JS|HELD

PERSPECTIVES

Critical Issues in Cyber Incident Response: What Happens After a Ransom Payment is Made

Our perspectives feature the viewpoints of our subject matter experts on current topics and emerging trends.

INTRODUCTION

Ransomware trends – specifically related to frequency, cost, and payout – should no longer surprise us. We depend on technology more and more, integrating it into every aspect of our lives. As for data management, there is simply more to handle. We continually create it.

Furthermore, payments continue to be made[1] – with 65%[2] to 95%[3] of victims paying to get data back – while supply chain attacks, double extortion, and ransomware-as-a-service tactics are still causing disruptions.[4] The confluence of these issues results in ransomware attacks continuing to be profitable for threat actors.

But what happens ***after*** a payment is made? What technical tasks remain open? Who determines the cost impact on the business?

These are important questions, requiring attention and care to close the loop on outstanding tasks caused by ransomware disruptions. In this article, we will be examining the technical and business impacts of a ransomware attack and what steps should be performed after ransom payments have been made. We will explore the common errors most organizations make post-payment and what gaps in protection and processes they may need to fill once such an attack and payment has occurred. This information is meant to aid risk managers, insurance professionals, legal counsel, and corporate executives when faced with this issue. While this discussion details the steps to take following a ransom payment, additional articles in this series will focus on how to prevent a ransomware attack.

TECHNICAL POST-PAYMENT REVIEW

After a ransom payment has been made, whether working within your organization or with outside incident response firms, the victim organization should be mindful of the following items.

Avoid complacency and validate remediation actions

With payment out the door and systems hopefully back to an operational state, it is easy to fall into the complacency trap and say, “we got past that one” and move on. This is a potentially fatal future position. The threat actor got in somehow. If that vulnerability is not remediated, the same (or different) actor could re-exploit that same opening. Invest the time and effort to figure out what happened, so it does not happen again. Otherwise, your actions may fall into the “penny wise, pound foolish” category.

Be mindful of scheduled tasks running in the system and on devices

While this issue should be on the minds of responders prior to payment, failing to disable some scheduled tasks could impact the root cause analysis. For example, if systems are configured to automatically dump files, conversations, or other types of data, key artifacts may be wiped out, impacting investigatory and remediation efforts.

Verify that the system is free and clear of compromise before re-launch

It seems obvious, but sometimes “the obvious” does get missed. Truth is, until you investigate the root cause, you may not know how long the threat actor, or malware, was lurking inside your environment. It is not unheard of to deploy backups and suffer reinfection from a tainted backup. Therefore, you must have a solid backup and restore strategy that is regularly tested.

Issues to consider include:

- Backup storage location
- Backup functionality testing
- Number of available backup copies
- Atrophy
- Types of media (e.g., hard disk, flash memory, tape drives, etc.)
- And of course, accessibility. A backup is no good to you if it is inaccessible.

[1] https://www.wired.com/story/ransomware-attacks-rise-2023/
[2] https://www.varonis.com/blog/ransomware-statistics
[3] https://www.gartner.com/en/articles/when-it-comes-to-ransomware-should-your-company-pay
[4] https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts

Close out tasks with incident response firms and external support

Open tasks and tickets with external partners can easily fall through the cracks. Ticketing and tracking systems may not be uniform and in the heat of battle, recommendations and remediation steps may not be as formalized or centralized. For example, tasks may be mentioned in emails, chat threads, or even verbally. Conduct a final reality check with your partners to ensure all suggested remediation steps and checks have been completed and then document the close-out within your internal processes or in an after-action report.

BUSINESS IMPACT POST-PAYMENT REVIEW

Paying a ransom is just a fraction of the costs an organization will incur after a cyber incident, whether you suffered a partial or complete shutdown of the business operations or the loss of any data.

Having a plan in place prior to an incident is crucial and will help a company respond to a cyber incident quickly to restore operations in an efficient manner.

Talking to the right people

Who should be involved within your organization when it comes to identifying key employees to discuss the financial impacts of the business? That will depend on the organizational structure. The key is to identify the person(s) who understands the intricacies of the revenue streams, associated expenses as well as what impacts the cyber incident had on the business financials. A business may need to consider hiring an independent forensic accountant to assist in determining the financial impacts.

Ensuring you have correct information ready to share with your insurance company

If company management determines they have a business interruption / extra expense claim, they will need documentation to support their claim. It is important to have proper back-ups of your historical financial information as it may have been compromised or lost as a result of the cyber event. One cannot rely on the encryption key from the cybercriminal to gain access to their data, as the data may have been corrupted. You should create a comprehensive plan to protect any data that may be needed to substantiate a claim. Not having such a plan may delay the review process and payment of your claim.

Downstream impacts of ransom payment on business interruption claims

It is important to understand the coverage afforded by your insurance policy, including its limits and exclusions. A ransom payment can significantly impact the amount of reimbursement you receive from your business interruption / extra expense coverage. If the policy allows for $5 million of total coverage and a $4.5 million ransom payment has been made, you may only have $500,000 remaining to cover your loss of income, extra expense, or other available recoveries, regardless if your losses are greater than $5 million.

Quantifying your business interruption claim

The first step is to understand how the cyber incident affected business operations. There is more to analyzing the claim than just looking at the differences in revenue or net income from month to month. One needs to understand what is causing those variations and ask whether revenues, costs of goods sold, and fixed or variable expenses have changed due to the impacts of the incident. The top three business impact and extra expense measurement issues when insurance carriers are reviewing claims are the sales projections, period of indemnity, and continued versus saved or avoided costs. It is also important to note that any claimed losses to net income need to be causally related to the cyberattack.

COMMON ISSUES, MISTAKES, AND GAPS

Some root causes of post-payment pains include:

Payment legality and mechanics

It is not only a matter of making the payment, but how the payment is made and to whom. Even though this article assumes payment has been made, make sure no anti-money laundering or sanction laws have or will be broken prior to making any payment. Check with your insurance carrier and counsel prior to making any type of ransom payment. Otherwise, an entirely different world of consequences could await.

No ransomware / negotiation playbook

Of course, having breach coaches, external counsel, and incident response firms helps, but going into an incident blind could result in a hasty or incorrect payment. Have a playbook that includes a negotiation strategy and a matrix for payment considerations.

Assuming a quick ending after payment

Remediation can take time, sometimes weeks. While the analysts and technicians may be fully involved during this time, leadership should track progress and ensure investigatory and remediation tasks are closed out.

Incomplete or invalid information when presenting your insurance claim

Know your policy requirements and exclusions. Hasty ransom payment, or tasks that may fall into the grey area of coverage, could prolong claims, or prevent payment. If working with an external party, seek to ensure invoicing is clear, concise, and detailed enough to meet a carrier's coverage requirements.

Misplaced trust in the threat actor

Remember you are dealing with somebody that just robbed you. Despite paying the ransom, do not assume exfiltrated data will be disposed of by the actor, which is why performing a business disruption and income analysis on data loss and reputation are vital post-payment activities. Make sure you maintain a backup of your current financials in the event you do not get your data back after receiving the encryption key necessary to retrieve your data.

Initial focus on technical restoration and postponing the review of the financial impact

Many decisions are made at the onset of the incident such as changing the way you do business to continue operations. This may include increasing labor costs or hiring outside vendors. It is important to discuss this with your carrier to determine coverage and what information is needed to support the costs. Always keep in mind that the quicker you can resume normal operations, the less likely you are to suffer a significant impact to your financial operations.

WHERE HELP IS MOST OFTEN REQUIRED

For organizations relying on just counsel and carriers for incident response support, having experts throughout the process can make your recovery and claim presentation process a smoother affair. Your disaster recovery plan should include the expectation and planned response to a cyberattack.

The best suited incident responders require more than technical capabilities. While vital to manage and provide surge support, a team possessing experience working with counsel and carriers will set you up for a quicker resumption of your normal operations and a smoother insurance claim process. If the team has a history of working under the direction of counsel and matters covered by insurance, you are in good hands. These responders can flag a potential downstream claims issue (e.g., clarifying workstreams, warning the client of potential enhancements that may not be covered under the policy, billing requirements, etc.).

Similarly, forensic accountants who regularly work with insurance markets are better positioned to identify roadblocks that can occur during business interruption claims, whether it

is an accounting issue with lost business income or helping to quantify data loss and alternative sources of supporting data.

CONCLUSION: DO NOT NEGLECT THE POST-PAYMENT ACTIVITIES

Incident tasks should not be considered complete because a ransom payment was made. Items to consider after the ransom payment include:

- Closing out all tickets (e.g., vulnerability patching, closing out ports, reconfiguration, etc.).
- Working closely with your carrier and vendors to understand your coverage, prepare your claims, and help expedite payment for all your losses.
- Maintaining and gathering proper documentation in response to the incident to support your claim to include identification of necessary backup supporting information.
- Making decisions related to short- and long-term monitoring (dark web, reputation monitoring, etc.)
- Performing an assessment and closing vulnerabilities to avoid repeat attacks.

Acknowledgments

We would like to thank Jessica Eldridge, George Platsis, and Ron J. Yearwood, Jr., CISSP, CISM, CIPM, for providing insights and expertise that greatly assisted this research.

More About J.S. Held's Contributors

Jessica Eldridge is a Vice President in J.S. Held's Forensic Accounting -- Insurance Services practice. She has over 19 years of investigative and forensic accounting experience in measuring financial damages involving business interruption, cyber, extra expense, stock, builder's risk, employee dishonesty / fidelity, personal injury, subrogation, and litigation support services. She also has extensive experience with the administration of common fee funds and the oversite of property damage claims for large construction projects.

Jessica can be reached at jeldridge@jsheld.com or +1 857 219 5720.

George Platsis is a Senior Director providing Digital Investigations & Discovery services in J.S. Held's Global Investigations practice. He is a business professional, author, educator, and public speaker, with an entrepreneurial history and upbringing of over 20 years. He has designed and delivered solutions, and led teams to improve breach readiness, enterprise-wide and business-unit specific incident response programs, and estate hardening for a series of Fortune 100 clients in healthcare, media, financial services, manufacturing, defense, and commercial electronics industries, including support of clients in the small and medium business space. Additionally, he brings complex investigation and emergency management experience to businesses and individuals seeking to reduce their risk posture. George is a Certified Chief Information Security Officer.

George can be reached at george.platsis@jsheld.com or +1 321 346 6441.