CYBERSECURITY RESOURCE ALLOCATION & EFFICACY INDEX
Q1-2021 SPOTLIGHT: NORTH AMERICA

LESSONS LEARNED: ORGANIZATIONS NOT TAKING CHANCES IN 2021

North American organizations increase investments in technology to improve their response to threats

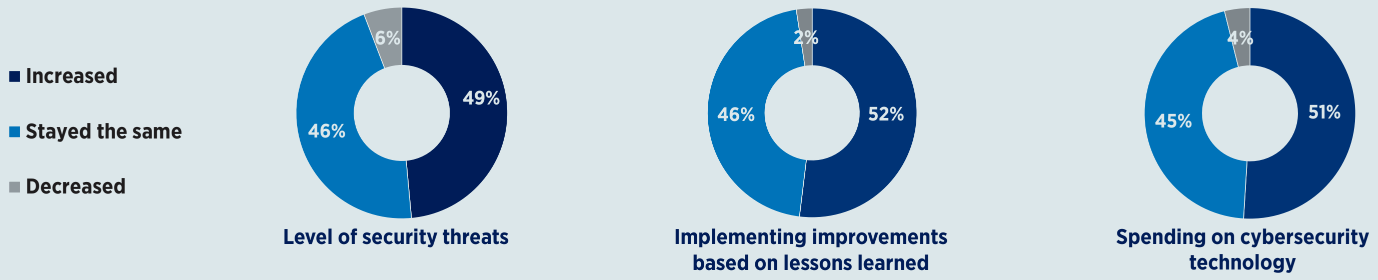
The Cybersecurity Resource Allocation and Efficacy (CRAE) Index survey revealed that nearly half (49%) of North American organizations experienced increased cybersecurity threats in Q1. Throughout the past 12 months, most, if not all, organizations have experienced some type of cybersecurity incident, and it stands to reason that 52% are now implementing improvements based on lessons learned. This includes spending on cybersecurity technology to strengthen network security, particularly in light of more devastating large-scale attacks and breaches this year. As a result, 60% of respondents believe they are more effective in responding to information security events compared to the end of last year.

> "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.)

On average, North American organizations are allocating roughly 17% of their IT budgets on security in 2021, which is slightly more than Europeans at 16%.

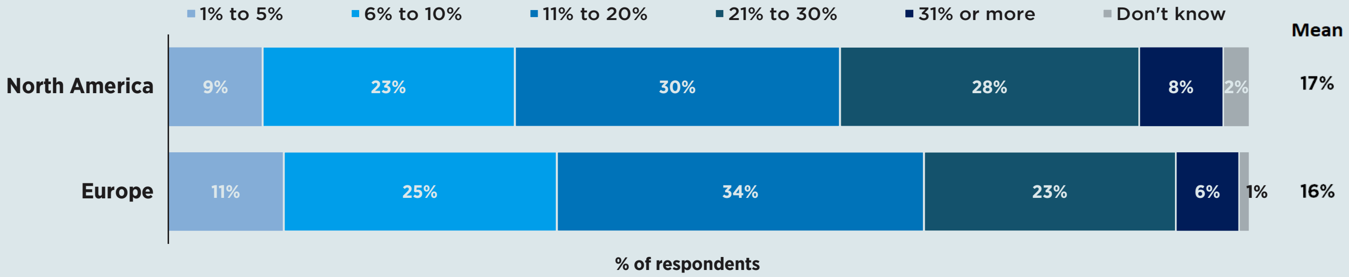
Changes in Q1 2021 vs. Q4 2020

(% of respondents)



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)



ivanti

CyberRisk Alliance | Business Intelligence Resources

CYBERSECURITY RESOURCE ALLOCATION & EFFICACY INDEX
Q1-2021 SPOTLIGHT: NORTH AMERICA

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 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.

ABOUT THE CRAE INDEX

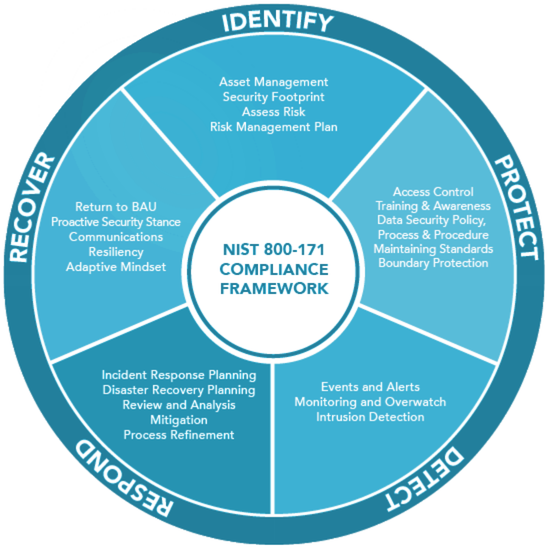
The CRAE Index is a quarterly, time-series tracker that reports the overall focus and direction of organizations' cybersecurity activities, spending, and perceived progress over time. It comprises two composite indices—Resource/Spending and Efficacy—to monitor the state of organizations' allocations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

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