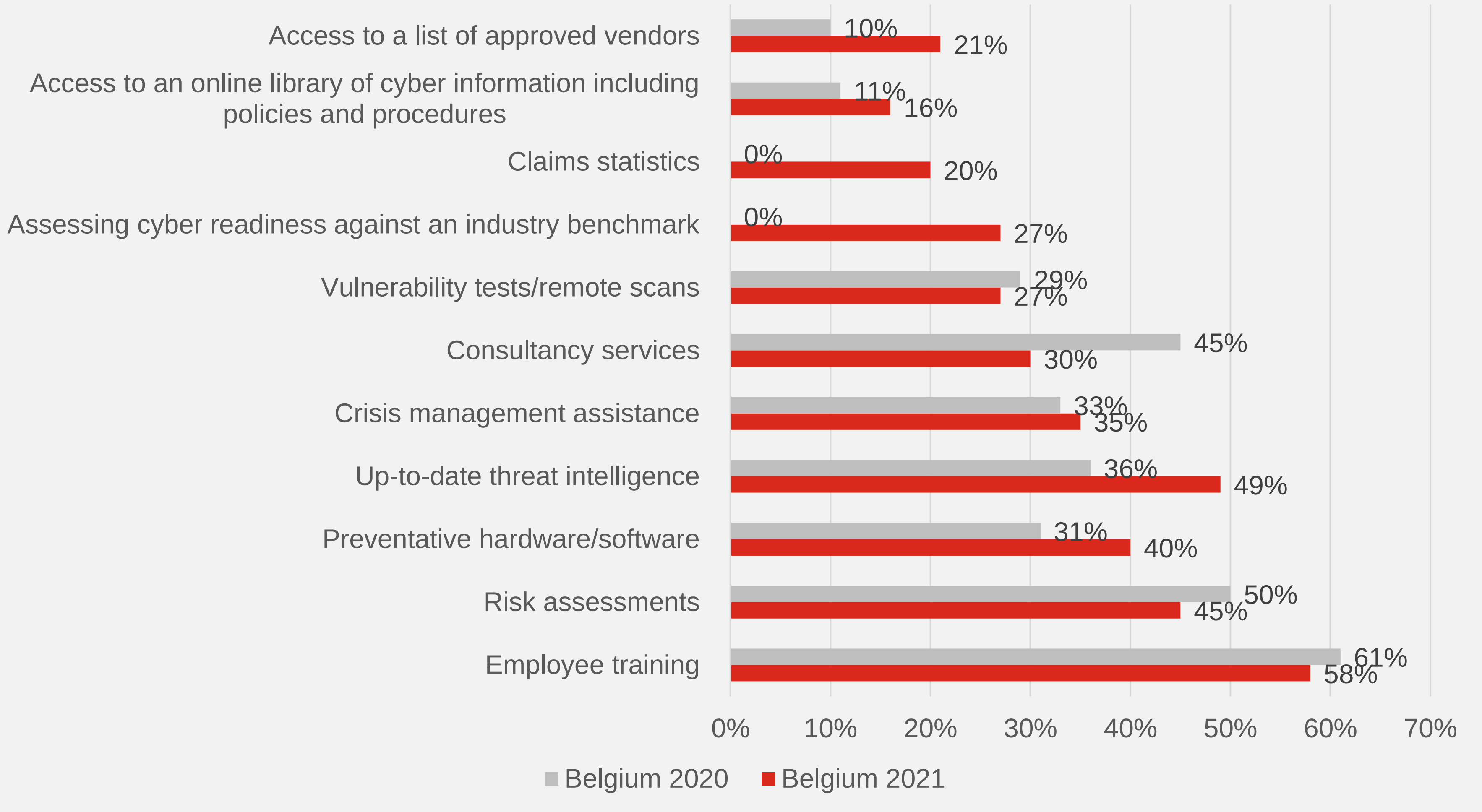
Standalone policies hold steady and plans to never purchase also decreased. More still likely to have a policy that's standalone compared to an addition to an existing policy.



Response base: Belgium 2020 response base: 394; Belgium 2021 - 353

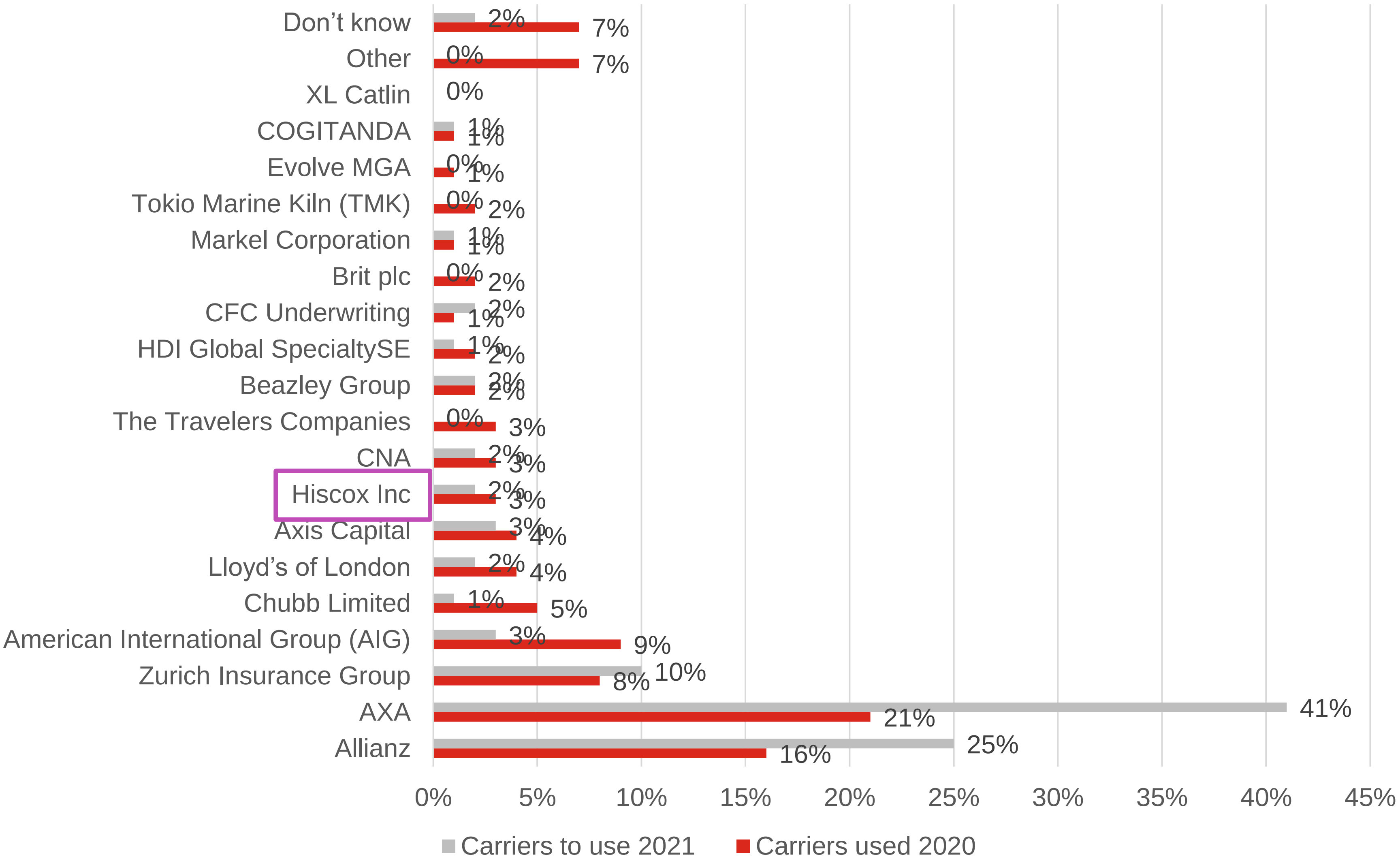
Hiscox Belgium - additional services

Customers in the Belgium are interested in the below additional services that might be offered through their insurance carrier.



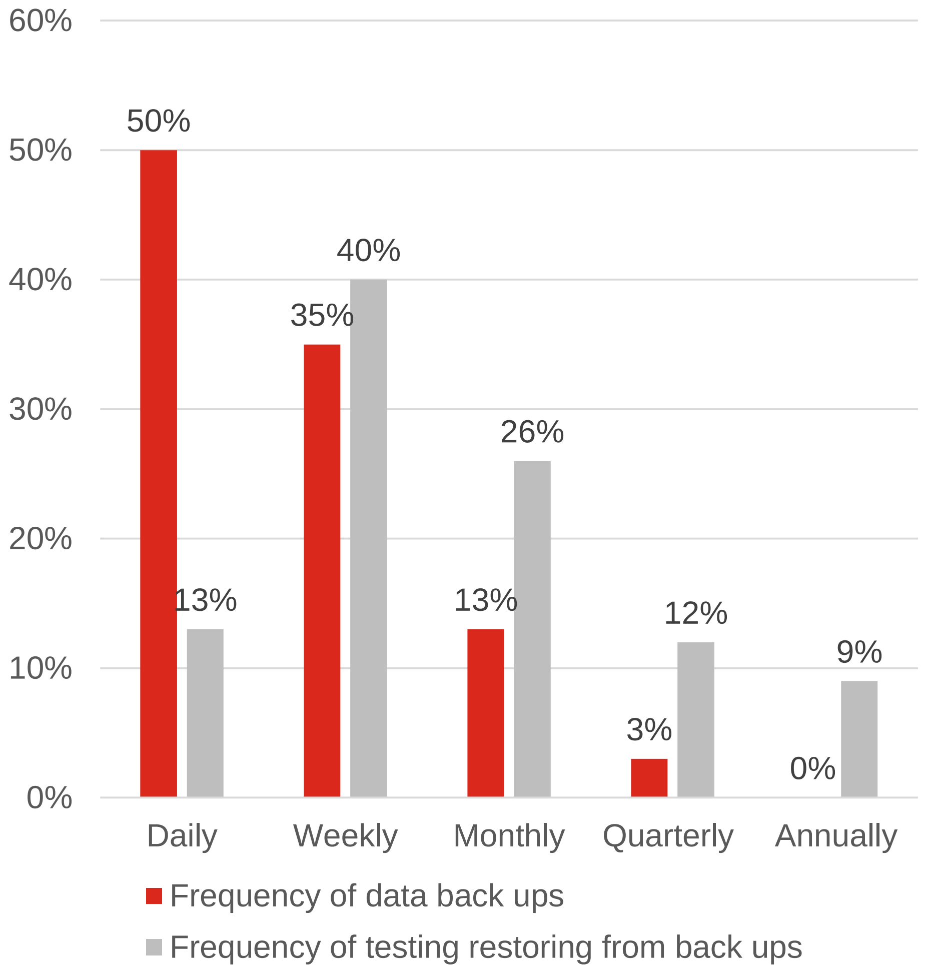
Response base: Belgium 2020 - 174; Belgium 2021 - 154

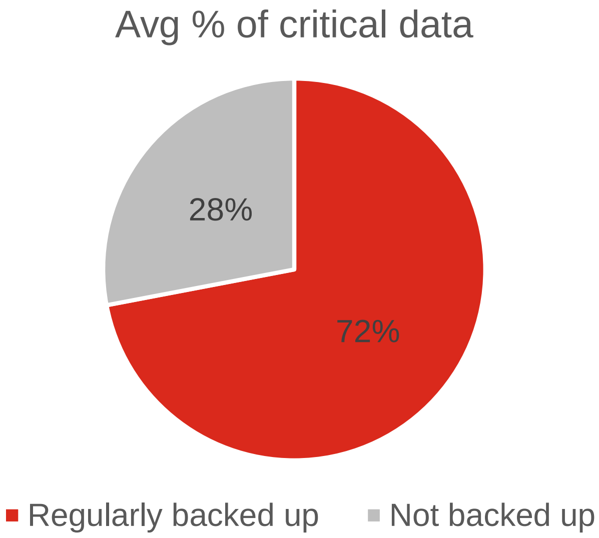
Hiscox Belgium– carriers for cyber insurance

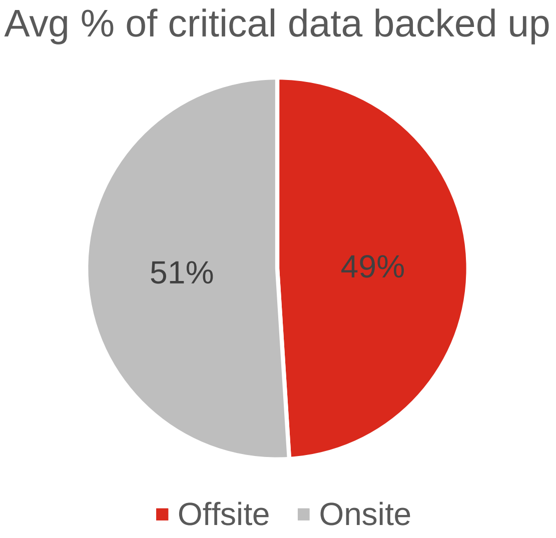


Response base: Belgium 2020 response base- 312; Belgium 2021 - 207

Hiscox Belgium - back-ups



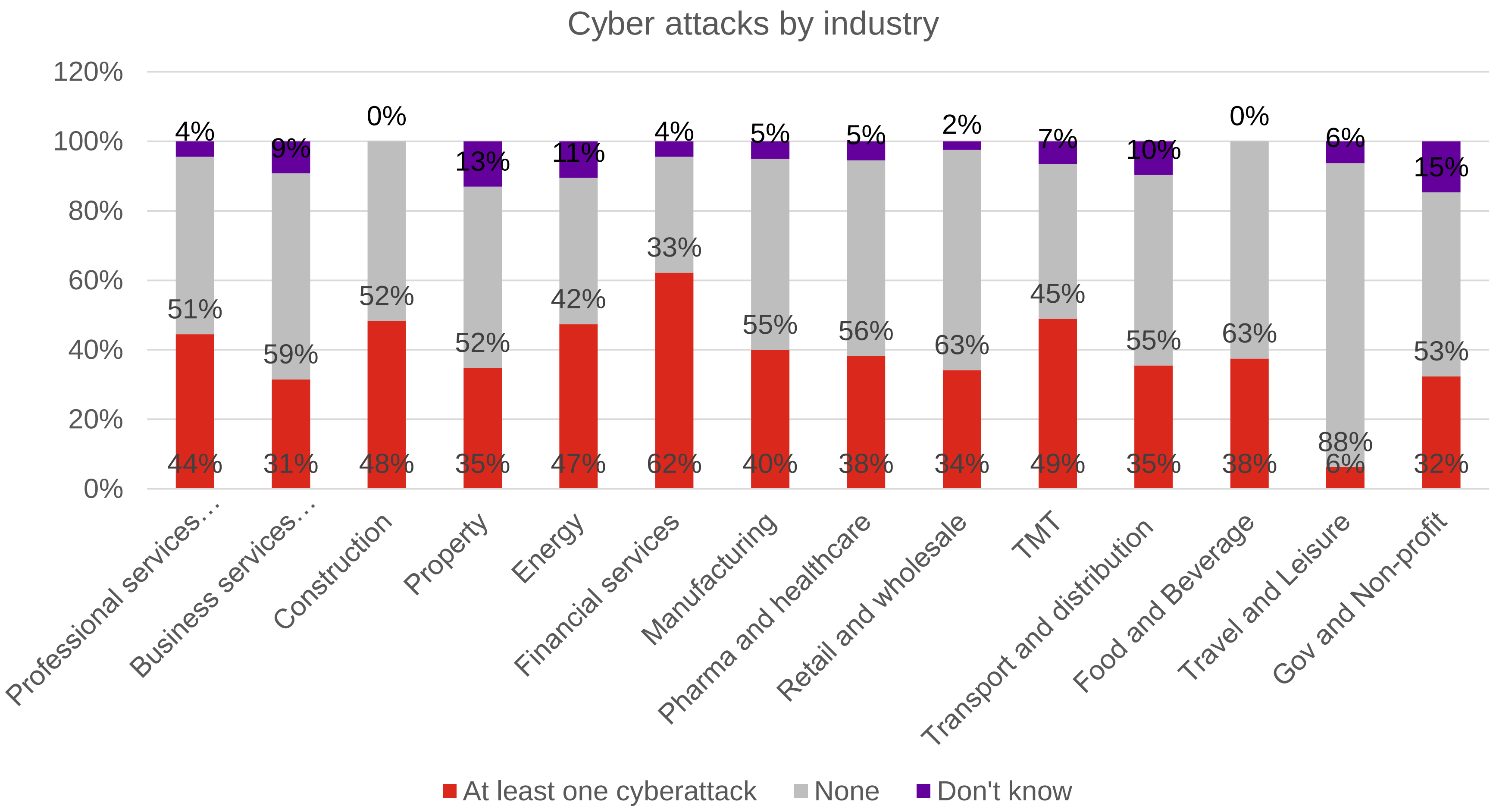




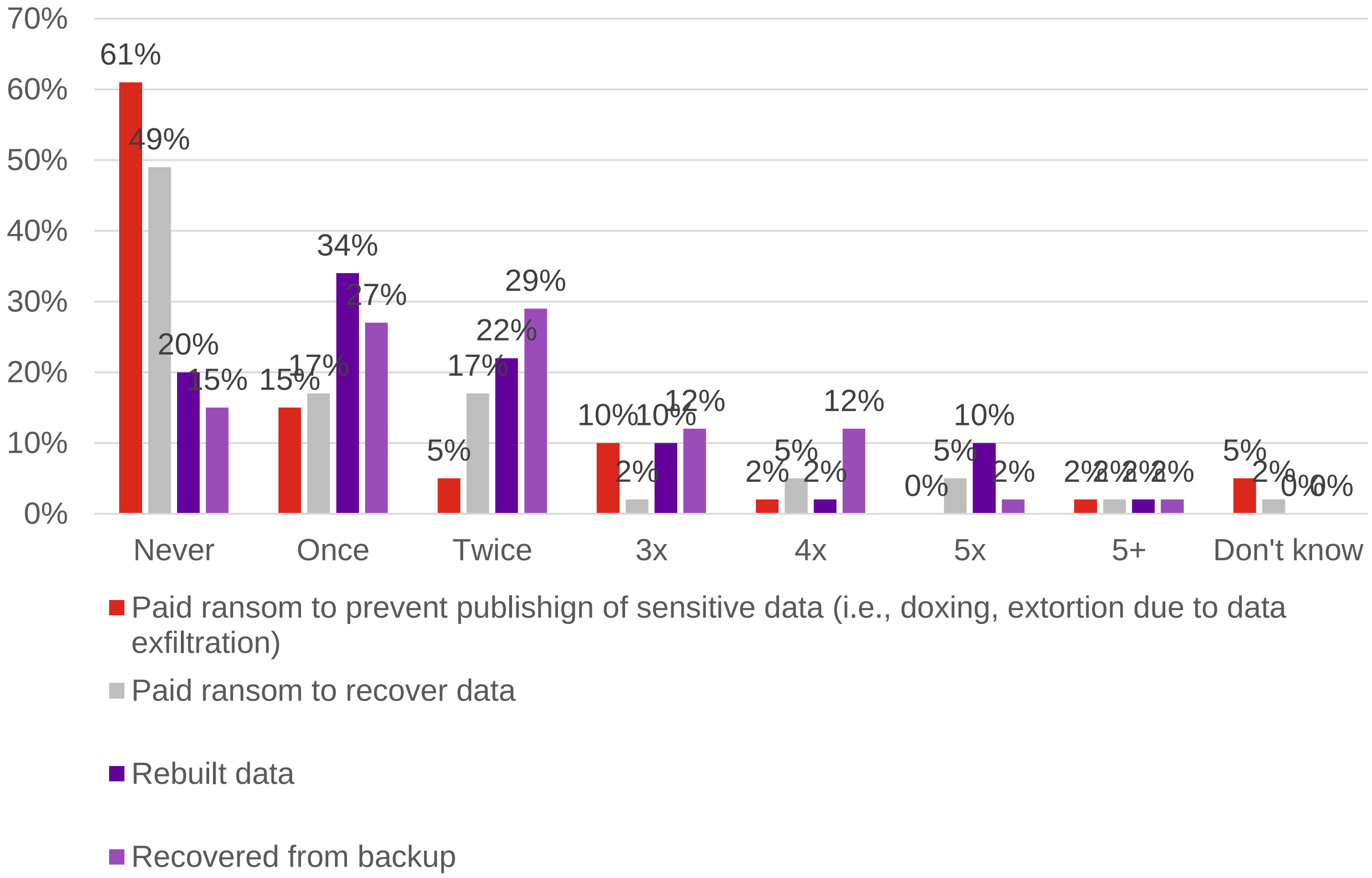
Response base: backups – 524; onsite/offsite – 514; frequency - 391

APPENDIX

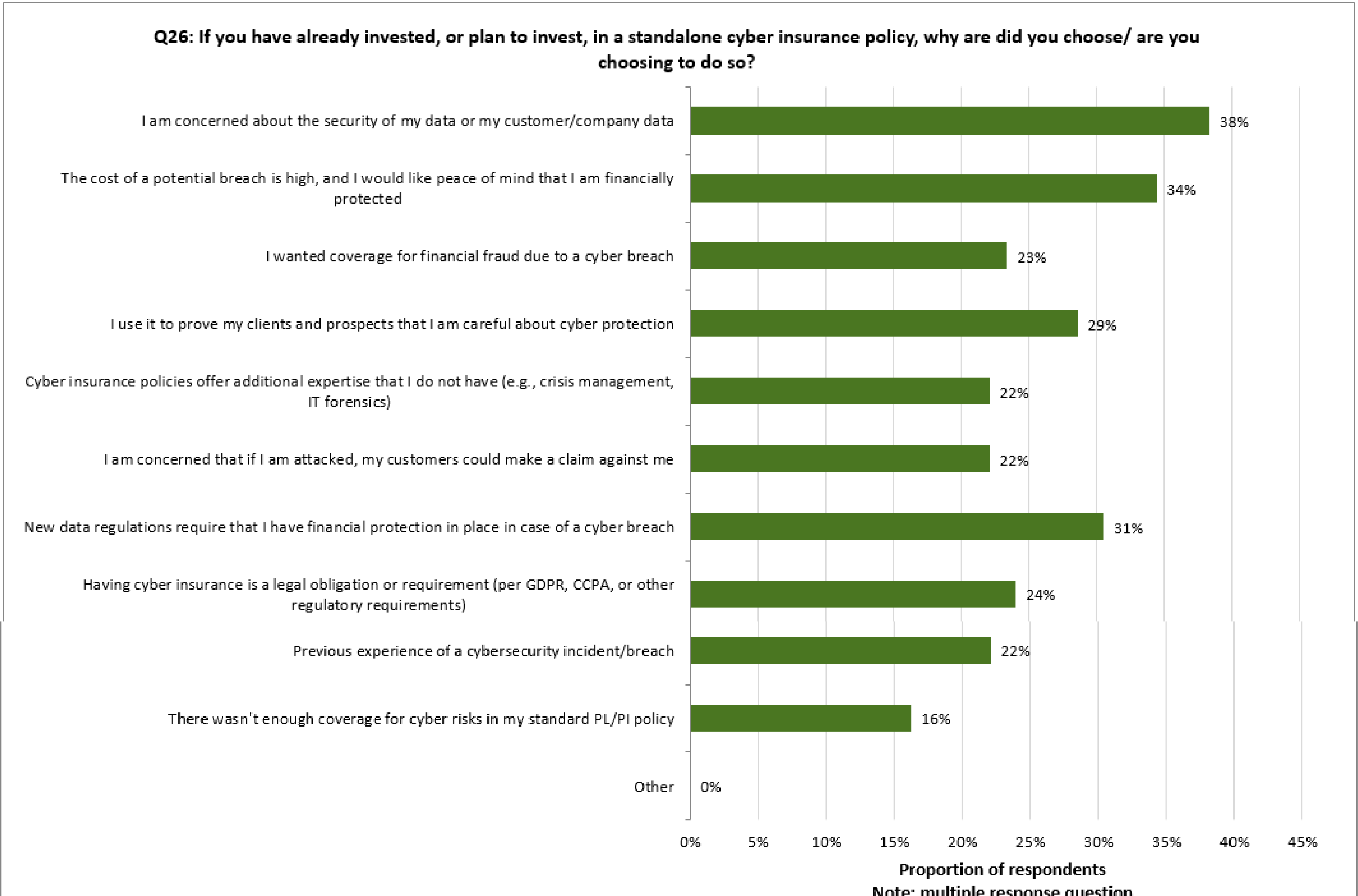
Belgium-specific requests: Attack by industry



Belgium-specific request: Recovery from ransomware



Belgium-specific request: Why purchase insurance?



Q26: If you have already invested, or plan to invest, in a standalone cyber insurance policy, why are did you choose/ are you choosing to do so?

Note: multiple response question

The fifth annual international Hiscox Cyber Readiness Report provides an up-to-the-minute picture of the cyber readiness of organisations, and offers a blueprint for best practice in the fight to counter an ever-evolving threat. It is based on a survey of executives, departmental heads, IT managers and other key professionals. Drawn from a representative sample of organisations across eight countries by size and sector, these are the people on the front line of the business battle against cyber crime.

About this year's report

The countries covered (Belgium, France, Germany, the Netherlands, Spain, the UK and the US) have been extended this year to include the Republic of Ireland. The size of the respondents has increased from 5,569 companies to 6,042, reinforcing the position of the Hiscox Cyber Readiness Report as one of the broadest of its kind.

We have adopted median rather than mean figures for numbers of attacks and costs this year and restated prior-year figures in the same terms. Given the extreme variation in the underlying figures between the very smallest and very largest companies, this provides a more accurate representation of the study group as a whole.

HISCOX

Thank you