Whitepaper

# A Guide to Soft Skills for Cybersecurity Leaders

OffSec
The Path to a Secure Future™

# 1 Soft Skills: An Essential Requirement for Cybersecurity Leaders

If you are a cybersecurity professional, you probably have a strong technical background. You likely have extensive knowledge about threat actors and their tactics, techniques, and procedures (TTPs). You understand the processes and technologies needed to protect information assets and detect and respond to cyberattacks.

As a cybersecurity leader, you need more soft skills than managers in most business functions.

However, if you want to succeed and grow as a cybersecurity manager or executive, you need to maintain your technical proficiency while mastering a range of soft skills that may have played only a minor part in your previous roles. These skills are essential to helping you perform key management activities such as obtaining resources, setting priorities, and building and motivating teams.

In fact, as a cybersecurity leader, you need more soft skills than managers in most business functions. Cybersecurity is a complex, fast-changing field where no one person can know everything that needs to be done and how to do it. That means that collaboration, effective teamwork, and good planning are essential for success. Moreover, cybersecurity managers today need to communicate with – and often persuade – an expanding list of stakeholders, including other business executives, top management and boards of directors, business partners, and auditors and regulators.

# 2 What Are Soft Skills?

One definition of "skill" on merriam-webster.com is "a learned power of doing something competently: a developed aptitude or ability."

Definitions of "soft skills" vary somewhat, but they are generally understood as non-technical skills that are useful across multiple business domains, including personal qualities that enable people to communicate with and lead others effectively.

In this paper we will consider two categories of soft skills. One is non-technical management skills that might appear on a job description, such as communication, goal setting, and team building. The other is personal qualities that enable managers at all levels to succeed, such as empathy, creative problem-solving, and leadership. Our goal is to help you develop skills and learn techniques that will make you a more effective manager of cybersecurity professionals and processes.

Our goal is to help you develop skills and learn techniques that will make you a more effective manager of cybersecurity professionals and processes.

# 3 Non-technical Management Skills

**Communication (upwards, sideways, and downwards)**
Communication within technical teams tends to focus on explaining clearly what tasks need to be performed, how to perform them, and when they need to be done.

Cybersecurity leaders need to communicate a lot of whats, hows, and whens, but also a lot more *whys, as in why are you doing these things instead of others? and why should I/we help you?* For example:

**Communication upwards,** to higher level managers and executives, often consists of answering questions about activities and plans (why are you doing these things instead of others?) and justifying requests for resources *(why do you think this would be a good investment?)*.

**Communication sideways,** to peer level managers inside the IT organization and business managers outside, frequently involves negotiating cooperation and mutual exchanges of support or resources *(why should I/we help you on this project?)*.

**Communication downwards,** to the teams you are managing, needs to include information and ideas to build a positive culture and motivate team members *(why should I give you my best efforts?)*.

Cybersecurity leaders need to communicate a lot of whats, hows, and whens, but also a lot more *whys, as in why are you doing these things instead of others? and why should I/we help you?*

None of this is rocket science, but answering why questions requires:

- Thinking systematically about the needs and desires of other parties and what your plans/requests/proposals/suggestions can do to help them achieve their objectives.
- Summarizing the details of your plans/requests/proposals/suggestions into language the other parties understand and objectives they value.
- Negotiating agreements on mutual commitments.

Fortunately, these are practices and skills that you can study and cultivate.

## Building an effective culture

A corporate, organizational, or team culture is the set of attitudes and procedural norms that define the work environment for that group of people. The term "culture" can sound rather vague, but anthropologists have found that cultures, including those in business organizations, involve mutually understood rules and expectations with tremendous influence on behavior.

And cultures can change when driven by external pressures, internal dynamics, and new leadership. Cybersecurity leaders have a big stake in guiding their teams toward a more effective culture, one that encourages collaboration, openness to new ideas, respect for all colleagues, and dedication to achieving the goals of the security group and the organization as a whole.

Although "culture building" sometimes involves executives spouting pie-in-the-sky platitudes, it certainly doesn't have to. Agile development practices, continuous improvement processes, Kaizen, and Total Quality Management (TQM) programs all provide rigorous methodologies that promote collaboration, experimentation, capturing input from all team members and stakeholders, and communicating positive organizational values. If you do a bit of research, you can find very hard-headed, practical methods for developing this "soft" skill.

> One of the most important aspects of corporate culture is the propensity for collaboration within and across teams. But collaboration is far from automatic, especially when security professionals have different motivations and approaches to their jobs. To learn practical strategies cybersecurity leaders can use to break down barriers and foster collaboration between security teams, watch the OffSec webinar The Art of Collaboration in Security: Breaking down barriers between Offensive and Defensive teams.

### Aligning goals with business strategy

Cybersecurity teams spend most of their time working toward goals that are established for them, such as finding and remediating vulnerabilities, responding quickly to incidents, and implementing new security technologies.

But part of the job of cybersecurity leaders is to set and prioritize goals that align with business strategies. This involves:

- Focusing existing cybersecurity activities on tasks that maximize risk reduction, taking into account damage to reputation as well business interruption and the loss of confidential information.
- Enabling the organization to pursue its new business and technology initiatives without compromising security.

In a broad sense, cybersecurity leaders should understand the organization's competitive advantages and ensure that the cybersecurity group works to protect them. For example, if the organization competes based on low costs and low prices to its customers, preventing interruptions to business processes may be a critical goal. If the organization succeeds through innovation, protecting intellectual property such as engineering designs or proprietary software might be paramount. If the organization relies on ecommerce systems that deliver a superior user experience, website uptime and securing customer data might be the best use of scarce security resources.

To align goals with business strategy, cybersecurity leaders need to learn how to think strategically about the organization's competitive advantages and directions, and how to work with security teams to understand the best ways to support them.

In a broad sense, cybersecurity leaders should understand the organization's competitive advantages and ensure that the cybersecurity group works to protect them.

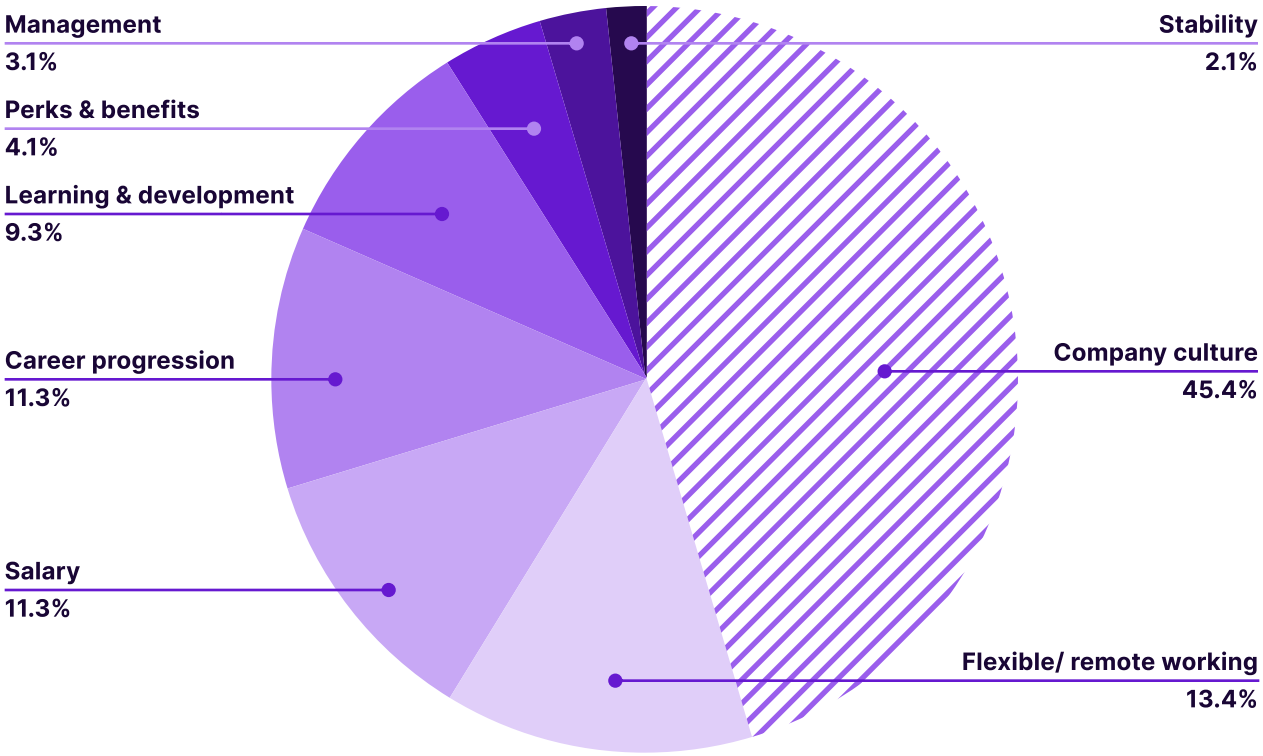
### Building teams and retaining staff

One of the biggest challenges cybersecurity leaders face today is recruiting and retaining experienced security professionals.

Offering competitive compensation is important, but numerous surveys and research studies have shown that non-monetary factors have an even greater impact on attracting and retaining IT staff. For example, a survey by hackajob, a recruiting company, found that four of the top five reasons IT personnel stay with their employer do not involve direct compensation:

| | |
|---|---|
| **Company culture** | **(45.4%)** |
| **Flexible/remote working** | **(13.4%)** |
| **Salary** | **(11.3%)** |
| **Career progression** | **(11.3%)** |
| **Learning and development** | **(9.3%)** |

What do you love about your current company and what makes you stay?




Other studies have highlighted the impact of areas like recognition for good performance, diversity, confidence in management, and organizational mission.

As a cybersecurity leader, you can have a tremendous impact on the success of your organization by understanding the professional and personal needs and desires of your team members (informal conversations and structured job satisfaction surveys are both good methods) and by directing resources toward meeting them.

> An OffSec blog post, The Role of Continuous Learning in Retaining Cybersecurity Experts, discusses continuous learning as a staff retention strategy and suggests several practical steps you can take create a learning culture, offer attractive learning options, encourage mentorship and knowledge-sharing, and continuously measure the impact of learning.

# 4 Personal Qualities of Successful Cybersecurity Leaders

### Active listening and empathy

As we noted earlier, cybersecurity is a complex, fast-changing field where no one person, however smart and experienced, can know everything that needs to be done and how to do it. That's why you need to practice active listening: drawing out other people, processing their ideas and suggestions non-judgmentally, and confirming mutual understanding. This includes mastering techniques such as listening to understand (rather than respond), noticing body language and non-verbal cues, asking open-ended questions, and restating and reflecting ideas back to the other person.

You need to practice active listening: drawing out other people, processing their ideas and suggestions non-judgmentally, and confirming mutual understanding... Of course, this doesn't mean you need to agree with everything others say or adopt all their ideas.

Of course, this doesn't mean you need to agree with everything others say or adopt all their ideas. Part of a manager's job is to say "no" or "not yet" quite often. But you want to be able to absorb data and good ideas from everyone in your organization, and when you can't use them immediately, explain why.

Good active listeners cultivate empathy. That includes striving to understand the other person's perspective, withholding judgment until you have heard them out, and ensuring that your own biases are not interfering with objectivity. It also means recognizing and taking account of non-rational motivations.

You can find a lot of very practical techniques on the web for practicing active listening and employing empathy. A few good introductions: Qualities of a Good Listener; Building Communication Skills: 9 Types of Listening; 15 Key Tips For Developing Active Listening Skills As A Leader. Not only will these improve your information gathering and decision making, they will also build your credibility as a manager who can engage and motivate teams.

### Creative problem-solving

Most cybersecurity professionals are exceptionally good at solving technical problems where the objectives are clear and results can be measured. But as management responsibilities grow, they are increasingly faced with the need to satisfy multiple stakeholders with unclear and competing objectives and subjective metrics. On the other hand, as managers, they often have increased latitude to try innovative approaches and draw in additional resources.

Creative problem-solving skills include:

- Identifying the root causes of problems
- Clarifying or redefining goals and objectives
- Generating innovative ideas
- Using testing, experimentation, and prototyping to refine ideas and uncover alternatives
- Communicating the benefits of innovations to build consensus and secure additional resources to implement solutions

Many authorities in this area have highlighted the importance of harnessing both divergent thinking (exercises like brainstorming and ideation that generate many potential solutions) and convergent thinking (techniques to leverage the knowledge and skills of teams and controlled experimentation to identify the most promising options).

Again, as a cybersecurity leader, you can find proven practices and tools that strengthen creative problem-solving in both individuals and teams. Here are three examples: Problem Solving as a Manager; What Is Group Problem-Solving?; Why Problem-Solving Skills Are Essential for Leaders in Any Industry.

Many authorities in this area have highlighted the importance of harnessing both divergent thinking (exercises that generate many potential solutions) and convergent thinking (techniques to identify the most promising options).

### Leadership and "servant leadership"

The word "leadership" has many meanings, but we'd like to highlight three aspects especially relevant to cybersecurity leaders.

The first is setting examples and modeling behavior for members of the group. Leaders who exhibit personal qualities such as open-mindedness, creativity, initiative, resourcefulness, integrity, and fairness encourage others to act in the same way.

The second is helping to imbue work with meaning and purpose beyond merely earning a paycheck. Meaning can derive from "making the world a better place." But leaders can also remind their teams that their activities at work make life better for customers or their community. Or that they are supporting their teammates and colleagues. Or are blazing new paths and demonstrating excellence in their profession. Or that they are fighting evil (that's what cybersecurity teams do, right?). These reminders don't need to be pretentious or heavy-handed, but a little bit can go a long way toward giving people a reason to do a good job and draw more satisfaction from their work life.

A third critical aspect of leadership is leadership style. Here we want to suggest that cybersecurity leaders investigate the concept of "servant leadership." In complex, fast-changing environments, a command and control leadership style won't be effective, because no one person knows enough to direct and micro-manage the members of a team, much less a larger group or organization. According to the principles of servant leader, leaders should instead provide direction and guidance, but otherwise see their job as making sure teams have the skills, resources, and processes they need to analyze problems, devise solutions, and implement the solutions. Servant leaders also focus on obtaining additional resources from upper management and negotiating working agreements with peer-level managers in other groups (see our discussion of communication, above). There are good articles and books on servant leadership in the Agile community. If you are interested in the idea you can start with a case study that illustrates many of the principles we have been discussing here: A Natural Servant Leader Unlocks the Power of Employees at a Global Contact Center.

# Conclusion

If you are a cybersecurity leader, you can use soft skills to dramatically improve the performance of your teams. The relevant soft skills are not innate or unteachable. On the contrary, skills related to communication, culture building, goal setting, team building, active listening, creative problem-solving, leadership, and similar topics can be learned and practiced by any intelligent person. A wide variety of blogs, books, and videos are available that explain key principles and structured techniques in all those areas. Cultivating these skills will not only make you better at your job, it will enable you to make greater contributions to the success of your organization and increase your own job satisfaction.