Man Proposes, Fraud Disposes

Authors
Tony Leary, MSc (Royal Holloway, 2019)
Geraint Price, ISG, Royal Holloway

Abstract

In May 2017, a strain of ransomware called 'WannaCry' infected 32 National Health Service (NHS) trusts in England. The NHS's report on the incident noted that all English local authorities reported being unaffected, despite also being connected to the NHS's own national network. Ultimately, the attack proved the NHS's centralised information governance to be weaker than the equivalent governance applying to local authorities. The critical difference in approach was that unlike local authorities, the NHS didn't require its organisations to test their security. There is also evidence of the NHS mistrusting local authorities' information security management, which may have biased the NHS against adopting areas of better practice, like testing, from local authorities. [a]

[a] This article is published online by Computer Weekly as part of the 2020 Royal Holloway information security thesis series https://www.computerweekly.com/ehandbook/Royal-Holloway-Man-proposes-fraud-disposes. It is based on an MSc dissertation written as part of the MSc in Information Security at the ISG, Royal Holloway, University of London. The full thesis is published on the ISG's website at https://www.royalholloway.ac.uk/research-and-teaching/departments-and-schools/information-security/research/explore-our-research/isg-technical-reports/.

Introduction

One of Royal Holloway, University of London's most famous paintings, 'Man Proposes, God Disposes' by Sir Edwin Landseer, suggests a grisly ending to Sir John Franklin's 1845 expedition to navigate the Northwest Passage. Franklin was an experienced explorer and had two well-prepared ships under his command, HMS Terror and HMS Erebus, but both were lost along with their 129 crew.

InfoSec professionals are unlikely to consider there to be many parallels between their day-to-day work and a tale of derring-do (or Victorian folly) from over 150 years ago. Modern-day IT security disasters, such as the WannaCry and Travelex ransomware attacks, have so far only resulted in metaphorical wreckage and maulings: Look up 'CISO tenure' and you will see a role with job security only envied by Premiership football managers.

Man Proposes, God Disposes, 1864, Sir Edwin Landseer (1802-1873). Royal Holloway, University of London art collection.

However, while the IT industry has made a huge contribution to creating a safer society, whether in medicine, transport, etc., like Landseer's God, IT giveth and IT taketh away. Its role as a dual-use technology is at the heart of this dichotomy. Unlike the 'weapons-that-can-useful' e.g., nuclear fission, explosives, guns, etc., IT, despite many components having an impeccable defence heritage, has only slowly become truly dual-use. The increasing risk that IT poses underpins the debate surrounding Huawei's involvement in 5G networks: a future malicious actor could wreak havoc in a near-future society that is presumed to be both hyper-connected and hugely dependent on 5G technology. The internet is an obvious enabler of this increasing risk, but all risks need vulnerabilities, and the IT industry duly creates these in huge, and increasing, quantities. For example, Figure 1 shows all Microsoft entries in the US national vulnerability database from 1995 to 2019.

The 'known unknowns' are the quantity and severity of undiscovered vulnerabilities, which would per-

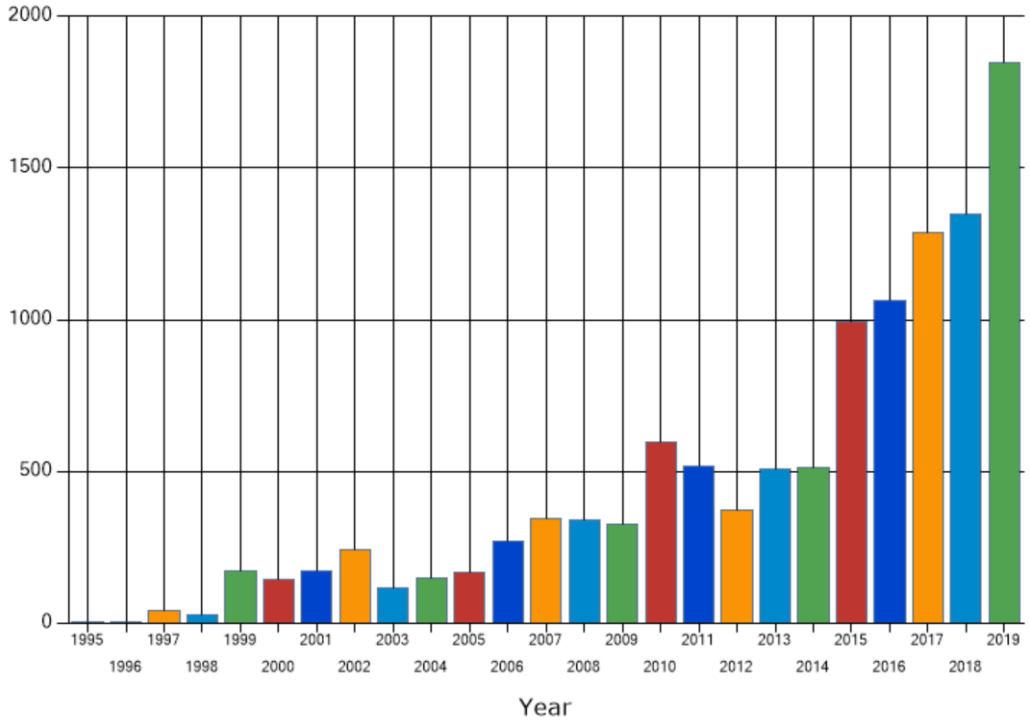

Figure 1: Microsoft reported vulnerabilities to the US NVD 1995 to 2019

haps stretch, like an iceberg, well below the graph's x-axis. It's certainly possible that the numerous bug bounty programmes now run by all large software companies, including Microsoft, are contributing to the increasing volumes shown, but the trend is nonetheless likely to warm the heart of any cybercriminal or nation-state espionage operation and, secretly perhaps, IT security vendors. Less happy will be the InfoSec professionals managing a near-constant flow of software patches, while also applying defence-in-depth controls to hopefully mitigate the risk of the known unknowns that may appear as zero-day exploits.

Fatalism would be a forgivable reaction of this now decades-long cybercriminal/InfoSec industry arms race. "There are two types of organisation, those who know they have been hacked and those that don't know they have been hacked." Not a quote from a demotivational poster, but by Cisco's Executive Chairman, John T Chambers. Realism, however, is a more practical mindset, particularly for those paid to maintain or improve organisational security. And learning from what went wrong (and perhaps right) from the victims of cybercrime, is essential.

Learning Lessons

When looking for an example of a well-documented cyber-attack to learn from, it is hard to look past the WannaCry attack that affected the NHS in England in May 2017. It has been the subject of much debate and analysis, not least within this magazine. Official reports were produced by the National Audit Office, NHS England and the UK Parliament public accounts committee, but of these, only the NHS's own 'lessons learned' report states: "Based on a 100% return from local authorities ... in the aftermath of WannaCry, no local authorities reported having been infected." This was an important finding: two interconnected organisations were at direct risk from the same cyber-attack, with only one affected. The difference in outcome between NHS trusts and local authorities presented a question to answer, did their InfoSec approaches differ and if so, was it a contributing factor?

First, the NHS (consisting of NHS trusts) and local government (consisting of local authorities including district councils, county councils and London borough councils) in England have a lot in common.

As well as being of a similar size and geographical reach, NHS trusts and local authorities are autonomous, so operate within a relatively flat structure, answerable to their relevant government departments. Second, NHS trusts and local authorities are interconnected via the outgoing NHS New National Network (N3) and the incoming Health and Social Care Network (HSCN). This connectivity supports the bi-directional flow of data needed for integrated health and social care.

One may reasonably expect both the NHS and local government to be closely aligned from a security policy perspective, if not the whole of government in the UK. However, while the government has both the authority and, through the National Cyber Security Centre (NCSC), the expertise, to set InfoSec policy, in practical terms, central government exerts little direct control over public sector information security in the UK.

The 'Security Policy Framework' issued by the Cabinet Office is the high-level 'scene-setter'. It provides indicators of good practice and refers to guidance issued by the NCSC but importantly, devolves responsibility for implementation to government departments and organisations that are ultimately answerable to Parliament, rather than the Cabinet Office. The delegation of security responsibility continues within government departments. For example, local authorities and NHS trusts are individually responsible for their own information security policy and management, with central policy control applied only tangentially: for local government, access to the public sector network (PSN) requires compliance with the Public Sector Network (PSN) Code of Connection, or CoCo, which is managed by the Government Digital Service (GDS). NHS Digital, NHS England's technology division, provides a similar role as a gatekeeper to the N3/HSCN networks, through its former information governance toolkit (IGT) and (spoiler alert) newer Data Security and Protection Toolkit (DSPT).

What Went Wrong?

There are four principal causes described in the NHS lessons learned report:

1. failure to patch promptly;
2. failure to keep anti-virus software up to date;
3. failure to manage the risk from obsolete equipment that was 'unpatchable', and
4. weak firewall/boundary controls for the internet and N3.

While the first three have a starring role in almost every successful cyber-attack, the last is particularly interesting due to the role of the NHS's own national network (N3) in allowing the attack to propagate within the NHS (though not to local authorities).

The actual source of the infection was never discovered, but it is assumed that organisations were infected via the internet or N3. It is certain that at least one NHS trust had a poorly patched Windows server, with vulnerable services exposed to the internet, whether intentionally or not. The absence of compensating controls, such as an effective intrusion prevention service on firewalls, or effective endpoint security on servers, allowed WannaCry to spread through that first NHS trust, but also elsewhere via the N3 network, demonstrating the similarly weak controls in those organisations. Perhaps some NHS trusts believed N3 to be more secure than the internet, so chose not to employ the same controls to both their internet and N3 connections. However, N3 and its successor, HSCN, are explicitly 'untrusted' networks, with no assurance for confidentiality or integrity, so should have been treated with a similar level of caution to the internet.

Security Immaturity

The security controls mandated for NHS trusts and local authorities at the time of the WannaCry attack differed significantly. Table 1 maps the WannaCry root causes against the NHS (IGT) and local

WannaCry Attack: Root Causes	**Most relevant Information Governance Toolkit Control**	**Most relevant PSN CoCo Control**
Failure to patch promptly.	All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures.	Vulnerability management (patch management).
Failure to keep anti-virus software up to date.	Information assets with computer components are capable of the rapid detection, isolation and removal of malicious code and unauthorised mobile code.	Include services to identify malware at the gateway & implement an equivalent level of protection at the endpoint.
Failure to manage the risk from obsolete equipment that was 'unpatchable'.	A formal information security risk assessment and management programme for key information assets has been documented, implemented and reviewed.	Security Gaps: mitigating the associated risk with an alternate arrangement ... or mitigating action, such as disabling or reducing access.
Weak firewall/boundary controls for the internet and N3.	Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely.	You will ensure that your network has appropriately configured boundary protection.

Table 1: Wannacry root causes and policy controls in place at the time

government (PSN) controls in place at the time of the attack.

Overall, the PSN CoCo provides clearer control coverage (for example, the IGT is vague about 'appropriate organisational and technical measures', whereas the PSN has an explicit policy for vulnerability management, and the PSN provides an explicit policy control for obsolete equipment) for the WannaCry control failures and perhaps, more importantly, the controls were externally audited. The PSN CoCo required an annual IT health check, which is a vulnerability assessment report provided by an accredited provider, whereas NHS organisations were not subject to any such compliance testing at the time of the WannaCry attack.

Comparing the full PSN and IGT schemes reveals a stark difference in governance philosophy between GDS and NHS Digital. In March 2015, GDS turned away from the control-focused approach of previous PSN CoCo versions by creating an exception-driven scheme that was far simpler than both the IGT, and the DSPT that has since replaced it. However, NHS Digital's response was a downgrade of the equivalence it gave PSN-compliant organisations, like local authorities, against its own IGT controls.

This seemingly cautious approach may be explained by the higher incident reporting standard the NHS has been held to since April 2013: most NHS security incidents are referred to the UK data protection regulator, the Information Commissioner's Office. In contrast, there is no formal incident reporting mechanism within the PSN CoCo, though local authorities are encouraged to report incidents. However, NHS Digital's opinion on the quality of security management in local authorities went beyond the updated PSN CoCo. A September 2016 report by NHS Digital on NHS security incidents drew a comparison between the 8 incidents reported to the NHS between April 2015 and March 2016 by the 122 English local authorities, and the single incident reported by 10,168 pharmacies (NHS acute trusts reported 305 incidents). The authors doubted the accuracy of local government incident reporting while explaining the single pharmacy incident thus: "pharmacies have no reason to put data at risk". This open mistrust of local authorities, and by association presumably, the PSN CoCo, means that pre WannaCry, NHS Digital clearly considered their approach to information security superior.

A New Stable Door

It is telling that NHS Digital's post-WannaCry response was to turn to Cyber Essentials Plus (CE+), a generic information security certification available to any UK organisation, rather than directly audit organisations against its own, bespoke, IGT. CE+ includes the requirement for a vulnerability assessment provided by a third party of both internal and external IT infrastructure. The final nail in the IGT's coffin was that no NHS trust could achieve CE+ certification during the period covered by the NHS and public accounts committee reports into WannaCry. Ironically, it is likely the same NHS trusts would have also failed to achieve compliance against the 'downgraded' PSN CoCo.

Since WannaCry, NHS Digital has released its new Data Security & Protection Toolkit (DSPT), which unsurprisingly includes both explicit control coverage for the WannaCry root causes and the requirement to conduct an annual vulnerability assessment. In contrast, GDS made no changes to the PSN CoCo used by local authorities over the same period.

What Did We Learn?

The adage "If it's not tested, it doesn't work" perhaps best sums up why the NHS was so vulnerable to WannaCry. The lack of verification of the assertions N3-connected organisations were making in their Information Governance Toolkit submissions meant that the assurance NHS Digital, and the wider NHS, gained was illusory. Meanwhile, the PSN CoCo used by local government focused heavily on external auditing, in the form of the IT health check report. Such testing not only provides an independent assessment of an organisation's security posture but may also reveal vulnerabilities staff supporting the infrastructure are unaware of.

While WannaCry showed the compliance regime to be broken, given the structure of the NHS, individual trusts bear the ultimate responsibility for their information security. And there are likely to be few readers that believe organisations with multi-million-pound budgets should have to be told to patch software or manage the risk from obsolete systems, especially ones that are delivering critical care.

The lessons learned from the WannaCry attack are clear, but what of Franklin's ill-fated expedition? Landseer's painting was a commentary on Victorian man-versus-nature, not an authoritative account: later expeditions discovered evidence that the ships had become trapped in ice and the crews starved to death, with some resorting to cannibalism. So, a strong, if unfortunate, case for empirical root cause analysis. And back to the present, continuous monitor, testing and open-minded learning, give us the best chance of keeping the wreckage and maulings from future cyber-attacks metaphorical.

Biographies

Tony Leary is a Principal Architect at cloudThing Ltd, an award-winning company that creates, designs and automates new digital experiences on the cloud. Tony has over 20 years of IT security experience, gained across a wide range of public and private sector organisations, and has been CISSP certified since 2004. Tony was awarded an MSc in Information Security (with Distinction) from Royal Holloway, University of London in November 2019.

Geraint Price obtained his B.Sc. in Computer Science from Royal Holloway University of London in 1994 and his Ph.D. from University of Cambridge in 1999. His Ph.D. dissertation analysed the interaction between Computer Security and Fault Tolerance. Since then he has worked on various projects including Denial of Service attacks in networks and the future of Public Key Infrastructures, funded by academia and industry. Geraint is a Senior Lecturer in the Information Security Group, and has a strong interest in the practice of information security. He leads the ISG's external engagement activities with business and government. Geraint is a regular attendee, panellist and speaker at a number of industrial fora, including I-4 and the ISF.

Series editor: S.- L. Ng