# TIME TO UPSKILL?

**James Hadley** *reveals why the defence sector must optimise its workforce with cybersecurity upskilling*


**We know that a single phishing email is all it takes for bad actors to launch an attack that could take down a multi-billion-dollar enterprise. This is one of the reasons cybersecurity professionals often talk about humans as a weakness in the defences of otherwise well-protected organisations. We disagree. In fact, humans are not a security liability but an untapped defence asset.**

We believe that a workforce can be optimised to become the ultimate defensive asset, with every single member of staff empowered with the skills, knowledge and judgement to tackle new and emerging cyber risks. Today, advanced simulations available in web browsers offer the ability to develop the cyber capabilities of every staff member. When simulations are built to reflect realistic environments and updated to reflect a changing threat landscape, they offer an unparalleled way of battle-testing resilience and preparing for emerging risks. Simulations are one part of a wider cyber optimisation strategy that develops capabilities across an organisation.

Immersive Labs recently announced that it is working with the British Army to continuously assess and optimise the cybersecurity capabilities of its entire workforce. Like any organisation, the Army can improve every aspect of its capabilities by focusing on the security skills of human employees, from soldiers fighting on overseas battlefields to digital deliverers or technical specialists working behind the scenes here in the UK.

Upskilling the British Army sets an example for the wider defence industry – as well as other sectors. Here, we will set out our argument that exposing staff to cyber workforce optimisation is the best way to prepare them for battle in the cybersecurity arena. Arm all human employees with the right cyber skills and they can all do their bit to defend every organisation they work with.

Traditionally, it was the job of the IT department to face down threat actors and mitigate cybersecurity risk. Today, everyone should be involved. When an adversary is looking for a way into a target network, they do not distinguish between ranks or divisions, but simply search for any method of achieving their goal.

In an era when everyone within an organisation is a target, it makes sense to argue that all members of staff can play a part in mounting a defence. Once an organisation has made this shift in thinking and started to recognise the role every employee, team or department can play in both risk and resilience, it must set about developing the individual skills of each person.

The first step in making the transition to a better security posture is an honest, in-depth assessment of cyber capabilities. Older methods of proving cyber resilience could include an external audit, which tend to be paper-based examinations of an organisation's ability to cope with a particular range of threats. These legacy techniques are now inadequate. They are static snapshots that cannot hope to stand up against the ever-changing threat landscape. They are unable to measure individual proficiency or assess important aspects of resilience, such as the ability of staff members or full teams to cope with a crisis or deal with a new situation that has never been faced before.

Certification schemes have a similar weakness. They offer accreditation that relates to a point in time, without measuring performance related to emerging threats. Classroom exercises are also insufficient, once again passing on lessons that relate to dealing with one threat and exposing staff to unengaging race-to-the-finish content.

## AGNISCIAS ET OFFIC TET IPSUNT QUI A CORESSIT, QUI OMMODIT ENIHILL ORENDAM VOLUPTUR

These methods of assessment are slow to adapt and hard to scale. They cannot be measured accurately and are limited in their breadth. Without data on the ability of the teams and individuals to respond to cyber risks and no way of building knowledge, skills and judgement at pace and scale, resilience is unachievable. When an organisation is reactive, exposed and on the back foot, its confidence in cyber risk mitigation is diminished.

A reliance on technological solutions is also not enough. While they can operate extremely effectively when faced with old or known threats, if the situation changes, the tech is rendered temporarily ineffective as vendors rush to issue patches and fixes.

**Like any organisation, the Army can improve every aspect of its capabilities by focusing on the security skills of its employees**

What organisations need is a way to gain a broader and deeper view of human cyber capability across all departments. This can be achieved by exercising cyber workforces to produce insights, which can then be used to reduce the risk of attacks of breaches originating from inside or outside the business. This data can also be deployed to provide evidence of an entire organisation's cyber resilience at any given moment and used to form board packs, reduce insurance premiums and improve security or credit ratings.

To begin turning its staff into a defensive asset, an organisation must first move beyond a one-size-fits-all approach towards a new paradigm, which not only continuously assesses human employees' skills and knowledge but also their ability to make decisions and judgement calls in the heat of the moment.

The use of targeted, updated simulations offers the ability to gain visibility of an entire organisation's cyber resilience. By exposing every member of an organisation to realistic simulations, which mimic the real-life situations they are likely to face, a realistic picture of risk can be created. Data gathered during simulations can be analysed to reveal granular details of weaknesses or points of strength, allowing decisions about further exercising to be made in the most informed way possible.

The upskilling process should follow a strategy which can be summed up in three parts: exercise, evidence and equip.

Firstly, teams and individual members of staff should go through realistic exercises that are role-specific yet incorporate cross-organisational aspects to mimic an incident that has impact across the entire organisation. These exercises should be adapted to reflect the nature of the organisation involved, as well as the current threats. In a defence industry context, a simulation could focus on a scenario in which criminals have stolen classified secrets. Participants could also undergo an exercise that evokes a situation in which nation-state threat actors have launched a devastating ransomware attack.

After exercise comes evidence. Data gathered during the exercise should be used to demonstrate confidence in cybersecurity or discover risk levels across all business functions. When simulations are performed regularly, data can be mapped against industry-standard frameworks to provide a real-time picture of risk.

Finally, the evidence can be used to equip individuals and departments with the knowledge, skills and judgement needed to tackle cybersecurity threats they are likely to face while working in their role. All data points can be benchmarked against peers or mapped against accepted cybersecurity frameworks. Senior leaders can also use the insight to make better-informed operational decisions and strategic investments.

Simulations are not a 'one-and-done' exercise. When using a cloud-based simulation platform and repeating the exercises, data can be continuously generated. A cyber workforce optimisation solution

Picture credit: US Dept Defense

should also collate insights and deliver quantitative analysis and visualisations of capability, expertise, confidence and improvement in individuals and teams.

Simulations and realistic exercises offer other benefits. If job applicants undergo simulated scenarios during their applications, they can be hired based on their ability to do the role, rather than previous experience, academic qualifications or professional certifications. This addresses the problem of unconscious bias in hiring and can drive increased diversity across security roles. It helps to identify untapped talent, improve social mobility and help neurodiverse individuals during job application processes.

## ILLABORERSPIS ABOREHE NTECUS VELLUPTAE SIM ENDANT VITAE. ADITATIBUS UT IDESTIIS

We use the phrase cyber workforce optimisation to describe the continual testing, measurement and improvement of cyber knowledge, skills and judgment. Cyber workforce optimisation is a philosophy that focuses on upgrading each member of staff. It grants organisations the ability to test every aspect of their defence, ranging from the performance of incident response teams to the ability of non-technical staff to play their vital roles in preventing and responding to an attack.

The constant evaluation offered by a cyber workforce optimisation solution can be used to prepare for landmark events such as meeting the regulator or speaking to the board, providing actionable, understandable data that is real-time evidence of the organisation's efficiency in dealing with cyber threats, compliance and strategic security risks. These data-driven insights can then enable an agile cycle of development, which improves cyber capabilities across the organisation. Staff may even enjoy the exercises and simulations, meaning they are much more likely to engage with the lessons and take on the best practices taught within them.

The defence sector is unique in the nature of its work. Yet it faces similar threats to any industry holding sensitive data or other information of interest to external threat actors. We know that nations including Russia, China and North Korea are always seeking opportunities to target the defence industry, whether it is to steal secrets, gain actionable military intelligence or simply cause damage. Cybercriminals are also looking for opportunities to make money.

When the stakes are high, the response must be appropriate. We have established that legacy methods of ensuring, proving and demonstrating resilience are ineffective. Traditional defences are suitable for known dangers of the past, but are unable to cope with a changing threat landscape and therefore cannot add to overall resilience.

Too many organisations in the defence industry and beyond are blind to their preparedness for the cyberthreats of today and have no way of demonstrating resilience. But leaders now have access to the tools to allow them to upskill and optimise their entire workforce, turning them into a valuable strategic asset. Optimise the workforce and together every member can build stronger defences. ●

**James Hadley** is CEO of Immersive Labs

**Advanced simulations offer the ability to develop the cyber capabilities of every staff member**