maxwellbond

BUILDING & MATURING GREENFIELD CYBER FUNCTIONS

WHERE TO START

JAKE ADSHEAD

SENIOR CYBER CONSULTANT
jake.adshead@maxwellbond.co.uk

maxwellbond

Introduction

Heading into a new role can be challenging, especially in cyber security where budgets are normally tight, resources are limited, and the risk often very high. It can be difficult to evaluate what you need to do first when you first start in a new business.

Senior Cyber Consultant, Jake Adshead, recently hosted a small roundtable with a number of leading cyber security professionals from around the UK to discuss what the priorities should be for professionals entering a new role or entering a greenfield cyber function.

The following whitepaper recaps some of the key discussion points and pieces of advice for cyber leaders entering a new cyber team or business.

37% of UK firms have reduced their cyber security budget within the last twelve months despite some reports suggesting there was approximately double the amount of cyber attacks in 2020 than in 2019.

maxwellbond

Building Relationships

When you join a business, it's important to start with the people. If you're entering a new, or young cyber security team, as a cyber security leader, at some point you're going to need to ask for a budget, and this is going to be signed off by senior Heads of and Directors. Therefore, having a transparent conversation with each of them about your role, the impact you will have, and the importance of security. You can also get relevant senior staff members involved in response tests and project mapping, so they become more invested in the cyber function. They're much more likely to buy into a later pitch if they already have a human connection with you.

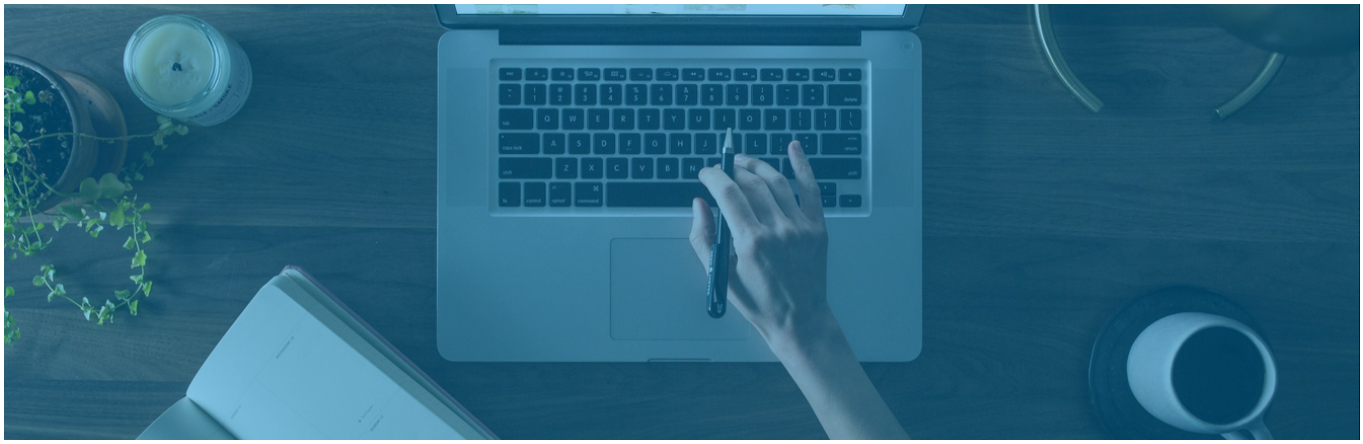
Plus communication with the wider team is fundamental to ensuring the full company is following the same security policies and training programmes. This communication naturally becomes much easier if you have a good relationship and understanding of each other's roles and their importance.

Assess Your Status

When you start in a new business you quickly need to evaluate the landscape which requires risk assessment or audit. Risk assessments are used to identify, estimate, and prioritize risk to organisational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation and use of information systems. Conducting this early on will allow for full visibility over the company's assets and any potential vulnerabilities and will help you create a roadmap of what to do next.

Low Hanging Fruit

Problems with an easy fix should be addressed quickly so you can start working on bigger projects without worrying about smaller loose ends. This could be as simple as delivering a series of training sessions across the company force to ensure everyone has the same level of knowledge of how to protect their assets and data online, especially if working remotely. Deliver low-hanging fruit quickly!



maxwellbond

Find a Mentor

Regardless of your seniority, you're never above asking for help or getting a second opinion. It's often the best way to solve problems in the most effective way. So don't shy away from finding someone who has experience in what you are trying to achieve and connecting with them for advice.

If this is the first time you are leading a new or young cyber security function, it's worthwhile seeking out advice from people who have been in the same position as you before. If you are taking over an existing cyber team, see if it is possible to speak with your predecessor and try and get as much information as possible about how the team has been run up until that point and to gage how to move forwards. And even if you have done it all before, it never hurts to get some extra advice to see if there is a quicker or more effective way to achieve the same thing.

NIST Framework

The National Institute for Standards and Technology (NIST) Framework can be a good place to start from a technological standpoint. The NIST framework is a cyber security framework which is underpinned by five functions: Identify, Protect, Detect, Respond, and Recover. Obviously, whilst you can't go in on day one with limited resources and knowledge and expect to action the full NIST spectrum, but you can select actionable elements to start with based on its core elements. Common priorities from the NIST framework are the "Identify" and the "Detect" elements, because from this you can usually determine what the "Protect" element requires.

Whilst the Response and Recover aspects of the framework are also important, it's important to first start by accurately gaining visibility over potential threats and ensuring you have the ability to identify and detect them correctly and quickly. This includes starting with the basics such as making sure your server and desktop estates are being patched, making sure all software is up to date, ensuring the logs are uploaded into the SIEM and that all the required alerts are set up. Fundamentals first! If you're leaving the front door wide open, why put an expensive alarm system in? Close the front door first!

One leader that we spoke to rated Rapid7's InsightIDR SIEM Tool as it integrated with so many other platforms that may already exist in the business, it's easy to use, it already has rules written in, it has machine learning, and cross source correlation. It's also important to consider how you build this out, especially if you are low on headcount. Some SIEM's like Splunk can be really heavy and labour intensive, so it's really important to evaluate what your teams capabilities are and select a SIEM that suits your business and team best.

maxwellbond

Find the Balance

Essentially you need to balance having good visibility, without overwhelming your resources, particularly in current times where it has been reported that around 37% of UK firms have reduced their cyber security budget (Think Digital Partners, 2020), which means smaller teams and less tooling. One way to circumvent staff shortages, if finances allow, is to automate early. This automation should be able to deliver large quantities of work, similar to that of large SOCs, with fewer people. It's easier to automate as you go, rather than going back and automating everything later, so it's definitely something to consider in the first instance. One contributor to this whitepaper suggested they use Rapid 7's Insight Connect, which works as building blocks so you can write your own scripts where required whilst also automating a lot of work straight away.

When shopping around for any new tools, it's important to select products that are suitable for your needs and budget, but also that are suitable for your team size and available resources. If you opt for something really labour intensive with a 2-man team, you're never going to get the most out of the product, regardless of how good it is.

Automation is a great tool to help save on time and resources, but the human element, particularly in penetration testing is so important in order to detect and identify abusive business logic, or the human discovery a flaw in the business logic or functionality of a website. This is much harder to trace and is most likely to be missed by automated tools.

DevSecOps: Worth Investing In?

There's a lot of buzz around the idea of DevSecOps, a closer relationship between development, operations, and security, but opinions from some leaders suggest that DevSecOps roles are, for the most part, unrealistic. To fill the gap that they are designed for, DevSecOps engineers truly need to be experts in DevOps and experts in Security. Each of those functions alone are huge and difficult to truly master. To expect one person to master the working practices, jargon, requirements, and consequences of both departments is quite unrealistic. But that's exactly what they would need to do to actually fill the communications gap between DevOps and Security.

Not only this, but current job specifications for DevSecOps Engineers tend to demand lots of experience and knowledge in DevOps and Security areas, as well as the ability to pen-test, but are offering massively low salaries for the amount of work and knowledge they expect to hire. This disparity between expectation and salary, will make this position very difficult to even recruit for, as people are likely to stick to either DevOps or Security and work their way up to senior positions and higher salaries.

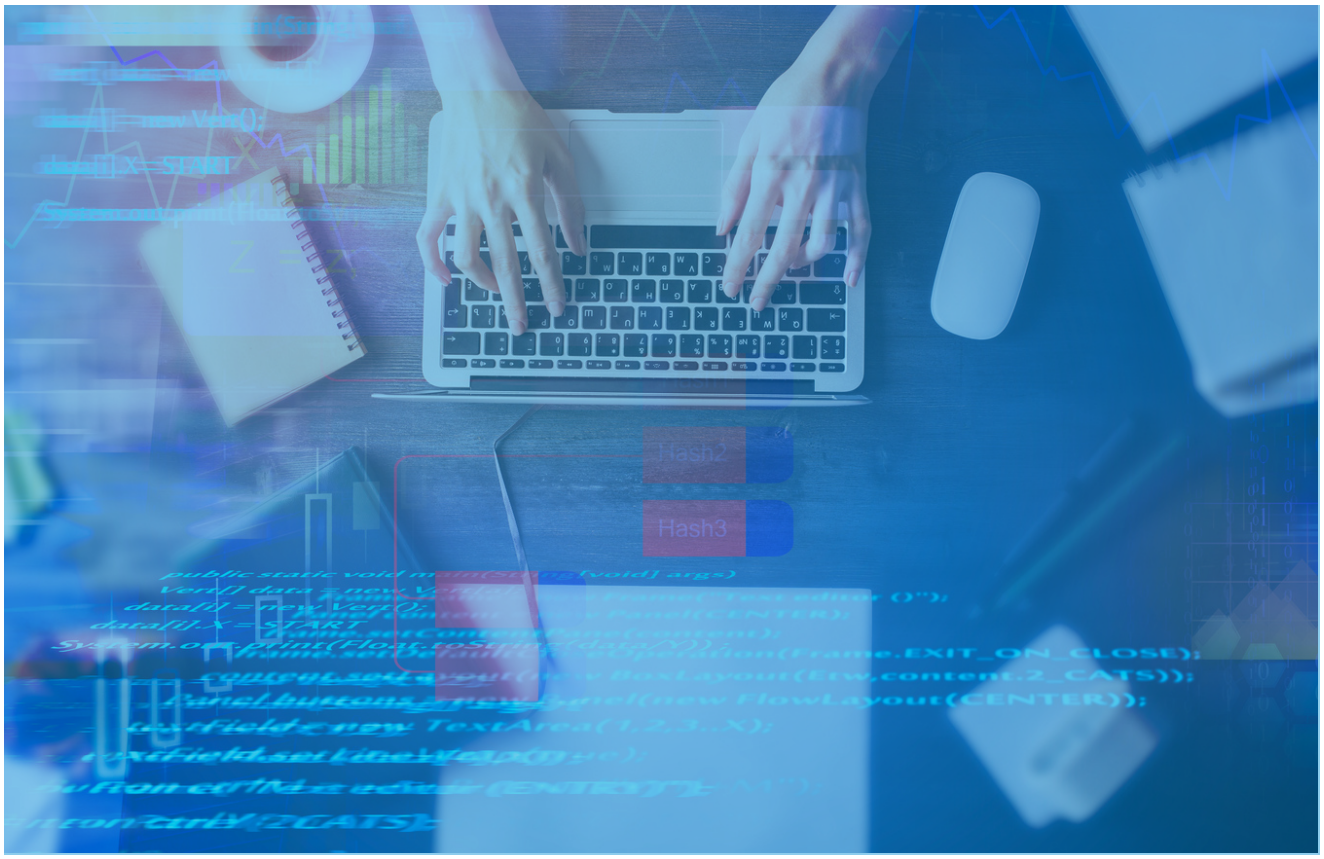
In theory, DevSecOps is a great idea to integrate security into development, however there could be more work to do around role definition, role expectations, and logistics if set DevSecOps specific roles are something companies will pursue. Potentially, it is more the communication and relationship between the two functions that needs improving, rather than the introduction of a new hybrid role.

maxwellbond

Summary

The general advice for cyber leaders starting in a new position and a new team which they aim to mature and grow, is to build relationships with your stakeholders, gain full visibility over the full tech estate, focus on improving the identification and detection of threats through frequent assessment, and research and demo as many tools as you can before purchasing. The right team with the wrong tools will be ineffective and you need to select tools with an awareness not only for your needs and budget, but also of your teams resources and capabilities.

For help building and maturing your cyber security functions, please get in touch with Jake Adshead to find out more about our market leading staffing solutions across perm and contractor hire in the UK, USA, and Germany.



Contact Us

Build high performing cyber security teams through exceptional contract and perm staffing solutions and business advice with Maxwell Bond, the recruitment partner of choice across the UK, USA, and Germany.

Jake Adshead
Senior Cyber Security Consultant
jake.adshead@maxwellbond.co.uk
0161 359 3280

Find out more at www.maxwellbond.co.uk