

Memo: Cyber Attack on Vaccine Test Center

From: Cybersecurity Response Team

To: Executive Leadership

Overview

On March 14, 2020, Hammersmith Medicines Research was targeted by the Maze ransomware group, resulting in stolen patient data. This memo highlights the impact and action plan.

Key Impacts

- **Patient Trust:** Privacy concerns due to leaked trial data. - **Global Impact:** Disrupts COVID-19 vaccine efforts and undermines collaboration. - **Threat Environment:** Healthcare organizations remain high-value targets.

Action Plan

Immediate Safeguards

- Implement real-time intrusion detection systems. - Encrypt sensitive data to prevent misuse after theft. - Conduct urgent employee training on phishing and ransomware threats.

Future-Proofing

- Deploy zero-trust security frameworks to restrict access. - Maintain offline backups for rapid recovery without ransom payment. - Partner with cybersecurity firms for proactive threat management.

Policy Recommendations

- Formalize an incident response plan and test regularly. - Mandate endpoint detection and response (EDR) tools. - Enhance transparency with patients and stakeholders about security measures.

Communication Strategy

- Use secure emails and online portals for stakeholder updates. - Host virtual training sessions for staff. - Post concise public updates via official website and social media.

Conclusion

By combining technical measures, policy updates, and transparent communication, Hammersmith Medicines Research can mitigate risks, protect patient data, and restore trust.