AUGUST 2022

CLOSING THE REVOLVING DOOR:

A Research Assessment of Factors Contributing to Cybersecurity Employee Turnover and Retention

Authored By:
Dr. Kathryn McIver, Researcher, ICIT

ICIT | Institute for Critical Infrastructure Technology
The Cybersecurity Think Tank

Closing the Revolving Door

A research assessment of factors contributing to cybersecurity turnover and retention

August 2022

Contents

Introduction

One of the most pressing topics in the cybersecurity industry is the talent shortage. In a January 2022 report evaluating diversity in cybersecurity, MITRE reported an estimated 3.1 million open cybersecurity positions globally, with 350,000 to 600,000 of these openings based in the U.S. (Lachow, 2022). Additionally, the Bureau of Labor Statistics (BLS) projected 33% annual job growth for information and cybersecurity professionals between 2020 and 2030 (U.S. BLS, 2022). Combined with President Biden's urging to "harden your cyber defense immediately," both public and private sector cybersecurity leaders are investing resources to immediately close the cyber talent gap.

In this paper, cyber talent is defined as professionals who have the necessary skills to maintain information or cyber systems security by preventing and neutralizing intrusions, mitigating the impact of cyberattacks, developing strategies and tactics to protect intellectual property, gathering intelligence for law enforcement or national security issues, or support cybersecurity programs, such as penetration testing or forensic activities.

Both private and public sectors have launched wide-sweeping efforts to increase the cyber talent pool by implementing programs to incentivize cybersecurity as a profession, developing public-private-academic partnerships, and increasing diversity in training and recruiting programs (Vogel, 2016). However, increasing the number of skilled professionals addresses only one aspect of the talent shortage. Retaining the employee once the professional is hired and trained is equally essential. Another way to think about the relationship between recruiting and retention is that recruiting is when the industry proactively makes a coordinated effort to develop and hire additional professionals. Conversely, retention is when employers reactively invest in keeping employees once hired.

This paper explores current, empirical research evaluating the factors contributing to cybersecurity employee retention or intent to leave. While there is overlap between recruiting and retention activities, this paper focuses solely on retention to provide cybersecurity leaders with recommendations to increase retention within their organizations.

This paper was developed using the Samueli Institute Rapid Evidence Assessment of the Literature (REAL) methodology. The REAL methodology utilizes a streamlined approach to a systematic review and incorporates subject matter expert viewpoints into the final recommendations (Crawford et al., 2015). Systematic reviews support strategic decisions by bridging the gap between research information and knowledge using subject matter expert perspectives. The expert opinions leveraged in this study are a composite of ICIT Fellow's dialogue and narrative captured during ICIT events, such as briefings, roundtables, and working groups. The conclusions of the REAL literature review were developed using a constructivist viewpoint which posits that "… human beings construct meanings as they engage in the world they are interpreting" (Behling, 2019, p. 7). A constructivist interpretation allows for translation via context and industry dynamics. Limitations of this study include inadvertently excluding insightful literature and researcher bias, as a sole author prepared this paper.

Background

As previously discussed in the introduction, the cybersecurity skills gap is a pressing global and national concern across all industries and sectors. The overarching problem is the vulnerability exposure due to the severe shortage of trained professionals (Parker, 2016; Pierce, 2016). This exposure can result in loss of profits and reputation, attacks on intellectual property and sensitive data, and disruptions to critical infrastructure (Pierce, 2016). Because there is a shortage of new cybersecurity professionals, it is vital that cybersecurity leaders, and arguably all executives, invest time and resources in retaining current employees.

The key driver for employee retention is the employee's commitment to the organization. When evaluating talent retention strategies for cybersecurity roles, Burrell et al. identified three significant types of organizational commitments that influence cybersecurity professionals (2020):

- Affective commitment is when the organization's mission and goals resonate with the professional personally.
- Continuance commitment occurs when professionals feel they have made a significant investment of either time or effort to the organization.
- Normative commitment is where the professional feels an obligation to the organization.

Influencing a professional's commitment to an organization directly impacts employee retention. Thus, effective cybersecurity leaders must understand and evaluate their employees' commitment to the organization when making retention decisions.

Another layer to the retention problem is the Great Resignation. In March 2022, the BLS reported that 4.5 million Americans quit their job in November 2021. The Great Resignation impacted all U.S. industries, compounding the strain on already understaffed cybersecurity programs. As such, an ongoing concern is the increased levels of burnout associated with remaining employees (Sheather & Slattery, 2021). This working environment generally results in a feedback loop where the additional strain and burnout may contribute to existing employees' intent to leave. Additionally, increasing workload and burnout may also increase turnover, creating an amplified demand for cyber talent. However, the economist Serdar Birinci cautions leaders against viewing the Great Resignation in a negative context but rather as the "Great Reallocation." He further urges leaders to remember that job switching stimulates resiliency in the workforce and the Great Resignation is an opportunity to recruit experienced employees or reskill existing workers (Birinci 2022).

In addition to the Great Resignation, leaders are grappling with the cybersecurity implications of the COVID-19 pandemic. After the initial outbreak, the FBI reported a 600% increase in successful attacks. Much of this volume is attributed to the sudden shift to remote work and the resulting increased employee vulnerability. In addition to the increase in attack volume, leaders have faced two pandemic-specific challenges: the disruption of effective cyber-hygiene training for new employees, which may increase human-element vulnerabilities, and the increased need for skilled workers in response to the surge in attacks (Borkovich & Skovira, 2020). The increase in job mobility and the demand for cybersecurity during and post-pandemic could make even a fully staffed, engaged cybersecurity department feel like they were facing insurmountable hurdles.

Research Assessment and Findings

A recurring theme throughout the research is the need for cybersecurity leaders to recognize the difference between intrinsic and extrinsic motivators. The concept of intrinsic and extrinsic motivation stems from Hertzberg's Two Factor or Motivator-Hygiene theory. Extrinsic motivators originate from an external source, like an employer, while intrinsic factors, such as job satisfaction, come from within the employee (Wan Yusoff et al., 2013). In this analysis of cybersecurity professionals, three of the five findings relate to intrinsic motivation. Thus, cybersecurity leaders must critically evaluate their organization's effectiveness at supporting intrinsic motivators.

This paper will start by examining three intrinsic factors: personal connection, self-efficacy, and a sense of camaraderie. Then, it will examine the two extrinsic factors: monetary recognition and role stressors.

Factors Influencing Cybersecurity Employee Retention

Personal Connection to Role

The most significant finding from this analysis is that the individual's connection to the role is a vital determinant of their retention. A personal connection can manifest as a sense of duty or be motivated by public service, personal interest in the work, or a desire for variety (Burley, 2011; Burrell et al., 2020; Haney & Lutters, 2019). While vastly different in execution, both a connection to mission and personal interest in the work are findings that leaders can use to develop messaging to motivate employees to stay. For example, a positive relationship between the organization's mission and the individual's preferred mission lower an employee's intent to leave (Burley, 2011; Haney & Lutters, 2019). In their research exploring management techniques for young cybersecurity professionals, Burrell found that millennials "…watched the reemergence of the American Hero" and are motivated to emulate this role model (2018). If leaders describe the organization's mission in terms that resonate with employees, they may feel an affective commitment to the organization.

Personal interest and a desire for variety at work are characterized by intellectual stimulation. While personal interest is the primary determinant for professionals entering the field, evidence indicates that employees interested in interdisciplinary work and multifaceted challenges tend to stay at organizations that provide them with opportunities to leverage these interests (Haney & Lutters, 2019; Orye & Faith-Ell, 2020). Once attracted to the role because of personal interest, diverse work challenges maintain excitement and foster a strong bond between the employee and the organization (Haney & Lutters, 2019; Orye & Faith-Ell, 2020; Osborn, 2015). Leaders can capitalize on this finding by diversifying role tasks or developing a rotation program that stimulates employees' intellect, thus avoiding employees feeling job stagnation.

Self-Efficacy

The next most-significant determinant of employee turnover is a sense of self-efficacy, which is the employee's feeling of control or autonomy over their professional progression (D. Burrell, 2018; D. N. Burrell et al., 2020; Dodge et al., 2012; Haney & Lutters, 2019). This finding overlaps with the desire for variety in work roles, as providing employees with personal and professional growth opportunities also allows them to diversify work tasks. Cybersecurity professionals are accomplishment focused, so if they feel they are not progressing at their desired rate, they will seek employment elsewhere (Burrell, 2018). As such, self-efficacy factors increase the professional's affective and continuance commitments to the organization.

Unfortunately, Burrell also found that cybersecurity managers exhibit an attitude of "paying your dues or that the only opinions worth listening to should come from someone with extensive work experience" (2018). This managerial attitude conflicts with the typical cybersecurity professional's "let me try and solve this problem" mindset (Burrell 2018). A large part of self-efficacy is an employee's self-confidence in his or her ability to develop knowledge, skills, and capabilities. Encouraging employees to share their analysis and interpretation of a problem, independent of experience level, may foster a feeling of self-efficacy and contribution to the team (Haney & Lutters 2019).

Sense of Camaraderie

Another intrinsic motivator that influences cybersecurity employee turnover is a sense of camaraderie, defined as a deep feeling of trust and friendship with coworkers rather than just a collegial working relationship. This finding is counter-intuitive to a commonly held belief that cybersecurity is a solitary profession and that employees attracted to these roles are lone wolves (Haney & Lutters, 2019).

When evaluating cybersecurity professionals' turnover intention, Sugiono et al. found that workplace relationships were the highest indicator of job satisfaction (2021). A sense of belonging shared with people who identify with an organization's mission is personally satisfying and vital for cross-functional collaboration (Haney & Lutters, 2019). Encouraging cross-functional collaboration and socialization allow employees to develop meaningful relationships and participate in diverse work assignments.

Monetary Recognition

No discussion of cybersecurity professionals would be complete without a high-level discussion of monetary recognition. The results of this research assessment challenge the conventional wisdom that tells leaders that extrinsic motivators such as compensation or benefits packages are a primary motivator for seeking other employment opportunities. Of note, in the studies that identified compensation as a retention factor, compensation was universally the least impactful (Burrell et al., 2020; Haney & Lutters, 2019). While monetary rewards were essential in the initial recruitment of staff, they did not serve as motivation for long-term retention (Orye & Faith-Ell, 2020).

Haney and Lutters reported a pragmatic viewpoint on the importance of compensation to cybersecurity professionals: "The way people indicate that you're providing real value to them is paying you."(2019). This pragmatic approach aligns with Hertzberg's observation that employees require extrinsic motivators to be motivated by intrinsic factors. More simply put, extrinsic motivators are the cost of admission (Wan Yusoff et al., 2013). Thus, if employers pay their cybersecurity professionals a fair wage, compensation is not a primary factor for employees seeking other employment. The use of compensation and other extrinsic motivators as effective recruiting tactics is outside the scope of this paper.

Role Stressors

While the evaluated literature offers insights into factors that decrease turnover, a final finding in this analysis is that role stressors, such as ambiguity increase an employee's intention to leave (Burley, 2011; D. Burrell, 2018; Vogel, 2016). A 2014 KPMG survey indicated that SOC analysts have a higher "churn rate than other I.T. and cybersecurity professionals (Vogel, 2016). Of note, there are conflicting findings related to the role that ambiguity plays. Significant evidence indicates that employees value variety in their role; however, the literature also indicates that employees value clear expectations and role definition, to the point that the absence of clear expectations is a contributor to employee turnover (Burley, 2011; D. N. Burrell et al., 2020; Sugiono et al., 2021). Increasing regular communication between employees and leaders may mitigate concerns about unclear expectations.

Another role stressor is physical working conditions. Both Sugiono et al. (2021) and Osborn (2015) documented physical working conditions, such as access to natural light, as considerations for employee turnover. Likewise, Orye and Faith-Ell discuss the value of working conditions and access to ergonomically appropriate equipment as a factor in intent to leave (2020). Evaluating the physical working conditions for psychological impact and appropriately modifying them is a direct intervention that does not impact an organization's cybersecurity strategy or employment policies and practices.

General Recommendations for Leaders

First, since intrinsic motivation is key to retaining employees while extrinsic motivators are more easily quantified for recruiting, organizations should take a phased approach. The recruiting team should focus on extrinsic factors, while internal leadership should focus on understanding the employee's intrinsic motivation. In addition to the above overall strategy recommended by the research, the literature suggested two strategies for retaining employees while addressing the factors driving the intent to leave: developing career paths and integrating gamification.

Develop Career Paths

Leaders should work with their employees to develop career paths that leverage cross-training and professional development. Doing so may address the professional's need for self-efficacy, intellectual stimulation, and career progression while enabling camaraderie. For example, the Air Force developed a hybridized accession model to balance long-term retention, program development, and a staffing mix between experienced and developing airmen. Following this, the rolling retention rate for the Air Force Cyber Units decreased, though the accession model may not be the sole contributor to the trend (Parker, 2016).

One of the reasons it is challenging to develop a more formal approach to career progression is the rapidly changing nature of the cybersecurity industry, as specific work roles continue to evolve based on emerging threats and technologies (Dodge et al., 2012). However, developing competency in core skills such as engineering, mathematics, human behavior, management, and creative thinking are transferable and applicable as the industry continues to evolve.

Integrate Gamification

Gamification is emerging as an effective tool for generating interest in cybersecurity as a profession for K-12 and college-aged students (Burrell et al., 2020; Estes et al., 2018; Orye & Faith-Ell, 2020). Shyam Nivedhan and Priyadarshini propose gamification as a retention tool because it supports intrinsic motivators such as ongoing learning and development, employee engagement, and professionalism (2018). Of note, some organizations use gamification as a vetting tool to assess cybersecurity skills during recruitment (Vogel, 2016). Including gamification in an organization's retention strategy could create a personal connection to the role and career progression by providing a structured avenue to expand skills beyond the professional's current roles and responsibilities.

While the benefits of integrating gamification into the employee experience are impressive, there are limitations to leveraging this tactic. The primary limitations are the lack of awareness of gamification and leadership skepticism about the benefits of investing in a gamification solution (Shyam Nivedhan & Priyadarshini, 2018). Of note, gamification in this context does not solely refer to video game experiences but also includes hack-the-box, scenarios, simulations, cyber ranges, or capture-the-flag training that utilizes points or a ranking system.

Conclusions

To find the contributing factors to cybersecurity employees' intent to switch organizations, this paper performed a rapid evidence assessment of relevant empirical literature to summarize research findings. Based on the conclusions from this assessment, there are five trends that cybersecurity leaders need to be aware of:

1. Employees need a personal connection to the role
2. Employees need self-efficacy
3. Employees value a sense of camaraderie
4. Monetary rewards are not intrinsically motivating
5. Role stressors cause employees to leave

There are many ways to leverage the above findings. Many recommendations are interspersed with the findings themselves, meaning this paper provides leaders with actionable suggestions to decrease the cybersecurity professional turnover they are experiencing. It also includes two strategies, developing career paths and integrating gamification, that address several of the above trends.

Decreasing employee turnover is daunting; however, understanding the factors influencing cybersecurity professionals' intent to leave will help cybersecurity leaders navigate the Great Resignation and thereby decrease turnover in their cybersecurity programs.

This report is produced by the Institute for Critical Infrastructure, a private 501 (c)(3) organization focusing on cybersecurity topics concerning U.S. critical infrastructure. Its research is nonpartisan and nonproprietary. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author.

References

Behling, C. J. (2019). Project success in virtual projects: A qualitative study of leadership behaviors. *ProQuest Dissertations and Theses*, *July*, 154.

Birinci, S. (2022). The Great Resignation vs. the Great Allocation: Industry-level evidence. *ECONOMIC Synopses*. https://doi.org/https://doi.org/10.20955/es.2022.4

Borkovich, D. J., & Skovira, R. J. (2020). Working From Home: Cybersecurity in the Age of Covid-19. *Issues In Information Systems*, *September*. https://doi.org/10.48009/4_iis_2020_234-246

Burley, D. (2011). Recruiting, educating, and retaining cyber security professionals in the federal workforce: Lessons learned but not yet applied. *Cyber Security Policy and Research Institute*. http://www.cspri.seas.gwu.edu/Seminar Abstracts and Papers/Burley Report.pdf

Burrell, D. (2018). Managing young cybersecurity and technical employees with love and logic. *International Journal of Economics, Commerce, and Management*, *6*(12), 26–48. https://www.researchgate.net/profile/Darrell-Burrell/publication/331559089_MANAGING_YOUNG_CYBERSECURITY_AND_TECHNICAL_EMPLOYEES_WITH_LOVE_AND_LOGIC/links/5c8031fb299bf1268d404f0d/MANAGING-YOUNG-CYBERSECURITY-AND-TECHNICAL-EMPLOYEES-WITH-LOVE-AND-LOGIC.pdf

Burrell, D. N., Springs, D., Burton, S. L., Dawson, M., Wright, J. B., & Modeste, R. (2020). Perspectives in talent management strategies for cybersecurity job roles in public safety and health in government organizations. *International Journal of Smart Education and Urban Society*, *11*(4), 1–17. https://doi.org/10.4018/ijseus.2020100101

Crawford, C., Boyd, C., Jain, S., Khorsan, R., & Jonas, W. (2015). Rapid Evidence Assessment of the Literature (REAL©): Streamlining the systematic review process and creating utility for evidence-based health care. *BMC Research Notes*, *8*(1), 1–18. https://doi.org/10.1186/s13104-015-1604-z

Dodge, C., Toregas, C., & Hoffman, L. (2012). Cybersecurity workforce development directions. *Proceedings of the 6th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2012*, 1–12.

Estes, A. C., Kim, D. J., & Yang, T. A. (2018). Exploring how the NICE Cybersecurity Workforce Framework aligns cybersecurity jobs with potential candidates. *Proceedings of the International Conference on Frontiers in Education: Computer Science and Computer Engineering (FECS)*, 58–64. https://www.proquest.com/conference-papers-proceedings/exploring-how-nice-cybersecurity-workforce/docview/2139455460/se-2?accountid=14542

Haney, J. M., & Lutters, W. G. (2019). Motivating cybersecurity advocates: Implications for recruitment and retention. *SIGMIS-CPR 2019 - Proceedings of the 2019 Computers and People Research Conference*, 109–117. https://doi.org/10.1145/3322385.3322388

Lachow, I. (2022). Diversity in the cyber workforce: Addressing the data gap. *MITRE*.

Orye, E., & Faith-Ell, G. (2020). Cyber workforce recruitment and retention: an awareness assessment. *NATO Cooperative Cyber Defence Centre of Excellence*. https://ccdcoe.org

Osborn, E. (2015). Business versus technology: Sources of the perceived lack of cyber security in SMEs.

Centre for Doctoral Training (CDT) in Cyber Security Technical Paper, *1*. https://ora.ox.ac.uk/objects/uuid:4363144b-5667-4fdd-8cd3-b8e35436107e/download_file?file_format=pdf&safe_filename=01-15.pdf&type_of_work=Research+paper

Parker, W. E. (2016). Cyber Workforce Retention. *U.S. Air Force Research Institute Papers*.

Pierce, A. O. (2016). *Exploring the Cybersecurity Hiring Gap*.

Sheather, J., & Slattery, D. (2021). The great resignation-how do we support and retain staff already stretched to their limit? *The BMJ*, *375*(October), 2–3. https://doi.org/10.1136/bmj.n2533

Shyam Nivedhan, S., & Priyadarshini, R. G. (2018). Gamification Elements used in Employee Retention and Enhancing Employee Productivity. *IOP Conference Series: Materials Science and Engineering*, *390*(1). https://doi.org/10.1088/1757-899X/390/1/012039

Sugiono, E., Ria Armela, S., & Efendi, S. (2021). The effect between job satisfaction, work stress, and work environment on turnover intention mediated by organizational commitment to the Indonesian National Cyber And Crypto Agency. *Multicultural Education*, *7*(10), 221–238. https://doi.org/10.5281/zenodo.5558002

U.S. BLS. (2022). How To Become An Information Systems Security Officer. In *U.S. Bureau of Labor Statistics*. https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-6

Vogel, R. (2016). Closing the cybersecurity skills gap. *Salus Journal*, *4*(2), 32–46. http://hdl.handle.net/1959.14/1074749.

Wan Yusoff, W. F., Tan, S. K., & Mohamed Idris, M. T. (2013). Herzberg's two-factor theory on work motivation: Does it works for today's environment? *Global Journal of Commerce & Management Perspective*, *2*(5), 18–22. http://www.academia.edu/5154446/HERZBERGS_TWO_FACTORS_THEORY_ON_WORK_MOTIVATION_DOES_ITS_WORK_FOR_TODAYS_ENVIRONMENT