Overcoming a cybersecurity breach in the education sector

Client challenge

A prominent post-secondary education institution in Canada, with more than 500 employees and 5,000 students, faced a significant cybersecurity incident caused by an insider threat. A trusted employee – acting as the threat actor – exploited their access to sensitive systems to exfiltrate confidential employee and student data to a personal device. In addition, the trusted employee compiled a report detailing the institution's vulnerabilities.

At the time of the incident, the institution was working to enhance its cybersecurity measures, including upgrading its Endpoint Detection and Response (EDR) system. Although the existing EDR tool was operational, the insider threat actor successfully bypassed it without detection. This exploitation allowed them to manipulate vulnerabilities within the institution's systems freely. However, as the new EDR solution was rolled out, it began to trigger alerts regarding the unauthorized activities performed by the employee. Recognizing the implications for privacy and confidentiality, the institution took swift action, assessing the alerts and notifying impacted individuals about the breach.

Solution

Within less than 24-hours of discovering the breach, the institution reached out to KPMG for assistance. Leveraging our pre-established relationship with the institution and our expertise in the education sector, KPMG responded swiftly.

KPMG initiated the investigation with a triage call to understand the incident, followed by a thorough scoping phase. Our multidisciplinary team of incident responders and analysts began accessing the institution's technologies and logs, prompting a detailed examination of flagged activities. Our thorough forensic analysis involved an in-depth review of system logs to detect malicious actions and evaluate forensic artifacts critically. A dedicated team of five KPMG professionals, each specializing in areas such as incident response, forensics, and threat intelligence, steered the institution through this challenging phase.

During our investigation, KPMG identified that the malicious employee had executed custom scripts to extract sensitive information from the institution's Enterprise Resource Planning (ERP) system, collected user account details (including hashed passwords), spoofed emails of executives, and conducted a penetration test on the institution's environment, ultimately compiling a report of their findings. KPMG documented these findings in a formal report for legal counsel (the institutions "breach counsel"). This report proved essential in assisting the law firm in furnishing legal guidance to the institution.

In collaboration with the breach coach, KPMG provided critical insights that highlighted the risks and implications of the breach, ensuring that the institution received actionable legal advice tailored to the specific circumstances of the incident. To benefit the institution, we provided a comprehensive breakdown of technical findings, including a detailed timeline of the threat actor's activities. Our proactive threat-hunting efforts identified indicators of compromise within the institution's environment, each of which were thoroughly documented in our technical analysis report.

The detailed information provided by KPMG enabled the institution to gain a deeper understanding of the incident and made necessary adjustments to their security measures. This case underscores the importance of vigilance, proactive threat-hunting, and robust incident response strategies in the face of an ever-evolving cybersecurity landscape.

The outcome: building cyber resilience

The outcome of our intervention was transformative for the institution. We established a trusted relationship with the college, demonstrating our commitment to not only providing evidence but also offering actionable recommendations. The college emerged from this incident more cyber-resilient, equipped with a clearer understanding of their vulnerabilities and the confidence that they had a responsive and proactive team dedicated to protecting them, especially vital considering the sensitive nature of students and minors in the educational sector.

The breach coach was able to rely on the findings from our work to inform them of their legal advice. This collaborative effort solidified our position as a trusted advisor in the eyes of the college, illustrating how we earned this title through effective incident management and security enhancement strategies tailored to their specific environment.

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