CYBERSECURITY

Condensed transcript from live Info Session.

How to solve challenges due to unexpected cybersecurity staff shortages

Speakers

- **Enza Alexander, Executive Vice President, ISA Cybersecurity.** Enza has over 25 years of experience across the technology sector in finance, operations, sales, marketing, and professional services. Enza was one of Canada's leading Women in Technology by IT Canada and CDN Magazine (2011).
- **Scott Bailey, Sr. Advisor, ISA Cybersecurity.** Scott has 25 years of experience in the Enterprise Technology and Services space, including progressive Sr. leadership roles at two of North America's largest and most successful Technology Service Providers
- **Andrew Birrell**, **Engagement Manager, ISA Cybersecurity.** Andrew has over 12 years of experience as a talent acquisition specialist and has worked both in Australia and Canada.
- **Lanny Barcelos, Security Solutions Architect, ISA Cybersecurity.** Lanny has over a decade of experience in helping clients with IT managed and hosted services.

Opening remarks

Enza: Almost every organization today is experiencing unprecedented absenteeism and impact to the workforce. In light of the "Great Resignation", we're seeing larger turnover in the technology industry and the cybersecurity sector, which has continuously had a war for talent and a gap in being able to identify the right certified professionals to assist us with enabling cyber environments and systems that will help us protect our businesses.

Scott: Understanding and addressing the gap between employee and employer expectations is a critical exercise and can provide a starting point to develop a platform for future success. Unexpected absences, skill shortages, and unfilled vacancies are frankly the new normal, especially in cybersecurity where resource demand continues to far outstrip supply.

This is exactly what's going on in the industry. Each week we realize that somebody is sick or off, or is in a household that has been affected by COVID-19 and can no longer work or may not have the remote tools to do that work remotely, so this is certainly something that's affecting most organizations.

1. What common challenges are companies facing as a result of unexpected cybersecurity staff shortages? What are some quick and reliable solutions?

Scott

- There are a very broad range of challenges that stem from an unexpected staff shortage. Important projects may be delayed, an organization may struggle just simply to keep the lights on and operate. Often remaining staff, those that remain after a resignation or a leave, get overburdened as other people exit and, frankly, the list goes on and on and on, but there are several things that you can do.
- Develop close relationships with your cybersecurity staff and look for behavioral predictors so you can circumvent issues and/or be prepared to take action if somebody leaves. The closer that your relationships are with everybody, the better. I know that's very hard to do with everyone being remote, but find time to connect with everybody and ensure that you have a good sense of how well everyone is doing while working from home and having the pressures of doing so.
- Ensure that your staff has access to various communication platforms is something that with the onset of COVID-19, everybody rushed to get modern workplace or something in place, but make sure that they know how to use it. I think a lot of organizations were able to react quickly and get the tools required to work remotely and not everyone managed to make sure that their staff were able to use those tools properly.
- Engage your resources to help find new and creative ways to deal with staffing shortages, encourage them, and, in cases where you can, reward them for increases in efficiency. It's interesting to see who, in the wake of a resignation or a termination or something, will step up and provide solutions to better the organization.
- **Bring in external expertise, when necessary, even if only to fill a temporary shortage. This will help and ensure that you don't overburden the existing staff and may help increase the likelihood that those that remain find more joy in their role, knowing that the organization is with them through those challenges. And consider using those external consultants to not just fulfill the gap, but to potentially train your staff and increase their skill set as a result of somebody leaving.**
- Build resource contingencies, where possible. Make sure that you don't have *one* person in your organization that knows a particular tool. Obviously, if that person leaves, you're going to be left short.

- Find opportunities to cross-train your staff and encourage self-paced skills development at every opportunity.
- Define your human resource value proposition and connect as many people in your org as possible to your business goals and, frankly, and maybe most importantly, figure out a way to embrace a hybrid or remote work culture.

1. What criteria should be used to determine the best solution for the challenges resulting from cybersecurity staffing shortages?

Andrew

- The skill shortage in cybersecurity, I would compare to be a lot like the software development industry. For both industries, the practitioners do really care about the craft and tend to be self-invested in continuing their education and amassing industry-relevant experience. And those practitioners appeal to many and enjoy interest in the market.
- And when we're establishing the criteria to address the business needs in a highly competitive marketplace, some of the most important aspects that I recommend before going to market would include, **know what compelling story it is that you're trying to tell**. Put it out there in the world to attract some security talent and retain them. **Are you competitive on salary? Is there management technical lead or other defined development pathways that you've got planned already? How are you communicating that to the talent pool that you're reaching out to?**
- Is the technical stack and improvement roadmap in place so that there's a clear vision of the work that this person will be contributing towards the success of. Are there specific work conditions, benefits, certifications, or other aspects of the company profile and work that can create a point of difference in the hiring process.
- And finally, have you wrapped all that into a cohesive kind of package that you take to market because, you know, really it's *hiring*, but it's also *selling* when you're in a competitive marketplace. So these are the sort of questions that I would assume most companies have sort of gone through in some sort of formal or informal capacity, you know, and then they are looking at pushing through a hire. **However before reaching that point, some of the key questions that I think should be asked, would include: do I need these skills internally or can I consume them from a third party, whether that's temporary, managed, hosted, or other, and how am I planning for redundancy to cover sudden departures, illness, and annual leave?**

Lanny

- I think it's also important to consider in your criteria current vs. future state: where are you now, where do you want to go and how do you want to get there?

- I'm going to cover some other scenarios that may resonate with our audience and I'll start with the dreaded perpetual hiring cycle.
- Let's just say that you had a recent departure: except it actually wasn't your first, but your *third* in two years, and now you're having a moment of pause on the in-house strategy.
- **This is where managed or hosted solutions may be a really good fit for you, when you partner with a managed security services provider - and, spoiler alert, ISA Cybersecurity is one of them – you actually reduce the total cost of ownership. So, let's take SIEM for example, something that a lot of organizations invest in heavily. It answers questions like 'who's going to triage, monitor, scale the environment, patch the environment, and troubleshoot it, all within a 24x7x365 timeframe?'.**
- **This is where having a Security Operations Centre manage all those areas allows your organization to refocus back on the core projects and initiatives, while taking advantage of a consumption-based model. There's also flexibility out there with a lot of providers, where they provide one-, three- and five-year term options, and that can suit various organizational timelines.**
- But let's move on from SIEM for a second. Perhaps that doesn't apply to you, perhaps you have an **endpoint protection or EDR platform, or a security awareness program that you want to launch because the "death by PowerPoint" flavour that you have in-house isn't really paying dividends. Or maybe you have a vulnerability management program that you want to launch or offload the existing program. These are all areas that we can help.**

2. How has COVID-19 affected the cybersecurity labour market?

Scott

- I think it's fair to say that COVID-19 has further complicated an already-complicated cybersecurity labour market. For a long time, there's been far too much demand and not enough supply. We've all seen that; everyone in that space knows that it affects the cybersecurity part of the IT landscape more so maybe than in the rest of the IT landscape.
- The desire for a flexible workplace has been something that's become very evident as a result of COVID-19. It's become something that was a requirement and is now teaching people that maybe it's *not* a requirement, maybe I love working remotely maybe this is something that I *want* and it's taken on new meaning during the pandemic, particularly among millennial and "Gen-Z" workers.
- **A recent study conducted by Info-Tech indicates that almost half of the workers in those categories say they will quit their jobs, if not given the opportunity to work remotely.**
- So, this is no longer being seen as a nice-to-have; this as being seen as a must-have, particularly across those workers.

- In that same report Info-Tech 2022 Tech Trends Report, it also shows that 18% of employees want to return to the office full time, but *70%* of employers want people back in the office full time; in other words, there is a very significant gap and we'll all need to cross that gap very, very soon, if not already.
- **Progressive organizations have developed some frankly brilliant human resource value props, combined multiple roles to justify higher compensation models, provided flexible work arrangements – two days in the office, three days remote – trying to keep their culture alive. Some have built very individually-focused roadmaps to increase their ability to attract and retain people.**
- I think it's showing a little personal attention to key people and to key roles to make them understand that they are valued in the organization, at a time where you know, frankly, that they're getting calls from recruiters, they're seeing job postings everywhere.
- I think how you communicate, how often you communicate, and the relationship you build with them is critical. Generally speaking, your resource costs, your salaries, your bonuses, and your compensation models – they have risen as a result of COVID-19, but they don't necessarily have to. **Well-defined roles, hybrid work cultures, rewards for efficiency improvement, and nurturing those genuine relationships all can make a huge difference in your ability to not only keep the people that you have, but to attract new people to the organization.**

3. How long does it typically take to find and engage a certified cybersecurity consultant?

Scott

- That's the million-dollar question, and that's the question that everybody wants answered and everybody wants it to be a pretty short duration. But the truth is there isn't really a repeatable timeframe on how long it's going to take to fill roles and frankly it varies a lot, but let me give you some insight.
- Any of us can take a quick look online at cybersecurity job postings or even IT job postings or frankly any job posting today, and you'll immediately notice a few things.
- You'll notice how long it takes for most organizations to fill those roles in this market, you'll note that roles can go unfilled for many months, whereas it used to be many *weeks* it's now many *months*, and you'll often see roles that go unfilled for a year or more.
- There are organizations that have been looking for certain people through the *entire pandemic* and unable to fulfill those roles. Despite the supply-and-demand inequities there, most full-time roles today still go unfilled after 8-12 weeks of active recruitment.

- It's frustrating to say the least. We've all been there, we know what it's like to have a role that we know we need filled, and we know we're overburdening other staff and we just can't find somebody to fill that role.
- But I would say speed to fill – so back to the question about how long does it take – speed to fill for an open role really shouldn't be the primary objective. *Accuracy* of the fill should be the main goal. We've all seen fast hires that don't stick and don't make it long term. You know, we feel good we found somebody, they took the job, we filled it, and as Lanny said, you know, a year later you've filled this role three times!
- **Yes, it's tough to find qualified people; yes, there are a lot of organizations looking for the same types of people and the same types of skills; and yes, ultimately compensation *does* matter: you have to pay what a market expects. But the main reason I offer you, and why organizations struggle to fill a role, is that they fail to define the role properly; they fail to focus on the key outcomes of that role; and they fail to create and have a role worth having in the first place.**
- The next time you have a minute to yourself, take a look at the average cybersecurity job posting, and you'll realize very quickly that they all sound exactly the same. Most of those postings tend to ask for a very large laundry list of desired skills and technologies and experience, and you know very, very, **very few of them actually highlight the importance of the role and what that role is really *about*, and why it's important to the organization.**
- Keep in mind cybersecurity professionals have choice – lots of choice – and they know it. You want to fill a role in less time than your competitors? Structure the role in a way that will attract somebody that has *more* than the required skills, attract somebody that wants, you know I hate to say it, but "more than a job".
- **In times of immediate need, consider engaging an external consultant for a defined period of time or for defined tasks. That external consultant can usually help alleviate some of the pressure from an unexpected resignation or an unplanned exit, and can also be engaged just to keep the lights on, so that you can move one of your other existing staff into maybe a role that's more important to the organization.** Take that as an opportunity to move somebody up in your organization, take them out of a role that's traditionally operational, give *them* the opportunity; after all, this is somebody that's obviously indicated that they want to stay.
- They'll be very hard to replace down the road as well, so you know those little things might help you retain the staff that you have.
- But back to my main point is, you know, really create a role that somebody's going to *want* and don't worry so much about speed to fill, worry about, you know, quality of the hire. I'd much rather take an extra month to hire somebody that I think is going to stick and offers the organization something, than me feel like I just filled that role quickly.

4. With "The Great Resignation" looming, what strategies can be used to avoid burnout and improve the retention of cyber talent?

Lanny

- So, if the "Great Resignation" is real then many organizations are going to be faced with stretching their existing talent.
- **What we see are a lot of examples like security engineers that spend more than half their time and operations which isn't really an attractive proposition to them, and it just increases the risk of flight. I think focusing on efficiencies through automation can play a significant role in this area.**
- **We have technologies out there, like security orchestration, automation response, or machine learning, even AI that can shave a 12-step process for your frontline analyst down to just a few steps that allows them to focus more on investigating legitimate threats.**
- We personally leverage those three technologies in-house and we also embed that within our hosted services, and we've seen the benefits from that.
- Also, I mentioned managed and hosted services earlier. It doesn't have to be a binary choice whether you decide to go completely in-house or partnering with an MSSP.
- **It can be a hybrid approach, where you consider your security folks your prize talent. Time invested in areas like triage, are very time-consuming. Perhaps you can leave that to areas of greater interest for your in-house talent such as threat hunting, while you offload the triage component to your security provider.**
- **Demonstrating that kind of support to reduce the pressure on your people could actually mean the difference between avoiding another hire on your prized in-house talent.**

Andrew

- Some of my thoughts, regardless of whether they're security operational hires or senior consultants, architects, or other domain specialists across the security stack. One of the things when you do inevitably lose some talent, or you have some gaps, is to try and reduce the noise – the surrounding noise for the existing staff that are still there and really kind of prioritize what's important and within their capabilities.
- **So I think that's an opportunity to go back up to that business risk level, look at the security roadmap, look at what the current plan was, and adjust accordingly, so that it's just not myopically going forward with an original plan that has now changed because you've lost two to three months of work product with someone leaving.**
- **So that would be one of the key things, tie the capability back up to the business objectives where possible.**

5. Audience Q&A

1. What is ISA Cybersecurity doing to retain cyber talent considering COVID-19 and the "Great Resignation"?

Andrew: I know that from top to bottom, we've employed a number of strategies; education grants; continuously providing access to vendor certifications; and ongoing ability to upskill.

But it's about also providing that mechanism to realize the benefits of upskilling, as in, changing the role and being able to get exposure to different domains within cybersecurity.

Those are some of the things, at least on the career growth part that's important. Obviously, we have to be continuously researching what the market rates are for the talent and being aware of that, so that we're staying ahead of that curve – another highly important point.

Finally, I think just the culture aspect and continuing to build those communication channels, to ask how people are doing and the common things that we all took for granted when we were on site that we now need to kind of try that little bit harder when we're remote.

2. Generally, how long does it take for ISA Cybersecurity to set up a managed and hosted environment?

Lanny: I would say the general average would range between 6-9 weeks, but that does depend on size of the environment, but it's safe to say that that is usually the track record that we have that we can endorse.

Enza: And it's very customizable, that's a key feature: we can co-manage, we can provide the hosted service platforms, etc.

3. How open should I be within my company about the resource challenges I'm facing? Am I risking more churn if I'm too open about it?

Scott

- Yeah, that's a really interesting question because I think what a hybrid work environment and having people work remotely has shown us is that, you know, we need to probably engage people more often; we need to check in on people more often. Andrew said that is something that ISA Cybersecurity has been doing and I've been witness to that.
- I think you have to first look at the culture of your own organization, and how open in general you are about things. But certainly in our experience when you are open with that it humanizes things.
- It realizes that we're all in the same boat. If we're in an organization that communicates our goals and objectives well, then we want more and more people to participate in the pursuit of those goals and objectives.

- **I would always suggest to be more open than not. I suggest that the people that *do* these roles every day generally have better insight than anyone else in the organization as to how those roles might be improved. Some of the best efficiency gains I've ever seen came from people that were doing the job, not somebody sitting in an office thinking "Hey, wouldn't it be great if".**
- People who really do this for a living and see it every day and use the tool, and "I know you gave us these two tools to work, but this tool is terrible: we don't want to work with this tool, you know, don't force us to use this tool, we should do the following".
- So, I think if you can be open, you will be surprised. I think it's important to *be* open and ask for help. Don't just be open and share your dirty laundry and say, "Oh God we can't find someone to fill this job", but to say, "Hey listen, it's a challenging marketplace right now."
- I've seen individuals step up and say, "I think I can do that job in addition to mine," and you get the opportunity to then look at, can you create a more efficient organization? Can you create a path for somebody who might be in an operational role and wants to get into an engineering role?
- **Lanny said it too: engineers, architects, they don't really want to keep the lights on, and that might be something that you can offload to a managed service provider, and then enrich the life of your resources to do things that are ultimately going to get you towards those objectives as an organization, quicker.**
- So, I don't think you're risking more churn. I think you're actually risking more churn if you *don't* and aren't honest with the staff of what's going on and ask for them to help. And frankly, when you ask a group of people for help, you'll see who steps up. There will be someone in that organization that steps up and wants to be a part of the solution.

6. Conclusion

Enza:

- Cyber is a sharing environment where we all need to work together to continue to beat the bad guys and reduce our threat vectors. As industry leaders and as a cybersecurity team of professionals we're here to help.
- **We can provide either role-based consulting or we can look at outcome-based solutions in managing your projects. If it's about skills, capacity and operational excellence we can assist with any of our managed and hosted services.**
- ISA Cybersecurity is here to help. If you are a practitioner, a certified cybersecurity professional, who is looking to join a great dynamic team as well, please let us know. As we continue to grow our skilled pool of consultants who we believe can provide world-class services to you and your team.
- **Contact us: info@isacybersecurity.com | 1-877-591-6711**