

Data Sheet

INCIDENT RESPONSE PLAN DEVELOPMENT

Prepare for the inevitable with a clear response plan

RESPOND TO FAST-MOVING THREATS

The rate at which threat actors are breaching organizations has never been more accelerated. Responding to these fast-moving threats requires thorough preparation. And the first step in cybersecurity preparedness is to have a plan.

IF YOU FAIL TO PLAN, YOU PLAN TO FAIL

When the inevitable cyber incident occurs, ensure that you and your organization are well prepared with a carefully crafted and detailed incident response plan.

A well-thought-out plan puts your cybersecurity incident response on strong footing. Whether your current plan needs revising or you are starting from scratch, the seasoned cybersecurity professionals at Echelon Risk + Cyber are here to guide you.

There is no cookie-cutter approach to incident response planning. After engaging with Echelon, you will have a highly effective plan that reflects your own specific situation and is tailor-made for your unique organization to reflect the capabilities of the people, tools and technology you have in place.

Echelon's cybersecurity experts will help you evaluate your current incident response program and capabilities to create a winning plan that sets you up for success.

KEY BENEFITS:

Highly effective incident response plan: An organized and well-thought-out cyber incident response plan allows your organization to act swiftly in the face of a threat to protect your systems, networks, operations and business reputation.

Strong defensible cybersecurity position: A solid plan signals to investors, regulators, board members and other parties that your organization takes cybersecurity seriously. Having an incident response plan puts you and your program in a strong, defensible position.

KEY SERVICE FEATURES

Incident response plan development is a partner-delivered service from Echelon Risk + Cyber, whose cyber professionals develop a tailored incident response plan that readies your team for cyber resilience.

A well-designed incident response plan takes your current team and organizational capabilities into account. Echelon will work with your team to understand the current state of your incident response capabilities across three planes of enablement: people, process and technology.

Echelon's incident response plans typically include the following sections:

- Roles and Responsibilities
- Incident Handling Process
- Preparation
- Detection
- Containment
- Eradication and Recovery
- Post-Incident Activities
- Severity Levels
- Incident Handlers
- Committees and Teams
- Third-Party Contacts
- Incident Categories and Classification
- Exercise and Testing Program
- Internal and External Communications

ABOUT ECHELON

Echelon Risk + Cyber is a cybersecurity professional services firm built on the belief that privacy and security are basic human rights. Echelon's comprehensive suite of services are customized and right-sized for each client, helping to solve even the most complex cybersecurity issues.

CONTACT CROWDSTRIKE

CrowdStrike: **We stop breaches.**

Learn more: www.crowdstrike.com/services/

Email: services@crowdstrike.com

Request information: [click here](#)

© 2022 CrowdStrike, Inc. All rights reserved.

WHY CROWDSTRIKE PARTNERS WITH ECHELON

CrowdStrike has established an ecosystem of trusted partners to deliver expertise and capacity in key areas of cybersecurity.

Real-world IR experience:

Echelon's team of cybersecurity experts, adversarial emulation engineers and senior defensive engineers all have experience working with organizations that have dealt with cyber incidents and know the importance of effective planning and response processes.

Proven IR maturity model:

Echelon uses a proven and effective incident response capability maturity model to have meaningful conversations with your team and take stock of your existing capabilities.

Tailored IR planning approach:

Echelon will create a highly effective plan that is tailored to your specific situation and reflects the capabilities of the people, tools and technology you have in place.

