# Ransomware: The internet's biggest security crisis is getting worse. We need a way out

zdnet.com/article/ransomware-the-internets-biggest-security-crisis-is-getting-worse-we-need-a-way-out

Steve Ranger

Organisations continue to fall victim to ransomware, and yet progress on tackling these attacks, which now constitute one of the biggest security problems on the internet, remains slow.

From small companies to councils, government agencies and big business, the number and range of organisations hit by ransomware is rising. One recent example; schools with 36,000 students have been hit, leaving pupils without access to email as attempts were made to get systems back online. That's at least four chains of schools attacked in the last month.

Ransomware gangs are getting craftier, and nastier, in their relentless pursuit of profit. It's not enough to break into computer systems and encrypt the data to render it useless. Now the crooks are stealing some of the data and threatening to reveal it. And it's not just data such as customer records: the cyber criminals will look for anything that might be sensitive or embarrassing on the network, and use the threat of publishing it as leverage against victims. And in many cases it seems to work.

So what can be done to stop these attacks? Organisations of all sizes need to understand the ransomware threat, and figure out how to improve their own security – even getting the basics right can go a long way towards deterring attacks. The software industry also needs to do a better job of building secure software. Is this going to happen? That's unlikely, as there's just too much pressure to ship software fast and generate profit. The multiple ways companies can customise and integrate software also means that even if it ships as perfectly secure, security holes will emerge as soon as it's used in the real world. Worse, ransomware groups are adept at seizing on newly discovered flaws and utilising them as part of their attacks, with the ransom money providing funds to sustain longer and more complicated attacks. In the longer term, the general shift to cloud computing, which has so far proved more secure, might help.

Tackling the perpetrators themselves is the next challenge, although here geography plays a big role. Many of these groups are located in Russia, which means that law enforcement has found it hard to pursue cases. It may be possible to disrupt the efforts of these groups in other ways: police have had some success in disrupting botnets and other online crime rings, so perhaps something similar is possible here, even if this disruption tends to be only temporary. Here again, there's little chance of improvement in the short to medium term, unless there's a significant thawing of international relations.

## To pay or not to pay?

One of the trickiest decisions concerns ransom payment. It's understandable that a company may feel it has no choice but to pay up to regain access to its data, given that the alternative is to go out of business. But every ransom paid rewards the cyber criminals and sends a signal to others that there's profit to be made.

Making it illegal for companies to pay ransoms seems like a very big step to take. But this is increasingly being mentioned. A recent report from defence think tank RUSI (Royal United Services Institute) notes that "policymakers should carefully examine the feasibility and suitability of making ransom payment illegal in the UK, which could lead in turn to a 'protective' effect resulting from the discouragement of ransomware attacks against UK targets."

It's a decision that could have some painful consequences.

News of the change would take a while to filter through, so if any country were to ban ransom payment there would, at the very least, be a short to medium term situation where companies were still getting hit with ransomware.

Ransomware gangs are opportunists and may not realise that a company is based in the UK, and may encrypt the systems anyway. They're unlikely to hand over the decryption key just because the victim can't pay up.

If companies can't pay ransoms and don't have any other way to restore their data, they will face huge costs and disruption – potentially enough to put them out of business. Even organisations with backups and the required technical know-how will be forced to spend time and money restoring their systems. That could put them at a significant disadvantage compared to ransomware victims based elsewhere.

Ransomware gangs are certainly capable of avoiding certain territories when planning attacks (they tend to avoid Russia for example), so, in the longer term, a ban on paying ransoms may have the desired impact by making UK organisations less profitable targets. Still, there's no sign that the government is currently planning on going down this route.

But as the cost of ransomware attacks continues to rise, we need to find a way to counter them – and soon.