
# HELD TO RANSOM

*Fighting the ransomware pandemic: what to do if you suffer a ransomware attack and how to prevent it*

**Ransomware remains one of the top cyber risks for businesses across a range of sectors. With several high-profile companies, such as the UK arm of Salvation Army and Ireland's Health Service Executive, falling victim to ransomware attacks in 2021, it's clear that no one is safe.**

"The end of last year was somewhat of a reckoning for ransomware," says Fabien Rech, VP EMEA at Trellix. "Though some gangs had previously been driven offline, as a result of a co-ordinated international effort, the use of ransomware proliferated. Our recent threat research found that financial services was the sector most targeted by malicious actors during the third quarter of 2021. However, we're unfortunately reaching a point with ransomware attacks where no organisation is safe, regardless of industry."

"The ransomware threat has never been more prevalent or more dangerous," says Pritesh Parekh, VP of Engineering and Chief Trust & Security Officer at Delphix. "In fact, data from our recent research report revealed that 91 percent of organisations have been attacked by at least one ransomware variant. With our rapidly evolving threat landscape, it's a matter of when – not if – an organisation will fall victim. As such, a strong recovery plan is essential."

"The recent cyber attack on The Works is yet another example of how severely cyber attacks can impact business operations. The reality is that all companies operating in today's landscape simply cannot afford to be offline. If they are, they risk not only financial loss, but also long-term reputational damage. In the worst cases, some companies never fully manage to recover," says Gary Cox, Director of Technology Western Europe at Infoblox.

**Maintaining proper IT hygiene is the single best thing you can do to combat even some of the more advanced tactics**

"Our data shows that unfortunately only one in ten (11 percent) businesses feel confident that they could recover from a ransomware attack in two days or less. This is proving costly, with most executives estimating that downtime for business-critical applications costs their companies between $10-million and $200-million per day. By still relying on outdated and ineffective solutions and methods, many are putting their mission-critical data at risk," explains Parekh.

In response to the increasing threat that ransomware poses to the country, the UK government has been forced into action in an effort to bolster the country's cyber security capabilities.

"In fact, in the last 12 months alone, the government has introduced both the UK Cyber Security Council and the new National Cyber Strategy. These measures are promising, but much more still needs to be done. Alongside the government mandated measures, it's down to both public and private sector organisations to protect themselves from ransomware attacks," says Rech.

Gone are the days of lone hackers operating from their bedrooms. As cybercrime has become increasingly organised in its nature, the threat that it poses has also grown significantly.

"Cyber crime is a business. They're not interested in your data, or slowing down your business. They just want your money. And so the professional advice is never ever to pay a ransom. Firstly, and fairly obviously, is that you're dealing with criminals. There is absolutely no guarantee that you will get your information back or systems unlocked. None. In fact, paying up puts you on the 'more likely to pay' list, opening up possibilities for second and third extortion attacks. Also, just because they've given your data back doesn't mean that they won't keep a copy or sell it on. Remember, this is all about them maximising the money they make, not about you or your business" explains Ramses Gallego, International Chief Technology Officer, CyberRes, a Micro Focus line of business.

Cox agrees and adds: "While it's tempting to pay up and move on, the harsh reality is that the majority of organisations that pay a ransom will be hit again. Paying a ransom also does not guarantee a return to normalcy. Once they've infiltrated a system, threat actors will often leave behind a hidden surprise for organisations – such as a Trojan horse – in order to continue blackmailing and profiting from their victims. And even if they don't leave code behind, the victim will be added to a list of known 'payers', meaning the likelihood of repeated attacks increases."

"Paying the ransom effectively funds future attacks," explains Gallego further. "The average ransom has risen from roughly $500 to $1,300 simply because people are paying up, the supply is there. But they need your money – that supply – to keep operating, just like any other business needs a regular stream of income. Linked to this, is that your payment qualifies their business model. Think of yourself as a prospect among the thousands of other targets. Even if just 1 percent of targets convert, the business is viable."

As attacks become ever more sophisticated, organisations need to focus on a dynamic strategy. One that is continually evaluated and updated to keep pace with changing methods of cyberattack.

"Just like with any other type of attack, when it comes to ransomware, prevention is always better than a cure," says Cox. "More often than not, attacks are successful when victims do not have an effective strategy in place. Therefore, businesses need to expect ransomware attacks and prepare accordingly. Getting detection and prevention right can give businesses the upper hand."

"Maintaining proper IT hygiene is the single best thing you can do, and can combat even some of the more advanced tactics," says Gallego. "Make sure robust processes for monitoring, control, visibility and escalation are in place. Your disaster recovery backups may also help – provided you can guarantee they are secure and uninfected themselves. If so this can really help mitigate system downtime and improve overall resilience in the face of various shocks, be they ransomware or otherwise."

> **THE PROFESSIONAL ADVICE IS TO NEVER EVER PAY A RANSOM – YOU ARE DEALING WITH CRIMINALS**

"In order to best protect their organisations, CISOs need to re-evaluate their priorities to ensure that the appropriate training measures and technologies are successfully implemented. For example, enterprises need a threat system that can evolve with the constantly changing threat landscape. This is where the idea of 'living security' comes in," explains Rech.

"A living security platform gets smarter and faster as the threats develop and eliminates any blind spots that may leave organisations vulnerable. This enables businesses and CISOs to focus on their priorities at hand and not concern themselves with whether the organisation is protected from end to end. By embedding this approach, organisations will be equipped to increase cyber resilience and ensure they're able to defend against attacks, both now and in the future."

There are several methods that organisations can use to bolster their cybersecurity and increase their protection. Some of which they may already use. For example, Domain Name System (DNS), which companies use for IT networking, can be utilised for cybersecurity as well.

"When applied to security, DNS can help protect against ransomware attacks by supercharging a company's phishing protection as well as detecting and blocking communication with known C&C servers. It can help stop an attack before it even starts since more than 90 percent of malware touches DNS to enter and leave a network. To take it to the next level, businesses can merge DNS with DHCP (Dynamic Host Configuration Protocol) and IPAM (IP Address Management) – all foundational technologies used for networking. Known as DDI, this combination provides visibility into network activities, and paired with DNS security, can identify compromised machines and correlate disparate

events related to the same device. This data is a goldmine of information to IT teams as they go about their job of defending the business," explains Cox.

At the same time, relying on existing systems is not always sufficient. "The reality for today's businesses is that their legacy backup solutions are simply not equipped to deal with modern ransomware attacks. The time to change this is now. IT execs must align preparation, knowledge and response to improve their organisation's ability to deal with ransomware. They should look for a complement to their existing backup solution that will provide more robust capabilities. Features like data masking – which protects data in a test and development environment – alongside the ability to recover in an isolated recovery environment are key for those looking to mitigate the effects of a ransomware attack and fight the cybercriminals head on," says Parekh.

**MOST ESTIMATES SHOW DOWNTIME COSTS BETWEEN $10 AND $200-MILLION PER DAY**

"It's no secret that the cybersecurity industry is more difficult to navigate than ever before. Continuous data breaches and ransomware attacks impacting commercial entities and governmental agencies prove that network-centric approaches no longer work," says Jim Hietala, Vice President, Business Development and Security at The Open Group.

"The dilemma in today's approach to cybersecurity is that it is no longer feasible, or even possible, to consider all elements of the service topology as 'trusted'. With the rise in supply chain attacks, for example, Zero Trust has become a critical concept, as research shows that in 66 percent of supply chain attacks, suppliers weren't aware or failed to report how they were compromised."

"The Zero Trust model offers a model which secures the data and assets which networks are there to carry," explains Hietala. "It is a critical concept, because it brings security to the users, data/information, applications, APIs, devices, networks, cloud, *etc.* wherever they are – instead of forcing them onto a 'secure' network. Rather than assuming that any device on a network must have passed a security checkpoint and is therefore trustworthy, Zero Trust assumes that every action is potentially malicious and performs security on an ongoing, case-by-case basis."

"In order to successfully implement this, the industry needs to establish standards and best practices for Zero Trust as the overarching information security approach for the Digital Age, and create models which are data and asset-centric, as opposed to traditional network-centric approaches," concludes Hietala.

At the end of the day, cybersecurity should be all about adaptability. Organisations that are aware of what is going on and change in light of that will be the ones that succeed ●

**The introduction of the UK Cyber Security Council and the new National Cyber Strategy are promising, but much more still needs to be done**