Insight Space

cyber insights programme

nccgroup

Executive Analysis

Three actions to reduce your cyber security skills gap during COVID-19

Stephen Bailey

Despite multiple initiatives to address the cyber security skills gap in the last decade, it is still a major problem for organisations: according to our research of 290 cyber decision makers, internal skills shortages are one of their main security challenges for the next six months.

These shortages have been exacerbated by cost-cutting measures during COVID-19: 40% of respondents admitted that they had frozen recruitment in cyber in 2020, with 29% reporting that they had made security personnel redundant. One in five had furloughed people responsible for cyber resilience programs.

However, organisations that cut their people budgets reported an increase in every type of cyber attack in the last 12 months, suggesting that the strength of your people is directly related to the resilience of your organisation.

With this in mind, we outline three actions to reduce your cyber security skills gap and build resilience against the new threat landscape that has emerged during COVID-19.

TARGET YOUR RECRUITMENT

Nearly two-thirds of respondents claimed that 'more heads in the team' would make the biggest improvement to their cyber security preparedness. However, recruitment can be costly and time-consuming, so it's important that it is focused on quality rather than quantity. Practically, this means that you should identify the specific skills that your organisation would benefit from and target your recruitment to provide those skills.

Firstly, review your business strategy and create a security roadmap to determine the skill sets that you will need to execute that strategy. For example, if you are launching digital transformation projects, you will need people with specific expertise around moving to the cloud. If you are acquiring or merging with another organisation, you need someone who can assess the risks of that organisation and how it will affect your security posture.

If you don't know what your current security requirements are, consider assessments such as red teaming exercises or cloud security reviews that can identify your risks in specific areas. Benchmarking tools can also help you to establish your short, medium and long-term priority areas, enabling you to recruit strategically and cost-effectively within those areas.

Ultimately, cyber security is such a broad subject that it is impractical to recruit experts in every area. By focusing on the specialisms that are most relevant to your strategy and security roadmap, you can cut through the competitive cyber recruitment market and acquire the skills that will tangibly increase your resilience against cyber threats.

DEVELOP AND RETAIN YOUR TALENT

The competition for skills has driven cyber salaries sky high, so it's not surprising that they were some of the first to be cut when budgets tightened during COVID-19. However, half of our respondents admitted that they had issues with recruiting and retaining cyber expertise, indicating that they are not confident of doing so even when they can afford it.

People regularly leave to secure a higher salary elsewhere, creating a revolving door effect that makes it difficult for organisations to address their skills gaps. However, skilled individuals also leave because their employers fail to deliver a well-defined career path for them, presenting an opportunity for you to develop and retain your talent more effectively.

Start by reviewing exit interviews to establish why previous employees decided to leave: 71% of decision makers told us that they are 'not confident' about improving their organisation's security posture, so ensure that you offer tailored training and development initiatives that empower people to do their jobs effectively.

You should also consider an apprenticeship and training scheme to develop the skills that your organisation requires internally. By giving your senior employees responsibility for training those apprentices, you can give them a greater sense of purpose and career satisfaction, reducing the likelihood that they will be tempted away by other organisations.

It's likely that you will need to recruit specialists in some areas. However, by investing in your existing talent, you can reduce your skills gap without committing huge chunks of your budget. You can also make your organisation more attractive to new recruits as budgets recover from the impact of COVID-19.

OUTSOURCE EFFECTIVELY

Outsourcing is one of the most effective ways for an organisation to complement and strengthen its internal resources, and 66% of respondents told us that they intended to trust more aspects of their cyber resilience activities to third parties in the next 12 months.

With budgets stretched, outsourcing offers decision makers a quick and cost-efficient method to improve their cyber resilience until they can afford to recruit dedicated specialists. It also allows organisations to determine their resource requirements before making firm commitments to spending on recruitment, enabling them to allocate their budgets more effectively.

For example, respondents told us that cyber threat intelligence and security monitoring and detection were the two areas of cyber resilience that were most likely to be outsourced in the next 12 months. Both of these fields require dedicated teams of experienced specialists working around the clock to stay ahead of threat actors and new attack trends, so it would not always be practical for many businesses to recruit here.

Outsourcing can also give organisations the flexibility to address specific short-term security requirements that can't always be addressed internally. For example, more than a third of respondents planned to outsource cyber security awareness training, indicating that they recognise its importance but are not confident that they have the resources to deliver it in-house.

Against the new threat landscape, this 'try before you permanently buy' approach could be an effective way to determine which skills your organisation needs to recruit and which you can afford to outsource. By relieving under-resourced security teams, it can also reduce the skills gap in the short and long-terms.

CONCLUSION

Understanding the threat landscape after COVID-19 was named as the biggest challenge facing our respondents in the next six months. The specific threats are yet to be fully realised, but the data suggests that organisations with strong internal skills and resources will be more resilient against them than those that have cut their people budgets in the last 12 months.

Skilled cyber experts are in short supply compared to the demand. However, by targeting their recruitment, developing and retaining their talent and outsourcing effectively, cyber security leaders can begin to reduce their skills gap as budgets recover during COVID-19.

Three actions to reduce the skills gap during COVID-19

1. **Target your recruitment:** review your business strategy and create a security roadmap to determine your specific security requirements.

2. **Develop and retain your talent:** invest in your people to develop the skills you need internally.

3. **Outsource effectively:** complement and strengthen your internal resources by outsourcing aspects of cyber resilience projects that would be impractical to recruit for internally.

Insight Space

cyber insights programme

nccgroup

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers worldwide to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience and global footprint, it is best placed to help businesses assess, develop and manage the evolving cyber risks they face.

To support its mission, NCC Group continually invests in research and innovation, and is passionate about developing the next generation of cyber scientists.

With over 1,800 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

To discuss how you can manage your people risk, speak to our team today.

+44 (0)161 209 5111

response@nccgroup.com

www.nccgroup.com