Vulnerable Vendors: Automakers' Data Breach Highlights Importance of Vendor Cybersecurity

Insights
9.07.18

This summer, several automakers, including Tesla, Toyota, General Motors, Ford, and Volkswagen learned that their closely held trade secrets were readily available on the internet. The source? An unprotected back-up server. The rub? The server did not belong to any of the car manufacturers. Instead, the server belonged to a vendor of industrial automation services, Level One Robotics and Control ("Level One"), who had performed work for each of the manufacturers.

Included in the 157 gigabytes of data found on Level One's server were the automakers' blueprints, factory schematics, contracts, invoices, work plans, and non-disclosure agreements – all information that the manufacturers would not have known was publicly available if not for a security researcher's routine search of publicly available connected devices. Once the security researcher realized what was inadvertently unprotected, he alerted Level One, who promptly took down the information and notified the affected customers.

Fortunately for the auto manufacturers, it seems that the security researcher who initially came across the data was the only person to download the information.

Takeaways
This latest cybersecurity incident highlights the importance of vetting your vendors. Employers should consider what information their vendors have access to, whether that information is confidential or personally identifiable information, and whether and how their vendors are storing that information. Employers should also carefully and thoroughly review vendor contracts for indemnification clauses, limitations on liability, and guidance as to the party who will be expected to pay in the event of a data breach. Finally, employers should consider adding provisions to their vendor contracts to explicitly address how vendors should store and protect such information.