CYBER SECURITY IN 2020

WITH MIKE KOSS

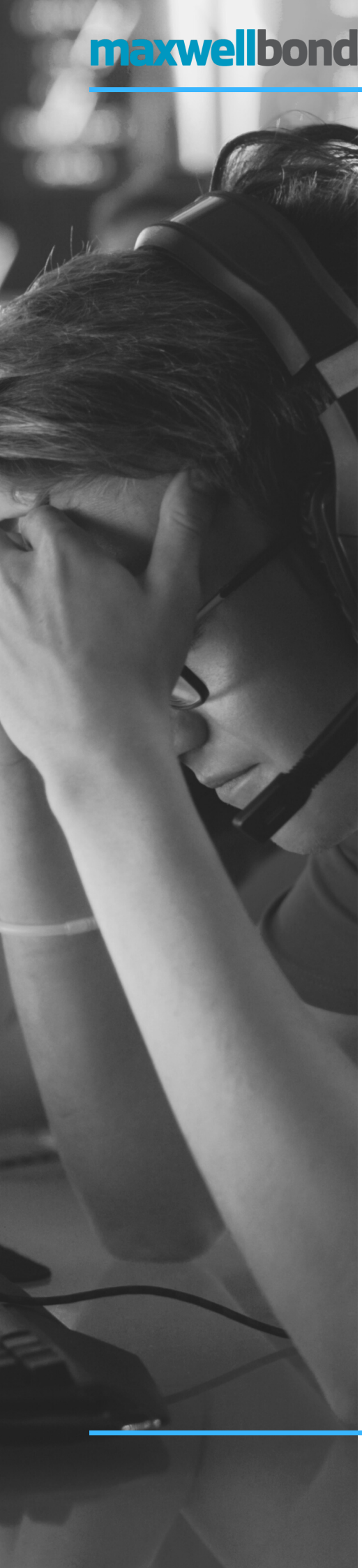
Mike Koss, former Head of IT and Security at N Brown, speaks about building an effective cyber-security team within a challenging environment and how he managed it. See inside for his key points and advice on how you can do the same to improve your cyber-security.

BUILDING SECURITY TEAMS IN CHALLENGING ENVIRONMENTS

'THERE'S NO ENVIRONMENT MORE CHALLENGING THAN A RETAILER WHO SETS A RESTRICTIVE CYBER BUDGET, AND WHO'S LACK OF CYBER KNOWLEDGE RESULTS IN AN UNWILLINGNESS TO ALLOCATE MORE FUNDING.'

Effective business cyber-security and information-security requires exceptionally talented and knowledgeable cyber-teams, who can implement and maintain technology and processes which will protect businesses.

However, executive boards often lack an adequate knowledge of cyber-security and a willingness to allocate enough funding to pay for the level of security necessary for a business. Changing this attitude, and educating people on the risks and consequences of cyber-attacks is fundamental to building effective security teams.



A CHALLENGING ENVIRONMENT

STARTING FROM SCRATCH

Mike Koss joined a company, like many others, that had a complete lack of cyber-security measures in place. Despite boasting a $1 billion turnover across 14 brands, the company had left itself vulnerable to a number of breaches and attacks, due to a lack of knowledge or resources.

The InfoSec budget was a mere £300k per year, and there was only 1 graduate, 1 risk employee, and a contract PEN tester. Due to this limited team, they hadn't patched in 4 years, they had poor vulnerability management, no pen testing schedule, outdated policies and zero compliance.The company even knew they were losing money through fraudulent activity, but it was simply accepted as manageable risk rather than being actioned.

FIXING THE PROBLEM

STRATEGISING TO MINIMISE VULNERABILITY

- Choose the right tooling to give visibility
- Win the board over
- Increase the budget
- Sell the vision
- Hire the right team
- DELIVER and keep delivering
- Finally, the most important thing is the CREDIBILITY of the team.

By using the above strategy Mike saved his company £270k in one month by identifying and then preventing fraudulent activity, and therefore managed to convince the board to increase their cyber-security budget, so that he could hire the right team. Whilst this was difficult due to the skill shortage, competitive salaries, keeping talent interested and getting them invested in the product, Mike emphasises the importance of remembering that interviews are a time for the company to pitch themselves to the candidate and not just be pitched to.

BUILDING A BLUE TEAM

THE BLUE TEAM WOULD FOCUS ON LOGS AND TICKETS, IS DATA-DRIVEN, AND IS OFTEN OVERLOOKED AS IT IS BAU.

Key Points:

- Getting the right tools is fundamental to operational success, in this case this was Splunk.
- Hiring the right people is imperative to having an efficient, hardworking security team.
- Junior Analysts should not be limited to closing tickets.
- Training is key. A good security team requires time, financial investment and a supportive, learning environment. This is also pivotal to attracting and retaining talent.

RED TEAMING EVERYTHING

THE RED TEAM TAKES A MORE OFFENSIVE RATHER THAN DEFENSIVE METHOD TO CYBER-SECURITY.

Key Points:

- As above, hiring the right person was fundamental to productivity.
- Tooling for this team was not as important, although this team did find a number of blind spots and issues within the tooling the business was using.

GETTING THE RESULTS

AFTER A VIGOROUS RECRUITMENT PROCESS AND EDUCATING THE BOARD ON CYBER RISKS AND MANAGEMENT METHODS, THE COMPANY IS FINALLY ON TRACK TO HAVING EFFECTIVE CYBER-SECURITY PROTOCOLS

The Infosec team is now currently at 9 permanent employees and has a proper patching schedule in place with a patching review board. Additionally they have implemented network anomaly detection, SIEM, SOC and 24/7 security coverage. With an established red and blue security team, the company now has a more mature approach to risk and third party vendor management. Plus, newly implemented vulnerability management is showing a downward trend, and the company has a fully integrated cyber-security solution which stretches across all projects and platforms.

Unlike before, the company now has a much more robust, strategic, and effective cyber-security approach which means it's exposure to risk is minimised and it's ability to respond to potential breaches is much improved. The key challenges included hiring and retaining the top talent and convincing the board to allocate more funding. There were overcome and achieved by personalised recruitment processes which showed an interest and investment in the candidates, and demonstrating to the board, the importance of cyber-security by providing financial and quantitative data and solutions.