CompTIA

State of Cybersecurity 2024

DACH

STATE OF CYBERSECURITY 2024: DACH

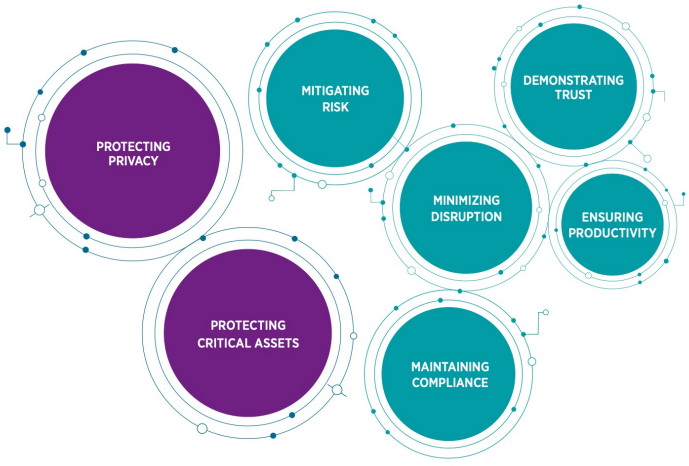
OVERVIEW

Cybersecurity is a constant balancing act. For years, the tug-of-war has been framed as a contest between security and convenience. In both business environments and the consumer space, tighter security controls often correspond with a lower degree of convenience, a tradeoff that most end users are hesitant to make. Organizations can force the issue with technology and policy, but this can open the door for risky workarounds.

Today, a new challenge is emerging. For chief information security officers (CISOs), chief information officers (CIOs) and others involved in maintaining corporate security, the conflict is not so much with convenience as it is with progress. As organizations go through digital transformation and tie technology initiatives tighter to business success, excessive cybersecurity measures can hinder overall progress. Of course, cybersecurity measures that are too relaxed can lead to serious incidents, resulting in potentially greater impacts for progress.

CompTIA's 2024 State of Cybersecurity report explores the many variables that must be considered in balancing the cybersecurity equation. As cybersecurity becomes a critical business imperative, every process must be scrutinized for potential vulnerabilities. This practice of risk analysis then drives decisions around workflow, skill-building and technology implementation. With technology trends evolving and attack patterns changing, true equilibrium is impossible to achieve. The balancing act is a full-time job.

Objectives for Cybersecurity



For proof of how difficult it is to find the right balance, look no further than the objectives behind organizational cybersecurity strategies. Six different geographic regions participated in CompTIA's 2024 State of Cybersecurity study, representing a range of economic and technical maturity. Across all six regions, the top priorities for cybersecurity strategies involve the traditional goal of protection, whether that involves protecting critical corporate assets or protecting the privacy of customer data.

Cybersecurity Changes in the Past Year

Addressing the big problem of cybersecurity requires a multi-faceted approach. Processes throughout the organization must be improved, especially those relating to incident response. Skill gaps need to shrink, whether that involves broad workforce education, dedicated cybersecurity resources, external partners or (often) a combination of all three. The toolbox has to grow, with targeted technology addressing specific activities and dashboards to pull everything together.

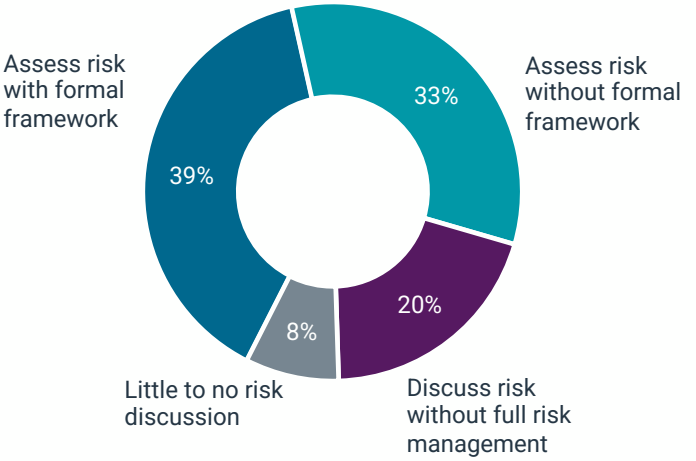
When it comes to the overall state of cybersecurity in the economy, 64% of survey respondents feel that the situation is improving. From an organizational perspective, 69% of respondents feel that their organization's cybersecurity is satisfactory, including 21% that rate things as completely satisfactory.

There is still plenty of room for improvement. In recent years, businesses have begun to consider cybersecurity as a critical function, intertwined with technology but standing on its own with metrics related to success. The next stage of maturity involves establishing and refining the operations of this standalone unit, using strategic policy and processes to drive tactical actions around personnel and products.

RISK MANAGEMENT AND PROCESS BUILDING

Over the past few years, risk management has been viewed as a component of cybersecurity, growing in importance but existing alongside other tactics as organizations built their overarching mindset. However, risk management is becoming the primary method for solving one of modern cybersecurity's greatest challenges: The connection between cybersecurity efforts and business operations.

Organizational Approaches to Risk Management



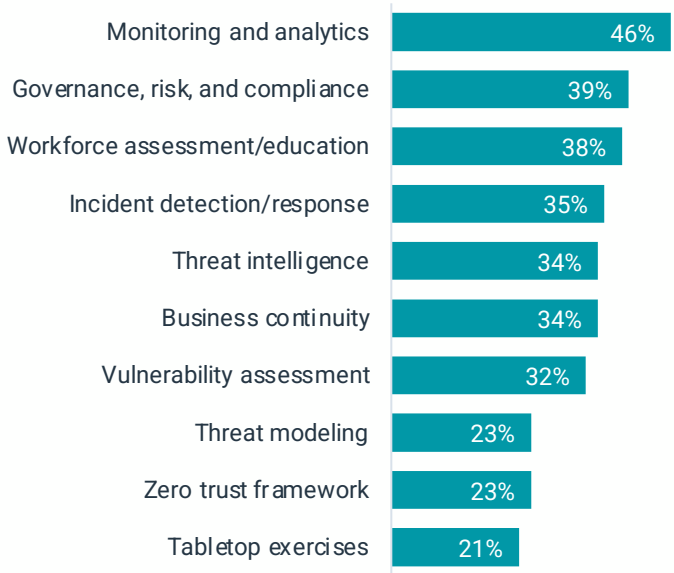
The overwhelming majority of companies in CompTIA's survey have at least some discussions around risk management. In some cases, these discussions basically serve to raise the level of awareness, possibly helping smooth over minor disagreements around cybersecurity initiatives. One third of companies take a more serious approach, assessing risks throughout the organization but not using a formal risk management framework. Nearly four in ten firms surveyed take a leading approach, using some type of formal framework to identify and manage risks and related spending.

One of the best reasons to use a formal framework is to help identify areas that may lie outside traditional IT system architecture. Among the sampling of topics presented in CompTIA's survey, there is healthy adoption across a wide range of interests. Cloud computing and mobile device usage are standard focus areas as organizations continue to adopt new architecture models, and the use of social media along with employee exit procedures provide examples where cybersecurity professionals may influence processes outside their immediate jurisdiction.

As organizations place more emphasis on the process piece of the cybersecurity puzzle, they are discovering that the influence of cybersecurity extends far beyond direct questions of security implementation. Following a comprehensive risk management discipline, both building cybersecurity processes and integrating cybersecurity into business workflows drives many functional decisions.

First and foremost, cybersecurity is becoming a primary factor when evaluating new technology. One challenge for many cybersecurity professionals, especially in the past decade, has been playing catch-up as new technology is adopted for digital transformation. The appetite for accelerating tech adoption has grown as companies seek to use technology for strategic advantage, and cybersecurity concerns have not always been top of mind when pursuing new technology initiatives.

Elements of Organizational Cybersecurity



Beyond technology implementation, other elements of cybersecurity strategy point to the impact cybersecurity is having on other business activities. For example, threat intelligence is no longer just about viruses or malware. New types of threats such as social engineering and ransomware highlight the intersection of technology systems and real-life circumstances.

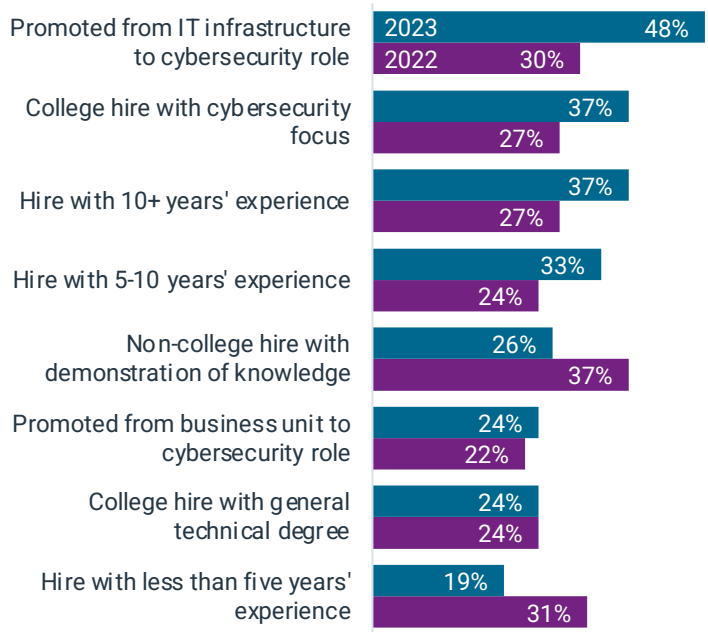
Another example is governance, risk and compliance (GRC). In the past, this specialization has largely applied within highly regulated industries. Today, the complex web of regulations governing digital business is driving every organization, regardless of size or industry, to become much more cognizant of how they conduct business.

The general intent of any cybersecurity process, whether direct or indirect, is to align with the principles of a zero trust framework. At a high level, a zero trust framework is simple to define—it means adding a layer of verification to any transaction rather than only trusting in the individual components. In practice, the details get more complicated. However, many businesses implement individual zero trust principles such as software-defined microsegmentation or multi-factor authentication without necessarily recognizing a comprehensive zero trust approach.

TALENT PIPELINES AND AI IMPACT

Organizations are clearly recognizing the importance of cybersecurity skills across their workforce. Recent years have seen a steady progression towards specialization, with companies establishing teams of dedicated cybersecurity professionals rather than relying on IT generalists with cybersecurity as just one part of the overall job description.

Pathways for Dedicated Cybersecurity Personnel

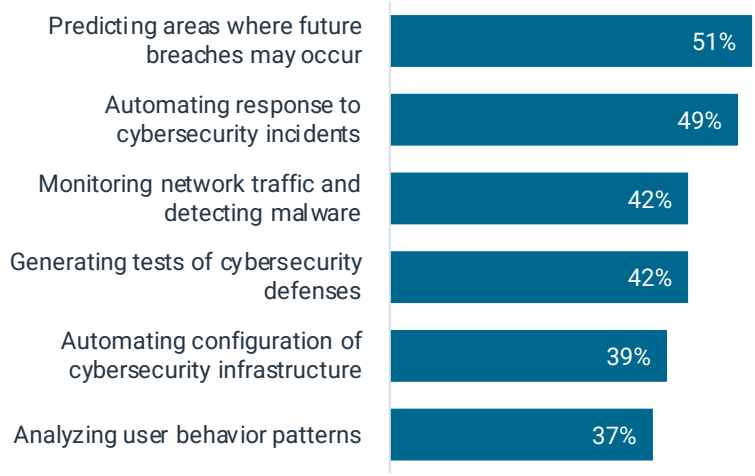


As they seek to build deep and sustainable teams, companies are turning toward methods that will bring in less experienced cybersecurity professionals who can then continue building their skills while also becoming familiar with corporate culture and objectives. The top choices for team-building options in 2023 were those options focused on current infrastructure specialists who can grow cybersecurity skills and college hires with a specialized cybersecurity focus.

As for the products these professionals have been using, the technology trend capturing the attention of both IT teams and business leaders has been generative artificial intelligence (AI). In fact, many believe that this new wave of AI, based on large language models (LLMs), is the biggest tech paradigm shift in decades. The possibilities are exciting, but as with most trends the situation is more complicated than simply delivering overnight success.

For background, generative AI should be viewed as a step forward in the general progression of AI. It may be a very significant step forward, but many companies have been building degrees of AI into their workflow for quite some time. Over one third of the organizations in CompTIA's survey (39%) indicate that they have already been working with AI and machine learning (ML), and generative AI moves that work to another level. Beyond that established group, 42% say that they have not worked with AI/ML before but that they are now seriously exploring generative AI tools, proving the enticing promise of this new technology.

Potential Uses of AI in Cybersecurity



As further emphasis of the potential, companies see a wide range of likely uses for AI in cybersecurity over the next two to three years. Many of these behaviors take place today, but they are newer additions to the cybersecurity repertoire (such as analyzing user behavior patterns rather than relying on authorized access to secure perimeters). As businesses face an uphill climb in adding new capabilities without dramatically expanding resources, they will certainly consider AI as a tool that can help handle the growing complexity.

Other potential uses are more novel. Predicting areas where breaches might occur or generating tests for cybersecurity defenses leverages the power of AI to find hidden patterns. In these cases, AI is helping break new ground, offering up solutions that are only achievable through intensive computation of large data sets and complicated mathematical modeling.

Of course, AI is like other emerging technologies: Not a standalone product by itself, but an embedded component of other products. The cybersecurity toolbox has been steadily expanding over the past few years, and now the challenge of managing a wide variety of cybersecurity tools is compounded by weaving AI capability into each one.

If there is a balancing act between ideal cybersecurity and productive business operations, achieving that balance has become a highly specialized skill. Each part of an organization owns some responsibility for cybersecurity, but only those with the proper training and expertise can bring all the pieces together for a minimal risk solution.

METHODOLOGY

ABOUT THIS REPORT

CompTIA's *State of Cybersecurity* study provides insights around key cybersecurity market trends.

The quantitative study within the DACH region consisted of an online survey fielded to technical and business professionals during July 2023. A total of 132 respondents participated in the survey, yielding an overall margin of sampling error at 95% confidence of +/- 8.7 percentage points. Sampling error is larger for subgroups of the data.

As with any survey, sampling error is only one source of possible error. While non-sampling error cannot be accurately calculated, precautionary steps were taken in all phases of the survey design, collection and processing of the data to minimize its influence.

CompTIA is responsible for all content and analysis. Any questions regarding the study should be directed to CompTIA Research and Market Intelligence staff at research@comptia.org.

CompTIA is a member of the market research industry's Insights Association and adheres to its internationally respected Code of Standards and Ethics.

ABOUT COMPTIA

The Computing Technology Industry Association (CompTIA) is a leading voice and advocate for the $5 trillion global information technology ecosystem; and the estimated 75 million industry and tech professionals who design, implement, manage, and safeguard the technology that powers the world's economy. Through education, training, certifications, philanthropy, and market research, CompTIA is the hub for advancing the tech industry and its workforce.

CompTIA is the world's leading vendor-neutral IT-certifying body with more than 3 million certifications awarded based on the passage of rigorous, performance-based exams. CompTIA's base of certified information technology professionals spans 232 countries worldwide.

CompTIA sets the standard for preparing entry-level candidates through expert-level professionals to succeed at all stages of their career in technology. Through CompTIA's philanthropic arm, CompTIA develops innovative on-ramps and career pathways to expand opportunities to populations that traditionally have been under-represented in the information technology workforce.