BEYOND blue

NEWSLETTER
JANUARY 2023

In this month's newsletter, we consider the G7's timely recent joint paper on the fundamentals of ransomware resilience, reflect on the role that the much-vaunted gamification can have on honing board-level engagement with cybersecurity and assess the virtues and vices of the trend towards SaaS-based security products.

David Ferbrache OBE, Managing Director

LESSONS FROM G7

For financial firms around the world, whether large or small, the threat posed by ransomware attacks continues to dominate. This is in spite of the fact that the likelihood of a successful ransomware attack remains relatively low. However, the impact of these attacks can be devastating and the broader consequences systemic. Moreover, success promises criminal actors very high rewards.

Financial regulators have also begun to take a serious interest in this area. In a notable recent example of this, the regulators of the G7 nations have released a joint paper aimed at outlining various key good practice guidelines for financial institutions on shoring up their defences against ransomware. This piece serves as a companion to a similar 2016 publication which looked more broadly at what key measures G7-based financial sector firms could do to shore up their cybersecurity. The decision by the G7 regulators to return to this theme just 6 years later albeit with an exclusive focus on ransomware highlights just how much concern exists in the global community about the threat posed to financial markets infrastructure (FMI) and systemically important firms from these attacks.

Much that the paper has to say is solid, sensible and actionable. However, a couple of elements deserve special mention.

Firstly, it's notable that the G7 regulators have decided to highlight the fact that governance of ransomware incidents is a firm-wide initiative and not merely the responsibility of information technology teams. A successful ransomware attack will likely hit every aspect of firm operations. Hence, effective governance will demand board-level oversight. Managing a ransomware incident effectively requires a high-level of coordination across business units, from communications to customer treatment. Failure to get buy-in from the top levels of management can make achieving this remarkably challenging. This is a lesson that unsuspecting firms are in danger of learning the hard way.

The second thing worth mentioning is the discussion of the role of cyber insurance. There is always the risk that cyber insurance policies are viewed as a substitute for embedding good cyber hygiene and resilient operations and technology within a firm so that they can respond adaptively to adverse cyber events. This is all the more concerning as cyber insurance policies are becoming more conditionalised and difficult to acquire, as insurers seek to manage their portfolio exposure. However, these concerns are flagged by the G7 regulators. So too is the often critical role that cyber insurers can have in incident management, providing invaluable guidance on matters such as forensics, public relations and communications with the attacker. This balanced view of the risks and rewards of cyber insurance is welcome

Of course, there will remain the challenge that all these wholeheartedly prudent recommendations still need to be embedded within organisations which are often large, complex and averse to change. This is no small feat. The recommendations being made by the G7 regulators are welcome. But they are non-binding. These changes will need to be driven internally and will require a buy-in at board-level and down. The difficulty for those working within financial sector firms to ensure they are operationally and technologically resilient to ransomware is that they must secure this endorsement if these recommendations are to be followed. One hope is that the clout of the G7 will go some way towards making it easier for them to achieve this.

GAMIFICATION: PLAYING IT SAFE

Cybersecurity can be a difficult topic to grasp, especially if it's not your day job. It's a little abstract, it's sometimes technical and there is a sea of competing good practice guidelines and standards users have to grapple with. (Should your password be a string of random, unconnected characters? Or should it be something memorable that you don't need to write down on paper to remember?) However, it's also something that all members of an organisation should be attuned to at some level. After all, each one of us has a part to play in protecting the organisations we work for whilst simultaneously engaging daily with complex digital systems, most of which are likely exposed to the public internet. This poses a unique strategic challenge: how can organisations ensure a near ubiquitous awareness of good cyber hygiene, even given that many employees are non-technical and that the borders between personal and home networks are becoming increasingly blurred.

For many, gamification promises to provide something of a solution to this problem. Gamification is the process of adding game mechanics into a nongame context with an eye to enhancing user interaction and engagement. Its use has been perhaps most conspicuous when deployed by marketing teams in developing gamified experiences to connect users with products and sales channels. But it has also been used by others to build experiences which enable users to share knowledge and learn. This latter application marries well with user awareness training and education.

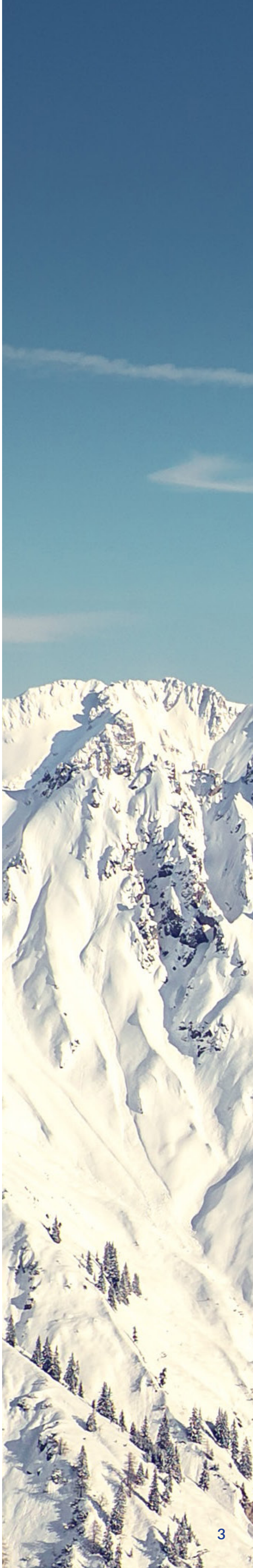
The hope held by many in the cybersecurity awareness and training space is that gamified experiences can provide both the accessibility and coverage to upskill their workforce. We all love those little dopamine hits our brain rewards us with, so when we integrate additional elements such as competition and the desire for reward, it makes the experience fun and the educational content might be more liable to stick. Moreover, there appears to be few limits on who can benefit from this approach. All colleagues can gain from thinking through the challenges of maintaining good cyber hygiene. These elements can be fed naturally into existing training programmes and initiatives to supplement the user's existing understanding. But there is also the hope that gamified experiences can go some way to improving board-level engagement with cybersecurity issues and investment decisions.

However, there is also the perceived risk of so-called gamification failure, i.e., the risk that gamified experiences can appear gimmicky and seem to trivialise an important issue. Ultimately, this can mean that these experiences simply distract from the deeper underlying issues at stake, with the user's attention focused squarely on the game mechanics like point-scoring and off the intended educational elements. This perceived gimmicky-ness can also make it difficult to encourage executives and the board to engage with such experiences. It's hardly surprising that busy people with stuffed diaries and substantial responsibilities might well balk at the prospect of losing an afternoon to a glorified videogame.

The nerdy stigma and air of triviality surrounding gamification is a significant hurdle that must be overcome if it is to be leveraged effectively to engage senior executives. The challenge is to bring to life the impact cybersecurity failures can have on corporate reputation, profits and operations by making the experience feel real to them. To do this, it is critical to dispel the gimmicks and any elements of the experience that make it feel like a computer game. Instead, you should be striving to create an immersive experience which feels both challenging and credible. What makes this particularly hard is that you must still try and make the experience enjoyable and constructively competitive. It should feel less like an escape room and more an immersive, interactive theatrical experience.

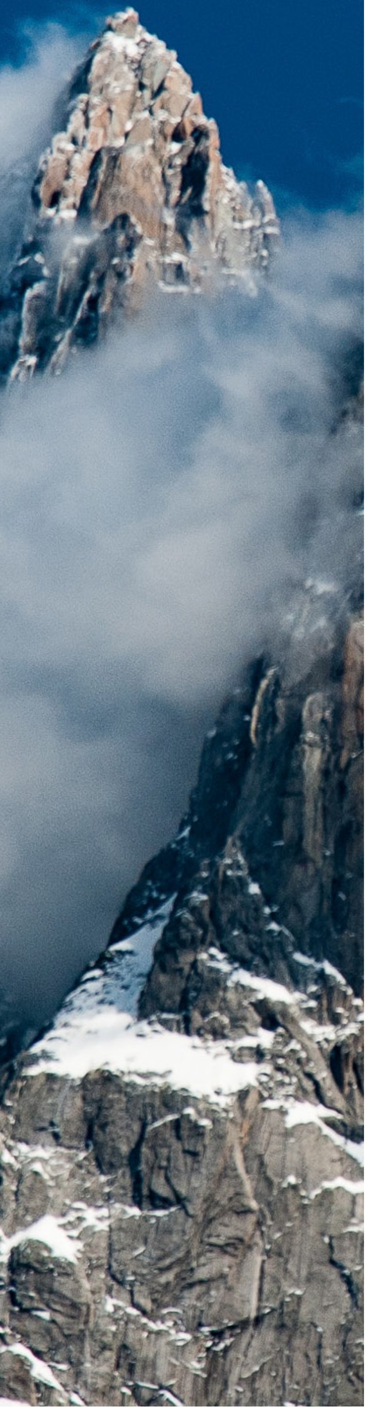
Success in these areas will often be determined by how you pitch the product. The focus of a gamified experience aimed at senior executives should be placed firmly on strategic decision making and incident management. Simulating an environment in which players are able to test these skills and in which they can witness the consequences of both good and bad decisions is the key. Relatedly, it is important to avoid too much jargon or an overt focus on technicalities. This will likely alienate many and is unlikely to have much of a bearing on the strategic and operational considerations that are at stake.

There is no doubt that much of the hyperbole surrounding gamification should be taken with a pinch of salt. However, it is more than just a buzzword. When deployed with care and attention, it can serve as an inspiring and beneficial learning tool. Moreover, it offers a unique opportunity for engaging executives with difficult and consequential strategic decisions in a dynamic and risk-free environment. *Watch this space…*



OPINION PIECE – *SAM HEWSON*

Sam joined Beyond Blue as a Senior Consultant in Summer of this year after working for several years in the UK financial sector. Sam previously held the position of Security Product and Delivery Manager for one of the UK's leading retail banks. Whilst in that role, Sam led on a number of key projects and enhancements in the Security Engineering space for the Chief Security Office.



TO MIGRATE OR NOT TO MIGRATE: **SAAS BASED SECURITY PRODUCTS**

Across all industries and technology types, the appetite to migrate to Software-as-a-Service (SaaS) cloud solutions is increasing by the day. The options for scalability, fewer on-premise dependencies, increased disaster recovery (DR) capabilities are just a few of the many benefits. Hand in hand with these near limitless capabilities, cloud companies small and large are also increasing the opportunities for security-based SaaS solutions.

On the market, there are currently a wide range of traditional and new vendors breaking through with cutting edge security offerings. Many of these make use of machine learning and AI-based tools to help mitigate the most sophisticated threats to your business. However, I've personally found that there is a stigma that these tools can be quickly adopted and deployed. This isn't surprising given the related stigma surrounding cloud and agile deployments/projects.

Inevitably, this has led to businesses adapting new SaaS-based security products without the correct due diligence. I want to focus in on a specific but very important kind of security product: endpoint security tooling.

Endpoint security is an organisation's first line of defence against threats inside and outside of its Network. Endpoint security products aren't just something you take off the shelf and which you can deploy to your organisation immediately. The foundation for deploying a new endpoint security product needs to be intelligence driven. This intelligence needs to be based off of data which incorporates as much Telemetry as possible. This will underpin your Custom Rule Detection and Threat Hunting Capabilities. Some of these threats your organisation needs to mitigate against will be custom to your organisation alone. This is why at the heart of one of these migrations, your intelligence and SOC analysts needs to be involved.

In summary, it's not incorrect to pair cloud and agility together. It's a proven fact that cloud is more agile and can certainly speed up a business's capabilities to deploy and release new products, services and capabilities. However, it is important to not take this stance with SaaS-based Security Offerings. There isn't and never will be a 'silver bullet' to cybersecurity. A security posture of a business is underpinned by data and intelligence and the same will always apply for SaaS-based Security Offerings as well.