CISO HIRING GUIDE

ONBOARDING, ENGAGING, AND RETAINING HIGH-VALUE SECURITY PROFESSIONALS

TABLE OF CONTENTS

Onboarding Matters

The first question about onboarding is, "Why do it?"—especially when it comes to independently minded cybersecurity professionals known for their finely tuned corporate nonsense detectors. Statistics tell the tale. Recent research demonstrates that well-executed new-employee onboarding programs significantly influence employee retention and productivity.[1] The following are some of the findings:

- On average, formal onboarding programs increase the probability of long-term employee retention by **25%** and improve employee performance by **11%**.
- Employees participating in formal onboarding are **69%** more likely to stay employed at an organization for three years or more.
- **15%** of employees leaving an organization for another role cite the lack of an onboarding program as a reason to jump ship.
- **17%** of employees quitting an organization abruptly do so in their first week on the job.

The same study reports that it takes the average new employee 8 to 12 months to reach "cruising altitude" levels of productivity. Needless to say, what happens in the first few weeks of an employee's tenure influences whether she or he will "hit the ground running" and embark on a steady ascent, or a struggle out of the gate in an attempt to navigate a game of "chutes and ladders."

[1] Vinay Patankar, "6 Checklists to Perfect Your New Employee Onboarding Process," Process.st, February 2, 2018.

This installment of the CISO Hiring Guide series is focused on onboarding, the last step in the context of a six-phase cycle for attracting, selecting, and engaging high-performance cybersecurity professionals:

1. **Defining and Writing Effective Job Descriptions**
2. **Mapping Out a Job Posting Campaign Strategy**
3. **Screening and Shortlisting Strong Candidates**
4. **Interviewing as Two-Way Communication Process**
5. **Selecting and Vetting the Winning Candidate**
6. **Onboarding, Engaging, and Retaining High-Value Security Professionals**

Including onboarding in this sequence—occurring after the hiring decision and new employee's acceptance of an offer—positions it as a form of follow-through as natural and as necessary to a successful recruiting action as it is to keeping your eye on the ball when swinging a golf club or tennis racquet.

Employees participating in formal onboarding are 69% more likely to stay employed at an organization for three years or more.[2]

[2] Ibid.

Macro- and Micro-Onboarding Processes

The objective of onboarding is to ensure that new employees feel welcomed, prepared, supported, and enabled. Large organizations have the resources to stage elaborate onboarding programs that can last several days or even weeks. Smaller organizations don't have the staff or the funds, even if they recognize the importance of this "luxury." For them, onboarding might consist of an hour or two in the HR department completing pre-employment paperwork, badging, a quick tour of the facilities, and an introduction to the new employee's manager.

Regardless, of available resources, a primary aspect of the onboarding process is not a matter of funds but one of "caring:" managers should periodically check in with new hires to ascertain whether they have questions or concerns. That can be as simple as periodically asking, "How are you doing?"

In their first few days on the job, cybersecurity staff should experience both a macro-introduction to the organization as a whole and a micro-survey of the organization's cybersecurity risk factors, objectives, current threat environment, security program, tools, and processes. This guide proposes a two-track onboarding program—first, a macro view of what an organization should provide to all new professional-level employees, and second, the nitty gritty of what cybersecurity staffers need to know.

Onboarding ensures that new employees feel welcomed, prepared, supported, and enabled.

Macro-Onboarding Checklist

To begin, onboarding programs for new cybersecurity employees should follow a formal checklist of briefing topics and activities. This works to build repeatable and consistent onboarding processes. There are four primary elements involved in the macro-onboarding process:

1. Paperwork, Functional Basics, and Amenities
2. IT Tools, Processes, and Security
3. Meet the Company
4. Meet the Team and Cybersecurity Specifics

The first three activities are at the company level; the last one occurs at the departmental level.

It's the first three months that define a successful onboarding; that's when organizations lose 17% of their new hires.[3]

[3] Allison M. Ellis, et al., "Your New Hires Won't Succeed Unless You Onboard Them Properly," Harvard Business Review, June 20, 2017.

1. Paperwork, Functional Basics, and Amenities

The idea here is to handle and complete the boring tasks first. Conducted by the HR department, this is the first thing new employees will do on their first day at work. This session normally takes place in a conference or larger meeting room, depending on the size of the group joining the organization on that day. Items covered include I-9 employment eligibility, 1098 tax withholding, workspace assignment, benefits sign-up, payroll/direct deposit forms, stock options/profit sharing programs, equipment issuance (computers, phones, VPN tokens, etc.), employee ID and facilities access cards, and network account and initial password log-in information. In addition, this session gives participants the opportunity to meet other recently hired employees from across the company and begin building professional relationships within the organization.

Information on amenities covers workplace facilities features, recreational resources, intra-company social opportunities, and the general sequence of all-hands and departmental meetings. This briefing should also include an introduction to the organization's intranet and an overview of the organization's event calendar, including sales close dates, quarterly earnings quiet period, and announcement dates.

2. IT Tools, Processes, and Security

Conducted largely by a representative from the organization's IT department, this classroom session focuses on how to access and use the organization's electronic resources. This should include an overview of the organization's:

- Intranet-based employee directory
- Benefits
- Expense reporting
- Purchasing
- Workflow management
- Employee performance management
- Other resources as appropriate

Content presented in this session shifts from "what exists" to "how-to" information on accessing IT-provisioned and other essential resources. Information includes instruction on how to use the organization's:

- Teleconferencing
- Remote/VPN access
- Cloud apps and storage
- Online office tools such as email, messaging, word processing, spreadsheet, presentations, storage and backup, etc.

This session should also address how to request IT-department help and details on trouble-ticketing processes.

New employees should also receive a briefing on the organization's cybersecurity policies and practices. This is a key opportunity for the new employee to get an overview of the organization's policies regarding:

- Network access privileges for employee-owned devices
- Cybersecurity hygiene do's and don'ts
- How to recognize and report potential indications of compromise
- Physical security practices (e.g., preventing laptop theft, access card loss, unauthorized facilities access)
- Personal security, including parking and transit, fire and emergency procedures, emergency phone numbers, and communications, etc.

3. Meet the Company

Depending on an organization's size, configuration, objectives, and resources, the onboarding process should also include briefings on the organization's business agenda. Unlike the past, when IT was isolated from many of the day-to-day operations of an organization, these meetings are particularly important for new employees hired by the CISO. They present an ideal opportunity for a new employee to gain context for specific needs in the new organization and allow him or her to become an active participant in the company. These briefings are best conducted by executives or senior staff and can address topics such as:

- **Organizational Overview, Mission, Vision, and Values.** Ideally, this is a dedicated session with the CEO or another member of the senior management team.
- **Sales.** This covers organizational structure, sales channels, partner programs, quarterly sales cycles, and how audience members can support the sales organization. Either the CEO covers this topic, or the head of sales or a designated member of the sales team.
- **Marketing.** This session discusses company positioning, market strategy, initiatives and programs, event marketing, and corporate communications programs, including media relations, analyst relations, and social media.
- **Finance.** This covers the organization's financial condition, day-to-day operations, expense management systems and policies, and investor relations.

Additionally, depending on the market segment and business, other macro-onboarding elements may include presentations or a panel discussion from manufacturing, operations, research and development, engineering, compliance, public relations, community relations, or the legal counsel.

4. Meet the Team and Cybersecurity Specifics

At this point, the CISO or other leader will informally introduce the new employees to other team members and give them time to get set up in their work spaces. From there, it's become something of a tradition to take the new member out to lunch with other team colleagues to help "break any social ice" and welcome the new colleague to the group. The employee's supervisor should also schedule a one-on-one meeting with the new team member on their first working day to cover team organization, roles and responsibilities, team objectives, and current projects and initiatives. This is also a good time to schedule an ongoing one-on-one for the rest of the year. Not only does this imply accountability, but it also allows the new employee to see himself or herself as a valued member of the CISO's team. Here, the supervisor should introduce how the organization's employee performance management and evaluation process works and discuss the new employee's first assignments and tasks.

It is important to note that meeting the team or fulfillment of any or all of these onboarding tasks should not indicate completion of the onboarding process. Onboarding, if it is to be effective and promote long-term benefits, does not end after a few days or weeks—or even a few months. Research shows that successful onboarding can take as long as a year if the organization is going to capitalize on the new employee's skills, knowledge, and even enthusiasm.[4] This is especially true of the CISO's team, which is constantly under pressure to ensure that company assets and systems are protected. As the saying goes, "Rome wasn't built in a day." And neither is the onboarding process for the new employee.

[4] Sara Stibitz, "How to Get a New Employee to Speed Up," Harvard Business Review, May 22, 2015.

Micro-Onboarding: Cybersecurity Specifics

Although much of the following will undoubtedly enter the discussion during the pre-employment recruiting process, new members of the cybersecurity team should receive a formal briefing covering the organization's cybersecurity posture and programs. New members should also be briefed on how their roles and responsibilities mesh with those of other teams and the greater organization. Topics should include:

- **IT Overview.** The role of IT in the organization's value creation processes. General layout and structure of the organization's network and IT infrastructure, as well as cloud and outsourced computing resources and services.
- **Organizational Cybersecurity Risk Factors.** What are the organization's "family jewels" that the cybersecurity organization needs to protect? What elements of the organization's infrastructure and business processes are particularly vulnerable to attack?
- **Threat Environment.** Who and what poses significant threats to the organization. How the cybersecurity group monitors them and stays current with emerging threats and intelligence.
- **Objectives.** How the organization as a whole defines "good security." Key Performance Indicators (KPI) and attainment goals. Progress and status in meeting these goals.
- **Compliance Standards and Mandates.** Any specific compliance regimes and government mandates the organization has committed to observe such as Payment Card Industry, General Data Protection Regulation, Federal Information Security Management Act, Common Criteria, etc.
- **Currently Deployed Technologies and Tools.** Hardware and software cybersecurity products installed in the network and infrastructure, managed security service providers and their specific duties and responsibilities to the organization, and software-as-a-service (SaaS) licensing subscriptions.
- **Processes and Procedures.** Day-to-day security processes, checklists, and dashboards. Software update and patching. Who is accountable for which responsibilities? How to make change happen and ensure that strategies are aligned and positioned with business requirements and goals? How often should processes and procedures be reviewed and evaluated?
- **Intrusion Prevention and Breach Detection Procedures.** Processes for monitoring and identifying potential threats and suspicious activities, prevention responses, and reporting. Breach detection processes and responses. Reporting breach information within the cybersecurity team and to responsible organization executive. Public and external communications and reporting procedures.
- **Employee Role, Responsibilities, and Team Relationships.** "Who's who" in the cybersecurity organization. How the new member fits in the cybersecurity organization and relationships with colleagues. Current and future expectations of employees.

The CISO should keep in mind that the onboarding process is an ideal opportunity for her or him to highlight to new team members why they are essential to the mission of the team and how their roles and responsibilities are critical to the short- and long-term success of the greater organization. For example, the CISO should consider creating 30-, 60-, and 90-day (and even annual) plans that include measurements and feedback to track a new employee's performance and contributions to the team and organization as a whole. This can help to instill a sense of ownership in the new employee as well as underscore the employee's current and future value to the organization.

An Architecture that Addresses the Security Skills Shortage

Even if you build a great security team with the help of our CISO Hiring Guide series, you will still struggle to cover all of the security threats across the attack surface and to deal with the complexity resulting from point products and evolving compliance requirements. The result is a security posture where you constantly find yourself playing catch-up.

But there is good news. The Fortinet Security Fabric introduces a security architecture that helps you to optimize and scale your security teams to address these challenges by seamlessly integrating all of your security elements and unlocking automation capabilities for compliance and other time-intensive manual workflows. For more information on the Fortinet Security Fabric, check the eBook, "Security Transformation Requires a Security Fabric."

www.fortinet.com