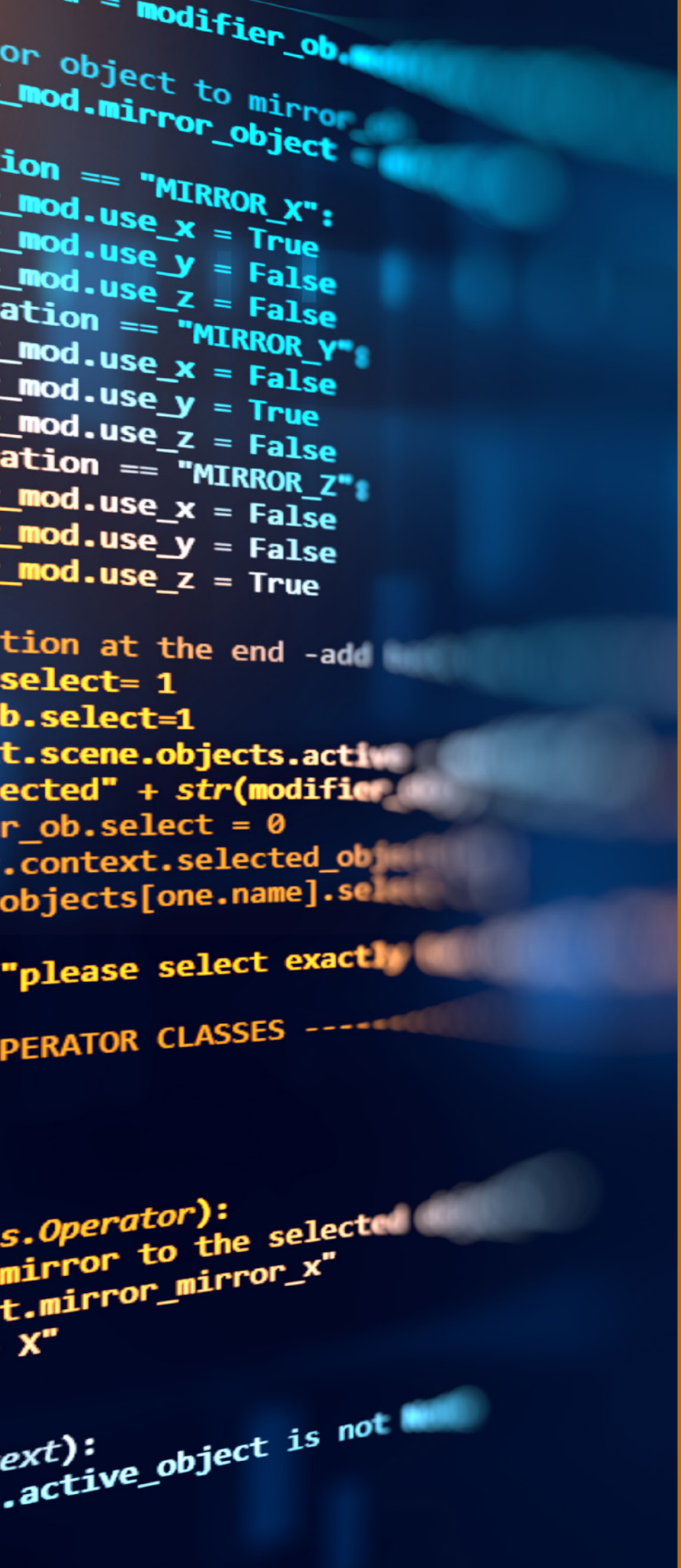
The PwC CFO Survey Series

Survey 2: Cybersecurity

July 2020

pwc


modifier_ob.
or object to mirror
_mod.mirror_object
ion == "MIRROR_X":
_mod.use_x = True
_mod.use_y = False
_mod.use_z = False
ation == "MIRROR_Y":
_mod.use_x = False
_mod.use_y = True
_mod.use_z = False
ation == "MIRROR_Z":
_mod.use_x = False
_mod.use_y = False
_mod.use_z = True
tion at the end -add
select= 1
b.select=1
t.scene.objects.activ
ected" + str(modifier
r_ob.select = 0
.context.selected_ob
objects[one.name].se
"please select exactly
PERATOR CLASSES ----
s.Operator):
mirror to the selected
t.mirror_mirror_x"
X"
ext):
.active_object is not

Introduction

The PwC CFO Survey Series

The current economic crisis due to the COVID-19 pandemic is rippling throughout businesses across the globe. To gauge its impact on Belgian companies, PwC Belgium has launched the CFO Survey Series, consisting of periodic surveys on the effects of the crisis on finance, operations, workforce, supply chains and much more.

Survey 2: Cybersecurity

PwC asked CFOs of large corporates in Belgium across a variety of sectors to weigh in on the effects of the crisis on their cybersecurity strategies, and their plans and predictions for a post-COVID-19 world.

Highlights

76%
of CFOs in Belgium say cybersecurity budgets are increasing throughout the crisis

48%
of respondents cite ransomware for financial gain as the main cybersecurity threat

66%
of CFOs indicated an uptick in cyber attacks during the crisis

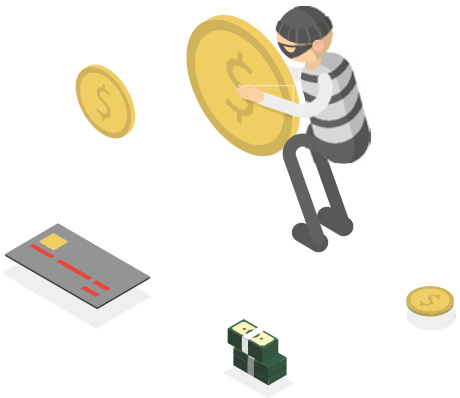
76%
of CFOs plan to increase cybersecurity awareness organisation-wide

CONFIDENCE BAROMETER 1: THE BELGIAN ECONOMY

Among respondents in PwC's CFO Survey 2: Cybersecurity, most (69%) expect Belgian economic growth to decline over the next 12 months, with 17% believing that the economy will contract greatly. This suggests growing optimism compared to the CFO Financial Resilience survey conducted in the week of 8 June 2020, in which 79% of respondents predicted economic decline and nearly half (43%) expected it to "decline greatly." The forecasted downward trend is in line with the National Bank of Belgium's recently predicted fall in GDP of 8.1% for 2020, a number that's been rising steadily since the onset of the pandemic.

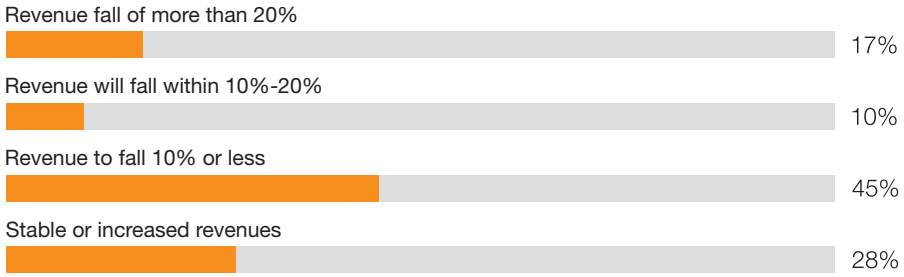
CONFIDENCE BAROMETER 2: REVENUES

When asked about the short-term outlook on company revenues, nearly half of CFOs surveyed (45%) indicated they expect revenues to fall by 10% or less in the coming six months, while just over a quarter (28%) predict stable or even increased revenues. This relatively optimistic outlook is likely an indication that company size and/or sector plays a significant role, with larger organisations and those in non-cyclical sectors being better positioned to survive the crisis than small- and medium-sized companies in affected sectors. The latest survey results on revenues, from the week of July 6 2020, are slightly more optimistic than CFOs' predictions in the previous survey.



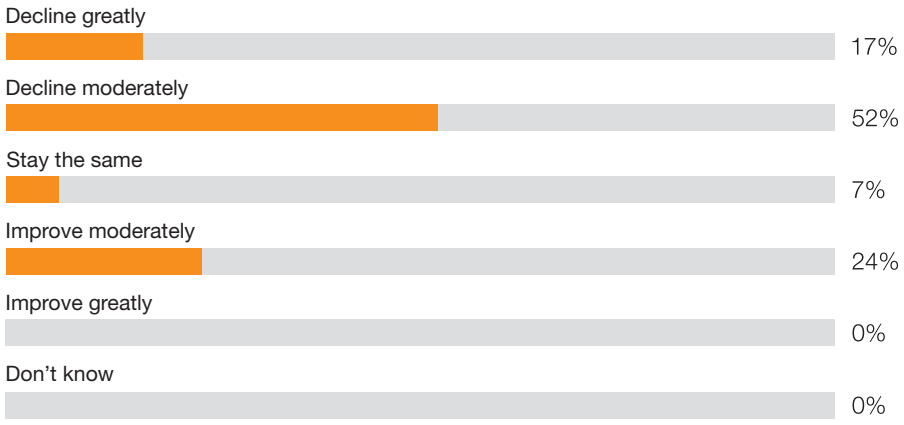
01

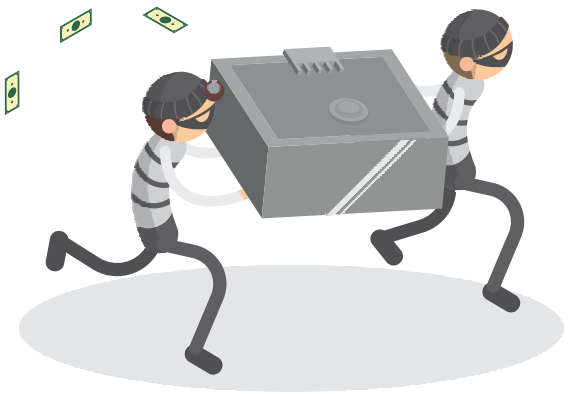
What are your organisation's predictions in terms of revenue in the coming 6 months?



02

Do you believe Belgian economic growth will improve, stay the same, or decline over the next 12 months?





CYBERCRIME: IT'S NOT A QUESTION OF IF, BUT WHEN

Advances in digital technology have drastically impacted day-to-day operations, both on an individual level and from a business perspective. But just as companies leverage technology to improve efficiency, so do cyber criminals: they're often a step ahead.

With over half of companies in Belgium falling victim to cybercrime,* the question is not if an attack will occur, but when. Insufficient preparation in the face of a threat can result in operational disruption, theft of intellectual property and other data, and serious financial and reputational damage.

Organisations need a robust cyber incident response plan to meet cyber threats head-on and minimise potential damage. Those that don't prioritise cybersecurity are leaving themselves open to malicious activities and potentially devastating data breaches.

*PwC Global Economic Crime and Fraud Survey

CYBERATTACKS DURING COVID-19

Cybersecurity is especially relevant in the current climate, as malicious actors are using the fear, uncertainty and doubt around COVID-19 to create their own epidemic of hacking attacks: in mid-April 2020, Google reported that every day it blocked more than 18 million malware and phishing emails related to COVID-19* that try to persuade users to click malicious links, enter their credentials on fake websites, or download malware, often masquerading as government announcements, charity or a cure for COVID-19.

*cloud.google.com

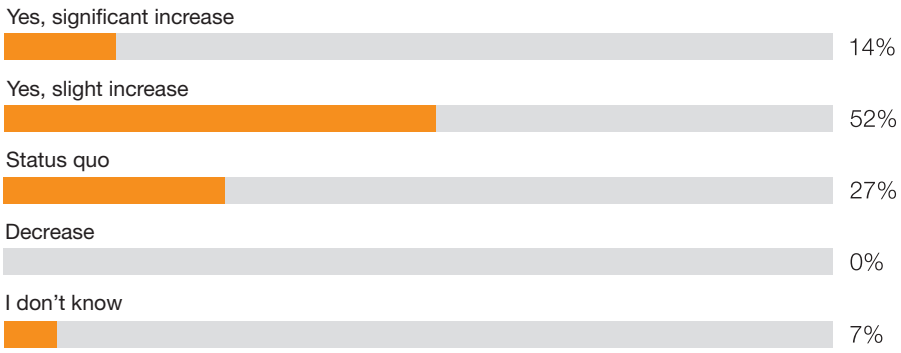
When asked if they perceived an uptick in cyberattacks since the onset of the pandemic, over half of CFOs in Belgium – 52% – replied that the rate of malicious cyber activity within their organisations has only increased slightly, while 14% cited a significant increase.

While cybercrime overall was already on the rise before the COVID-19 crisis started making headlines, the trend of recent attacks to target individuals continues. With a significant portion of the workforce operating remotely, hackers see their odds improve and they are zeroing in on those remote workers. Cyber criminals are playing on people's fear while leveraging the fact that online safety and security measures at home aren't always bulletproof.

Ingvar Van Droogenbroeck
Partner in PwC Belgium's Cyber & Privacy practice

03

Have you experienced an increase in security threats or attacks since the beginning of the COVID-19 outbreak?



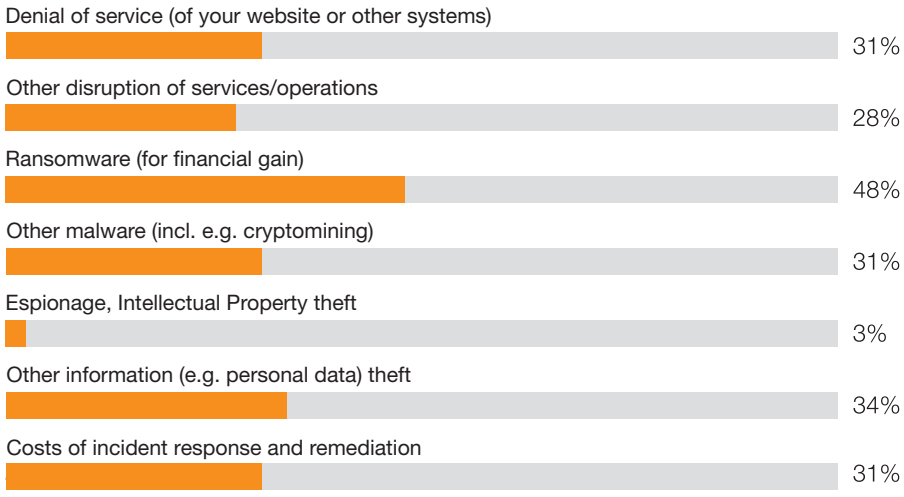
TOP CYBER THREATS TO ORGANISATIONS

When it comes to ranking the most significant cyber threats facing their companies, nearly half of CFOs in Belgium (48%) cited ransomware for financial gain as their top concern, followed by information theft, as indicated by 34% of respondents.

Ingvar Van Droogenbroeck provides an example of the latter: “There are threat actors out there effectively and systematically stealing intellectual property,” explains Van Droogenbroeck. “Rather than spending the time and money – which can be significant – on developing blueprints in-house, for example, there are shady organisations that have them stolen from competitors instead. This translates into major operational cost savings for the former, while costing the latter dearly.”

04

What are the main cyber threats your organisation is facing?

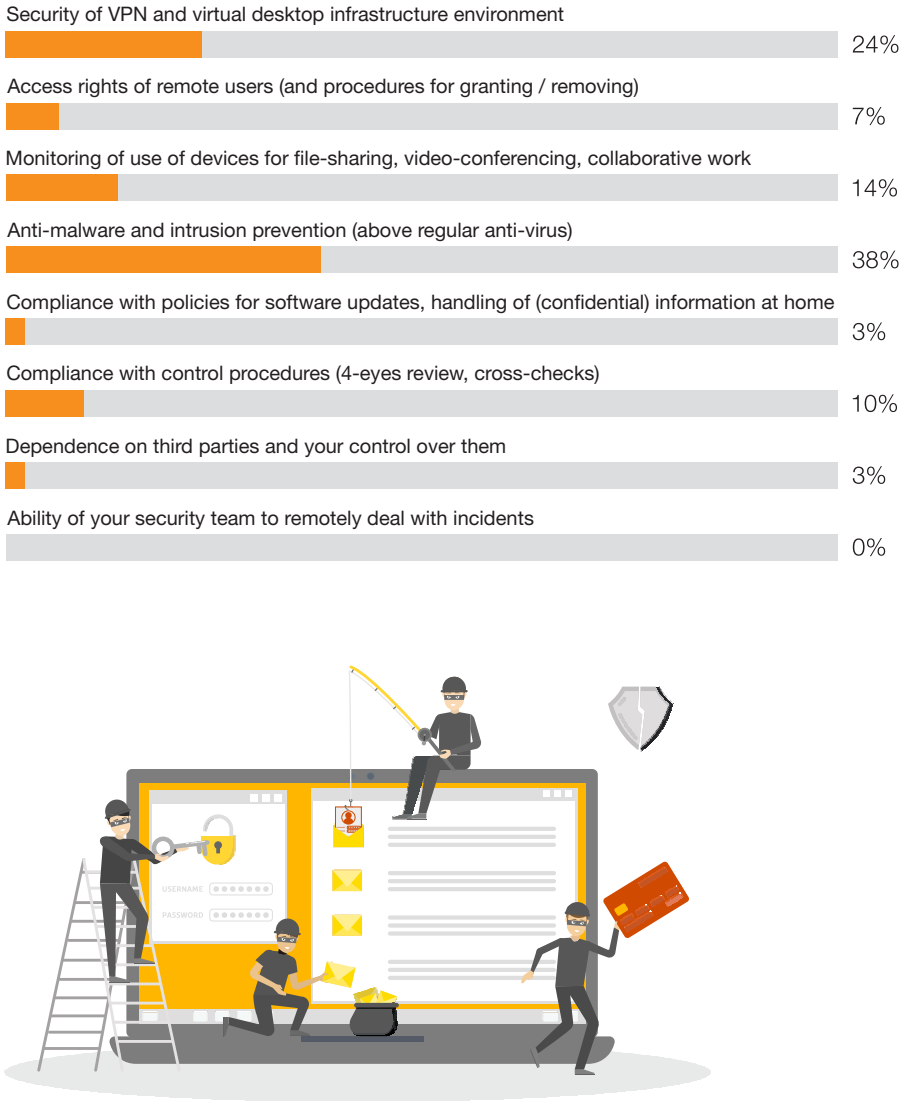


Cybersecurity and remote working

Widespread teleworking during the pandemic has increased risk in several areas. Among survey respondents, 38% pointed to malware / intrusion prevention as their top security concern related to working remotely. The second most prevalent concern, according to 24% of CFOs, is the effectiveness of the virtual private network (VPN) and the virtual desktop infrastructure (VDI).

05

What is your main security concern related to remote working? (Indicate top 3)

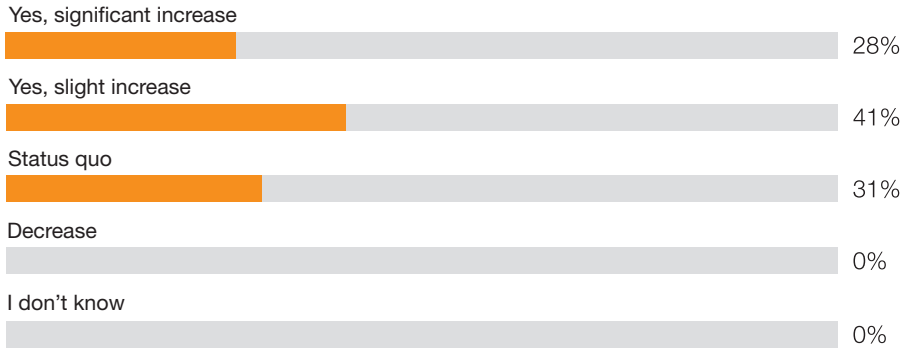


COVID-19 and cybersecurity defense strategies

Among CFOs in Belgium, 69% of those surveyed indicated that the importance of their cybersecurity strategies has increased due to the crisis, with 28% claiming it has “increased greatly.”

06

Has the COVID-19 pandemic increased the importance/relevance of security defense strategies in your organisation?

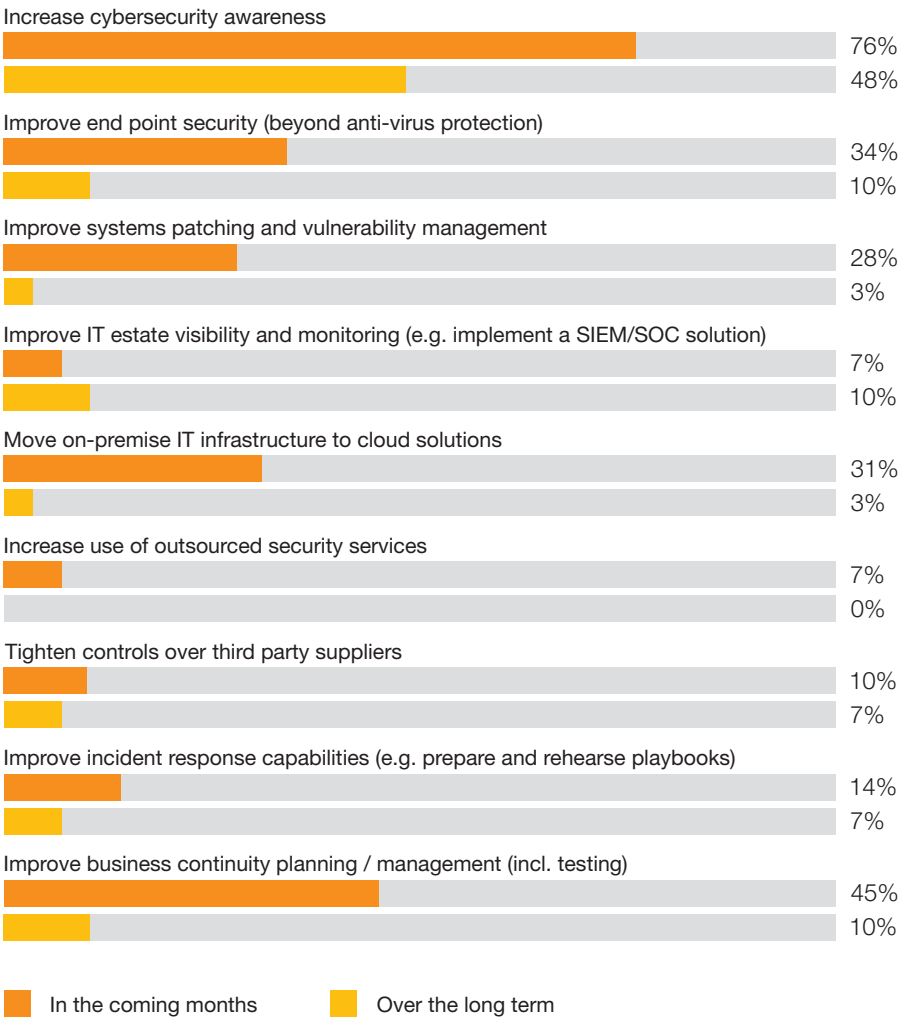


CYBERSECURITY PRIORITIES: NOW AND POST-COVID-19

When asked to list the actions they plan to take in the coming months, a large majority of survey respondents (76%) aim to increase cybersecurity awareness organisation-wide. Business continuity planning is also high on the agenda, at 45%, followed by 34% who intend to improve endpoint security. Over the longer term, 48% of CFOs in Belgium plan to continue to prioritise increasing awareness.

07

Which of the following actions will you take in the future? (Indicate top 3)

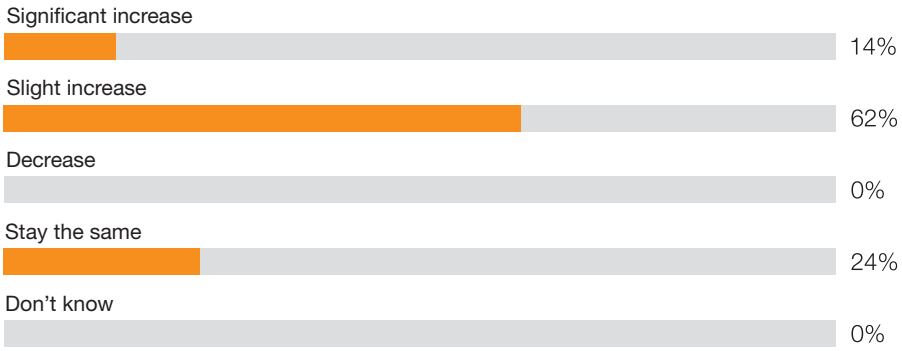


PANDEMIC SECURITY SPENDING

A majority of survey respondents (76%) indicated that cybersecurity budgets will increase as the crisis continues. In relative terms, this suggests the allocation of an even larger proportion of funds to cybersecurity than other areas. Ingvar Van Droogenbroeck offers insights: “Due to the economic downturn, companies are cutting costs across the board. Projects are being revisited on a regular basis and often postponed or cancelled completely. You could argue that as expenditures are being cut in other areas while cybersecurity budgets are on the rise, security spending becomes even greater in relative terms.”

08

How will your IT security budgets evolve over the coming period?



This reflects the findings of the recent *PwC global Digital Trust Insights Pulse Survey*, which showed that significant investments in the past two to three years helped companies weather the current crisis. These include remote work enablers (such as a virtual private networks – VPNs, mobile device management and endpoint security); crisis management initiatives (disaster recovery planning, incident response services); and data-driven risk management (such as real-time threat intelligence, use of data analytics and quantification of cyber risk).

What should organisations do to optimise cybersecurity?

COVER THE BASICS

- Make sure that remote work arrangements are secure.
- The long-term view is often different from the short-term view. Watch for blind spots.
- Crises precipitate new approaches: re-assess the cybersecurity strategy and investment priorities.

LAUNCH AWARENESS CAMPAIGNS

Communication on cybersecurity needs to be a focus. Security messages must be embedded company-wide through campaigns involving phishing exercises, security notifications, etc. Mature organisations are usually doing this to varying degrees, yet some rely solely on a security briefing during onboarding, which is largely insufficient.

FIRST PROCESSES, THEN KPIS

Companies often make the mistake of starting with cybersecurity KPIs, while processes and controls are not yet mature. This is a flawed approach. Different types of targets are relevant when rolling out a new solution vs. when in run mode. Similarly, visualisation dashboards are only useful when you're sure of the quality of the underlying data.

An action plan depends greatly on the organisation's sector, risk acceptance and competitors. As Ingvar Van Droogenbroeck illustrates, "Companies can invest endlessly in technology solutions, but they need to spend smartly and pay commensurate attention to the people and processes that make the technology work. Don't be the gazelle at the back of the herd who gets eaten, or the one at the front who's overspending, potentially on the wrong aspects."

For questions about the survey or additional information on cybersecurity, don't hesitate to get in touch, or visit **www.pwc.be/cyber**.

Contact

Ingvar Van Droogenbroeck

ingvar.van.droogenbroeck@pwc.com