FIRST LINE OF DEFENCE

William 'Hutch' Hutchison *unpacks the biggest cybersecurity challenges facing operational technology and explains why mil-spec cyber-preparedness can stand companies apart in the face of cyber threats*

From an issue swept under institutional carpets, to a central risk mitigation tool upending the priorities of large organisations, cybersecurity has become the new battleground for businesses in 2023. Tactics, techniques and procedures (TTPs) from nation-state-backed groups have been accelerating in their sophistication since the onset of the Russian war in Ukraine. Now, they are being used against businesses, as corporate leaders are faced with challenging investment decisions.

Echoed in the boardrooms of critical national infrastructure providers around the world are the same questions. "How can I operate effectively and protect my top-line growth?", "how do I concurrently validate cyber protections for IT, OT and physical systems?" and "how do we benchmark, improve cyber effectiveness and measure our security ROI?".

If correctly answered, CISOs and their boards can guide security strategy to a place of cyber-readiness, creating well-poised organisations ready for the ransomware and data extortion techniques of groups like Killnet and Darkside. Conversely, untested security stacks can leave infrastructure open to popular methods such as denial of service attacks. This has the potential to disrupt the manufacturing industry's ability to produce metals and machinery, the agriculture sector's ability to produce food or even nuclear reactors' ability to generate power.

For private and publicly owned organisations, the outcome of the cyberwar on critical infrastructure will depend on which organisations can acquire the threat intelligence to test their systems with accuracy, and which subscribe to a top-down compliance model not fit for purpose in the new, nation-state-backed era of cyber threat.

The UK Army recently conducted the largest military-led, live-fire cyber exercise in Western Europe

The Russian invasion of Ukraine represents the first hybrid war, as collaborative attacks in physical and cyber realms position cybersecurity as the new battleground dictating the safety of critical national infrastructure. However, information warfare is just one way hackers are achieving their ideological and financial aims.

Coordinated Russian attacks on Polish transportation infrastructure rendered 80 percent of the Polish train network inoperable for over a day. Even more worryingly, cyber-attacks have been used as a means of tactical warfare in the assistance of kinetic military attacks, as evidenced by Russia's hacking of the Viasat satellite network just hours before Russia's invasion of Ukraine. The attack by Russian government hackers launched wiper malware on Viasat modems and routers, erasing data and effectively destroying hardware, which also affected around 5,800 German wind turbines – prompting intervention from the EU.

Although we know attacks are growing in scale and frequency, the immediacy and sophistication of them means that critical infrastructure can no longer rely on a GDPR, tick-box approach to secure their most valuable assets. Security stacks need to be continuously tested against advanced threat techniques, garnering information on which tools need improvements to improve their cybersecurity posture.

Organisations are overwhelmed, trying to keep up with the pace of attack paths as teams are struggling to enable expensive tools in their armoury as they move towards a Cybersecurity Mesh Architecture (CSMA). CSMAs can leverage data and intelligence from a multitude of different security tools and enterprise data sources. Gartner predicts that by 2024, organisations transferring to a CSMA approach can reduce the financial impact of security incidents by an average of 90 percent.

INFORMATION WARFARE IS JUST ONE WAY HACKERS ARE ACHIEVING THEIR IDEOLOGICAL AIMS

However, the fragmentation of such a system combined with the need for government-grade cybersecurity means organisations require a way to test the interoperability of point products and APIs to form an intelligent security layer before it is deployed. Simply put, systems must be tested against an ever increasing level of detail.

Mil-spec cybersecurity environments like cyber ranges can provide a high-fidelity, live-fire range for teams to test and train their security stacks against the most sophisticated TTPs. By training systems to failure in a like-for-like digital environment, organisations can avoid the potential hazard of damaging networks and assets through testing in production.

In the early Noughties, the MIT Lincoln Laboratory, a research component of the US Department of Defense, developed the first virtual testing environments known as cyber ranges. The need for this technology originated in government bodies and intelligence agencies around the world protecting the personally identifiable information of civil servants and military personnel, as well as arms systems and confidential documents. However, as critical infrastructure emerges as a prime target for hackers today, increased importance has been placed on the quantity and complexity of operational technology (OT) testing environments.

Research from Microsoft recently revealed that cyber-attacks targeting critical infrastructure globally doubled from 20 percent, to over 40 percent of all nation-state attacks. Large critical national infrastructure organisations require the most advanced threat intelligence and cyber ranges provide this with the capacity to test three years of attacks in just 24 hours. The UK Army has also applied simulated environments to their operations, recently conducting the largest military-led, live-fire cyber exercise in Western Europe – Defence

Cyber Marvel 2 (DCM2). By performing these exercises, governmental bodies and large organisations alike aim to train Cyberops teams to achieve a deeper understanding of analytics and an ability to assess team performance and respond quickly to an emerging threat. All of these areas can be an invaluable in the event of an OT environment under emergency conditions.

UNTESTED SECURITY STACKS CAN LEAVE INFRASTRUCTURE OPEN TO UNWANTED ATTACKS

High-fidelity ranges are flexible enough to build in great detail and act as a live-fire rifle range, with security teams inputting attacks as they would be conducted in the real world. The industrial scale of the range allows for matched terrain and active traffic, giving a realistic feel of over 400,000 end point environments. This means metrics can be gathered on all tools within the security stack.

Armed with this insight, CEOs and their boards can make informed decisions about which tools and processes are working well, which require optimisation and, ultimately, which are expendable. The financial optimisation of cybersecurity tools can save organisations 50 percent time reductions and tens of millions in cost savings.

As critical infrastructure organisations improve their success in identifying key weaknesses and discovering new success benchmarks, they enable the alignment of people, processes and technology. Attacks on critical infrastructure in the last 12 months have awoken many organisations to the systemic risks attached to cyberwarfare, however many CISOs do not have the solutions to combat these risks.

Organisations embracing simulated cyber environments can get ahead of the newest tactics and techniques used by hackers and the increasing agility of their movements. Around the world, government departments and critical infrastructure organisations such as transportation operators, ports, airports and telecommunications providers should be battle-testing their cybersecurity infrastructure in light of a cyber threat that has reached critical mass.

Few individuals would have predicted the threats now posed by hacker groups leveraging ransomware-as-a-service, spear phishing attacks and malware. The stakes are too high for large organisations with a duty to protect their share price to be complacent in our collective war against attackers, but CISOs and their boards need the metrics to prove a return on investment from their expenditure. Government-grade cybersecurity can provide the measurable, military-grade assessment that is needed for today's ever-changing threat landscape.

In a world of elevated risk, CEOs want to cut through the noise of silver-bullet solutions and protect the lives and livelihoods of men and women operating machinery in OT environments. The protection and prediction against the fatal effects of an attack were articulated by Former State Secretary of Defense, Donald Rumsfeld, who developed the "unknown unknowns" framework. The implementation of cyber ranges as a risk mitigation tool removes the unknown unknowns and the blind spots of cyber threat, identifying attack vectors often missed by more rudimentary programs. Consequently, organisations can achieve the battle-readiness needed to secure their infrastructure for the unknown unknowns of the future ●

William 'Hutch' Hutchison is CEO and co-founder of SimSpace.

Russian government hackers launched wiper malware which effectively destroyed hardware and affected around 5,800 German wind turbines