TIME TO LEAD

The latest ransomware attacks should be a catalyst for a more strategic approach to cybersecurity, argues **MALCOLM TAYLOR**

For many in the cybersecurity industry the recent WannaCry ransomware global outbreak was, loathe as they might be to admit it too loudly, in some respects just what they had been waiting for. Not as has been suggested because of the opportunities it presents for making money, but because there has been a feeling in the industry for a while now that the 'cyber' issue was gaining publicity but no real transformative traction.

As Kris Hagerman, chief executive of security firm Sophos, said: "It is sort of a worldwide wake-up call, that we have to really redouble our efforts to get the basics right in security." So will we all do so – is there a global wake-up, a call to arms, an alarm ringing in every cabinet office and boardroom in every country? These and similar sentiments filled the media recently as health services, delivery firms, banks, individuals and more fell victim.

But an argument can be made that such a call to arms is not going to help much and may in fact cause many more problems than it solves. This argument is rooted in the approach to cybersecurity taken to date – which indeed arguably led to the success of WannaCry in the first place – and even the approach taken in the immediate aftermath of the attacks. In other words, if this is a call to arms there is a significant danger that it is simply a call for more of the same, when an altogether different approach is urgently required. That this is true beyond individual organisations – meaning among governments and policymakers too – makes it even more pressing.

TACTICAL THINKING

Currently, cybersecurity is more often than not seen as, and addressed as, a tactical issue with a technical heart. As cybersecurity is the domain of IT professionals in many (if not most) organisations, that tactical approach is almost inevitable. It creates purely technical solutions from the inside of an organisation outwards, and because these are seen as costs, not investments (not least because of their genesis in that part of an organisation), then cost is all too often a decisive factor.

Nor is this approach limited to the corporate sector. Governments are scrambling to catch up with the threat and, as ever, are slower to react. Cost is a huge factor here too with many economies yet properly to recover from the global crash of 2008 and treasury departments holding purse strings close. Witness the National Health Service in the UK, where the WannaCry attack was so problematic; the largest public sector organisation in Europe has no evident strategic approach to cybersecurity, running old and unsupported software to drive an operation carrying enormous volumes of highly sensitive health data.

One of the few senior British ministers brave enough to comment on the issue, UK Home Secretary Amber Rudd, said in the aftermath that the NHS 'may' have lessons to learn; in her delivery and phrasing of this message she unwittingly passed accountability downwards and encouraged further the failing tactical approach. The very same thing, in this argument, that caused the problems in the first place.

There are common themes in media reporting on cyber attacks and these undoubtedly play a significant role too. Fear is one; fear of the consequences and, just as importantly, fear of the solutions because of their 'otherness'. In other words, this is something that can destroy us and yet is impossible for most to understand. 'Inevitability' is a second theme; cybersecurity looks like a battle that cannot be won and yet is being fought in our houses and even on our smartphones. Finally, significant cost is implicit through much of it; if something is this difficult, inevitable and damaging, it must be prohibitively costly to prevent.

These themes do not encourage prophylactic action – quite the opposite. The media is getting a message out and that is welcome, but it is not 'the' message; it is in fact a call to arms when what is needed is a call for change.

If we are to move ourselves to a better and more secure place online then a new approach to cybersecurity is not needed – it is essential. It must address the gap between our knowledge as a society and the reality. It needs to place accountability where it should be. It needs to bridge the divide much more effectively between the public and private spheres and it needs to do it in a way which builds rather than undermines trust.

LEADERSHIP

It starts with leadership – from governments, from CEOs and boards, from those whatever they call themselves with the power to influence strategies and with the necessary financial authority to enact them. Cybersecurity is not an issue for IT professionals. They, quite rightly, run IT and

deliver performance; IT and cybersecurity are two separate disciplines. Cybersecurity belongs in the boardroom alongside the multiple other risks to business, and at cabinet tables alongside other strategic risks to prosperity, growth and, especially, critical national infrastructure. From here needs to come the informed and strategic decisions essential for a new approach.

Neither chief executives nor prime ministers understand enough about the subject – but nor, arguably, do the lawyers, accountants or the myriad other professionals needed to run a company or a country. As a result, the temptation for them to push decision making downwards is almost irresistible. Instead a way needs to be found to place the issue at the informed heart of decision making, be that a chief information security officer with full executive powers – or a department of cybersecurity or cabinet minister with responsibility for it.

This exposes another tension at the heart of many governments and therefore the policy they make; currently in the US and the UK at least, leadership of cybersecurity is coupled with technical intelligence collection. The recently created National Cyber Security Centre in the UK, for example, emerged out of, and remains a part of, the Government Communications Headquarters (GCHQ). The same is true in the US, with the added complication that the National Security Agency (NSA) has been blamed in some quarters for knowing all about the vulnerability exploited by WannaCry but not sharing this knowledge due to a competing need to exploit it in the name of national security. The intelligence communities should not be blamed for this tension.

Recognising cybersecurity as a strategic risk, rather than a tactical threat, is an essential first step. Technical staff will need to be removed from the decision-making positions into which they have been thrust. Then they will need to be led.

SPREADING AWARENESS, FORMING PARTNERSHIPS

That there is a skills gap in cybersecurity is well known, but it extends well beyond the delivery arm of the cybersecurity industry itself. There is an awareness gap too. Awareness means the recognition of the problem to a sufficient extent for it to be passed on (or too often down) for a solution; it needs to become awareness of accountability. Those who need to lead do not yet know it.

One means of starting this conversation comes from government action and policy; a close, genuine and symbiotic partnership between government, universities and industry. Again, this has, to date, been about addressing the tactical skills gap – building technicians, in other words. It needs to come up a level, to help build the understanding that cybersecurity is a strategic threat and needs managing as such. It needs to be something that people running organisations of all types, both public and private, understand enough about to be able to manage it strategically.

Involvement of the intelligence agencies in government cybersecurity roles is certainly a further difficulty; are corporations really going to be willing to risk the perception that they hand over the security of their data to a spy agency? Particularly, the giant corporations, such as Microsoft, Amazon and Apple, may fear such links the most (as the latter clearly demonstrated during the San Bernardino iPhone case). The ghost of Edward Snowden looms large for such corporations – especially in the US where state intrusion into the communications of US citizens, real or imagined, is a matter of enough concern to be judged a risk to retaining customers.

> **A call to change offers a chance to build something more effective and enduring.**

These agencies may have many of the right skills, but that shouldn't stop the necessary segmentation between them and the public sector more broadly. Public-private partnerships are too important for this not to happen, and are in fact themselves a matter of national security.

REGULATION AND LEGISLATION

Health and safety legislation is much reviled in countries such as the UK, portrayed as red tape and a burden on innovation. In fact, its primary aim is to prevent people from being killed or injured at work. Such legislation is essential, as too is cybersecurity and data protection legislation. In the EU, the General Data Protection Regulation (GDPR) comes into effect in May 2018 and is now being described as the most draconian act of its type in the world. It threatens sharp teeth and is broad reaching, but it remains to be seen how it will be enforced across national boundaries and with what kind of consistency. It is a step forward, but more could be done.

Some US states have laws requiring cyber attacks and data loss to be reported but they are believed to be widely ignored. The GDPR's reluctance to define data security beyond 'comprehensive but proportionate governance measure' is perhaps a stepping stone to something more useful (and helpful to industry) in future. And all data protection legislation challenges the internet at its core – the global, instant and untrammelled sharing of information of all kinds.

Reconciling that with the right levels of controls feels difficult – and is. But as data – our individual data – has increasing value, is it right not to even try? Individuals are being commoditised at speed through their online activity – it is said that when two people have an affair, or are contemplating such, their data providers will be the first to know. All of that demands and deserves protection.

A partnership between the public and private sectors is essential here too. Getting legislation right requires it, but it can also drive better policy including in privacy. Governments are trying to help, but there is much more they could be doing. The GDPR is a stick but incentives are few beyond avoiding the (substantial) fines. The insurance industry is building a cyber response but could benefit from government help. Tax incentives could help drive security innovation and implementation. Collecting better data could only help shape and improve the way security is enacted. Even just more availability would help – as we saw in WannaCry, to whom should we turn for help?

CONCLUSION

A call to arms is better than nothing. A call to change offers a chance to build something more effective and enduring. We need to build awareness in our decision makers, build skills in our technicians, and build partnerships between the right parts of government and the private sector. Build, in other words, a strategic and top-led approach to cybersecurity. And as the attackers won't wait we should start now.

MALCOLM TAYLOR *is head of cybersecurity at G3 (Good Governance Group), which has offices in Berlin and London. See g3.eu*