Strategies for Orthopedic Resilience During a Cyber Attack: Lessons from a Complete System Shutdown

Michael Robert McDermott, Naem Mufarreh, Charles Edan Spieser, Samuel Lee Shepard, Ante Rebic, Gavin Scott, Darren Bruce Malek, Evelyn Thomas, H Brent Bamberger

INTRODUCTION:
Healthcare cyber attacks are becoming more frequent and increasingly sophisticated, posing a significant threat to patient care across healthcare systems. For orthopedic practices, where care often depends on precise surgical plans, advanced imaging, and long-term continuity, a full-scale systems failure can be catastrophic. The healthcare industry has seen a record number of data breaches and patient records exposed in recent years, with 2023 and 2024 seeing millions of records compromised. This abstract recounts a real-world incident in which a severe cyber attack left our hospital's computers out of commission, the internet disconnected, and the phones without service. We describe the strategies our orthopedic department implemented to maintain clinical operations and highlight key infrastructure elements that would allow others to prepare for and respond effectively to a cyber attack.
METHODS:
Following the attack, our orthopedic team rapidly established an independent and resilient operational framework. First, a crisis leadership group was formed, including two attending surgeons, a senior resident, and a non-clinical executive, to coordinate the response. The biggest initial challenge was the loss of any record of what patients we had in the hospital and the status of their treatment. In response, we immediately sought a way to create a HIPAA-compliant cloud-based drive, that was external to the hospital’s network. This system served as a central hub for patient face sheets, standardized paper documentation templates, and real-time patient tracking. The second challenge was the loss of communication throughout the hospital network. To address this, we began having team huddles twice daily to ensure updated workflows, coordinated patient care, and facilitated communication. Next, a dedicated resident was assigned to each emergency department (ED) daily, serving as a liaison by providing direct contact information alongside the on-call physician details daily. Additionally, an advanced practice provider was stationed full-time in the postoperative care unit to streamline discharge planning and improve throughput. The third challenge was rather unique, we had the ability to capture radiographic imaging, however, they could not be uploaded or viewed electronically. Instead, the images could be manually viewed on the machine, but identifying the machine used for each specific patient was a taxing process. To address this, we designated a single portable X-ray machine in each ED exclusively for orthopedic use, storing images locally to facilitate quick access. The last major challenge resolved around laboratory testing. There was no way to track the results of the ordered labs or ensure that they were completed. To address this, we created a manual tracking system within our secure drive and assigned staff to follow up on pending labs for each patent. To prevent delays in elective cases, especially those requiring preoperative labs for anesthesia clearance, patients were directed to obtain labs at outside clinics and bring printed results on the day of surgery.
RESULTS:
These practical, low-tech interventions proved remarkably effective. Our orthopedic department maintained approximately 70% of its typical surgical volume. Elective cases, often the first casualties in crises, were only suspended for one day. Interestingly, a substantial number of the canceled elective cases were robotic total joints that required imaging, as the system shutdown hindered the ability to upload the images. All urgent and emergent cases were handled without delay or compromise in quality.
DISCUSSION AND CONCLUSION:
This experience provides a pragmatic blueprint for orthopedic practices facing the growing threat of cyber attacks. It underscores the necessity of having pre-established plans for communication, documentation, and imaging access. The single most impactful strategy was the development of a HIPAA-compliant, which we recommend everyone set up as a general safety precaution, as having one established would allow for seamless adaptation when institutional systems failed. Our experience offers a clear, actionable framework for healthcare teams aiming to build resilience in an increasingly vulnerable digital landscape.