DEBATE SECURITY

Converging Threats: Lessons Businesses can Learn from the National Security World

Converging Threats: Lessons Businesses can Learn from the National Security World

Twenty years ago there were two worlds: the national security world, which faced sophisticated threats from other nation states, and the commercial world, which faced threats from low-level criminals and hobbyists. For the commercial world, it was an innocent age, and not one that could last.

Today, the threats have converged. Nation states do not restrict their activity to attacking other governments, and high-end criminals share many of the same sophisticated capabilities as nation states. Commercial organisations are facing a dramatically different set of adversaries.

The potential impacts have converged as well. Through most of the history of electronics, the only truly serious impact from a "cyber attack" was the loss of military or diplomatic secrets – for example, through second world war codebreaking efforts. Today, cyber attacks can result in damage in innumerable ways. The loss of any individual piece of customer data might be no more than mildly embarrassing, but the loss of huge aggregated datasets can be catastrophic. And potentially even more damaging, cyber attacks can lead to loss of operations, loss of funds, and even physical damage. Many of these new impacts concern individual organisations rather than the nation state.

With converged threats and a converged level of potential impact, it is perhaps surprising that approaches to protection vary dramatically between the national security world and the commercial world. Can this innocent age persist, or must protections converge as well?

How could we replicate the cybersecurity strategies of the national security world?

Historically, national security organisations protected themselves against sophisticated threats by maintaining physical isolation between computer systems – the traditional 'air gap'. Bringing this approach to the commercial world was a non-starter due to the negative impact this would have on business efficiency. Far better simply to take the risk.

But within the national security world, the past two decades have seen some very significant change, driven by a yet further area of convergence: that of business requirements. For commercial organisations, the imperative to do business online and take advantage of the efficiencies offered by a networked world has been overwhelming. And at times of course, this has left security trailing. In the national security world, security has been the dominant concern: but traditional security approaches have meant that responding to and operating in a networked world has been extremely challenging.

Political pressure to deliver greater efficiency and greater effectiveness mean that national security organisations have been faced with a conundrum: how to take advantage of the tools and techniques pioneered by the commercial world without compromising their security. The result has given rise to some deep thinking, which is only now starting to emerge from the shadows. Innovation in the national security world is complex and challenging, faced with a range of unique requirements and bureaucratic overhead. It is rare that swords can be beaten directly into ploughshares. But are there learnings that commercial organisations could take advantage of while maintaining commercial needs for efficiency and cost?

Actually, we've already started

As recently as ten years ago, security operations centres were rarely found outside the national security world. Since that time, the commercial world has seen an explosion in cyber monitoring. Like the national security world, organisations have started to recognise that they should plan for failure, and be ready to detect and respond to attacks that manage to breach their defences. But in the national security world, monitoring and incident response is always a fall-back plan. To quote one senior DoD official: "we can't monitor our way out of this problem". If we want to improve our core defences, what can we learn next?

At a detailed technical level, there are some interesting learnings that are emerging specifically in the United Kingdom as a result of some recent organisational and political changes at the Government Communications Headquarters (GCHQ). In 1969, the Communications Electronic Security Group (CESG) was merged into GCHQ and for nearly 50 years thereafter, GCHQ focused its defensive role on securing the UK government. Extensive security advice (predominantly CESG branded) was released, but with circulation restricted to government security specialists.

In 2016, the UK government created the National Cyber Security Centre (NCSC). It's also part of GCHQ, but it absorbed the old CESG activities as well as various other cyber defence activities around UK government. In contrast to CESG, NCSC has a remit to protect the cyber security of the UK as a whole – not just government systems. For example, 2018 saw open publication of how to safely import data (https://ncsc.gov.uk/guidance/pattern-safely-importing-data) – the sort of authoritative technical guidance which was previously restricted to government readers.

Don’t trust security vendors

But at a more strategic level, the key learning that commercial organisations should take from the national security sector is this: don’t trust security vendors.

It is hard to overstate the difference between the two markets in this area. In the commercial world, technology buyers start from a position of “I trust what you’re saying.” In the national security world, buyers start from a position of “nice try, but I bet it’s as secure as a leaky sieve.” Sadly, nine times out of ten, the cynical view is the right one.

This then has been the core challenge for the national security world. Without security technology, they are restricted to the traditional air-gap approach – a technology which is grossly inefficient, but which through its fundamental simplicity is easy for even cynics to trust. How then have national security organisations been able to build trust in more sophisticated security technologies?

One answer has been in the development of security patterns which have been evaluated against sophisticated attackers – for example those which are now starting to be published by NCSC. The other answer has been in the creation of deeply technical security evaluation teams, and the investment of man-years of effort in evaluating the security of individual products and product vendors.

The challenge – for both the national security world and for the commercial world – is how to make this scale. From a commercial perspective, individual organisations cannot afford the skills and time required to evaluate every potential product and vendor. And from a national security perspective –even in the US military – it is hard to support a sufficiently diverse vendor base creating genuinely trusted products within such a restricted market.

The objective must therefore be to scale. Given the scale of the cyber security challenge, it is abundantly clear that investor appetite is there: the bottleneck is evidence of commercial demand, and the capacity to carry out the sort of in-depth technical evaluations at the necessary scale. One option is self-organisation: existing industry bodies could seek to replicate the national

security model and engage with high-end security testing labs both to carry out product evaluations and the training for how to interpret them.

The other option is to build out from the national security world, piggybacking on those countries (such as the UK) which are showing (at least some) desire to engage constructively with the commercial world. In the short term here, the opportunity for commercial organisations is to take advantage where possible of products already trusted by national security. In many cases of course this will be infeasible, because of differing business requirements, export restrictions or price sensitivity. But in some cases there are specific opportunities to make short-term tactical gains. In the medium term, organisations could then look for models to co-fund product assessment activity that builds on what is already in place.

The world knows how to create much stronger cyber security protections than those most organisations currently buy. If the commercial market demands them, investors will fund them, vendors will build them, and everyone will be that much more secure.

DEBATE SECURITY

About the author

Henry Harrison, CTO of Garrison

Henry is a seasoned technology industry executive and serial entrepreneur who has spent the last ten years focused on cyber security both as an independent consultant and as Technical Director for Cyber Security at UK defence and security company BAE Systems. Henry's previous ventures include a desktop videoconferencing startup, and he has been responsible for developing and selling advanced electronics solutions into governments, telecommunications companies and financial services organisations amongst other sectors.