

# Incident Readiness and Response Partnership: AUTOMOTIVE MANUFACTURER

## Client challenge

After recovering from a business email compromise, a global automotive manufacturer realized they needed to shore up their defenses and be better prepared should a more significant incident occur. It was a wakeup call — the incident response effort had exposed key gaps in their IR plan. Post-breach, they wanted to take the lessons learned and better prepare for the next time the plan was put into action. A key first step was to identify a long-term partner able to help them not only better defend and prepare for future incidents but be at the ready to assist them every step of the way should an incident occur again. After interviewing a number of incident response consulting firms, this manufacturer chose the team they had come to trust during their email compromise investigation: The Crypsis Group.

## Crypsis solution

While no company wants a cybersecurity event to occur, occasionally they can serve as a catalyst for the organization to refocus its attention on security and the overall resilience of the company. For one global automotive manufacturer, a business email compromise prompted the enterprise to get more proactive about incident response. They called in the Crypsis experts to assist them in developing an in-depth incident response (IR) plan customized to their unique environment.

The Crypsis team conducted an in-depth review of the manufacturer’s IT environment, security tools, processes, procedures, and documentation. They identified security gaps as well as incident response plan deficiencies and assisted the company in bolstering its security defenses and building a complete, tailored IR plan to better protect the business. Once the teams were comfortable with the IR plan, Crypsis tested the plan through a series of tabletop exercises to better familiarize the teams with the new workstreams and validate that the plan works.

### AT A GLANCE

A large automotive manufacturer needed to strengthen their defenses following a business email compromise, which exposed key gaps in their IR plan. They turned to the Crypsis team for in-depth incident response planning customized to their environment and ongoing IR retainer services.

The organization viewed the retainer and these proactive services as the beginning of a long-term relationship. This client can rely on Crypsis to be ready to assist should a future incident occur. Crypsis created a “Go Book” for the client that provides information for both Crypsis and the client on key contacts, processes, and resources, which will help expedite the response to an incident if needed. A Crypsis “security advisory group” — including staff from risk management, forensics, leadership, and more — meets with the client team quarterly to perform a security health check, make any needed adjustments or assessments (such as vulnerability scans or penetration testing), ensure the “Go Book” is still up to date, and perform periodical tabletop exercises.

## RESULTS

Due to the expertise of the Crypsis team, this manufacturer is better able to defend its IT environment from attack and more quickly and confidently respond to a cybersecurity incident. They now have well-defined, documented, and regularly updated processes and procedures and a team of experts on speed dial who can help in an instant in containing, responding, and recovering from cyberattacks.