Cybersecurity Incident Response Plan Development Service

- Be prepared for any cybersecurity challenge
- Collaborative development delivers a tailored and supportable IR site plan
- Easy to follow and update IR program handbook

Introduction

Are you comfortable with your cybersecurity emergency incident response (IR) plan? Is it current? Has it been tested? More importantly, do you even have one? Most organizations have developed some form of Disaster Recovery Plan (DRP) but few sites have an Incident Response Plan (IRP) specific to a cybersecurity breach/attack. Unfortunately, for those that have a cyber IRP, those plans quickly become obsolete because they are not kept current. Even worse, many plans are created with a focus on meeting compliance regulations. These plans may please the auditors, but are you willing to bet the company that the plan will guide you through a major security breach?

The Emerson Incident Response Program Team utilizes elements of the Trellix product and services offering and is ready to provide you expert guidance in building a complete IR program. Our IR consultants have deep expertise in collaborative and cross-functional emergency planning. From the initial kickoff interview through plan signoff and adoption, we will deliver confidence throughout your organization and ensure you are prepared for any cybersecurity challenge. Our goal is to help you build a plan that is supportable and works.

IRPs provide instructions for responding to a number of potential scenarios, including data breaches, denial of service/distributed denial of service attacks, firewall breaches, virus or malware outbreaks or insider threats. Without an IRP in place, organizations may either not detect the attack in the first place, or not follow proper protocol to contain the threat and recover when a breach is detected. An IRP can benefit an enterprise by outlining how to minimize the duration of and damage from a security incident, identifying participating stakeholders, streamlining forensic analysis, hastening recovery time, reducing negative publicity and ultimately increasing the confidence of corporate executives, owners and shareholders. The plan should identify and describe the roles/responsibilities of the IR team members who are responsible for testing the plan and putting it into action. The plan should also specify the tools, technologies and physical resources that must be in place to recover breached information.

EMERSON

Benefits

Be prepared for any cybersecurity challenge: A clearly defined and in-place Cybersecurity IRP will help you through those initial tense moments with guidelines on what to do first when you suspect a cybersecurity breach or malware infection. Then, by following step-by-step documented procedures, the IRP will guide you through the steps required to identify, contain and recover from the attack.

Collaborative development delivers a tailored and supportable IR site plan: We combine the skills and experience of our IR and DeltaV specialists with your site's IR team to develop, implement and exercise your specific site IRP.

Easy to follow and update IR handbook: An IR handbook allows you to maintain and keep current the policies and procedures as your system and support team changes. This ensures that you are prepared for any cybersecurity challenge and will ultimately save you time and money during an incident.

Service Description

The Emerson Cybersecurity IRP Development Services team can engage with your site personnel to develop an IRP specific to your site's needs and reporting compliances. We are staffed with some of the best and most experienced IR talent in the business, and we can develop a cybersecurity site IRP specific to your plant or enterprise.

Methodology

Emerson's proven IR program development methodology is thorough, relevant, modular and adaptable. An IR program touches many groups in your organization: security, IT, operations (OT), legal, human resources, compliance and others. Our thorough planning approach is more effective because it is cross-functional and inclusive of all stakeholders. We assure your plan is relevant to your organization because we create a custom plan for each client. Our plan methodology consists of a modular framework, allowing you to choose which components are included. Finally, our plans are adaptable. We produce an IR program handbook that is easy to update. This allows you to keep your plan current as personnel, networks and equipment change.

Emerson's IRP development methodology is specifically design for DeltaV systems. Emerson does not provide Emergency Incident Response services, therefore customers are required to obtain emergency IR services from other service providers before the IRP can be completed.

The Emerson Cybersecurity IRP Development is based on a seven-step process:

1. Client interviews
2. Gap analysis
3. Creation of IR documents
4. Internal IR training
5. Dry-run exercises
6. Management presentation
7. Plan adoption and sign-off

Deliverables

The Cybersecurity IRP Development engagement includes:

- Stakeholder interviews including documented summary notes
- IR Program Document (Policy)
- IR Program Handbook (Procedures)
- Gap-analysis document if needed
- Dry-run exercise(s)
- Management summary presentation

Scope

A typical engagement varies in length depending on the size of the organization, maturity of existing plan, the number of stakeholders and scope. We are committed to your success and are flexible. We will design an engagement strategy that meets your timing, requirements and budget.

Ordering Information

Description	Model Number
Cybersecurity Incident Response Plan Development Service	Contact your Local Emerson Services Representative

Other Related Cybersecurity Services

- Cybersecurity Incident Response and Forensic Investigation Service
- Cybersecurity Site Policies and Procedures Site Development Service
- Cybersecurity Assessment Service
- Integrated Patch Management Service
- Backup and Recovery Service
- Cybersecurity Remediation Service
- Other Emerson Cybersecurity Application Solutions include:
  - Endpoint Security For DeltaV Systems
  - Application Whitelisting for DeltaV Systems
  - Security Information and Event Management for DeltaV Systems
  - Network Security Monitor for DeltaV Systems
  - Threat Monitoring Solutions for DeltaV Systems

This product and/or service is expected to provide an additional layer of protection to your DeltaV system to help avoid certain types of undesired actions. This product and/or service represents only one portion of an overall DeltaV system security solution. Emerson does not warrant that the product and/or service or the use of the product and/or service protects the DeltaV system from cyber-attacks, intrusion attempts, unauthorized access, or other malicious activity ("Cyber Attacks"). Emerson shall not be liable for damages, non-performance, or delay caused by Cyber Attack. Users are solely and completely responsible for their control system security, practices and processes, and for the proper configuration and use of the security products.

To learn more, contact your local Emerson sales office or representative, or visit **www.emerson.com/deltavcybersecurity**.

Contact Us
www.emerson.com/contactus

EMERSON