

♥ S T O
T T A N
D M A Y



Cyber
Security
in focus

ABOUT THE RESEARCH

Cyber Security in Focus 2020

The Stott and May *Cyber Security in Focus Survey* examines the key issues that have made an impact on the market over the course of this year. Our research is based on the collective experience of 55 cyber security leaders sourced from Stott and May's professional network. Respondents were asked to share their views across a wide range of issues including, but not limited to, the skills shortage, the boardroom perception of cyber security, talent attraction and the challenges associated with securing business in the cloud. In conjunction with our primary quantitative research, qualitative interviews were also conducted with leading thinkers in the cyber security space.

Executive Summary

Findings show that businesses are still struggling to resource their cyber security functions, inhibiting their ability to execute on strategy at a time where security is becoming a more important part of the value proposition.

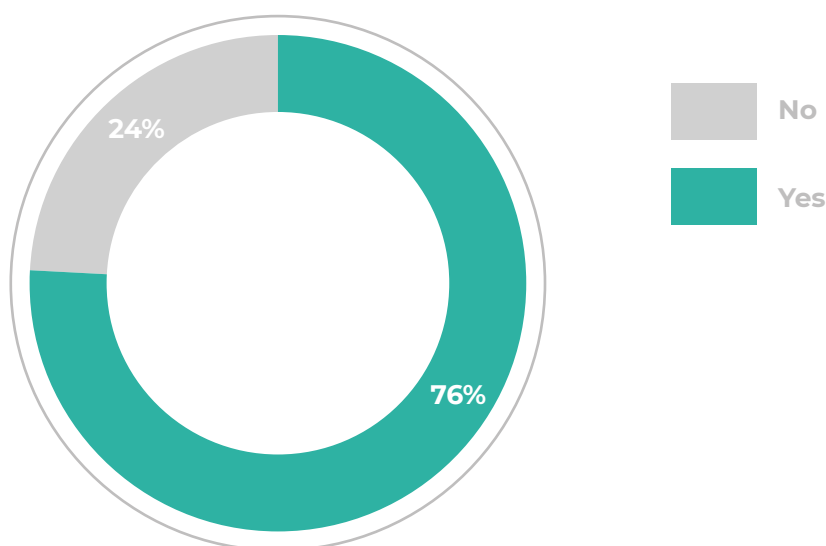
- **Most respondents (76%) believe there is a shortage of cyber security skills in their company, which represents a marginal improvement on 2019 (88%), however, the problem still seems more potent for mid-market and large enterprise businesses.**
- **Organisations are still struggling to source cyber security talent (72%) with no material improvement around time-to-hire from 2019.**
- **Internal skills still represent the biggest inhibitor in delivering cyber security strategy (39%), while senior security leaders report increased year on year challenges around budget (30%).**
- **The business perception of cyber security is moving away from unnecessary expense (15%) towards strategic priority (54%) in the wake of well publicised breaches resulting in fines and reputational damage.**
- **Customers are becoming more educated and demanding around the issue of cyber security, driving most respondents (69%) to conclude that their business feels that functions can add value to their companies' overall proposition.**
- **As more business move towards the cloud 54% of cyber leaders believe we will see an increase in incidents.**
- **Security leaders are getting more creative around resourcing their functions with 30% looking internally for transferable skills and some (46%) believing that AI and Machine learning could be used to offset staffing issues.**

The skills shortage is still evident

Over the past 5 years the cyber security skills shortage has been well publicised, almost leading to a certain level of fatigue around the issue for those in the industry.

Our respondents indicated a marginal, if not statistically significant, year on year improvement in the situation with 76% reporting a shortage of cyber security skills (down from 88% in 2019). But with unfilled positions crossing the 4 million mark globally, the skills gap discussion is unlikely to go away any time soon until grass roots initiatives begin to make an impact. Based on our findings there is no clear evidence to conclude that things are improving, putting talent acquisition and retention strategies in sharp focus.

Do you believe there is a shortage of cyber security skills in your company?



The need to cope with the surge in demand for cyber security skills was more evident for US based respondents with 81% pointing to a shortage of resources in their company, closely followed by the UK (72%) and mainland Europe (60%). This arguably stands to reason with Germany, France, Israel and Russia representing four of the more sophisticated cyber security markets, offering strong grass roots foundations and above average salaries that are attractive to those willing to relocate.

Cyber security skills shortage by region

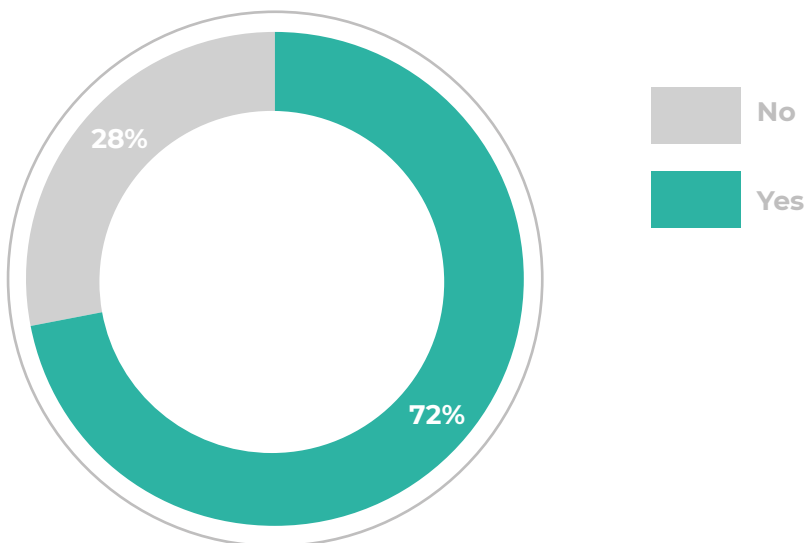


Our survey data also reveals that mid-market businesses (83%) are feeling the most pain in terms of the skills shortage, followed by large enterprises (79%) with SMB's still significantly impacted at 64%. This may say something about the complexity of the perceived threat in businesses with over 100 employees. What is clear is that cyber security leaders need to remain mindful of the impact that the skills shortage is having on staff workload and morale. Less resource means less time collaborating with the business and less time developing skills in new technologies.

The talent market remains highly competitive

Based on the skills shortage data, it's perhaps not surprising that 72% of our sample stated that they struggle to source cyber security talent for their business. The challenge comes partly down to a scarcity of skills in the market alongside a lack of budget for headcount and recruitment initiatives.

Do you struggle to source cyber security talent for your business?



Hiring managers are seeing particular challenges around the more technical skillsets associated with areas such as: cloud security, SOC analysis, penetration testing and incident response. The scarcity of candidates in this space coupled with a desire for 'softer skills' is causing significant bottlenecks at the entry level, whilst putting pressure on line managers to nurture and retain the experienced talent they currently have at their disposal. Further up the organisation we are seeing more availability of CISO candidates in the market. Interestingly, our survey found that 'Head of' and 'Manager' respondents struggled more in terms of sourcing talent (88%) than the CISO group (65%). Again, the mid-market businesses tended to struggle more with sourcing security talent (83%) compared with 76% in large enterprise and 57% in SMB.

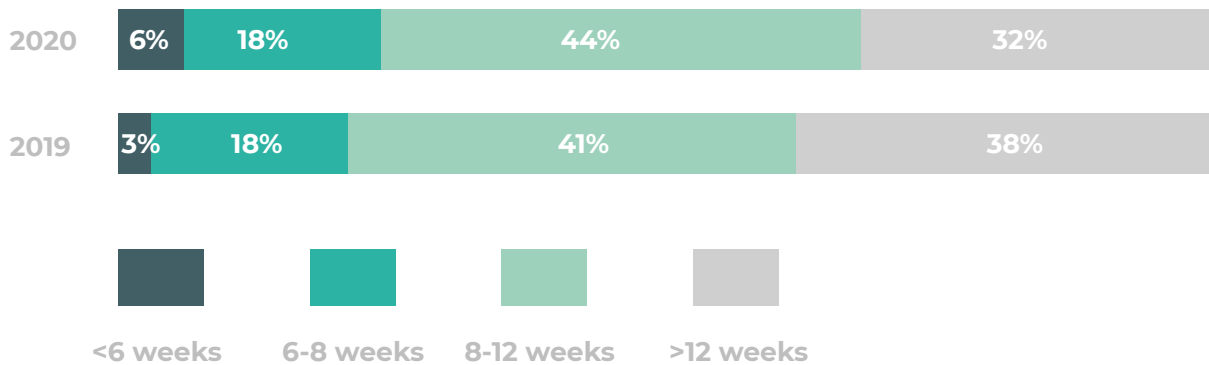
Cyber security talent acquisition challenge by company size

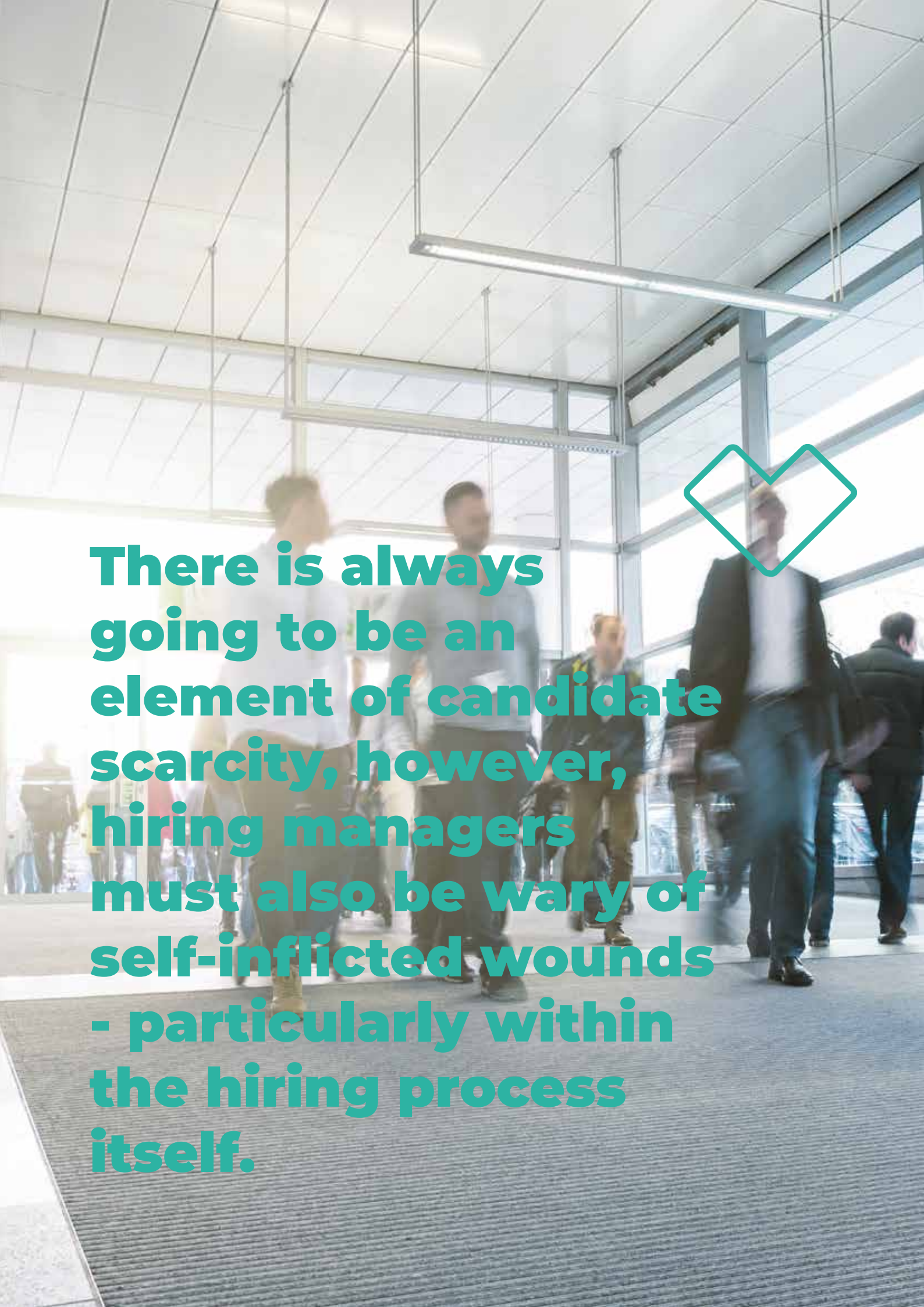


Time to hire still represents a significant challenge for security leaders. Our results show limited year on year improvements with 32% of respondents experiencing open roles for in excess of 3 months. There is always going to be an element of candidate scarcity, however, hiring managers must also be wary of self-inflicted wounds - particularly within the hiring process itself.

Collaboration with HR and internal recruitment needs to be strong to ensure job descriptions balance neatly against compensation packages. The hiring process should be streamlined to ensure 'high potential' candidates are not lost to a protracted and drawn out series of interviews. Tapping into a more diverse, untapped talent pool should also remain a priority placing a sharp focus on the employee value proposition and career progression plans. Cyber security leaders also need to play a greater role in exposing their functions to talent communities in the shape of meetups and 3rd party events. Marginal gains can be achieved in this space by being more visible, precise and realistic.

Time to hire security professionals



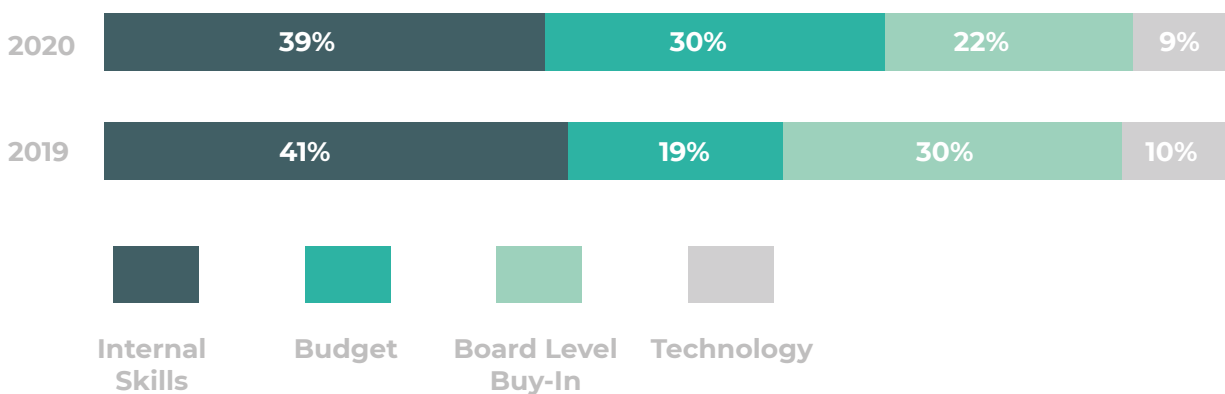


There is always going to be an element of candidate scarcity, however, hiring managers must also be wary of self-inflicted wounds - particularly within the hiring process itself.

Lack of internal talent still a major barrier to strategy execution

Our survey shows that internal skills remains the biggest inhibitor to the delivery of cyber security strategy (39%). The barrier that saw the largest year on year increase (from 19% to 30%) was budget. Technology is still perceived to be the smallest impediment for security leaders in delivering key initiatives (9%). In fact, many CISO's cited that a strategy that is too technology or tools focused can cause ineffective outcomes as a result of a siloed approach.

What do you believe is the biggest inhibitor to delivering cyber security strategy?

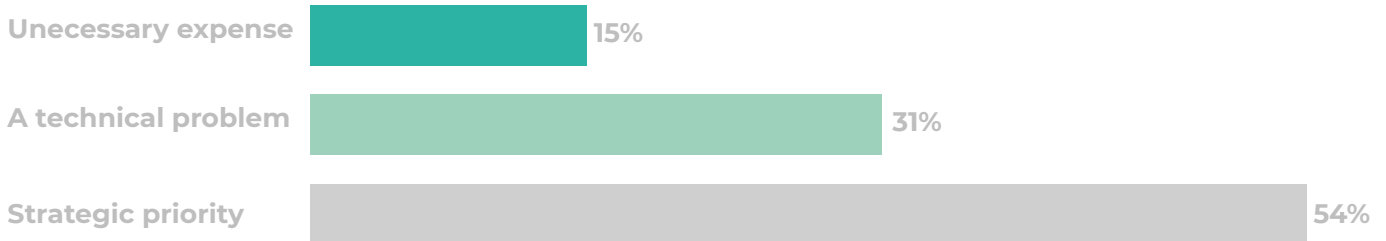


It's worth noting that none of the inhibitors above are mutually exclusive. CISO's need to consider how much their teams can reasonably deliver with the internal skills at their disposal and factor that into budget discussions. Requests for budget need to align back to the goals of the business, whether that be around protecting against reputational damage or improving the value proposition. Credibility is also key here. If you ask for budget do it off the back of a collaborative business case and make sure you deliver on it.

CISO's we spoke to also pointed to challenges around organisational design and process as key barriers to delivering on security strategy. The reporting line is important for CISO's to ensure their message is being heard (and understood) at the board level. But we also need to ensure the approvals process is agile enough to support the security function's ability to support the business at the pace it wants to operate at.

Cyber security moves up the value chain

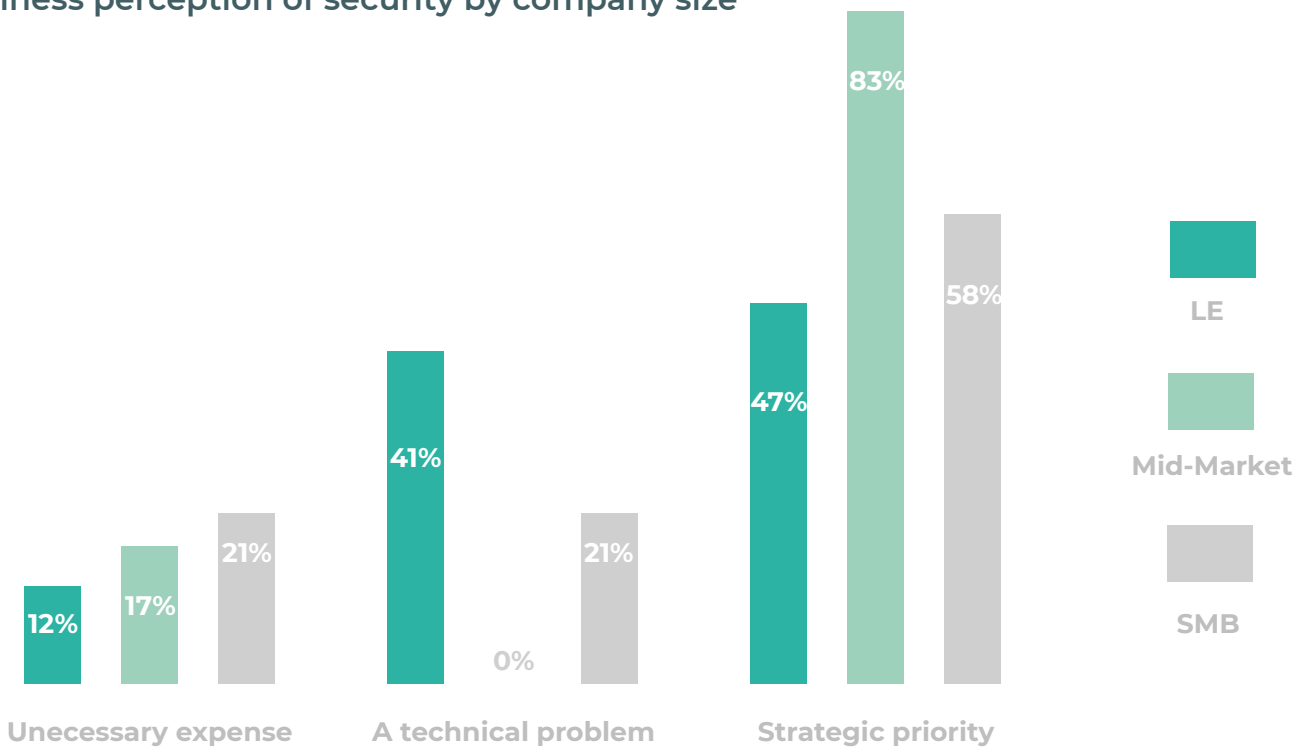
How does your business perceive cyber security?



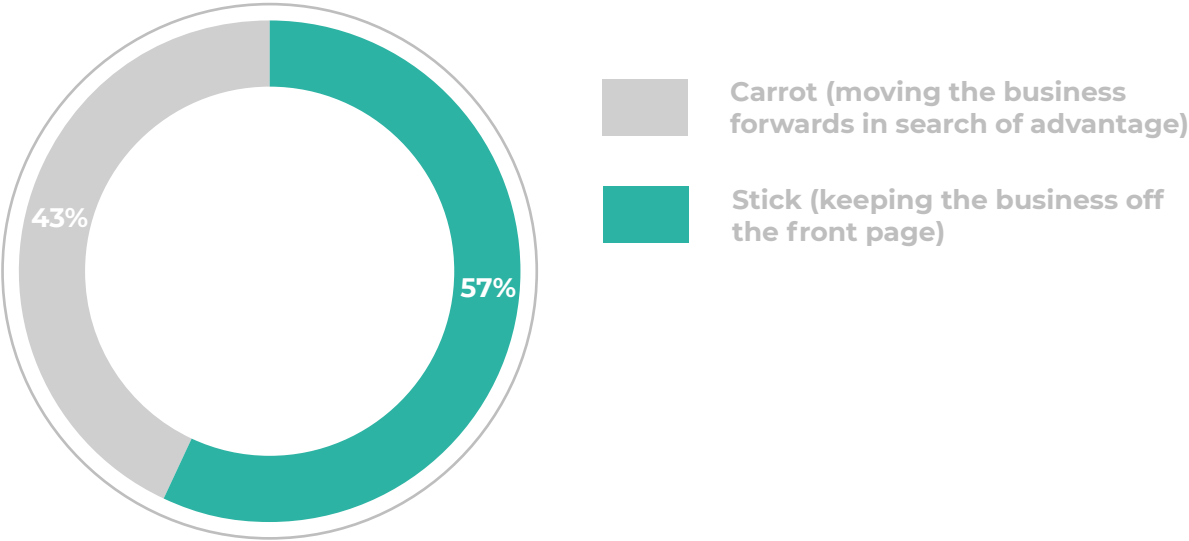
There's little doubt that our respondents see cyber security moving up the list of boardroom issues, with 54% stating their businesses treat the issue as a strategic priority. This perception seems to be even stronger in high growth mid-market firms, with 83% pointing towards its strategic significance.

This is perhaps unsurprising given the growing importance of security to the overall digital transformation strategy. As companies continue to evolve their digital presence, they will continue to create more vulnerabilities and points of entry that, if exposed, can have a far-reaching impact on the profitability of the business.

Business perception of security by company size



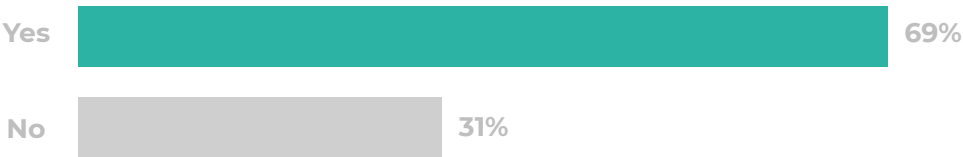
Is cyber security investment driven by the carrot or the stick in your business?



Our survey suggests that building the business case for cyber security investment is largely driven by the ‘stick’ of ensuring the company does not become front page news (57%). The ever-evolving cyber threat to the business is always going to sharpen the mind of the board particularly given the nature of high profile data breaches we have seen globally over the last three years. The evolving regulatory landscape in the shape of the CCPA, and fines, associated is also likely to help grab boardroom attention and present a platform for investment in data protection.

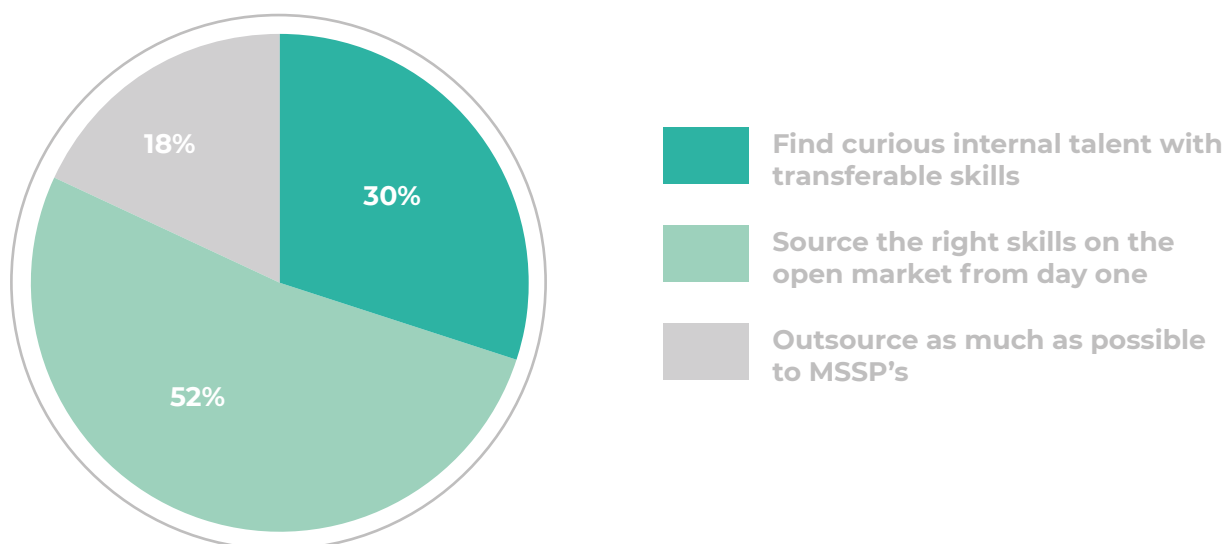
The reality is that any investment in cyber security is about a combination of sticks and carrots. It’s pleasing to see that 69% of our sample believe in the potential for the function to enhance the value proposition to customers. We see this particularly in software and services companies where security features are a pre-requisite for buyers but also more generally as customers become more aware of cyber risk. The challenge for CISO’s is to instil a security culture into the organisation and embed security tightly within increasingly agile and fast moving development functions.

Does your business believe the cyber security function in your company enhances the value proposition to customers?



Hiring managers are getting more creative around resourcing functions

Which statement best sums up your companies approach to building cyber security teams?

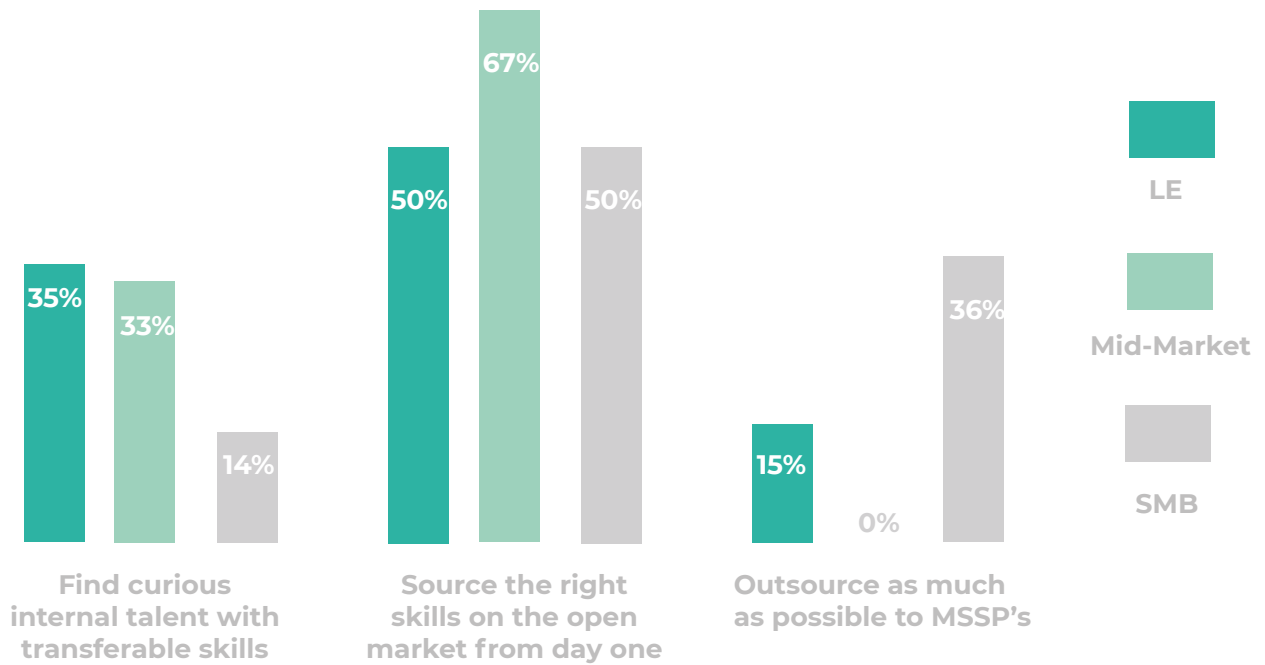


In light of the cyber security skills gap, our survey suggests that hiring managers are becoming more creative around how they resource their functions from hiring strategies through to the use of AI and Machine learning to offset work. Some hiring managers (30%) are beginning to look internally first in the hunt for the transferable skills and core competencies, such as curiosity, in an attempt to reduce the bottleneck. This strategy is clearly more common in large enterprises (35%) and mid-market organisations (33%) where internal candidates are more readily available.

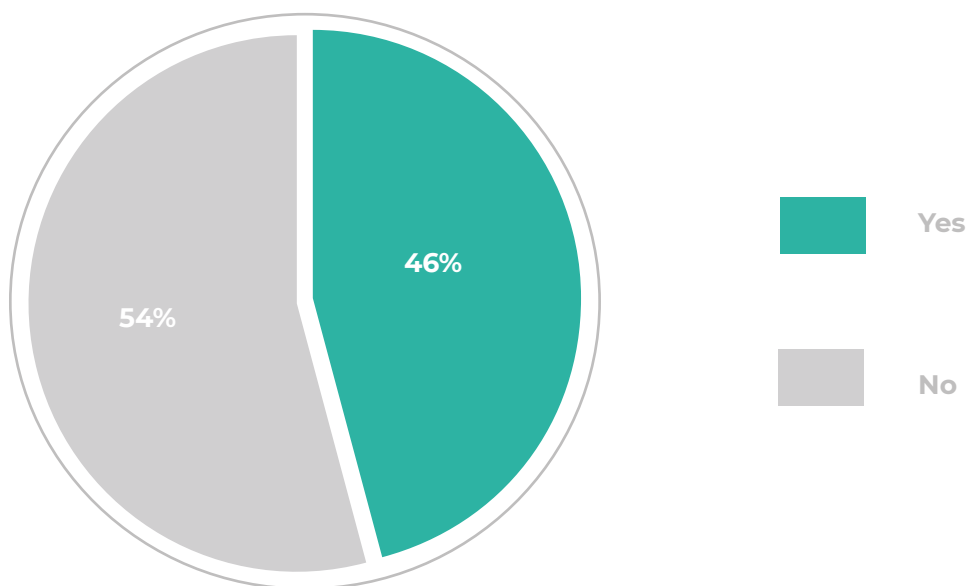
Another option available to CISO's is to outsource areas such as SOC to MSSP's. Our results suggest that this option is more popular with SME's (36%) and large enterprises (15%) with mid-market businesses seemingly keener to keep efforts in-house. The overwhelming preference (52%) is to find the right skills on the open market from day one but where that isn't possible CISO's are having to think more creatively.

Some CISO's we spoke to were conscious of the need to automate as much as possible in order to free up valuable people resources for more complex investigations, projects and interaction with the business. 46% of our sample stated that they saw the potential for AI and Machine Learning to help in offsetting the resource challenge in this space. AI is already being deployed in cyber defence and is becoming even more important as businesses continue to move towards the cloud. It's clear that AI and Machine Learning also represents a threat, in terms of enhancing malware and analysing vulnerabilities in target networks, as much as it does an opportunity for cyber security functions and will be an interesting space to watch in the year ahead.

Approach to building cyber security teams by company size



Do you believe AI and Machine Learning can be used to offset security hiring challenges?



Safely does it in pursuit of cloud benefits

Do you believe security incidents will increase as a result of companies pursuing a cloud first strategy?



Our survey suggests that we are reaching a tipping point regarding the perception of security in the cloud. 54% of our security leaders believed that we will see an increase in security incidents as a result of companies moving towards the cloud. As businesses continue on the path to digital transformation, increasing cloud adoption becomes inevitable to leverage the ease of use and scalability on offer. CISO's remain concerned about potential data loss with the distributed nature of the cloud presenting challenges with visibility and control. CISO's must assess their cloud security posture on a regular basis and have well-rehearsed incident response plans in place covering cloud applications.

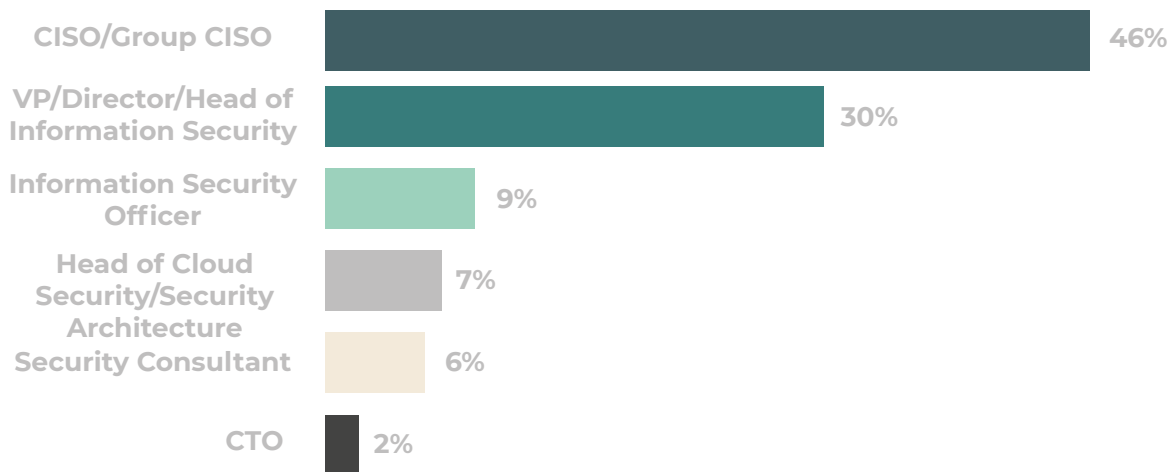
CISO's must assess their cloud security posture on a regular basis and have well-rehearsed incident response plans in place covering cloud applications.



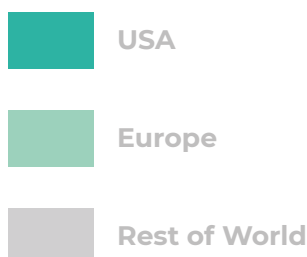
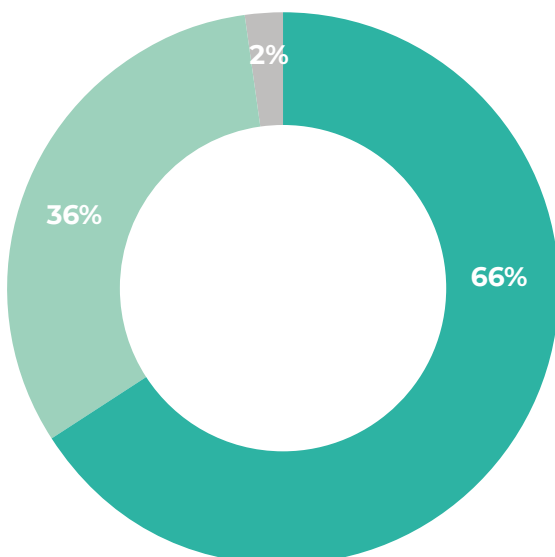
Survey respondent demographics

The sample comprised of 55 pre-qualified cyber security professionals from Stott and May's professional network. Completion of the survey was voluntary, and respondents were not incentivised to take part in the research. The survey consisted of 12 questions including 4 qualifiers to protect the integrity of the sample.

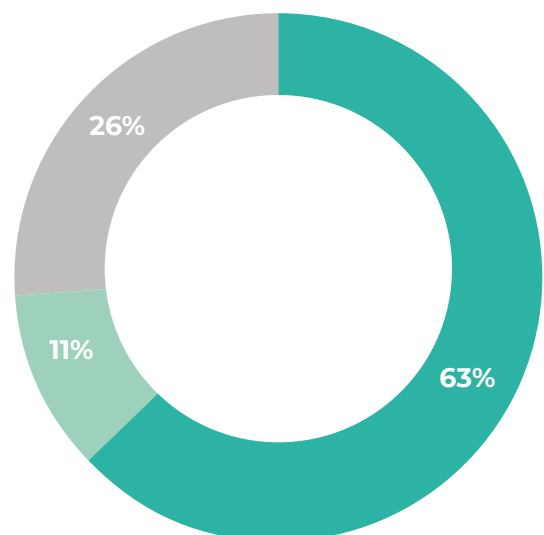
Respondents by job role



Respondents by country



Respondents by company size

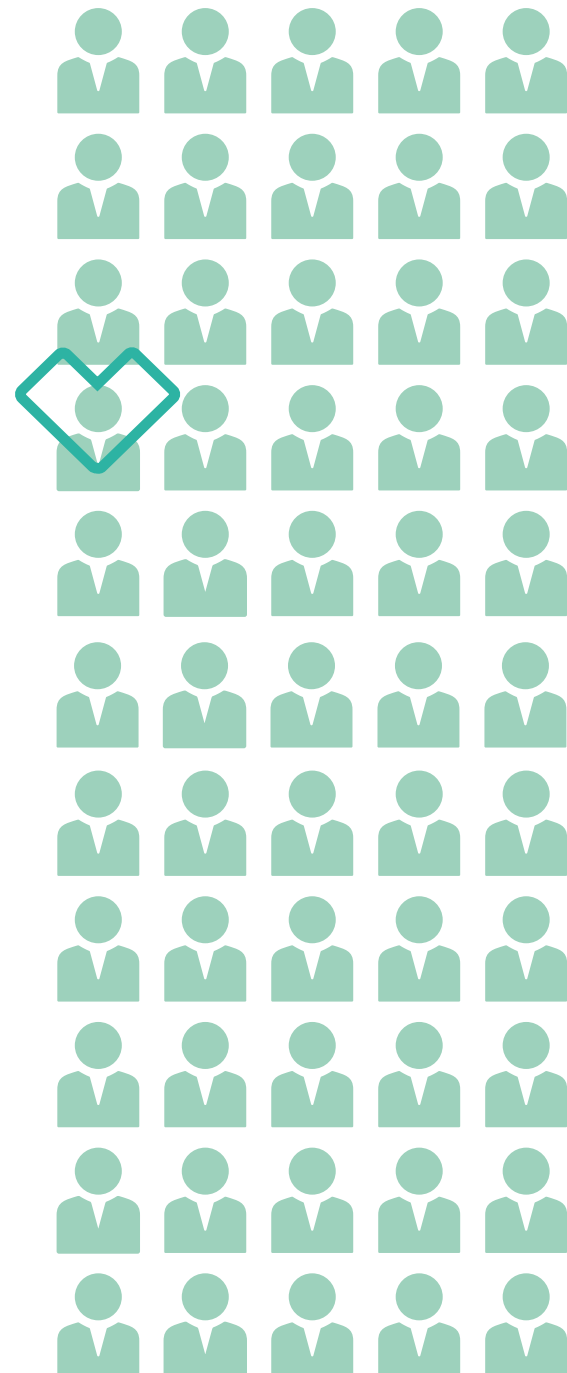


CISO in focus

Jim Rutt – CISO, Dana Foundation

Jim Rutt, CISSP-ISSAP/ISSMP, CCSP, CSSLP, CISM, CISA, CGEIT, CRISC, C|CISO, CCSK, is the Chief Information Officer/ CISO at the Dana Foundation. His responsibilities include providing strategic planning for information and technology management and overseeing all back-office technology operations necessary to support the Foundation. Jim is an early adopter of cutting-edge cloud security solutions, having led Dana through a complete cloud transformation five years ago. Jim has frequently spoken to peer organisations on corporate cyber security strategy and risk management, and also advises early stage technology companies on their business strategy to the financial and healthcare sector.

Jim is a graduate of Stetson University, where he received a B.B.A. degree. He has 22 years of technology experience (spanning financial, healthcare and pharmaceutical sectors) and has been at Dana for nine years. Jim has presented at multiple CIO and leadership conferences and has been quoted in the Wall Street Journal (among other publications) for his view on mobile security and governance. Jim is the former President and Chairman of the Board of Technology Affinity Group (TAG) and is Vice President and Board Director for the New York Metro Chapter of the Cloud Security Alliance, as well as an Advisory Board member of the EC-Council C|CISO Advisory Board, as well as a founding advisory board member of BWG Strategy LLC, a Work-Bench Venture Capital Mentor/Advisor, advisor to Lightspeed Ventures, a Silicon Venture capital company, advisor to Vation Ventures, Glilot Partners, and board advisor to multiple startups including ShieldX, Tala Security, Baffle, Axonius, Minerva Labs and Pixm, amongst others.



What do you see as the key challenges sitting in front of the CISO community in 2020?

Obviously, the landscape has changed slightly as a result of the COVID-19 situation where CISO's will now be looking to get a better handle on their remote and mobile workers. I think a lot of cyber leaders who thought they had a solid strategy in this area, with a limited set of remote workers, are now finding those plans to be tested. I would expect that we are likely to see a lot more focus and investment in this area.

But over and above these more recent events there are a range of other priorities sitting in front of the CISO for 2020. We certainly need to be focusing on gaining improved maturity in terms of risk measurement and metrics. Particularly when reporting these metrics to our respective boards. Asset management would also be a priority item. I think a lot of CISO's don't have the same level of experience of asset management that many CIO's do. The fact remains though that you cannot protect what you don't know you have, so focus needs to be applied in this area.

Insider threat will also be front of mind for CISO's. Nobody's got a robust plan from what I've seen in terms of monitoring suspicious internal behavior whether it's intentional or otherwise. Automation remains another challenge. We are already seeing some efforts towards automation, but I think they've potentially been targeted at the wrong places. We shouldn't be putting our workforce in charge of automating out elements of their own jobs. It's just not going to work. It should be more of an architectural concern.

API security is also critical as we are still seeing a disconnect between development and security. There needs to be an increased focus in closing that gap, which is all too often a knowledge gap as much as anything else. There are a lot of API's that are being exposed out by corporations that haven't been vetted properly and there's no real way of monitoring that from a top-level governance perspective.

What would your advice be to security leaders who are struggling to embed a culture of security in their business?

At a very high level, the best advice I think I could give to CISO's here is make sure you tell every stakeholder 'what's in it for them'. You're asking people to change the way they work and that can have a whole range of downstream effects causing the population to be resistant to change. But it's a challenge you need to overcome because the users are the largest gap in any organisation's security operations program. CISO's need to ensure that with every initiative, whether that be digital transformation or new applications being rolled out, they make the security features and 'asks' prominent within the project. Raise awareness of where the issues exist and where the gaps could be exposed. Collective commitment is going to be essential to maintaining a holistic security posture.



What are the technology focus areas that you think that CISO's should be exploring further in 2020?

Automation and insider threat are going to be key plays as I have already alluded to. A new and evolving area in my view is around DevSecOps, where we have that gap between development operations and security. There are a lot of new development paradigms we are seeing out there like containerization, microservices, orchestration with platforms like Kubernetes and there's not a lot of understanding about the security implications of deploying these new technologies. Luckily, I think we are less than a year away from maturity for some of the solutions out there targeted towards DevSecOps.

Some of the newer items I am starting to look at in 2020 and beyond are around the impact of quantum computing and quantum cryptography. As these standards get solidified it will have a definite impact which will be essential in protecting our data moving forwards. We need to start thinking 5 years ahead in this space and consider how we integrate these technologies into legacy business processes.

Do you buy into the skills shortage in security? What roles do you find particularly challenging to hire for?

I would say that I 'somewhat agree' there is a skills gap in our industry. I think it's more apparent in individual contributor roles like Security Architects, Security Engineers and high level SecOps professionals. There's definitely a shortage of good talent in those areas, emphasizing the word 'good'. But at that leadership level, whether it be Directors or CISO's, I see no real shortage.

In terms of the roles that are more challenging to hire for I would say the issue is most concentrated in the positions that often have the highest amount of churn. First and second level SecOps types roles would be a good example here, because these jobs are perceived as more of a steppingstone in people's career, where there's a desire to

progress through these positions within one to two years. This presents real challenges from a retention perspective. Security leadership and human resources need to start thinking more creatively around how we can keep these individuals engaged for longer by investing more in personal development. There's a real cost to failing to retain talent in this area.



What advice do you have for CISO's looking to leverage their existing people resource more effectively?

The first thing that most CISO's are going to gravitate towards is trying to leverage some form of artificial intelligence or automation. There's upside here in terms of making teams work a lot smarter and reducing the volume of manual tasks. Often the challenge is the burden on building these initiatives falls on the SOC team rather than the architectural or leadership teams. These individuals are less likely to understand, from an enterprise perspective, what they should be automating and where the priorities sit. CISO's need to be looking at solutions that reduce manual work, but they need to really have skin in the game from a technical and process perspective about what's going on and what is going to be viable.

What challenges are cloud adoption and the IoT throwing up for security leaders?

Looking at cloud adoption first, the biggest challenge for both security and operational leaders in IT is the perception that you can just take what you have on-premise, migrate it to the cloud and you can keep the same controls in place and everything will work out fine. CISO's need to get a lot more educated on what they truly need from a defensive posture in a cloud environment. They should work more closely with their CIO's to understand the technical and migration ramifications around some of these workloads. It's key to beef up their understanding of how this new world of cloud really works and how to defend it properly.

When it comes to the Internet of Things there are a multitude of challenges. We've got this almost geometric growth of sensors generating data at scale. There's also a vast difference in the way a lot of these sensors work coupled with the different protocols that they use. We don't often know what the vulnerabilities of these protocols are – some of which can be very old. I think there's been a reasonable effort out there to develop solutions around securing IoT but we are in

the really early innings and it will be a number of years before we see a maturity around the technical controls needed to defend an IoT network.



A woman with dark, curly hair is shown from the chest up, wearing a light blue button-down shirt. She is looking off to the right with a thoughtful expression, her arms are crossed. The image is framed by a large teal circle. The background is a blurred office setting.

Cyber Security Salary Guidance 2020

Cyber Security Salary Insight

United Kingdom (£)

Role	Perm			Contract (Day Rate)		
Manager/Executive Level	Low End	High End	Average	Low end	High End	Average
CISO	125,000	500,000	200,000	1,000	2,500	1,500
Deputy CISO	90,000	150,000	110,000	800	1,400	1,100
Head of Information Security Risk	90,000	150,000	110,000	700	1,400	1,100
Senior Manager, Information Security Risk	80,000	110,000	95,000	650	1,100	800
Director, Security Engineering	100,000	180,000	120,000	750	1,400	1,000
Director Application Security	110,000	190,000	130,000	750	1,400	1,000
Director, Incident Response & Security Assurance	95,000	160,000	120,000	700	1,300	900
Director, Security Operations & Threat Management	100,000	150,000	110,000	700	1,300	900
Director, Identity & Access Management	90,000	130,000	105,000	700	1,300	1,000
SOC Manager	75,000	125,000	95,000	600	900	700
Security Architecture	Low End	High End	Average	Low End	High End	Average
Chief Security Architect	100,000	150,000	120,000	800	1,500	1,000
Application Security Architect	80,000	130,000	100,000	600	1,000	750
Infrastructure Security Architect	75,000	110,000	90,000	550	850	700
Product Security Architect	80,000	125,000	90,000	650	1,100	800
Network Security Architect	65,000	95,000	85,000	500	850	600
Digital Security Architect	75,000	120,000	95,000	600	900	750
Enterprise Security Architect	90,000	125,000	110,000	650	1,200	800
DevSecOps Architect	80,000	130,000	100,000	650	1,100	750
Cloud Security Architect	80,000	120,000	95,000	650	1,100	750
GRC Information Security Architect	80,000	120,000	95,000	550	900	700

Role

Perm

Contract (Day Rate)

Security Engineering/Operations	Low End	High End	Average	Low End	High End	Average
SOC Team Lead	70,000	100,000	85,000	500	800	600
Senior Security Analyst	50,000	90,000	65,000	400	600	500
Security Analyst	35,000	60,000	50,000	300	450	400
Cyber Threat Hunter	55,000	110,000	75,000	500	900	600
Threat & Vulnerability Engineer	50,000	95,000	75,000	400	800	550
Penetration Tester	45,000	110,000	70,000	400	1,100	600
Software Security Engineer	65,000	110,000	75,000	550	1,000	650
Cloud Security Engineer	60,000	105,000	85,000	550	900	650
Application Security Engineer	60,000	105,000	85,000	550	900	650
Incident Response Engineer	60,000	80,000	65,000	450	800	600



Cyber Security Salary Insight

Europe - DACH (€)

Role

Perm

Contract (Day Rate)

Manager/Executive Level	Low End	High End	Average	Low end	High End	Average
CISO	110,000	200,000	150,000	1,000	2,500	1,500
Deputy CISO	85,000	150,000	120,000	800	1,400	1,100
Head of Information Security Risk	85,000	125,000	95,000	700	1,200	1,000
Senior Manager, Information Security Risk	80,000	110,000	95,000	650	1,000	750
Director, Security Engineering	80,000	150,000	125,000	750	1,400	1,000
Director Application Security	85,000	150,000	135,000	750	1,400	1,000
Director, Incident Response & Security Assurance	85,000	160,000	120,000	700	1,300	900
Director, Security Operations & Threat Management	100,000	150,000	110,000	700	1,300	900
Director, Identity & Access Management	90,000	130,000	105,000	700	1,300	1,000
SOC Manager	75,000	105,000	85,000	500	900	650

Security Architecture	Low End	High End	Average	Low End	High End	Average
Chief Security Architect	85,000	125,000	100,000	800	1,500	1,000
Application Security Architect	80,000	130,000	100,000	600	1,000	750
Infrastructure Security Architect	75,000	110,000	90,000	550	850	700
Product Security Architect	80,000	125,000	90,000	650	1,100	800
Network Security Architect	65,000	95,000	85,000	500	850	600
Digital Security Architect	75,000	120,000	95,000	600	900	750
Enterprise Security Architect	85,000	120,000	100,000	650	1,200	800
DevSecOps Architect	80,000	130,000	100,000	650	1,100	800
Cloud Security Architect	70,000	120,000	90,000	650	1,100	750
GRC Information Security Architect	70,000	100,000	85,000	550	900	650

Role

Perm

Contract (Day Rate)

Security Engineering/Operations	Low End	High End	Average	Low End	High End	Average
SOC Team Lead	65,000	90,000	75,000	500	800	600
Senior Security Analyst	45,000	70,000	50,000	400	600	500
Security Analyst	35,000	65,000	45,000	300	450	400
Cyber Threat Hunter	55,000	85,000	65,000	500	900	600
Threat & Vulnerability Engineer	50,000	85,000	60,000	400	800	550
Penetration Tester	45,000	100,000	75,000	400	1,100	600
Software Security Engineer	65,000	120,000	90,000	550	1,000	650
Cloud Security Engineer	65,000	120,000	90,000	550	900	650
Application Security Engineer	65,000	120,000	90,000	550	900	700
Incident Response Engineer	65,000	100,000	90,000	450	800	600



Cyber Security Salary Insight

Europe - Benelux (€)

Role

Perm

Contract (Day Rate)

Manager/Executive Level	Low End	High End	Average
CISO	110,000	200,000	150,000
Deputy CISO	85,000	150,000	120,000
Head of Information Security Risk	85,000	125,000	95,000
Senior Manager, Information Security Risk	80,000	110,000	95,000
Director, Security Engineering	80,000	150,000	125,000
Director Application Security	85,000	150,000	135,000
Director, Incident Response & Security Assurance	85,000	160,000	120,000
Director, Security Operations & Threat Management	100,000	150,000	110,000
Director, Identity & Access Management	90,000	130,000	105,000
SOC Manager	75,000	105,000	85,000

Low end	High End	Average
1,000	2,500	1,500
800	1,400	1,100
700	1,400	1,100
650	1,100	800
750	1,400	1,000
750	1,400	1,000
700	1,300	900
700	1,300	900
700	1,300	1,000
600	900	700

Security Architecture	Low End	High End	Average
Chief Security Architect	85,000	125,000	100,000
Application Security Architect	80,000	130,000	100,000
Infrastructure Security Architect	75,000	110,000	90,000
Product Security Architect	80,000	125,000	90,000
Network Security Architect	65,000	95,000	85,000
Digital Security Architect	75,000	120,000	95,000
Enterprise Security Architect	85,000	120,000	100,000
DevSecops Architect	80,000	130,000	100,000
Cloud Security Architect	70,000	120,000	90,000
GRC Information Security Architect	70,000	100,000	85,000

Low End	High End	Average
800	1,500	1,000
600	1,000	750
550	850	700
650	1,100	800
500	850	600
600	900	750
650	1,200	800
650	1,100	750
650	1,100	750
550	900	700

Role**Perm****Contract (Day Rate)**

Security Engineering/Operations	Low End	High End	Average	Low End	High End	Average
SOC Team Lead	65,000	90,000	75,000	500	800	600
Senior Security Analyst	45,000	70,000	50,000	400	600	500
Security Analyst	35,000	65,000	45,000	300	450	400
Cyber Threat Hunter	55,000	85,000	65,000	500	900	600
Threat & Vulnerability Engineer	50,000	85,000	60,000	400	800	550
Penetration Tester	45,000	100,000	75,000	400	800	600
Software Security Engineer	65,000	120,000	90,000	550	1,000	700
Cloud Security Engineer	65,000	120,000	90,000	550	1,000	750
Application Security Engineer	65,000	120,000	90,000	550	900	650
Incident Response Engineer	65,000	100,000	90,000	450	800	600



Cyber Security Salary Insight

USA (\$)

Role

Perm

Contract (Hourly Rate)

Manager/Executive Level	Low End	High End	Average	Low end	High End	Average
CISO	230,000	450,000	300,000	<i>100-120</i>	<i>400-500</i>	<i>200-250</i>
Deputy CISO	200,000	300,000	250,000	-	-	-
Head of Information Security Risk	200,000	355,000	230,000	-	-	-
Senior Manager, Information Security Risk	210,000	300,000	250,000	-	-	-
Director, Security Engineering	210,000	300,000	250,000	-	-	-
Director Application Security	220,000	325,000	260,000	-	-	-
Director, Incident Response & Security Assurance	210,000	285,000	225,000	-	-	-
Director, Security Operations & Threat Management	180,000	300,000	220,000	-	-	-
Director, Identity & Access Management	175,000	300,000	215,000	-	-	-
SOC Manager	140,000	250,000	180,000	<i>60-75</i>	<i>200-250</i>	<i>100-120</i>
Security Architecture	Low End	High End	Average	Low End	High End	Average
Chief Security Architect	200,000	350,000	250,000	<i>100-120</i>	<i>350-425</i>	<i>150-180</i>
Application Security Architect	170,000	300,000	200,000	<i>80-95</i>	<i>200-250</i>	<i>125-150</i>
Infrastructure Security Architect	190,000	290,000	230,000	<i>80-95</i>	<i>200-250</i>	<i>125-150</i>
Product Security Architect	200,000	280,000	240,000	<i>80-95</i>	<i>200-250</i>	<i>125-150</i>
Network Security Architect	180,000	260,000	230,000	<i>80-95</i>	<i>200-250</i>	<i>125-150</i>
Digital Security Architect	180,000	260,000	230,000	<i>80-95</i>	<i>200-250</i>	<i>125-150</i>
Enterprise Security Architect	220,000	320,000	250,000	<i>80-95</i>	<i>200-250</i>	<i>125-150</i>
DevSecOps Architect	200,000	300,000	250,000	<i>80-95</i>	<i>200-250</i>	<i>125-150</i>
Cloud Security Architect	200,000	300,000	230,000	<i>80-95</i>	<i>200-250</i>	<i>125-150</i>
GRC Information Security Architect	200,000	280,000	250,000	<i>80-95</i>	<i>200-250</i>	<i>125-150</i>

Italic = W2

Bold = 1099/C2C

Role

Perm

Contract

Security Engineering/Operations	Low End	High End	Average	Low End	High End	Average
SOC Team Lead	135,000	220,000	165,000	<i>70-85</i>	<i>150-180</i>	<i>115-140</i>
Senior Security Analyst	150,000	180,000	170,000	<i>70-85</i>	<i>150-180</i>	<i>115-140</i>
Security Analyst	120,000	150,000	135,000	<i>50-60</i>	<i>130-155</i>	<i>80-95</i>
Cyber Threat Hunter	140,000	180,000	160,000	<i>70-85</i>	<i>150-180</i>	<i>115-140</i>
Threat & Vulnerability Engineer	150,000	180,000	160,000	<i>60-72</i>	<i>140-165</i>	<i>110-130</i>
Penetration Tester	140,000	180,000	160,000	<i>40-50</i>	<i>150-180</i>	<i>100-120</i>
Software Security Engineer	160,000	210,000	175,000	<i>70-85</i>	<i>150-180</i>	<i>115-140</i>
Cloud Security Engineer	170,000	220,000	190,000	<i>70-85</i>	<i>150-180</i>	<i>115-140</i>
Application Security Engineer	170,000	220,000	190,000	<i>70-85</i>	<i>150-180</i>	<i>115-140</i>
Incident Response Engineer	155,000	190,000	170,000	<i>60-72</i>	<i>140-165</i>	<i>110-130</i>

Italic = W2

Bold = 1099/C2C





About Stott and May

Founded in 2009 Stott and May are a professional search firm with a passion for helping leaders achieve complete confidence that they have hired the right talent, first time in fiercely competitive markets. We believe you should never have to make the choice between quality of candidate and time to hire.

As a result, our business has been founded on the principle of offering a premier standard of search service delivered in vastly accelerated timescales, that our competition simply cannot match. Because after all this is about more than just recruitment, it's about turning your business vision into reality.