QA Consultants
an ALTEN company

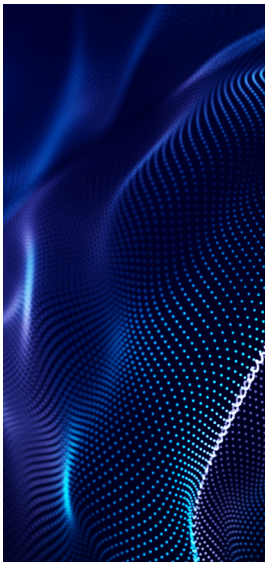
# WHY CYBERSECURITY
## IS AN ORGANIZATIONAL IMPERATIVE

# Cybersecurity remains one of the biggest topics of 2024, as well as one of the greatest barriers to organizational success.

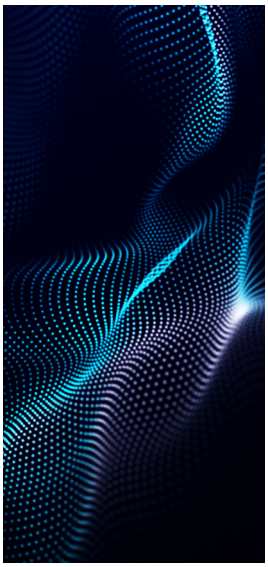
Within the past year alone, over 190 million articles and pieces of content have been published on Google alone. The cybersecurity landscape is more volatile than ever with organizations facing ever-changing threats due to an increased reliance on cloud-based services and technologies ridden with cybercriminals and hidden cyber threats. From ransomware attacks to data breaches to phishing, and now AI-powered attacks and advanced persistent threats (APTs), the frequency, sophistication, and scale of attacks are escalating at a rapid pace.

These threats – and the substantial risk at stake if and when an organization is hit by one – have organizations on edge, forcing them to consider and adopt strict cybersecurity strategies and policies, bolster cybersecurity defense infrastructure, and increase specialized staffing resources.

Meanwhile, government entities and trade organizations are grappling with the global threat, trying to implement regulations and standards to protect people, property, and security at the national level. Recently enacted regulations, including the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States, are serving as the basis for protect critical infrastructure from cybercriminals. Organizations must now realize that cyberthreats aren't a government issue or a national issue; cyberthreats are a very real threat at the organizational and even individual level. With the increasing frequency of cyberthreats and the potential for substantial financial and reputational impacts,



**with each incident costing an average of $4.88M** (Forbes Advisor, 2024),



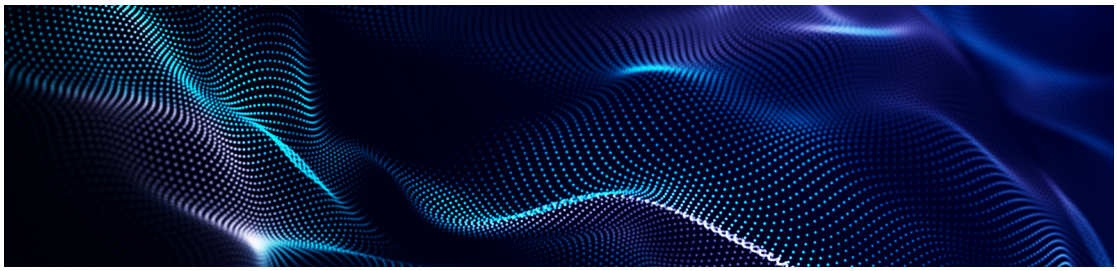
cybersecurity is now one of the top organizational priorities. In fact, Korn Ferry reports that "preparing leaders for rapid technological advances and the AI revolution," which are the foundation for cyberthreats, is the number one priority for organizations in 2025 based on its Workforce 2024 Global Insights Report (Korn Ferry, 2025).

**If cybersecurity awareness and preparation are not in the top three priorities for your organization, it should be.**

At the center of every organization's strategy should be cybersecurity. Its importance is so great that proactive cybersecurity strategies are a clear differentiator and even requirement to do business with certain entities and financial institutions. Partners, providers, investors, and even employees see cybersecurity prevention practices as a key to resilience and organizational continuity. It is so important to organizational success that it is an important component of the Environmental, Social, and Governance (ESG) framework, as "cyber risk is the most immediate and financially material sustainability risk organizations face today" (World Economic Forum, 2022). For organizations that don't take cybersecurity seriously, they will naturally be less resilient and sustainable, resulting in decreased attractiveness for investors and other stakeholders. When organizations aren't resilient against natural and man-made threats, this "has an impact on the other organizations they rely on, and ultimately on the stability of companies, communities, and governments" (Forbes Advisor, 2024). Global resilience and sustainability is, at least in part, dependant on the resilience – including cybersecure state – of each organization.

# Why is cybersecurity so important?

According to the World Economic Forum, the importance is vast. Primarily, it presents a threat to value – primarily intangible value of which the most valuable asset is data, including personal, financial, security, and behavioral (2022). Second, it presents a threat to society, as data breaches have a huge impact on citizens with an increased risk across multiple industries, including healthcare, government, financial, insurance, utilities, and consumer goods. When cyber incidents hit community-based infrastructure systems, such as utilities, these incidents result in loss of income, basic quality of life services, and strain area businesses. In May 2021, one password gave hackers access to Colonial Pipeline's system, which resulted in a disruption to fuel supplies across the southeastern United States. If Colonial Pipeline would've had a multi-factor authentication (MFA) in place, this outage could've been avoided (World, 2022).



Finally, another reason why cybersecurity is so important to organizations, nations, communities, and individuals are: insurance can't mitigate the risk indefinitely. As the likelihood of claims increase, insurers continue to narrow the cyber policy coverage scope, which limits actual coverage options available to insureds when a cyber attack happens. When an insured makes a claim for a cyber attack, this will greatly limit the insured's ability to maintain the coverage or secure other coverage in the future. Good governance must start at the organizational level. Organizations must take proactive steps to prevent cyber attacks and mitigate risk on their own.

Don't wait for a cyber incident to test your organization's resilience.

## Ready to get started?

REQUEST A APPLICATION SECURITY ASSESSMENT →

or go to qaconsultants.com/contact and fill out the form requesting our Application Security services.

Sources


CIO, "The state of cybersecurity in 2024: Key findings," October 7, 2024

ComptTIA, "State of Cybersecurity 2025," September 2024

Cybersecurity & Infrastructure Security Agency (CISA), "Cost of a Cyber Incident: Systematic Review and Cross-Validation," October 26, 2020

FBI, "What We Investigate: Major Crimes," 2024

Forbes, "Alarming Cybersecurity Stats: What You Need to Know in 2024," June 5, 2024

Forbes Advisor, "Cybersecurity Stats: Facts and Figures You Should Know," August 28, 2024

IBM, "Cost of a Data Breach Report," 2024.

Korn Ferry, "Top 5 Leadership Development Trends to Develop a Future-Forward Mindset," N.D.

National Security Agency (NSA), "Cybersecurity Information," March 2018

The White House, "Fact Sheet: 2024 Report on the Cybersecurity Posture of the United States," May 7, 2024

The White House, "Fact Sheet: Biden-Harris Administration Announces National Cybersecurity Strategy," March 2, 2023

The White House, "National Cybersecurity Strategy," March 2023

USA Today, "Cybersecurity statistics in 2024," October 4, 2024

Visual Capitalist, "The Soaring Value of Intangible Assets in the S&P 500," November 12, 2020

World Economic Forum, "Cybersecurity is an environmental, social, and governance issue. Here's why," March 1, 2022