Picture credit: Carlmagnus Johansson

MOD FIGHTS BACK

Gary Barlet *explains why it's wartime against cyber criminals for the Ministry of Defence*

As a Western economic, political and military powerhouse, the UK has always been a common target for cyber warfare from nation-state adversaries and cyber criminals. Over the last five years, the Ministry of Defence (MoD) has experienced a 400 percent increase in data breaches, which reflects the UK's lack of resilience to such threats. Despite the government increasing its cyber security spending by 21 percent last year, the data breaches have continued. The rapid evolution of technology means any cyber advantage is often short-lived, creating a constant game of cat-and-mouse. So, how can the MoD become more resilient and rebuild public trust in the UK's national defence in this new age of cyber warfare?

Legacy technology continues to expose the MoD to escalating cyber risks. Outdated systems and insecure connections create significant vulnerabilities, making the MoD an attractive target for cyber criminals. Many legacy defence systems still in use today were designed without considering the interconnected nature of modern cyber threats. For example, military installations, much like small cities, have their own power, water and communication systems. The defence industry has made strides in designing more modular and upgradable systems. However, many old systems remain in place, posing substantial risks.

Also, the cost and complexity of replacing these critical legacy systems can be prohibitive. The continued reliance on such systems creates easy entry points for attackers. For instance, legacy IoT devices, control systems and communication networks on military installations mirror the vulnerabilities found in commercial infrastructure.

The use of third-party providers further exacerbates the MoD's cyber risk. Many of these providers do not adhere to the strict security standards necessary to protect sensitive defence information. This creates significant weak links in the ministry's security chain, expanding the attack surface and making it difficult to predict the source of the next breach. So, how can this challenge be addressed effectively? The first plan should be to prioritise updating and patching legacy systems, even if replacement is not immediately feasible. This includes implementing modern security protocols around older technology to mitigate risks.

Additionally, the ministry should conduct thorough security assessments of all third-party providers, ensuring they comply with the highest security standards. Regular audits and continuous monitoring are essential to maintain a secure defence network. Once these basics have been achieved, it's crucial to consider proactive security strategies like Zero Trust.

Zero Trust has become a key focal point in the public sector's defence strategy across the globe. Although only the US government has mandated its implementation, it's become a key strategic consideration across various industries in the UK. However, time is of the essence, and a Zero Trust strategy is critical for the MoD to enhance its security posture. It operates on the principle that no entity, whether inside or outside the network, should be trusted by default. This approach contrasts sharply with traditional security models that often assume internal entities are inherently trustworthy.

During my time as a Squadron Commander at an Air Force base, one of my biggest concerns was the interconnected assets within the network. The weapon systems had robust built-in security mechanisms. However, the assets to support those weapons systems, like power substations or water transfer points, didn't have the same mechanisms. So, any potential breach in such assets could enable lateral movement. However, Zero Trust can effectively address such risks.

The strategy requires continuous verification of all users and devices attempting to access resources. This model demands rigorous authentication, authorisation and validation at every access point, significantly reducing the risk of unauthorised access. To begin, the ministry should map out its entire network, identifying all assets, users and data flows. Understanding the complete landscape is essential for implementing effective access controls and monitoring systems. Next, the MoD needs to segment its network to create isolated environments. This segmentation minimises the potential damage from breaches by containing them within smaller, controlled network sections.

Multi-factor authentication should be mandatory for accessing sensitive systems and data

Strong access controls are fundamental to Zero Trust. Organisations must ensure that users and devices are granted the minimum level of access necessary to perform their functions. This principle, known as the principle of least privilege, helps to limit exposure and reduce the attack surface. Additionally, multi-factor authentication (MFA) should be mandatory for accessing sensitive systems and data. MFA adds an extra layer of security, making it significantly harder for attackers to gain unauthorised access.

The ministry must deploy advanced monitoring tools that can detect suspicious activities in real-time. These tools should utilise machine learning and artificial intelligence to identify anomalies and potential threats quickly. Regular audits of security policies and access controls will help ensure that the Zero Trust framework remains robust and effective.

It's also important to remember that implementing Zero Trust is not a one-time project, but an ongoing process. Organisations must be prepared to adapt its strategy as new threats emerge and technologies evolve. This continuous improvement approach will help maintain a high level of security over time.

Implementing Zero Trust requires careful planning and execution to avoid common pitfalls. One of the primary mistakes we see organisations make is assuming a one-size-fits-all approach. The MoD includes several entities such as the army, Royal Air Force (RAF), Royal Navy (RN), and nuclear sites. Each of these branches works very differently and uses different technologies. Therefore, a tailored Zero Trust strategy is essential.

Another common mistake is treating Zero Trust implementation as a project with a defined endpoint. Zero Trust is an ongoing process that needs continuous attention and adaptation. Organisations must avoid the trap of believing that once certain controls are in place, the job is done. Cyber threats evolve rapidly, and the MoD's defences must evolve in parallel.

Focusing on one aspect of Zero Trust at a time, such as completing one security pillar before moving on to the next, is a flawed approach. The MoD should work on all aspects of the strategy simultaneously. This holistic approach ensures that all components of the security framework are integrated and function cohesively.

THE USE OF THIRD-PARTY PROVIDERS FURTHER EXACERBATES THE MOD'S CYBER RISK

Another critical error is neglecting legacy systems during Zero Trust implementation. Legacy systems often pose the greatest security risks and should be a focal point of the Zero Trust strategy. The MoD must implement modern security measures around these older systems to mitigate their vulnerabilities.

Also, failing to provide adequate training and communication about the Zero Trust model can undermine its effectiveness. All personnel must understand their roles within the new security framework and the importance of adhering to security protocols. Regular training sessions and updates on emerging threats will keep staff informed and engaged.

For any citizen, seeing their national defence being frequently targeted by foreign adversaries is significantly worrying, even if it's on the cyber front. Unsurprisingly, the central government's increasing vulnerability to data breaches has also negatively impacted public confidence. A recent survey by Illumio revealed that nearly one-third of the public lacks trust in the government's capability to protect their data.

This lack of confidence is not just a public relations issue; it impacts national security and the overall effectiveness of defence strategies. Rebuilding this trust is essential. So, establishing public communication and assurance should be a top priority in the national cyber security agenda.

In the United States, President Biden's Zero Trust memorandum has positively impacted public confidence. The executive order outlined clear directives for improving cyber security across federal agencies, demonstrating a committed approach to tackling cyber threats. This public declaration of intent reassures citizens that the government recognises the problem and is actively working towards a solution.

The UK government must adopt a similar approach to restore confidence in its cyber security measures. A clear and transparent strategy must be communicated to the public, emphasising the steps being taken to secure national defence systems. This strategy should include a commitment to increasing focus and resources dedicated to cyber security. By publicly acknowledging the challenges and outlining a concrete plan of action,

the government can begin to rebuild trust. The first step in this process is recognising the scale of the problem and the necessity for a coordinated response. The MoD must prioritise cyber security at the highest levels, ensuring it receives the attention and resources required. This includes investing in modern technologies, training personnel and adopting best practices in cyber security. Publicising these efforts demonstrates the government's commitment to addressing cyber threats head-on.

IMPLEMENTING ZERO TRUST IS NOT A ONE-TIME PROJECT, BUT AN ONGOING PROCESS

Moreover, the government should engage in regular communication with the public about cyber security initiatives. This could include updates on progress, success stories, and explanations of how new policies and technologies are enhancing security. Transparency in these efforts will help to demystify cyber security and show that the government is taking tangible steps to protect national interests.

International collaboration is vital for strengthening cyber security resilience. Effective information sharing about threats and vulnerabilities allows for quicker responses and better-prepared defences. Countries can benefit from each other's experiences and develop more robust cyber security strategies.

Collaborative efforts can include joint training exercises, coordinated cyber defence initiatives and shared research on emerging threats. These partnerships help create a united front against cyber adversaries. For instance, NATO and other international coalitions regularly engage in cyber defence exercises to improve collective security measures and response strategies. Moreover, international collaboration can facilitate the development of standardised protocols and frameworks for cyber security. This harmonisation can reduce the complexity of managing cyber threats across different jurisdictions and improve overall security.

The UK can leverage global expertise and resources by working closely with international partners. This cooperation strengthens the nation's cyber defences and demonstrates a commitment to collective security. It also reassures the public and allies that it is proactive in addressing the ever-evolving cyber threat landscape.

The future of cyber defence lies in agility and continuous adaptation. As technology evolves, so do the tactics of cyber criminals. Staying ahead requires constant innovation and the rapid adoption of new technologies. Artificial intelligence and machine learning will play increasingly important roles in detecting and mitigating cyber threats. These technologies can analyse vast amounts of data in real-time, identifying patterns and anomalies that indicate potential attacks.

However, the rapid pace of technological change also means that defences must be regularly updated. Cyber defence strategies must evolve to counter new types of threats, such as those posed by quantum computing and advanced persistent threats. This requires a commitment to ongoing research and development. Building a skilled workforce capable of handling sophisticated cyber challenges will be essential. The defence sector must attract and retain top talent, ensuring that personnel are well-equipped to manage and respond to cyber incidents.

Finally, fostering a culture of cyber security awareness at all levels of the organisation is key. Regular training, clear communication and a focus on best practices will help create an environment where security is a shared responsibility. By embracing these principles, the UK can build a resilient cyber defence infrastructure capable of withstanding future threats ●

Gary Barlet is Public Sector CTO at Illumio.

The MoD must prioritise cyber security at the highest levels, ensuring it receives the attention and resources required

Picture credit: Crown Copyright