halcyon

Ransomware: Impacts to Business
The True Costs of Ransomware

News about ransomware always starts with an attention-grabbing headline that focuses on the amount of money the victim paid to get their data back. What the headline dollar figure leaves out is the true and total cost of remediating the ransomware event from start to finish.

According to Forbes, the average cost of a ransomware payment is "north of $300,000" though we have seen from other reports that the actual average amount paid is greater.

While upcoming legislation in the U.S. may change reporting requirements, many ransomware attacks go completely unreported by organizations seeking to lessen the overall impact after falling victim to a successful ransomware attack.

In addition to the actual ransom amount victims are asked to pay, they also pay in:

- **Business disruption and downtime**
- **Incident Response**
- **Data recovery**
- **Legal costs**
- **Negative brand reputation impact**
- **Infrastructure and remediation costs**
- **Increase in cyber insurance premiums**

BUSINESS DISRUPTION AND DOWNTIME

According to the U.S. Chamber of Commerce, the average downtime due to an attack is 21 days, and on average it takes an organization 287 days (about 9 and a half months) to fully recover from an attack. It is quickly apparent that the average ransomware payment can be minuscule compared to the overall costs to an organization.

INCIDENT RESPONSE

Organizations that have prepared for a ransomware incident by deploying incident response, disaster recovery, restoration from backups and business continuity plans prior to becoming a victim, will pay a smaller cost when it comes to forensics and recovery.

Organizations that have not prepared will fare far worse. Forbes notes that the average cost of ransomware attack recovery is estimated at nearly $2 million, while the average cost of a forensic engagement is more than $70,000.

DATA RECOVERY

In a perfect-world scenario, a ransomware would simply victim pay the ransom to prevent stolen data from being leaked publicly and they receive the decryption key from the attackers. However, studies show that only 8% of ransomware victims who paid actually received keys and recovered their data. The remaining 92% do not regain their data by working with the attackers.

So, not only did they pay a hefty ransom, they had to also pay for complete data recovery, restoration from backups and other remediation efforts. According to ZipRecruiter, the average cybersecurity salary is $54 per hour, which illustrates how quickly the cost of recovery adds up.

LEGAL COSTS

With ransomware attacks continually on the rise and data breaches becoming more prevalent, governments have stepped in to try to ensure organizations are doing all they can to protect sensitive data. While organizations can take all the necessary steps to ensure they are compliant with these regulations, once a data breach occurs and customer records are compromised, a host of penalties and fines can befall the ransomware victim. These penalties can reach into the hundreds of millions of dollars.

NEGATIVE BRAND AND REPUTATION IMPACT

The most difficult cost for a ransomware victim to measure is the negative impact to their reputation and brand, but they can be the longest lasting impact to the business following a successful ransomware attack.

Customers who believe an organization has been careless with their personal information or suspect a brand has not been entirely forthcoming about a ransomware attack may never do business with that brand again. In some cases, it can take organizations many years to recover the lost customer volume due to a successful ransomware attack.

INFRASTRUCTURE AND REMEDIATION COSTS

In addition to the costs associated with paying a ransom and the countless hours spent recovering from the current breach, organizations must make investments to ensure that future attacks are unsuccessful.

Organizations will need to spend on improved infrastructure, better security tools, and additional highly skilled personnel – as well as developing and implementing response plans.

In many cases, victims of ransomware attacks are hit again not long after the first successful attack, and often by the same attackers. Organizations that fail to make this infrastructure investment following an attack will find themselves in the exact same situation.

CYBER INSURANCE PREMIUMS

The costs of ransomware incidents are unlikely to be fully covered by a cyber insurance policy, even if all the prerequisites were met. Even if an incident is covered by an insurance policy, the premiums paid by the business post-incident may significantly increase, which adds yet another recurring cost to the organization following an attack.

TOTAL COST OF A RANSOMWARE ATTACK

According to Datto, "the cost of downtime is nearly 50x greater than the ransom requested." Factor in the potential for millions of dollars in fines from regulators, and it is easy to see the devastating and lasting impact a successful ransomware attack can have on even the largest and most well-prepared of organizations:

$2,000,000 AVERAGE COST

21 DAYS OF DOWNTIME ON AVERAGE

287 DAYS RECOVERY TIME

92% DO NOT GET THEIR DATA BACK

Minimizing The Impact from a Ransomware Attack

Halcyon has built the only ransomware-specific detection engine available in the market to solve this problem. Halcyon is also the industry's first adaptive security platform that combines multiple advanced proprietary AI/ML-powered detection and prevention engines combined with AI/ML models focused specifically on detecting and stopping ransomware attacks.

By reducing the probability that an attack is successful, eliminating the impact of an incident if it does succeed, and minimizing the recovery time after an attack, Halcyon lowers all categories of risk posed to an organization by an incident.

Because Halcyon Works

Ransomware protection requires multiple layers of defense. The risk of letting ransomware run rampant through an organization is too large to leave to a single AI/ML or behavioral model. Halcyon uses several unique layers that work in unison to stop the process of ransomware from completing its task.

If a single layer fails, Halcyon can respond accordingly. Even the best defenses can be breached by a persistent threat actor, which is why Halcyon designed an autonomous isolation and recovery layer as a last resort to prevent the spread of ransomware across an organization.

For more information on how Halcyon efficiently and effectively defeats ransomware attacks, contact our Sales Team at sales@halcyon.ai or visit halcyon.ai to request a free ransomware readiness report today!