Gartner Research

Midsize Enterprises Must Welcome New-Collar Workers in Cybersecurity

Patrick Long

2 February 2024

Gartner

Midsize Enterprises Must Welcome New-Collar Workers in Cybersecurity

Published 2 February 2024 - ID G00803972 - 8 min read

By Analyst(s): Patrick Long

Initiatives: Midsize Enterprise IT Leadership

Midsize enterprises are often unable to attract and retain security talent the same way large enterprises can. To bridge the skills gap, MSE CIOs must change their approach to recruiting security talent by embracing the new-collar workforce.

Overview

Key Findings

- Tactical cybersecurity education can be driven through certification programs and other nontraditional education routes, such as hackathons and bootcamps, as an alternative to degree programs.
- Staffing and hiring processes in MSEs are too traditional and restrictive, making the already-limited cybersecurity talent pool even smaller.
- While most security roles in MSEs are tactical and call for less management training, they do require a combination of coaching, sponsorship and mentorship for success.

Recommendations

MSE CIOs focused on security and risk management should:

- Refine the list of necessary competencies for their organizations by exploring and evaluating nontraditional education that provides sufficient training in cybersecurity.
- Open up talent acquisition pools to new-collar workers by reconsidering the organization's approach to staffing and hiring practices.
- Support the long-term growth of new-collar workers by providing resources for coaching, sponsoring and mentoring.

Introduction

Across industries, midsize enterprise (MSE) IT budgets are, on average, 4.9% of annual revenue. [1] Only 5% of the IT budget is allocated to security. A ratio of one dedicated cybersecurity full-time equivalent (FTE) for every 20 IT FTEs makes an MSE CIO's approach to cyber and information security all the more challenging. Yet, the need to create a strong, mature security posture remains.

Ginni Rometty, former CEO of IBM, recognized that skilled, technical positions such as cybersecurity experts were getting harder to come by. To help articulate the issue, she introduced the term "new-collar workers" — workers who have the relevant skill sets but not the educational backgrounds most HR departments and recruitment leaders normally require. [2] Traditional requirements (such as degrees and years of experience) do not account for the many different paths to achieving the same skills. In response, organizations are redefining and filling roles based on capability versus traditional measures.

Current CEO of IBM Arvind Krishna has expanded on this idea. [3]

> **Talent is everywhere; training opportunities are not. This is why we must take big and bold steps to expand access to digital skills and employment opportunities so that more people — regardless of their background — can take advantage of the digital economy. This will help democratize opportunity, fill the growing skills gap and give new generations of workers the tools they need to build a better future for themselves and society.**
>
> *— Arvind Krishna, CEO, IBM*

Kelli Jordan, IBM's director of career, skills and performance, has implemented this idea in IBM's hiring practice. [4]

> **It's not a traditional blue-collar job. It's not a traditional white-collar job. It's these new-collar roles that prioritize capability over a credential.**
>
> *— Kelli Jordan, Director of Career, Skills and Performance, IBM*

MSEs can adapt the same mindset toward hiring cybersecurity new-collar workers to help close the gaps that aren't addressed by managed services or current internal capabilities.

Analysis

Leverage Nontraditional Cybersecurity Education Sources

Companies keep increasing their investments in cybersecurity — and the demand for specialized resources with them — creating a very competitive cybersecurity talent market. [1] On top of that, a bachelor's degree is still considered a requirement by a majority of employers. [5]

Yet, degree programs are expensive: An undergraduate in the U.S. will accumulate, on average, $33,448 in debt, while a master's degree student will accumulate $80,494 in debt. [5] Student loan debt is becoming more pressing for those looking to enter the workforce, further narrowing the talent pool to people who have invested time and money in getting a degree, driving salary expectations even higher. MSEs typically cannot afford higher salary levels. However, there are alternative education paths that demonstrate experience and tactical know-how, providing MSEs a wider base of potential candidates.

> **Information security analysts typically need a bachelor's degree in computer and information technology or a related field, such as engineering or math. However, some workers enter the occupation with a high school diploma and relevant industry training and certifications.**
>
> *— U.S. Bureau of Labor Statistics*

Associate degree programs for cybersecurity and information security offer a knowledge base similar to what one can get through degree programs of four years or more, but are more geared toward being immediately useful in the workforce. They also cost significantly less than a bachelor's or master's degree program, making them an attractive option. Graduates of a two-year community college program are also certification-ready and may have previous IT experience.

Industry certifications are the most common way to show experience and understanding of cybersecurity. Certifications require varying levels of knowledge, ranging from basic understanding to tool- and use-case-specific knowledge. Some certifications, such as the Certified Information Security Systems Professional (CISSP), require a certain amount of time spent in the profession before being awarded (see Note 1 for examples of industry-recognized certifications). MSE technology leaders should prioritize training for new-collar workers. The opportunity to attain certifications by working for a MSE can be an incentive for new-collar workers looking to grow their cybersecurity skills.

Cybersecurity bootcamps and hackathons are accelerated programs (bootcamps are typically 16 weeks; hackathons last, at most, 48 hours). More often than not, they focus on network and security system administration, offering opportunities for up-to-date certifications while focusing on problem solving and proof of knowledge — two things MSEs value when sourcing cybersecurity talent.

Adapt Staffing and Hiring Processes to Allow for New-Collar Workers

Staffing and hiring practices must also be adjusted to source new-collar workers. Diversity of thought can help create a more mature MSE cybersecurity effort by embracing innovative approaches. MSE technology leaders should consider practical insight and experience in addition to academic knowledge. A technical evaluation, including incident response, can be included in the interview process to test this.

In conjunction with HR, MSE technology leaders should look to local talent pipelines specifically with new-collar workers in mind. The following groups can help gauge interest in current opportunities and match them to the level of skills that currently exist:

- Local technical schools (Note: If there is significant interest from local technical schools or cybersecurity bootcamps, MSE technology leaders can engage with school leadership teams to tailor the curriculum to meet their needs.)
- Veterans groups

- Groups representing underrepresented peoples in cybersecurity (such as women, people with disabilities, and racial and ethnic groups)
- Cybersecurity training and cyber range vendors (many are now collecting data on participants to help them find jobs)

Cybersecurity job descriptions are notoriously all-encompassing. MSE technology leaders need to remember that they are hiring for a specific role. When hiring a developer, MSE technology leaders specify in the job description which programming language they need (such as Python, C++, Java and JavaScript); this same specificity should be used when hiring for cybersecurity roles. Adopting this practice will help technology leaders identify the organization's specific needs (such as vulnerability management, monitoring and access management), which may contribute to any gap assessments they are conducting.

Support the Long-Term Growth of New-Collar Workers

Like any other type of external hire, new-collar cybersecurity workers will require certain resources to become viable, valuable members of the security function. MSE technology leaders should create a development plan that includes:

1. Support
2. Tool-specific training
3. A growth path

New-collar workers require support from within the organization. Coaching, sponsorship and mentoring by members of the organization will help solidify that growth path. Each of these relationships is valuable in its own way (see Table 1).

Table 1: Coaching, Sponsoring and Mentoring Relationships

(Enlarged table in Appendix)

Relationship Elements	Coaching	Sponsoring	Mentoring
Reporting	Formal manager-staff member relationship or requested to coach by manager	Formal manager-staff member relationship or a relationship outside the line manager-employee relationship	Takes place outside the line manager-employee relationship
Initiative	The coach directs the learning and instruction	The sponsored employee is in charge of learning	The mentee is in charge of learning
Focus	■ Developing skills individuals need for their current or next role ■ Enabling others to solve problems and make decisions ■ Engaging in dialogue by asking and listening	■ Providing career advocacy ■ Developing skills toward career advancement	■ Gaining professional development that may be outside the mentee's area of work ■ Enabling others to solve problems and make decisions ■ Engaging in dialogue by asking and listening
Length	Relationship ends as the individual transitions into a new role or masters the target skill	Relationship continues until career advancement or indefinitely	Relationship may last for a specific period (e.g., 12 months) or continue indefinitely

Source: Gartner

Likewise, new-collar workers will need to be trained on the MSE's toolset; two-year degree programs often use free versions of tools, which have limited functionality.

New-collar workers will also require advancement opportunities within the MSE. Because they have less degree-based education, these employees might be hired with titles such as junior security analyst, with a path to become a security analyst or senior security analyst when all internal competencies requirements have been met. A growth trajectory is important for the retention of new-collar workers.

Evidence

[1] IT Key Metrics Data 2024: Industry Measures — Insights for Midsize Enterprises

[2] The New Collar Workforce, IndustryWeek

[3] IBM Commits to Skill 30 Million People Globally by 2030, IBM Newsroom

[4] Average Graduate Student Loan Debt, Education Data Initiative

[5] How to Become an Information Security Analyst, Bureau of Labor Statistics

Note 1: Certification Examples

Examples of industry- recognized certifications include:

- Certified Wireless Security Professional (CWSP)
- Certified Ethical Hacker (CEH)
- Certified Information Security Manager (CISM)
- EC-Council Certified Security Analyst (ECSA)
- Certified Information Systems Auditor (CISA)
- CompTIA Security+ (SEC+)
- Certified Information Security Systems Professional (CISSP)
- System Security Certified Practitioner (SSCP)
- GIAC Security Essentials Certification (GSEC)

Document Revision History

Midsize Enterprises Must Embrace New-Collar Workers in Cybersecurity - 29 April 2022

Recommended by the Author

Some documents may not be available as part of your current Gartner subscription.

Midsize Enterprise IT Organizational Design: 3 Structural Archetypes to Meet Discrete Enterprise Needs

How Midsize Enterprises Can Exploit the NICE Framework to Secure Cybersecurity Talent

Tool: Identifying Adjacent Talent for Key Cybersecurity Roles

---

Table 1: Coaching, Sponsoring and Mentoring Relationships

Relationship Elements	Coaching	Sponsoring	Mentoring
Reporting	Formal manager-staff member relationship or requested to coach by manager	Formal manager-staff member relationship or a relationship outside the line manager-employee relationship	Takes place outside the line manager-employee relationship
Initiative	The coach directs the learning and instruction	The sponsored employee is in charge of learning	The mentee is in charge of learning
Focus	■ Developing skills individuals need for their current or next role ■ Enabling others to solve problems and make decisions ■ Engaging in dialogue by asking and listening	■ Providing career advocacy ■ Developing skills toward career advancement	■ Gaining professional development that may be outside the mentee's area of work ■ Enabling others to solve problems and make decisions ■ Engaging in dialogue by asking and listening
Length	Relationship ends as the individual transitions into a new role or masters the target skill	Relationship continues until career advancement or indefinitely	Relationship may last for a specific period (e.g., 12 months) or continue indefinitely

Source: Gartner

Actionable, objective insight

Position your organization for success. Explore these additional complementary resources and tools for midsize enterprise leaders:

Research

Strategies for Midsize Enterprises to Mitigate Insider Risk

See the risk of internal threats.

Download Now

Infographic

2024 CIO Agenda: A Midsize Enterprise Perspective

Explore the top priorities, technologies and challenges for midsize enterprises.

Download Now

eBook

3 Must Haves in Your Midsize Enterprise Cybersecurity Incide Response Plan

Find out how to be prepared for a cybersecurity incident.

Download Now

Roadmap

2024 Technology Adoption Roadmap

Benhmark your technology adoption and deployment plans.

Download Now

Already a client?
Get access to even more resources in your client portal. Log In

Connect With Us

Get actionable, objective insight that drives smarter decisions and stronger performance on your mission-critical priorities. Contact us to become a client:

U.S.: 1 855 811 7593

International: +44 (0) 3330 607 044

Become a Client

Learn more about Gartner for IT Leaders
gartner.com/en/information-technology

Stay connected to the latest insight

Gartner®