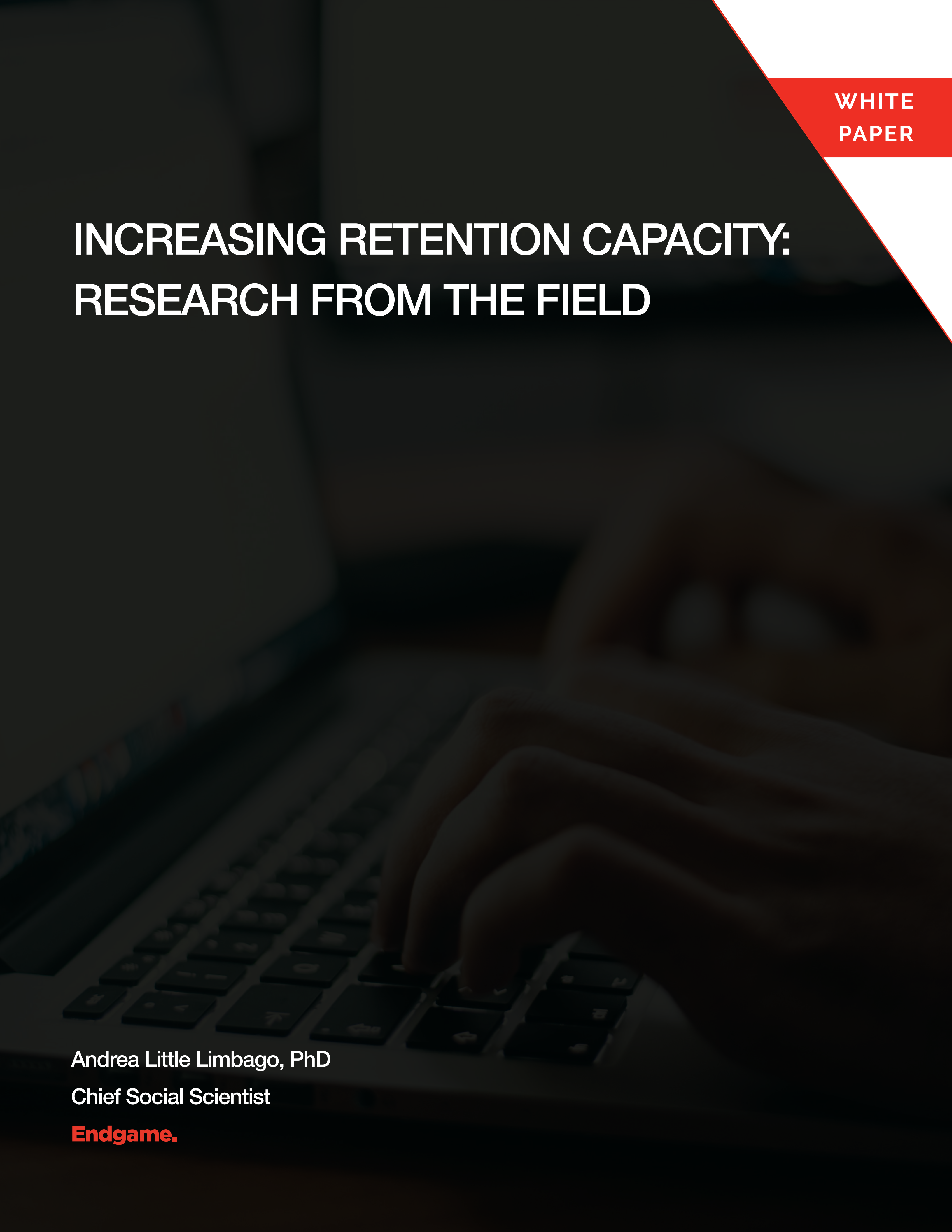
WHITE PAPER

INCREASING RETENTION CAPACITY: RESEARCH FROM THE FIELD



Andrea Little Limbago, PhD

Chief Social Scientist

Endgame.

EXECUTIVE SUMMARY

The workforce shortage in cybersecurity is well documented, with profound implications for both U.S. national and economic security. By 2022, the industry may face a shortage approaching two million qualified security personnel. For the most part, explanations of a pipeline problem abound, especially when it comes to underrepresented groups. While focusing on university programs and K-12 education should continue, those efforts are quickly offset if the industry cannot retain the talent. The average tenure in the tech industry is three years, and by one analysis, roughly a third of men and over half of women leave the industry. This retention problem negates even the best pipeline solutions.

SURVEY RESULTS

Over 300 security professionals, across a broad range of industries, responded to a survey between August and September, 2017, on topics pertaining to retention. Respondents reflected a range of experience within the industry, with three-quarters having worked in the field over five years, and 35% over eleven years. The survey responses highlighted three key factors that have the greatest impact on retention.

- **Ill-defined Career Path:** The lack of professional advancement, a well-defined career path, and work that at times is not challenging were strong factors for respondents when considering leaving the industry and why they left their previous employment.
- **Burnout:** Stress and burnout, coupled with long hours, topped the list for why respondents left a position or consider leaving the industry.
- **Industrial Change:** The industry culture is among the top reasons respondents consider leaving the industry. Discrimination and harassment at professional conferences far exceeded that found within company work environments. Moreover, males were significantly less likely to experience harassment or discrimination than non-males. Industry culture is further shaped by stress and burnout, with little means to assuage them, and can add to a toxic professional culture if not addressed.

RECOMMENDATION SUMMARY

Social systems change via mutually constituted structural factors (i.e., material constructs, institutions, environmental constraints) and agents (i.e., motives, ideas, and actions of individuals). There is no silver bullet, as social change requires efforts across both categories. The key factors are listed below.

- **Structural factors:** Corporate policies (e.g., performance metrics, PTO, social events); Conference culture & representation; Visual cues (e.g., workplace, marketing materials).
- **Agents:** Leadership (e.g., by example, policies & values); Cultural entrepreneurs (grassroots leadership to shape culture, provide accountability, foster social capital).

INTRODUCTION

The workforce shortage in cybersecurity is well documented, with profound implications for both U.S. national and economic security. By 2022, the industry may face a shortage approaching two million qualified security personnel. For the most part, explanations of a pipeline problem abound, especially when it comes to underrepresented groups. While focusing on university programs and K-12 education should continue, those efforts are quickly negated if the industry cannot retain the talent. The average tenure in the tech industry is three years, and by one analysis, roughly a third of men and over half of women leave the industry. Looking specifically at gender retention in computer science, unlike in other tech industries, when a woman leaves a job in computer science, she tends to leave the field entirely. This retention problem negates even the best pipeline solutions.

In many ways, addressing the retention challenge is harder, as it forces the industry toward self-reflection as opposed to casting the blame elsewhere. Fortunately, there is a slow shift in the community, with thought leaders advocating for this kind of introspection. This year both BlackHat and DerbyCon keynotes included a plea for greater decency and civility within infosec. But cultural shifts alone won't provide sustainable retention rates. Additional challenges pertaining to professional development and burnout also must be addressed.

This paper combines social science research on retention coupled with the results of a survey distributed in August and September to infosec professionals. Most efforts for retention and inclusion fail, often because they focus on the easy, stereotypical 'solutions' (e.g., perks like ping pong tables and beer fridges) as opposed to taking the hard and often laborious steps required to truly enact change. Improving retention is key to ensuring all of the efforts to grow the pipeline don't go for naught. After discussing the survey findings, this paper will highlight those structural changes organizations can take to improve retention, as well as what individuals can and should do as agents of change. Importantly, the mission is a key motivator for retaining talent. Security professionals want to stay in the field - let's help make it easier.

SURVEY ANALYSIS: KEY FINDINGS

In August and September 2017, I distributed an open survey via social media. The survey was intentionally short (roughly twenty multiple choice questions) to maximize responses, and covered both those factors that retain talent, as well as those driving factors that may negatively impact retention. I also followed up with a few respondents for additional input. Over 300 people responded, largely reflecting demographics within the industry with 81% self-describing as male, and 86% self-describing as white.[1] This clearly is a limitation, with most results weighted toward this demographic. However, I also reviewed the results based solely on responses of the remaining 19%. In most cases, the key findings persist, and are discussed below. In addition, over three-quarters of respondents have worked in the field at least five years, and 35% have worked in it over eleven years. The major findings are summarized below.

ILL-DEFINED CAREER PATH

A lack of advancement and growth was the main reason respondents left their previous employment. Over half of respondents pointed to this lack of career advancement as a key factor, followed by their manager/boss at 41%. Moreover, almost 20% of respondents pointed to limited advancement or growth as a factor when considering leaving the industry. This points to an interesting challenge within the industry, where good tech leadership is so necessary, but companies are not providing the career paths and development to help prepare future leaders. These findings are supported by previous research which notes that 65% of security professionals lack a well-defined career path.

This resonates even more when exploring a question based on how challenged respondents are in their current position. Only a third noted they are professionally challenged, followed by 28% who are somewhat challenged, and 14% not challenged at all. Although security research and analysis can be extremely challenging, there also are a series of redundant steps and processes that often negate the attraction of the more challenging work. When the position becomes stagnant, and consumed by these rote processes, security professionals may opt to leave for greater professional development and advancement.

These results highlight the necessity for clarity in the career trajectory, especially when it comes to maintaining a hand in the technical aspects of the industry even when progressing towards leadership. As one respondent noted, early in careers, security professionals are enthusiastic and excited to learn about a broad range of technologies. Eventually, professionals focus on more targeted problems aimed at specific solutions, become an expert on those and may go on the con talking circuit or choose to teach at local schools or universities. Finally, based on the follow-on interviews, for those that want to advance beyond these scenarios, there may be limited opportunities for technical management. If someone wants to advance, they often have to take on more programmatic, consulting, or sales positions, or remain stuck in senior roles that become relatively stale despite changes in technology. This point reinforces findings that only 10% feel very challenged, and over half left their previous job due to limited advancement. In one case, a respondent pointed positively to a 'higher expert' track that led to vice president positions which entail leveraging technical knowledge to influence corporate strategy. There is a broad desire for more tracks of this nature which combine technical expertise with broader impact within an organization.

> "BECAUSE THERE IS NO UNDERSTANDING OF SECURITY, AND MOST OF THE TIME NO EXPERT/ TECHNICAL CAREER PATH, THE ONLY WAY FOR EXPERT TO HAVE A RAISE IS SWITCHING COMPANY."

A BURNOUT CULTURE

The next consistent finding focused on security's burnout problem, which surfaced via two specific questions focused on why respondents left their previous job, as well as reasons they consider leaving the industry. Across each question, the results were very similar. The top two reasons respondents left their previous employment were burnout (32%) and stress (28%). The results were reinforced for those considering leaving the industry, with 40% and 30% choosing burnout and stress, respectively. These were followed by industry culture, and then 28% pointing to work/life balance. These results are not surprising, and support previous research on the industry which points to a culture of unachievable expectations with performance based on whether there has been a breach. At a time when 80% of companies report they have been successfully breached at some point, many in the industry feel they are held to unrealistic standards that cannot be solved by security professionals alone.

> "WITHOUT SOMETHING TO MOTIVATE, AND THE GRUELING WORK, BURNOUT IS NEARLY INEVITABLE. ON TOP OF THIS, MANY PEOPLE SIMPLY DON'T CARE OR VALUE OUR WORK, OR EVEN WORSE, REACT NEGATIVELY/ANGRILY TOWARDS IT."

Moreover, 70% of survey respondents work 41-60 hours, and 10% work over 60 hours each week. These results are supported by similar research, which finds most

[1] It is important to note that only 57% of respondents chose to answer the question on race and ethnicity, so that it is 86% of 176 respondents

security professionals work on weekends. Almost 40% of respondents also highlighted the role of validation or recognition of their work as something they most value in the workplace. However, in follow-on discussions, many respondents expressed frustrations over the limited or non-existent recognition for their hard work. In short, couple the long hours with the constant fear of job loss due to a breach, limited recognition for their work, and work that may not be challenging, and it is not surprising that burnout and stress rate so influential among survey respondents.

INDUSTRIAL CHANGE

The survey provided a handful of additional insights, which together dispel some common stereotypes of the industry. First, almost half of the respondents are 31-40 years old, in contrast to omnipresent stock photos of hackers as youthful, shady characters. In fact, although roughly 20% of our respondents were under 29, other research notes that only 7% of the security workforce are under 29. Interestingly, it seems most companies target their perks and benefits at this younger demographic, such as games and alcohol, when in fact only 12% of respondents pointed to limited perks as a factor for leaving a job. In short, the workforce is aging and there is a need to attract new, younger talent into the industry, while focusing on creating a culture to retain the expertise and talent of those already in it.

"I WISH THE BRO CULTURE WOULD DIE. IT'S KILLING SECURITY."

The cultural aspect remains a key challenge for both retention and attracting new talent. Almost a third of respondents noted industry culture as a key factor when considering leaving the security industry. 85% of non-male respondents experienced some level of discrimination at professional conferences, and over half have experienced harassment at those events. These numbers do drop when focusing solely within the corporate environment itself, with almost 60% of non-male respondents experiencing discrimination at their company, and 44% experiencing harassment within their company or company events. This contrasts dramatically with the male respondents, 30% of whom have felt discriminated against and 23% harassed within the company and company events. Meanwhile, 36% of male respondents have at some point felt discriminated against and 31% harassed at professional conferences. Clearly, there are different experiences based on gender, but, based on the survey results, professional conferences writ large have a much worse track record of harassment and discrimination when compared to company culture. The differences across genders is not surprising, and is supported by a recent Pew Study which also finds stark differences between both gender and ethnic groups when asked about the prominence of discrimination.

While there are many phenomenal aspects to the security culture, as the Black Hat and DerbyCon keynotes highlight, a cultural shift is also needed, and is hindering retention within the industry. So what can be done? The next section offers some suggestions.

TOWARD THE NEXT-GEN SECURITY WORKFORCE EXPERIENCE

Given the mission criticality of security, coupled with the workforce shortage, addressing these challenges to retention should become a top industry priority. The survey highlights the need for a cultural shift to address the industry's burnout, career path, and inclusion challenges. Culture refers to both "a set of evaluative standards (such as norms and values) and a set of cognitive standards (such as rules and models) that define how social actors exist in a system, how they operate, and how relate to one another)."[2] Culture strongly shapes the incentives for different kinds of behavior within a given setting. However, most efforts aimed at these kinds of changes tend to fail miserably. Take, for example, diversity efforts in the tech industry. The majority have yet to produce substantive change, often because they tend to focus on changing external perceptions as opposed to making the harder, internal changes required for true cultural change. Fortunately, there is a wealth of social science research on social and organizational change.

AGENTS AND STRUCTURE

Many social scientists view the social world as comprised of agents and structure, with long debates about which takes primacy. The agents are individuals who possess free will and can instigate change, while structure focuses on those external factors (such as institutions or environmental conditions) that constrain behavior. How does this impact retention? Cultural change requires understanding that the agents and structures are mutually constituted, and therefore solutions must address both factors. Viewing retention through this lens highlights some concrete steps those in the industry can take now to address these key factors that are negatively impacting retention, while maintaining and promoting those positive factors that attract and retain great talent to the industry.

STRUCTURAL FACTORS

There are a range of environmental and policy changes that can directly impact the professional development and culture of organizations. Burnout and inclusion often go hand in hand. Creating an environment wherein employees have the chance to rest and feel socially comfortable in the workplace should become top priorities for retention. The technical difficulties of getting the code right isn't necessarily the greatest challenge, the human element is, which is why so many efforts aimed at cultural change fail. Insights from the survey results, coupled with extant research, highlight some key factors organizations should address to help retain not only their security workforce, but also craft a more inclusive work environment for everyone.

WORK POLICIES & ENVIRONMENT

Policies aimed at addressing burnout and inclusion should take priority. Fortunately, several policy recommendations address both. For instance, follow-on interviews reinforced the necessity for more realistic performance metrics. Instead of placing sole blame on the single IT analyst responsible for the entire enterprise security, security should become everyone's responsibility.

"KEEPING UP" TECHNICALLY IS TAXING, ESPECIALLY WHEN FIRM DOES NOT SUPPORT PROFESSIONAL DEVELOPMENT"

Unfortunately, this is easier said than done. In a recent workplace survey, over 80% of respondents felt security hampered innovation, and limited the ability to complete work. Additional policies such as those that integrate security experts into the organization, instead of isolating them, could foster a more amicable relationship between the security experts and the rest of the company. This could include interactive collaboration, such as internal PSAs for security, or internal corporate simulations and exercises, but must avoid the tedious, click-through security training that tend to waste time and provide minimal educational value. Embedding security professionals within each of the development teams could also help ensure security is part of the development process and not an afterthought. The U.S. Department of Homeland Security offers a range of guidance and activities for the workforce to foster a culture of security. These kinds of security awareness activities and organizational structures could contribute to the overarching performance metrics, and help spread

[2] Katzenstein, page 6.

the responsibility. In short, performance metrics should not be based along the binary of breach or no breach, as some respondents noted. Instead, security needs to be understood as an enterprise-wide problem. With that change in mindset, performance metrics for security professionals should be more nuanced, including both successes and failures, an improved understanding of the organization's threat model, and taking into account available resources.

On this latter point, it is important to include security professionals when making technical resource decisions that could affect the corporate security posture. Ideally, this is common practice, but it is worth reiterating. Increasingly, enhanced human-computer interaction has proven to help workers across a range of industries, especially helping workflows with repetitive tasks, data overload, and quick responses. In this way, corporations could focus on those technologies that help automate some of the time-intensive tasks, and enable faster and targeted data exploration. Most importantly, corporations should work with their security professionals to define future technological requirements with priorities focused both on security, but also productivity and helping reduce burnout by enabling them to progress beyond repetitive activities and towards the more challenging analysis and investigations which drive (and thus retain) security professionals.

In addition, transparency on, and greater opportunities focused toward career advancement could also address the pain point of limited professional growth opportunities. One respondent recommended a path to vice president that retains a combination of leadership, management, and technical requirements. Another respondent lamented that technical career paths largely lead to thought leaders and consultants who are increasingly separate from the day to day technical activities. Many commented that the notion of technical director remained fuzzy, and felt the need to ensure that as security experts progressed, they need to be empowered to make corporate decisions regarding security strategies. There was not any explicit mention of CISO involvement, but CISO sponsorship and career paths could also help elevate the range of career trajectories. Clearly, this is an evolving challenge, and it must also ensure these defined career paths are meritocratically based, with solid understanding of and addressing unconscious bias in bias in meritocratic-based policies, which could go a long way to supporting inclusion and retention. Given the growing demand for technical leadership, this is in the interests of both organizations and the security professionals.

As the survey validates, security professionals are willing to work long hours, and love the mission, but corporations can better harness this enthusiasm through greater flexibility in schedules and remote work options. Often companies believe unlimited PTO addresses this issue, but that is not necessarily true. Security professionals often do not take advantage of these programs, rarely using their time off, and instead worry that if they are not in the office they will be punished. In fact, across industries in the United States, workers increasingly don't know how to take time off. Managers and leaders must be aware of these concerns, mandating time off and vacations are properly taken as one means to limit burnout.

Finally, social events should focus on inclusion and offset ingroup/outgroup dynamics. Alcohol often dominates corporate and industry events, and can foster toxic environments. There have been numerous reports on the tech sector as a whole, and its alcohol-driven party culture, which can leave many to feel left out or underappreciated. These kinds of corporate events can be a key detractor for retention. As noted, these kinds of perks ranked very low on the survey of what retains security professionals.

Instead, social events should provide other activities,

[2] Katzenstein, page 6.

such as reading groups, meetups, or outdoor activity. These can include alcohol, but it no longer becomes the driving organizational factor. Importantly, these social activities not only address issues of inclusion, but also burnout. So often security professionals refuse to go afk (away from keyboard - and yes, the fact that there is an abbreviation for this is telling). Social events - with leadership buy-in - provide the gentle nudge to get security professionals to put away the laptop, and get outside, interacting, and finding new and old hobbies. These additional kinds of social events also foster greater engagement, and have a positive impact on retention and inclusion throughout the entire company. While these kinds of social activities may seem superfluous to the bottom line, they can positively impact retention, workforce engagement, and inclusivity by building cross-cutting social networks.

SECURITY CONFERENCES

In the social sciences, the boomerang effect refers to the role of external influences in changing internal or domestic behavior. What does this have to do with cybersecurity? Security conferences (e.g., factors external to an organization) can influence retention within an organization through the direct influence on inclusion, professional advancement, and the role of the security culture. Only 5% of respondents do not attend any professional conferences, so this is broadly applicable, with over a third of respondents attending 3-5 conferences per year. There has been a lot of discussion about codes of conduct at security conferences, often stemming from incidents of harassment or discrimination at these events. But the enforcement of these codes of conduct remains a problem, especially if there are not any compliance mechanisms. Despite some of these challenges, conferences are a key source of professional development, networking, and helping security professionals stay on top of the latest innovations in the industry.

There should not be a trade-off between maintaining the hacker culture and fostering and attracting a more inclusive atmosphere. Many security conferences already do this, but there is always room for improvement. First, codes of conduct can help attract (or detract) security professionals from attending a conferences. It must be more than a piece of paper, with the onus on everyone to help ensure it is followed. In some ways, having a code of conduct is a first step at admitting there are inclusion issues that need to be addressed within the industry. Next, conferences should make concerted efforts to ensure speakers reflect diversity of all kinds, and avoid #manels. This does not require a trade-off between quality and diversity. One proven way to obtain greater diversity - while maintaining a high caliber of speakers - is to conduct blind review of submissions. While it is not a panacea, it is a step to help ensure a broader range of diverse voices are represented, and minimize the persistence of manels at conferences. For example, O'Reilly Security conducts blind review, and in their first two years achieved over 30% of speakers from underrepresented groups, well above industry averages. Conferences aimed at addressing some of these challenges - such as the Women in Cybersecurity Conference and the Diana Initiative - also provide additional options for members of the community who may not feel as comfortable at other security conferences.

Of course, members of underrepresented groups also need to submit. In several discussions, conference organizers have noted the lack of submissions from underrepresented groups, in one case less than 10% of submissions were from women. Corporate policies can help change these statistics by including

> "LETTING YOUR TEAM MEET NEW PEOPLE, PUBLISH THEIR WORK, TRAIN, GET NEW IDEAS. FOR ME IT IS REALLY A MUST HAVE IN TERMS OF TALENT RETENTION"

attendance - and even presenting - as part of their professional development programs. Sponsorship of security professionals - not just mentoring - could help prepare them make this transition. In the survey, over half of respondents believe their companies are supportive or very supportive of professional development, while almost a quarter found they aren't supportive or were neutral. This is an area for improvement, as conference attendance has multiple benefits, including the professional development needs of the workforce, the desire for challenging work, additional training opportunities, and they can help companies with brand awareness. This can be a big step for many in the industry, and so it is worth reiterating the necessity for sponsors and recognition for security professionals when they take the first big step of submitting to and speaking at a conference.

VISUAL CUES

A final, and often overlooked structural factor is the actual environment itself. Just as bright colors and art can transform downtrodden cities into thriving urban centers, so too does the office environment and visual cues impact a variety of factors relevant to retention, such as teamwork, inclusion, and innovation. What are some of these most important visual cues? The office space is a good place to start. The physical environment sends cues about whether an individual belongs, referred to as ambient belonging. In many cases, stereotypical posters or offensive content written on marker board walls can quickly trigger a sense of inclusion or exclusion.

Similarly, corporate websites, conference material, and marketing material equally signal a corporation's perspective toward inclusion and its culture. The notorious stock photo of a shadowy figure in a hoody only perpetuates out-dated stereotypes that continue to hinder the industry's branding. In the survey, almost a quarter of all respondents did not feel represented in their corporate material, and only 6% felt very represented. These findings hold when controlling for gender identification, demonstrating the broad impact these materials can have. Finally, corporate schwag signals values and culture more than many would expect. For instance, for the most part, the cybersecurity community targets corporate schwag at young men. There perhaps is no better visual cue that entire groups are unwelcome, either at the conference or within the company. Be cognizant of ordering mens and womens sizing, and offer alternatives to giveaways that only focus on booze or whose text may be offensive. Simply attend the Grace Hopper Conference and you'll quickly see how many alternative options exist.

These are all aspects of an organization's day to day operations. The key is to intentionally consider the implications on ambient belonging. Importantly, these three factors - office space, marketing material, and schwag - all impact recruitment as well. They serve as an immediate signal about the company's culture and values, an impression that is hard to change once influenced. Moreover, while these recommendations seem solely focused on inclusion, they also affect burnout. Employees who don't feel like they belong are more prone to depression and the fatigue of not fitting in, all of which fuel burnout, an impact which is race, gender, and ethnicity agnostic.

AGENTS OF CHANGE

Structure alone is not the panacea toward retention. Key agents also are necessary to serve both as trailblazers and leaders in shaping those core issues that impact retention. Although corporate leadership plays a major role, cultural change requires support and buy-in throughout the organization. This section will focus on how leadership can make or break the required cultural change, and introduce the idea of cultural entrepreneurs to truly spark the necessary changes required to address many of the key impediments to retaining talent. Together, these two categories within agents of change address the top-down and bottom-up forces that drive cultural change.

CORPORATE LEADERSHIP

At the end of the day, corporate leaders are responsible for setting the policies, crafting the workplace environment, and supporting those social activities and values that shape the corporate culture. They also must serve by example. The only topic that seems to grab headlines at a pace on par with cyber attacks are those of executives completely mishandling situations (and even being forced down) due to the corporate culture they fostered. Contrast those examples with strong leadership whose commitment to an inclusive and innovative culture is more than a public relations pitch, and the outcomes are quite stark. Interestingly, the cybersecurity industry has not been as vocal about corporate culture - especially in the realms of inclusion and diversity - as the tech sector writ large. This is starting to change, as the keynote examples demonstrate, but there clearly is still a long way to go.

Corporate leadership teams - from the executive team to advisory boards - are responsible for implementing those structural factors discussed in the previous section, and should be held accountable via the appropriate metrics. For instance, there is much discussion about the vast sums of money spent toward fostering an inclusive culture within Silicon Valley, often with minimal impact. Companies such as Intel invested $300 million in diversity, and CEOs lament that they wished they had built diversity into their culture from the start. Admitting that the problem exists is an important step, but this rhetoric has yet to translate into a more diversified workforce. A concerted effort by major tech companies to address diversity resulted in at most a 1% increase in gender diversity and an even smaller increase in ethnic diversity. Leaders need to move beyond throwing money at the problem, and focus on those structural aspects to enact change, which starts with leading by example.

As the previous section illustrated, many of those key factors for addressing retention don't require significant resources, but rather more thoughtful allocation of those resources and policies. Leadership should focus on retention rates across different groups, especially comparing those that work in security positions to those who don't, as well as across demographics. They should make concerted efforts to truly address issues related to burnout and find those policies and environments that best address the core problems. Finally, executive teams committed to diverse perspectives and backgrounds should reflect that commitment. Security professionals are in high demand and, all else equal, may leave positions for leadership that better personifies the commitment toward inclusion.

CULTURAL ENTREPRENEURS

Structural factors and leadership support are essential. These are the core enablers, but alone are not sufficient for instigating the cultural change that could help the industry's retention challenges. Cultural change also requires grassroots momentum, led by cultural entrepreneurs across the industry and organizations. Similar to the role of policy entrepreneurs in pushing forth new ideas in the public sector, cultural entrepreneurs are key individuals who can use their technical credibility to push forth ideas and promote solutions for any cultural challenges they identify or experience. By serving as a gateway between various aspects of an organization, cultural entrepreneurs can move an organization and ideally the industry beyond its current sub-culture state and succeed at both retaining and attracting talent.

Cultural entrepreneurs are required to ensure an organization's culture is inclusive and purpose-driven, fosters an environment that acknowledges and addresses burnout, and helps craft new career paths, instead of perpetuating the status quo. Cultural entrepreneurs, and their ability to foster grassroots cultural shifts, may be the missing link in many of these cultural and diversity initiatives, as well as those that shape a healthy work environment.

Importantly, cultural entrepreneurs cut across organizational stovepipes and the industry itself to help stimulate change. First, cultural entrepreneurs can help foster social capital, those personal connections that help social systems function, develop, and even innovate and heighten civic engagement. A recent Gallup Poll reinforces just how hard it is to foster social capital, with results confirming that over 70% of the American workforce does not feel engaged. A disengaged workforce is extremely hard to retain, while an engaged workforce performs better, and stays longer at a company.

Cultural entrepreneurs can also provide a layer of accountability for leadership policies, and bring in new ideas to customize those structural factors to best fit a given organization. For conferences, cultural entrepreneurs can ensure codes of conduct are adhered to and call out inappropriate behavior when they see it. Cultural entrepreneurs can encourage or informally organize inclusive activities, provide a check against stereotypical or biased marketing collateral, and by providing internal and external thought leadership through blogs, presentations, and marketing can go a long way toward helping produce true cultural shifts within the industry.

All of the amenities in the world are not enough to overcome the security industry's cultural challenges that not only persist, but seem to be exacerbated through social media. Instead, cultural entrepreneurs can - and in many cases already are - fomenting the grassroots changes required for cultural shifts in the industry.

CONCLUSION

Retention deserves as much attention, if not more, as that given to the pipeline challenges. All of the resources expended toward building a solid pipeline of talent will go for naught if the security industry cannot retain professionals. As noted, when security professionals leave a job, they may leave the entire industry, and never return. This not only is a waste of time and resources, but reflects a significant loss of expertise in an industry where expertise is so impactful.

Fortunately, almost half those surveyed identified mission as a core factor within the workplace, highlighting the comparative advantage of the security industry. Over two-thirds of respondents also chose stimulating work, professional development, work/life balance, and a supportive manager or boss as the most important factors. This is a core opportunity for retaining a workforce who is willing to work long hours on complex problems to keep personal and corporate data secure, and protect the country's national and economic security.

Comparing these important factors with those reasons people leave, highlights several key priorities. First, challenging work with clear professional growth must be prioritized. Second, burnout is a real and growing factor within security, and organizations must actively shape policies and corporate culture to minimize its occurrence. Finally, the security culture maintains many phenomenal characteristics that prompt innovation, community, and collaboration. There also are aspects of this culture which must become more inclusive, and minimize any toxic elements which drive some to leave the industry. By addressing these factors, not only can retention rates dramatically improve, but it will also reinforce many of the ongoing pipeline efforts and truly begin to hack away at the workforce shortage.