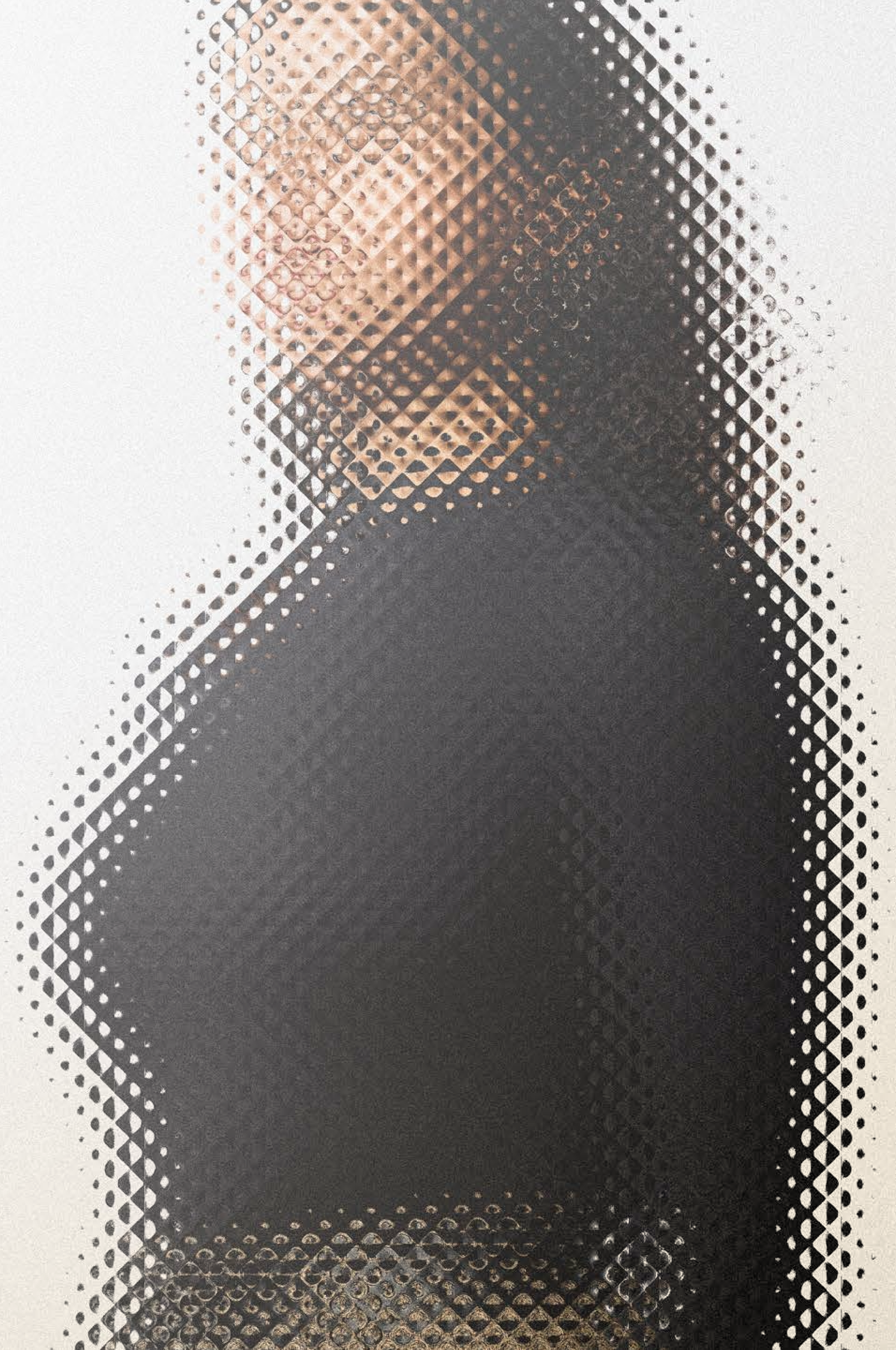
Cybersecurity Talent Management Playbook



Toronto Metropolitan University

ROGERS cybersecure catalyst

Contents

Acknowledgments

Rogers Cybersecure Catalyst (“the Catalyst”) would like to acknowledge the efforts of the primary author, Randy Purse, CD PhD and CTDP and the Catalyst team who created the Cybersecurity Talent Management Playbook.

Also, we could not have completed this initiative without the active participation and contributing insights from our Advisory Council:

Adam Evans
Senior Vice President & CISO, RBC

Charlotte Johnston
Principal for Cloud DevOps and Security at Slalom Consulting Inc

Daphne Lucas
Partner at Deloitte Canada

Ciaran Luttrell
Director of Service Operations EMEA, eSentire

Sundeep Sandhu
Vice President, Cyber Security, Rogers Communications

Lisa Tetrault
Global Vice President, Global Security Operations, Arctic Wolf

John Tziortzis
Associate Vice President, Information Technology and Chief Information Security Officer at Centennial College

Rob Watson
Vice President, Security Services, eSentire

Finally, a big thank you goes out to the many organizations and their HR teams and Hiring Managers who participated in the four workshops that helped verify and elaborate on the content included in this playbook.

The participating organizations include:

Rogers
CIBC
Air Canada
Loblaws
Deloitte
Gore Mutual
eSentire
Digital Boundary
ISA Cybersecurity
HCL Tech
ORION
RSM- Canada
BCLC
BDO
RBC
Canarie
CDW
Centennial College
Control Gap
Difenda
Ontario Health

Preface

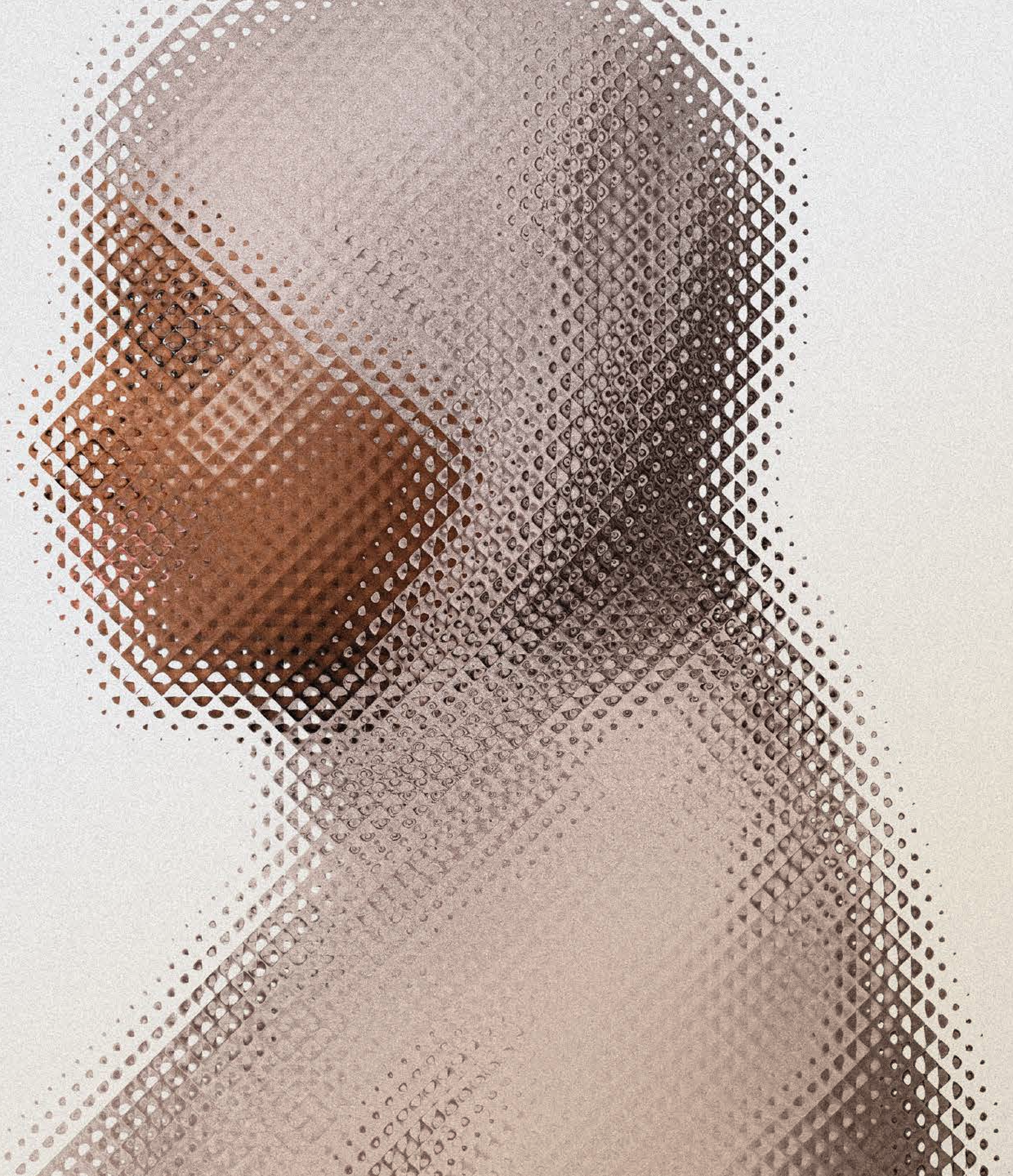
Canada continues to face a cybersecurity talent shortage that poses a significant threat if left unchecked.

Our cyber talent shortage impacts the organizations that depend on cybersecurity talent to protect and sustain their businesses and industries. But the shortage also impacts all levels of the economy as Canada expands its investment in the digital economy and accelerates efforts to connect every Canadian to it.

If our cyber talent shortage continues – alongside other issues plaguing cybersecurity talent generation – the shortage will become acute and create significant organizational risks. These risks will impact whole communities, sectors, regions, and our nation.

Our Cybersecurity Talent Management Playbook transforms the challenges associated with Canada's talent shortage from the abstract into concrete actions by offering best practices for finding, attracting, hiring, and retaining cybersecurity talent. The Playbook gathers expert insights from industry, academia and government and acts as a guide to help organizations deal with their immediate cybersecurity staffing issues. And the insights shared can also guide collaboration between regions and sectors to establish an effective and sustainable cybersecurity talent pipeline to address local, regional and national needs.

Introduction



Introduction

Purpose

The Cybersecurity Talent Management Playbook intends to:

- Help organizations better identify and manage cybersecurity talent by introducing best practices and demonstrating how organizations can adapt these practices to any organizational context.
- Give a roadmap to identify common needs and facilitate collaborative solutions to address community, regional and sectoral cybersecurity talent requirements.

Why?

Organizations across all sectors need help finding and retaining cybersecurity talent.

The continuing lack of cybersecurity talent translates into operational, legal, financial, reputational, and even strategic risk for Canadian organizations, impacting public safety, critical infrastructure security and the economy.

This Playbook strives to help organizations tackle their immediate cyber talent challenge. In doing so, it also seeks to streamline greater cyber talent generation and create more cybersecurity workforce stability to increase public safety, security and economic prosperity within the digital economy on a national level.

Strategic Outcomes

The Playbook will guide activities toward the following strategic outcomes:

- Generate successful cyber talent development strategies and processes, which organizations or institutions can define and measure.
- Establish a collaborative leadership team to create and sustain a national cybersecurity talent pipeline.
- Create a demand-driven Canadian cybersecurity talent pipeline that is responsive to dynamic sector and industry needs.
- Give cybersecurity employers access to a network, required tools and talent management best practices that they can use and/or adapt to address their organizational needs.

Playbook Structure

We created the Playbook as a practical guide for human resource professionals, hiring managers, and other organizational roles related to any part of the cybersecurity talent management lifecycle.

We focus our discussion on five areas in cybersecurity talent management:

1. **Finding and Attracting Talent**
2. **Recruitment and Onboarding**
3. **Developing Talent**
4. **Compensation and Recognition**
5. **Talent Retention and Career Transitions**

In each focus area, we identify specific challenges associated with that stage of talent management and give best practices that organizations can implement at scale to solve their talent management issue. Each focus area also includes a section titled Community-level Activities. These sections cover common issues and collaborative solutions that the cybersecurity community, an organization's community or an entire sector can apply to resolve broader cybersecurity talent challenges.

We close the Playbook by sharing regional and sectoral stakeholders' insights into developing a local cybersecurity talent pipeline management strategy.

For any contextual information like the factors that drive our cyber talent shortage, cybersecurity roles and understanding cybersecurity as a field of work, or alternative options to traditional cyber talent pools to recruit from, please refer to the Appendix.

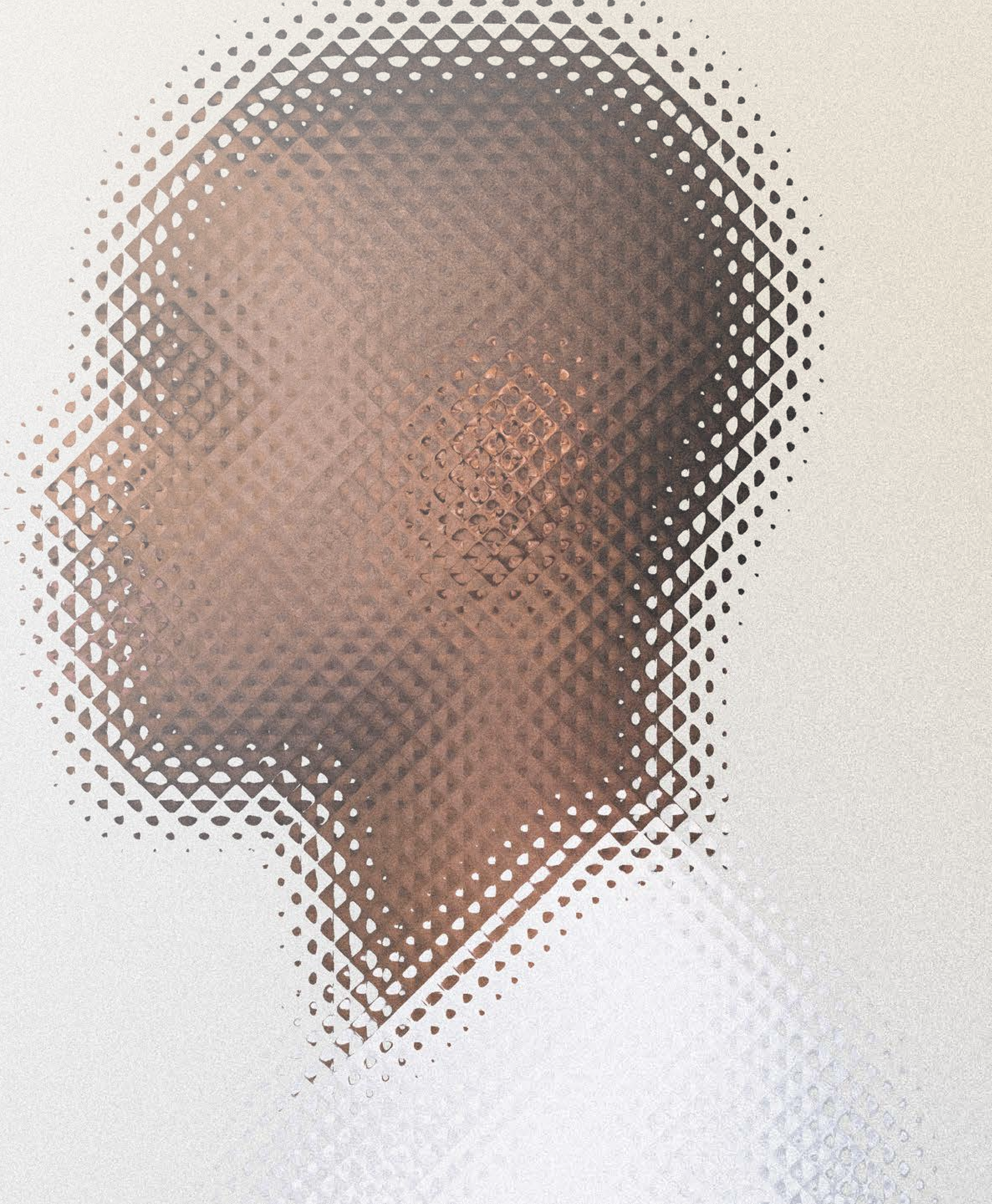
Finding and Attracting

For the Playbook, we've bundled the stages of finding and attracting since they are complementary activities with similar goals: identifying and drawing people into the field from diverse talent pools.

Definitions:

Finding: seeking out and identifying desired talent pools and prospective candidates.

Attracting: actively engaging prospective candidates and enticing them to consider cybersecurity as a profession and your organization as an employer.



Finding Talent

> *You need to know what you're looking for; then, you'll understand where to look.*

The Problem

Labour market data shows we are experiencing low unemployment in a competitive landscape. That means finding talent is difficult. But organizations have an even harder time finding cyber talent due to inaccurate and inconsistent cybersecurity job postings.

For example, you can find a range of experience requirements by looking at job postings for entry-level cybersecurity operations analysts. Some demand a certification that requires a minimum of five years of experience in the field. Others ask for anything from a couple of years of experience with a basic credential to very advanced technical expertise and numerous years of experience.

The Digital Governance Council developed the Cybersecurity National Occupational Standard (NOS) to form a common understanding of the field and provide a lexicon around cybersecurity work. At the time of the Playbook's publication, the Digital Governance Council has yet to publish the NOS. So, we don't yet know how effective it will be. But given that the Cybersecurity NOS is based on the U.S. Workforce Framework (which already has good visibility within the cybersecurity community), the hope is that a Canadian version will have the same appeal within our country's cybersecurity community.

In the meantime, employer job postings are the best indicator of Canada's cyber talent need.

We've noted several commonplace approaches to defining and documenting organizational talent needs:

- The cut-and-paste approach is where organizations seek out a type of talent because that is what everyone else is asking for. Organizations cut and paste other job descriptions, assuming it is close enough to what they need. Unfortunately, if organizations ask for what others are asking for, they will not likely get what they actually need.
- The everything and the kitchen sink approach creates a laundry list of everything the organization might like in a cybersecurity professional. (Organizations often create these lists from several different sources.) But this approach has no semblance of a practical scope of work, so it does not accurately depict the type of experience needed. Organizations may use this approach when they need a generalist (e.g., for a corporate security officer) but expect the generalist to have specialist-level knowledge. Needing a generalist versus a specialist are two distinct requirements. The organization should identify which of the two is most appropriate based on its need.
- The expert expectations approach relies on experts defining the job requirements that mirror their own. The approach is reasonable if the organization needs to fill an expert's role. But if an organization uses this approach to fill other positions, it sets higher-than-needed expectations.
- The bring 'em in and train 'em approach is a reasonable and often rewarding approach that lowers the bar to entry, providing that the candidate can learn and do the job with limited training. But a problem exists in this approach that is two-fold. First, this approach increases the dependence on the screening and selection processes that will identify talent potential as opposed to concrete evidence of capability. And second, organizations need a good understanding of what the cyber roles entail and must have sufficient capacity to support the learners' needs as they prepare for the roles. But most organizations are not prepared for either, based on our research and observations.

- The let's go with what we have approach is when an organization uses an existing job or position description that may capture the gist of the job but doesn't reflect the actual job requirements. The primary problem with this approach is that organizations get what they ask for – which might differ from what they actually need. For example, if an organization uses a previous job description for a cybersecurity operations analyst but truly requires an incident handler, it will not get what it needs.

These are just some commonplace approaches that impact an organization's ability to find and attract the appropriate talent. These job posting approaches also make the market data less reliable and create confusion around cybersecurity as a field of work.

Defining the Talent Need

The first step to identifying talent needs is explicitly confirming those needs. For example, hiring more people may not address an organization's problem.

An organizational needs assessment can help organizations determine if it is genuinely cybersecurity talent they're looking for. The following questions can help if a needs assessment isn't available:

- Is human intervention the only way to close the performance gap?
- Is cybersecurity talent needed (e.g., cybersecurity tasks would consume much of their work)? Or are tasks needed that others could perform in the organization?
- Is there a different way to allocate or segment the work that would reduce the need for a cybersecurity professional? (e.g., Can the IT team or service set up and monitor the perimeter defence?)
- What other capabilities is this role expected to perform?
- How many cybersecurity people do we need, and in what roles?

Accurately defining the need at the organizational level ensures that the organization gets the appropriate talent and works to create more valid labour market data that helps define the local and national employment picture.

An organization should conduct a job or competency analysis before creating a cybersecurity job description. (We give an example in Figure 1.) If you already have the results of such an analysis or can conduct one, that's great. However, you may want to validate the results with experts in the cybersecurity community, as these results will form the basis for your job description.

Note that the job description is not the same as a job posting.

The job description is the primary source of information for the job posting. So that's why the job description must be accurate and transparent. The job description documents the job requirements and, in many cases, should be defensible. The organization can use it to validate compliance requirements, adherence to collective agreements, and other requirements.

Job postings often include organizational elements that can help candidates self-select for fit. The job posting should include branding, culture, financial and non-monetary benefits, etc.

The job description is the primary source of information for the job posting. So that's why the job description must be accurate and transparent.

Figure 1: Example Job Description Template

Job Title:

Reports to:

Works with:

Tools, technology, people (teams, colleagues, etc.)

Overview of job:

Primary duties and responsibilities:

Including cross-functional responsibilities such as communications, intra-team interactions, etc.

Key work tasks:

Qualifications:

Education and training; Experience, Certifications, credentials or Specific skills (if required); Other competencies, including needed or desired psycho-emotional (e.g., ability to work under stress, attention to detail, team player) and physical attributes that relate to work performance (e.g., visual acuity)

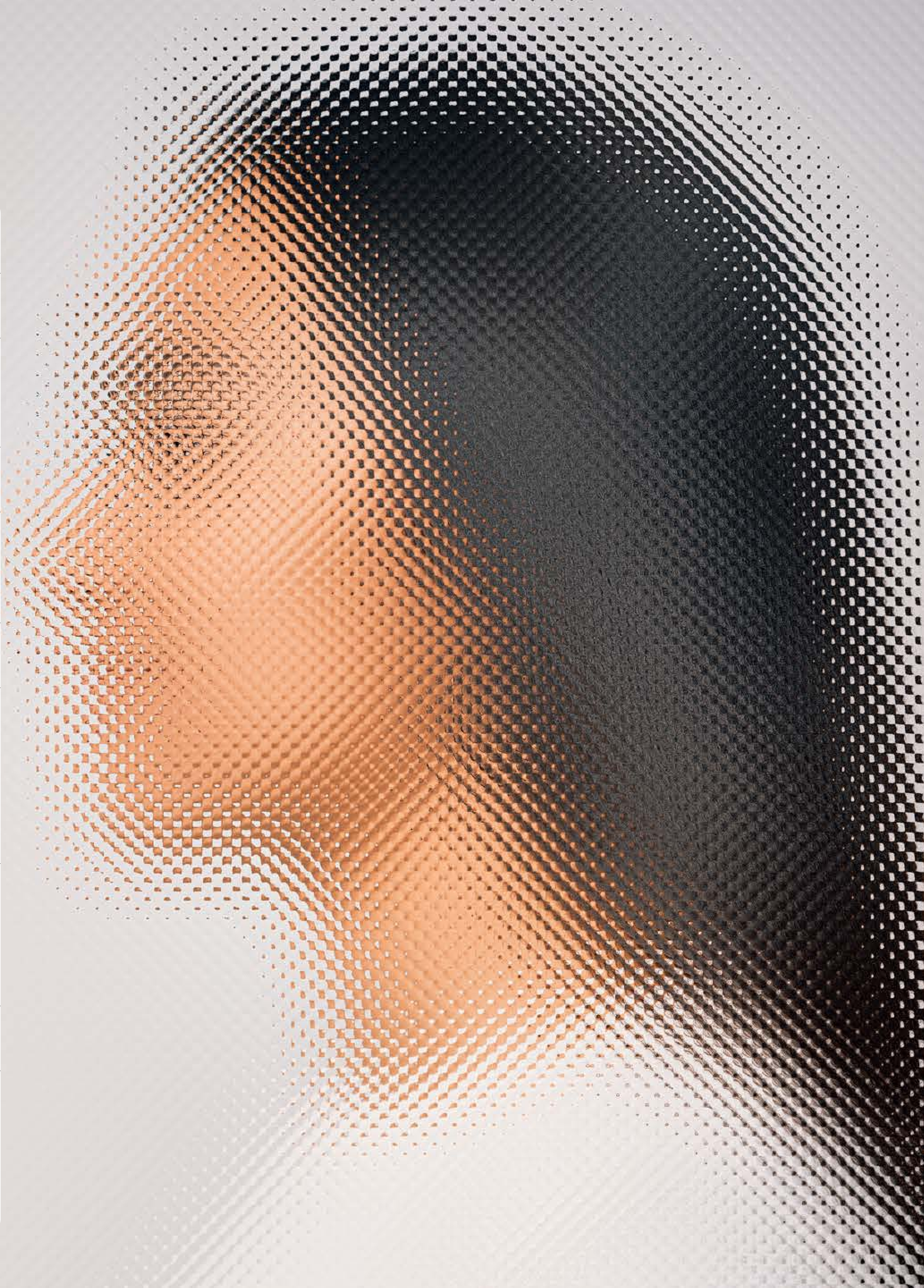
Work environment:

Physical conditions and expectations; Psychological and/or mental conditions and expectations; Work period and duration; Social conditions (e.g., team, independent, etc.)

Salary or salary range:

Other stipulations:

Union membership if required; Other occasional roles and/or responsibilities outside of the typical role requirements



There are relatively simple ways to capture the needed information if you don't have the benefit of a job or competency analysis. For example, conducting interviews or focus groups with employees in the roles and their supervisors can give the most valid descriptions of their tasks. (Note that this information may not reflect what tasks the role should be responsible for.)

Organizations can draw questions from the job description to help prime the job interview. But they can also develop a persona and performance analysis to help guide talent need decisions.

Persona Development

Developing a persona is a relatively low-investment approach gaining traction in the human resources (HR) community – first used in user-centred design (Figure 2). A persona is a hypothesized representation of a person or group in a similar role.

HR or workforce development professionals often construct personas with data from focus groups, interviews, or surveys conducted with those most familiar with the job requirements. Experts, hiring managers, and HR professionals can develop personas independently but often collaborate to create them.

You should answer several questions as you develop the persona to help you define the type of candidate you are looking for and capture expectations beyond specific work tasks. Personas will better inform your job description when you don't have any recent job analysis.

Figure 2: Persona Development

Who are we looking for?

Persona development and prioritization of qualities/capabilities.

Roles or job title(s)

Key responsibilities / tasks

Cross-functional competencies

Demographics / background

Work orientation

Work preferences

Perspective on security work and learning

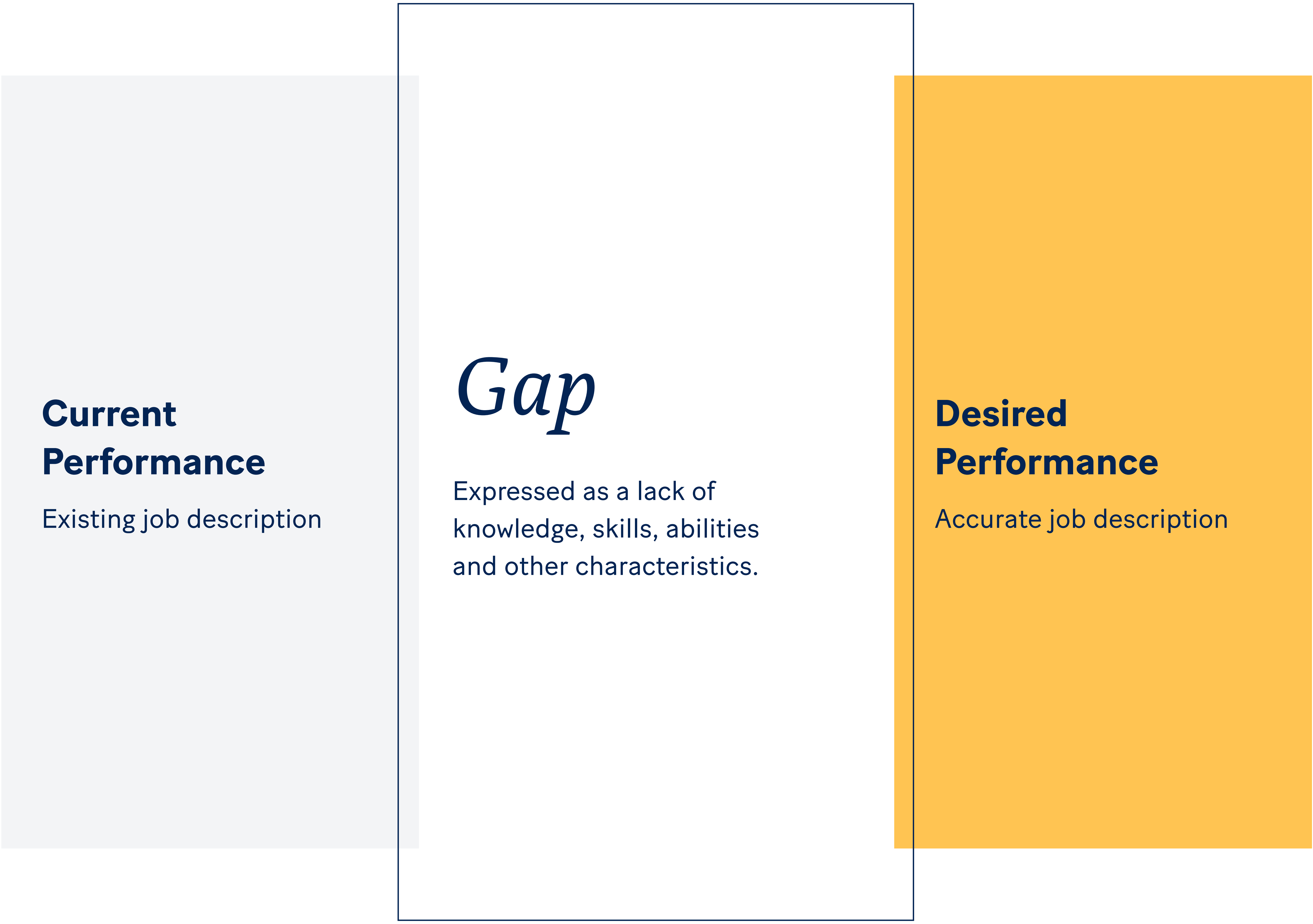
Other expectations

Performance Gap Analysis

Organizations or workforce development stakeholders can easily guide a performance gap analysis using current employees.

A performance gap analysis (Figure 3) requires you to identify the desired state of the role and compare it to the existing or current state of performance to define the gap. Analyzing the gap allows you to take the existing job description and add the missing elements from your analysis to develop a job description that meets expectations.

Figure 3: A Performance Gap Analysis



Quick Check:
Defining talent needs

- ☑ We've concretely defined the cybersecurity capabilities we need.
- ☑ We've identified the type of talent needed to support our organizational cybersecurity goals.
- ☑ We have validated that the role is cybersecurity (not an adjacent role with some cybersecurity requirements).
- ☑ We have developed an accurate job description, including technical and non-technical competencies needed to perform the role.
- ☑ We know how many people we need to fill our cybersecurity roles.

Finding Talent Pools

Once we've defined our cyber talent needs, we're in a better position to identify the kinds of candidates we are looking for. But to find that talent, we should consider a range of traditional and alternative approaches to finding candidates, given Canada's significant cyber talent shortage.

The Catalyst found that the cybersecurity community predominantly relies on two approaches to finding talent. The first is personal referrals. The second is hiring a staffing or recruiting service. These two approaches are reliable ways to identify prospective candidates, but each has limitations.

Personal referrals: Personal referrals have many advantages, including the potential for character insights that are generally unavailable through other means. We want cyber candidates we can rely on to do the work and demonstrate integrity, resilience and trustworthiness. Personal referrals usually give organizations more confidence that the referral has the skills and character traits they're looking for. Personal referrals also often work in favour of the candidate, as the candidate's relationship helps to 'grease the wheel' with the organization. However, personal referrals tend to limit the recruiting pool and can result in a more homogenous workforce. In some cases, referrals may cause the organization to go against its best interests by poaching talent from other organizations.

Hiring staffing and recruiting organizations: These types of services can be tremendously advantageous, particularly for those organizations that do not have the HR expertise or ability to advertise, collect, vet and initially engage with a range of potential candidates. Organizations contract these services with the hope that they will sufficiently understand the organization's needs and only deliver suitable candidates. But these types of services can be costly. And these services can also cast a wide net to get as many 'hits' as possible. Using these services can result in more false positive applicants who don't meet your organization's needs. Further, these services often do not target specific cyber talent pools you may be interested in drawing from.

Finding talent is finding the human capability needed to perform required organizational functions. Organizations can find human capability across many alternative and traditional talent pools, like technical education graduates and the cybersecurity workforce. Still, we need to be more creative about how we assess talent and where we look to find it.

We want cyber candidates we can rely on to do the work and demonstrate integrity, resilience and trustworthiness.

Sources of Talent

Internal talent: One of the most overlooked areas for talent is your existing workforce. You may have employees who could build on the skills they possess with minimal training and development to meet your needs. Upskilling existing talent is particularly helpful if you're a smaller organization that doesn't need a dedicated cybersecurity team.

High school graduates: These graduates may not have the experience, but many demonstrate significant enthusiasm and are looking for opportunities to perform and do well.

New Canadians: Many organizations have job-seeking assistance programs to attract new Canadians specifically. However, these programs often don't have the insights needed to determine if candidates are suited for cybersecurity work.

Mid-career job seekers: Many mid-career professionals are looking to explore new opportunities. Often, these professionals take less time to reach competency in a cybersecurity role because they bring valuable skills and experiences from their past work history.

Serving or retired military, law enforcement or other similar roles: These professionals tend to have related skills and abilities for cybersecurity work that are not typically found elsewhere, including a pre-disposition to the security mindset.

Community and other representative groups: There are thousands of community or representative groups across Canada that can help develop talent by fostering individual learning, development and success in cybersecurity. Hiring from these groups can also help your organization secure diverse talent for your cybersecurity team. These community groups are often an untapped talent source with a high cybersecurity potential. However, these groups are typically uninformed about what we are looking for in cybersecurity candidates. Therefore, they may think only people with technical diplomas or degrees are suitable for a cyber role.

Apprenticeships, internships, co-op or work-integrated learning program participants: Our research found that many co-op students have not yet chosen a career track. Looking to these types of programs can help students find the cybersecurity careers they didn't even know they were looking for. Also, consider students from outside of technical education programs as they may have talents that the organization needs.

Post-secondary institutions: Post-secondary institutions will continue to produce graduates from technical and non-technical programs that will feed cybersecurity needs. There are also improved short-cycle, continuing education and certificate programs that may deliver on talent needs, including opportunities to help internal talent move into a cybersecurity role.

Temporary help services and consultancies: You may only need to fill a short-term requirement or temporarily supplement your cybersecurity team. There are a variety of HR, talent and contracted services that you can use to fill this need.

Sharing or partnerships: Fractional, part-time or contracted employees are reliable sources of talent that often go untapped. You can work with other suppliers or partners to borrow or rent their talent to address immediate or emerging cybersecurity program needs.

Service providers: IT, cloud and cybersecurity providers often have cybersecurity staff that could give various services to support your organizational goals. This approach is tremendously beneficial if you have ongoing cybersecurity needs you can't meet due to a lack of expertise, people, processes or technology.

Automated processes: Automation's role in cybersecurity is increasing. If you're struggling to find talent who can perform standard cybersecurity functions, there may already be automated tools that can do much of the work.

Consider Organizational Fit in Your Search

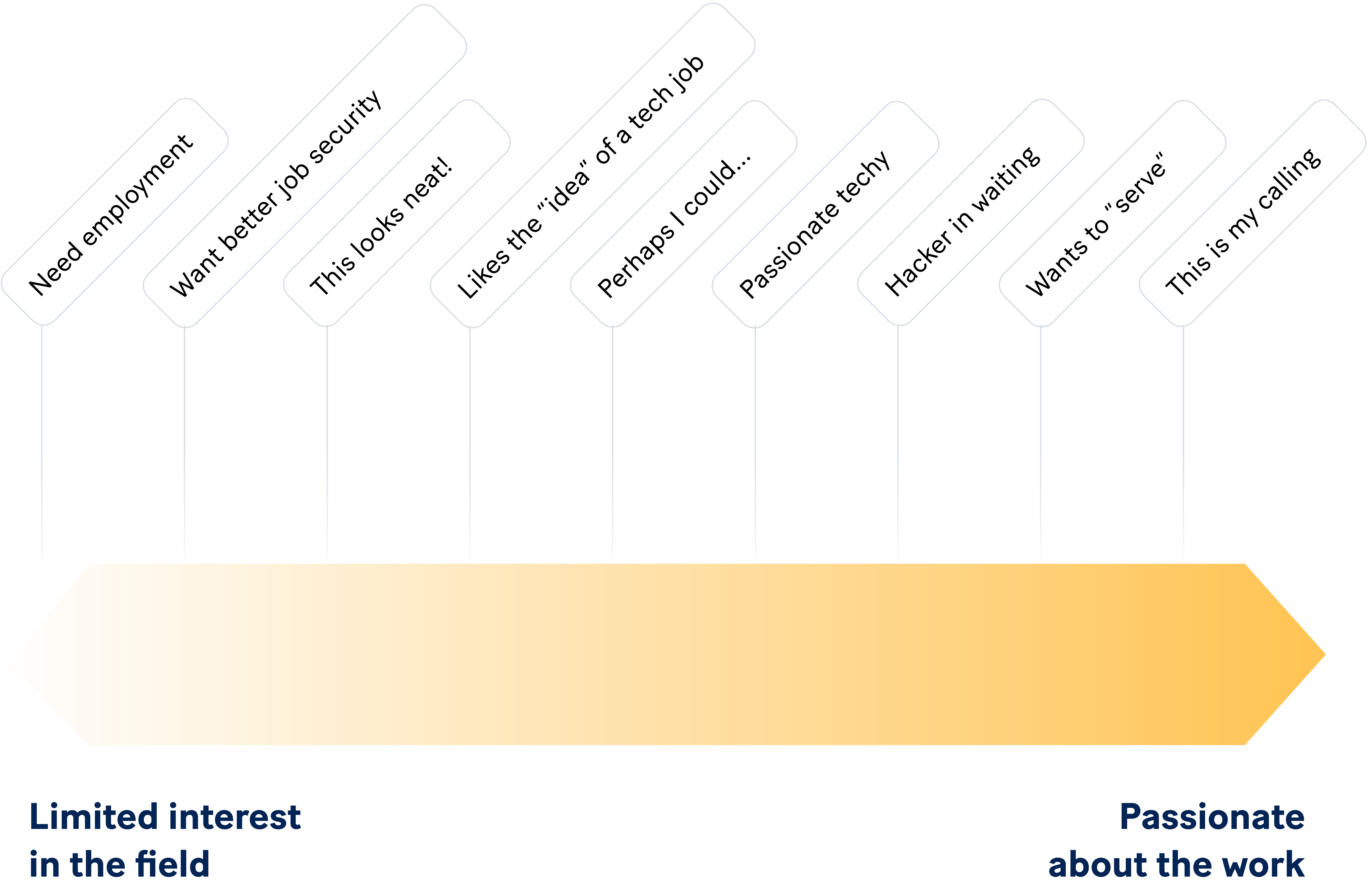
Understanding what attributes will make up an applicant's fit is critical for determining who you are looking for and in which talent pools you will likely find them.

Our research shows that many organizations rule out applicants based solely on credentials – a common practice across the larger tech community. Having concrete knowledge and skills that meet job requirements is undoubtedly essential. But in many cases, developing the required technical knowledge and skills could be a relatively low lift if the candidate you're considering is otherwise the right fit for your organization and the role.

For example, if you struggle to find someone with the right technical knowledge and skills, what other attributes or competencies would you seek to supplement those lacking skills?

Capturing the fit of a role is more important to get right at the start of the process than you might imagine. Candidates have different degrees of interest or engagement when they're applying for a vacant role. We should consider those possible interests when hiring (as shown in Figure 4). For example, there's a significant difference between an applicant just looking for a dependable job and an applicant with a passion for the work. That is not to say that the nominal job seeker won't become passionate over time. But it is important to understand the fit of the candidate you want to attract, why, and the investment you must make to take that person from an applicant to an engaged and effective employee.

Figure 4: Candidate Motivations – Interest and Engagement in the Field



Community-level Activities

We've suggested ways for organizations to improve how they define cyber roles in job descriptions and identify appropriate cybersecurity talent pools to attract applicants.

At the community level, workforce development stakeholders can scale these activities and apply them to the local cybersecurity ecosystems or sectors. For example:

Leverage the Cybersecurity NOS when defining cybersecurity roles in terms of community needs.

Enhance dialogue around cybersecurity work, what it is and the types of roles where talent is needed.

Market cybersecurity as a profession that gives opportunities to people with technical and non-technical interests opportunities.

Explore different talent pools.

Develop community-wide initiatives to find solutions where talent is not readily available such as sharing resources, engaging remote workers, developing a local talent pipeline, etc.

Quick Check:
Finding talent pools

☑ We have identified critical technical knowledge, skill requirements, and non-technical competencies and attributes that will support prospective employees within their roles.

☑ We realize that not all candidates will meet our initial expectations. So, we have identified a development pathway for those who demonstrate 'fit' with the organization but may not be quite ready for the role.

☑ We have investigated traditional and non-traditional sources of talent.

☑ We have established networks in those talent pools that can help us better understand and access desired talent.

Attracting Talent

> *You might have found them, but can you capture their interest?*

The Problem

Defining the kind of cyber talent we need and the types of talent pools we'll use to find candidates doesn't guarantee getting people in the door. There are other challenges in attracting candidates to cybersecurity work or our specific organizations. And it's not always about the money.

Cybersecurity has a public relations (PR) problem. We in the cybersecurity community see the field for what it is – a growing, nuanced, exciting and vibrant work sector. But from the outside, the cybersecurity field can look:

Invisible: There is minimal visibility on careers in cybersecurity. Additionally, inconsistencies in cybersecurity work prevent people from forming an accurate picture of the field.

Less desirable: Often cybersecurity jobs are in direct competition with other tech and business roles that people usually perceive as more appealing, rewarding, and progressive than a role in security.

Conservative: People can view cybersecurity as a conservative field focused mainly on protecting, fixing and repairing rather than innovating. This perception is due to the ongoing social discourse around cybersecurity.

Closed off: There are many perceived barriers to entry for a cybersecurity role. These perceived barriers range from needing technical expertise upon entry to the sometimes unappealing portrayal of cybersecurity professionals as "lone wolf" hackers.

Stagnant: There are also perceptions that cybersecurity career advancements are almost exclusively limited to the technical domain.

These negative perceptions can get in the way when we're trying to attract cybersecurity candidates.

Beyond PR, there are common issues that come from what organizations say and do when recruiting that can hurt attraction efforts for cyber roles. The Catalyst discovered some common issues:

Generally, people want to feel engaged in their work and organizations. How are we connecting with potential recruits about what we do? How are we articulating the employee value proposition (EVP) of cybersecurity and our organizations?

Increasingly, candidates are looking for something other than a career-long relationship with a single employer. Instead, they're leaning toward greater diversity in their work experiences. What opportunities do we have in our organizations that communicate the potential for work diversity? How can we better market these opportunities to the broader community?

There are greater calls for work flexibility in terms of type, location and hours of work – particularly in the tech community. How are we talking about the flexibility inherent to some cybersecurity work? What additional opportunities can we create and promote across the community?

Attraction Is a Critical Part of the Talent Pipeline

Organizations can do several things to help attract the right candidates. They may have a good sense of the type of candidate they want, but they also need to step inside that ideal candidate's shoes to try and understand what that candidate expects from an employer.

Organizations can engage in a wide range of potential attraction activities, including:

- Appreciating the local or 'reachable' talent landscape.
- Generating a fulsome employee value proposition that differentiates your organization from others – why should candidates come work for you?
- Aligning attraction strategies with different talent pools by developing unique messaging and activities to support attraction from each.
- Creating a profile for your organization:
    - What is your mission and vision?
    - Who are your leaders or leading cybersecurity professionals?
    - What is your market? Who do you help?
    - What does your organization offer that others may not?
    - What roles and opportunities, career and otherwise, await new employees?
    - How do you work with other organizations?
    - What emerging technologies do you use to combat cyber threats?
- Ensuring the work described in the job posting reflects your organization's need and accurately communicates other expectations of the role.
- Giving opportunities for applicants to experience the work and the company character through different activities such as workshops, capture-the-flag events, cyber challenges, informational interviews, expert panels, career chats, etc.
- Being flexible on non-critical job criteria, looking at alternative hires and communicating that in job postings.
- Employing mechanisms to help candidates self-screen if they aren't likely to be a good fit.
- Using multiple channels to advertise a vacant role, focusing on the channels your desired candidates are most likely to use and channels that go beyond those traditionally used in cybersecurity recruitment.
- Contributing to and attending industry and academic events where job seekers may be plentiful.

> *Ensure the work described in the job posting reflects your organization's need and accurately communicates other expectations of the role.*

Community-level Activities

Cybersecurity attraction campaigns within the community can be self-defeating since we all attempt to draw much of the same talent from the same pools. So to bring new talent into our cybersecurity community, we should:

Promote cybersecurity as a progressive, interesting and rewarding field of work.

Benchmark and adopt best-in-class attraction strategies from other fields.

Establish a recruiting network that allows us to reduce the competitive nature of the current recruiting environment and find ways to collaborate on collective needs that help our community overall. For example, many candidates that don't fit one organization could be an excellent fit for another.

Develop marketing collateral (videos, posts, etc.) that resonates with potential candidates beyond the tech community – people who may have never considered a career in cybersecurity. This collateral should demonstrate how cybersecurity offers:

- Different pathways and opportunities: technical, non-technical, generalist and specialist roles, academic, research, managerial, and leadership careers.
- Work flexibility.
- Benefits of working within an elite community of professionals dedicated to helping protect Canadians and Canadian organizations.

Offering and widely advertising work-integrated learning, co-op and internship opportunities.

Offering complimentary workshops on job-related topics.

Quick Check:
Attracting the right talent

☑ We know who we're looking for and why.

☑ We've made realistic and accurate job descriptions.

☑ We have considered attraction best practices.

☑ We are working collaboratively with the cybersecurity community to give us the most significant reach.

☑ We have articulated the EVP.

☑ We have differentiated ourselves as an employer.

☑ We use language and channels to give us better access to the talent pools we want to attract applicants from.

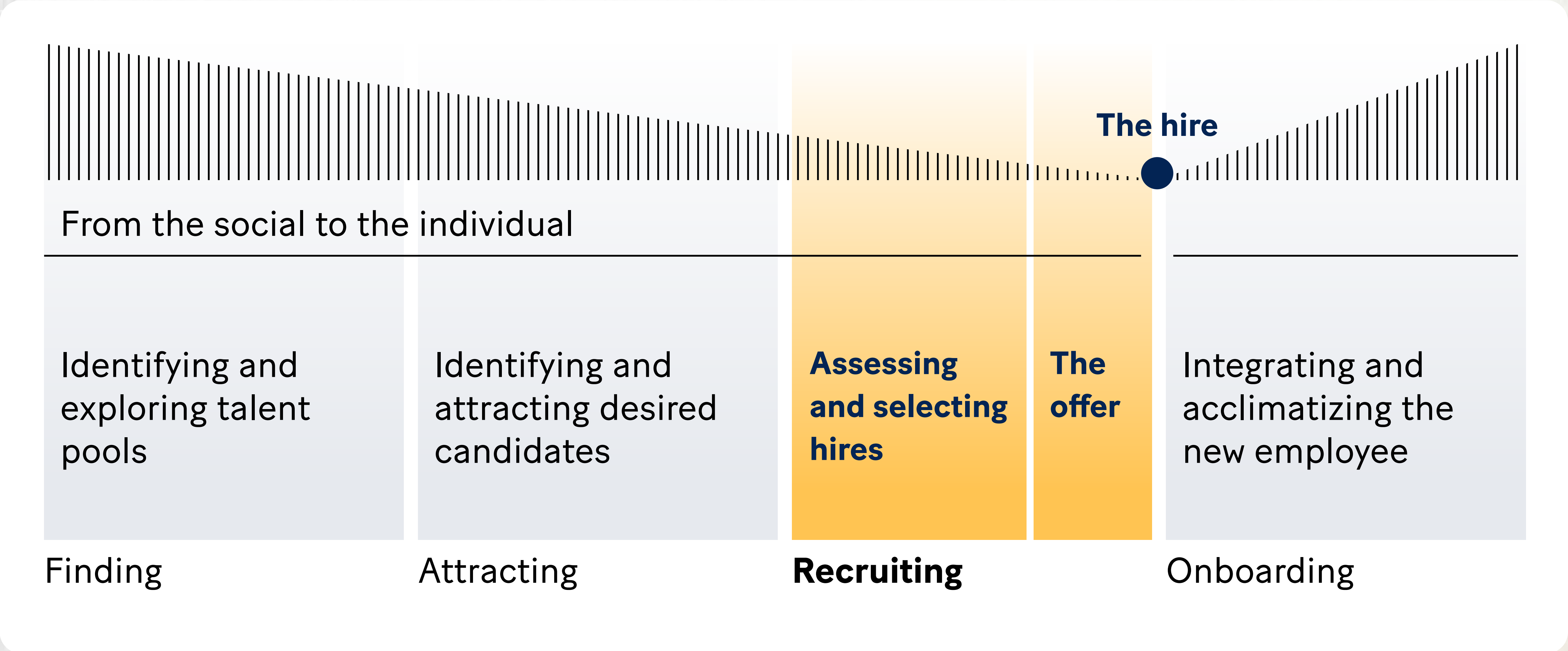
Recruiting and Onboarding

Once we've found our talent and they've accepted our offer, we need to bring them aboard.

For the sake of the Playbook, we've distinguished finding and attracting from the actual recruiting process, as shown in Figure 5.

Cybersecurity recruitment aligns with the definition of recruiting, which is "to enlist" or "to enroll." Recruitment is identifying viable candidates to assess, select, and hire for desired roles. Onboarding follows recruiting and strives to integrate and acclimatize new employees into the organization, their team and their work.

Figure 5: Recruiting and Onboarding as Distinct from Finding and Attracting



The hire

From the social to the individual

Identifying and exploring talent pools

Identifying and attracting desired candidates

Assessing and selecting hires

The offer

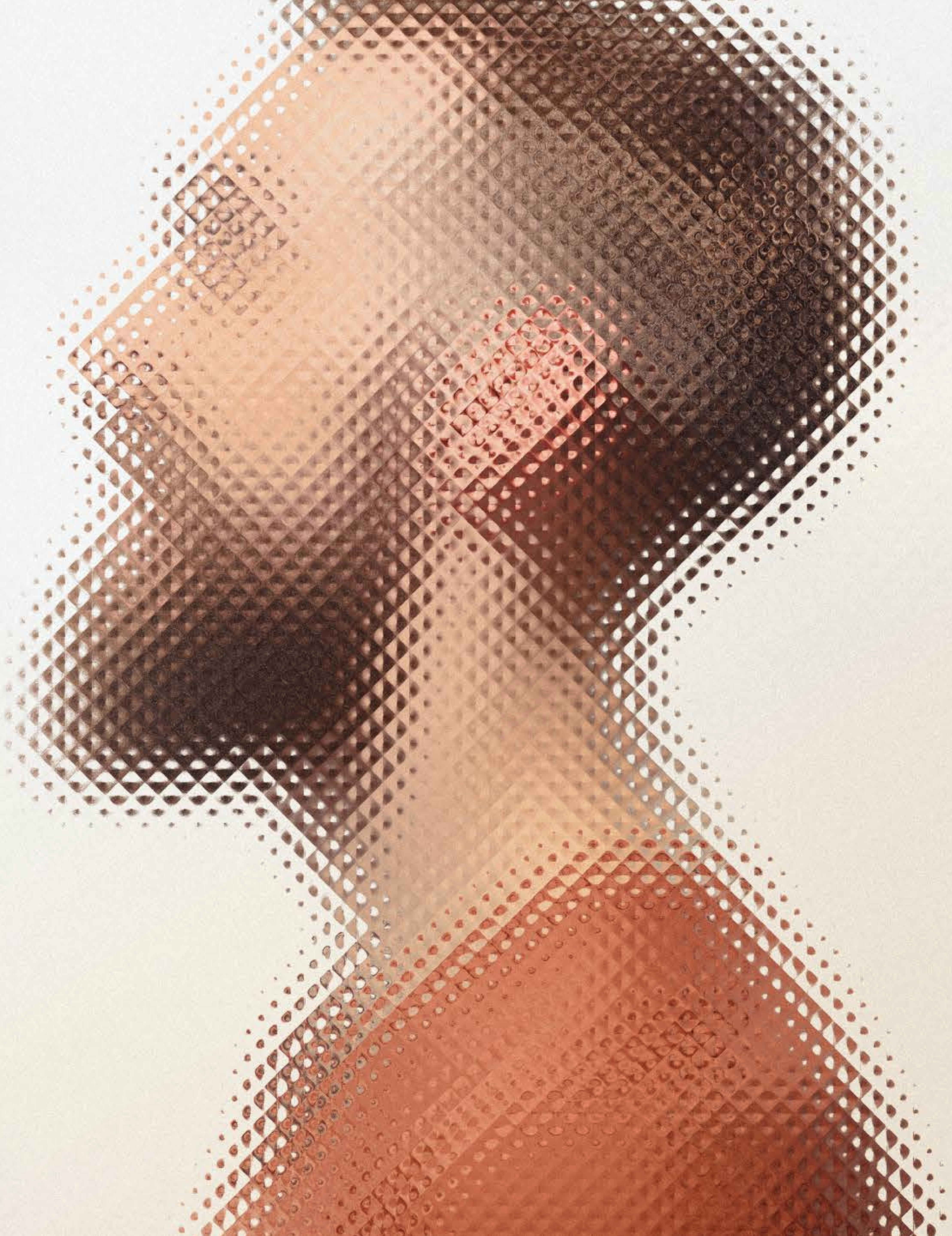
Integrating and acclimatizing the new employee

Finding

Attracting

Recruiting

Onboarding



Recruiting

> *Recruiting is not about filling a gap but finding the right person.*

The recruiting process typically involves three sub-processes: making a selection, creating an offer and hiring the chosen candidate. These sub-processes confirm that the organization only accepts candidates that meet the requirements.

The Problem

The primary challenge to cybersecurity recruitment isn't specific to the field. Rather, it's a challenge that persists across many sectors. That challenge is the tension between the organization's recruitment capacity, capabilities and expectations.

Organizations might have specific HR needs that they can't fill internally. In that case, they may invest in contracting recruitment experts and tools to properly find, attract, and recruit suitable candidates. But organizations' investments tend to fall below what a competitive labour market requires.

That's why organizations may not fill vacancies – even after investing in recruitment. But a vacant cybersecurity seat can directly increase an organization's risk exposure – and its employees' and community's risk exposure. That's why getting cybersecurity recruitment right the first time is crucial.

Beyond improper investment, Catalyst research and community discussions uncovered other recruitment challenges:

- Lack of a process. Some organizations take an ad hoc approach to talent recruitment. An ad hoc approach offers flexibility and creativity. But it can also give candidates the impression that the process is uncertain and unorganized and that decision-making may be more personality based than requirements based.
- Lack of consistency in the process. Different departments often share the recruiting processes and sub-processes across the organization. But candidates can get deterred when there is confusion or inconsistencies throughout the recruitment process. Candidates may assume that their experience reflects the organization and may not want to be associated with an organization without a well-honed process.
- Lack of consistency in the expectations. One of the most common issues in recruitment is finding consistency in expectations when different parts of the organization have different candidate expectations. For example, a hiring manager may seek a specific cybersecurity skill set, while the security officer may look for a candidate with more non-technical skills. At the same time, HR could want to ensure a problem-free hire, while senior leaders might be looking at the future potential of every candidate. These discrepancies are why organizations should consider ways to consistently address different needs in the job descriptions and assessment processes to avoid giving candidates confusing or conflicting messages during the process.
- Demand significant effort on the part of the candidate. Organizations can deter potential candidates by making the process unnecessarily difficult and time-consuming. For example, numerous interviews, tests and calls consume significant time and can give applicants the perception that the organization doesn't have a well-thought-out recruitment process.
- Lack of engagement throughout the process. Candidates applying for an open role are likely excited about working at your organization. But other employers may be trying to attract the same candidates. If you do not regularly engage with the candidate or keep them apprised of where they stand, they may feel that you've lost interest and gravitate to other offers.

For example, the Catalyst discovered a case where an organization had initially screened cybersecurity candidates and then asked them to undergo a month-long security screening process. But the employer dropped contact with the candidates in that month's timeframe, which frustrated some candidates and caused them to accept other offers.

- Limited reinforcement of benefits and WIIFT (what's in it for them). You will lose candidates from your pipeline in a competitive labour market if you do not regularly remind them of what attracted them to your organization in the first place. Engagement is more than a touchpoint; it is a rolling opportunity to reinforce why your organization is still the right choice. And it can also be a chance for candidates to learn more about or engage with your organization.
- Lack of data collection along the process. Collecting valuable feedback (e.g., recruits screened and hired) is crucial. Other measures, such as post-hire recruitment experience surveys or internal exercises to identify which candidates failed to screen and why, can help identify issues with your organization's recruiting processes.
- An inconsistent or lacklustre offer and lack of follow-up. It's amazing how much effort some organizations can put into finding, attracting and assessing candidates, only to have their offers fall flat. The offer is the primary decision point for the candidate. The offer should not have any untoward surprises and should express the candidate's value to the organization. Despite how crucial and delicate this moment in recruitment is, some organizations are known to:
    - Place an unreasonable time limit on the response (regardless of how long the candidate has waited).
    - Fail to follow up with the candidate to help answer any questions.
    - Fail to respond to a counteroffer.

Refining Recruiting Practices

Recruiting processes are the critical last mile in getting the right people into your organization. Recruiting for cybersecurity is different from recruiting for more traditional occupations. For some cyber roles, we might be attracting candidates who aren't entirely familiar with the cybersecurity community or the work.

The issue of cyber unfamiliarity mixed with the inherent competition with other technical occupations, the competitive labour market, and the risks associated with making a wrong cybersecurity hire require us to refine our cybersecurity recruiting processes. That's why we should ensure that our recruiting processes both 'fill the gap' and bring the right people into the field and our organizations.

To counter the many challenges cyber recruitment is up against, we should adopt a recruitment strategy that:

- Ensures an investment that reflects both the need to fill a role and the risks of a vacant role.
- Uses the right type of expertise and tools throughout the process.
- Works to give candidates a consistent and frictionless experience.
- Engages candidates throughout the process.
- Collects, analyzes and responds to meaningful data to support continuous improvement.

> *It's amazing how much effort some organizations can put into finding, attracting and assessing candidates, only to have their offers fall flat.*

We have also identified some specific best practices related to recruitment sub-processes showcased in Table 2. Organizations may already employ many of these practices, but they are worth a review to help secure cyber talent.

Table 2: Recruiting Sub-process Best Practices

Selection

Your assessment and selection processes should:

- Be valid and reliable.
- Use evidence-based methods (including, but not solely based on opinion).
- Include assessment tools that are accurate, user-friendly, reliable and dependable.
- Ensure trained assessors know how to conduct the assessment and have the means to ensure validity and reliability across assessments. This practice may warrant a frame of reference training to ensure all assessors are on the same page.
- Be sufficiently comprehensive to assess against work requirements and also be manageable for the organization or candidate.
- Be impartial and provide a fair assessment against the required criteria.
- Be defensible because a candidate may challenge the results through an official complaint (e.g., human rights, employment standards, wrongful hire litigation, etc.).

Offer

The offer should be:

- Transparent. Consistent with the previous discussions of expectations.
- Clear and offered in precise and unambiguous language around work conditions, compensation, and expectations.
- Comprehensive and include the needed details for the candidate to make an informed decision. It should also communicate why the organization regards this candidate as the right fit.
- Fair. Compensation should reflect the potential value the employee will bring. And if you are hiring for more than one candidate, keep in mind that they will likely communicate about their respective offers.
- Reasonably timebound. Give candidates sufficient time to seriously consider the offer, despite your desire for a quick response.
- Flexible. Be prepared with a counteroffer.

Hire (the legal step to making a candidate an employee)

When hiring, it's important that:

- There is a welcoming process.
- There are no unexpected (unwanted) surprises.
- The hire follows within a reasonable amount of time after the offer.
- Hiring includes all of the administrative requirements but is not onerous.
- Hiring echoes the commitment to the new employee and the alignment of values.
- Onboarding flows directly from the hiring process without a significant gap. The organization should support segmented onboarding if this is impossible due to workflows. The actual hire should flow directly into a complete onboarding. And if not a full onboarding, at least some aspects.

Community-level Activities

Recruiting is often process and context-driven based on organizational needs. However, collaborative activities also serve our larger community needs to help us identify and retain interested recruits for cybersecurity. These activities include:

- Communicating salary ranges based on role.
- Sharing recruitment data.
- Sharing leading best practices.
- Directing unselected candidates to other organizations that may present a better fit.
- Sharing sector or community-based general recruitment and screening processes.
- Developing self-assessments that can guide potential candidates to suitable roles.

Quick Check:
A supportive recruiting process

☑ Recruiting processes are aligned and integrated across the organization.

☑ Recruiting processes and practices are frictionless for applicants.

☑ Our organizational values are reflected and reinforced throughout the recruiting process.

☑ Opportunities are available for candidates to learn more about the organization during recruitment.

☑ There is a comprehensive and timely offer process in place.

☑ We collect feedback from the recruit and integrate it into future process improvements.

☑ We identify candidates we didn't select and refer them to other organizations.

☑ Recruitment data and other relevant information are shared within our community or sector.

Onboarding

> *The best onboarding experience evokes a feeling of welcome and belonging.*

Onboarding is commonly understood to be the process of integrating and acclimatizing a new employee into an organization. There is no one process for onboarding. Instead, every onboarding process depends on the organization, the role requirements, and the employee's needs.

The Problem

Our research uncovered that a central challenge for onboarding is that the process may not align with a new employee's expectation based on what they understood about the role from the recruitment process. Other onboarding challenges included:

- Lack of preparation to receive the new employees, which appears more consistently in remote work or work-from-home situations.
- Limited coordination or fluidity across the various elements in the onboarding process.
- Changes to how the organization introduces the work relative to previous discussions during recruitment. These can be changes in the primary work tasks or type of work, the location of work, the work team, or the conditions of employment.
- Limited attention to the psycho-social needs of new employees to make them feel welcomed and a part of the organization.
- Lack of engagement from the employee's new team or supervisor.
- Limited ability for the employee to learn about the organization or their new work.

Any combination of these can make new employees feel isolated or, even worse, neglected. It is not unheard of for employees to resign within or at the end of the onboarding process simply because what they experienced wasn't aligned with their expectations.

Onboarding Best Practices

We asked stakeholders for their insights into what characteristics an ideal onboarding process would possess. Figure 6 captures their insights and can help guide activities.

Figure 6: Characteristics of an Ideal Onboarding Program

- Welcoming
- Engaging
- Easy to follow
- Feeling like a part of the team
- Comprehensive
- Transparent
- Executive engagement
- Measured delivery of information
- Follow-up
- Interactive
- Orientation to equipment / tools
- Aligned with mission / vision
- Inclusive
- Relationship-oriented
- Job-related
- Informative
- Points of contact
- Easy to complete

Note that the phrases in Figure 6 don't emphasize administrative processes or training. Instead, the ideal characteristics shared by stakeholders capture an atmosphere that understands that new employees are transitioning to a new (and generally unfamiliar) work and social environment. Table 3 identifies three overarching perspectives that should inform the opportunities to support the new employee experience.

Table 3: Three Overarching Themes for Onboarding

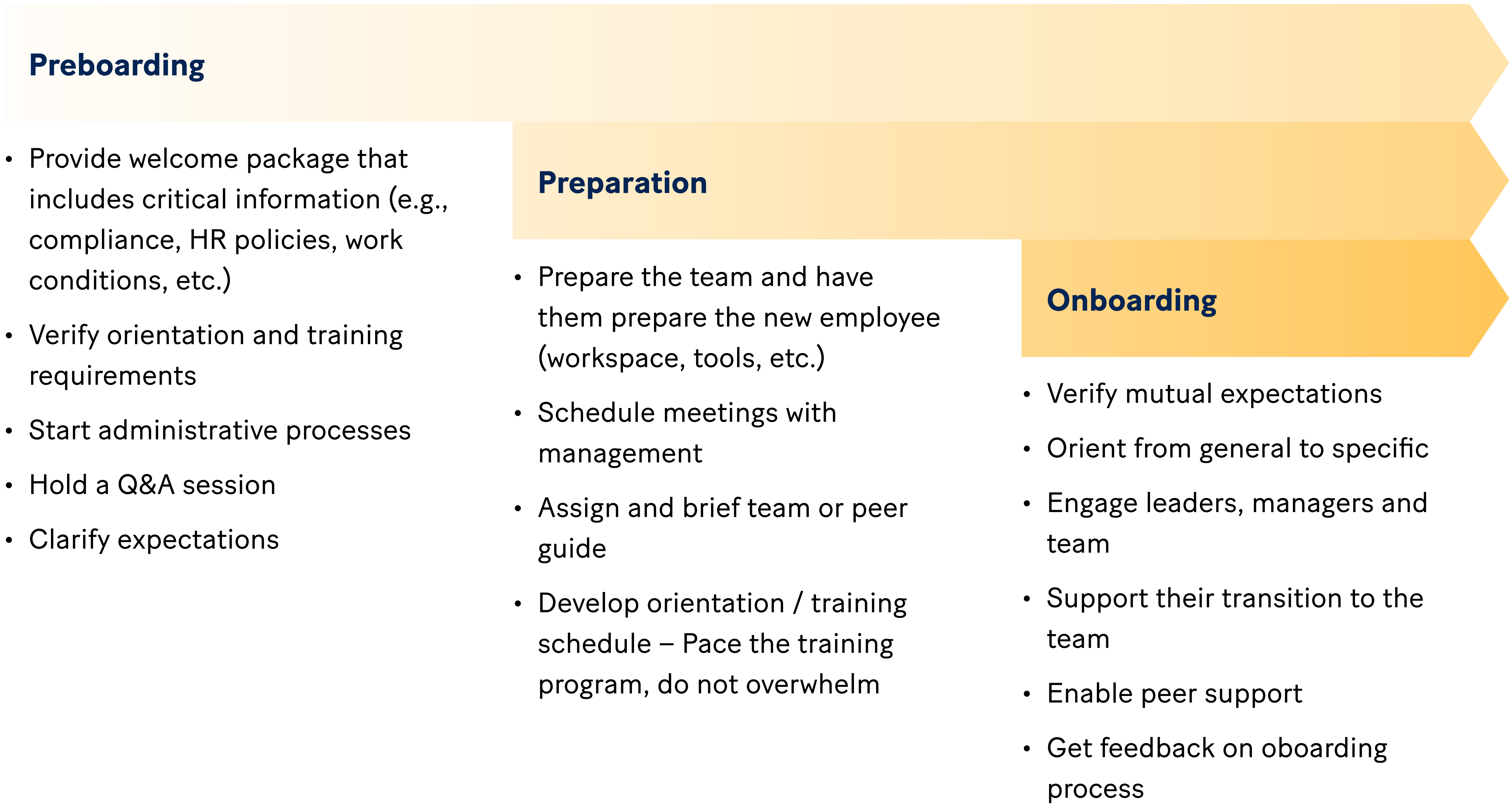
Inclusion: More than "Do I belong?" onboarding should address "How do I belong?"

Respect: "Does the organization recognize the value I bring?" and "Have I correctly assessed my value to the organization?"

Fairness: "Am I being treated similarly to others?" and "Is there a reasonable rationale for why the organization might treat others differently?'

Onboarding will always come with mandatory administrative and training processes. But onboarding should also emphasize how the organization situates these processes as part of the employee's transition. Figure 7 gives an onboarding roadmap example highlighting key activities that support a new employee's transition and orientation into the organization.

Figure 7: Onboarding Roadmap



Preboarding

- Provide welcome package that includes critical information (e.g., compliance, HR policies, work conditions, etc.)
- Verify orientation and training requirements
- Start administrative processes
- Hold a Q&A session
- Clarify expectations

Preparation

- Prepare the team and have them prepare the new employee (workspace, tools, etc.)
- Schedule meetings with management
- Assign and brief team or peer guide
- Develop orientation / training schedule – Pace the training program, do not overwhelm

Onboarding

- Verify mutual expectations
- Orient from general to specific
- Engage leaders, managers and team
- Support their transition to the team
- Enable peer support
- Get feedback on oboarding process

Critical cybersecurity onboarding issues

01

Organizational messages to the new employee are consistent with those from recruitment.

02

There is a firm understanding of mutual expectations.

03

New employees are oriented to their work and team immediately.

04

Leadership or senior managers acknowledge the potential of the new employees and the value of their cybersecurity role for the organization.

Community-level Activities

Onboarding processes are specific to each organization. But they allow us to collaborate on a few elements, such as:

Sharing best practices.

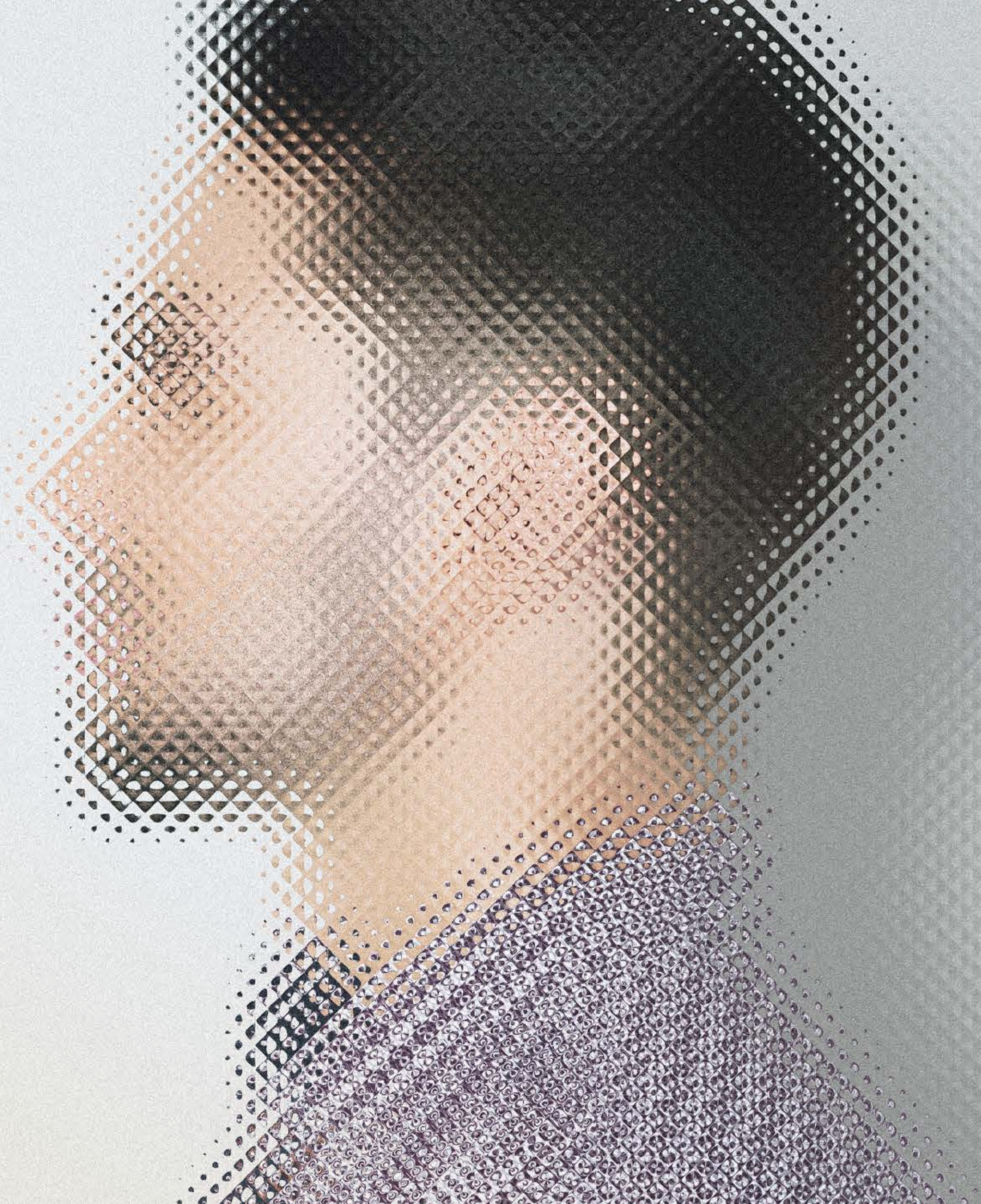
Sharing onboarding resources for general cybersecurity topics, particularly for smaller organizations in the same sector.

Sharing onboarding data.

Quick Check:
Value-added onboarding

- ☑ We have an onboarding roadmap that ensures a consistent and smooth transition from recruit to new employee
- ☑ We have a system that supports the new employee’s physical, social and emotional needs as they transition to their new job
- ☑ The work environment is set up and ready to go once the new employee joins the team, including tools, processes, job aids, etc. This preparation equally applies to a remote work or hybrid work environment
- ☑ We onboard a new employee into the organization, the work, and the team.
- ☑ We assign a peer guide or a colleague to help them with orientation and acclimation into the organization and team.
- ☑ We create opportunities for leadership or senior managers to address the new employee(s).
- ☑ The training during onboarding is well-paced and doesn’t overwhelm the new employee.
- ☑ We keep administration only to what the onboarding process requires.
- ☑ We ask the new employee for feedback on the onboarding process and integrate that feedback into our continuous improvement.
- ☑ We share onboarding data with the local community and our sector

Development



Development

> *Development is about creating opportunities to learn and grow.*

The Playbook uses development as a short form for "learning and development," which comprises planning, investing in and supporting the learning and professional growth of people in cybersecurity roles.

A common theme from our research was the importance of learning and development for cybersecurity professionals. Core to the culture, employers often discuss continuous learning as one of the key desired competencies. One of the reasons that continuous learning is so engrained is that effective cybersecurity depends on professionals who are up to speed on the threats and best practices to defend the systems for which they are responsible. That's why learning and development is not only an essential part of the ongoing development of cybersecurity professionals but is often a significant factor in retaining cybersecurity talent.

The Problem

A few foundational challenges persist across the cybersecurity community and impede learning and development.

The first challenge is the limited appreciation of the financial investment often required for cybersecurity professionals to stay current. Organizational training budgets can be meagre – even in prosperous times. Training in technical tools or procedures tends to be expensive, as many still perceive cybersecurity as a specialization. The training to remain current in cybersecurity commonly exceeds the average individual training budget.

Also, peer-to-peer exchange is one of the most important ways cybersecurity professionals grow. And there are many ways cyber professionals can learn from their peers, like through conferences, symposia and other events. Even though these events are costly, they're highly sought after because they offer learning and networking opportunities. (Networking is of particular value within a small specialist occupation like cybersecurity.)

The second foundational challenge is employers' emphasis on requiring a university degree and related credentials. The emphasis on post-secondary degrees and credentials is (in part) due to the relatively rapid cybersecurity workforce transition from a highly specialized field to more occupational work, where most of the roles are vocational. But many employers still demand a university degree – even though the emphasis on degrees and credentials is slowly shifting as college programs become a more prevalent pathway for entry-level roles.

The irony in this demand for degrees is that many graduates from university technical programs supplement their education with hands-on college or private-sector training to make themselves more marketable or gain confidence through hands-on work. We hope that the National Occupational Standard (NOS) and the normalization of cybersecurity work will reduce this employer demand. But until expectations become more consistent and emphasis on degrees lessens, cybersecurity professionals are under pressure to continually train or be involved in experiences to help them meet the breadth of employer expectations.

Continuing Professional Development Best Practices

Establishing a fulsome professional development program ensures an organization's cybersecurity professionals are on top of their game and can access opportunities to mature, thrive, grow and evolve to meet changing needs.

Our research and discussions identified common concepts and ideas for establishing effective learning and development programs. These concepts fall into three major areas, shown in Figure 8.

Figure 8: Contributing to Effective Learning and Development

Relevance

- Role-based experiences
- Provides baseline knowledge for organization
- Includes new software, processes, or concepts
- Needs-based

Style

- Provides guide, job aids and other materials
- Follows adult learning principles
- Incorporate mentorship
- Continuous
- Accessible

Goal-oriented

- Clear, unambiguous goals
- Supports individual and/or team learning goals
- Future leaning
- Supports certification, achievement recognition

A coherent and comprehensive cybersecurity professional development program should exhibit the following characteristics:

Supports organizational goals and balanced investment: The program offerings should be carefully curated by those who fully understand the learners, the learning needs and the organization's cybersecurity capability requirements, and the vision for the future. These considerations will honour the organization's time, resources and funding investment.

Are flexible and ongoing: The program avoids the one-and-done or starts-and-stops challenges to learning. Instead, it gives available opportunities when and where needed. Flexible and ongoing offerings are even more important when considering 24/7 team operations or hybrid work environments where work hours or locations vary.

Features collaboratively developed objectives: Collaboratively developed objectives are professional development objectives that work for both the organization and the employee. Identifying these objectives ensures that the investment is relevant to organizational needs and that employees feel heard and supported in their goals.

Provides fair and ready access: All cybersecurity employees have access to appropriate learning and development opportunities. Larger organizations with multiple teams should pay particular attention to access, as there may be disparity across cybersecurity teams that could be divisive.

Are followed with recognition or reward: Organizations should recognize successful formal learning achievements and experiences or specific milestones. And the organization should support noteworthy successes through rewards. (Refer to the next section for suggestions on recognition and rewards.)

Offers multiple pathways to achievement: Offering multiple pathways to achievement recognizes that not all learners learn the same way or can take equal advantage of all available opportunities. Pathways should include informal to formal learning, openness to self-guided learning, and leveraging existing capabilities. For example, job shadowing, coaching, and team challenges are all common avenues that can give fantastic learning opportunities with limited structure or cost.

Encouraging a trajectory: There is more than one potential career path in cybersecurity. Broadly, we know that someone can have a successful and rewarding career as a technical specialist, a generalist, or in management. So not all cybersecurity professionals have mapped out their careers. Still, performance reviews should include discussions about the employee's desired trajectory so that they can identify learning opportunities that support their career goals through developing technical and non-technical competencies.

> *The program offerings should be carefully curated by those who fully understand the learners, the learning needs and the organization's cybersecurity capability requirements, and the vision for the future.*

Community-level Activities

We can draw several community-level activities from our discussion on learning and development. These include:

- Keeping up with social and work trends.
- Adopting and sustaining a community-based networking tool for cybersecurity learning and development.
- Offering professional development opportunities through conferences, symposia or other activities that support ongoing learning.
- Creating community touchpoints throughout the year.

Quick Check:
Effective and efficient learning and development

☑ The learning and development opportunities offered align with our current and future goals.

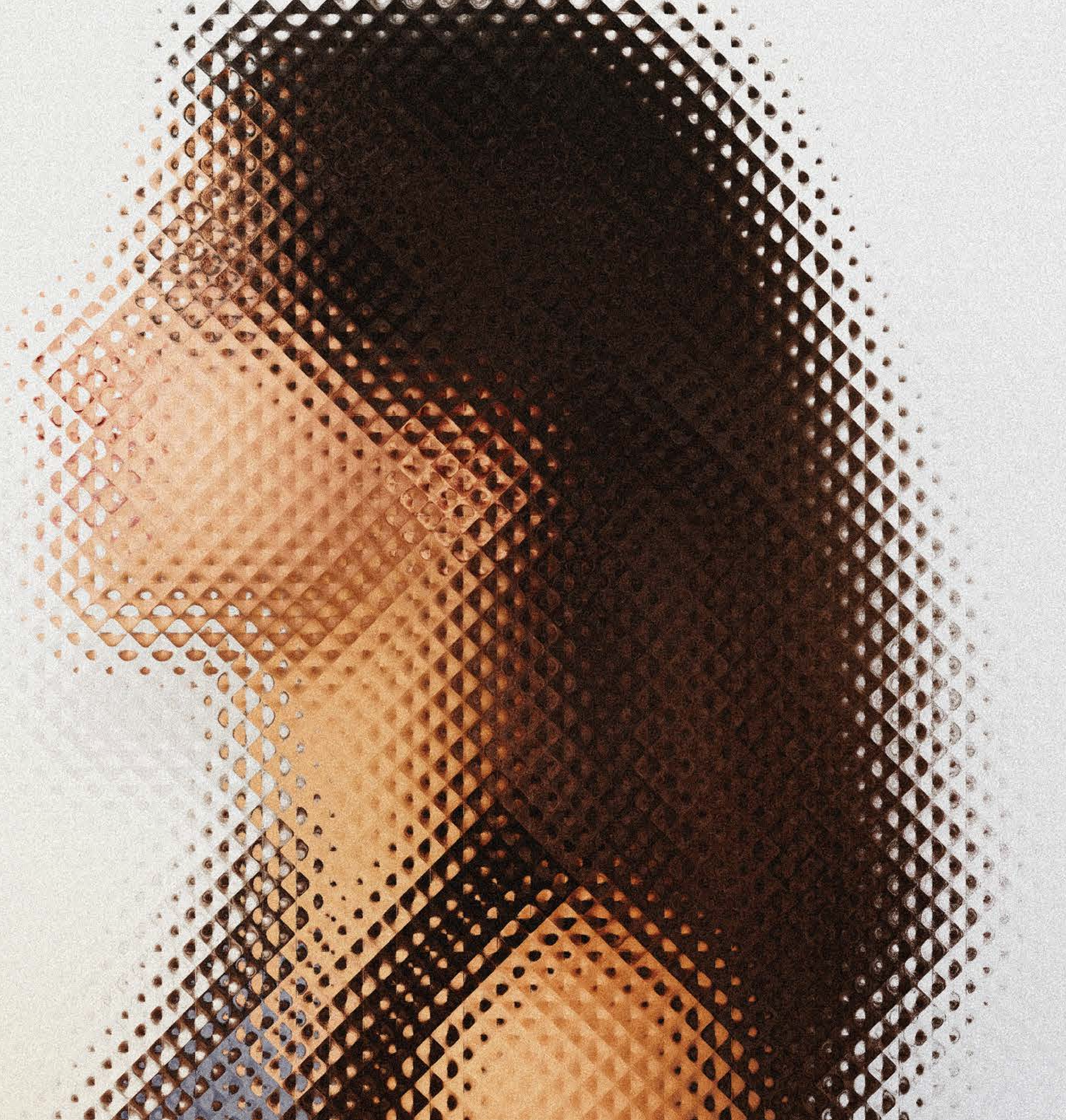
☑ We solicit input from our cybersecurity team(s) and employees on their required learning and development.

☑ We offer relevant, role-based learning experiences.

☑ Our professional development program is accessible to all employees.

☑ We have a spectrum of formal to informal learning opportunities that meet various learners' needs.

Compensation and Recognition



Compensation and Recognition

> *It's not just about money but about recognizing the employee's value to the organization.*

Compensation and recognition go hand in hand, particularly in cybersecurity. Cybersecurity is a competitive labour market, so employers should consider the monetary compensation offered for a role. But as our research shows, it's not just about the money.

The Problem

Organizations often view compensation and recognition as relatively stable cost centres that support the attraction and retention of human capability – a cost of doing business. Every organization engaged in our research understood that compensation involves far more than monetary benefits in today's market. That's why organizations need to understand what monetary and non-monetary compensation levels they should offer to secure good people in a competitive labour market.

A challenge to that understanding is the inaccurate or unreliable job or salary data that does not reflect the Canadian labour market. In some cases, authors of Canadian labour market reports insert U.S. or global data. In other cases, the data comes from scraping Canadian job postings. But cybersecurity job postings don't accurately depict the market simply because not all job postings reflect the employer's true needs (as we discussed in the earlier section, Finding Talent).

Cybersecurity continues to be an emerging field. So, there is no one-size-fits-all approach, and compensation benchmarking is often difficult due to the variations in cybersecurity work, even within similar sectors or regions. So organizations must determine whether they are underpaying or overpaying for their market. But we suspect that this is a temporary struggle.

Cybersecurity will continue to be dynamic, but it has started normalizing around vocational, engineering, and management roles. That stability makes data somewhat easier to compare and share across organizations within the same labour market. Still, there will always be unique contextual considerations that will influence organizational compensation strategies.

Organizations often undervalue cybersecurity employees in terms of compensation. Cybersecurity professionals need help make the business case for cybersecurity. The inability to make that case causes organizations to largely view cybersecurity as a cost centre rather than a business enabler, causing leaders and their financial advisors to focus on costs rather than value. This undervaluing extends to the discussion of employee compensation. Often cybersecurity employees are grouped with other technical employees with similar skill sets. But this grouping doesn't consider that the lack of effective cybersecurity talent often correlates to critical business risk. That is why the internal discussion about compensation calculations should go beyond skills to include the value of risk reduction and business continuity to which the cybersecurity employee directly contributes.

The COVID-19 pandemic and the consequent increase in hybrid and work-from-home (WFH) environments impacted compensation discussions. First, there was a significant increase in demand for cybersecurity professionals with a corresponding increase in talent competition. Second, hybrid and WFH also presented an opportunity for professionals to work remotely – an attractive option for many. That is why cybersecurity professionals' expectations have shifted to include compensation that reflects the demand and the opportunity to work in a hybrid or WFH environment.

The final issue related to cybersecurity compensation is the degree to which compensation goes beyond the employee's value and reflects the organizational values around the perceived importance of cybersecurity. Job postings are in the public domain, and stakeholders, investors and the broader cybersecurity community can view them. People can read between the lines of these job postings and conclude to what degree the organization values cybersecurity.

Best Practices: Compensation matters

It's true; compensation matters. But again, it's not just about money. Organizations should consider several best practices in non-monetary compensation.

Monetary compensation best practices are more than just salary. They extend to other elements such as:

- Salary benchmarking
- Annual raises
- Performance or skills-based bonuses
- Investments and/or profit-sharing
- Pensions or RRSP buy-ins
- Financial benefits (medical, dental, mental health services, sick leave, bereavement leave, vacations, childcare, discounts, etc.)
- Reimbursement or subsidization of professional fees and training costs
- Reimbursement or subsidization of home office costs
- Paid time off or sabbaticals
- Cost sharing (e.g., across partner organizations)

Non-monetary compensation and recognition in cybersecurity are increasingly giving employers a competitive edge.

Better pay continues to lead as a key attraction incentive and primary consideration in retention. However, our research shows that non-monetary compensation, the concept of culture as compensation, and the value of the organizational brand are also important. We've categorized non-monetary compensation findings into three areas in Figure 9.

The following are other considerations organizations should include in compensation discussions:

Transparency: Employees are likelier to share compensation information with peers. That's why organizations should consider the value of transparency within the bounds of privacy. For example, publishing salary ranges versus specific salaries of employees.

Equity and fairness: Organizations should make every effort to ensure that the compensation is equal and fair – similar pay for similar work. Equal and fair also apply to other benefits.

Consistency: Consistently applying compensation policies is critical to maintaining employee trust. For example, if performance bonuses are part of the compensation, it is important to ensure that the criteria are fairly and consistently applied.

Fiscal constraints: All organizations are working under fiscal constraints. Those responsible for compensation and employees need to appreciate these constraints. Most employees will understand changes to compensation levels if the organization makes them aware of constraints and acts in good faith.

ROSI: Our research shows a greater attempt to establish a return on security investment (ROSI) regarding risk reduction, lack of cyber losses, and increased business continuity. (Establishing a ROSI helps change cybersecurity perception as a cost centre.) And so, cybersecurity compensation should reflect this value and ROI.

Outsourcing: Organizations continually face the business case of whether to hire or outsource cybersecurity work. Whatever option an organization chooses should influence compensation decisions. An important consideration is to ensure that the organization identifies the total cost of either option.

Implementation costs: The organization should factor in the costs of designing, implementing and sustaining the monetary compensation and any changes to how it calculates compensation.

Figure 9: Non-monetary and Recognition Best Practices

Work environment

- Work from home or hybrid
- Office setting
- Team setting
- Flexible work
- "Perks" (e.g., meals, coffee, etc.)
- Feedback and communication

Work type

- Creative / research opportunities
- Increased responsibilities
- Mentorship / coaching / teaching opportunities
- Experiential opportunities
- Team / work group assignment
- Personal project

Social context

- Collegial norms
- Cohesion
- Sense of collective purpose
- Career growth / promotion
- Public recognition (e.g., awards)
- Status identifiers (e.g., badges)
- Mental health breaks

Community-level Activities

Organizations are less likely to share compensation and recognition data in the community – particularly in a competitive labour market. But we've identified several collaborative activities that could help organizations better address compensation and recognition challenges. These activities include:

Seeking or soliciting better data on employment, job types and salary ranges.

Finding ways to moderate salary expectations from potential recruits and create marketing or communications collateral on non-monetary compensation and recognition practices that could reduce the salary demands.

Better communication and improvement of work norms and practices that support the socio-cultural disposition of employees (e.g., work-life balance).

Raising the profile of best practices within the community and communicating what works within different organizations.

Collaborating to increase awareness across the community on common compensation and recognition practices.

Quick Check:
The total compensation package

✓ Our leaders and managers understand the cybersecurity compensation context.

✓ We are cautious of the data we use to drive compensation and recognition practices.

✓ We are transparent on the types of compensation offered, set realistic expectations, and include checks to ensure equity and fairness.

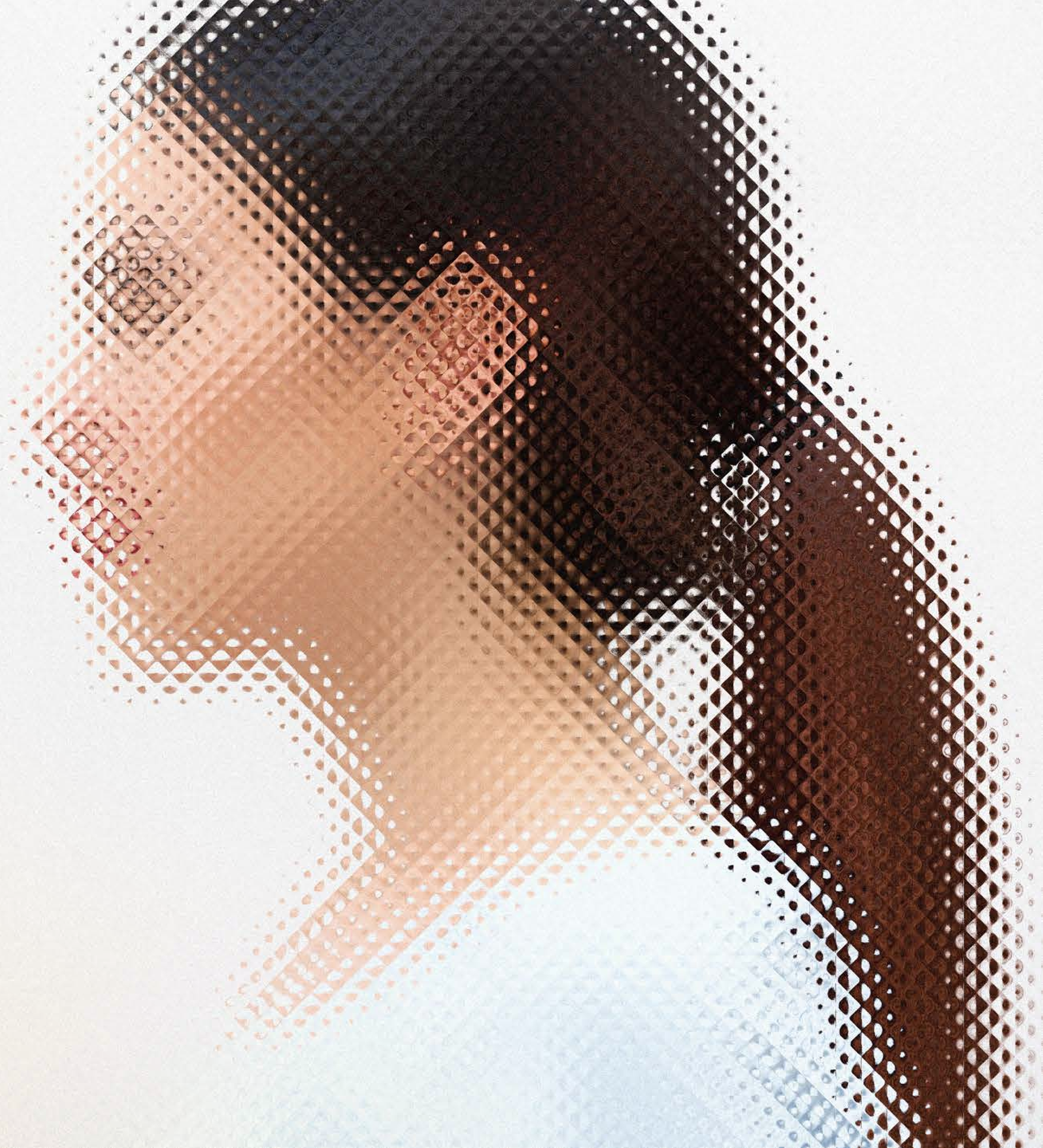
✓ We have integrated the concept of cybersecurity employee value (risk reduction, business sustainment, etc.) into our compensation calculations.

✓ We take a balanced approach to creating a competitive compensation package within our sector and the given labour market.

✓ We understand that our organizational compensation, values, and brand are connected.

Retention and Career Transitions

Everything discussed in the Playbook so far feeds into retention and career transitions. But earlier sections discussed these topics around the rationale and strategic perspectives versus specific retention and career transition activities.



Retention

> *Fundamentally, respecting the people we employ across the employment lifecycle is a significant part of any retention strategy.*

Retention is a simple enough concept to grasp from an HR perspective– keeping or holding onto employees until they are no longer needed. But there are many reasons why people leave an organization, several of which have nothing to do with the organization, work or compensation. Some of these reasons include changes in a family situation, broadening one's horizon, exploring new careers, or retiring. Retention doesn't focus on trying to keep employees whose reason for leaving wouldn't change due to any changes made by the organization. That's why our discussion on employee retention focuses on items in an organization's control, such as pay, work conditions, work tasks, environment, etc.

The Problem

If an organization finds they need a retention strategy, they may have a problem. The loss of good talent could result from factors outside of an organization's control, such as labour, economic or sociocultural factors. But there are also many factors that an organization can control. Our research uncovered several common reasons people leave:

Pay and monetary benefits: The labour market is extremely competitive in cybersecurity. Sometimes, the pay differential between smaller and larger organizations is substantial and may outweigh any other factors that would otherwise stop an employee from leaving.

Stress and burnout: Certain cybersecurity roles or functions put significant demands on the employees that perform them. That higher demand may result in the employees leaving to pursue a more sustainable work pace. This turnover is more pronounced when organizations don't recognize their employees' strain or give them respite from it.

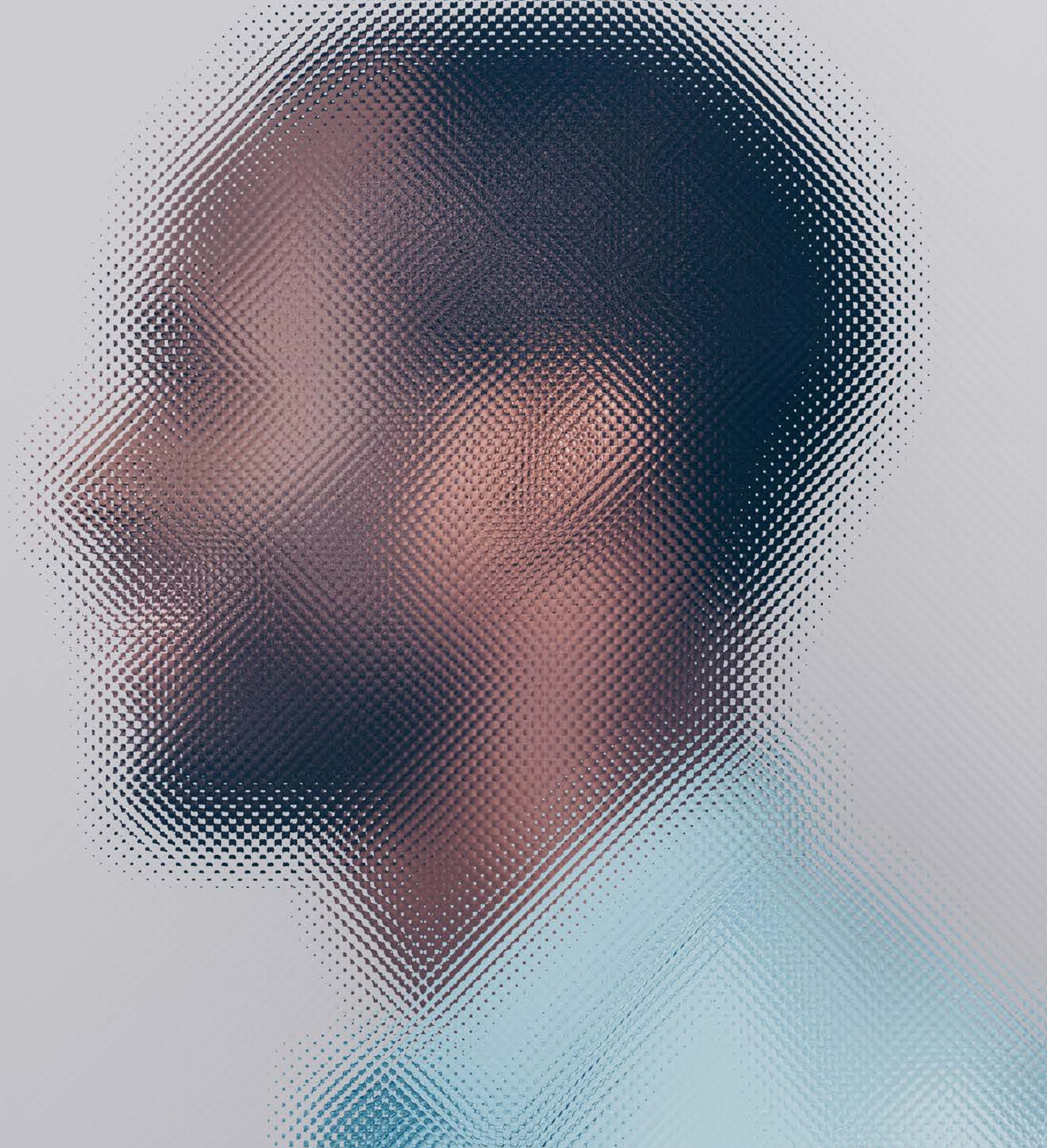
Lack of opportunity to develop: Cybersecurity is a highly dynamic field. Threats are significant, and the tools, techniques and procedures needed to combat them evolve quickly across the field. Cybersecurity professionals know that they need to learn and develop their skills continuously. And cyber professionals know that if they don't upskill, it will impact their work, potentially stagnate their careers, or even make them obsolete. That's why leaving a work setting to find a new organization that will support professional development is high on the list of issues regarding challenges to cyber retention. Cyber employees may also seek professional development beyond training for their current role. They could be looking for development opportunities to move laterally or upward to roles in technical specialization or managerial positions.

Poor leadership: Poor leadership creates many organizational challenges that result in weak retention. Leadership affects employee treatment, respect, and communication. It also affects the decisions made and the expectations set for each role.

Cybersecurity is a demanding profession that largely employs specialists. Cyber professionals should understand the expectations of each role across the field. But leaders and managers must also understand the cyber work environment and the differences between roles and responsibilities to set their expectations appropriately. Leaders and managers negatively affect cyber retention when they have unrealistic expectations, poor knowledge of roles, or a lack of appreciation for the roles' demands on employees.

Lack of flexible work: The COVID-19 pandemic and the consequent shift to work-from-home (WFH) and remote work environments proved how many cybersecurity professionals could perform equally, if not better, in those work settings. So many cybersecurity professionals didn't understand the rationale as organizations started the shift back to the office or introduced hybrid work schedules. That resulted in some professionals shifting allegiances to organizations that support WFH or remote work.

Poor work conditions: The physical space in which cybersecurity professionals perform their roles brings up a range of issues, such as lack of proper tools, poor office setting or physical work environment, poor workflows, lack of guidance or direction, limited access to resources, etc.



Retention Best Practices

Our primary goal is to retain people we value. And Figure 10 captures those foundational retention best practices well.

The business case for retention is quite clear. Strong retention prevents attrition, reduces turnover and the significant HR costs related to turnovers, and reduces disruption. The cost of disruption and recruiting, onboarding, and setting up a new employee can be a third, if not several times higher, than an annual salary cost, depending on the specialization level.

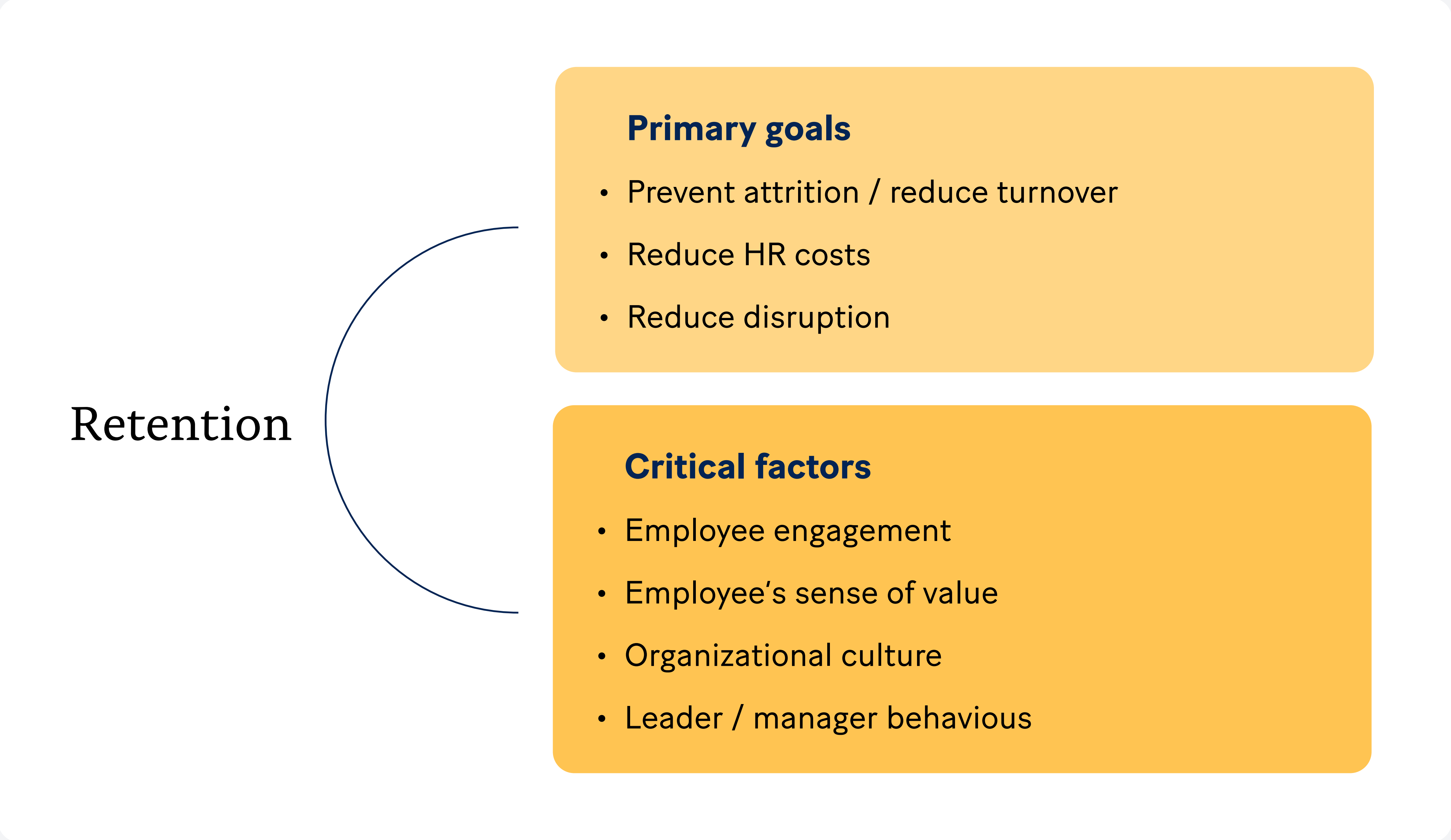
The primary reasons for leaving outlined in Table 6 indicate that the best way to retain people may be simply turning those negative issues into practices that will support retention. For example, an organization can acknowledge, address and solve poor work conditions, transforming the working environment for employees.

One of the greatest shortcomings is not knowing why people leave until they decide to go. Organizations need to get data they can respond to by engaging employees throughout their tenure – not just in the exit interview. Engaging employees by finding ways to address their needs or simply communicating why the organization can't meet a specific need demonstrates that you value them.

Additionally, establishing a welcoming culture beyond onboarding is crucial. Employees should always feel a sense of belonging that will translate into loyalty. And leaders and managers are also responsible for creating a positive environment that breeds loyalty by demonstrating clear communication, transparency, fairness, good judgement and support.

Our research uncovered many common reasons behind turnover, which are the basis for several of the best practices that support retention already discussed in the Playbook. Figure 11 captures many of these best practices from the employee's perspective.

Figure 10: The Foundation for Retention Best Practices



Retention

Primary goals

- Prevent attrition / reduce turnover
- Reduce HR costs
- Reduce disruption

Critical factors

- Employee engagement
- Employee's sense of value
- Organizational culture
- Leader / manager behavious

Figure 11: Best Practices to Support Retention

Recognition (that they value)

Compensation (that is competitve)

Work arrangements (that are balanced, flexible)

Well-being & benefits (that are suited to need)

Career growth (that provides options)

Tools & support (for their tasks, work, career)

Org values & culture (that they are aligned with)

Community-level Activities

At the community level, the primary concern around retention is ensuring that people stay in the cybersecurity field.

Many of the reasons for leaving identified previously extend beyond organizations to retention in the broader cyber community. For example:

Monitoring attrition from regions or sectors and conducting research into what may be the cause.

Providing reliable labour market data for a more realistic view of other occupational work and salaries.

Offering professional development through conferences, symposia and other activities, often including low or no-cost learning opportunities.

Establishing work exchanges that allow for diversity of experiences without impacting operational capabilities.

Providing cybersecurity professionals with the opportunity to showcase what they do.

Continuously marketing the profession beyond new entrants to established professionals to remind them of their value to society and create a collective sense of pride and cohesion. For example, cybersecurity professionals often consider themselves “guardians.” Building upon this professional persona is likely to help retention in the field.

Quick Check:
Align practices to support retention

☑ Our leaders and managers understand the tangible and intangible costs of losing talent.

☑ We gather employee job satisfaction data to identify potential issues that may impact retention, such as pay, benefits, or work conditions.

☑ We offer competitive salaries and benefits, where possible.

☑ We monitor relationships and review performance management documents to discern any trends.

☑ We monitor employees to identify any issues that may impact their work.

☑ We encourage continuous learning and professional development.

☑ We reinforce the importance of the leaders' and managers' roles in creating a supportive culture.

☑ We also reinforce the positive performance culture and the importance of being part of a team.

☑ We recognize their contributions and relevance to the mission.

☑ We conduct exit interviews to gather data about why employees leave. We then analyze the data to improve practices that support retention.

Career Transitions

> *Our organization is judged by how we treat our current employees and how we treat them when they are moving on.*

Our final topic is career transitions. We are spotlighting this topic because it is part of the employee experience that can significantly impact the employee and the organization.

We define career transitions as moving from one type of work or field to another. That may include an employee making a significant change in their work or role at their current organization or leaving for another organization. In any of the scenarios, it's in the organization's and employer's best interest to support an employee's transition.

The Problem

Employers and organizations have many potential reactions when a good employee has made the difficult decision to move on. (How employees approach their departure will significantly impact an organization's reaction.) The response from managers and team leaders can range from a sense of loss to a feeling of betrayal. Feeling loss is likely unavoidable. But negative emotions beyond that typical response could easily result in counter-productive behaviours.

Supporting an employee's transition can be difficult to achieve. Most organizations – particularly those that only consider the short-term bottom line – view losing an employee as the loss of an asset, an inconvenience, and a cost to replace. But being supportive of an employee's transition has other benefits. For example, an organization that doesn't handle an employee's transition well can cause various issues. And some of those issues can work against the organization's self-interest in three ways:

Reputation: The cybersecurity community is a relatively tight-knit, highly-connected community that talks. How an employee experiences an employer will likely spread through the larger community and impact future recruitment.

Operations: The potential impacts on organization operations could be very real. For example:

- Former employees may land at other organizations that could be (or become) partners, suppliers, clients or customers. Their experience with their former organization will colour how they relate to any business dealings, which could include taking their business elsewhere.
- Former employees will likely continue to have a relationship with some of their former colleagues and have a high chance of sharing their positive or negative experiences of their former employer. The former employee's experiences could impact the current employees' attitude toward their employer or shape their job performance.

Recruitment: "Boomerang" employees leave an organization for another opportunity and then return to the original organization in the same or a new position. Boomeranging happens a lot in cybersecurity since it's such a small community. Boomeranging is sometimes even encouraged when an employee transitions from a technical specialization to a broader managerial position because the diversity of the experience helps prepare the employee for different roles. But if the employee has a negative experience transitioning out of the original organization, it increases the odds that they won't boomerang back.

Transition Best Practices

A foundational best practice is to view all transitions as inevitable and make the most of them. Transitions are often emotional events that can be positive, exciting and bring about a welcomed change. But they can also create fear, anxiety, and uncertainty. An organization's objective should be to find ways to contribute to the positive over the negative emotions to the degree it can.

Two of the most effective practices that organizations can do to get themselves and their employees prepared for transitions are to 1: ensure that there are career discussions embedded into performance management practices and 2: consciously engage in career pathing.

Career pathing is when an organization works with its employees to determine their potential career trajectory. A career pathing session is an aspirational yet practical discussion about where and how employees envision their career progressing over a reasonable horizon (5-10 years). Team leaders or managers should revisit these career pathing discussions during performance reviews. When leaders and employees revisit these discussions, they should include the potential for internal or external opportunities and required professional development or training.

These discussions are important in two ways. First, they show employees you are engaged and interested in their development. Second, it gives insight into the employee's intentions, preparing you for potential internal or external transitions.

Table 7 gives us four key actions to support career transitions. Organizations can apply these actions to an internal or external move.

Table 7: Transition Best Practices

Career transition services

Giving employees various supports for their transition, including:

- Decision support and counselling
- Resume assistance
- Informational interviews
- Job search

Outplacement

Creating a formal process for an employee to obtain permanent or temporary employment in another organization.

- Bridging work experience opportunities
- Internships for increased responsibility or specialization
- Fractional or shared work
- Secondments and job exchanges

Exit interviews

Facilitating a dialogue with transitioning employees to identify:

- Why they are leaving, if unknown
- What improvements they would suggest
- What support you can offer

Ongoing engagement

Recognizing the value of former employees and the benefits of sustaining a relationship. (Also called an alumni model.) Organizations can achieve ongoing engagement by leveraging the following:

- An alumni membership
- A web portal for alumni
- A newsletter
- Social events
- First access to temporary work or projects
- Opportunities to coach or mentor

Community-level Activities

Maintaining a vibrant cybersecurity ecosystem.

Creating an information network in the local community for both employees and employers that can identify opportunities and resources available. Any information network should include a listing of temporary positions, secondments, internships, or job exchanges that might offer employees alternatives to a resignation.

Giving training opportunities to support the major roles supporting cybersecurity, such as consultancy, management, education or technical specializations.

Having specialized cybersecurity job transition services to support key transition points such as moves to independent consultancy, management, education or technical specializations.

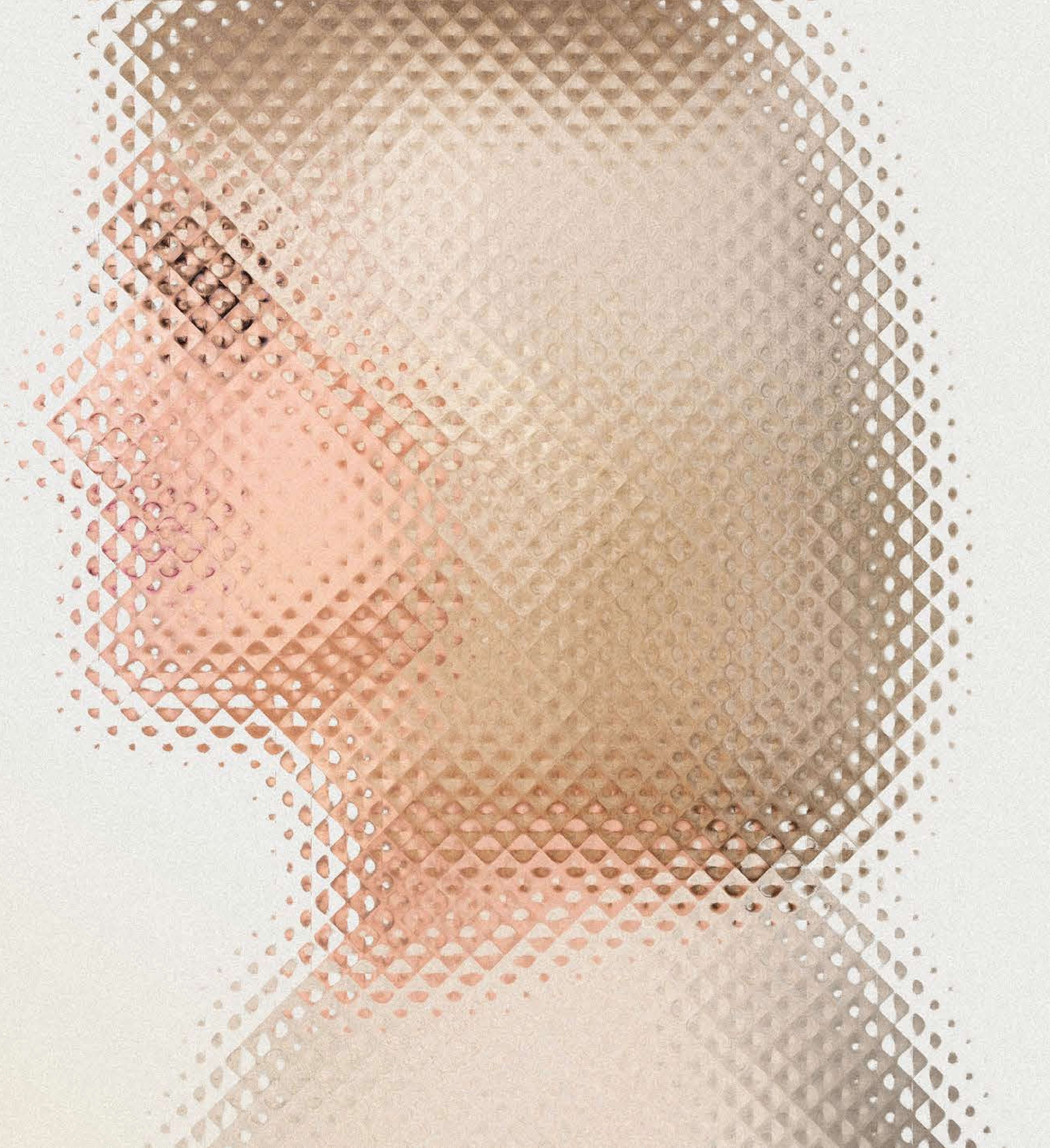
Offering training to leaders and managers on transition counselling and support.

Quick Check:
Preparing for and supporting transitions

- ☑ We acknowledge the principle of reciprocity and understand that employees who leave may continue to influence our organization in different ways.
- ☑ We have transition supports in place.
- ☑ We have exit interviews.
- ☑ We consider alternative employment arrangements that will give diverse opportunities to support career growth.
- ☑ We have contingencies to support operations if a critical employee departs unexpectedly (e.g., retainer for services, third-party access, shared resources, etc.).

Regional and Sectoral Considerations

Our Playbook has primarily focused on cybersecurity requirements in organizations. But our research and discussions unearthed regional and sectoral issues affecting how many organizations within them attempt to meet their cybersecurity talent requirements. The following gives a quick primer on the regional and sectoral considerations that impact. cybersecurity talent management.



Regional Considerations

There is a cybersecurity talent shortage across Canada. But some regions fare better than others. Regions with access to a broader pool of talent, one or more post-secondary institutions with relevant programs and a concentration of cybersecurity expertise have fewer challenges.

But most regions across Canada don't have access to these talent sources. Instead, many regions experience talent challenges such as:

- A lack of relevant education and training.
- Limited ability to attract new talent based on location.
- Limited ability to compete against higher wages offered mainly in urban areas.
- Limited opportunities and pathways for cybersecurity professionals to advance their careers.
- Little to no access to cybersecurity expertise or local services.
- Reduced telecommunications infrastructure and limited redundancy.
- Relatively poor insights into the local labour market.
- A sense of isolation from the mainstream market.

Cyber threats are boundaryless and pervasive, making no distinction between regions. That is why deliberate threat actors, accidental occurrences and natural events can have an outsized impact on regional economies without industrial or commercial diversity. A significant cybersecurity incident against government offices, critical infrastructure, and an industry or commercial enterprise in these areas can create greater impacts on the local economy and result in undue human suffering. So, what can regions do to protect themselves?

First, regions must consider cybersecurity a necessary investment in community safety and prosperity. Regions should include cybersecurity scenarios in emergency management and regional risk management discussions to 1) develop an appreciation for how cybersecurity affects prosperity and 2) so an incident's impact on prosperity can be surfaced, analyzed and addressed. Addressing regional priority cyber risks will help ensure community safety and economic stability.

> If you only had one fiber cable going into your community, what would be the impact on work, education and public safety if it was severed? What alternative communications exist in the event of a cyber failure at that scale?

Second, regions should identify their local cybersecurity talent needs and recognize that lacking talent poses a risk to regional public safety, security and economic stability. Where is cybersecurity expertise required, and to what level across the region?

- How are organizations managing the lack of cybersecurity talent?
- Where are the greatest vulnerabilities resulting from a lack of cybersecurity talent?
- Which organizations are critical for public safety and the local economy?
- What is the forecast for cybersecurity talent as regions look into the future?
- To what degree can we rely upon remote talent to support regional cybersecurity?
- Where can we upskill people with cybersecurity responsibilities to reduce the need for and investment in cybersecurity talent?
- What talent may be available within the local labour market?
  - What talent pools have we explored, and which remain untapped?
  - What are the potential impacts of tapping into those talent pools? (E.g., there are risks associated with moving talent from one area of need to another.)
  - What other impediments to entering a cybersecurity career exist in our region?
- Is there a career path for talent beyond the initial job?
- Are there opportunities for talent to expand or move laterally with their expertise?

> Often, people in IT or OT positions only need some cybersecurity training to make a significant difference. Equally, the professionals responsible for assessing and managing risks can readily integrate cyber risks into their discussions and take additional actions to mitigate risks – often without any additional technical expertise or significant investment (e.g., user security training, security policy enforcement, effective data categorization and management, ensure effective personnel screening, etc.).

Third, regions can use the information in this Playbook to identify opportunities and close their talent gaps once they've understood their talent needs. For example:

For talent pools in the region:

- What training or education might the people in the available talent pools need?
- What training and education is available (on location or virtually)?
- What other learning pathways can people explore to reskill or upskill for cybersecurity?
- What messaging and channels can we explore to get the right people interested in cybersecurity work in the region?
- What subsidies or benefits can we offer people interested in pursuing a cybersecurity career in the region?
- What should we explore as we look at retaining existing talent?
- What alternatives are there if we simply can't find the required talent?
    - Upskilling existing people
    - Automating tasks
    - Outsourcing to regional third-party service providers

If we need to look beyond the region:

- What resources and channels do we have to find and attract talent?
- What advantages does the region offer to prospective talent?
- What kind of subsidies or benefits can we offer people interested in pursuing a cybersecurity career and moving to the region?

Sectoral Considerations

Cybersecurity talent gaps exist within all Canadian economic sectors – including critical infrastructure.

This Playbook will help organizations close their cybersecurity talent gap. But whole sectors can use the information in the Playbook – particularly the community-level activities – to help establish sector-based cybersecurity and organizational resilience. Industry, sector, or commercial associations can help by leading the processes to define sectoral cybersecurity talent gaps.

The following prompts help define sector-based cybersecurity talent gaps:

What are the specific requirements of our sector? Business, technical or threat contexts often require specific cybersecurity talent needs. For example, the increased reliance on data-driven technology and automation in advanced manufacturing means cybersecurity experts must understand automated systems' vulnerabilities and mitigations.

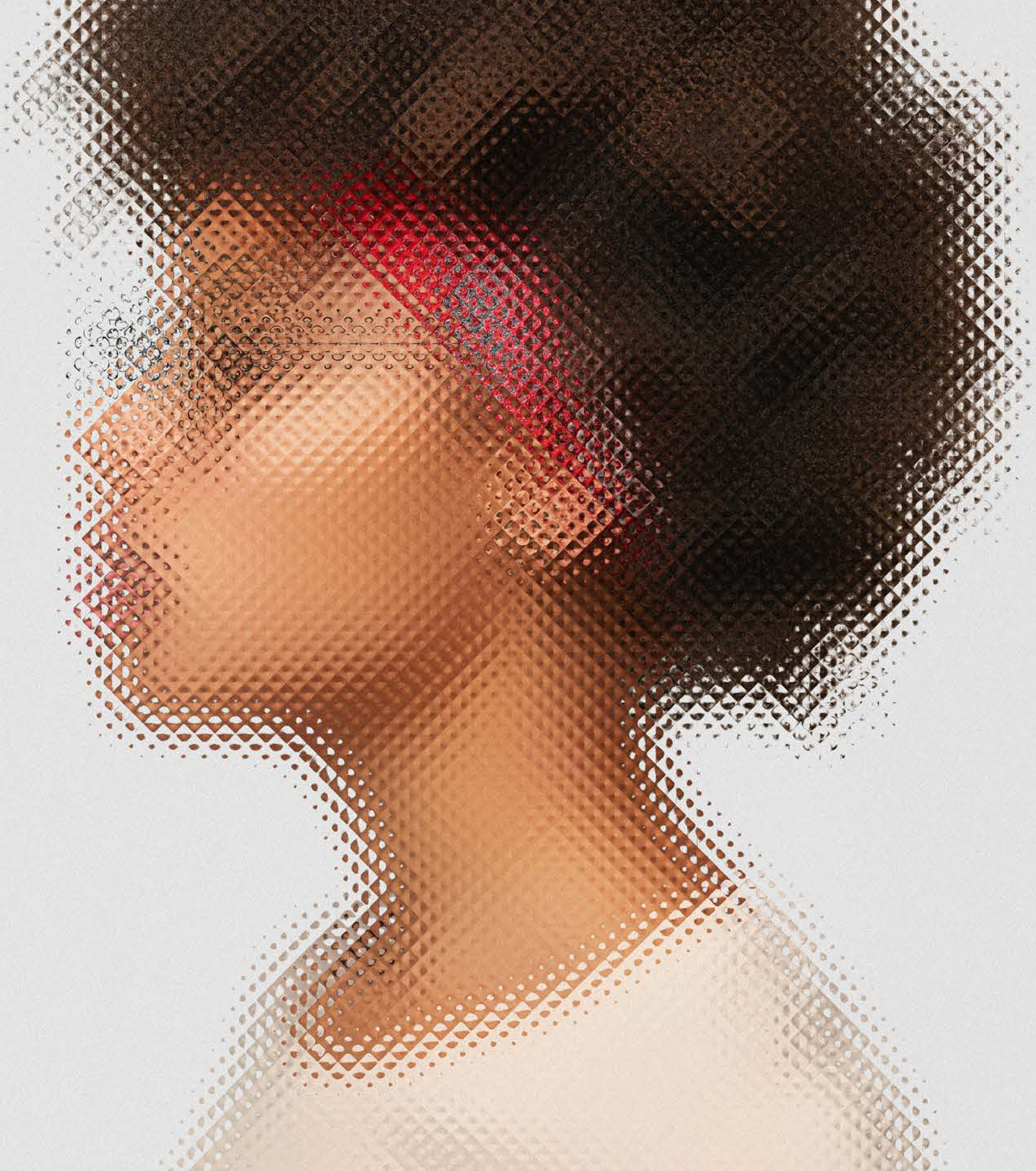
How is cybersecurity talent distributed across the sector? Talent is only sometimes equally distributed across a sector. Mostly, talent clusters in regions with large-scale industries and more opportunities. Sectors should apply the regional approach to cybersecurity talent development in areas where talent is unequal.

How do cybersecurity professionals in our sector sustain their expertise and capabilities? Business and related technology will rapidly evolve in some sectors. That presents new vulnerabilities, new risks and new threats. That's why rapid evolution creates the need for new technologies, processes, or expertise to sustain cybersecurity. Sectors with a high pace of change should establish continuous learning or professional development opportunities to ensure their cybersecurity professionals stay on top of their game.

What opportunities exist for cross-sector cooperation? Sectors do not stand alone. Supplier, partner and client relationships often hinge on the survival of other sectors. So, sectors have the potential to reach across sector lines to share expertise, technologies and resources to help everyone in the chain combat cyber threats.

> *Business and related technology will rapidly evolve in some sectors. That presents new vulnerabilities, new risks and new threats. That's why rapid evolution creates the need for new technologies, processes, or expertise to sustain cybersecurity.*

The Need for a Talent Pipeline Management Framework



The Need for a Talent Pipeline Management Framework

The cybersecurity talent gap extends well beyond individual organizations and affects all sectors, provinces, regions and the nation. This Playbook has given talent management processes with a focus on individual organizations. But many of the practices shared in this Playbook can extend differently to the broader cybersecurity and workforce development community.

We need to work together to collect accurate labour market data, define the cyber needs and close the gaps as they arise to tackle the sectoral, regional and national cybersecurity talent challenge. Collaboration is how we can help to ensure cybersecurity for all Canadian organizations and, by extension, all of Canada's economy.

We can create a talent pipeline management framework using the best practices within this Playbook and paying particular attention to the shared responsibilities at the community level. A talent pipeline management framework is one of many solutions. But it brings the greatest potential to help address the talent gap.

The Rogers Cybersecure Catalyst (the Catalyst) is a national talent generation hub that can lead collaboration within this talent pipeline management framework to achieve provincial, regional, and sectoral goals.

The Catalyst has created a system and a community engagement process to help regions and sectors tackle their cybersecurity talent gaps. That system includes:

- Defining the scope of the associated ecosystem, including IT and cyber-related services, businesses and business associations, local government, education and training institutions, and economic and workforce development stakeholders.
- Facilitating discussions on topics related to:
  - The actual talent gap across the region or sector.
  - Current and forecasting future cybersecurity talent demand.
  - Regional or sectoral risk-based priorities.
  - Opportunities for collaboration.
  - Potential solutions.
  - Determining metrics and measures of success.
- Establishing collaboratives with interested stakeholders.
- Analyzing and working with workforce supply channels to gauge capacity in achieving talent goals (e.g., recruiting organizations, training and education providers).
- Designing talent supply chain components (pathways, preferred providers, and contributors).
- Identifying potential sources for funding and sustainment.
- Giving workshops on implementing, sustaining, evaluating and measuring the effectiveness and efficiency of the talent pipeline to support continuous improvement.

Conclusion

Catalyst acknowledgments:

Randy Purse, Senior Advisor

Agata Kazimierski, Senior Advisor

Juliana Scharrer, Associate Director, Cybersecurity Workforce Training

Andrea Dermody, Employer Relations Specialist, Cybersecurity Workforce Training

Catalyst Sponsors:

Rushmi Hasham, Director, Cybersecurity Workforce Training

Charles Finlay, Founding Executive Director

It is important to look through the lens of the cybersecurity employee life-cycle to appreciate all potential investments to support effective talent management. Finding, attracting, recruiting, developing, compensating, and transitioning employees to other career pathways requires a broad set of individual and organizational competencies that organizations can bring together in a successful talent development strategy to achieve their goals. We hope that the guidance in this Playbook will be useful to everyone engaged in developing and implementing the cybersecurity talent management strategy.

We also need to appreciate that both cybersecurity capabilities at the organizational level rely on talent management beyond the boundaries of the organization. There are clear steps that the broader cybersecurity community can take to support sectoral and regional talent needs. But these steps require collaboration over competition. We must bring together our combined knowledge and capacity if we are ever going to overcome the cybersecurity talent gaps that plague our nation.

The Rogers Cybersecure Catalyst is an action-driven leader in cybersecurity talent development. By implementing innovative training and talent programs, the Catalyst equips cybersecurity professionals with the essential skills Canadian companies, governments, and communities demand.

Appendix

Critical Context

The Cybersecurity Talent Problem

It's estimated by the broader workforce development community that the cybersecurity talent shortage will progress relentlessly into the next decade.

There are many drivers behind this shortage.

- **We need a clearer picture of the cybersecurity talent gap.** Organizations looking for cybersecurity talent understand their needs, but Canada still needs to define its own talent gap. We are getting a better picture through better labour market tools. But we still need to clearly define the types and quantities of need at the community, regional and national levels.
- **Over-dependence on traditional post-secondary education (PSE).** Traditional PSE needs to be the primary pipeline for preparing new talent as a response to the rapidly evolving workforce. But PSE has yet to generate the type and quantity of talent needed.
- **Restrictive immigration policies.** We must look abroad for talent to sustain our population and productivity as Canada's nominal birth rate slows. Even though we've seen positive changes to immigration policies, there is still too much dependence on a review of educational credentials – which is only one determiner of capability. A more open and fair assessment is needed. That assessment would include training, education and experience to increase the number of viable acceptable immigrants.
- **Portability of roles in a global work environment.** Canadian organizations generally remain committed to in-person work, despite operating in a field with stiff competition for talent and increasing opportunities for remote work. That practice makes attracting talent to some locations difficult, particularly when there is strong evidence that professionals can perform their roles remotely.
- **Cybersecurity is a 'low visibility' occupation that the public often misunderstands.** Cybersecurity has a public relations problem as a field of work. Many false perceptions about cybersecurity work across workforce development and career counselling communities exist. This lack of awareness and visibility means that people who could be well-suited for cybersecurity work may not even know that it is an option for them.
- **Talent initiatives focus on technical skill development versus fit.** Organizations should emphasize the type of fit alongside technical skill in talent development initiatives. But unfortunately, there's often a disconnect between what a cybersecurity role requires and how talent initiatives are funded and measured. Typically, funding gets poured into short-term talent development initiatives to get 'bums in seats.' But much of the talent in the pipeline will leave within a few years of being on the job. That's because cybersecurity is a unique occupation requiring more than technical know-how. Cybersecurity professionals need mastery of several non-technical competencies to be effective. Most importantly, talent must possess a competency for continuous learning. That is why there should be more focus on that type of fit within talent initiatives to ensure that the initial investment gives a sustained return.

> *Organizations looking for cybersecurity talent understand their needs, but Canada still needs to define its own talent gap. We are getting a better picture through better labour market tools. But we still need to clearly define the types and quantities of need at the community, regional and national levels.*

[1] Public Safety Canada (2018), National Cyber Security Strategy, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx#s21

[2] Canadian Centre for Cyber Security, (2023), Glossary, https://www.cyber.gc.ca/en/glossary

Cybersecurity as a Field of Work

Cybersecurity is distinct from other technical fields. So, we need to know what cybersecurity work is and who does it to help us define the talent challenge.

Canada's National Cybersecurity Strategy defines the field as such, "(c)ybersecurity is the protection of digital information and the infrastructure on which it resides."[2] The Strategy expands on this definition, stating, "More specifically, cybersecurity includes the body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability."[3] In short, the field is not simply limited to technology. Instead, it encompasses the people and processes and the application of technology to achieve cybersecurity.

But Canada has struggled with defining cybersecurity work for over two decades. The Digital Governance Council has developed a National Occupational Standards (NOS) scheduled for release in fall 2023. The NOS helps normalize cybersecurity by giving a lexicon and using a role-based framework and a business-oriented lens (versus a national security lens). The NOS' business-oriented lens excludes highly specialized work within the national defence, intelligence and law enforcement in favour of more broadly applicable organizational cybersecurity functional areas adapted from the NIST Cybersecurity Workforce Framework (2011): Oversee and Govern, Design and Develop, Operate and Maintain, and Protect and Defend (Table 9). The NOS describes several dedicated cybersecurity roles within these four functional areas, considered "core." These roles include chief information security officer, secure software developer, cybersecurity operations analyst, incident responder, digital forensics analyst, etc. These core roles require unique knowledge, skills and abilities relative to other occupations.

The NOS also recognizes cybersecurity as a team sport. It takes many people in an organization to support organizational cybersecurity. These "cybersecurity adjacent" roles are not employed full-time in cybersecurity but require some cybersecurity knowledge, skills and abilities. Such roles include board members, chief executive officers, boards, chief information officers, learning and development professionals, enterprise architects, business analysts, software developers, IT helpdesk or customer service representatives, system administrators, etc.

Most organizations do not need cybersecurity professionals on staff. However, almost all organizations connecting to the internet operate with cyber risks they must manage. So, there is an overarching requirement for almost all management and employees to have some level of cybersecurity knowledge, skills and abilities that will support organizational cybersecurity goals (Figure 12). Many cybersecurity consultants and services are available if an organization requires specialized expertise.

Table 9: Cybersecurity Functional Areas

Oversee and Govern

Directing and managing organizational cybersecurity requires a balance of technical and non-technical roles.

Design and Develop

Planning and developing the secure digital infrastructure, system and software emphasizes project-based and technical roles.

Operate and Maintain

Ensuring secure digital infrastructure operations, systems, and software primarily focused on technical roles.

Protect and Defend

Conducting cybersecurity operations.

[2] Public Safety Canada (2018), National Cyber Security Strategy, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx#s21

[3] Canadian Centre for Cyber Security, (2023), Glossary, https://www.cyber.gc.ca/en/glossary

[4] Though they occasionally draw from the civilian talent pool, these work domains which tend to create their specifications, standards and training based upon their unique requirements.

[5] The Canadian Cybersecurity Skills Framework initially created by TECHNATION in 2019 and funded through the Government of Canada (see https://technationcanada.ca/en/future-workforce-development/cybersecurity/cybersecurity-skills-framework/), was adopted in 2023 by the Canadian Centre for Cyber Security https://www.cyber.gc.ca/en/education-community/academic-outreach-cyber-skills-development/canadian-cyber-security-skills-framework

Figure 12: Cybersecurity Needs and Organizational Role

Organizational need	General role	Training opportunity
Need to advise on and conduct specialized cybersecurity functions	Specialists	Specialist role based training and skill development. Experiential learning. Specific competency development.
Need to advise on and conduct cybersecurity	Cybersecurity professionals	Common cybersecurity skills training and functional competency development
Need to integrate cybersecurity into organizational security practices	Generalists and other security professionals	Context-relevant cybersecurity foundations
Need to acquire, manage, operate, and maintain IT assets to support cybersecurity	IT professionals	Context relevant rolebased cybersecurity training
Need to direct, allocate, and manage organizational cybersecurity resources and activities	Business operations and management	Cybersecurity and risk management
Need to integrate cybersecurity into work practices	General users	User / individual cybersecurity responsibilities

Most organizations

There are many options that organizations or other talent stakeholders can explore to help address talent challenges, such as:

- Segregating sensitive or valuable data and critical operations from internet-connected digital technologies (avoiding cyber risk).
- Outsourcing the needed technical expertise and technologies to a trustworthy third party.
- Building and maintaining internal capacity by ensuring existing employees have the knowledge, skills and abilities to assume critical cybersecurity functions.[6]
- Sharing resources with partner organizations or in a trusted business community.
- Automating key cybersecurity functions.

[6] Keeping in mind that many of the cybersecurity functions are people or process driven so deep technical knowledge may not be required. As well, even many of the technical preventative and routine cybersecurity activities such as access control, patch management or data segregation can be performed by individuals with IT experience.

Flipping the Script on Talent Development: A cybersecurity talent ecosystem approach

The cybersecurity field and the cyber landscape are moving too fast for traditional post-secondary education (PSE) programs to produce graduates who can reliably meet industry needs.

We all need to rethink and expand our understanding of talent pools, learning and development pathways and the scope of cybersecurity work to keep pace with the demand.

Exploring New Talent Pools. PSE will continue to be a source of well-educated talent, but there are other talent pools we can investigate. To explore these other pools, we must first release our dependence on defining talent via academic credentials. Instead, we need to better understand what talent and capability for cybersecurity require in the current landscape. We must look to diverse sources of talent and alternate sources of capability beyond PSE programs. And we must vet talent with different assessment and selection processes to help us better identify where the potential exists.

Learning and Development Pathways. We will continue to rely on PSE to give a well-rounded education to workforce graduates. But, hopefully, the gap between what graduates learn in school and what the work demands will shorten as educational institutions increase their collaboration with the industry. That collaboration should work to integrate more experiential and competency-based learning to shape an adaptive curriculum development model.

We also need to explore other means to develop the required talent. That means looking at the continuum of potential learning from informal to formal, supporting competency development, distinguishing between credentials and their accurate reflection of competence, using a variety of assessment processes, and finding contributors that can better support continuous learning.

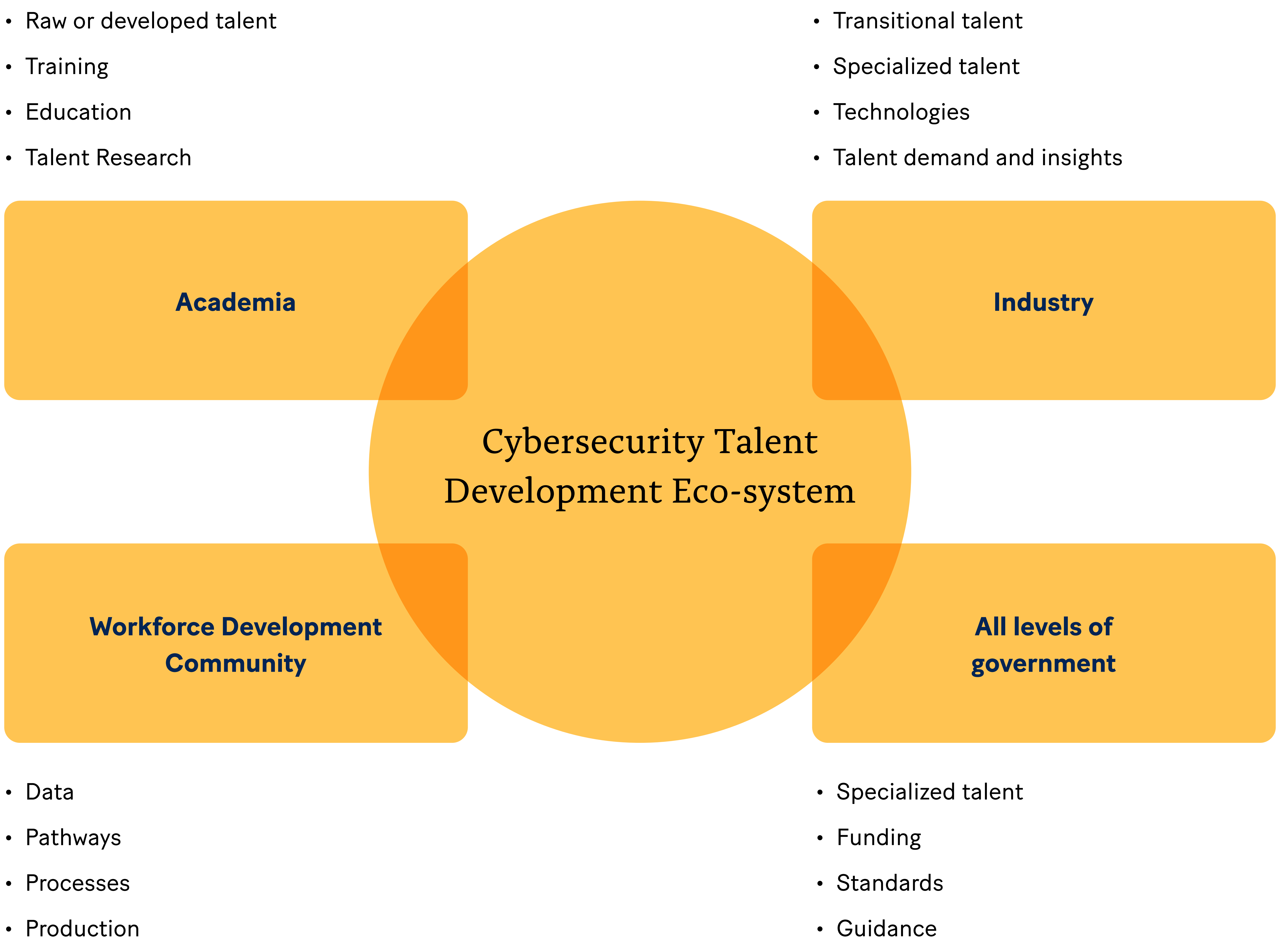
Scope of Cybersecurity Work. We must understand the difference between cybersecurity and cyber-adjacent roles to achieve a robust cybersecurity talent ecosystem. For example, all connected organizations need some level of cybersecurity if they wish to protect their digital information and infrastructure. But not all organizations need to employ a cybersecurity professional. We must clearly distinguish between cybersecurity work and other work supporting cybersecurity. That understanding will help organizations define the type and quantity of people needed to fill cyber gaps, and it will also help identify the knowledge, skills and abilities required in other roles that support effective cybersecurity.

Once we understand how to 'flip the script,' we can envision an extended cyber talent pipeline that includes:

- Non-traditional talent.
- Common and cooperative outcomes.
- Learning pathways that leverage a full continuum of opportunities from formal to informal learning.
- Recognition of achievements earned beyond a post-secondary academic credential.
- Technical and non-technical competency development.
- The use of non-cybersecurity professionals to close capability gaps.

Flipping the script on talent development will not happen in isolation. Nor can we focus only on one organization, region or sector to the detriment of others. We need to leverage the entire cybersecurity talent development ecosystem (Figure 13) to collaboratively tackle the talent shortage challenge to ensure we address organizational needs while supporting local, regional and national requirements.

Figure 13: Cybersecurity Talent Development Ecosystem



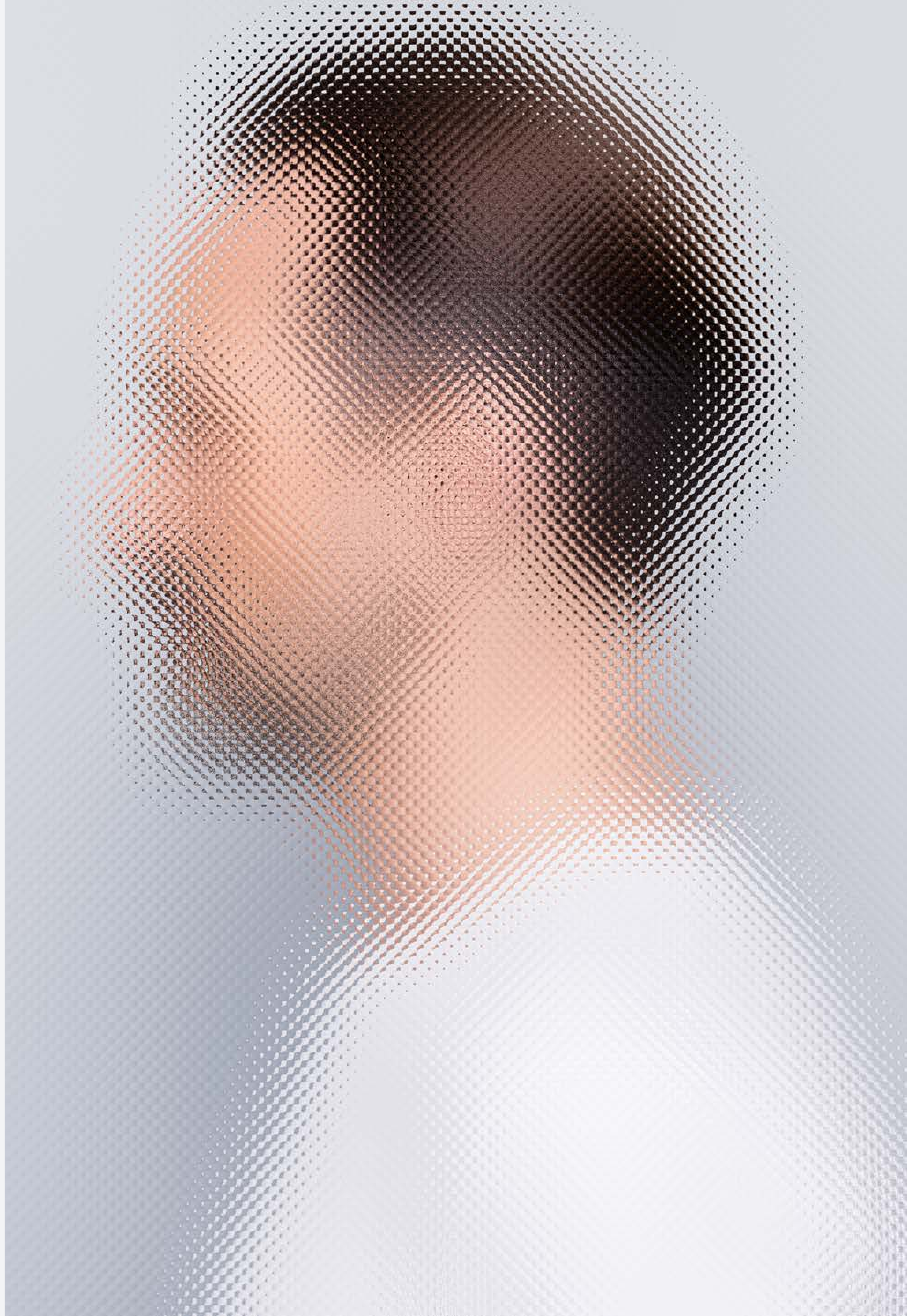
- Raw or developed talent
- Training
- Education
- Talent Research

- Transitional talent
- Specialized talent
- Technologies
- Talent demand and insights

Academia
Industry
Cybersecurity Talent Development Eco-system
Workforce Development Community
All levels of government

- Data
- Pathways
- Processes
- Production

- Specialized talent
- Funding
- Standards
- Guidance



Cybersecurity Talent Management Playbook

For more information, please contact:

Rushmi Hasham, Director,
Cybersecurity Workforce Training

Rushmi.Hasham@torontomu.ca

Toronto
Metropolitan
University

ROGERS
cybersecure
catalyst