McKinsey & Company

Cybersecurity Practice

Securing your organization by recruiting, hiring, and retaining cybersecurity talent to reduce cyberrisk

Shed the conventional methods. Talent-to-value protection defines the most important cybersecurity roles that demonstrate the greatest reduction in risk for the enterprise.

This article is a collaborative effort by Venky Anant, Michael Glynn, Justin Greis, Nick Kosturos, Ida Kristensen, Charlie Lewis, and Leandro Santos, representing views from McKinsey's Cybersecurity Practice.

June 2022

To meet the security requirements to face evolving threats and changing technology, organizations must adapt and shift how they previously managed cybersecurity. While technical controls and capabilities still remain a priority and a commonly accepted method of securing the environment, adapting to a new approach for hiring cybersecurity talent can solve a leading concern of many leaders in a cost-optimized and risk-effective manner.

Hiring cybersecurity talent normally uses a top-down approach that fills most senior roles first before filling roles further down the organizational chart. However, because of cybersecurity worker shortages and the need to focus on specific capabilities from a talent pool—sometimes with nontraditional backgrounds—the standard hiring approach is less effective in this competitive job market.

While one answer may be to throw money at the problem and hire as many workers as possible to grow your organization over time, this approach does not necessarily lead to reduced risk. No matter what approach to resourcing companies use, the changing nature of cyberrisk means companies need to manage talent flexibly to adapt to new threats.

By preplanning and understanding the organization's cybersecurity needs holistically, it is possible to lay out a hiring road map that focuses specifically on the most critical cyber initiatives. Assessing risks, understanding priorities, and then filling those roles based on capabilities and associated skills can reduce risk and protect business value.

Apply talent to value protection

Leading organizations understand the impact and likelihood of cybersecurity and technology risks and seek to reduce those risks to enable the business. It is not just about what capabilities to prioritize, it is also about what skills are needed, if you can find those skills from within the organization, and if you need to hire or outsource.

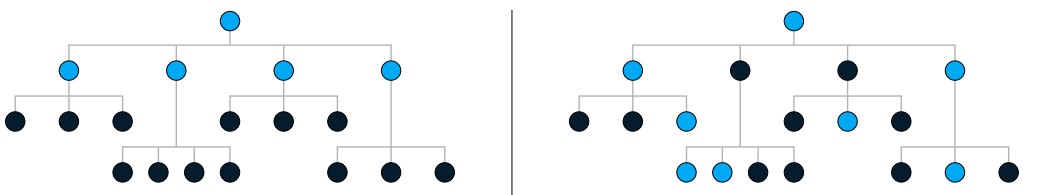
The talent-to-value-protection approach defines the most important roles that show a maximum reduction in risk or create the greatest amount of security value (Exhibit 1). Priority roles should be filled with the right skills to eliminate risk as soon as possible, utilizing all resources, capabilities, and recruiting efforts.

As a case in point, an organization undergoing a cyber transformation sought to fill more than 150 roles across all capabilities. After applying the talent-to-value-protection approach, the company's leaders prioritized hiring based on

Exhibit 1

Talent-to-value protection allows organizations to reduce cybersecurity risk with fewer employees and resources.

Comparison of approaches for security talent management



Traditional security talent management aligns the most experienced personnel with the highest responsibility or span of control; the most important roles are defined by hierarchy

Talent-to-value protection defines the most important roles as those that reduce the maximum amount of risk; this approach allows for ~50% fewer new hires for equivalent risk reduction

critical business risks and what knowledge and skills were required first to secure the business.

Using talent-to-value protection allows you to move in the right direction and reduce risk through focused hiring and talent development. The strategy helps identify which skills and associated roles are the highest priority to reduce cybersecurity risk—or, in other words, which can demonstrate the most "return on risk investment." It allows you to hire the right person at the right time—ensuring that personnel spending is aligned with where it should be based on growth aspirations.

Understanding where to focus recruiting efforts is important, as the global dearth of qualified security personnel available to hire requires creative approaches to finding talent.

Shortage of cybersecurity workers

There is a global shortage of 2.72 million skilled cybersecurity workers, according to the 2021 Cybersecurity Workforce Study by the International Information System Security Certification Consortium, or (ISC)^2. Cybersecurity professionals said in the study that the workforce gap remains the number-one barrier to meeting their organizations' security needs. Sixty percent of respondents report that a cybersecurity staffing shortage is placing their organizations at risk. The consequences of cybersecurity staff shortages are real and create challenges for organizational success (Exhibit 2).

Depending on your type of organization, talent-to-value protection can work in a few different ways:

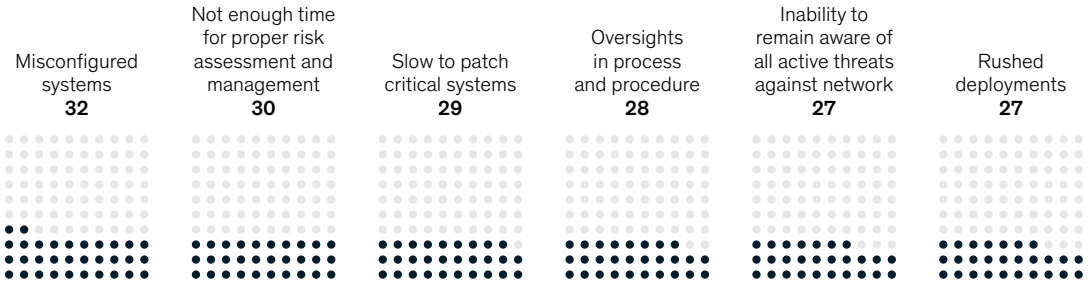
1. *Early-stage cybersecurity organizations.* For organizations just beginning their security journeys, the first focus is getting key players in place and setting up program management capabilities. This approach focuses on executing strategic initiatives and improvement activities in parallel; it fills management roles proactively and overweighs the importance of leaders (for example, managers and directors) to manage controls and operate capabilities.

2. *Steady-state organizations.* For organizations with well-established cybersecurity capabilities, the main priority is to make continued improvements to protect against emerging risks. This approach focuses on targeted improvement opportunities; it emphasizes high-impact experts or key frontline employees and places

Exhibit 2

Cybersecurity staffing shortages can create real challenges within an organization.

Share of cybersecurity leaders reporting impact due to insufficient cybersecurity staffing, %



Source: *(ICS)^2 Cybersecurity Workforce Study, 2021*, (ISC)^2, 2021 (n = 4,750)

The first priority is to understand what capabilities directly impact the systems and processes that drive business value: the crown jewels.

less weight on managers and directors because of the existing leadership structure.

3. *Transforming organizations.* Companies undergoing transformations prioritize new hires and skills against where the new risk will be or to protect the most valued part of the new business. This approach prioritizes new hires to safeguard the value gained from a business transformation, finding new talent or new skills to reduce potential risk.

Protect the crown jewels

The first priority is to understand what capabilities directly impact the systems and processes that drive business value: the crown jewels. The crown jewels are the assets, the data, and the applications that are most critical to business value and operations. Implementing a risk-based approach to protecting these assets requires mapping required controls and selecting the right people to implement them. Organizations can use existing frameworks, such as the National Initiative for Cybersecurity Education (NICE) led by the National Institute of Standards and Technology (NIST), to focus the organization on the types of skills needed for priority controls. This self-examination helps identify personnel who can be upskilled or determine when new hires are needed.

For example, a large Latin American oil and gas company reprioritized its cybersecurity spending, capability development, and leadership after analyzing its crown jewels. The organization identified what mattered most and clearly defined the most critical risks. This crown jewel identification effort helped provide an understanding of the most critical talent needs and allowed the organization to build a targeted recruitment campaign to build its team's capabilities.

As organizations across all industries race to defend their business value, it is critical that they accelerate to close gaps on controls to reduce risk and stay ahead of evolving attackers. According to a 2021 McKinsey survey, only 10 percent of organizations were found to be approaching advanced cybersecurity functions, while 20 percent surpassed mature cybersecurity, which left 70 percent yet to fully advance to a mature approach—further highlighting the need to prioritize for risk-reducing activities that focus on value protection first (Exhibit 3).[1]

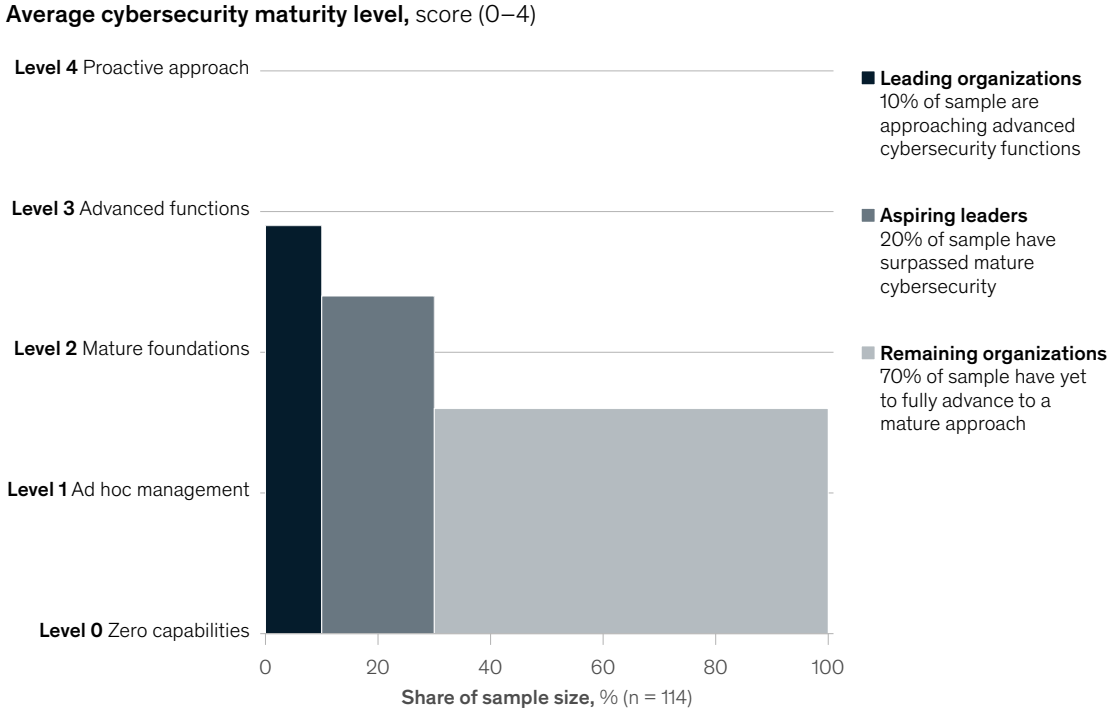
Hiring based on assumptions

Less mature organizations often assume they must hire based on cyber roles, regardless of the specific risks they face. Talent-to-value protection focuses on hiring or training the right personnel

[1] "Organizational cyber maturity: A survey of industries," McKinsey, August 4, 2021.

Exhibit 3

Most companies have yet to reach the advanced levels of cybersecurity maturity demanded by today's business environment.



at the right time, bringing risk in line with the risk appetite of the organization.

Too often, chief information security officers (CISOs), chief information officers (CIOs), and vice presidents of security are inundated by the daily firestorm of cyber activity. Using talent-to-value protection helps leaders gain clarity on where to apply resources to best reduce risk. Instead, leaders can focus on laying out a road map to identify the top security priorities and pair talent against them. Leaders can progressively reduce risk in key areas rather than attempting to mitigate it all at once.

A three-step approach to implementing talent-to-value protection

This approach requires a collaborative effort to understand and communicate what the risk is, what will reduce that risk, and who will be needed to reduce that risk. Organizations can use a three-step approach to adopt a talent-to-value-protection framework. First, identify the most important cybersecurity activities based on the needs of the organization and most pressing risks that must be mitigated. Second, define the most important roles that lead to maximum risk reduction. Third, build job descriptions for the priority roles and determine whether upskilling or hiring is the best option for each position.

Step 1: Identifying prioritized activities. Through risk modeling and assigning scores to potential vulnerabilities based on risk, talent-to-value protection makes it possible to create a list of activities to identify top priorities needed to execute on the security strategy. Each organization assigns scores differently—but all should work to

assess risk based on the business or operational impact. Risk scores combine the likelihood and intent of an attacker to act and how vulnerable the organization is to that particular risk. For example, a technology organization realized after risk modeling that cloud compromise was one of its top cyberrisks, requiring the company to prioritize activities that brought down the most risk, including implementing cloud security controls over on-premises ones. Through this identification, it then became possible to match activities with roles needed to hire, which required upskilling, and which should be outsourced.

Step 2: Defining priority roles. The next step would be to define and prioritize security roles needed to fulfill the top risk-based priorities. For the organization mentioned above, it became a priority to fill cloud security roles to execute the activities necessary to implement the most critical cloud controls. Once priority roles are defined, it is possible to create the job descriptions of what the company needs in each role.

Step 3: Building job descriptions and determining to upskill or hire. The final step is to determine if the priority role should be filled by upskilling existing employees or hiring new talent. One way to do this is to develop a job and role architecture that is linked to the organization's security services catalog. Security service catalogs can be built around functional groups like cybersecurity operations, governance, engineering, and service groupings like cloud security or data governance. The job and role architecture organizes jobs into families, functions, positions, and roles. Roles can end up assigned a category and specialty area sourced from well-known frameworks like NIST/NICE.

Each job description for the priority roles should be described in detail: first, by building a high-level summary of tasks, skills, and background for the person who will fill the role; second, by writing role details; third, by identifying the tasks, knowledge, skills, and abilities relevant to the role.

When the job descriptions for the priority roles are complete, leaders can analyze who in their current cybersecurity team could fit well in those roles. In some cases, it is faster and less expensive to upskill that team member through training. Sometimes, upskilling is not feasible. In that case, leaders can use the detailed job description to jump-start the hiring search—with high confidence in the type of individual they need to recruit. For one technology company, building and filling a variety of cloud-security-engineer job descriptions was a priority. The company quickly recognized a need to hire additional cloud security roles after analyzing the team's knowledge and skills using NIST/NICE frameworks and seeing a gap in the ability to reduce key risks.

In-house or outsource

Even with this approach, building an in-house, organization-specific cybersecurity team may not be feasible due to available talent, resourcing, or another reason. Sometimes it makes sense to outsource talent to accelerate implementation and scale security support faster. For example, while undergoing a large-scale cyber transformation, an oil producer prioritized outsourcing security operations given its geography and the skills that existed on the security team, thereby reducing risk.

The CISO, who had a strong cybersecurity background, built a lean team of several program managers with a general understanding of cybersecurity. Outside of this small team, all other cybersecurity functions were outsourced. By understanding what the organization needed and where to hire talent versus purchase services, the company was able to hit its cybersecurity maturity targets by its deadlines and grow its operational-technology security to new levels.

Template to success

Talent-to-value protection creates a template for the roles and the needs of an organization where companies can start to create a plan on how to

attract, retain, and train talent and find the gaps within their security programs and talent pool. It helps prioritize who the organization needs to target for recruiting and how to focus on retaining the most critical personnel. It helps identify new cybersecurity requirements—helping determine whether those needs can be met by upskilling employees. If the organization cannot upskill its teammates, it then can go hire.

Talent-to-value protection helps the company understand what it needs, who it needs to hire, and when. Leaders learn the job specifications and the jobs they have to hire for, which allows them to say, "I don't need a cloud security manager; instead, I need cloud security architects with experience shifting workloads to the cloud."

In this era of a lack of qualified security personnel, talent-to-value protection allows organizations to be more strategic about their hiring. By tying this into the risk-based approach, an organization will have a prioritized list of roles to hire to build a secure enterprise.

Venky Anant is a partner in McKinsey's Bay Area office; **Michael Glynn** is a consultant in the Washington, DC, office; **Justin Greis** is a partner in the Chicago office; **Nick Kosturos** is an expert in the New York office, where **Ida Kristensen** is a senior partner; **Charlie Lewis** is an associate partner in the Stamford office; and **Leandro Santos** is a senior partner in the Atlanta office.

Designed by McKinsey Global Publishing