Centrilogic

White Paper

AWARENESS & CYBER RESILIENCE IN THE ERA OF RANSOMWARE

By Steven Cohen – VP, CyberSecurity Practice

The Cybersecurity threats and consequences posed by Ransomware attacks are increasing at an alarming rate. Companies of all shapes and sizes are being targeted with sophisticated attacks that are increasing in severity and potency. We are also seeing increased frequency of Ransomware attacks throughout our network of customers, partners, and their end-users.

Centrilogic

White Paper

TABLE OF CONTENTS

03 What is a Ransomware Attack?

03 How do Ransomware Attacks Happen?

04 An Executive Point of View

05 Statistics & Proof Points: It Can Happen to You

07 Examples of High-Profile, Public Ransomware Attacks

08 Centrilogic Customer Example

09 Ransomware Readiness Assessment: Be Prepared

10 Supplementary Services – Prevention & Recovery

WHAT IS A RANSOMWARE ATTACK?

"Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption." [1]

HOW DO RANSOMWARE ATTACKS HAPPEN?

A Ransomware attack can be executed against your organization through many different techniques. There are primarily two forms of ransomware – Crypto Ransomware and Locker Ransomware. There are many common attack vectors for Ransomware to infiltrate an organization, including:

- Email Phishing
- Malware
- Malicious Web Links
- Instant Messaging
- Text Messages
- Social Engineering

Ransomware can also be impactful within a Supply Chain Attack by disrupting operations via partners, suppliers, distributors, or logistics organizations. Cybercriminals are constantly developing new and more sophisticated ways to ensure malware spreads as widely as possible throughout your organization.

1 https://www.cisa.gov/stopransomware

AN EXECUTIVE POINT OF VIEW

Successful Ransomware attacks can disrupt your operations for a prolonged period, or worse – put you out of business entirely.

Not only will you incur a significant and unplanned expense if you have no choice but to pay the ransom, you also have no guarantee that the malicious actors will return access to your systems and data after the ransom is paid.

In addition to the ransomware disruption itself, organizations should also be aware of the negative impacts to overall operations, inability to deliver on service or product commitments, and long-term damage to the brand of the organization.

Many companies we engage with are not adequately prepared to protect against a targeted and sophisticated Ransomware attack, and many are not able to recover in the event of a successful attack against their organizations.

ALL ORGANIZATIONS SHOULD BE PREPARED FOR RANSOMWARE.

Best practices should include a combination of appropriate defenses, risk prevention, and recovery strategies. Having a thorough understanding of your risk level, hardening your prevention mechanisms and controls in place, and establishing recovery strategies in the event of an attack will enable your organization to better protect itself against an attack, identify an attack quickly if it occurs, and recover swiftly if you become a victim.

HOW TO PREPARE YOUR ORGANIZATION

We've compiled some statistics and examples below that demonstrate the magnitude and severity of these attacks.

We've also developed a Ransomware Readiness Assessment designed to help your organization prepare for Ransomware attacks, and develop a strategy to react and recover in the event of a successful attack. We recommend that all companies complete an assessment to determine their level of risk and identify ways to improve their overall Cybersecurity posture.

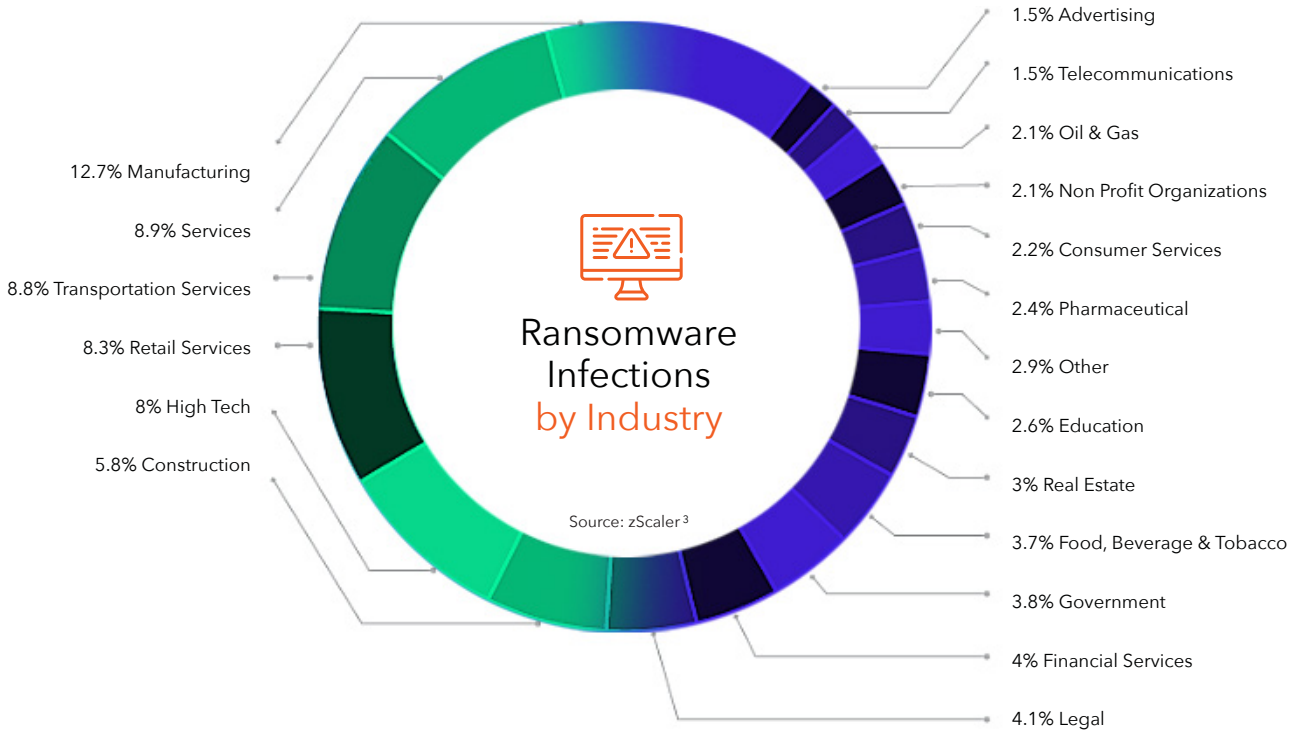
STATISTICS & PROOF POINTS: IT CAN HAPPEN TO YOU

ORGANIZATIONS ARE WORRIED ABOUT CYBER VULNERABILITY AND RANSOMWARE, AND FOR GOOD REASON.

Ransomware hits every industry – take a look at the graphic below.

According to a recent Gartner Survey[1] of over 150 executives covering top organizational risks for 2022, cyber vulnerability and Ransomware ranked as the two most important risks out of over 30 risks identified. Of those polled, 96% and 88% of respondents (respectively) rated both topics as "very important."

In the Sophos "State of Ransomware 2021" survey[2] of over 5,400 IT decision makers worldwide, 54% of respondents believed cyberattacks are now too advanced for their IT team to handle on their own.



1 Gartner Document #4009297, Survey: "2022 Top Enterprise Risk Benchmarks for Audit: Cyber and IT, ESG, and More"

2 Sophos, Survey: "State of Ransomware 2021"

3 zScaler, Ransomware Report: "Sophisticated Double Extortion Attacks are Targeting Essential Industries Causing Significant Business Disruption"

Centrilogic

White Paper

STATISTICS & PROOF POINTS: IT CAN HAPPEN TO YOU

Ransomware attacks are happening frequently and are costing organizations millions.

The average ransom payment in 2021[1] hit $570,000 – **82% higher** than $312,000 in 2020.

True costs of a Ransomware attack are estimated by Sophos[2] to be **$1.85M** in 2021 on average.

Cybersecurity Ventures[3] estimates worldwide Ransomware damages at **$20B** by the end of 2021.

Costs will increase over the next decade. Cybersecurity Ventures[4] predicts that ransomware could cost organizations a collective **$265B** by 2031 (A **30%** increase every year for the next 10 years).

In 2021, **37%** of global organizations[5] said they were the victim of some form of Ransomware attack.

HIDDEN COSTS SURROUNDING ATTACKS:

- Downtime
- Service credits and/or refunds
- Lost revenue/sales
- Legal costs
- Crisis communications & PR
- Headcount time diverted from business-driving efforts
- Increased insurance premiums
- Brand & reputation damage
- Market capitalization reductions for publicly traded companies

[1] Paloalto Networks, "Extortion Payments Hit New Records as Ransomware Crisis Intensifies"

[2] Sophos, Survey: "Ransomware Recovery Cost Reaches Nearly $2 Million, More Than Doubling in a Year"

[3] Cybersecurity Ventures, "Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021"

[4] Cybersecurity Ventures, "Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031"

[5] TechTarget, "Ransomware trends, statistics and facts in 2022"

EXAMPLES OF HIGH-PROFILE, PUBLIC RANSOMWARE ATTACKS

Public, high-profile attacks can be good case studies and examples of why an awareness of Ransomware is essential for businesses today. They're not only expensive but can cause PR or IT nightmares for CIOs and internal teams alike.

CNA FINANCIAL

After being locked out of their network for two weeks and having a sizable portion of company data stolen in Q1 2021, CNA Financial paid the hackers $40 million in ransom to regain network access.

COLONIAL PIPELINE

On May 7, 2021, the Colonial Pipeline, which supplies nearly half of the East Coast USA's gasoline, "went down for several days, causing gas panic-buying, shortages, and price spikes in some states", costing the pipeline roughly $4 million in Bitcoin as ransom.

KIA MOTORS

In 2021, Kia Motors America experienced an extended system outage because of a ransomware cyber attack conducted by DoppelPaymer, which included a $20M ransom (in Bitcoin) demand that would grant Kia a decryptor and guarantee that their sensitive data would not be leaked.

CENTRILOGIC CUSTOMER EXAMPLE

Companies of all sizes are being targeted, not just large businesses.

One of Centrilogic's customers was affected by a successful attack in early 2022 when their end-customer fell victim to Ransomware.

The attack rolled up into our client's infrastructure environment, resulting in a fully encrypted environment and an immediate business continuity effort required to mitigate the attack and restore services (SMB in the telecommunications vertical).

HERE'S WHAT HAPPENED:

- Over 100 virtual machines hosting critical applications and data across development and production environments were fully encrypted.
- Malicious actors demanded ransom in exchange for returning access to their virtual machines.
- The customer was adequately prepared for recovery in the event of a Ransomware attack.
- Centrilogic worked with our customer's internal team to begin execution of their multistep ransomware response efforts, and gradually brought services back online.
- Snapshots of each VM obtained through managed backup and storage services allowed us to migrate them to an entirely new environment and resume regular business operations with minimal impacts.

Our customer was able to minimize the consequences and avoid paying the ransom and was able to recover most information and data due to their strong backup and retention schedules. If that hadn't been the case, the consequences could have been severe – both financially and operationally.

Centrilogic is still reviewing ways to identify new methods to improve the detection and prevention capabilities of the customer to help them identify and prevent future attacks faster.

Centrilogic

White Paper

RANSOMWARE READINESS ASSESSMENT: BE PREPARED

We offer customers a thorough Ransomware Readiness Assessment designed to help you gain peace of mind.

We **evaluate** and **identify** your current risk level for a Ransomware attack, identify specific gaps in the Ransomware preparedness, and **recommend** steps required to improve your organization's overall Cybersecurity posture, and developing a plan to recover swiftly in the event of a Ransomware attack. Assessments include, but are not limited to the following components based on the NIST Cybersecurity Framework. The assessment is designed for most organizations of all sizes, and across all industries and verticals.

IDENTIFY:
- Identify and locate all critical business assets that could be susceptible to risk
- Identify and document existing anti-malware controls
- Identify any gaps or issues with current controls and overall cybersecurity posture
- Assess the current threat level to the organization

PROTECT:

Assessment of processes & controls in place to protect against attack, including:
- User permission & awareness
- Endpoint configuration
- Server configuration
- Change & patch management processes
- Web protection
- Network protection
- Email protection
- Data backup & storage processes

DETECT:
- Assessment of all anti-malware security software and hardware products
- Evaluation of how quickly your team and systems could detect an attack

RESPOND:
- Assessment of current Incident response processes & plans in place in the event of a Ransomware attack
- Assessment of internal team structure

RECOVER:
- Assessment of ability to recover in the event of an attack based on steps 1-4
- Walkthrough of existing Business Continuity & Disaster Recovery (BC/DR) plans
- Evaluation of system backup and storage efficacy
- Evaluation of any external vendors required to assist your organization in steps 2-4

Centrilogic

White Paper

SUPPLEMENTARY SERVICES – PREVENTION & RECOVERY

You're in good hands with Centrilogic's range of Cybersecurity & Infrastructure services.

There is no one-size-fits-all playbook that can be deployed to facilitate Ransomware prevention and recovery. Much of an organization's ability to prevent Ransomware and recover in the event of the attack is dependent on its overall systems, data, and infrastructure architecture. Oftentimes, proper prevention and recovery is only possible through a combination of Cybersecurity and Infrastructure services being in place. We have a comprehensive portfolio of both, which can be architected to support most Ransomware prevention and recovery strategies. Some of these services that we offer include:

CYBERSECURITY SERVICES THAT CAN HELP PROTECT/PREVENT THEIR INFRASTRUCTURE AND APPLICATIONS:

CISO-as-a-Service

Incident Response & the Development of Incident Response Processes

24x7 Managed Security / SOC Monitoring

Intrusion Detection & Prevention

Email Security

Security Awareness Training for End Users

INFRASTRUCTURE SERVICES THAT CAN ENABLE SWIFT RECOVERY IN THE EVENT OF AN ATTACK:

Managed Backup

Managed Storage

Disaster-Recovery-as-a-Service (DRaaS) – Virtual Continuous Replication

Backup, Storage, Restore, & Recovery solutions across leading Public Cloud platforms

Options and recommended solutions will vary based on application and infrastructure environments

Now's the time to act. If you are concerned about your organization's vulnerability to Cybersecurity threats and Ransomware attacks, and think you can benefit from a Ransomware Readiness Assessment, please contact us today.

Centrilogic's Ransomware Readiness Assessment is a paid engagement. Costs can vary based on a variety of factors. A no-obligation discovery call will allow us to produce a Statement of Work that's tailored to your business needs.