Including cyber incident response (CIR) as part of your organization’s information environment is a key step in protecting not only important data but also your reputation and operations.

**Key Drivers**
- Increase of cybercrime and data breaches continue to pose major problems for organizations in today’s digital world
- Adversaries create service disruption, attack, and penetrate systems against traditional defense mechanisms
- Adversaries strategically target individuals and corporations for their most valuable asset – data
- Advanced methods of penetrations and breaches are specifically designed to remain dormant and undetected on the network, while they collect and capture valuable information

**Benefits of IR**
- Crisis Management: Neutralize threats as soon as they occur and address the uncertainty crisis creates
- Reduced Risk: Reduce the impact that a data breach can have on your organization by containing the attack
- Intelligent Investigation: Understand the nature of an attack through advanced investigatory means
- Cost Savings: Reduce the cost of data loss
- More Effective Governance: Introduce management rigor and controls that benefit enterprise value

**4 Keys to Cyber Threat Management**
IR is most effective when addressed as part of a comprehensive threat management program. The combination of strategy, people, process, and technology can help you address today’s most advanced threats - both internal and external. The four keys to a threat management program include:
- Defend: Attack mitigation and preparation
- Detect: Threat intelligence and analysis
- Respond: Incident response and containment
- Recover: Incident remediation

Effective IR begins with intelligent investigation:
- Looking at the right things, not necessarily everything
- Following logical leads, not all leads because they exist
- Digging into the data with a precise understanding of the goal of the dig, keeping an eye out for but not getting distracted by the nuggets
- Bringing to bear the right intelligence and information resources
- Applying automation to routine tasks and using analytical techniques that accelerate the investigation

**The Path Forward**
Cyber Incident Response Work Streams

Core areas that apply to most cyber events:

**Compromise Investigation**
- The primary focus of the compromise investigation is to confirm the indicated avenue of the event and identify the post event network activity related to system infiltration and data exfiltration. Additionally, the compromise investigation further attempts to identify additional compromised endpoints and user accounts.
  - Understand potential breadth and scale of the incident
  - Identify locations of potentially compromised systems
  - Identify and examine logs available for the incident
  - Determine any priority systems or logs with a tier based system for further collection and examination
  - Identify if an immediate, remote assessment or collection is required.

**Damage Assessment**
- The damage assessment focuses on ascertaining the data accessed or exposed, as well as providing an understanding of what the adversary sought, and what relevant issues will need to be addressed in future actions. The damage assessment can also provide further guidance on the impact of the data exfiltration on your business.
  - Files accessed
  - Indicators of file use and adversary intelligence gathering
  - Files potentially or actually exfiltrated
  - Adversary’s next steps

**Remediation**
- During remediation, we can help you get your systems back to normal as quickly as possible while ridding the systems of your adversary. Additionally, we use incident indicators and system/application patch levels to identify short-, mid- and long-term remediation efforts that can further bolster your organization’s security posture.
  - Identify exploited known vulnerabilities
  - Identify unknown vulnerabilities
  - Recommend patching and upgrades
  - System off-lining and rebuilding
  - Long term remediation project