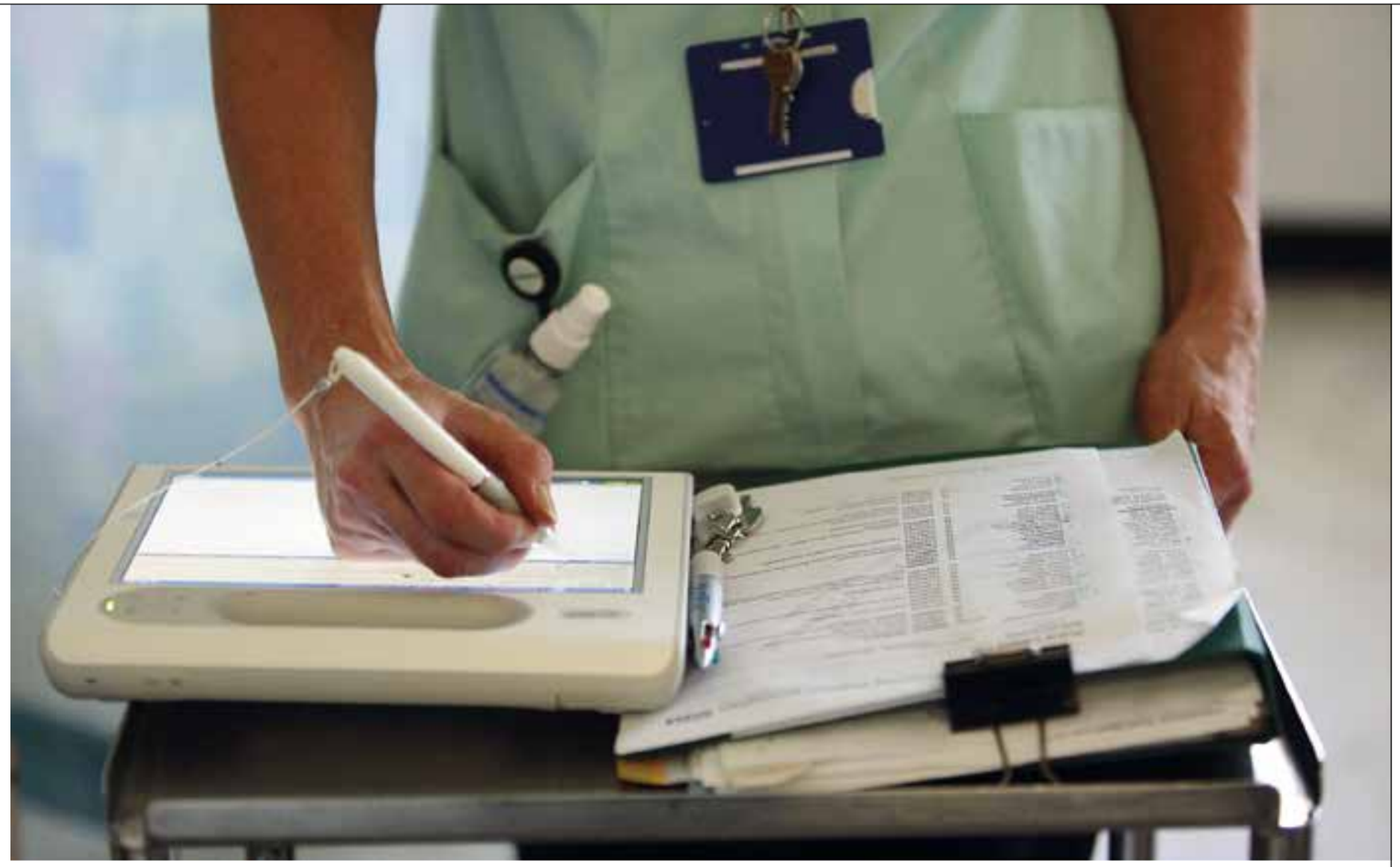
# HELD TO RANSOM

**Nik Whitfield** *reports on the lessons learnt from the WannaCry ransomware attack and the proposed changes security professionals should make to better protect themselves*



Picture credit: Getty

**Organisations need to adopt good cyber hygiene**

**WannaCry has clearly demonstrated that organisations of all sizes are exposed to the risk of destructive malware. However, before we get swept away in the media sensationalism that we could be sat on the precipice of a cyber apocalypse, we need to be clear on why attacks like these continue to succeed.**

Ultimately, it was not a sophisticated attack. It spread like wildfire because organisations are failing to maintain good cyber hygiene. This is because maintaining cyber hygiene is much harder than it sounds. It requires ongoing focus and resources. We don't need to labour on WannaCry itself. Moreover it needs to serve as a wake-up call and catalyst for organisations to get on the front foot with their cyber hygiene.

So let's be absolutely clear - WannaCry dominated the headlines because of the high-profile victims involved, other organisations don't need to become experts in the threat itself. It's just like in healthcare.

## WANNACRY WILL DEFINITELY LEAD TO INCREASED SCRUTINY AND INVESTMENT IN IT

In general, people don't need to know about every possible disease, we just need to eat well, stay hydrated, wash our hands and so on. Then, most of the time we'll be fine. We don't need to become experts in every disease. Similarly, every organisation needs good cyber hygiene: they need to understand what assets they have, keep software up to date, patch regularly and educate their employees. This forms the best foundation for cyber protection.

In security, we often confuse the negative effect suffered by an organisation, which is the victim of an attack and the positive return achieved by the attacker. Sure, there are some instances when they are directly related, such as when the attacker's motives are to cause havoc. However, in most cases this is not the ultimate motive.

The WannaCry ransomware attack is a case in point. As has been widely reported, the attack compromised a large number of machines, data, users and ultimately business processes and it propagated all around the world. This was indiscriminate, mass disruption. High-profile organisations such as the UK's National Health Service (NHS) and global companies including Telefónica, FedEx, and Renault were infected and continue to face disruption. Many companies face shareholder and customer backlash, not to mention potential fines from regulators.

How does this correlate to the gains achieved by the perpetrators? Despite the enormous success rate in infection, the ransomware campaign has only raised roughly $137,000 to date, according to Elliptic's tracking of Bitcoin payments. Some have predicted that the cryptocurrency may crash and lose half its value, so the actual take home could be significantly less, depending on when, or if, they choose to cash in. Don't get me wrong, it's still a small gain but it's infinitesimal compared with the scale of the compromise.

This evidences the asymmetry – the defenders losses and attacker gains were not in line. It could have played out very differently. Here are some scenarios:

**Increased return:** the attackers could have changed aspects of the attack in order to realise a larger return on their investment. This could have involved higher ransom charges, lower ransom charges, different threats, better targeting, different timescales – ultimately they could have optimised the attack to maximise their return.

**Different motive:** what if the attackers were just hell bent on destruction, rather than making money? What if, for example, they'd used the exploit to delete files or possibly worse still, change them? Mass wiping of data on this scale has not been seen, but it would have hugely increased the disruption.

**Covert operation:** it has been shown that at least one covert operation was underway, which was designed to harness the computing power of the compromised machines to mine Bitcoins. But it's possible (some would say likely) that other attackers could have compromised those machines and stolen IP or personal information. The potential downsides for the victims in these scenarios are much higher.

Clearly the impact of WannaCry could have been worse. The adversaries did not get the potential value available to them from the exploit they used (the recently patched SMB vulnerability). From an attacker's perspective, it was a 'waste' of a recently patched exploit.

Those of us tasked with defending an organisation's digital footprint do not have an easy life. Achieving the aim of 'adequate security' in any large organisation is fraught with issues of politics, legacy technology, scarce technical skills, attacker's agility, broken promises by technology vendors and more. In addition, there is a fundamental difficulty in prioritisation activity and a challenge in understanding and articulating risk.

## GETTING LUCKY?

So how does this ongoing challenge pertain to the success of WannaCry? The ransomware itself was not particularly innovative – once on the system, it looked for items to encrypt, encrypted them and demanded the ransom – on quite reasonable terms it seems. The only real innovation was meshing this together with a worming capability that could automatically transmit itself both within a network and between networks. Given the prevalence of the SMB vulnerability it exploited, it scaled well.

There is a debate within the industry about patching, and why it does or doesn't happen. The two competing viewpoints can be summed up as: "Patch your systems, then you won't be exposed" and "Patching is hard, so stop stating the obvious". As with many arguments, both points of view are valid. Effective upgrades and patching should be carried out, and yes, it can be difficult. The resulting conclusion is that organisations should be encouraged to focus on this thorny challenge, and to allocate sufficient resources to do this as effectively as is possible within their constraints. This sounds obvious – so why isn't this already the case? There are three issues that should be taken into account:

**Risk and the prioritisation of action to mitigate is hard:** the explosion of technology and security tools to monitor it has lead to an overload in pertinent data. Getting your arms around it in order to make the most impactful decisions is difficult.

**Security and IT teams struggle to articulate this situation to their Risk Committees:** therefore the Risk Committee is challenged in making the right prioritisation calls and how to allocate resources accordingly.

**The upkeep of ageing technology is a creeping risk, not a 'punch between the eyes' moment:** this raises a question of what the Risk Committees' view of the risk was prior to WannaCry. For example, in the NHS, was the risk considered non-critical? Was it discussed? What action was prioritised? This is the toughest job as it has to be compared and prioritised against spend associated

with mitigating immediate risks to patients' lives. These creeping risks often miss the opportunity to be seen as urgent and important.

It's these three issues that must be addressed to ensure we have more resilient systems, which are less likely to fall victim to attacks of this (and other) natures.

Answering them is a complex task. In the first instance the onus has to be on harnessing the data an organisation holds about its IT security to produce better insight into risk. Organisations using platforms like ours at Panaseer address this problem directly, using advances in data science and open-source technologies. This means they have

**ORGANISATIONS OF ALL SIZES ARE EXPOSED TO A REAL RISK OF DESTRUCTIVE MALWARE**

continuous visibility into their IT performance and risks and make better security decisions as a result.

Secondly, there must be an increased focus on IT and security hygiene. This must permeate across the technology building blocks – being clear on an inventory of hardware assets, software assets, monitoring vulnerabilities and (crucially in the case of WannaCry) applying priority software patches. Bigger, more complex organisations can use software like Panaseer's to bring together a view of these risks to enable them to prioritise best value risk reduction – for example, patching the most critical machines with critical vulnerabilities, which are likely to be exploited in the near term.

## COMMON VOCABULARY

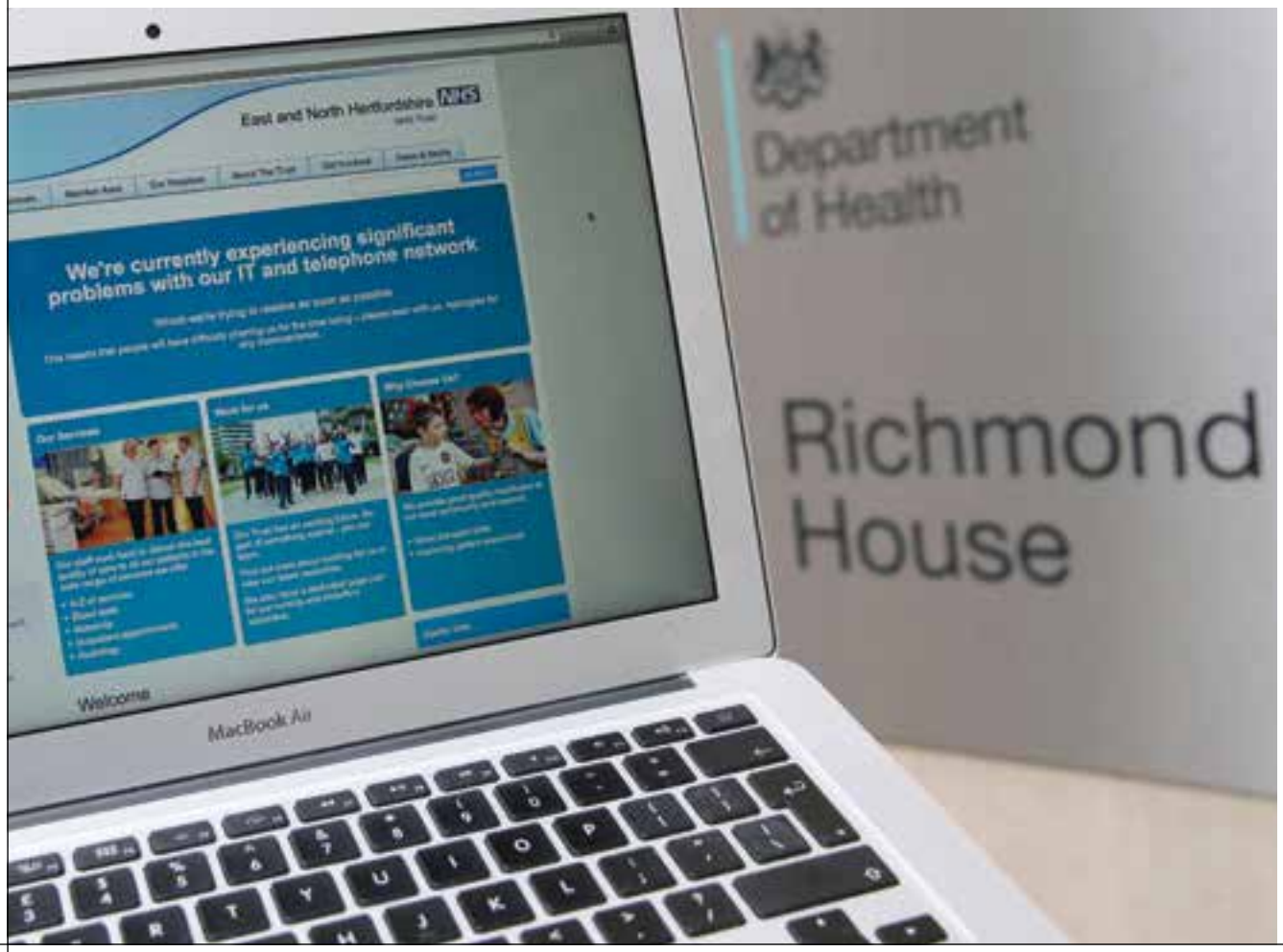
Lastly, organisations that harness their data need to use this as an opportunity to translate that information into risk pictures, which make sense to board-level decision makers. Establishing a common vocabulary with the Risk Committee around security threats, and having real data to drive that conversation, leads to a change in awareness and understanding, and in turn a sharper focus on what needs to be done to become more secure.

In the immediate aftermath of WannaCry there will be a renewed focus on enhancing cyber security and patching, vulnerability management, upgrades and end of life technology. This is human nature – whenever there is a failure, it becomes a priority to fix the problem. Over time, however, as other priorities emerge, this importance fades and resources and attention are diverted elsewhere.

In which case, let me proffer a controversial view on the WannaCry attack itself. Given that creeping risks don't get addressed until there's an incident, perhaps there is a case for suggesting that WannaCry was a good thing? It has caused relatively little downside compared with other possible scenarios and it will definitely lead to increased scrutiny and investment in IT and security hygiene. Not only that, but it's effectively neutered the specific vulnerability (and so protected against much more malicious attacks) by exploiting it so widely, as all other organisations will now have patched it ●

**Nik Whitfield** is a noted computer scientist and cyber security technology entrepreneur. He founded Panaseer in 2014, a cyber security software company that gives businesses unparalleled visibility and insight into their cyber security weaknesses. Nik has held leadership positions in cyber security, banking and technology through 20 years of working in the industry.

**The NHS was just one organisation infected**




Picture credit: Getty