CYBERSECURITY RESOURCE ALLOCATION & EFFICACY INDEX
Q3-2020 REPORT

November 2020

POWERING THROUGH THE PANDEMIC

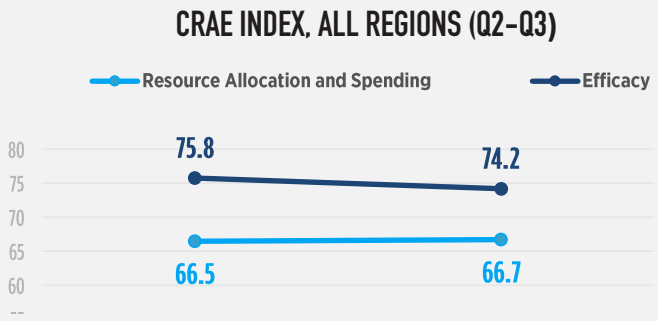
ORGANIZATIONS UNDER STRESS REMAIN VIGILANT IN DEALING WITH CYBERRISKS

The Cybersecurity Resource and Spending Allocation (CRAE) Index edged up to 66.7 in Q3 from 66.5 in Q2. This composite index, which is based on CyberRisk Alliance's (CRA) quarterly survey among U.S. and European organizations, points to negligible growth of resource and spending allocations in mitigating the increased cyberrisks associated with WFH employees during the Covid-19 pandemic. The latest survey reveals that more than half of all respondents (52%) continue to deal with phishing attacks and were often targets of endpoint malware, Web/cloud attacks, unauthorized resource, application, or data access, and exfiltration of sensitive data. However, despite respondent accounts of increased downtime, reduced productivity, and revenue losses, their confidence about cybersecurity remains strong as indicated by the Efficacy Index reading of 74.2, although a 1.6-point dip in Q3 hints that positive sentiment may be waning.

Overall, three out of five NIST sub-index component index readings ("Identifying," "Protecting", and "Recovering") rose in Q3 as organizations reported increased resource and spending allocations for proactive cybersecurity measures, such as process improvements, system and software upgrades, and increased employee awareness and training. Efficacy sentiment for four out of five activities also increased, although at a slower pace in Q3. "Recovering" efficacy expanded slightly faster on average, reflecting the increased confidence of respondents about their initiatives to recover from information security events and breaches.

CRAE INDEX, ALL REGIONS (Q2–Q3)

Includes North America (U.S. and Canada) and Europe (U.K., France, and Germany)



What respondents are saying:

- "WFH increased the efforts in trying to identify cyber threats from datacenter focus to endpoint." (Financial Services, U.S.)
- "Covid-19 has meant that many people are working from home using their personal computers. Consequently, we have had to ensure all those all devices used have the necessary software to ensure all sensitive info is protected. This has proved expensive and time consuming." (Financial Services, France)
- "Majority of white-collar workforce working from home due to pandemic has put more stress on VPN and mobile security systems/tools." (Manufacturing, U.S.)
- "COVID pandemic has increased cyber threats against our IT infrastructure. We are finding a lot more email attempts to breach our infrastructure." (Manufacturing, France)
- "Outside vendors being hacked into and getting our patients' information." (Healthcare, U.S.)
- "Increase in healthcare industry security incidents overall, but also one particular incident that impacted our organization that has accelerated investment in cyber security." (Healthcare, U.S.)
- "We experienced an attack on our organization that exposed email address, usernames, names, etc. of many costumers… We had to increase our cybersecurity budget and improve the technology we use in order to respond to cyberattacks in the future." (High Tech/Business Services, U.S.)
- "The teams evaluate new potential dangers on a daily basis; you can identify weak points in the daily exchange with other colleagues and hackers." (High Tech/Business Services Germany)
- "The move to a remote workforce has meant massive education for our workforce to deal with not only compliance with our own systems, but shadow IT problems as well." (High Tech/Business Services, Canada)

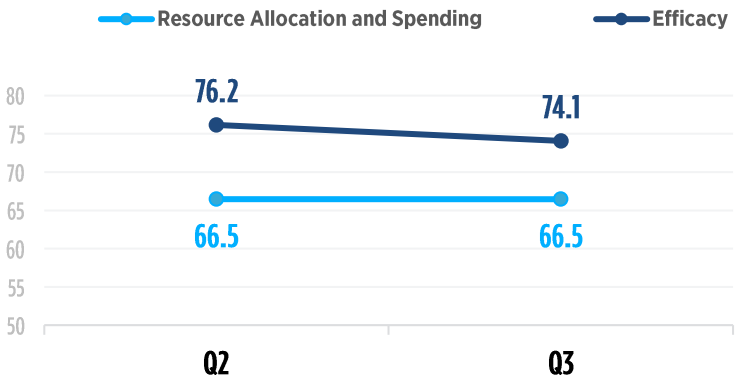
CYBERSECURITY RESOURCE ALLOCATION & EFFICACY INDEX
Q3-2020 REPORT

"Increased activity towards remote workers has increased our vigilance and controls for accessing the network remotely."
(U.S.)

CRAE INDEX, NORTH AMERICA (Q2-Q3)

In North America, the Q3 Resource Allocation and Spending Index held steady at 66.5 while the associated Efficacy Index dropped 2.1 points to 74.1. Although organizations in the U.S. and Canada reported the same levels of increased cybersecurity resource and spending allocation as Q2, total efficacy readings declined 2.1 points to 74.1 in Q3, signaling an easing of expanding optimism about cybersecurity activities and investments among North American organizations.

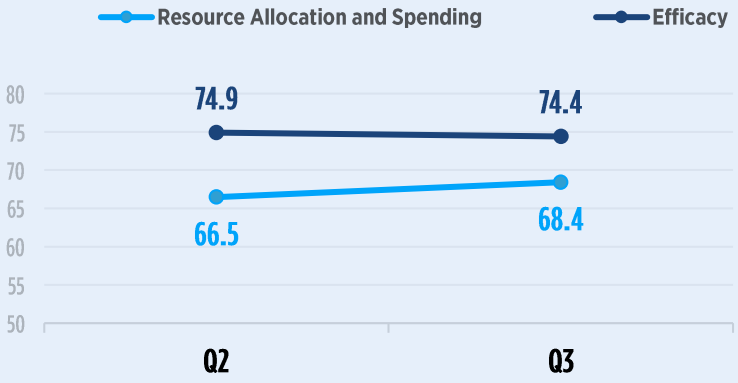
In this quarter, U.S. and Canadian respondents reported their increased focus on remote workforces forced them to upgrade their security tools, ramp up employee IT security training, and improve communications between executives and employees. One U.S. respondent described a "culture change" as security was pushed further into their organization.



CRAE INDEX, EUROPE (Q2-Q3)

The European Q3 CRAE Index for Resource Allocation and Spending increased to 68.4 from 66.5 in Q2 while the associated Efficacy Index dipped to 74.4 from 74.9.

Thanks to GDPR, European companies have been investing in securing privacy data for several years, and the pandemic has amped up their overall cybersecurity concerns. Additionally, with the end of the Brexit transition period fast approaching, the impact to cybersecurity regulations and availability of qualified IT security talent are concerns for many UK organizations.



CYBERSECURITY RESOURCE ALLOCATION & EFFICACY INDEX
Q3-2020 REPORT

A DEEPER DIVE

INDEX	RESOURCE ALLOCATION/SPENDING					EFFICACY				
	Q3	Q2	Change	Rate of Change	Trend	Q3	Q2	Change	Rate of Change	Trend
CRAE - All Regions	**66.7**	**66.5**	**0.2**	**Faster**	**Expansion**	**74.2**	**75.8**	**-1.6**	**Slower**	**Expansion**
Identifying	67.2	66.4	0.8	Faster	Expansion	72.4	75.8	-3.4	Slower	Expansion
Protecting	69.7	68.1	1.5	Faster	Expansion	75.0	76.5	-1.5	Slower	Expansion
Detecting	66.7	67.3	-0.6	Slower	Expansion	73.9	77.0	-3.1	Slower	Expansion
Responding	63.3	64.4	-1.1	Slower	Expansion	75.2	75.7	-0.5	Slower	Expansion
Recovering	66.5	66.0	0.5	Faster	Expansion	74.5	73.8	0.7	Faster	Expansion
CRAE - North America	**66.5**	**66.5**	**-0.01**	**Slower**	**Expansion**	**74.1**	**76.2**	**-2.1**	**Slower**	**Expansion**
Identifying	66.3	66.9	-0.6	Slower	Expansion	71.8	76.2	-4.4	Slower	Expansion
Protecting	68.8	68.1	0.7	Faster	Expansion	73.1	77.4	-4.4	Slower	Expansion
Detecting	65.3	67.8	-2.5	Slower	Expansion	73.5	76.9	-3.4	Slower	Expansion
Responding	65.0	64.0	1.0	Faster	Expansion	76.0	76.7	-0.7	Slower	Expansion
Recovering	66.9	65.6	1.3	Faster	Expansion	76.0	73.5	2.4	Faster	Expansion
CRAE - Europe	**68.4**	**66.5**	**2.0**	**Faster**	**Expansion**	**74.4**	**74.9**	**-0.5**	**Slower**	**Expansion**
Identifying	69.2	65.4	3.8	Faster	Expansion	73.5	75.0	-1.5	Slower	Expansion
Protecting	71.6	68.3	3.3	Faster	Expansion	79.0	74.5	4.5	Faster	Expansion
Detecting	69.8	66.4	3.4	Faster	Expansion	74.5	77.0	-2.5	Slower	Expansion
Responding	65.8	65.3	0.5	Faster	Expansion	73.5	73.5	0.03	Faster	Expansion
Recovering	65.8	67.0	-1.3	Slower	Expansion	71.5	74.5	-3.0	Slower	Expansion

Across all regions, organizations registered a slightly faster expansion of resources and spending allocations in Q3 for the proactive components of the NIST framework – identifying cybersecurity risks and protecting systems and assets – driven mostly by the point gains in Europe for these sub-index readings. The "Recovering" component, which includes reactionary measures for handling cybersecurity, increased marginally overall (0.5 point) for resource/spending allocations and efficacy (0.7 point), is mostly attributed to the upward trend of this sub-index for North America.

North America is more rapidly expanding reactive cybersecurity measures, as readings inched up to 65.0 for resource/spending allocations for "Responding" and 66.9 for "Recovering." "Recovering" efficacy rose to 76.0 as a result of a 2.4 point increase in Q3, suggesting increasing respondent confidence about recovery measures. European organizations, on the other hand, more rapidly expanded resource/spending allocations for the proactive NIST components and slowed expansion for "Recovering" (-1.3 points). The European efficacy reading for the "Protecting" sub-index, which includes educating/training employees, developing processes to secure assets, and purchasing/implementing technology, outpaced all others in Q3, with a 4.5 point increase since Q2.

"We use AI and log analysis products for threat identification and use this data to evolve our response and monitoring strategy."
(U.K.)

CYBERSECURITY RESOURCE ALLOCATION & EFFICACY INDEX
Q3-2020 REPORT

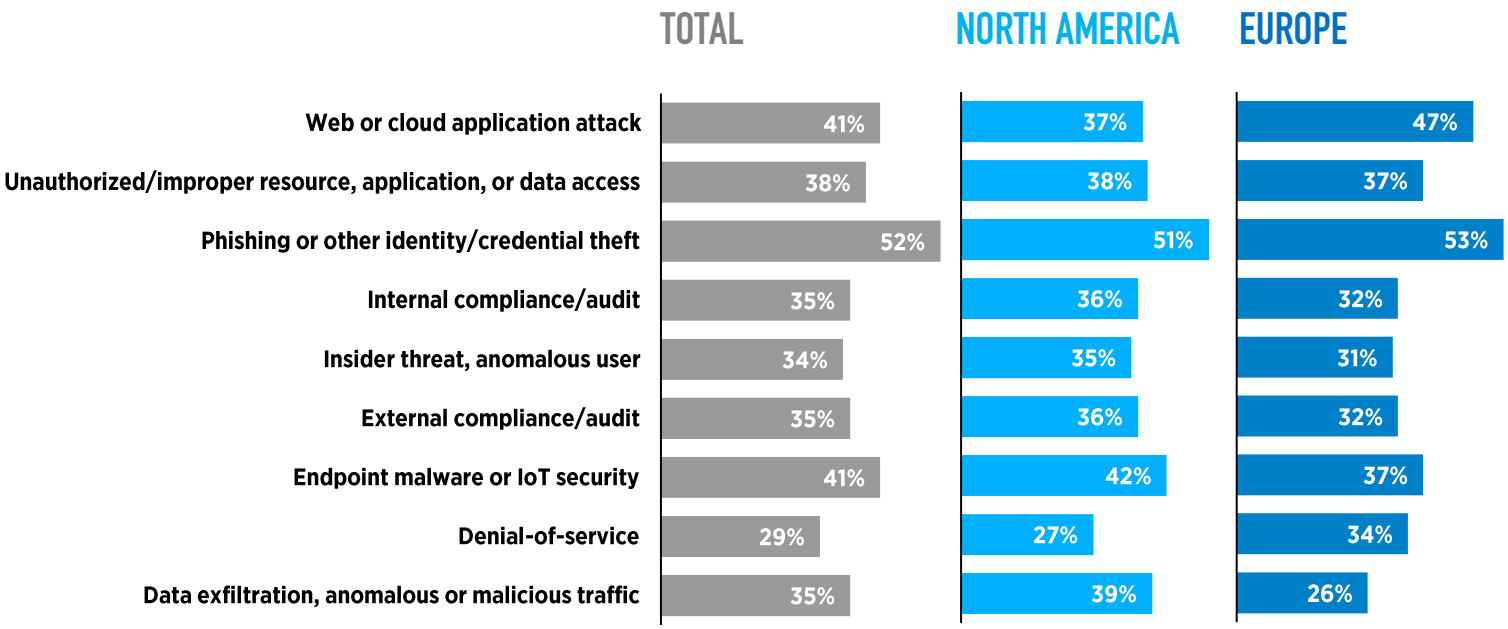
"My organization has been very cautious and aware since a recent cyber threat. We are now carefully monitoring all activities in regards to protecting data."
(U.S.)

TOP CONCERNS

Respondents reported having the most issues with phishing or other identity/credential theft (52%); endpoint malware or IoT security (41%); and web or cloud application attacks (41%). Additionally, more than one-third (38%) of respondents across all regions experienced unauthorized or improper resource, application, or data access, and hence many indicated that protecting their organization's data is a chief concern. North American respondents (39%) were significantly more likely than Europeans (26%) to have encountered data exfiltration, anomalous, or malicious traffic; North Americans were also twice as likely to report such problems than those in France or Germany (U.K. respondents experienced similar rates to those of the U.S. and Canada).

Which of the following events did your organization identify, detect, respond to, or recover from in Q3?

(Select all that apply)

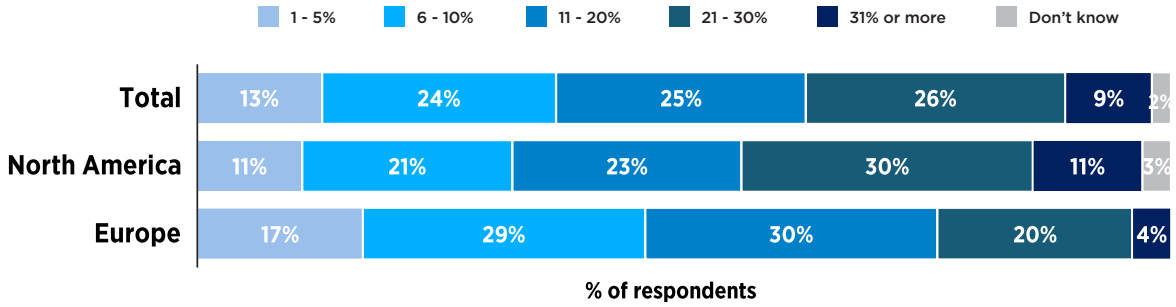


CYBERSECURITY BUDGETS

On average, 35% of respondents reported allocating more than one-fifth of their IT budgets to cybersecurity. North American respondents are more likely than their European counterparts to have a larger share of their budget going towards IT security – 41% of North Americans compared to 24% of Europeans allocate more than one-fifth of their IT budget to cybersecurity solutions.

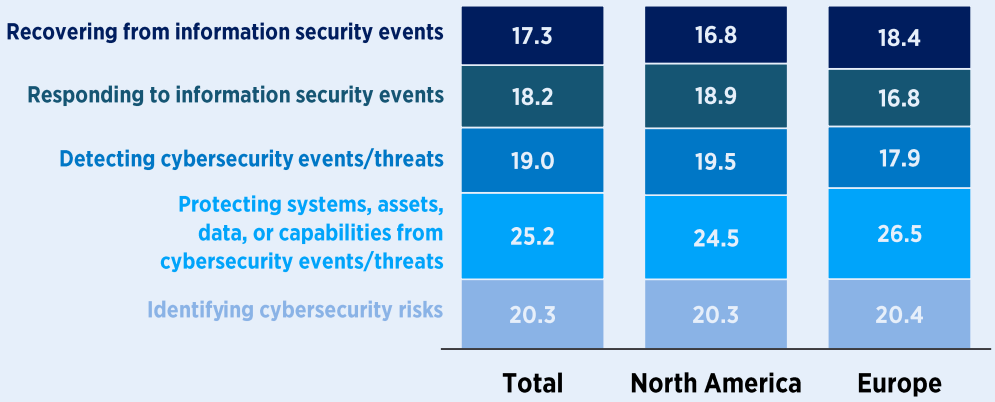
What percent of your organization's 2020 total IT budget is/will be spent on cybersecurity solutions in 2020?

(% of respondents in each category)



How is your organization's total 2020 cybersecurity budget or spending allocated across each of the 5 cybersecurity categories?

(% of budget))



BUDGET ALLOCATION

Overall, respondents reported allocating about 45% of their cybersecurity budgets or spending to the two proactive components of the NIST framework: Identifying" (20.3%) and Protecting (25.2). Many organizations noted an increase in proactive measures since the onset of the pandemic, particularly in monitoring user behavior, device monitoring, and employee training.

CYBERSECURITY RESOURCE ALLOCATION & EFFICACY INDEX
Q3-2020 REPORT

ABOUT CRA BUSINESS INTELLIGENCE

CRA Business Intelligence is a full-service market research capability focused on the cybersecurity industry. Drawing upon CRA's deep subject-matter expertise and engaged community of cybersecurity professionals — along with a newly recruited, world-class market research competency — CRA Business Intelligence is unique in our industry.

These components together enable delivery of unparalleled data and insights anchored in our engaged community of cybersecurity professionals and business leaders eager to share their perspective on the market's most important concerns.

CRA Business Intelligence provides:

- Ground-breaking proprietary research to inform and engage our community
- Custom research to support strategic product and marketing initiatives
- Innovative thought-leadership content development and promotion
- Brand engagement through business activity indexes, interactive tools and assessments, and more

ABOUT THE CRAE INDEX

The CRAE Index is a quarterly, time-series tracker that reports the overall focus and direction of organizations' cybersecurity activities, spending, and perceived progress over time. It comprises two composite indices – Resource/Spending and Efficacy – to monitor the state of organizations' allocations and spending on cybersecurity activities and their perceptions about the efficacy of these measures.

Index data is derived from quarterly surveys among 300 business, IT, and cybersecurity professionals at organizations with at least 500 employees in manufacturing, high tech/business services, financial services, and healthcare industries in North America and Europe. Sub-indices are developed based on each of the National Institute of Standards and Technology (NIST)'s five Cybersecurity Framework components, which are averaged to create the two composite indices. (For each sub-index, a diffusion index is calculated to describe the change in resource allocations, spending, and efficacy by calculating the sum of the percentages of respondents indicating "higher" and half of those indicating the "same" when comparing resources, spending, and efficacy to the previous quarter. A reading of over 50 indicates an increase relative to the prior quarter, and a reading below 50 indicates a decrease.) Quarterly point increases and decreases indicate whether a trend is changing faster or slower.

This index was developed by CyberRisk Alliance Business Intelligence and underwritten by Pulse Secure (acquired by Ivanti).

ABOUT PULSE SECURE

Pulse Secure (acquired by Ivanti), the exclusive underwriter of the CRAE Index, provides Secure Access solutions for people, devices, things and services that improve visibility, protection and productivity for its customers. Pulse Secure integrates cloud, mobile, application and network access to enable hybrid IT in a Zero Trust world. Over 24,000 enterprises entrust Pulse Secure to secure their workforce.

Pulse Secure®
Acquired by Ivanti

THE NIST CYBERSECURITY FRAMEWORK

The NIST Cybersecurity Framework is a set of best practices, standards, and recommendations that help an organization improve its cybersecurity measures. It organizes its core material into five functions, which are subdivided into a total of 23 categories. Collectively it defines 108 subcategories of cybersecurity outcomes and security controls.

Source: https://www.nist.gov/cyberframework