FIELD EFFECT / Partners

CYBER DEFENDERS, LLC

Minimize the impact and reduce the costs of a cyber incident

When an incident happens, time is critical. Unfortunately, the more time passes, the greater the impact of the incident. Also, mistakes made even with the best of intentions can increase both cost and impact.

In most cases, the largest obstacles in the way of resolving the incident are trying to figure out what to do and who to involve. Having a plan in place will greatly reduce both the costs involved and the time to recovery should an incident occur, because you will have an actionable plan in place.

In an unprepared organization, undue delays and costly mistakes are much more likely due to the following limitations:

- Lack of internal process and procedures to handle an incident.
- Not knowing who to call and who needs to be involved.
- Lack of data and information about your network.
- Failure to know when and how to act quickly.

Preparing an Incident Response plan is an important and straightforward way to strengthen the maturity of your organization's incident response capacity and ensure that if an incident ever occurs, you know the path to minimize its impact and associated costs.

How it works

An Incident Response Preparedness Exercise ensures that if an attack occurs, the impact to the business is minimized because most of the remediation steps and process to follow have already been identified. The procedures to follow, as well as the stakeholders involved, are documented.

More than just protection and insurance alone, Incident Response Preparedness provides the most efficient path back to business as usual.

PHASE 1

Research and Discovery

Our security team will work with you to assess and identify existing incident response procedures and policies. A review of existing and relevant IT policies and documentation may also be performed.

Field Effect security analysts will review the information to validate any existing plans, and to identify gaps, missing procedures, or technical settings in your network (things as specific as configuration settings, or log retention periods).

Optionally, you may choose to have Field Effect store any documentation provided as supplementary or assistance material for analysis should an incident ever occur.

PHASE 2

Discussion and Review

Following the discovery phase, a detailed and interactive discussion between your team and Field Effect occurs, to review the material from Phase 1, and to further discuss existing measures and monitoring in place.

This discussion also serves as an opportunity for you to ask questions, and for Field Effect to clarify information provided to date.

PHASE 3

Recommendations

The final deliverable within the Incident Response Preparedness exercise is a set of observations and recommendations for implementation. These recommendations will be provided in a written report and include a summary of all information reviewed and catalogued.

These recommendations will:

- Offer notes regarding gaps in internal documentation and procedures. This includes identification of important resources to have available, such as recommendations related to Cyber Insurance.
- Include strategies for safeguarding data, link to best practices, and help ensure cyber security goals and operations are aligned with modern practices and standards.
- Provide prioritized technical recommendations.
- Serve as a resource for guiding your incident response preparation, and for improving the resiliency of your network and business operations.
- At your discretion, Field Effect will also retain the documentation and network architecture information provided to serve as a resource for future services or in the event of an incident.

No one wants to think about a security breach – it's an unpleasant thought, and most IT and InfoSec teams are busy enough as it is. However, the reality is that it does regularly happen, and a little investment now goes a long way should an incident ever occur. Contact Field Effect today to learn more about our Incident Response Services, and how they can help you in the future.

Start securing your business today.

Email:

Phone: