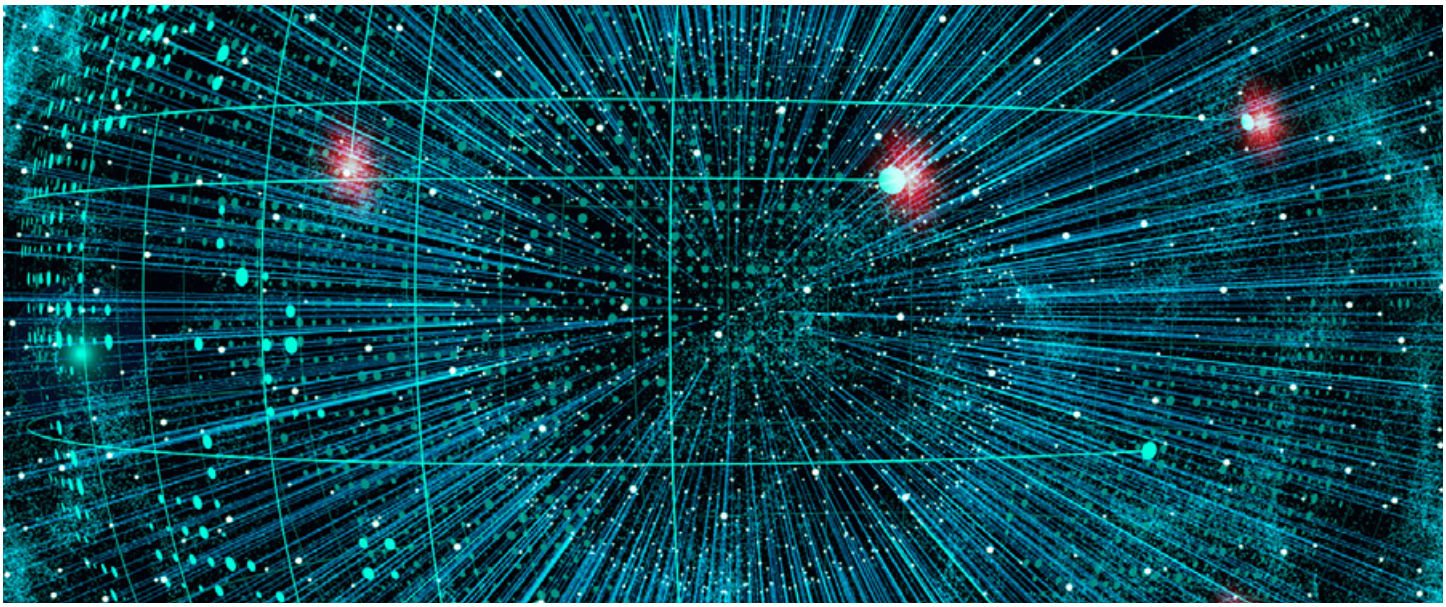

When it comes to confronting a ransomware attack, two teams are better than one

Ransomware attacks can hit companies hard and fast. By bringing in Deloitte shortly after the onset of an attack, one law firm was able to quickly get back to work and on the road to recovery. And by tapping Deloitte's deep suite of cyber services, it's now better able to defend against future attacks.

The client dilemma

Early one Saturday morning, the IT security manager for a midsized law firm received the worst news of his career: His firm had fallen victim to a devastating ransomware attack. More than 80% of the systems under his management were affected. Over the next two weeks, he and his team of four engineers tried to figure out how it happened, what data was affected, and if data was stolen. At the same time, they were trying to restore services and applications and rebuild user workstations.

The Deloitte response

Faced with too many business-critical issues to address at once, the team called in Deloitte to assist with investigating and repairing the damage from the attack.

After a quick briefing call, Deloitte deployed a team of subject-matter specialists within just a few hours (on a weekend, no less).

- The team swiftly triaged the event, contained the malware, and eradicated threat actors from the environment
- Incident responders performed data forensic procedures to understand how the attack was perpetrated
- Simultaneously, recovery specialists worked with business stakeholders to develop an action plan to restore services and applications in order of priority
- This same team spearheaded a workstation rebuild process to get the firm's attorneys and support staff back to work

More than results … recovery

The incident responders determined the threat actors had been in the environment for a few weeks prior to the attack and were able to deconstruct their methods. With the knowledge of how the attack happened, the IT security manager and his team worked with Deloitte cybersecurity specialists to formulate a road map to make the environment more secure, implement better detection mechanisms, and build a plan to follow so they'll be better prepared in case it happens again.

Let's connect.

Andrew Morrison
Principal
Cyber Risk Services
Deloitte & Touche LLP
anmorrison@deloitte.com

Wayne Johnson
Senior Manager
Cyber Risk Services
Deloitte & Touche LLP
wajohnson@deloitte.com

Isaac Kohn
Principal
Cyber Risk Services
Deloitte & Touche LLP
ivkohn@deloitte.com

Mike Wilson
Specialist Leader
Cyber Risk Services
Deloitte & Touche LLP
mwilson@deloitte.com