‘Make ransomware payments illegal’ say 78% of consumers

New study from Talion reveals 79% of security professionals also want ransomware pay outs to become illegal

London, UK – June 24th, 2021 – A new study into ransomware from managed security service provider, Talion, has revealed that 78 percent of consumers and 79 percent of cyber security professionals believe ransomware payments to cybercriminals should become illegal.

The study is announced to support the launch of a new cyber security movement founded by Talion and backed by the Research Institute for Sociotechnical Cyber Security (RISCS) called #RansomAware, which encourages organisations to speak up about ransomware attacks.

Today, the world is seeing businesses of all sizes suffer devastating attacks from ransomware. In the last few months massive attacks on Colonial Pipeline and JBS have disrupted services and earned cyber criminals millions of pounds. These attacks have been well-publicised, and the CEOs have been openly talking about the incidents – boldly going where few have gone before. Until recently most ransomware attacks have been kept out of the spotlight with businesses opting to pay the ransom to restore services, without letting their customers know.

Ciaran Martin, Professor at Blavatnik School of Government and former CEO of the National Cyber Security Centre, knows first-hand just how damaging ransomware is to UK businesses, “I welcome initiatives like this. We need to look at all the different reasons why ransomware is causing so much harm. That includes tackling the tough questions like the flows of money, including looking seriously at payment bans. But we need to provide more support for victims too, and help them protect themselves in the first place.”

Talion’s study also highlighted that 81 percent of security professionals believe sharing information between businesses who have been attacked is the key to building better defences against ransomware.

#RansomAware supports this mindset shift and has been set up to encourage organisations to openly talk about the attacks they have suffered, so we can pool intelligence and collaborate to make defences more effective. “We believe we need to stop cyber shaming organisations and move away from a culture of blaming individuals to a place where we can be open and transparent about how these attacks are taking place. Cybercriminals collaborate on their attacks, so we must collaborate to make our defences stronger. It is ‘us’ against ‘them’,” said Michael Brown, CEO at Talion.

As part of the campaign, Talion is forming a coalition of cyber security experts, businesses, academia, and government to promote collaboration and information sharing. The coalition is formed of 16 founding members, including Talion, BAE Systems, RISCS, 36 Commercial, Insight Enterprises, Inc., KnowBe4, UK Cyber Security Association, Comparitech, Siemplify, Eskenzi PR, IT Security Guru, Outpost24, Cydea, Devo Technology Mishcon de Reya and Decipher Cyber.

“We see examples of collaboration and intelligence sharing in other industries, the medical sector for example has a formal process whereby when a medical mistake is made, the information is shared across the community to educate others and avoid the mistake being repeated. We need to band together with peers in our industries to look at ways of taking a collective response against ransomware attacks. Imagine if every law firm, university, or utilities provider stood together and publicly stated, we will not pay ransoms. Cyber criminals will follow the money, what we need to do

is cut them off at the source, said Madeline Carr, Director of RISCS & Professor of Global Politics & Cyber Security at UCL.

Additional findings from Talion's study on consumers and cybersecurity professionals also revealed that when consumers were asked how they would want their employer to respond to a ransomware attack affecting their personal data, 37 percent said refuse to pay. When UK consumers were asked how the government should respond if nation-state cybercriminals launch an attack on the UK's fuel services, 46 percent said try to restore systems manually but suffer a longer shortage of fuel. Worryingly, other responses to the same question revealed that 14 percent said, 'respond with a nuclear or physical military attack', a figure that grew to 43 percent among 18 – 24-year-olds.

ENDS

Additional quotes from #RansomAware coalition members

Robin Oldham, Founder & CEO of cyber consultancy Cydea:

"Ransomware is inflicting debilitating attacks on critical infrastructure and posing a threat to national security, it's for this reason that, the response cannot be left to private companies alone. We need to encourage information sharing and we need governments to develop policy to support this fight: let's learn from public health and begin collecting and analysing data much like we have done for Coronavirus throughout the global pandemic. Then we can formulate a holistic response that tackles the root causes of cybercrime and protects and promotes digital business."

Gunter Ollmann, Chief Security Officer at Devo Technology:

"The battle against ransomware isn't so much a fight against gangs of misguided teens peddling a particularly malicious flavour of malware - it's the battle against a global ecosystem of tens of thousands of suppliers, distributors, enforcers, and money launderers managed by organized-crime cartels and nation-states."

Adrian Nish, Head of Cyber at BAE Systems Applied Intelligence:

"Since early 2020, we have monitored the blogs of criminal actors running ransom and extortion campaigns. We currently track 30 such blogs and have identified over 2,300 victims to date. Ransomware has escalated at an alarming rate in the past 18 months, and shows no signs of going away soon. This has resulted in a >$250 million a year enterprise for a small set of criminal actors. There is much to be done to tackle this, from enforcing greater regulations around cryptocurrency to improving defences and encouraging victims to not negotiate with these actors."

Stu Sjouwerman, Founder and CEO of KnowBe4:

"Unfortunately, there isn't a quick fix to combat ransomware; and while back-ups are good, they are not enough – especially with the extortion techniques now being used by cybercriminals. As ransomware evolves, security practices must keep pace. Raising awareness within organisations is crucial in the fight against ransomware, especially when it comes to phishing and ensuring staff can identify and report these attacks. RansomAware is a worthy campaign that will help spread awareness of ransomware issues and give affected or worried organisations a great platform to get help as well as share information about ransomware and work towards making it less successful."

36 Commercial:

"In the absence of a developed legal framework, public and private sector institutions are facing great difficulties in making decisions about how to respond to ransomware demands that have far-reaching consequences. At 36 Commercial, we recognise that reducing and combatting the ransomware threat will require global cooperation due to the decentralised nature of cryptocurrency, the sophisticated nature of the criminal networks involved in view of the fragmented and outdated legal and regulatory regimes around the world. We are committed to forming a coalition of cyber security experts, businesses, academia, and government to promote collaboration and information sharing so as to build an integrated legal framework together."

Yvonne Eskenzi, founder and director of Eskenzi PR:

"*Today we are seeing an increase in ransomware attacks targeting industries and businesses of all sizes. Many of these organisations have no idea how to respond to attacks or the action they need to take in terms of remediation and communication to stakeholders and customers. Providing organisations with a platform to share intelligence is a great step forward. As has been proved time and time again, preparation is the single most important defence against ransomware. The organisations that have their response and crisis communications clearly defined before they are hit will come out the strongest, minimising financial losses and brand damage."*

Bob Diachenko, security researcher at Comparitech:

"Often, companies ignore the basic cyber hygiene principals and think that ransomware gangs operate mostly as nation-state actors to target big, critical infrastructure organisations. This is not the reality as there are a huge variety of ransomware actors that simply scan for exposed databases, which they take advantage of and hit with a ransom demand hoping the organisation will be caught off guard enough to pay. It's why Comparitech has created a tool to help companies of all sizes to gain a clearer picture of ransomware incidents across the globe and highlight the importance of good cyber hygiene."

Notes to editors:

This study was commissioned by Talion and carried out by One Poll in June 2021 and examined the attitudes of 1000 UK employed adults and 200 UK IT security professionals.

Visit https://talion.net/ransomaware to learn more about the #RansomAware movement.

About Talion

At Talion, we're changing the way organisations interact with their Managed Security Service Provider. Born out of BAE Systems, our service is built on first-hand knowledge of military engineering and defence-grade security, together with an in-depth understanding of the threat landscape facing the commercial world today.

When it comes to cyber security, we believe every organisation deserves full visibility and complete control over how threats are monitored, how decisions are made, and how their business is protected. That's why we prioritise transparency and collaboration across our service lines, implementing

security programs that give businesses the control and freedom to pursue ambitions and realise goals, safe in the knowledge that we've got their back, 24 hours a day, 7 days a week.