How KPMG enabled a global food processing corporation in Canada recover from a ransomware attack

Client challenge

A global food processing corporation headquartered in Canada, employing over 500 staff members, found itself in a crisis due to a debilitating ransomware attack. The incident led to the encryption of servers and data within the clients' IT environment, prolonged downtime during which critical business operations were unavailable, and risks to confidential recipe information, impacting production, employee safety and confidentiality. The organization sought immediate support through legal counsel and a cyber insurance provider for incident investigation and recovery.

Solution

KPMG's cyber incident response team responded swiftly, initiating a call within 30 minutes with the client and their legal counsel (breach coach) to scope and triage the ransomware incident. Prioritizing confidentiality and privacy per the law firm's directives, KPMG secured access to the affected systems. Members of KPMG's team conducted extensive threat hunting activities and deployed endpoint detection and response tools to effectively contain and investigate the breach. Comprehensive log collection and artifact reviews were included in the scope of KPMG's review. Recognizing the urgency of the incident, KPMG established 24/7 monitoring of the IT environment to deter further threats.

To further assist, KPMG and legal counsel engaged a third-party negotiator associated with the ransom demand and provided support for decryption and recovery, including testing decryption keys. KPMG also assisted with the rebuilding of IT and operational technology environments in collaboration with the client where necessary. Our approach ensured data confidentiality while addressing production impacts and operational implications.

The outcome: building cyber resilience

As part of KPMG's services, the client received a detailed forensic investigation report which included an incident timeline illustrating the activities performed by the threat actor. KPMG's investigation uncovered additional malicious activities performed in the clients' IT environment in addition to the ransomware deployment that had previously gone undetected. Through collaboration with KPMG, the client not only restored business operations but also enhanced its incident response capabilities as well as monitoring and detection expertise. Our holistic approach addressed vulnerabilities and facilitated the creation of a strategic roadmap for improving the clients' overall security posture. Recommendations included various security investments, which resulted in the client selecting a managed security service provider, completing penetration testing within its IT environment, and revision of certain business processes. By collaborating with KPMG, the client fortified its IT environment against future threats, while underscoring its commitment to cybersecurity resilience.

To learn more about our Cyber Incident Response services and how we can help your organization, click here: Cyber response - KPMG Canada.

If you have experienced or have a question about a cyber incident, contact our team of incident response specialists email us at cyberincident@kpmg.ca or call our Toll-free telephone number: 1-844-576-4911

Contact us

Our dedicated team is here to support your organization's unique needs.

Alexander Rau

Partner, Advisory Services - Cybersecurity
KPMG in Canada
+1 416-777-3450
alexanderrau@kpmg.ca

Guillaume Clément

Partner, Advisory, Cybersecurity
KPMG in Canada
+1 418-653-5335
guillaumeclement@kpmg.ca