# MURRAY STATE UNIVERSITY

# Ransomware Prevention Methods and Attack Response

Student: Aaron David | Professor: Dr. Randall Joyce, Professor of Cybersecurity & Network Management

## Abstract

Ransomware is becoming more and more of a prominent attack in our present day. In essence, it is a type of malware that prevents one from accessing a device or information stored in that device. 75% of these attacks begin with either a phishing email or Remote Desktop Protocol (RDP), with 60% of ransomware cases ending up having malware directly installed on one's desktop or sharing apps. With that in mind, it is important that organizations know about it and know what they can do to mitigate it. Although some organizations won't be affected as much (take the San Francisco 49ers attack from last year for example), many can be affected majorly. Successful attacks can heavily damage an organization and could set them back years or make them go out of business. With some better knowledge, policies, tools, and equipment in place, organizations can be better prepared if a ransomware attack were to happen on their network. Having strategies for prevention, preparation, response, and recovery can also help aid in defense. Organizations need to start preparing for a ransomware attack as they quickly grow more and more popular. It doesn't matter if an organization is big or small and it doesn't matter if the chance for an attack is low. A successful attack can prove to be detrimental to an organization. It could not only hurt financially, but also tank an organization's reputation with the public.

## Products

paloalto NETWORKS

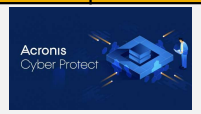
- Next-Generation Firewalls
- Wildfire
- Cortex XDR

CROWDSTRIKE

- 24/7 Threat Hunting
- Real Time Monitoring
- XDR

LogRhythm The Security Intelligence Company

- SEIM Tools
- Event Correlation
- Logging and Alerting




- Forensic Backup
- Continuous Data Protection
- Cyber Protection Operations Center

SentinelOne

- XDR
- Real Time Monitoring
- Timeline Analysis

## Strategy

A strategy needs to be established and documented to provide guidance on what exactly to do to prevent and prepare for a ransomware attack. If a ransomware attack is present, then the strategy will show how to deal with in the most efficient and least-impactful way possible. The table below highlights the four phases and some of what is done in each phase:

| | |
|---|---|
| **Prevention** | • **Multi-factor authentication**<br>• **External email notification**<br>• **Training for all employees** |
| **Preparation** | • **Knowing who to communicate with**<br>• **Knowing who makes the decisions**<br>• **Preparing for all situations** |
| **Response** | • **Notifying law enforcement**<br>• **Activating third-parties if applicable**<br>• **Gathering forensics and other info** |
| **Recovery** | • **Verifying if threat agents have said information**<br>• **Using alternative methods to get data back.** |

## Other Methods

Plenty of other tools and methods can be applied to help an organization defend against a ransomware attack. It always helps to have plenty at your disposal to better the chances of being wiped by ransomware. Below are some examples of more options:

- Having and maintaining backups so they are ready to use.
- Looking over port settings and endpoints of the network.
- Implementing IDS tools to locate malicious traffic and send out alerts.

## Conclusion

Ransomware attacks are only going to get more frequent and complex as time goes on. It is important that organizations implement efficient methods and tools to better combat these attacks. While it can be time consuming and expensive, the benefits greatly carry more weight than the outcomes of a ransomware attack.

## References

Boehm, J., Hall, F., Isenberg, R., & Michel, M. (2022, February 14). *Ransomware prevention: How organizations can fight back*. McKinsey & Company. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/ransomware-prevention-how-organizations-can-fight-back

Gast, K. (2022, January 21). *Top ransomware detection techniques*. LogRhythm. https://logrhythm.com/blog/top-ransomware-detection-techniques/

Keary, J. (2022). Rebuffing Russian Ransomware: How the United States Should Use the Colonial Pipeline and JBS USA Hackings as a Defense Guide for Ransomware