STAY ON TARGET

Laura Libeer *highlights eight ways to bolster your cyber security resources without blowing your budget*

IT security breaches are becoming more frequent and costly. According to IBM Security's Cost of a Data Breach Report 2023 UK organisations shell out an average of £3.4-million for data breach incidents. There isn't a CISO around that doesn't wish they had that kind of budget to spend on IT security. The tools to help security teams do their job more effectively are out there, but getting them approved in the annual budget is not guaranteed and investment can sometimes be too late. So what can UK IT leaders do to make sure they continue to improve their IT security without blowing their budget? Here are eight ways to bolster cyber security resources:

RECRUIT MORE STAFF

Hiring experienced IT security specialists can be expensive and the job market is fiercely competitive. However, there is a benefit to hiring less experienced staff. Cyber security is a team sport after all and there are plenty of cyber security team roles that don't require years of experience. Adding ambitious junior staff to support the day-to-day tasks will ease some of the pressure on the rest of your team.

On top of that, it gives you a pool of fresh talent you can train to fit the needs of your team. More people means more room for everyone to focus on their dedicated tasks. A full cyber security team, where every role is filled will make operations run more smoothly – and it never hurts to have an extra pair of eyes looking out for security risks.

The ever-evolving IT landscape demands a continuous and adaptive approach to cyber security

UPSKILL YOUR TEAM

The ever-evolving IT landscape demands a continuous and adaptive approach to cyber security learning. To try and keep pace with the latest developments in this ever-changing field, it is imperative that your team's upskilling initiatives place a strong emphasis on staying abreast of emerging trends.

This demands gaining a comprehensive understanding of the functions of artificial intelligence (AI) within automated security systems, devising measures to combat malware specifically tailored for mobile devices and applications, navigating through the complexities and potential risks associated with cloud migration, implementing security protocols for Internet of Things (IoT) devices, and formulating strategic approaches to effectively thwart targeted ransomware attacks.

A well-structured progression plan for your cyber security staff will aid in identifying specific gaps in skills and knowledge (and therefore your defences) essential for their roles. With numerous cyber security education programmes available, the onus is on you to identify the areas where your team needs to improve, and dedicate resources that offer a worthwhile return on your investments. A comprehensive approach to upskilling not only fortifies expertise but also equips your team with the resilience and adaptability needed to excel.

As well as training in core areas of IT security, organisations should look at developing their team's soft skills – how to work under pressure, think on their feet and resolve problems quickly. The team needs to know how to respond in emergency situations, maintain a professional demeanour and stay calm when a security breach or disaster strikes.

By fostering a culture of continuous improvement and investing in both technical and soft skills, your team becomes better prepared to address the evolving challenges of cyber security with confidence.

MONITOR THE PERFORMANCE OF RESOURCES

To ensure the sustained effectiveness of your cyber security measures, cultivating a culture of continuous improvement is paramount. A key approach to achieve this is by creating open communication and feedback loops within your team. This practice helps identify areas for improvement and it involves regularly evaluating and updating Key Performance Indicators (KPIs) to remain in harmony with evolving threats and industry standards.

It is also important to recognise the correlation between the rise of burnout and factors that contribute towards this, such as unclear expectations, inadequate performance management and a lack of career perspective. The fact that a staggering 79 percent of UK employers report experiencing burnout underscores the urgent need for proactive measures.

A deeper understanding of these factors allows organisations to proactively address issues that may lead to burnout among their employees. Clear and transparent communication about expectations, coupled with effective performance management strategies, can help create a healthier work environment. Providing employees with a clear career path and opportunities for professional development can also contribute significantly to mitigating burnout.

Companies should also consider implementing ongoing training programmes for cyber security professionals. Updating and informing about the latest technologies and methodologies not only enriches their skill set, but also fortifies a proactive cyber security approach.

Cultivating a mindset of continuous learning and improvement equips your team to adeptly navigate emerging challenges, ensuring they consistently uphold the highest security standards.

SMART SYSTEMS SHOULDN'T COST THE EARTH

The more IT teams know about the dangers their business is facing, the better equipped they will be to defend against them. The right software will help you to monitor and protect everything from individual computers to mobile devices, to the entire network infrastructure.

For an optimal cyber security strategy, consider investing in a comprehensive tool that provides a deep understanding of your IT infrastructure. This tool should empower your IT team to uncover hidden elements, establish a comprehensive inventory of your IT assets and fortify your cyber security measures.

Look for features that facilitate vulnerability detection, patch application, upgrades and adherence to prominent cyber security frameworks. These capabilities will contribute significantly to the robustness of your cyber security strategy without incurring exorbitant costs.

Cloud migrations and the proliferation of IoT are now the norm and so the integration of all facets of IT is paramount. Cloud migrations have become integral to modern business operations, offering scalability, flexibility and enhanced collaboration.

Embracing cloud technologies requires a cyber security approach that safeguards data both in transit and at rest, ensuring the confidentiality and integrity of sensitive information.

IT environments will continue to grow and become more complex, and so it becomes essential to adapt cybersecurity measures accordingly. Ensure that your chosen cyber security solution is flexible enough to encompass diverse IT ecosystems, including cloud-based and IoT components, to effectively address the challenges posed by the interconnected nature of modern IT infrastructures now, and in the future.

OUTSOURCE SOME IT SERVICES

If your payroll is constrained, it might be a viable option to outsource some of your IT support services. However, outsourcing IT support only really works if you can find a Managed Service Provider (MSP) that can either do it cheaper than hiring someone yourself (often not the case) or if IT services are budgeted differently within your company than payroll.

Outsourcing to an MSP or Managed Security Services Provider (MSSP) is, however, a good way to get expertise in the short term in the current challenging labour market as finding IT engineers with the correct level of expertise can be difficult. By outsourcing some of your team's day-to-day responsibilities to a trusted third party, you can save time and focus on core business activities.

Picture credit: Adobestock

EVALUATE CYBER SECURITY SUPPLIERS

If you're expanding and optimising your IT team, *and* looking for new software *and* investigating outsourcing opportunities it can be easy to overlook the importance of managing the existing suppliers you already have. Running a thorough review of suppliers and the services they provide might present opportunities where you can reduce your cyber security spending.

By doing a full cyber security review, you can weigh each service you have against the cost and renegotiate your agreement or look for a more worthwhile alternative. Ask your team what value they are getting from your current suppliers and compare them with other options. Alternatively, ask your existing supplier what more they could offer. You may end up with a better service, boosting your overall IT security.

FOLLOW BEST PRACTICES

IT security is a company-wide responsibility – and this needs to be made clear to everyone. The better your workforce is informed about cyber security, the easier the job will be for your IT security team. Training your entire workforce may seem like a big investment. However, knowing that the average cost of a cyber attack in 2022 was $4.35-million, it can be argued that it is worth it.

Make IT security an important part of employee onboarding and introduce regular training sessions for staff members. Focus on the essentials like strong passwords, how to spot phishing emails, keeping software updated, suspicious links and multi-factor authentication. Involve the whole workforce in keeping your company safe. This should help minimise damage and disruption to your business and make everyone more accountable for IT security.

MORE TIME TO DO WHAT MATTERS

It's important to focus your IT team's time and effort on the tasks that really matter. Find the tasks that take up the most time and investigate whether these processes can be automated. You might think that cyber security automation is expensive, however, once you compare the cost of automated cyber security tasks with that of the labour required to do everything manually, it should be a no-brainer.

For example, automating the identification and inventory process for your complete IT infrastructure is entirely possible through the use of IT Asset Management software. The effective management of IT assets plays a vital role in bolstering IT security efforts since safeguarding the unknown is challenging. Through routine automated scans, you can consistently maintain an accurate and current record of all devices linked to your network, thereby providing a more robust IT environment support for your various IT endeavours.

In a world where IT security threats and challenges will continue at a frantic pace, the imperative to safeguard sensitive data and digital assets is undeniable.

Navigating this bombardment of attacks while shoring up your defences calls for strategic resource allocation, by smartly recruiting, upskilling, outsourcing, and making judicious technology investments.

However, all is not lost and companies can fortify their defences without having to endure significant financial strain. These strategies pave the way for enhanced cyber security, marked by resilience and security without having to blow your IT budget. ●

Laura Libeer, Technical Content Writer at Lansweeper, brings over 7 years of experience working in IT asset management, and currently serves as a Technical Content Copywriter at Lansweeper.

A full cyber security team, where every role is filled, will make operations run much more smoothly