KOVRR
Cyber Risk Modeling

www.kovrr.com

Leveraging CRQ to understand the growing costs of ransomware attacks

DECEMBER 2021

KOVRR
Cyber Risk Modeling

Today decision makers at the world's largest enterprises, from the CISO to the CEO, are increasingly recognising cyber risk as a threat to the profitability or even the solvency of their business.

Ensuring that the business has prioritised their budgetary resources, sought appropriate insurance cover, analysed their capital reserve requirements and initiated a governance regime to monitor this dynamic risk have become ever more critical.

However, without a consistent and continuous CRQ (Cyber Risk Quantification) to financially quantify cyber risk, it is challenging to understand and respond to the changing nature of cyber risk that analyses a full spectrum of potential cyber loss scenarios.

The manner in which ransomware costs are evolving is one example of this.

Ransomware Trends: Increasing Volume and Costs.

Every day the media reports of more companies falling victim to ransomware attacks. In fact, it's estimated that by the end of 2021 one business is expected to suffer a ransomware attack every 11 seconds.

And these attacks are proving increasingly costly.

A recent report by Palo Alto Networks reported a sharp 82% increase from last year and indicated that the average cost of each ransomware payment in 2021 to be $570,000.

This is while another report by Coveware claims that 50% of data leak victims pay the ransom.

In addition, the average downtime caused by a ransomware attack is 22 days of business interruption.

However, other payments were notably higher.

In 2020 travel company CWT Global paid $4.5 million in Bitcoin to the Ragnar Locker ransomware gang and this year there was the high profile case which saw Colonial Pipeline give into ransomware demands of $4.4 million.

The resulting increase in both frequency and severity of these ransomware incidents has also negatively impacted cyber insurers, which have seen costs from attacks go up by a factor of 10 and has put some carriers into loss making territory.

Naturally, these trends make it even more critical for businesses to come to terms with as the cyber insurance premiums are rising sharply and the coverages available to them are being slashed; In some cases, major insurers are excluding ransomware payments, pushing businesses to reassess capital reserve levels and risk management strategies.

© 2021 Kovrr All Rights Reserved

Ransomware's Evolution:
How One Event Can Cause many types of Financial Loss

CISO's, Chief Risk Officers and the Boards report they are grappling with an even more concerning phenomenon: Ransomware attacks where losses transcend the extortion payment and cause a wide range of other potential financial impacts that include those stemming from data theft, business interruption, regulatory fines and others.

By only factoring the ransom payment part of the equation, and failing to quantify and account for all of the additional potential financial losses, could lead to an unbalanced and incomplete assessment of a company's potential financial exposure.

Below are two examples that illustrate how this could happen.

Case Study One: Kaseya

On July 2nd, a cyber attack was launched against the IT solutions company Kaseya.

Kaseya provides IT solutions including VSA, a unified remote-monitoring and management tool for handling networks and endpoints. In addition, the company provides compliance systems, service desks, and a professional services automation platform to over 40,000 organizations worldwide.

The cyberattack has been attributed to the REvil/Sodinikibi ransomware group whose ransomware was first detected in April 2019. The group's usual propagation method is phishing emails containing malicious links. Some of the group's most prominent victim industries in the last two years were healthcare facilities and local governments.

REvil has offered a decryption key, allegedly universal, that is capable of unlocking all encrypted systems for the 'bargain' price of $70 million via bitcoin (BTC) cryptocurrency.

On July 13th, all of REvil's online activity stopped and the groups data-dump websites were shut down without further information, leaving the victims of their latest attacks hostage with encrypted files and no valid payment address or decryption keys.

Who was impacted?

On July 2nd, Kaseya claimed that the attack affected only a small number of on-premise clients. But in a press release published on July 5th, the company estimated that the number of clients impacted by the attack was between 800 and 1500 businesses.

Such an event could lead to financial losses from the following costs:

- Extortion Fee
- Data Recovery costs
- Business Interruption and loss of profit

© 2021 Kovrr All Rights Reserved

Case Study Two: Apex Laboratories

In a data breach notification published December 31st, 2021, the company announced that, on July 25, 2020, it discovered a cyber attack that resulted in systems being encrypted and therefore inaccessible.

Apex said it was able to secure its network, restore affected data, and resume operations on July 27, and claims that its investigation into the incident did not reveal evidence of unauthorized access or acquisition of patient information.

"However, on December 15, 2020, Apex learned that the hackers posted information on their blog about the attack and listed data taken that contained personal and health information for some patients," the company revealed.

While looking into the attackers' claims, Apex discovered that the data might have been stolen from its systems between July 21 and July 25, 2020.

The medical services provider says that, for some of its patients, stolen data includes names, dates of birth, phone numbers, Social Security numbers, and test results.

Such an event could lead to financial losses from the following costs:

- Extortion and Recovery fees
- Business Interruption (Inc. Loss of income)
- Regulatory Fines
- Liability
- Data theft
- Legal expenses

The Importance of Focusing on the Impact

Kovrr's approach is built upon using multiple streams of data to always deliver the most up-to-date view of risk exposure to our clients that they can access on demand. The continuous stream of global cyber threat intelligence data that we incorporate helps us better understand the frequency of attacks and develop a rich understanding of the technological footprint of the business.

In addition, we have built a fact-based approach to calculating the severity of a loss that utilizes multiple sources of loss data which includes cyber insurance claims data, tracking the financial impact of global cyber incidents, regulatory filings, and many more. The combination of data enables us to simulate the possible financial impact of hundreds of thousands of tailored cyber loss events.

By focusing on the impact, one recognizes that whilst a cyber event may be triggered in a variety of ways, the key to managing cyber risk is to understand its overall impact on an organization.

This is especially true given that one event will often lead to multiple types of impact. For example, a Ransomware attack leads to the ransom demand or data encryption that causes a network interruption which disrupts the businesses operations and results in lost income.

© 2021 Kovrr All Rights Reserved

There are several advantages of looking at events with a focus on impact. For example whilst there are multiple different event types (E.g. Phishing attack, DDOS, Accidental Cloud Misconfiguration etc) they notably all end in one of a few distinct kinds of impact:

- Data Confidentiality and Availability
- Network Interruption
- Ransom Demands

Each impact has an associated cost connected to them. For example, network interruption caused by the exploitation of vulnerability can cause business interruptions that can involve loss of income, forensic investigation costs, and require PR campaigns.

Kovrr's approach uses data regarding the vulnerabilities and exposures exploited in the attacks, and the tools and techniques employed for these exploits, which enables a better and more granular classification of events.

The combination of exploit and payload data enables us to understand the attack impact, such as a ransomware payload having a different effect than a data wiper payload. Additionally, the exploitation techniques enable Kovrr to classify the possible attack targets.

The end result is a financially quantified output that can model multiple types of losses, including the ability to help understand the evolving loss dynamics that a threat like ransomware can lead to - beyond the payment itself.

Using Financially Quantified Cyber Risk Insights to Mitigate and Manage Financial Business Exposure

Understanding and accounting for all potential financial impacts, and their likelihood of occurring, is crucial for companies looking to implement robust cyber risk governance controls and business continuity plans.

> To find out more about how Kovrr's know- how financially quantifying the cyber risk exposure for the world's largest insurance carriers and global multi-billion dollar enterprises can help you make more data-driven capital allocation, risk transfer and cyber risk management decisions click the link **here** and schedule a demo with the team.

© 2021 Kovrr All Rights Reserved

KOVRR
Cyber Risk Modeling

The Author

Tom Boltman

VP Strategic Initiatives

About Kovrr

Kovrr's cyber risk modeling platform delivers global (re)insurers and enterprises transparent data-driven insights into their cyber risk exposures. The Kovrr platform is designed to help chief risk officers, chief information security officers, underwriters, exposure managers, risk professionals and catastrophe modelers understand, financially quantify and manage cyber risk by utilizing AI-powered risk models.
To learn more please contact the Kovrr team: contact@kovrr.com

© 2021 Kovrr All Rights Reserved