CYBERSECURITY RESOURCE ALLOCATION & EFFICACY INDEX Q1-2021 REPORT

May 2021

LARGE-SCALE CYBERATTACKS AND BREACHES WREAKING HAVOC IN 2021

CRAE Index shows organizations were victims of more damaging threats, attacks and data breaches in Q1

The Cybersecurity Resource Allocation and Efficacy (CRAE) Index survey, fielded in April/May 2021 and reflecting respondent activities in Q1 2021, revealed a rise in large-scale attacks, breaches and data leaks. The devastation was described by repondents as everything from: “We were attacked by ransomware and were forced to pay a substantial amount of $” to “Blackout of our electrical equipment as a result of cyberthreat” to “We were victims of a cyber attack and are still recovering from it.” But organizations fought back, deploying everything from strategic risk management, new processes, employee training, cyberrisk governance policies and technology, as well establishing internal “centers of excellence,” monitoring external vendors and partners and engaging with managed security service providers (MSSPs).

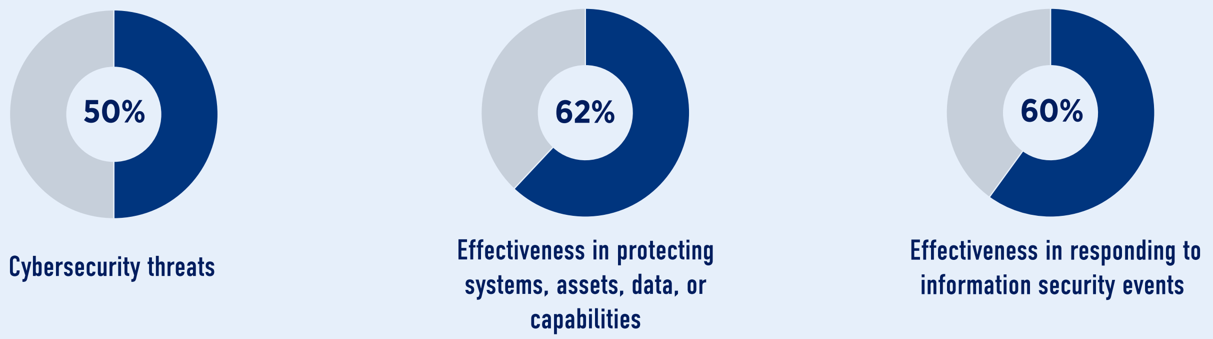
> “We were victims of a cyber attack and are still recovering from it.”
> (Canada)

While half of all respondents (50%) reported increased cybersecurity threats to their organizations in Q1, a greater share (62%) believed they were more effective in protecting their organization’s systems, assets, data, and capabilities compared to the previous quarter, and 60% said their effectiveness in responding to information security events increased. While more serious attacks facilitated increased investments and budget increases by victimized organizations, so did the fear of being attacked. According to one respondent, “We have been very lucky this past year that nothing has occurred, but we don’t want to take chances, so we are spending a lot of money to protect ourselves at this time.”

Q1 CRAE Index readings are available here.

Increases in threats and effectiveness

(% of respondents)



DEALING WITH THE DAMAGE

Organizations report serious threats and improved hacker strategies

Ransomware, phishing, data exfiltration and other tactics are not only increasing, they are succeeding, wreaking havoc on organizations' operations and their bottom line. Many respondents noted the number of attacks to their organizations significantly increased in Q1, while some said they faced constant external threats day after day. Moreover, respondents believe hacker strategies have improved and they are experiencing more "professional attacks" than in recent years.

Many described how their organizations were victimized by phishing and ransomware attacks in early 2021. A U.S. respondent working in the healthcare sector said they were "attacked by ransomware and forced to pay a substantial amount of [money]," while a Canadian-based healthcare employee reported "a large scale data breach where our systems were hacked, and half the organization was unable to work for a day." A "blackout of our electrical equipment as a result of cyberthreat" was recounted by a U.K. respondent from a high tech / business services firm.

Whiile not all respondents reported attacks to their organization in Q1, many were nonetheless on high alert, particularly those who believed they were in targeted industries. "Our specific industry was targeted heavily, and we saw multiple vendors and competitors get hit with ransomware, etc." noted a respondent from a U.S. manufacturing firm.

> "We had a security breach, which was bad for our name and reputation as a company, so it drove us to invest more in cybersecurity to stand firm and protected."
> (U.S.)

ORGANIZATIONS TAKING MORE ACTIVE ROLES IN CYBERSECURITY

Budget increases were often direct responses to severe attacks

All too often, it took a serious attack or data breach causing financial or reputational damage for corporate and security executives to become more aware of the risks to their organization. Some reported increased cybersecurity budgets for 2021 as a direct response to a breach experienced in the first quarter. Increased attention to cybersecurity issues with third-party vendor interactions and services was also mentioned as an increasing concern for several organizations.

Some respondents also reported increased involvement from upper management: "Our management became aware of customer concerns related to cybersecurity regulations while using our manufactured devices…and established a Product Cybersecurity Center of Excellence (PC-CoE) to manage and lead all aspects of our company's product cybersecurity program," according to a respondent employed at a U.K. manufacturing firm.

> “We got buy-in from senior management to recognize the importance of meaningful employee education on identifying cyber threats.”
> (Canada)

PEOPLE, PROCESSES, POLICIES AND TECHNOLOGY

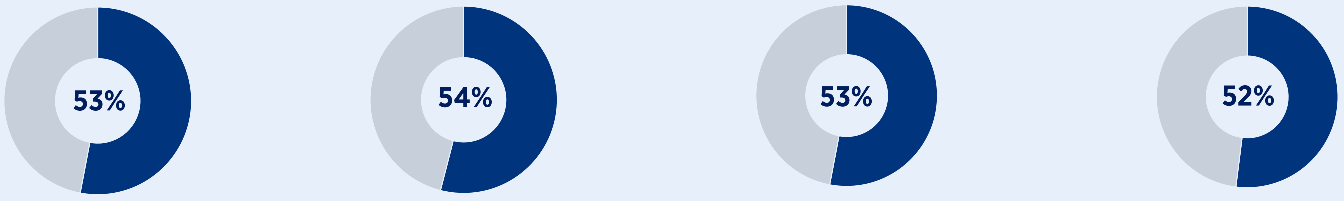
A shift in business priorities drove increased resources and investments

The security challenges so far this year created a sense of urgency, leading to increased investment in security hardware, software, services and consulting with an emphasis on employee training and elevation of cybersecurity as a business priority. Within their organizations, many respondents indicated they had made progress addressing increased threats and attacks as well implementing more holistic security strategies – uniting security teams and stakeholders to monitor and coordinate infrastructure, policies, processes and best practices, and employee training and communication. To that end, organizations reported increased resources in the following areas during the quarter:

- Educating/training employees about cybersecurity awareness (53%)
- Developing/modifying processes to secure digital or physical assets (54%)
- Developing or modifying a cybersecurity policy or governance program regarding users, roles, privileges, applications and/or data (53%)
- Purchasing, building, upgrading, or implementing technology to protect against or limit the impact of cybersecurity events/threats (52%)

Training, processes, policies and technology

(% of respondents reporting an increase in Q1)



Educating/training employees about cybersecurity awareness

Developing/modifying processes to secure digital or physical assets

Developing/modifying a cybersecurity policy or governance program

Purchasing, building, upgrading, or implementing cybersecurity technology

PHISHING, DATA BREACHES AND MORE

Organizations are dealing with a variety of threats and attacks

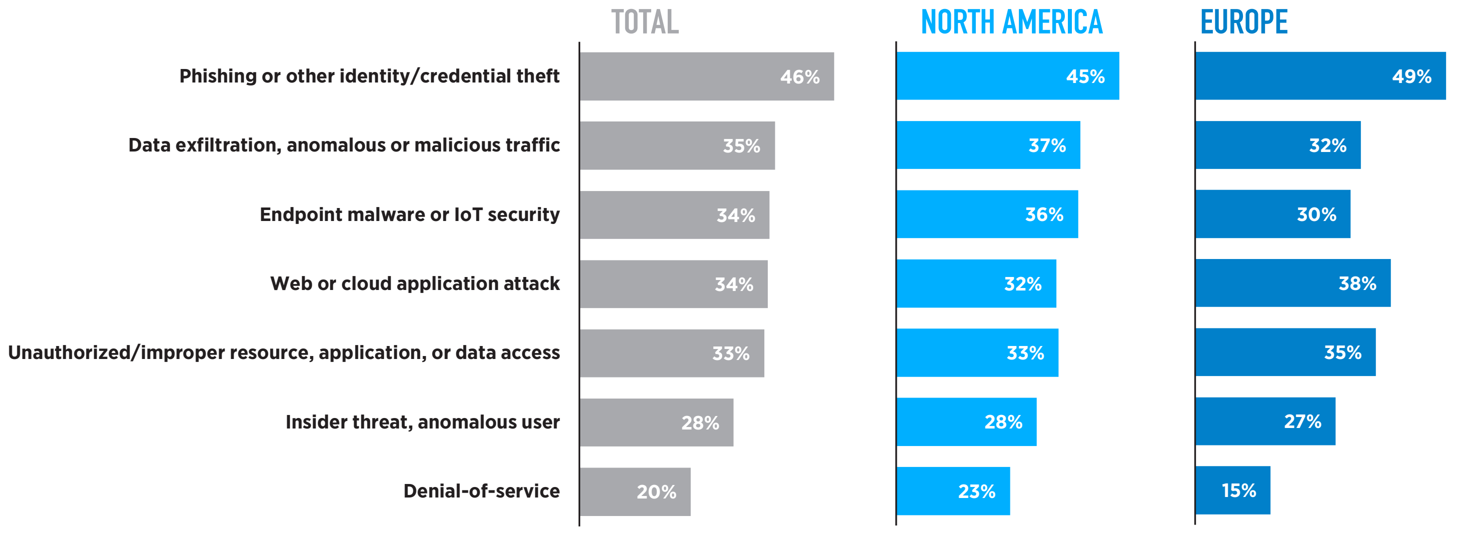
Overall, 94% of respondents reported some type of IT security event in Q1. While phishing remains the top threat for organizations worldwide in early 2021, organizations also dealt with a variety of other types of events, including data exfiltration, anomalous or malicious traffic and endpoint malware and IoT security events. "Hacking attacks, virus emails, phishing attacks and other illegal network attacks, forced us to deal with many challenges," according to one respondent working in high tech / business services.

Europeans reported a higher rate of phishing (49%), Web / cloud application attacks (38%) and unauthorized resource access (35%) than North Americans. Phishing was higher among manufacturing (59%) and financial services (54%) firms and more common among the largest organizations overall (59%). Data exfiltration was also highest in the high tech / business services sector (46%). At least one-third of respondents also reported endpoint malware or IoT security threats or Web / cloud application attacks.

> "We had attacks on our company's web pages... trying to get into our systems."
> (Germany)

Which of the following events did your organization identify, detect, respond to or recover from in Q1?

(Select all that apply)

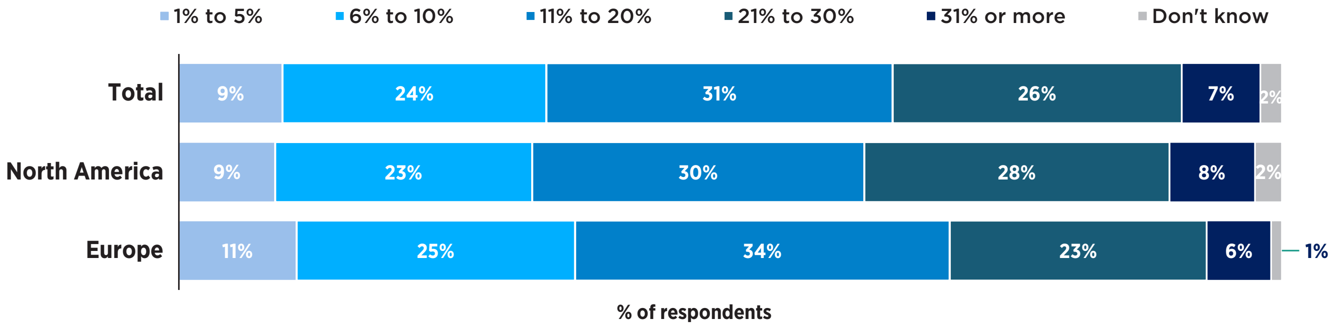


16% OF IT SPENDING ALLOCATED TO CYBERSECURITY

On average, respondents in North America and Europe are budgeting roughly 16% of their IT spending for cybersecurity in 2021. Consistent with last quarter, one-third (33%) of respondents said they allocated more than 20% of their IT budgets to cybersecurity. For North American organizations, the largest segment (30%) spent 11% to 20% of their budgets on cybersecurity; the greatest share of European respondents (34%) also designated 11% to 20%.

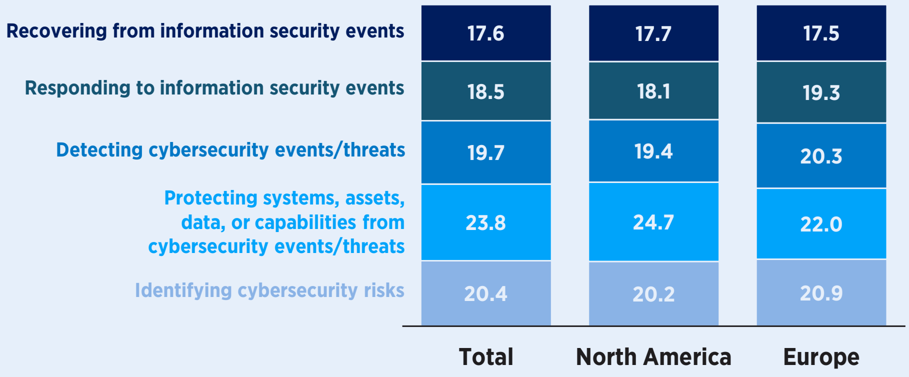
Approximately what percent of your organization's 2021 total IT budget will be (or is expected to be) for cybersecurity solutions?

(% of respondents in each category)



How is your organization's total 2021 cybersecurity budget or spending allocated (or expected to be allocated) across each of the 5 main cybersecurity categories?

(% of budget)



44% SPENT ON PROACTIVE

In 2021, respondents are allocating roughly 44% of their cybersecurity spending to the two proactive components of the NIST framework: "Identifying" (20.4%) and "Protecting" (23.8%). The remaining is allocated to reactive components, including "Detecting," "Responding" and "Recovering."

The largest spending category – protecting systems, assets, data, and capabilities – accounts for just under one-quarter of organizations' overall cybersecurity budgets. This cateory includes spending on employee cybersecurity training, developing or modifying processes and procedures, and implementing cybersecurity technology.

CYBERSECURITY RESOURCE ALLOCATION & EFFICACY INDEX Q1-2021 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 Ivanti.

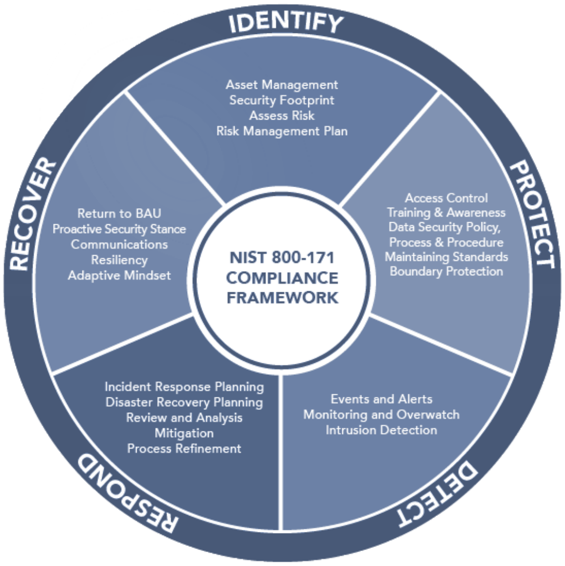
ABOUT IVANTI

The Ivanti automation platform makes every IT connection smarter and more secure across devices, infrastructure and people. From PCs and mobile devices to virtual desktop infrastructure and the data center, Ivanti discovers, manages, secures and services IT assets from cloud to edge in the everywhere enterprise—while delivering personalized employee experiences. In the everywhere enterprise, corporate data flows freely across devices and servers, empowering workers to be productive wherever and however they work. Ivanti is headquartered in Salt Lake City, Utah and has offices all over the world.

For more information, visit www.ivanti.com and follow @GoIvanti.

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