EMMA BOAKES

CONVERGING SECURITY

Why cyber and physical security should collaborate, and what it takes to achieve this.

Organisations are increasingly reliant on internet-based technologies for physical assets such as building management systems, internet of things (IoT) devices and operational technology. Such technologies create new vulnerabilities that can be exploited through a cyber-attack. Indeed, the number of attacks where a vulnerability in cyber security has been used to target physical systems or vice versa, have been increasing (Symantec, 2019). Looking specifically at IoT devices, a 600% increase in attacks was reported in 2017 (Symantec, 2018). Gartner's *Predicts 2020* report highlighted "...incidents in the digital world have an effect in the physical world, as risks, threat and vulnerabilities now exist in a bidirectional cyber-physical spectrum".

To understand and mitigate threats that cross the boundary between what is cyber and what is physical, some organisations have integrated their security resources to encourage them to work more closely together. While intuitively it makes sense for security functions to converge, to date there has been little evidence to support this. Indeed, there remains a lack of guidance on how to effectively implement converged security. Without evidence and guidance, organisations seeking to adopt convergence may be setting themselves up for failure and even be implementing new structures and processes that will allow new vulnerabilities to emerge. Research is needed to build an evidence-base that will help organisations make informed decisions when deciding how to implement convergence.

> Without evidence and guidance, organisations seeking to adopt convergence may be setting themselves up for failure...

My research aims to provide such an evidence base. Structuring my research around evidence-based practice (Briner, 2019), I carried out three qualitative studies with security staff from a range of organisations and industries that operate converged security from around the world:

1. I conducted interviews with five senior security experts who have experience implementing convergence to start to identify a web of interconnected factors that support the implementation and operation of convergence.
2. I carried out a three-round Delphi study with a panel of 23 security professionals to validate the factors identified in the first study and to rate them on their importance for effective convergence.
3. Finally, 15 senior staff involved in the decision to converge in their respective organisations were interviewed using an epistolary interview technique (i.e., interviews using a series of written communications), carried out over email. These interviews identified how organisations decided to adopt converged security and the process and activities they used to design its implementation.

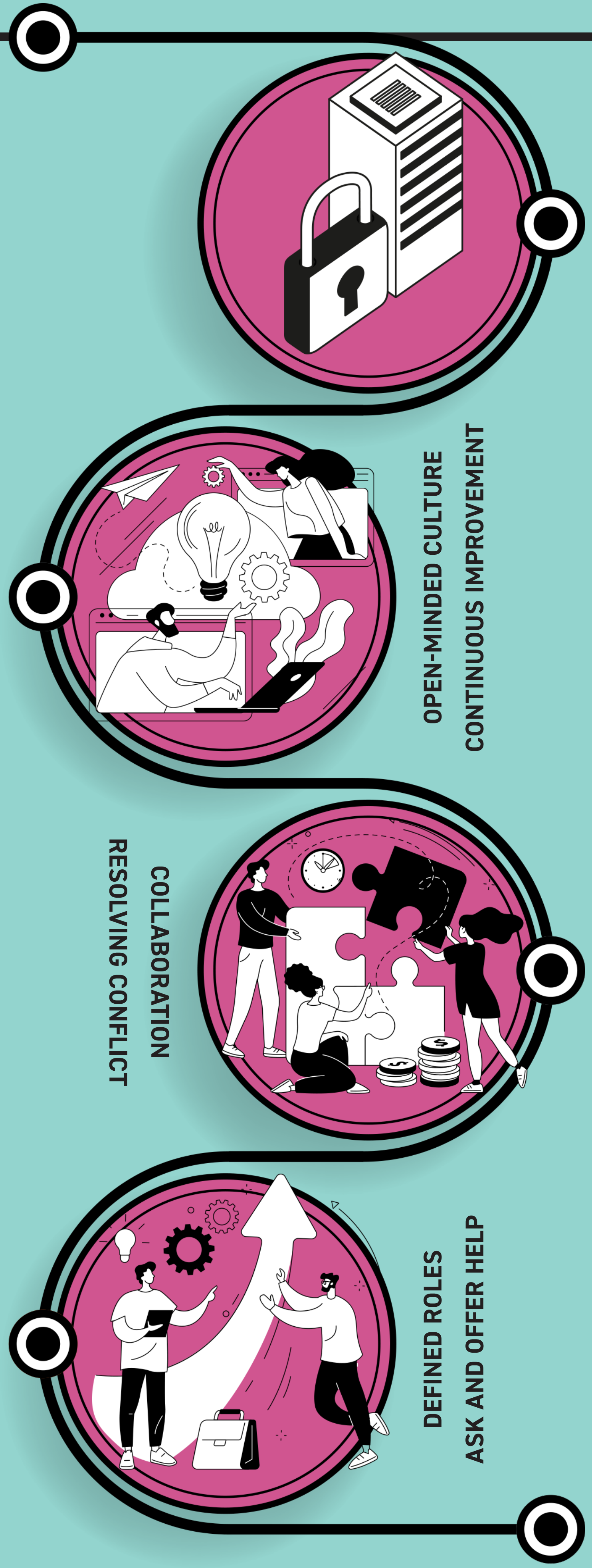
ESTABLISHING CONVERGED SECURITY

My research established that organisations adopt convergence in an effort to:

- Manage risk in the changing threat environment.
- Reduce complexity across the security function.
- Improve efficiency and make cost savings.

Convergence is often instigated by the insights of key security personnel but is also influenced by other organisations, government and industry associations.

The decision to adopt convergence is only one element of the decision-making process. My results showed that organisations have different ways of implementing convergence as it is dependent on organisational context. To achieve an appropriate and workable implementation of convergence, organisations need to draw on insights from within their security functions and consult with staff to capitalise on their first-hand experience of security in context.



> Convergence requires facilitation and active management to engage staff in the appropriate collaboration.

ACHIEVING COLLABORATION

The establishment of organisational structures that bring security resources together under a common management and with a common goal are not enough to ensure convergence. Convergence requires facilitation and active management to engage staff in the appropriate collaboration. My research found that convergence relies on a web of interconnected factors, and to achieve collaboration, organisations need to cultivate each of these building blocks:

- Organisations need to foster a culture within security that encourages staff to be open-minded, promoting continuous improvement, setting the precedent that security will develop over time.
- Staff need to buy-in to the idea of collaboration, and management can play an active role in enabling this, from reviewing progress to resolving conflict.
- Collaboration is facilitated by staff having clearly defined roles and responsibilities. They need to be provided with opportunities to engage with each other formally and informally to help build working relationships and to enable them to ask for and offer help from each other.

WHAT DOES THIS RESEARCH MEAN?

The final stage of the research will be to use these findings to generate an evidence-based roadmap. The roadmap will specify the design decision organisations need to make when adopting convergence, and will help them identify the different sources of information they can use to inform those decisions.

The roadmap will also indicate the range of factors that organisations will need to consider to support effective convergence. The roadmap will, therefore, provide organisations with an evidence-based guide that helps them navigate the adoption and implementation of convergence in their context.

Emma Boakes is a final year PhD student at the University of Portsmouth. Her research explores security convergence.

Image credit: Adapted from *Gstudio, alestraza* and *Visual Generatio* | stock.adobe.com