BLUVECTOR®
A COMCAST COMPANY

The True Cost of Ransomware Goes Beyond the Ransom Payment

Ransomware attacks have become a leading security concern for most organizations. With the emergence of the Ransomware as a Service (RaaS) model, sophisticated malware has entered the hands of a growing number of cybercriminal groups.

As a result, ransomware attacks are becoming more common and targeted as threat actors specializing in gaining access to corporate networks use their skills to deliver ransomware. In the first half of 2021, **ransomware attacks increased 151% worldwide** compared to the same time the previous year.

While the ransom payment is the most visible cost of a ransomware attack and what makes the headlines, it accounts for only a portion of the costs of a successful ransomware attack. Companies incur a variety of different costs as part of a ransomware infection, making solutions that can minimize the probability and impact of these attacks, such as network detection and response solution, a logical cybersecurity investment.

Factors Affecting Cost of Ransomware

Ransom demands are the most visible cost of a ransomware attack. In 2021, **nearly a third of ransomware victims** paid the ransom, and the average ransom payment for a mid-size organization was $170,404.

While this represents a significant cost to the organization, it is only a fraction of the true cost of ransomware. On average, recovering from a ransomware attack **cost organizations $1.8 million in the second half of 2021**.

The reason for this discrepancy is that ransomware victims face various costs as a result of a successful ransomware infection. Some of these costs are directly related to the process of managing and recovering from the ransomware infection, while others are the less tangible effects that a ransomware attack has on an organization's business.

Downtime Costs

Ransomware attacks can cause significant downtime for an organization. A successful infection encrypts vital company data and renders critical systems unusable. Until the company can restore that data and remove the malware from those systems, the productivity of a company and its employees will suffer.

In many cases, the cost of downtime surpasses the actual ransomware demand or payment. After a ransomware attack, a company **experiences approximately nine days** of downtime on average. While the cost of downtime to a company can vary, the average cost of $8,662 per minute places the price of downtime for a company at over $112 million.

Downtime can also have an impact on an organization's contractual relationships, especially if the services that a company provides are covered by service-level agreements (SLAs). The nine days of downtime caused by a successful ransomware

infection may exceed that allowed under applicable SLAs. If so, this breach of contract could cause an organization to incur additional downtime-related expenses due to the need to compensate affected customers and partners.

Resource Hours Spent on Recovery
One of the main reasons companies suffer so much downtime after a ransomware infection is that incident investigation, remediation, and recovery are complex. Ransomware attacks are growing increasingly sophisticated, and the result of a successful attack is critical systems rendered unusable until they are recovered from backups or by paying the ransom.

On average, an organization spends 2.5 months investigating a ransomware attack. Ransomware recovery and investigative efforts require access to specialized incident response personnel with experience in managing these types of incidents. With cybersecurity talent in short supply and the growth in ransomware and other attacks, this expertise can be expensive, driving up the cost of an attack.

Multi-Part Attacks
At its core, a ransomware attack is designed to encrypt an organization's valuable files and demand a ransom for the encryption key needed to restore them. However, if an organization can restore from backups, an attacker loses their chance of a payout.

As a result, many ransomware variants now steal an organization's sensitive data before encrypting it. This provides the attacker with additional leverage to force the victim to pay the ransom. Companies that attempt to recover without paying may have their data sold to the highest bidder or publicly leaked on the ransomware gang's website.

Combining a ransomware attack with a data breach or other attack drives up the cost of the incident to the organization. The average cost of a data breach in 2021 was $4.24 million, which dramatically amplifies the attack's impact on its victim.

Follow-Up Attacks
A ransomware infection can be a nightmare. However, if an organization is the victim of a successful ransomware attack—especially if they pay the ransom—cybercriminals might not stop with a single attack.

Ransomware attackers are in the business to make money, and a company that pays the ransom has demonstrated that they are willing to do so and that they are a potential source of future payouts as well. Also, an attacker who has gained access to an organization's environment once may have left backdoors or identified vulnerabilities that they could exploit to regain access in the future.

As a result, follow-up attacks against past ransomware victims are a regular occurrence. In fact, of those organizations that paid a ransom in 2021, 80% were the victims of a second attack. In 46% of cases, the organization believed that the same group performed the second attack.

Insurance Premiums
Cybersecurity insurance is a common way by which companies transfer the risks associated with ransomware attacks. With cybersecurity insurance, companies can address the costs of ransom payment, recovery, public relations, and other costs associated with a successful ransomware attack.

However, the rapid growth of ransomware attacks and the costs associated with them have made insurers leerier of covering ransomware attacks. As a result, the costs of cybersecurity insurance that covers ransomware increased by 28.6% in 2020, and insurers are imposing more stringent cybersecurity requirements on applicants.

Lost Business
Downtime and outages of critical systems affect more than an organization's employees. If employees can't work, they can't support their customers. Additionally, customer-facing systems may be impacted by the attack either directly or via the encryption of critical databases that they rely upon.

As a result, a successful ransomware attack can cause a significant loss of business for an organization. In fact, nearly two-thirds of ransomware victims report a substantial loss of revenue in the wake of a successful ransomware attack.

Lost Customers
In recent years, cybersecurity has become a major focus of consumers. As customers have grown more aware of how companies collect and use their data, the protection of that data has become a significant factor in their purchasing decisions.

In some cases, ransomware attacks incorporate data breaches, and all ransomware attacks involve access to sensitive data, which often includes customer records. As a result, ransomware victims may lose customers who believe that the attack demonstrates that the organization is not properly protecting the customer data that has been entrusted to it.

Public Relations Expenses
Ransomware attacks can significantly damage an organization's reputation and brand image. The inability to provide services due to downtime can shake customers' faith in an organization. In addition, a company's perceived inability to protect customers' data can hurt brand reputation if it doesn't drive customers away entirely.

Repairing the reputational and brand damage caused by a successful ransomware attack can require significant spending on public relations. An organization may need to run special campaigns or provide additional services or incentives as part of its ransomware recovery strategy. For example, in the wake of a ransomware attack that results in the exposure of customers' personal data, an organization may offer identity protection or similar services to help mitigate the attack's impact on its customers.

Regulatory and Legal Penalties
Access to an organization's sensitive data is essential to the success of a ransomware attack. For an organization to be willing to meet a large ransom demand, the attackers must have something of value. Often, this is the secret key required to decrypt an organization's sensitive data, but it might also include the threat of exposure of sensitive data stolen by the ransomware before encryption.

This means that a successful ransomware attack likely has access to data covered by data protection laws such as the EU's General Data Protection Regulation (GDPR), the Payment Card Industry Data Security Standard (PCI DSS), and others. A failure to properly restrict access to customer data protected by these laws - as demonstrated by the ransomware's ability to encrypt and potentially leak this data - could result in regulators levying penalties for non-compliance. Additionally, an organization may face civil lawsuits from customers whose data it failed to protect.

The Value of a Network Detection and Response Solution

With many factors contributing to the cost of a ransomware attack, a successful ransomware infection can carry a price tag in the millions.

The most effective method for managing the cost of a ransomware attack is to prevent the attack from happening. If an organization can identify and block ransomware malware before it infects corporate systems or before it begins encrypting files, then it can dramatically decrease the cost and damage that the malware can cause.

Preventing a successful ransomware attack requires the ability to identify it. A network detection and response (NDR) solution can dramatically increase an organization's ability to accomplish this. NDR solutions can potentially identify the initial malware infection (including multi-stage delivery), exfiltration of data stolen by the ransomware malware, or any command-and-control communications.

If an NDR solution can detect these communications and allow an organization to head off an attack, then it can create significant cost savings for the organization. With the price tag of a potential ransomware attack in the millions and these attacks growing more common and expensive, an NDR solution that enables an organization to reduce its ransomware risk offers significant value and return on investment (ROI).

Managing the Potential Costs of a Ransomware Attack

Ransomware attacks are an evolving and ever-present threat that carries significant costs to an organization. While the ransoms demanded by

the leading ransomware groups are bad enough, a successful ransomware infection also carries a variety of additional costs to its victims, such as downtime, recovery, and reputational damage. Furthermore, there are potential costs from related incidents, such as a data breach bundled with a ransomware attack or an attacker that returns to target the same organization over again.

The best way to minimize the cost and impact of a ransomware attack is to detect and block the infection before it can cause severe damage to the organization. Accomplishing this requires the right tools for the job, such as an NDR solution that enables the corporate security team to detect and respond to a ransomware infection before encryption begins.

BluVector dramatically improves organizations' network visibility and ability to identify and rapidly respond to ransomware attacks. With supervised machine learning, BluVector Advanced Threat Detection can identify even novel ransomware campaigns and offers a near-zero false positive rate. Learn more about how BluVector can help to improve your organization's ransomware defenses by requesting a demo with an expert today.

Sources

[1] https://www.bluvector.io/quarterly-threat-report/relentless-ransomware-threat-report-second-half-2021/
[2] https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf
[3] https://www.welivesecurity.com/2021/10/11/ransomware-cost-us-companies-almost-21billion-downtime-2020/
[4] https://www.ibm.com/security/data-breach
[5] https://www.cybereason.com/hubfs/dam/collateral/ebooks/Cybereason_Ransomware_Research_2021.pdf
[6] https://www.pinecc.com/hubfs/sophos-guide-to-cyber-insurance-wp.pdf?hsCtaTracking=5d4df9e3-2a07-4beb-a32b-3e0810a1c937%7C06c85b54-ed92-4943-98be-fe9e9612e1bf
[7] https://www.cybereason.com/blog/research/report-ransomware-attacks-and-the-true-cost-to-business

ABOUT BLUVECTOR

BluVector is a machine learning innovator with more than a decade of experience applying AI to detect and hunt down cyber threats. BluVector solutions strengthen the cyber defenses and protect the assets of some of the world's most discerning customers. With multiple patents, BluVector continues to help customers leverage AI-based and automation approaches to manage the volume, velocity, and polymorphic nature of today's and tomorrow's cybersecurity threats.

BluVector
4501 North Fairfax Drive, Arlington, VA 22203
www.bluvector.io

BLUVECTOR
A COMCAST COMPANY | COMCAST