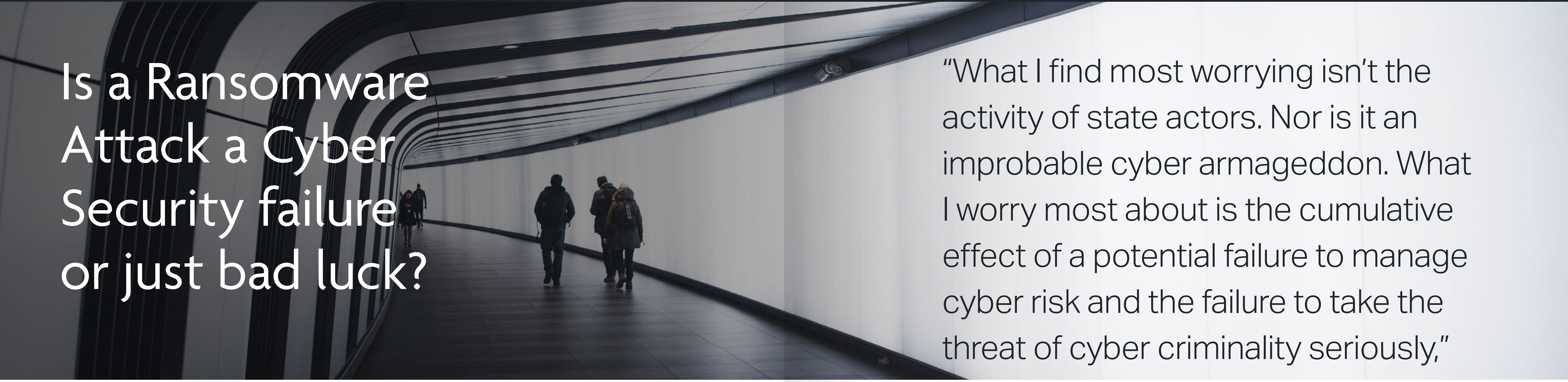
TALION

Ransomware Perceptions Report, 2021

#RansomAware

Share your story



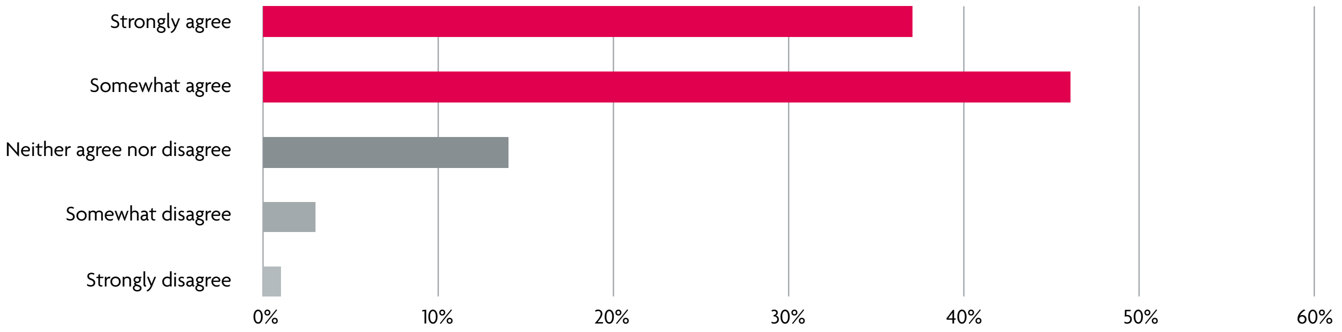
Is a Ransomware Attack a Cyber Security failure or just bad luck?

A recent study, commissioned by Talion and carried out by One Poll in June 2021, surveyed the attitude of 1000 UK employed adults and 200 UK IT security professionals.

From the research it emerges that the vast majority, 83% of respondents, consider being hit with ransomware a cyber security failure

Ransomware is currently the most dangerous and insidious cyber security threat facing the country, according to National Cyber Security Centre's (NCSC) CEO, Lindy Cameron.

It is a cybersecurity failing when an organisation is infected with ransomware

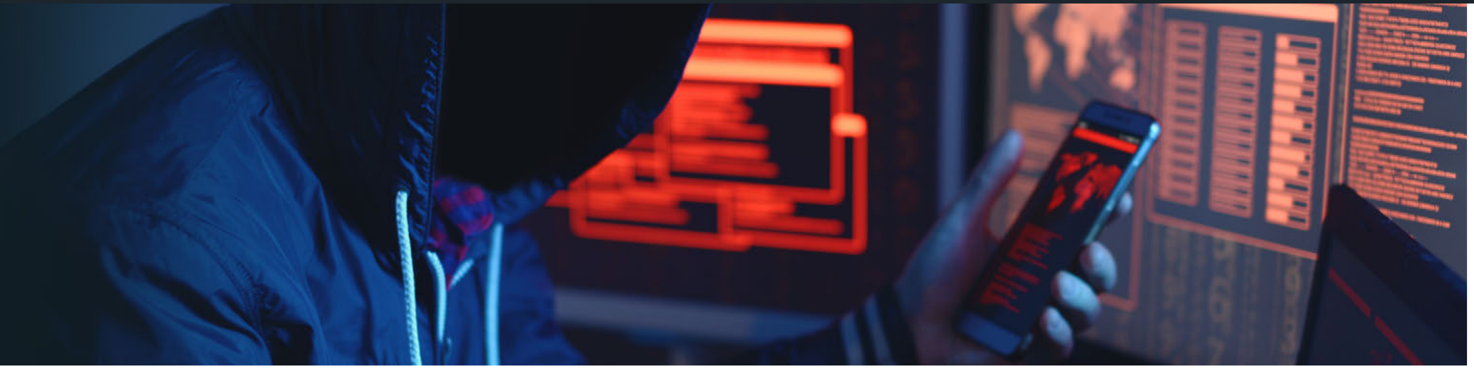


> "What I find most worrying isn't the activity of state actors. Nor is it an improbable cyber armageddon. What I worry most about is the cumulative effect of a potential failure to manage cyber risk and the failure to take the threat of cyber criminality seriously,"

Cameron told a virtual audience at the Royal United Services Institute (RUSI) think tank's annual security lecture on 14th June 2021.

> "For the vast majority of UK citizens and businesses, and indeed for the vast majority of critical national infrastructure providers and government service providers, the primary threat is not state actors but cyber criminals, and in particular the threat of ransomware."

Computerweekly.com

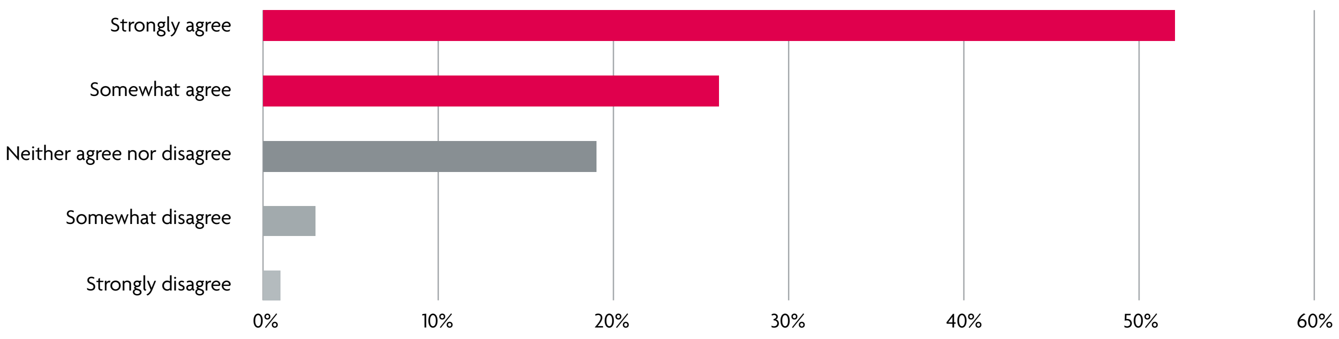


The research also shows that 78 percent of consumers and 79 percent of cyber security professionals believe ransomware payments to cybercriminals should become illegal. Paying a ransom does not guarantee the return of data or regaining control of systems, rather it will help cybercriminals get more funding to conduct further attacks.

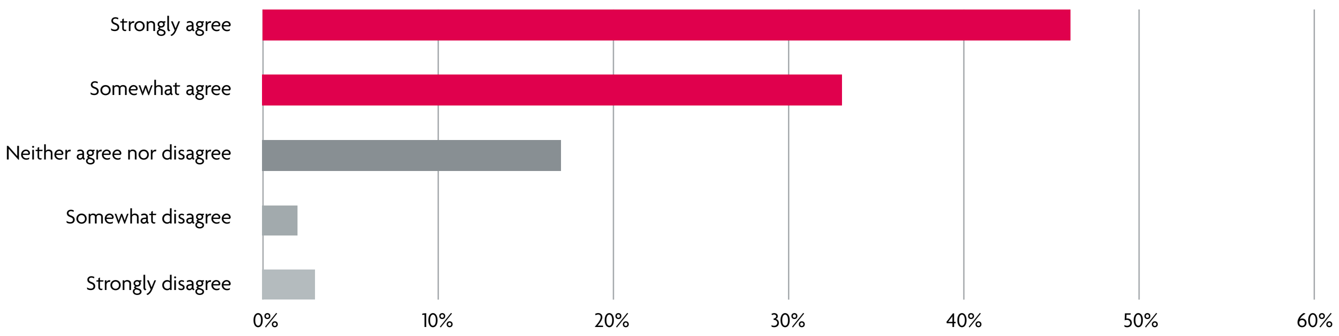
This is also documented by The State of Ransomware 2021 report from Sophos, based on responses from 5,400 IT managers in mid-sized organisations in 30 countries, revealing that an alarming 92% of organisations that paid a ransom did not get all their data back. On average, organisations that paid a ransom recovered only 65% of their data that had been stolen and encrypted by hackers.

Ransomware payments to cybercriminals should be made illegal

Consumers

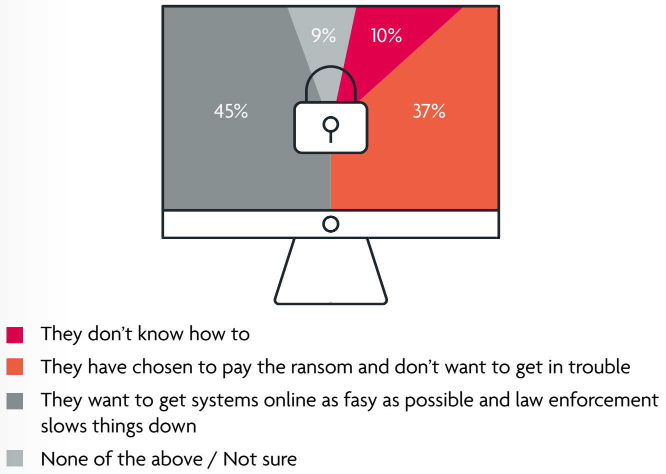


IT Security Professionals



Looking further at the responses, we can observe that organisations appear to be unsure of how to respond to a ransomware attack or what the right thing to do is. Almost half of respondents (45%) believe that law enforcement will impede getting systems back online quickly, while 37% believe they might also get in trouble for reporting payment being made to attackers.

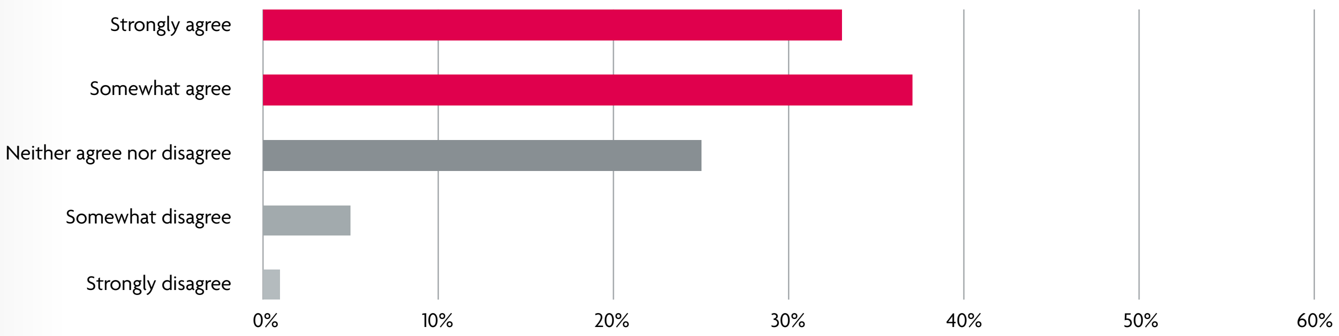
What do you think is the main reason that some companies don't report ransomware to law enforcement?



This highlights the true need of a response at government level, starting with a framework that informs businesses on how best to respond to a ransomware attack, operationally and legally. NCSC has recently announced the creation of a Ransomware Task Force with the aim to develop a robust plan to tackle the global ransomware threat, through deterring and disrupting the actors while helping ensure organisations are equipped to prepare and respond. The disruption ransomware is now causing means that this is no longer a cyber security issue for organisations; as the Task Force's report notes, it has become a national security risk that has the potential to impact public safety, particularly when hospitals and other critical national infrastructure are targeted.

There is also much debate on the impact cyber insurance is having in the ransomware market place. While some argue it encourages better cyber security practices, 70% of cyber security professionals believe that insurance payments to companies that have paid a ransom demand only exacerbate the problem and cause more attacks.

Insurance payments can worsen the problem



Spotlight on 2020 Threat actors from our Threat Intelligence team

Our Threat Intelligence Team observed gangs upping intimidation techniques, with companies being threatened over the phone if they refused to pay the ransom.

The notorious Maze operators established the first ever large-scale ransomware cartel, Operators of Ryuk reportedly reached a staggering $150 million worth of Bitcoin repayments from their attacks. Ransomware-as-a-service (RaaS) expanded its offerings, with never-before-seen products dedicated to phishing and espionage operations and if that does not panic you enough, we witnessed the first death and homicide case opened after a ransomware attack on a German hospital shut down lifesaving equipment.

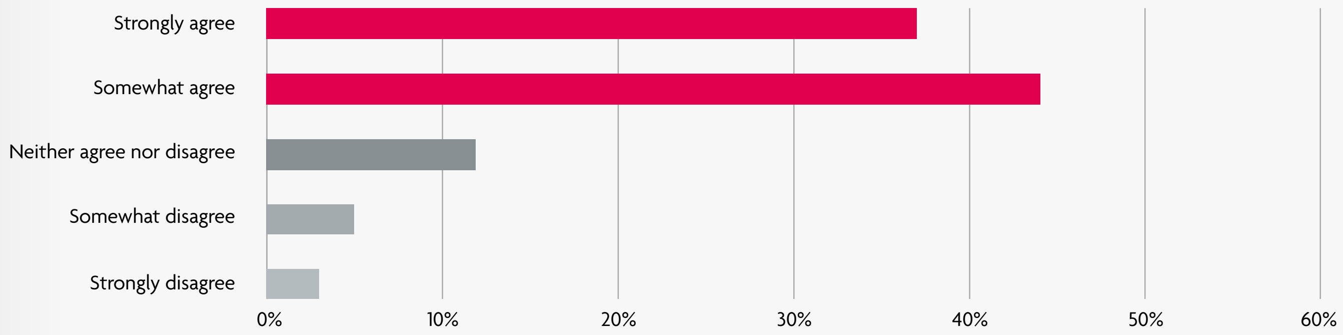
The healthcare sector, already facing a colossal strain from the fight against COVID-19, became a leading target for attackers. Some thieves made the ethical choice and promised not to shut down emergency services, while others made no such promise, notably the operators of Ryuk. Reports from the healthcare sectors saw that half of the attacks launched against them in 2020, were linked to ransomware which unfortunately in most instances could have easily been avoided if patching had been prioritised.

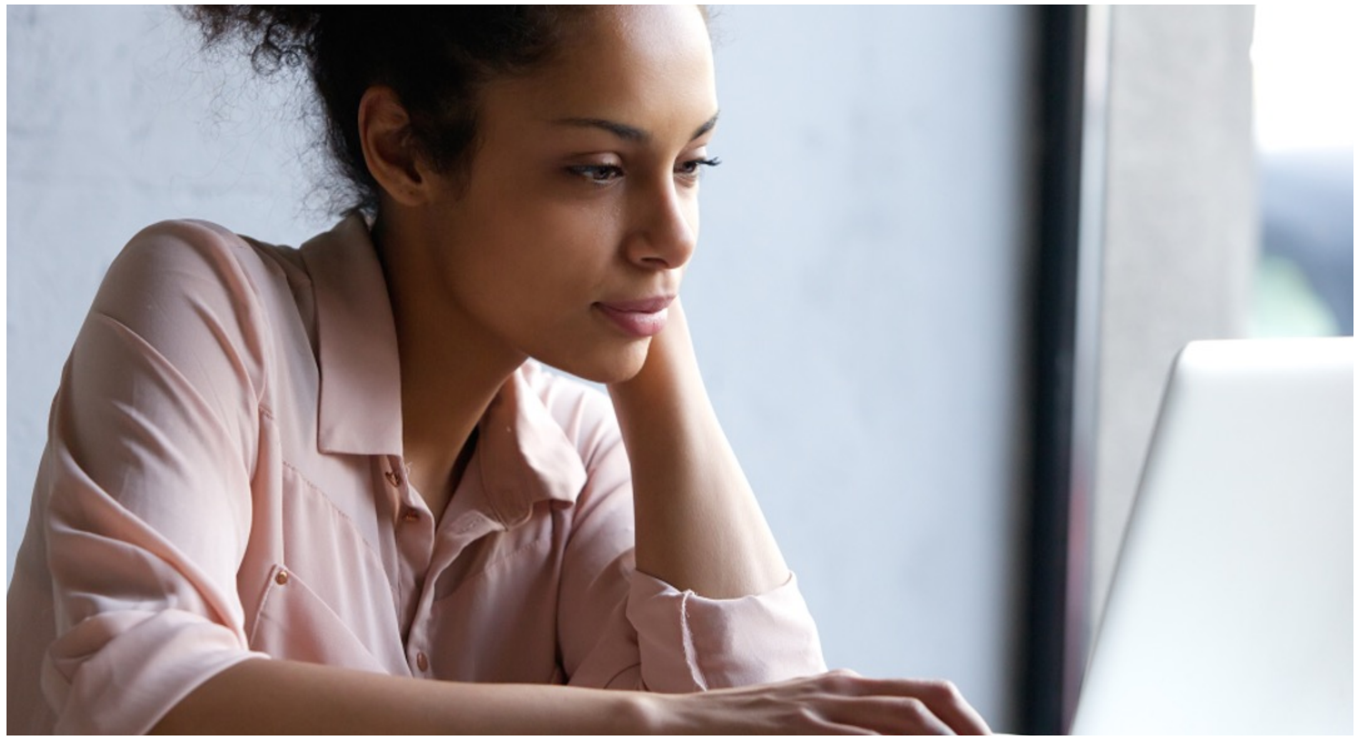
Weaknesses identified in the higher education sectors infrastructure – due largely to its move to remote learning – saw the sector face more attacks than ever before, with state actors desperate to retrieve any information they could related to COVID-19 and the production of a vaccine. The National Cyber Security Centre (NCSC) issued a warning for higher education in the UK to be put on high alert, specifically against ransomware attacks. While sectors such as technology, who have traditionally received a large portion of these attacks, continued to do so, we also observed previously unaffected sectors, receive a huge surge in ransomware attacks reiterating the unselective and boundless nature this tooling now carries when infecting organisations.

Of what we did witnessed in 2020; Ryuk, Sodinokibi and (prior to its retirement) Maze accounted for the top 35% of attacks. Regarding infiltration methods, researchers found that nearly half (47%) of attacks seen last year, took advantage of employees working from home and utilised remote desktop protocol (RDP). Further, 26% of instances were traced back to phishing emails, while 17% made use of known vulnerabilities, the remaining 10% were attributed to account takeovers. Half of these attacks adopted an approach we have only recently seen become extremely popular; exfiltrating and publicising stolen data, regardless of a ransom being paid, with operators able to make large profits via hacker forums and other parties interested in this sensitive information.

Another important question posed to our survey population, revealed the importance of acting as one. Over 80% of IT Security professionals agree that sharing information between businesses is key to build better defences against ransomware attacks. At Talion, we strongly believe in this too. We have recently founded a coalition of members to tackle this problem, by sharing experiences, exchange ideas and pool intelligence.

Sharing information between businesses who have been attacked is the key to building better defences against ransomware

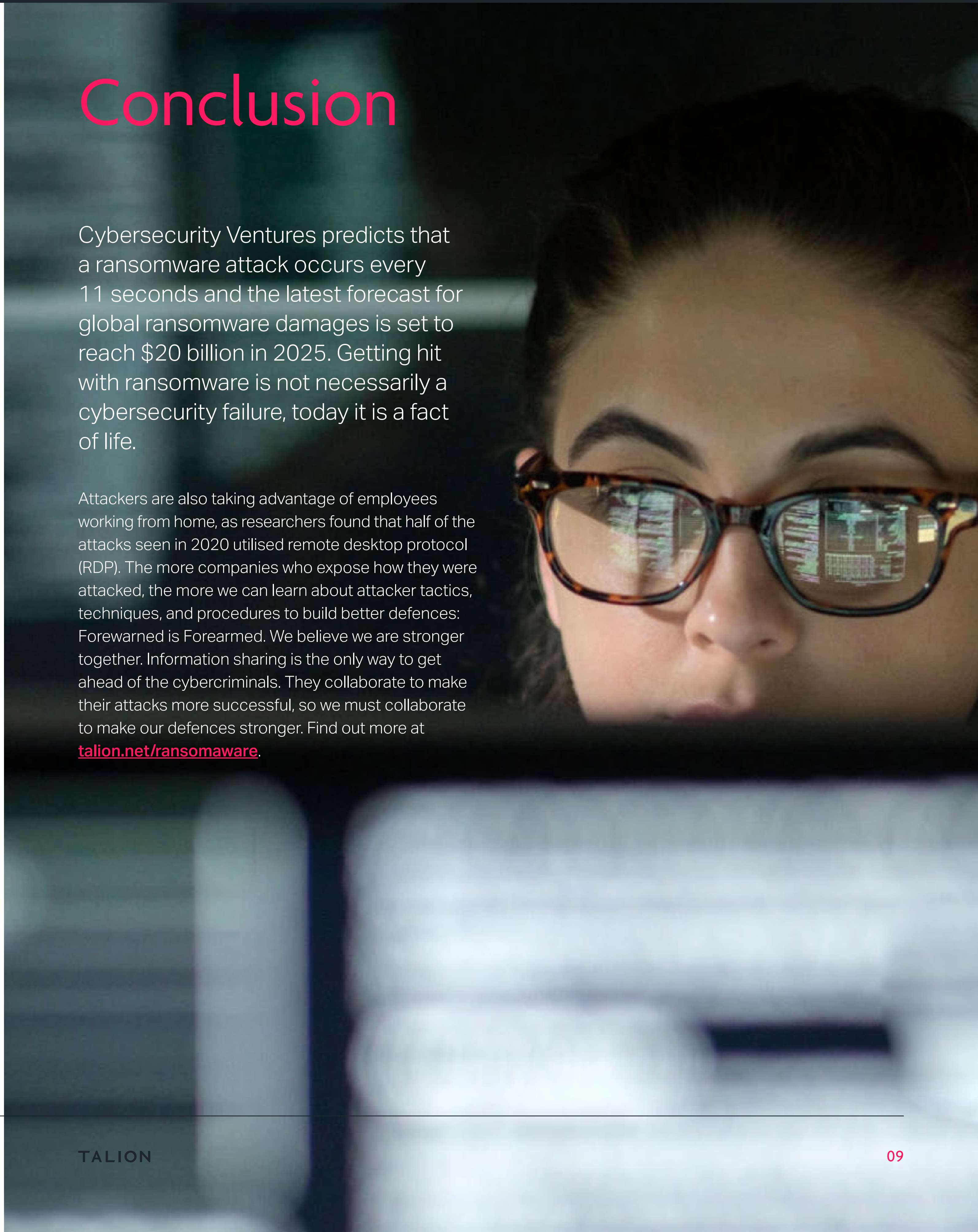




Top recommendations to prevent ransomware attacks

There are also ways that help reduce the risk of falling victim to a ransomware attack. Among the top tactics we advise to:

- **Prioritise Remote Working Security** – Organisations can begin with some very simple steps, such as utilising strong passwords & two-factor authentication across your network, also that your organisation is using the latest versions of operating system and software by ensuring patching is implemented promptly.
- **Invest in User education** – Implement regular training educating employees on how to recognise social engineering techniques and expose your users to planned phishing email tests.
- **Prioritise patching** – As mentioned above, patching will improve remote working security and the potential for attackers to utilise known exploits to infiltrate your system.
- **Update passwords regularly** – To avoid attackers performing an employee account take over to access your network, ensure you enforce users to regularly update their password on your system, highlighting the importance of your employees not reusing or duplicating personal passwords on your system.
- **Keep up to date with the latest techniques** – tactics and procedures being utilised by attackers. At Talion we monitor and alert threats to our clients as they emerge, advocating effective, timely procedures to defend their estate.



Conclusion

Cybersecurity Ventures predicts that a ransomware attack occurs every 11 seconds and the latest forecast for global ransomware damages is set to reach $20 billion in 2025. Getting hit with ransomware is not necessarily a cybersecurity failure, today it is a fact of life.

Attackers are also taking advantage of employees working from home, as researchers found that half of the attacks seen in 2020 utilised remote desktop protocol (RDP). The more companies who expose how they were attacked, the more we can learn about attacker tactics, techniques, and procedures to build better defences: Forewarned is Forearmed. We believe we are stronger together. Information sharing is the only way to get ahead of the cybercriminals. They collaborate to make their attacks more successful, so we must collaborate to make our defences stronger. Find out more at talion.net/ransomaware.

TALION

TALION.NET

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.

Speak to one of our experts today

hello@talion.net
+44 (0) 800 048 5775

HQ

The Hub, Fowler Avenue
Farnborough GU14 7JF

Security Operations Centre

Marshall's Mill
Marshall Street
Leeds LS11 9YJ

Engineering Centre

Unit 32-01, Level 32
The Vertical Corporate Office
Tower B , Avenue 10
Bangsar South, No 8
Jalan Kerinchi, 59200
Kuala Lumpur, Malaysia

Security solutions
you can see