# CYBER INCIDENT RESPONSE

## Global Cyber Risk Services

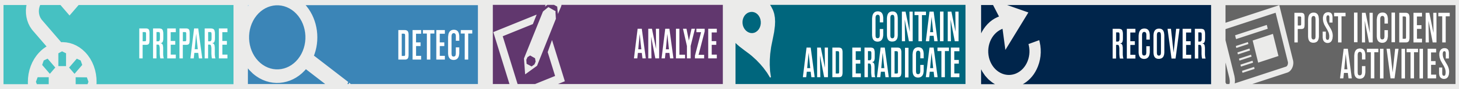
**Alvarez & Marsal has been accredited by the National Security Agency as a Cyber Incident Response Assistance (CIRA) firm.**

**Cyber breaches will happen – we can provide a response that is efficient and effective.**

The frequency and severity of recent cyber threats mean that many organizations' incident response capabilities are no longer adequate. A cyber incident can impact customer relationships and business operations and launch regulatory scrutiny. Stock prices and corporate reputations may be damaged — and recovery can be challenging.

Whatever type of cyber incident you encounter — an employee's inadvertent loss of a laptop, a social media crisis or a serious attack on your network — Alvarez & Marsal's (A&M) cyber security experts will contain the breach, preserve your company's data and address its vulnerabilities. Our global response team of experienced specialists can be onsite within hours and will work alongside your team to increase your ability to solve problems and prevent future losses. We develop incident response frameworks that are distinct to the needs of your company and advise on the numerous risks associated with business operations.

We draw on deep experience in responding to complex crisis situations and anticipating future ones. Our team brings an independent, objective and hands-on approach, providing and implementing recommendations for enhanced cybersecurity policies and measures. Leveraging our significant technical experience, we are skilled in advanced detection and prevention methodologies and provide training for business leaders and law enforcement officials around the world.



PREPARE | DETECT | ANALYZE | CONTAIN AND ERADICATE | RECOVER | POST INCIDENT ACTIVITIES

**A comprehensive incident response plan begins with reviewing the existing plan for gaps, writing a new plan or improving upon an existing plan.**

ALVAREZ & MARSAL

### PREPARE

- Cyber Simulation Exercises
- Risk Assessment
- Policy and Procedure Review / Development
- Deployment of New Security Measures

### DETECT

- Cyber Threat Identification
- Network Monitoring
- Log Review and Analysis

### ANALYZE

- Normal Behaviors
- Gather Network and System Data
- Determine Incident Scope
- Impact Analysis

### CONTAIN AND ERADICATE

- Preserve Evidence
- Triage
- Develop Indicators of Compromise
- Remediation Recommendations

### RECOVER

- Rebuild Systems
- Deploy Patches
- Security Device Reconfiguration
- System Hardening

### POST INCIDENT ACTIVITIES

- Root Cause Analysis
- Monitor for Anomalous Activity
- Persistence Detection
- Reporting
- Lessons Learned

## REPRESENTATIVE EXPERIENCE

A **large hosting company** was the target of a phishing email containing a malicious file link that compromised more than 100 employee computers and the corporate network. A&M established a crisis response center for managing the breach and closed all security vulnerabilities.

The customer website of a **large bank** experienced an attack that acquired and cracked encrypted PIN data, manipulated customer accounts and resulted in a loss of millions of dollars. Working alongside the banking staff, we assisted in the initial response, addressing vulnerabilities and developing a systemic approach specific to banking risks and the customer base.

A **credit card processing company** was the subject of an organized crime attack that targeted full card track data, as well as data out of the credit card processing environment, and used the information to commit massive credit card loss. A&M enhanced the company's ability to detect a variety of vulnerabilities, including the exfiltration of information outside of the processing network.

After determining a breach brought by malware occurred over the course of a year and resulted in significant loss of intellectual property for a **manufacturing company**, A&M developed a cyber crisis action plan to mitigate breach impact and remove intruders from the network. We provided forensic analysis of the compromised systems, identified attack vectors taken by the intruders once inside the company and minimized harm to ongoing business operations.

An **insurance company** experienced a breach that targeted its major data center, impacting customer information, which potentially qualified as a reportable incident, per industry regulations. A&M determined the extent of the breach, developed institutionalized policies and procedures for the company's data center, and created plans for an annual tabletop exercise to prepare staff to respond to potential future incidents.

A **luxury brand company** was allegedly hacked by Chinese organizations attempting to steal the company's intellectual property. We identified the breach location and remedied worm / malware open systems, as well as assessed the overall security posture, identified possible infrastructure vulnerabilities and offered recommendations to protect against future invasions.

For immediate assistance with a cyber breach, contact us at:
**gcrs@alvarezandmarsal.com**

Follow us on:

## ABOUT A&M DISPUTES AND INVESTIGATIONS

Alvarez & Marsal sets the standard for delivering results on critical matters. With an increase in the complexity of corporate investigations, regulatory enforcement actions, and high stakes litigation, that ability is more important than ever. From the boardroom to the court room, A&M professionals draw on their deep skills and experience in business investigations, litigation consulting, forensic technology, and expert testimony to provide clients with the solutions they seek to achieve their goals.

ALVAREZ & MARSAL