REDUCING CYBER INSURANCE CLAIM EXPENSES

BLUE TEAM ALPHA™

Authors:

Mathew Quammen, Head of Channels and Alliances, Blue Team Alpha

Peter Martinson, Director of Incident Response, Blue Team Alpha,

INTRODUCTION

Claim expenses are creating difficulties in the cyber insurance market. As loss ratios are exceeding 60-75% and rising, carriers need to find ways to control claim expenses. From 2020 to 2021, the cost to recover from a ransomware attack increased 228%[1]. Even though the cyber insurance market is anticipated to grow 21% annually through 2025[2], insurance carriers need to reduce loss ratios to maintain a stable cyber insurance market.

High claim costs in cyber insurance are primarily caused by extortion demands, losses due to business operations disruptions, and DFIR (Digital Forensics and Incident Response) expenses. Combined, these costs exceed millions in payouts by cyber insurance carriers based on the current model of incident response during a ransomware claim.

It is possible to reduce the total claim expense by prioritizing business operations during incident response before, or while, negotiating extortion demands for decryption keys.

This paper will review the current model of incident response for ransomware cases and explore a new model that has reduced the total cost of extortion demands by millions of dollars and the overall cost of cyber insurance claims[3].

1. Rials, William. "Top Cybersecurity Trends for 2021 and Beyond." Homeland Security Affairs: Pracademic Affairs 1, Article 3 (May 2021). www.hsaj.org/articles17153
2. According to Statista Research Department
3. According to Blue Team Alpha Incident Response Customer Data

CURRENT RESONSE MODEL FOR CYBER ATTACK CLAIMS

"COSTS AN AVERAGE OF $500,000 - $2,000,000 PER INCIDENT"

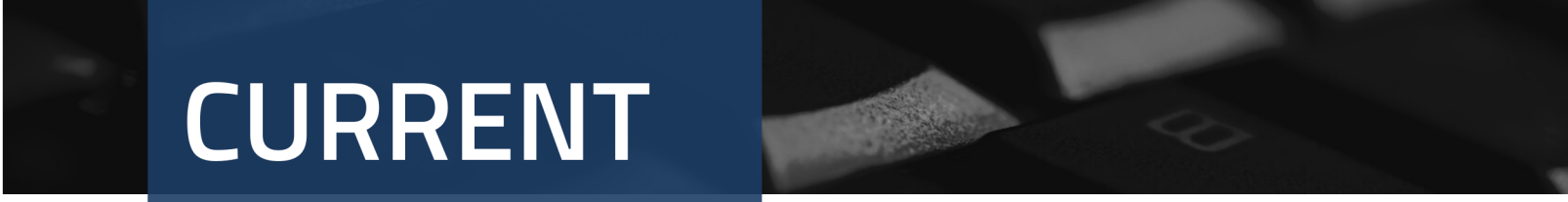
The current industry standard response model for cyber insurance carriers costs an average of $500 thousand to $2 million per incident, not including the cost of extortion demands, which has increased 83% from 2020 to 2021[4].

The rise in cost can be attributed to:

- Increasing extortion demands from threat actors
- Duration of insured business operation disruption
- Third party damages and regulatory fines

By moving quickly to restore business operations, better outcomes are driven to both reduce business interruptions losses and to reduce extortion demands. This excess expense can be rectified efficiently by implementing process changes during a ransomware attack response.

4. According to Infosecurity Magazine



CURRENT RESPONSE MODEL

The current response model can be broken down into six phases:

1. Insured contacts claims department
2. DFIR firm assigned
3. DFIR firm negotiates and facilitates payment for decryption keys
4. Forensic investigation results in lengthy down time for victim
5. Decryption keys used; service is restored, attacker is likely not eradicated
6. Claim expenses continue to increase

In this model, once the insured has notified the insurance carrier regarding a cyber breach, the insurance carrier contacts a law firm who then contacts an incident response firm. All too often, incident response firms look to extortion payments as a FIRST step, not as a final option. This model drives unnecessary extortion payments and very excessive claim costs.

PAYING THE EXTORTION DEMAND:
WHAT IT DOES DO AND WHAT IT DOES NOT DO

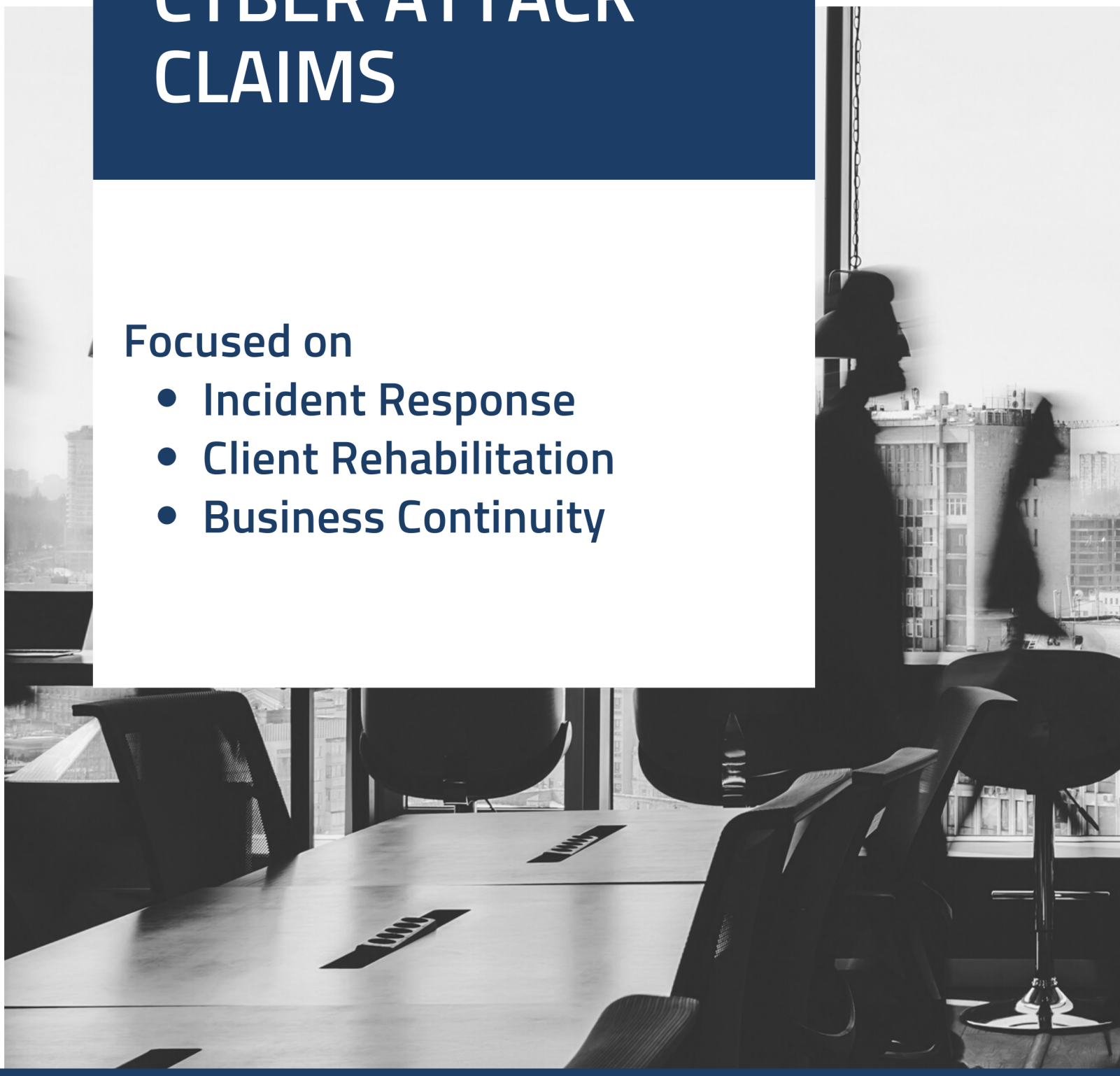
PAYING THE EXTORTION DEMAND:

1. Provides decryption key(s)
2. Grants insured access to environment
3. Complies with threat actor to stop active extortion and/or data disclosure

PAYING THE EXTORTION DEMAND DOES NOT:

1. Guarantee that the decryption key will work as expected, or at all
2. Ensure the threat actor is out of the environment
3. Guarantee that the threat actor will stop active extortion or data disclosure
4. Restore lost data
5. Prevent a future attack
6. Repair reputational damage

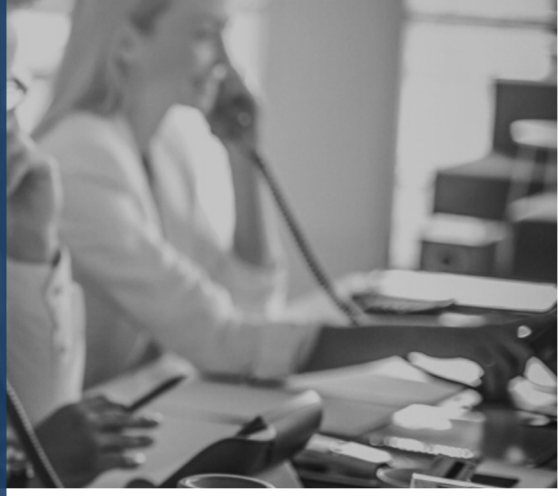
PROPOSED MODEL FOR CYBER ATTACK CLAIMS



Focused on

- Incident Response
- Client Rehabilitation
- Business Continuity

The proposed model is four phases, with key steps happening simultaneously.



1. Insured contacts claims department
2. DFIR firm assigned
3. Forensic data is collected for analysis

   Threat actor removed; client restored to critical operations

   Forensic analysis finalized & complete service restoration
4. Post incident debrief

The proposed model shifts the focus of the DFIR from paying the extortion demand to incident response and client recovery.

DIFFERENTIATORS BETWEEN CYBER ATTACK RESPONSE MODELS

EXPERTISE OF DFIR TEAM

SPEED OF BUSINESS OPERATION RESTORATION

FORENSICS AND RECOVERY TIMING

Ransom Payment & Timing of Business Operation Restoration

The goals of the DFIR team should be to collect forensic evidence, expel the threat actor from the insured's environment, while rehabilitating the insured's business operations via service restoration and recovery. It's important to note that forensic evidence needs to be collected before any individual component is recovered, but more damage to the business (and claim expense) will likely be done if recovery is put "on hold" until the investigation is completed. Paying the ransom should be the last possible resort of any DFIR team.

Ransom Payment & Timing of Business Operation Restoration

Once an Incident Response team is deployed, they are on the clock. The insured's business is at risk and the losses from business interruption start to pile up. Initial steps in response can make a significant difference in the insured's recovery and reduction of cyber claim cost.

By prioritizing the recovery of business-critical operations, a well executed incident response is able to extradite the threat actor from the insured's environment without paying the extortion demand and return the insured to normal business operations 80% faster on average. Once this has occurred, the threat actor has significantly less leverage to demand extortion payments. This produces a better recovery for the insured and a much lower claim expense.

When choosing incident response organizations to work with, look for organizations that:

- Execute forensics, active threat hunting, and critical business service recovery simultaneously
- Prioritize recovery of the insured as a first step to minimize both claim expense and the impact to the insured
- Pay ransom only as a last resort
- Have experience negotiating to lower the extortion demand (only if it must be paid) and identifying compromised data
- Provide business acumen and expertise in prioritizing and restoring the business's critical services
- Provide a roadmap for next steps to continue to secure and strengthen the company

Avoid organizations that:

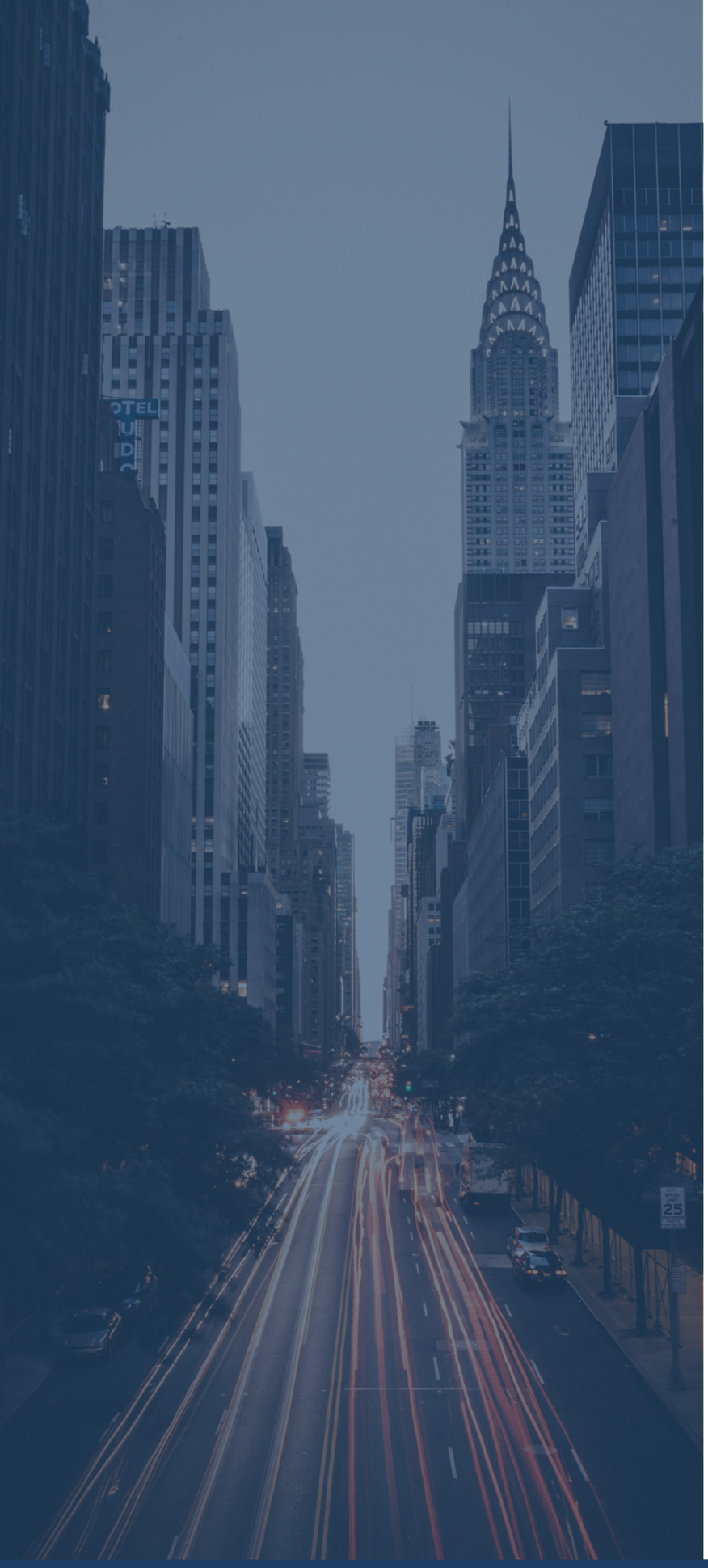
- Look to pay extortion demands as their first step to recovery
- Complete forensic investigation before beginning business service restoration
- Do not remediate vulnerabilities that caused the incident
- Perform forensics only
- Do not plan next steps

FORENSICS AND RECOVERY TIMING

Adding forensics to the recovery phase enables businesses to return to normal operations an average of 18 days faster than the average recovery time of 21 days in a ransomware attack. Integration of forensic analysis and recovery can greatly reduce downtime and claim expenses due to lost revenue and fixed operational costs. Although full recovery from the attack will take additional time, the insured's critical business operations should be prioritized.

POST INCIDENT DEBRIEF

Removing the threat actor from the environment and remediating vulnerabilities does not eliminate the chances of the insured being attacked again; most cyber attack victims are attacked again within 6 months of the initial attack. Once the insured is back to operational and the attack has been remediated, a post-incident debrief with the client helps to outline the details of what happened and lessons to apply in an attempt to prevent fast follow attacks.



CONCLUSION

Reprioritizing the insured's business operations provides significant advantages to both the insured and the insurance carrier while reducing or eliminating the returns to threat actors. The insured benefits from a quicker return to normal business operations, less reputational damage, and a reduced chance of another attack. Insurance carriers benefit from less business interruption losses and both fewer and drastically reduced extortion payment costs. With this different approach to ransomware events, carriers can greatly reduce claim expenses to stabilize the cyber insurance market while removing the incentive for cyber criminals.

BLUE TEAM ALPHA

Contact us at info@blueteamalpha.com