Memorandum

From: John Mitchell, Chief Information Officer
To: Providence Medical Group, Northwest Region, Executive Leadership Team
Re: Ransomware attack: immediate and long-term response
Date: March 26, 2020

Situation Update

Beginning March 24th, Providence staff members began receiving emails purporting to contain Covid-19 emergency protocol information. They were in fact part of a coordinated attack – known as "NetWalker Ransomware" on health care providers across the United States and Canada. The emails contained a malicious attachment that – if opened – would attempt to encrypt our patient data and critical systems, potentially crippling our ability to provide care during the COVID crisis.

Several of these emails were opened, but due to the rapid response of our IT security operations center, their threat was neutralized within minutes. Other health care providers have been less fortunate, and several have been forced to take critical systems offline while they attempt to recover.

In view of the ongoing and critical threat to Providence's operations, the drastic step was taken of temporarily quarantining **all** email attachments. We understand and sincerely apologize for the disruption that this has caused to patient operations. This memo outlines our plan to rapidly – but judiciously – return to normal operations, and the strategic plan to defend our organization from future attacks.

Operational Recovery Plan

This attack combined sophisticated technical methods with psychological manipulation, exploiting COVID-19 anxiety to bypass normal staff vigilance. Our response addresses both the technical vulnerability – through enhanced monitoring, and the human factor – through comprehensive staff training.

Immediate Actions (March 27):

- Release company-wide PSA to raise threat awareness and ensure confidence in our response

Phase 1 (March 27-28): Controlled Communications Restoration

- Filter and release attachments from verified healthcare providers
- Institute manual review process for critical communications from other sources

Phase 2 (March 29-30): Enhanced Protection and Awareness

- Deploy advanced threat protection with healthcare-specific rules
- Distribute staff training module on COVID-themed phishing tactics

Phase 3 (April 1-2): Full Communications Restoration

- Return to normal email operations with enhanced monitoring and threat intelligence

Strategic Vision

This crisis has demonstrated the resilience of our organization in the face of operational threats, and a reminder of a mission imperative: to maintain patients' trust by protecting their data. This is not just a mission imperative, but a competitive advantage: patients who cannot trust us with their data will go elsewhere.

To maintain this competitive advantage, we will:

Develop a culture of data stewardship

- Reframing training from "data compliance" to "data stewardship"
- Ensuring every staff member is aware and invested in their role as guardians and protectors of patient information
- Providing state-of-the-art training in the latest data protection techniques

Use advanced data-analytics methods to identify and respond to attacks in real time

- Develop machine learning models that can spot anomalies – such as behavioral anomalies, and network traffic patterns - in real time.
- Create automated threat responses that will both rapidly neutralize the immediate threat, and alert IT staff for any further human intervention

Use predictive risk analytics to anticipate future threats

- Analyze patterns from global threat feeds to identify potential threats to healthcare systems
- Identify likely methods of attack, and allocate resources to proactively protect vulnerable components of our systems
- Implement early warning systems that detect shifts in adversarial tactics

Conclusion

This crisis has been a test of our organization's collective skill and resilience – and of its leadership. I would like to thank you all – my fellow leaders – for your forbearance during this difficult time. I look forward to our future collaboration in ensuring that Providence is not just a world leader in patient care, but in patient trust.

John Mitchell
Chief Information Officer
Providence Medical Group, NW Region