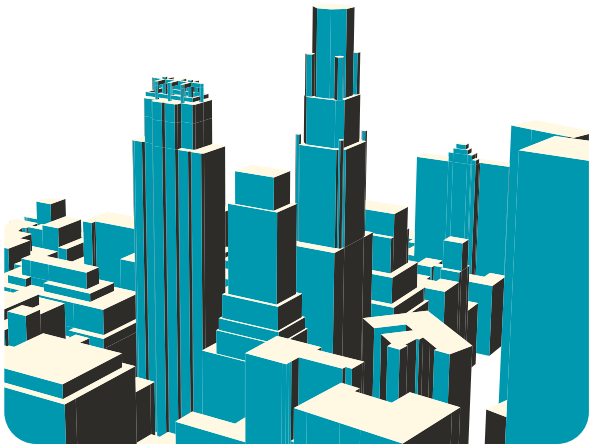
Redpoint
Cybersecurity LLC

REDPOINT INCIDENT RESPONSE USE CASE



THE PROBLEM

A large architecture & design firm with a global distribution network lost access to critical infrastructure following a compromise:

- **A ransomware attack was quickly contained, but in stopping the spread of malicious activity, numerous critical servers were rendered offline and inaccessible.**
- **The client's IT Director was out of the country and no one on site had the skillset needed to identify and troubleshoot the situation to resolution. Much of the client's staff was unable to access needed resources.**
- **Critical server infrastructure had to be brought back up and running in a safe manner to facilitate a digital forensics collection and analysis procedure before restoring accessibility to the needed services and data.**
- **Following confirmation that the infrastructure was safe to be fully restored, troubleshooting was necessary to fully restore connectivity and service accessibility.**

TOOLS & TECHNIQUES

- **First Response:** A discussion with involved parties determined an engineer was needed on-site immediately. A Redpoint engineer was engaged and deployed on-site same day, with initial investigation and discovery beginning that evening.
- **Immediate Findings:** It was discovered quickly that critical storage infrastructure had encountered hardware failure following improper shutdown procedures. Migration plans were made to bring the storage back up to facilitate forensic artifact collection.
- **Forensic Investigation:** Improvisation allowed a portion of the storage network to be restored using resources available on-site. The forensic investigation was kicked off and further steps were taken to get replacement infrastructure.
- **Full Restoration:** Replacement infrastructure was acquired within 48 hours and migration procedures concluded quickly. Configuration steps and challenges were handled by Redpoint on-site in coordination with the client's CISO and IT Director.
- **Remediation:** The forensic collection process was concluded within 36 hours of gaining access to the missing storage infrastructure. Analysis was performed on-demand and to provide clearance for full restoration of access.

OUTCOMES

- Redpoint gained momentum in the triage & investigation and forensic collection & analysis processes by providing **remote-based IR support within 3 hours of incident** being reported.

- **Identified and resolved** numerous technical challenges in restoring functionality to missing components on the network that had been compromised by the threat actor (attacker).

- Investigation & analysis allowed compromised systems to be identified and **remediated** while clearing other systems to be fully brought back online, allowing the client's business to resume work.

CONTACT US TODAY

TAB BRADSHAW

tab@redpointcyber.com

Principal

Redpoint Cybersecurity

RUSSELL SAFIRSTEIN

russell@redpointcyber.com

President

Redpoint Cybersecurity