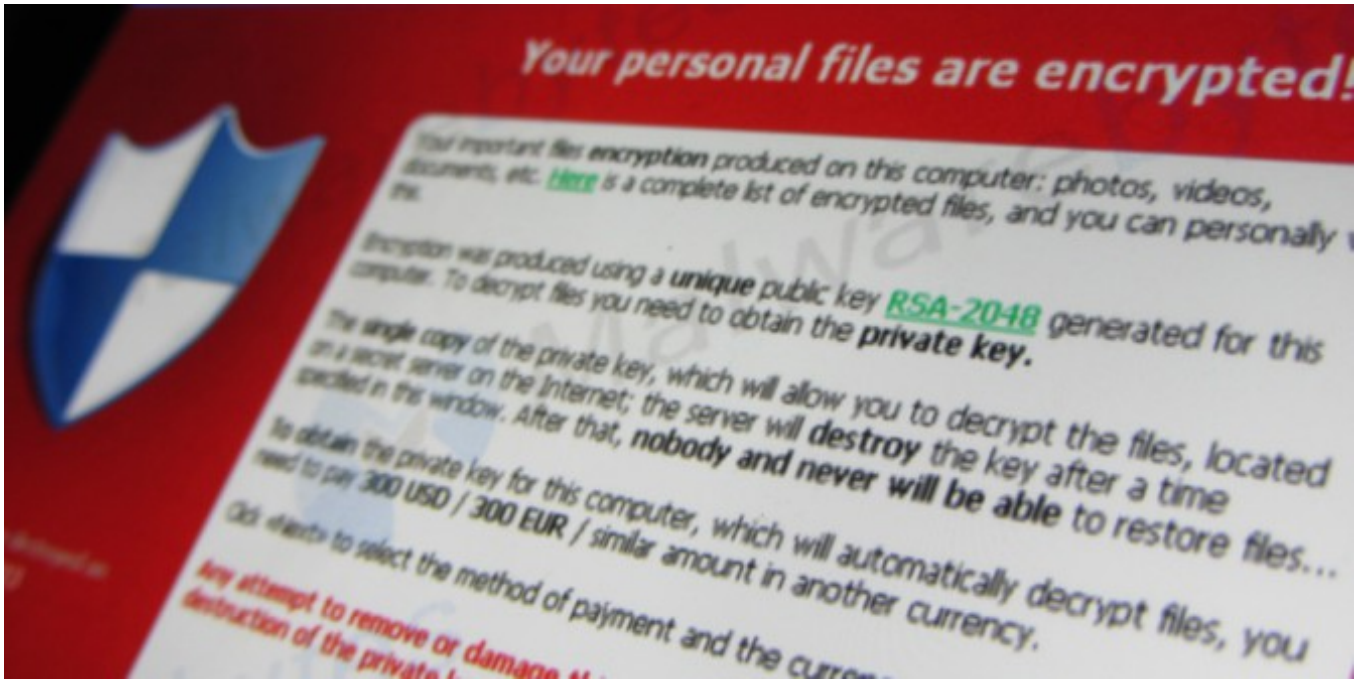
Surviving the global information security war

blogs.lse.ac.uk/businessreview/2017/05/18/surviving-the-global-information-security-war/

5/18/2017



Lessons from the fate of the NHS Trusts:

- **You will not survive a war on more than one front**

Over the past week many NHS Patients became collateral damage as the ten-year arms race between online predators and the vendors of information security products and services escalated into global warfare after a new ransomware variant produced by a supposedly North Korean team went viral. The ability of the Trusts to defend themselves had been sapped by their ongoing battles (dating back to the very formation of the NHS) over who runs anything: management (on behalf of the government of the day) or the various feuding tribes (alias professions) of clinicians (on behalf of "their" patients). It was not just responsibility for security that was unclear.

This has lessons for those running any organisation that wishes to survive the rising tide of online crime, whether targeted, as with the $100 million Bangladesh bank heist, or untargeted, as when four bitcoin accounts linked to Cryptolocker processed over $27 million inside three months from those whose systems had been held to ransom.

This was not the first time Barts NHS trust had been hit, and there will be questions as to why it went down while other major London Hospital Trusts did not, and why it remained shut down for so long. Most of the reasons so far given do not bear scrutiny. The supposed cuts were illusory, the damage was not confined to obsolete operating systems. It was also greatly exaggerated by faulty press cover. Had the Trusts which went down, as opposed to rapidly recovering from minor incidents, been businesses in a competitive market, they would by now be awaiting receivership or take-over by those which did not.

- **Data availability and integrity are more important than privacy**

Few patients die because their privacy has been breached. Several dozen may die because tests and treatment have not been carried over the past week. But that is many times less than die annually because errors in their records lead to erroneous dosage or mistreatment. Also it is not just criminal behaviour that brings systems down.

Both RBS and British Airways have had their ATMs and Booking Systems off air for days after closing down their in-house IT teams and moving the work to India to cut costs. Time lags in communication along sub-contracting chains led to minor problems escalating and clashing with overnight updating.

Meanwhile communications networks go off air because of power outages, cable breaks or bad weather with monotonous regularity. Reliance on cloud-based systems without multi-sourced communications and local back-up is hazardous. One of the lessons from the events of the weekend was the need for defence in depth. ***The top priority for any security policy is availability and resilience, not "just" privacy.*** If the incumbent (BT in the UK) is the main supplier, the other suppliers should not share single points of failure with them.

- **Robust data governance, including the use of encryption, is about authentication and integrity, not just privacy. Obsession with General Data Protection Regulation (GDPR) compliance is a menace.**

Last year I argued that Brexit should include a more effective partnership with the rest of Europe to unravel the global politics of privacy, security and choice. I quoted from Gordon Carera's book "Intercept" on how the order of importance of robust encryption was understood in the 1960s. The same order applies with regard to medicine and banking today.

1st Attribution – only the President can order a nuclear strike: you have to know it is him

You need to know who (or what) recorded the data so that you can decide on its reliability.

2nd Integrity – lest the text becomes corrupted and the missiles have the wrong target

Lest the text become corrupt and the patient gets the wrong medicine or the payment goes astray

3rd Non-repudiation – you cannot allow the President to say it was not him

You cannot allow the clinician or customer to say it was not them.

4th Infinity/Availability – however many times you run the system it must give the same result

Clinicians and customers must be able to trust the system.

5th Secrecy – to provide reasonable confidence it will not be read by those not authorised to do so, bearing in mind the ways of getting at the text before it has been coded and after it has been decoded

It must also be easier to do things securely than insecurely so as to remove the need to bypass security and/or give your keys to your colleagues or children – thus negating the 1st objective.

- **Security processes must be tested if they are to be trusted**

Last year the Culture Media and Sport Select Committee, in their report on cybersecurity, looked at issues from the perspective of the victims, including the main board directors who may be held liable. When I blogged on the report and its implications for business I said that my own elevator pitch to the board of any major organisation would be:

- have clear chains of responsibility for security processes, training, reporting and incident management and ensure they are practiced and updated at least annually;
- use staff and customer education programmes to reduce the damage when breaches occur and report the results to the board and outside world;
- report who audits your systems, to what standards, whether you have an incident management plan and when it was last exercised, to the board, your customers, your suppliers and the outside world;
- check the processes of current and potential subcontractors, because you will be held liable and may not be

able to get whoever sold your information jailed, especially if they are offshore.

- prepare for when losses from impersonation replace whiplash and payment protection insurance (PPI) as the target income stream of ambulance-chasing lawyers, so that you can rapidly sort the genuine claims from the rest.

Conclusion

What changed this week was the response of the government. The National Cyber Security Centre flexed its muscles – moving rapidly to issue and update guidance. There is talk of global cooperation to identify those responsible. There is also talk of class actions using civil law to help victims obtain redress from those who aided and abetted the attackers by design or by neglect (whether software providers, internet service providers, telecommunications companies, domain name registrars or local management).

These are likely to be far more effective than regulatory action in transforming attitudes among the Internet community towards their responsibilities for helping identify and "remove" online miscreants and predators. At this point you can see, however, why governments and regulators find it so difficult to act. Even most of the "less challenging" recommendations from the ground-breaking EURIM – IPPR study *Partnership Policing for the Information Society* remain unimplemented.

♣♣♣

Notes:

- *The post gives the views of its author, not the position of LSE Business Review or the London School of Economics.*
- *Featured image credit: Cryptolocker ransomware, by Christiaan Colen, under a CC-BY-SA-2.0 licence*
- *Before commenting, please read our* Comment Policy.

Philip Virgo was co-founder of PITCOM in 1981 and principal consultant in charge of technology assessment and national issues at the National Computing Centre until 1986 when his operations were spun out as Winsafe Ltd. He is on the advisory board of the Digital Policy Alliance and the executive of the Conservative Science and Technology Forum. His views are his own.