

# CYBERSECURITY RESOURCE ALLOCATION & EFFICACY INDEX

## Q2-2020 REPORT

August 2020

## PROACTIVE CYBERSECURITY MEASURES OUTPACED REACTIVE IN Q2

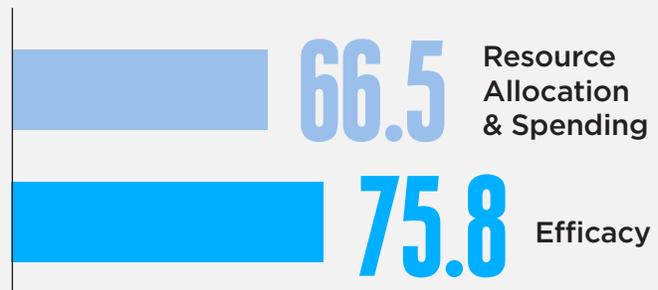
Under pressure, large companies' cybersecurity forces leaned in, and got the results they intended

Amid the extreme challenges cybersecurity teams experienced in the second quarter of 2020, a newly released business-activity index shows that companies with 500 or more employees in North America and Europe emphasized proactive security measures to protect assets and detect breaches during the period, outpacing more reactive activities, such as identifying, responding or recovering from breaches. The index also showed security professionals who took such proactive measures were significantly more satisfied with the impact of their efforts than those who did not.

For most organizations, second quarter 2020 activities were heavily influenced by fallout from the pandemic itself and the related far-reaching economic downturn. Their approach to these conditions suggests confidence in the cybersecurity strategies they had in place as they entered the crisis period. The Cybersecurity Resource Allocation and Efficacy (CRAE) Index is a quarterly tracker of momentum in cybersecurity investment and sentiment about the impact of cybersecurity programs, developed by CyberRisk Alliance (CRA) Business Intelligence and underwritten by [Pulse Secure](#). The inaugural index compared the momentum of spending and sentiment in the second quarter of 2020 to that of the first quarter.

### CRAE INDEX, ALL REGIONS

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



INDEX	RESOURCE/ SPENDING ALLOCATION		EFFICACY	
		Q2 v Q1		Q2 v Q1
<b>CRAE - All Regions</b>	<b>66.5</b>	<b>Increased</b>	<b>75.8</b>	<b>Increased</b>
Identifying cybersecurity risks	66.4	Increased	75.8	Increased
Protecting systems, assets, data, or capabilities from cybersecurity events or threats	68.1	Increased	76.5	Increased
Detecting cybersecurity events or threats	67.3	Increased	77.0	Increased
Responding to information security events	64.4	Increased	75.7	Increased
Recovering from information security events	66.0	Increased	73.8	Increased

### 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, IT/Tech, 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.)

This index was developed by CyberRisk Alliance Business Intelligence and underwritten by Pulse Secure.

# CYBERSECURITY RESOURCE ALLOCATION & EFFICACY INDEX

## Q2-2020 REPORT

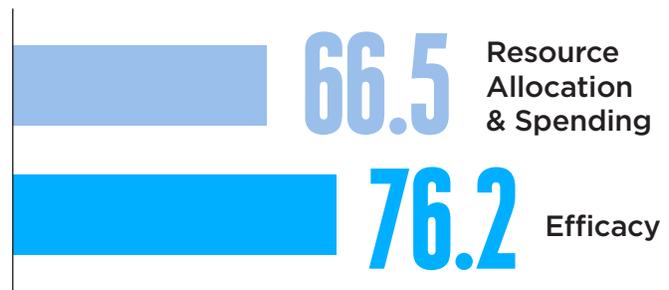
**“COVID has forced a reevaluation of security processes and detection. The increase of work at home users required a shift from campus focused security to remote security.”**  
(U.S.)

### CRAE INDEX, NORTH AMERICA

The North American Q2 CRAE Index for Resource Allocation and Spending was 66.5 while the associated Efficacy Index was 76.2.

Like the rest of the world, organizations in North America spent the second quarter adjusting to the impact of COVID-19, particularly the extent to which it resulted in white collar workers being told to work from home, outside of the protection of the corporate firewalls and the rest of the cybersecurity infrastructure. IT organizations scrambled to scale up VPNs and scrutinize the security of cloud-based collaboration technologies, some newly deployed and others being used more intensively. Meanwhile, attackers exploited the situation with pandemic-themed phishing and social engineering exploits.

Despite the challenges, the index suggests most survey participants felt they were responding effectively.

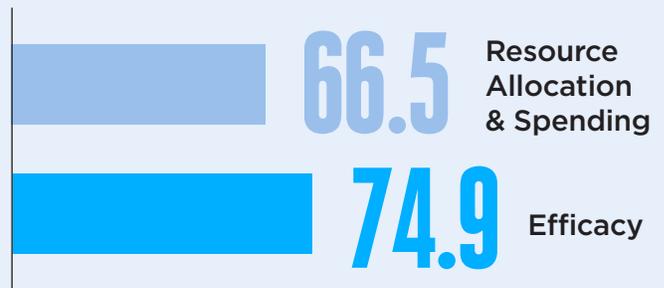


### CRAE INDEX, EUROPE

The European Q2 CRAE Index for Resource Allocation and Spending was 66.5 while the associated Efficacy Index was 74.9.

The spending score is a few points higher for Europe than for North America, possibly propelled by standards for cybersecurity and the protection of privacy set by the European Union's GDPR.

Despite having to meet a higher standard, the Europeans also indicated that the effectiveness of their efforts was improving rather than degrading during the crisis.



# CYBERSECURITY RESOURCE ALLOCATION & EFFICACY INDEX

## Q2-2020 REPORT

### A DEEPER DIVE

On a global basis, survey participants described similar patterns of investment and efficacy across all the major components of a security program, giving average scores ranging from 64.4 to 68.1 for Resource and Spending Allocation and 73.8 to 77.0 for Efficacy.

That suggests equal attention to investing in, and achieving results with, each of the elements of the NIST security framework. They are also looking for ways to stretch those investments. As one U.S. respondent told us, “Due to changes in the business landscape as a result of the current pandemic, we are constantly looking for ways to do more with less.”

North American organizations reported the greatest increase in Resource and Spending Allocation for the “protecting” category of their cybersecurity programs (68.1).

Digging deeper into the two components of this sub-index, resources and effort invested scored higher (70.5) than money spent (65.7). That is a common pattern in these numbers, probably reflecting the fact that it’s often easier to reassign staff and divert money than to increase the cybersecurity budget.

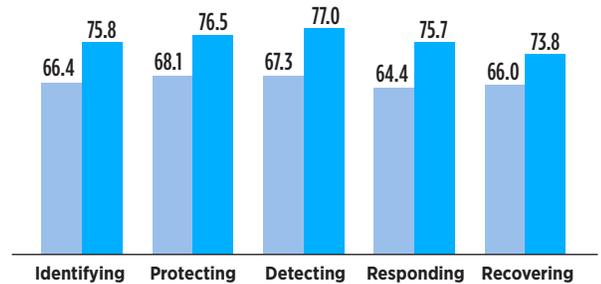
For Efficacy, the highest scores were in the categories of detecting and responding to incidents.

The resource and spending scores for Europe were generally consistent with those from North American organizations, plus or minus a point or two. In both geographies, organizations say they are spending more but also express increased confidence that their efforts are effective.

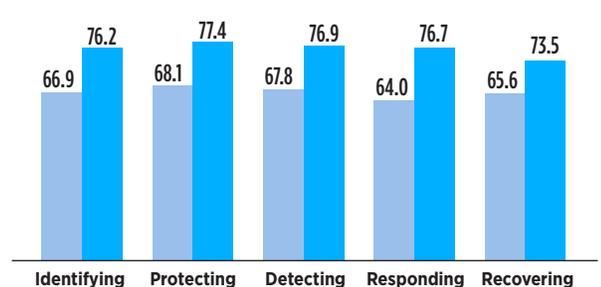
However, Europeans say they are spending a greater share of their IT budgets on cybersecurity efforts.

■ Resource Allocation & Spending ■ Efficacy

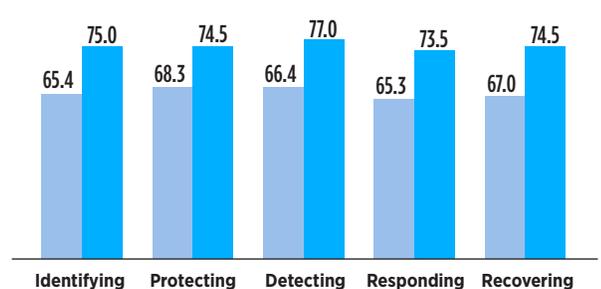
#### CRAE Sub-Indices, All Regions, Q2 - 2020



#### CRAE Sub-Indices, North America, Q2 - 2020



#### CRAE Sub-Indices, Europe, Q2 - 2020



“Greater awareness means more attacks, which has resulted in increased spending on security-related services.”  
(Germany)

# CYBERSECURITY RESOURCE ALLOCATION & EFFICACY INDEX

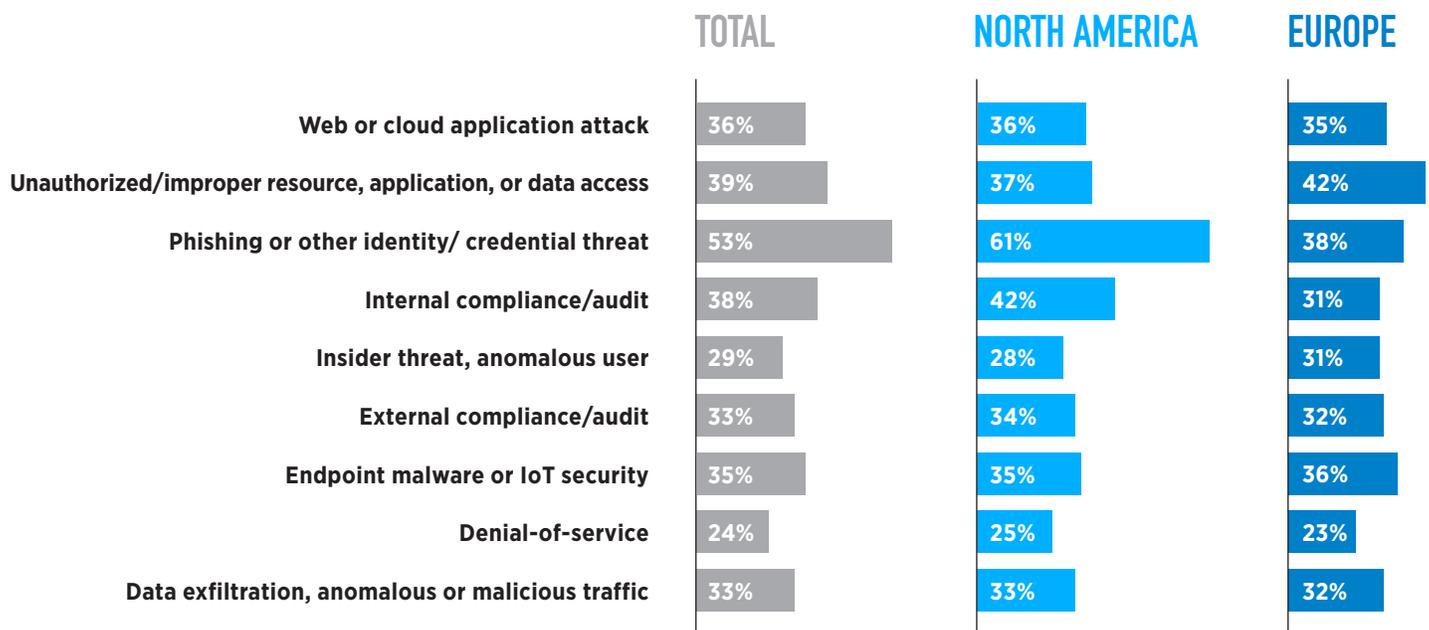
## Q2-2020 REPORT

### TOP CONCERNS

Phishing and identity theft caused the most grief for respondents, particularly those in North America. Concern with phishing was slightly higher in Canada (68%) than in the U.S. (59%). Canadians were also significantly more likely to report having experienced denial of service attacks (48%) and incidents involving insider threats and anomalous user accounts (58%) than their peers in the U.S. Unauthorized/improper resource, application, or data access was cited as the next highest concern (39%), and it was at the top of the list for Europeans (42%).

### Which of the following events did your organization identify, detect, respond to, or recover from in Q2?

(Select all that apply)



# CYBERSECURITY RESOURCE ALLOCATION & EFFICACY INDEX

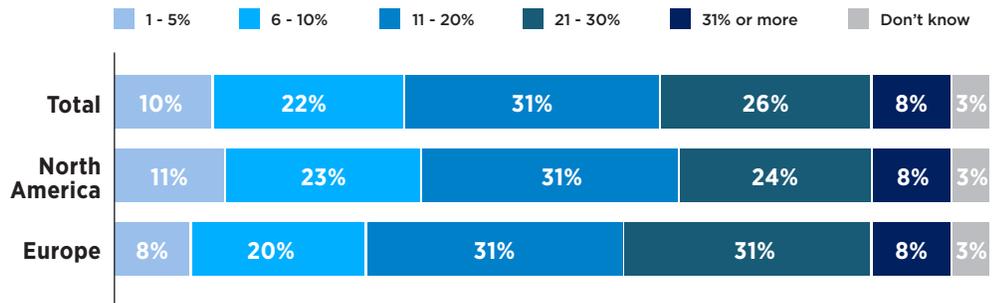
## Q2-2020 REPORT

### CYBERSECURITY BUDGETS

At least one in three (34%) organizations allocated more than 20% of their IT budgets to cybersecurity, with European organizations budgeting a greater share, on average, than those in North America. We suspect tighter European privacy and security regulations such as GDPR account for the difference.

What percent of your organization's 2020 total IT budget is or 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

Protecting systems, assets, and data has the largest allocation of cybersecurity budgets, on average. That is followed closely by spending to detect cybersecurity events and threats.

In the category of protecting information assets, participants from the U.S. reported spending significantly more (26%) than peers in Canada or the U.K.

# CYBERSECURITY RESOURCE ALLOCATION & EFFICACY INDEX Q2-2020 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 PULSE SECURE

Pulse Secure, 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.



## 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>

