Ransomware Response Recommendations for Wayne State University

Executive Summary

In the evolving landscape of cybersecurity threats, Wayne State University must enhance its resilience against increasingly sophisticated attacks. This report examines a simulated scenario involving ransomware, phishing, and data breaches, and provides practical recommendations to mitigate risks, strengthen infrastructure, and improve response strategies. The focus is on using existing capabilities while also identifying areas for improvement in training, systems management, and incident response.

Key recommendations include updating operating systems, implementing Zero Trust Architecture (ZTA), improving employee training on phishing and cybersecurity policies, and enhancing incident response procedures.

Table of Contents

1. **Executive Summary**
2. **Introduction**
3. **Cyber Threats to Wayne State University**
    a. Ransomware
    b. Phishing
    c. Data Exfiltration
4. **Critical IT Systems and Processes**
5. **Recommendations**
    a. Update Operating Systems and Software
    b. Phishing and Email Security
    c. Zero Trust Architecture (ZTA)
    d. Cyber Incident Response Plan (CIRP)
    e. Employee Training and Awareness
    f. Backup and Recovery Systems
    g. Public Communication and Crisis Management
6. **Risk Management Strategy**
7. **Conclusion**
8. **References**

Introduction

Wayne State University, like many organizations, faces growing cybersecurity threats that could impact the integrity and confidentiality of sensitive information. Recent simulated events—including a ransomware attack, a phishing scam, and data exfiltration—highlight weaknesses in the institution's current cybersecurity posture. The aim of this report is to assess these events and propose actionable steps to safeguard the university's digital assets.

Cybersecurity resilience is critical for maintaining trust, continuity, and legal compliance. This report offers recommendations that reflect best practices while remaining achievable within the university's current structure.

Cyber Threats to Wayne State University

1. **Ransomware:** A ransomware variant targeting state and local organizations has been identified, with Wayne State potentially at risk. The university experienced a simulated ransomware attack demanding $53,000 in Bitcoin for a decryption key, jeopardizing critical data and operational continuity.
2. **Phishing:** Employees received a fake email appearing to come from the Vice President of Finance, leading some to open a malicious PDF. This incident revealed gaps in employee awareness and email security.
3. **Data Exfiltration:** Suspicious DNS traffic outside business hours indicated possible data theft from the university's HR department. Critical Personally Identifiable Information (PII), including employee social security numbers and banking details, was accessed by threat actors.

Critical IT Systems and Processes

Key systems that are vital to Wayne State University's operations include:

- Human Resources systems that store PII of employees.
- Financial systems for managing transactions, budgets, and sensitive financial data.
- Student records management systems that handle academic, personal, and health information.

These systems must be protected, and any compromise to their integrity could lead to operational paralysis or reputational damage.

Recommendations

1. **Update Operating Systems and Software**

   Issue: The university's current operating system no longer receives security patches, increasing vulnerability to attacks.

   Recommendation: Wayne State should prioritize migrating to a supported operating system. Regular updates and patches must be applied across all devices to reduce exposure to malware and ransomware.

2. **Phishing and Email Security**

   Issue: Several employees fell victim to a phishing scam, despite attempts to verify the authenticity of the email.

   Recommendation: The university should strengthen its anti-phishing efforts by:

   - Conducting mandatory phishing simulations as part of regular cybersecurity training.
   - Implementing enhanced email filters to detect and block suspicious attachments or links.
   - Training employees on recognizing phishing attempts and reporting them through a streamlined process.

3. **Zero Trust Architecture (ZTA)**

   Issue: Suspicious DNS traffic and data exfiltration from HR systems suggest inadequate network monitoring and segmentation.

   Recommendation: Implement a Zero Trust Architecture, which assumes that threats could come from inside or outside the network. This includes:

   - Limiting access to sensitive data based on user roles.
   - Regularly monitoring and logging all network activity.
   - Ensuring multifactor authentication (MFA) is in place for accessing critical systems.

4. **Cyber Incident Response Plan (CIRP)**

Issue: The response to the ransomware attack was delayed, and the decision-making process on paying the ransom was unclear.

Recommendation: Wayne State should revise and expand its Cyber Incident Response Plan to:

- Include clear guidelines on ransomware scenarios, including when to engage with external partners and legal counsel.
- Provide explicit instructions on restoring data from backups to reduce downtime in the event of an attack.
- Train staff on CIRP protocols through frequent tabletop exercises and drills.

5. **Employee Training and Awareness**

   Issue: Employees opened a malicious PDF attachment, which points to a need for improved training.

   Recommendation: Enhance the cybersecurity training program to include:

   - Regular refresher courses on identifying phishing, ransomware, and social engineering attacks.
   - Specific training for system administrators on managing privileged access and securing critical systems.
   - Integration of cybersecurity into new employee onboarding processes.

6. **Backup and Recovery Systems**

   Issue: The ransomware attack highlighted the importance of secure backups to ensure rapid recovery.

   Recommendation: Wayne State should ensure:

   - All critical data is backed up regularly to an off-site location or cloud storage service.
   - Backup copies are tested for integrity and recovery speed at least quarterly.
   - A rapid restoration plan is in place, with a goal to restore primary systems from backups within 24 hours.

7. **Public Communication and Crisis Management**

   Issue: The news of the cyber incident attracted media attention, creating a potential reputational risk.

Recommendation: The university should develop a clear public relations strategy that includes:

- Pre-scripted messages for different types of cyber incidents.
- Coordination with legal and PR teams to ensure accurate and timely communication.
- Training communications staff on cybersecurity terminology to confidently engage with the media.

Risk Management Strategy

Wayne State University must strengthen its risk management practices by:

- Conducting regular risk assessments to identify and prioritize vulnerabilities.
- Implementing a vulnerability management program focused on mitigating known exploits in internet-facing systems.
- Applying the principles of Zero Trust to limit access and enhance security across all systems.

Wayne State should align its risk management strategy with the NIST Cybersecurity Framework, which helps identify, protect, detect, respond, and recover from cyber incidents. By using this framework, the university can ensure it stays ahead of evolving threats.

Conclusion

The cybersecurity challenges faced by Wayne State University reflect broader trends in higher education and beyond. By taking immediate steps to update systems, enhance training, adopt Zero Trust Architecture, and improve incident response, the university can greatly reduce its exposure to cyber threats. Through these actions, Wayne State can build a more resilient cybersecurity posture, protecting its students, faculty, and staff from future attacks.

References

Cybersecurity and Infrastructure Security Agency (CISA). “Zero Trust Maturity Model.” CISA, 7 Sept. 2022, www.cisa.gov/zero-trust-maturity-model.

Cybersecurity and Infrastructure Security Agency (CISA). “Alert (AA20-302A) Ransomware Activity Targeting the Healthcare and Public Health Sector.” CISA, 28 Oct. 2020, www.cisa.gov/uscert/ncas/alerts/aa20-302a.

National Institute of Standards and Technology (NIST). “Cybersecurity Framework.” NIST, 16 Apr. 2018, www.nist.gov/cyberframework.

Scarfone, Karen, and Peter Mell. “Guide to Intrusion Detection and Prevention Systems (IDPS).” NIST, Feb. 2007, nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf.

Coveware. “Ransomware Payment Amounts Decline as More Victims Resist Extortion Demands.” Coveware, 28 July 2021, www.coveware.com/blog/2021/7/28/ransomware-payment-amounts-decline-as-more-victims-resist-extortion-demands.