STO
TTAN
DMAY

Cyber Security in Focus 2022

In partnership with

FORGEPOINT

About the research

Our research provides an insight into the thoughts and core priorities of a snapshot cohort of 55 security leaders. This study examines critical themes including, the skills shortage, inhibitors to strategy execution, and the business perception of cyber security functions.

Respondents were sourced from Stott and May's professional network across EMEA and North America. The roles surveyed included Cyber Security Directors, Security Operations Directors, VPs of Product Security, with 36% of our sample originating directly from the CISO community. In conjunction with our primary quantitative research, qualitative interviews were also conducted with leading thinkers in the cyber security space.

This report also includes insights from William Lin, Managing Director at Forgepoint Capital, on the emergence of the engineering-centric CISO, and James Dolph, CISO at Guidewire Software, on product security, a vital component of any company's value proposition and operations.

Executive summary & highlights

The pressure on security leaders has perhaps never been more intense. Against a backdrop of dramatic acceleration towards digital transformation and the heightened importance of security to the value proposition, leaders are facing significant challenges in acquiring the appropriate skills to execute on strategy.

- The perceived shortage of cyber security skills within businesses seems to be widening, with 87% of cyber security leaders reporting challenges, which represents an increase on 2021 findings (76%).
- Security leaders continue to experience challenges sourcing experienced talent, with 73% highlighting it as an area of concern. Time-to-hire also remains a potent issue. 35% pointed to positions being left unfilled after a 12-week period.
- Further evolution surrounding the working pattern of security professionals looks likely, with 73% of security leaders favoring a hybrid approach and an additional 22% going fully remote.
- Internal skills continue to represent the single most significant barrier to strategy execution for 43% of cyber security leaders - up from 39% in 2021.
- The significance of cyber security is becoming even more broadly recognized internally, as 80% of security leaders believe their business perceives the function as a 'strategic priority' – up from 54% last year.
- 100% of our sample of cyber security leaders now either agree (38%) or strongly agree (62%) that their business feels the function plays a role in improving the overall value proposition to customers.
- There is growing concern among 51% of respondents that cyber security investment is not keeping pace with the drive towards digital business.
- 54% of hiring managers believe that salaries have increased in excess of 11% YoY, further highlighting the demand for talent.

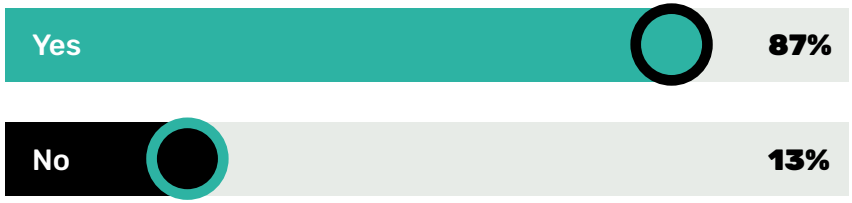
Contents

The cyber security skills shortage continues to intensify

The narrative around the internal shortage of cyber security skills has been consistent over the last decade. Yet, in 2021, we have seen unprecedented demand for security talent. An evolving regulatory landscape, coupled with a sharp focus on digital transformation, has made it essential for CISOs to re-evaluate how their functions are resourced in order to protect rapidly evolving environments.

87% of our cohort of security leaders highlighted a shortage of skills in their business, an increase on 76% last year. Resourcing concerns are perhaps felt most prominently in disciplines such as detection & response, product & application security, and cloud security, where more experienced hires are typically required due to the critical nature of these operations. The skills shortage continues to drive notable wage inflation coupled with double-digit compound annual growth rates in the MSSP market.

Would you say that there is a shortage of cyber security skills in your company?

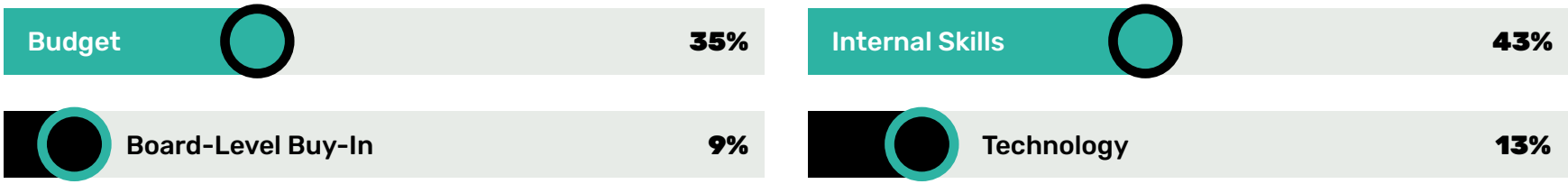


Lack of internal talent continues to be a bottleneck for strategy execution

For the third year running security leaders point to internal skills as the biggest barrier to executing on cyber security strategy. 43% of respondents cited this as their number one challenge, an increase from 39% in the previous year's findings. It is notable that the CISO's whiteboard of priorities has lengthened significantly this year. Increased complexity surrounding the support of business as usual activity, expanding attack surfaces, mitigating against internal and external threats, and supporting increasingly agile software engineering practices all create a myriad of challenges for security leaders to resource.

Budget remained the second-highest impediment to delivering on security roadmaps for security leaders. 35% of the sample stated this was a key issue, up 5% year on year. In contrast, board-level buy-in was the lowest-ranked inhibitor for the first time in our study. Security leaders must capitalize on increased awareness of the impact of cyber risk on business operations to win more support and resources. Technology was seen as the largest obstacle by 13% of our sample, up from 9% in the previous year. The proliferation of security tools and vendors within the enterprise is culminating in increased complexity for security leaders, putting stress on security operations and resourcing. Technology consolidation will be a key focus for many in 2022.

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



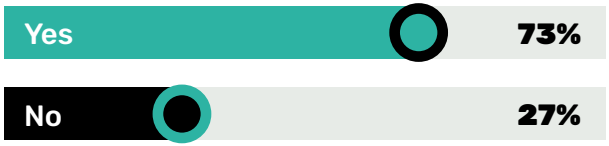
Security leaders need to think differently to drive improved candidate pipeline

Our analysis suggests that the cyber security talent market remains heavily candidate-led, with 73% of security leaders highlighting that they face challenges in creating demand for their vacancies. This figure is consistent with the previous year's data (up 1%), suggesting that CISOs need to start thinking differently around strategies to build an improved candidate pipeline.

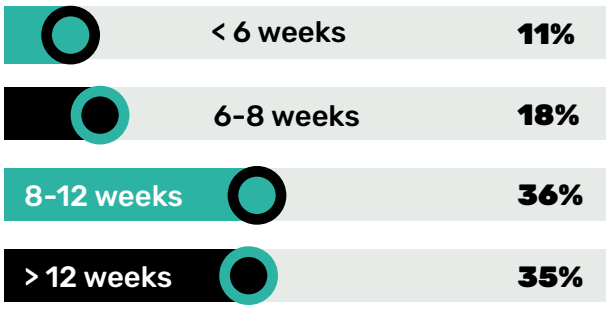
Increased time-to-hire is an inevitable by-product of a tighter talent pool, and this has been reflected in our findings. 71% of the security leaders in our sample saw their vacancies unfilled after an 8-week period, with 35% of this group encountering time-to-hire in excess of a 12-week period and beyond. CISOs and internal talent acquisition professionals need to create tighter collaboration and uncover a range of marginal gains surrounding recruitment processes. Time spent educating internal talent teams, ensuring that job specifications are realistically scoped, and defining a unique employee value proposition - specific to the function - will pay dividends for security leaders and be recouped later in the hiring process.

Our research also suggests that security leaders are increasingly looking internally for individuals with an adjacent skillset to help bridge the gap. 53% of our sample stated that their approach to building teams is based upon finding curious talent internally with the transferable skills to succeed. This is a notable year-on-year increase from 30% and perhaps is symptomatic of external market conditions in terms of candidate scarcity and wage inflation. There was a noteworthy decrease in sentiment to outsource to MSSPs, with 5% selecting this option down from 18% the previous year. CISOs will continue to focus on automation in 2022 to free up valuable resources.

Do you face challenges in sourcing cyber security talent for your team/business?

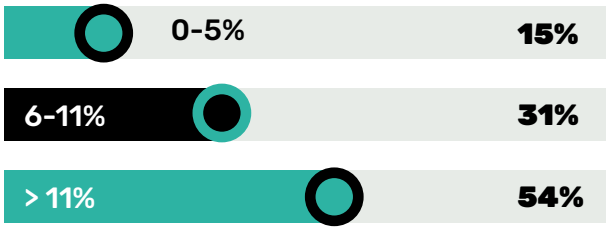


How long does it take to fill cyber security positions in your company?

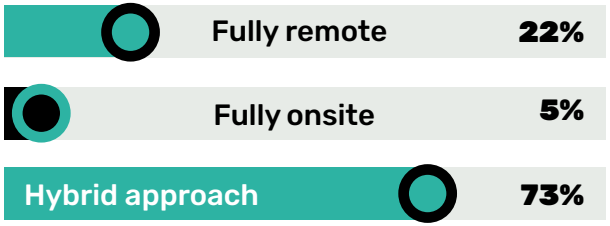


Which statement best sums up your approach to building cyber security teams?

In your view, what % change in salaries has the security industry seen in the last year?



What will the future of the workplace look like for your security team going forwards?



How likely are you to counter offer a member of your team should they hand in their notice?

Keeping pace with reward and the new world of work

A high volume of security executives (54%) reported that they had seen an 11% plus increase in salaries across the industry over the last year. A further 31% have noted that wage inflation sits between 6 and 11%. This surge in compensation, linked to demand, places further stress on CISOs as they seek to allocate budgets. Security leaders certainly need to be conscious of this issue from both a talent attraction and retention perspective and understand the trends at a micro-level by job discipline and location in the benchmarking salaries.

It is not all about compensation. Security leaders are rapidly acknowledging that the world of work is shifting for cyber security professionals. We have seen a massive shift towards hybrid working. 73% of our sample believe that this represents the future working pattern for their teams going forward. A further 22% of security executives envisage fully remote security teams, in contrast with only 5% that had a preference towards entirely onsite. The prospect of more distributed teams certainly presents an opportunity to adopt a broader search radius for critical hires, increasing the volume of suitable candidates. CISOs and talent teams need to consider how reward and flexible working can be leveraged as part of the overall employee value proposition to attract candidates into their respective functions.

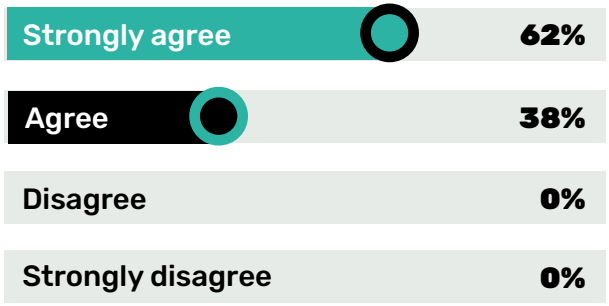
Our snapshot panel of security executives also demonstrated a high propensity to counter-offer team members when they hand in their notice. 57% of our sample were either likely or very likely to do this. This is a significant footnote to hiring managers in this space, highlighting the importance of managing the candidate experience from offer acceptance through to onboarding to negate the risk of counter-offers.

Security moving up the boardroom agenda

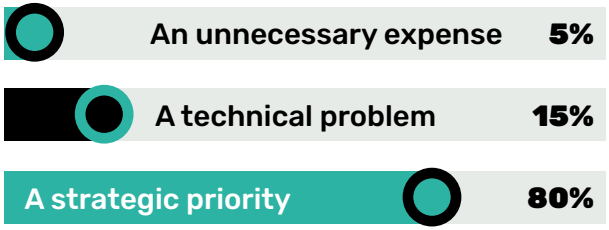
The frequency and magnitude of high-profile data breaches, more educated customers, increasing regulation and accelerated digital strategies have created the perfect storm for the security function to add value to the business. For the first time, our findings show that 100% of security executives believe their business perceives that the security function improves the overall value proposition to customers (38% agree, 62% agree strongly). This contrasts with last year's findings, where 31% did not believe that security had an impact in that context. Cyber security is moving to the forefront of business decision making, and CISOs need to leverage this sentiment and position their teams as an enabler to growth.

80% of the security leaders in our sample stated that their business perceives security as a strategic priority (up from 54% last year). Worryingly 5% still suggest they feel their company sees the function as an unnecessary expense. This figure is down from 15% the previous year. As the pace of software development continues to accelerate and engineering headcount scales, the security function has a pivotal role to play in enabling innovative and secure solutions that drive top-line performance.

Do you agree with the following statement: 'My business feels that the cyber security function improves the overall proposition to customers'?

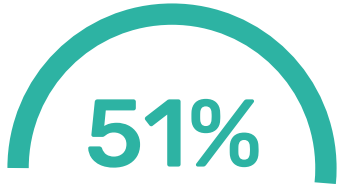


How does your business perceive cyber security?



Concerns around keeping pace with digital business

Digital transformation presents a massive opportunity for business but also introduces unprecedented risk – particularly when executed at pace. 51% of the leaders in our sample expressed concerns that security investment is struggling to keep pace with digital business. This is perhaps no surprise when you examine the growing to-do list of the CISO from security operations through to vendor management. At this time of change, CISOs need to double down on efforts to drive meaningful alignment with the business.



suggest investment in cyber security is not keeping pace with digital business

The emergence of the engineering-centric CISO

William Lin - *Managing Director*
Forgepoint Capital

If you were creating your own cyber security start-up, what CISO challenge would you fix and why?

Let me highlight a few of the challenges I am seeing and hearing on the practitioner side. As a theme, there has been a lot more thinking going on around remediating product or software-related issues. We are undergoing a journey now where security is becoming more and more integrated and reactive to the output of the engineering function as we build solutions or products.

Few could have predicted the impact that the Agile development methodology would have on both vulnerabilities and visibility. It has become harder to protect applications as the pace of development increases. My theory is that these factors are all driving and accelerating the need for a new type of CISO – 'the engineering-centric CISO'.

Tooling will need to evolve to enable 'the engineering-centric CISO'. So, if it were up to me, I would be thinking about this new category of customers and the problems that remain unsolved on their behalf. One topical example, due to SolarWinds, is around the time-to-remediate vulnerability. Prioritization has been a common problem for a very long time. Which of these many vulnerabilities should I care about? Triaging and prioritizing have created a whole ecosystem in itself.

Now that we have these scanning tools, the next step is to remediate the vulnerabilities that are genuinely important. That means going into the engineering team and identifying the person that wrote that specific line of code that created a specific vulnerability. It is a complex web to untangle, and that makes tooling to remediate vulnerabilities a compelling problem to fix right now.

What impact will the requirement for the engineering-centric CISO have on companies' recruitment processes?

I spend a lot of time helping CISOs become successful in their careers. The ones that stand out in my mind generally tend to have that engineering mindset. One change in the dynamic in the CISO pool is that there is a lot more demand than supply of engineering-centric CISOs right now.

The minimum bar is a CISO that can interact positively with the engineering team. But what organizations are really looking for in the long term is security leaders that can be deeply integrated with the development team. It is about having a CISO that has the credibility and ability to influence security from beginning to end.

There is a lot of uncertainty about where to jump into that development lifecycle. There is no one way to do it, but having the credibility to have a productive conversation with engineers separates CISOs. They still need to have all the other traditional skills around compliance, IT security, network security, endpoint security, etc. This is a new skill that I think everyone expects from their future CISO, but not all CISOs have, which is the engineering mindset.

When you look at CISOs in the market, are they more inclined to favor point solutions or platforms?

CISOs have long complained about the lack of integration and consolidation, too many tools, too much noise, too much confusion. Over time frustration has grown around the sheer volume of vendors and point solutions. The wave of consolidation that we are currently seeing will certainly be welcomed by that group of CISOs.

When you look at the engineering-centric CISO, it is a slightly different scenario because there are not that many tools available to support them. So, we see certain tools really take off even though they are only a point solution, but the growth of that point solution is so high that there is potential to spawn a platform company out of them. Tooling is still raw enough for the engineering-centric CISO, and I think they appreciate the openness of point solutions. Still, a common problem, though, is that there is no silver bullet or de facto standard tool that solves all CISO challenges.

There is generally more openness from the engineering-centric CISO group towards point solutions. You must remember, though, there is a natural reason why point solutions exist. As a startup, it is easier to fix one compelling problem and build credibility in one specific space rather than trying to solve six hundred problems at once. If the problem is compelling enough, it will get CISOs attention.

What is the most common reason cyber security startups fail to meet their full potential?

The big one for me is that a lot of startups do not have a deep enough empathy for the problem that they are solving. They need to go one step deeper to understand why CISOs are asking for certain features. They cannot make assumptions. When that level of empathy is missing, the industry can shift quickly, and startups get left behind.

I have seen successful teams and companies not realize their full potential because the market has shifted away from them, and they were not prepared for it and did not quite know how to react. They knew why they were initially popular but were not thinking about the evolution of the problem. The security industry rapidly shifts because it is still maturing, so empathy for the problem you are solving is critical for successful startups.

Are there any hard-to-solve security problems that you see being solved this year?

I think that there are probably three themes that I am excited by, and we are seeing real progress around this year. One of them is cloud security. It has always been a tough problem to solve. There has always been a lot of investment. But I think that there is a lot of good activity, interest, and teamwork between vendors, startups, investors, and practitioners working towards creating standards in this space.

There is also a lot more interest and action in the data security world. This has been a really underserved area for a while, and I am happy to see more activity in this space. If you wanted to start from scratch and build a defense, what is the first thing you want to protect? When you think about threats and risk and the difference between an incident and a breach – it all revolves around data loss. That is when you need to call the lawyers in and deploy the incident responders. That all really solidifies the importance of protecting your data. I would say that COVID-19, coupled with high-profile breaches, has really helped practitioners prioritize data as the fundamental thing you need to protect first.

The third theme is more around consolidation. Not necessarily one company buying the next – that is not important. What is important is that I am seeing practitioners start to look at problems that are somewhat close and previously had two solutions take one solution to fix their issues. So, we are starting to see CISOs enabling themselves to reduce complexity without depending on the vendors to do it for them, which has been rewarding to see.

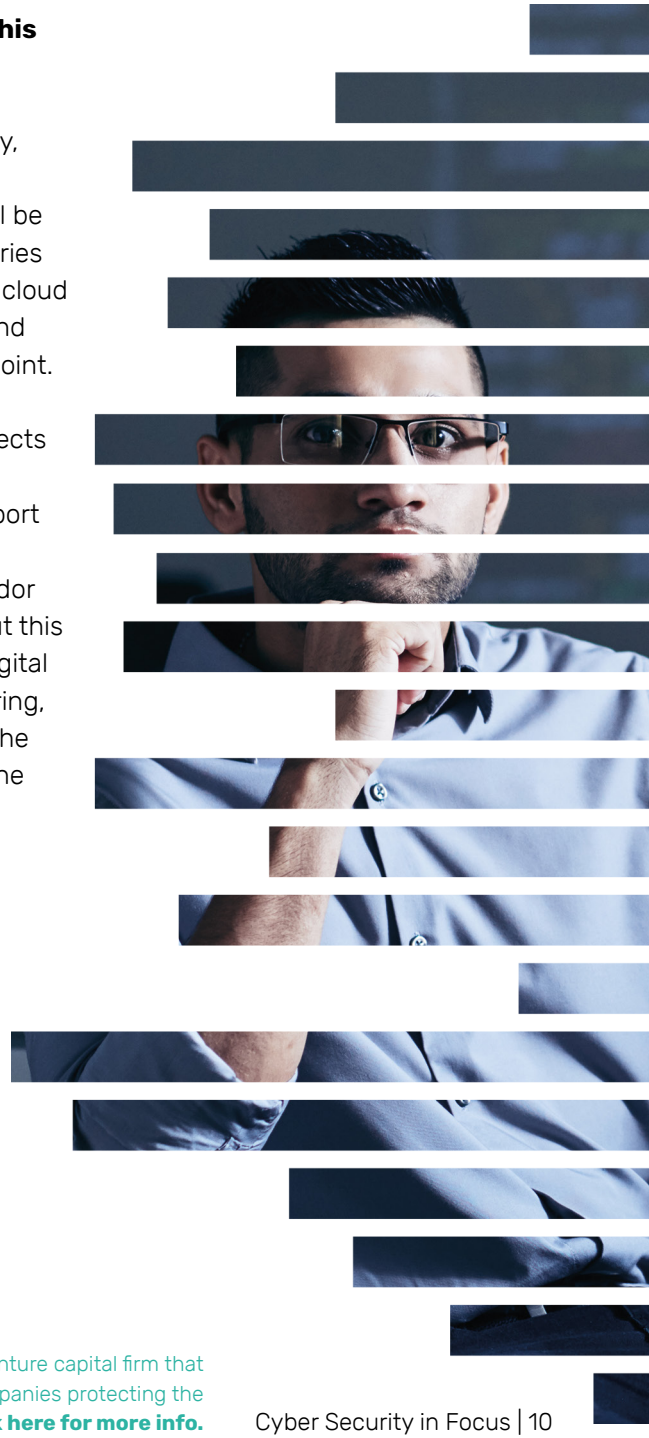
How can the engineering-centric CISO play a bigger role in accelerating digital transformation?

The role of the CISO is to help deal with risk across multiple different dimensions; generally, they are there to deal with technology risk. The CISOs that are good at helping deal with risk are those that enable. They know the common problems and understand what represents a real risk and what does not. The benefit of this knowledge is that it allows you to short circuit decisions that may feel risky at the time but at the end of the day are not risky at all. That is the power of the engineering-centric CISO. A lot of digital transformation is inherently going to be driven by engineering, and finding a CISO that can empower developers with knowledge, tooling, and experience will enable outcomes to be achieved faster and more securely.

What projects should CISOs be focusing on this year?

It is worth noting that every practitioner, company, and team is different, and priorities will vary to a degree depending on the environment. CISOs will be prioritizing projects that fit into a range of categories this year, from looking at newer developments in cloud security and data to 'getting back to basics' around identity, response, application security, and endpoint.

There are potentially also some more topical projects that have been driven by recent events. Security practitioners will continue to have to own or support the remote working experience, for example. Solarwinds has also placed a sharp focus on vendor risk, and I expect CISOs to be really thinking about this issue this year. Finally, the continued theme of digital transformation equates to more work in engineering, more engineers, and a stronger requirement for the engineering-centric CISO that can add value to the overall initiative.



"A lot of digital transformation is inherently going to be driven by engineering and finding a CISO that can empower developers with knowledge, tooling, and experience will enable outcomes to be achieved faster and more securely."

William Lin - *Managing Director, Forgepoint Capital*

Forgepoint is a multi-stage venture capital firm that invests in transformative companies protecting the digital future. **Click here for more info.**

Product Security in the spotlight

What is the difference between application and product security?

Lots of companies see them as interchangeable, but for me, there are fundamental differences. At the very basics, application security is a set of tactics that can be used by a range of disciplines within security in order to secure software, many of which we should be automating to a much greater extent.

But product security is an elevated discipline primarily driven by the context around how the application is used by the customer, the expectations of the customer, and the goals of the business. A product security engineer has to have a broader understanding of how the software feature is actually used by the customer. That's because if you build security in a vacuum, you are not going to have good usage or good outcomes. There is a lot of crossover between product security and user experience in this regard.

How challenging is it to embed security into the software development lifecycle?

It can be very challenging, depending on the organization. Once you clear the handle on why it is important and why it matters to the strategic outcomes of the business and to the customer, then it gets easier.

The main challenge is to get real alignment and buy-in across the entire spectrum of the business, from senior leadership to engineering and product management. This only comes when everyone is clear about why embedding security is vital to protecting customer data and therefore building trust between the customer and the business.

How do you achieve the right balance between pace and haste when integrating security into the development pipeline?

Ultimately businesses need to be competitive, and that means they need to be both fast and secure. There is a perception that you can't do security fast in CI/CD, but that's not true. Security by default should be part of the entire process from product planning and work definition through to continuous deployment. Rather than happening all at the end or after release, it happens early in planning and a little bit at every point in the process. Only then do you get to speed.

What are the major differences between security by design and security by default?

Both are important. At the very basics, companies should be designing security into their products because anything they build needs the capability to be secure.

The main difference between design and default is being opinionated about the state of that capability. Security by default means having security on and not letting the customer turn it off, or if there is the capability to turn it off, then it

James Dolph - *Chief Information Security Officer, Guidewire Software*

is about ensuring the customer really understands the implications of doing so. There must be transparency around what has a security impact and what doesn't.

Security should not be something customers have to opt in to. Software should be secure without the need for any configuration. Look at the way Apple has implemented access to its photos. The default setting is that no application has access to a customer's photo library. Customers have the ability to grant access on a very granular level, but they understand they are making a security trade-off in doing so.

What is the general maturity level of organizations in the market when it comes to implementing security by default?

Only a few companies are doing it well. While most companies realize they need to build security into their products, the reality is not every company sees the strategic advantage of security by default. This means we see a lot of enterprise software that by default is insecure and results in a lot of common exposures of data that are totally unnecessary.

What tips do you have for other CISOs and CTOs that are looking to shift security into the product development lifecycle?

It has to start with alignment around what the customer expects from security and ensuring teams across the business, including engineering and product management, understand this.

Do some UX research and look at what customers want and also what they think you are doing from a security standpoint. Help your engineering teams understand that building things securely is just what is done. I live by the mantra that secure and done is done, insecure and done is not done. It really is as simple as that. Embedding that into the company culture is vital because security is not and cannot be viewed as an add-on – it is not optional and should be part of the company's value proposition.

What are the top challenges associated with building a product security function?

Once you have alignment within the business, agreement from the leadership team around the importance of a product security function, and the necessary funding, the biggest challenge becomes building and maintaining context around how products are actually being used by customers. That's because you can't build an effective product security function without understanding how customers are using the product itself.

This requires ongoing effort by the security team and means we have to look for people who not only have the technical knowhow but the emotional intelligence to understand things from the customer's perspective. Soft skills are just as important as the technical when it comes to building a product security function.

What areas of the business need to be involved in a product security program?

You have to have your senior leadership team on board because, ultimately, it does not come for free. Beyond this, where it fits and who needs to be involved depends on the size and makeup of the organization itself.

While it makes sense for the security team to own and manage the product security program, it's important to ensure the product management and engineering teams are aligned at a very minimum, as well as the risk and compliance, release management, and DevOps teams, respectively.

Each of these teams has a role to play in the success of a product security program, and each should be credited for its success.

What does a fully functioning product security team look like?

A fully functioning product security team should be aligned across the business and have engagement within it. And given product security should be part of a company's value proposition, businesses should be able to prove its effectiveness and celebrate it.

A product security team should also understand how to enact change management as the security environment continuously evolves as new threats and vulnerabilities emerge.

At the end of the day, when we are building products, we are trying to get an outcome for our customers, which then builds stickiness and revenue for the business, so the effectiveness of a product security team depends on the results it generates for the business.

What do you look for when hiring a product security engineer as opposed to an application security engineer?

I look for people with excellent communication skills, strong emotional intelligence, and customer-facing qualities - people who are comfortable influencing without authority. Of course, technical skills are important, but it's about finding people who can truly understand the customer and have the necessary soft skills to hit the ground running.

"A fully functioning product security team should be aligned across the business and have engagement within it. And given product security should be part of a company's value proposition, businesses should be able to prove its effectiveness and celebrate it."

James Dolph - *Chief Information Security Officer, Guidewire Software*

2022 salary benchmarking

Basic salary exclusive of equity, stock and LTI.

Low-end/Average/High-end

Manager/Executive Level	US - West Coast ($)	US - East Coast ($)	UK&I (£)
CISO	230,000/325,000/550,000	225,000/325,000/550,000	140,000/200,000/350,000
Deputy CISO	200,000/260,000/315,000	190,000/250,000/310,000	120,000/150,000/200,000
Head of Information Security (Early Stage)	200,000/230,000/300,000	190,000/225,000/300,000	120,000/150,000/170,000
Head of Information Security Risk	215,000/250,000/370,000	210,000/240,000/365,000	110,000/130,000/150,000
Director Security Engineering	200,000/250,000/325,000	200,000/250,000/325,000	100,000/130,000/180,000
Director Application Security	190,000/240,000/300,000	190,000/240,000/300,000	115,000/135,000/200,000
Director Incident Response & Security Assurance	180,000/230,000/300,000	180,000/230,000/300,000	100,000/130,000/170,000
Director Security Operations & Threat Management	190,000/240,000/300,000	190,000/240,000/300,000	105,000/120,000/160,000
Director Identity & Access Management	175,000/225,000/280,000	175,000/225,000/280,000	100,000/115,000/140,000
Application Security Manager	180,000/220,000/260,000	180,000/220,000/260,000	120,000/130,000/160,000
Product Security Manager	180,000/220,000/260,000	180,000/220,000/260,000	90,000/100,000/125,000
Cloud Security Manager	190,000/230,000/270,000	190,000/230,000/270,000	100,000/120,000/140,000
Detection and Response Manager	190,000/230,000/270,000	190,000/230,000/270,000	100,000/120,000/140,000
Offensive Security Manager	160,000/190,000/225,000	160,000/190,000/225,000	100,000/115,000/130,000
Senior Manager, Information Security Risk	215,000/235,000/310,000	210,000/230,000/300,000	95,000/100,000/120,000
Security Operations Manager	150,000/190,000/250,000	150,000/190,000/250,000	80,000/95,000/125,000

Security Architecture	US - West Coast ($)	US - East Coast ($)	UK&I (£)
Chief Security Architect	205,000/255,000/350,000	200,000/250,000/350,000	105,000/130,000/155,000
Application Security Architect	180,000/205,000/315,000	170,000/200,000/300,000	100,000/110,000/140,000
Infrastructure Security Architect	190,000/235,000/295,000	190,000/230,000/290,000	80,000/95,000/120,000
Product Security Architect	205,000/250,000/295,000	200,000/240,000/290,000	95,000/100,000/135,000

Security Architecture (Continued)	US - West Coast ($)	US - East Coast ($)	UK&I (£)
Network Security Architect	180,000/240,000/270,000	180,000/230,000/265,000	70,000/85,000/100,000
Enterprise Security Architect	225,000/260,000/320,000	220,000/250,000/320,000	105,000/125,000/145,000
DevSecOps Architect	200,000/255,000/310,000	200,000/250,000/310,000	105,000/125,000/145,000
Cloud Security Architect	200,000/250,000/305,000	200,000/245,000/300,000	100,000/130,000/150,000
GRC Information Security Architect	200,000/255,000/290,000	200,000/250,000/280,000	90,000/110,000/130,000

Security Engineering	US - West Coast ($)	US - East Coast ($)	UK&I (£)
Security Automation Engineer	160,000/200,000/240,000	160,000/200,000/240,000	100,000/120,000/150,000
DevSecOps Engineer	170,000/210,000/240,000	170,000/210,000/240,000	110,000/130,000/160,000
Detection Engineer	160,000/200,000/235,000	160,000/200,000/235,000	65,000/75,000/90,000
Security Data Engineer	160,000/200,000/235,000	160,000/200,000/235,000	65,000/75,000/90,000
Corporate Security Engineer	140,000/180,000/225,000	140,000/180,000/225,000	55,000/70,000/85,000
SIEM Engineer	130,000/170,000/220,000	130,000/170,000/220,000	90,000/100,000/120,000
Product Security Engineer	170,000/200,000/240,000	170,000/200,000/240,000	100,000/115,000/130,000
IAM Engineer	120,000/165,000/225,000	120,000/165,000/225,000	50,000/70,000/90,000
Cyber Threat Hunter	140,000/165,000/185,000	140,000/160,000/185,000	60,000/80,000/115,000
Threat & Vulnerability Engineer	140,000/170,000/200,000	140,000/170,000/200,000	55,000/80,000/100,000
Penetration Tester	120,000/165,000/180,000	120,000/165,000/180,000	60,000/80,000/125,000
Software Security Engineer	170,000/200,000/240,000	170,000/200,000/240,000	70,000/80,000/115,000
Cloud Security Engineer	170,000/200,000/240,000	170,000/200,000/240,000	75,000/95,000/110,000
Application Security Engineer	170,000/200,000/240,000	170,000/200,000/240,000	80,000/100,000/120,000
Incident Response Engineer	160,000/185,000/225,000	160,000/185,000/225,000	65,000/75,000/90,000

Looking for more salary data for your next hire?
Request a bespoke salary benchmark **here.**
(Contract rates also available)

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.

Find out more about our cyber security recruitment practice **here.**

stottandmay.com