UNDER ATTACK!

Dan Jones *explains how new cyber resilience legislation aims to combat rising ransomware threats*

The UK government is planning to introduce new legislation next year to beef up the nation's cyber resilience. Details of the Cyber Security and Resilience Bill were revealed in the King's Speech during last summer and are designed to improve UK cyber defences and protect essential public services.

In its most recent update concerning the Bill's progress, the Government spelled out exactly why the new legislation was needed. "Our digital economy is increasingly being attacked by cyber criminals and state actors, affecting essential public services and infrastructure. In the last 18 months, our hospitals, universities, local authorities, democratic institutions and government departments have been targeted in cyber attacks," it said.

It went on: "Recent cyber attacks affecting the NHS and Ministry of Defence show the impacts can be severe. Our laws have not kept pace with technological change, so we need to take swift action to address vulnerabilities and protect our digital economy to deliver growth. The Bill will strengthen the UK's cyber defences and ensure critical infrastructure and the digital services companies rely on are secure."

While it touches on a number of issues, it also singled out what it described as a: "recent ransomware attack impacting London hospitals" and the importance of incident reporting "including where a company has been held to ransom". Even at this early stage in the legislative process, it's clear that the Government has its eye on the rise in ransomware attacks.

All too often, when these pernicious events happen, businesses or organisations tend to focus on the immediate damage of an attack. However, the disruption to operations can be far more catastrophic with ransomware jamming entire networks and bringing businesses and other organisations grinding to a halt.

For example, as a result of the ransomware attack affecting the NHS in England in June, more than 10,000 outpatient appointments and 1,693 elective procedures were postponed across King's College Hospital, and Guy's and St Thomas' Hospital.

Of course, the financial impact of such an event in terms of cancelled procedures and operations is extremely damaging to a health service already under strain. But the trauma and disruption caused to patients – who may have to wait months for a new appointment – is hard to imagine.

In truth, organisations often struggle to quantify the true impact of an attack – especially in the immediate aftermath of an incident. Some may downplay the true extent of the damage. There may even be those whose first reaction is denial. Similarly, there are those who are prone to exaggerate.

While such human responses are understandable, they cannot be allowed to shape the response to any attack.

Deeper analysis is essential if leaders are to fully grasp the impact of what's happened and put in place measures to mitigate further risk.

This means objective, forensic analysis to establish all the facts. It means getting to the bottom of how such a breach could happen, its causes and the response. And it means being open and honest regardless of how difficult such conversations might be.

But it's not simply a question of looking at the nuts and bolts of the attacks. Organisations need to think beyond the immediate threat and cost of a ransom demand. After all, there are other things to consider such as operational losses, the cost of restoring and protecting data, and the long-term erosion of customer trust.

In the case of the recent attack on London hospitals, the true cost of the event shouldn't be measured alone in terms of the financial cost, but also with regard to people's health and well-being. Even their lives.

The Government's decision to bolster legislation is to be welcomed, but it's people – not regulations – that form the first line of defence. A true cyber security strategy empowers employees to be vigilant and responsive in the face of threats.

That's why fostering a robust cyber security culture is imperative to staying ahead of evolving threats. The goal of any enterprise cyber security programme should be to manage incidents in a way that limits further damage, reduces recovery time and costs, and protects the organisation's reputation.

There's no one-size-fits-all approach to incident response. That's why regular 'tabletop exercises' are vital to build up familiarity with response processes and to ensure preparedness. Ultimately, though, organisations need to ask themselves whether they have complete confidence in their data. Why? Because regulation aside, it is real-time data visibility – paired with a strong security culture – that separates those who simply survive cyber incidents from those who are prepared to thrive in today's threat landscape ●

Last June, more than 10,000 outpatient appointments and 1,693 elective procedures were postponed as the result of a ransomware attack on the NHS in the UK

Dan Jones is Senior Security Advisor, EMEA, at Tanium.