Cybercrime insurance is making the ransomware problem worse

November 14 2022, by Subhajit Basu

Many businesses simply choose to pay a ransom than suffer the consequences of a cyber attack. Credit: Zephyr_p/Shutterstock

Cybercrime insurance is making the ransomware problem worse During the COVID-19 pandemic, there was another outbreak in cyberspace: a digital epidemic driven by ransomware.

Several organisations worldwide fell victim to cyber-extortionists who stole data either to sell to other criminals or held it as a ransom for a profit. The sheer number of attacks indicates that cyber security and anti-ransomware defences did not work or have limited effectiveness.

Businesses are turning to cyberinsurance companies in desperation to protect themselves from attack. But the growth of the cyberinsurance market is only encouraging criminals to target companies that have extortion insurance.

A 2021 study from the University of Leeds found there was a massive acceleration in major cyber-attacks on organisations during the pandemic. The paper also showed a "shift in offender tactics which scale up levels of fear in victims … such tactics include a shift towards naming and shaming victims, the theft of commercially sensitive data and attacks targeting organisations which provide services to other organisations."

A report by global cybersecurity firm Sophos found that 66% of organisations surveyed, from across 31 countries, were hit with ransomware in 2021, up from 37% in 2020. The average ransom paid increased nearly fivefold to US$812,360 (£706,854). Insurance companies often opt to pay the ransoms that cybercriminals demand—82% of UK companies pay up.

Where are the attacks coming from

According to US think tank the Council on Foreign Relations 22 countries are suspected of sponsoring cyberattacks, including the United States.

And a new black market in which cybercriminals provide products and services to other cybercriminals is flourishing and driving the surge in

ransomware attacks. So-called ransomware allows everyone from teenagers to skilled amateurs to professional criminals to rent malware, encryption tools, and even Bitcoin wallets.

It is like a criminal renting a gun from another criminal who manufactured it.

In July 2020, three teenagers hacked Twitter. The attack resulted in the hijacking of 130 accounts—some of which included high-profile targets including Joe Biden, Barack Obama, Apple, Elon Musk and Bill Gates. The bitcoin accounts associated with their ransomware scam received more than 400 transfers totalling over US$100,000 (£87,000).

What's the problem with insurance?

The past few years have seen a surge in specialist cybercrime insurance policies. The global cybercrime insurance market is predicted to grow from US$7 billion in gross written premiums (GWP) in 2020 to US$20.6 billion by 2025.

Insurers need to do more to discourage incompetent security practices. Car drivers must pass theory and practical driving tests. But cyberinsurance policies rarely audit the IT security of an organisation before the policy is finalised.

A standardised ISO norm (quality management standards internationally agreed by experts) for software did not exist until 2015. It means customers have no way of judging the security standards of anything produced before 2015. Even now, some of the risk assessments a software would go through in its lifetime could be less rigorous than for the kettle in our home. And ISO testing is voluntary.

The market lacks understanding of large-scale, sophisticated, cyber-

attacks. The insurance sector works by determining the probability of an incident happening and the impact it would have. The cyberinsurance market struggles to forecast the likelihood of cyber-attacks because changes in digital technology can be so unpredictable. Attackers' capabilities and intentions shift rapidly.

Most insurers currently have no long-term data for cyberincidents or ransomware. This has led to underfunded cyberinsurance programs, which rely heavily on optimistic financial models.

As a result it is getting more difficult to secure cyberinsurance as the growing number of claims is forcing valuers to be more discerning in the clients they accept. Lloyds of London released new rules in December 2021 stating that underwriters will no longer cover damage caused by "war or a cyberoperation that is carried out in the course of the war".

Insurance premiums increased by 22% in 2020 and a further 32% in 2021 across 38 countries. The cost incurred by the business gets passed on to customers. The ransomware demand will contribute to the overall rise in living costs as ransomware costs are being passed on to the customers.

As part of my work with the Northern Cloud Crime Centre, I looked at the effectiveness of laws in the UK to regulate criminal activity in the Cloud. I found the cybercrime legislation in the UK has failed to keep pace with technological and market developments over the past 30 years. The Computer Misuse Act 1990 needs updating to make it more effective at policing cybercrime. If we cannot fix the situation, it will threaten jobs and investment in the UK.

What is the solution

Ransomware attacks are so effective because they exploit human

weaknesses and organisations' lack of technological defences.

Law enforcement authorities advise ransomware victims not to pay the ransom because it encourages further attacks and fuels a vicious cycle.

But prevention is the best solution. Organisations need to put more effort into developing security measures such as a multifactor authentication system. Managers also need to carry out penetration testing, where a cybersecurity expert searches for vulnerabilities in a computer system.

Businesses are legally obliged to have a fire plan in place. The time has come for mandatory ransomware and phishing resilience testing. The insurance industry needs to set minimum security requirements as part of the risk assessment. Organisations need greater transparency regarding what security they do and do not have in place.

Consensus is growing among researchers that solid cybersecurity can't be achieved with technology alone because a human errors are to blame for a huge amount of incidents. The UK government is proposing new laws to regulate cybersecurity standards. But these laws won't work if it doesn't invest in public education about phishing threats.

Cybercrime insurance can help minimise business disruption, provide financial protection, and even help with legal and regulatory actions after a cyberincident. But it will not solve the problems that created the vulnerability to an attack in the first place.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation

Citation: Cybercrime insurance is making the ransomware problem worse (2022, November 14) retrieved 28 January 2023 from https://techxplore.com/news/2022-11-cybercrime-ransomware-problem-worse.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.