# BREACH READINESS SERVICES

GoSecure Breach Readiness Services deliver a comprehensive review of response capabilities and prepare organizations to defend against attacks.

## 3 PILLARS TO PREPARE

GoSecure Breach Readiness Services take a holistic approach to understanding the readiness of an organization to respond to an incident. GoSecure will evaluate:

- Business Continuity
- Incident Response
- Disaster Recovery

The experts at GoSecure believe that to determine if an organization is prepared, the entire program to respond—and all the people, processes, policies, and technology involved—must be evaluated.

GoSecure takes the 3 Pillar approach to preparation because a breach has not been fully addressed until the organization is back to business as usual.

*Osterman Research Survey Report

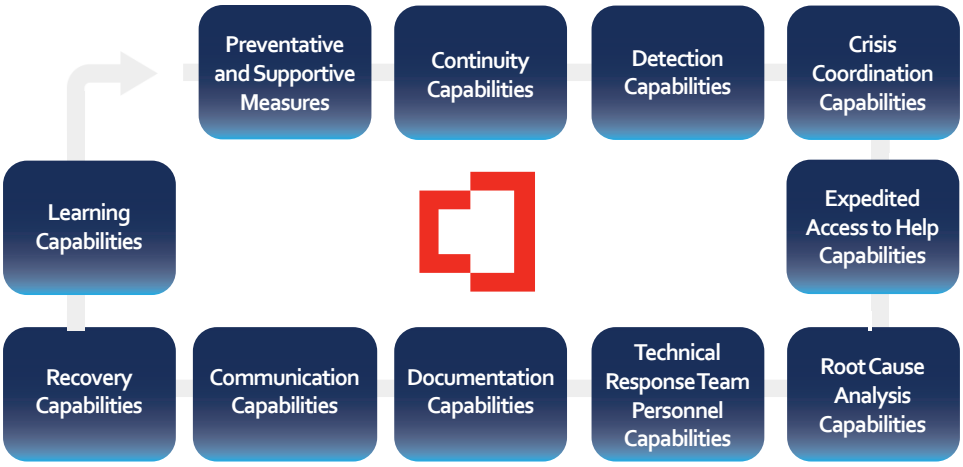
## PREPARE FOR CYBERATTACKS

In a recent survey, 81% of organizations reported being the victim of some type of data breach during the previous 12 months*. Organizations are concerned with rising threats from ransomware, malware, malicious insiders and more. GoSecure offers two Breach Readiness Services to help organizations evaluate their people, processes, policies, and tools positioned to respond in the event of a major incident or crisis.

## GOSECURE BREACH READINESS ASSESSMENT

The **GoSecure Breach Readiness Assessment (BRA)** offers a comprehensive evaluation of incident preparedness ensuring that the people, processes, tools, policies, plans, playbooks and runbooks are ready when a breach happens.

### 11 Critical Concepts of a GoSecure Breach Readiness Assessment




Based on the critical concepts, the skilled and experienced team at GoSecure has developed a proprietary **75-piece Breach Readiness Assessment framework** that deeply examines an organization's capability to prepare for, defend against and respond to an incident or crisis—then learn to improve for the future.

GoSecure experts interview staff and collect available documentation to evaluate the organization's processes, policies, tools, and plans dedicated to incidents, business continuity and disaster recovery. Clients receive a detailed report including their maturity posture score against a target profile.

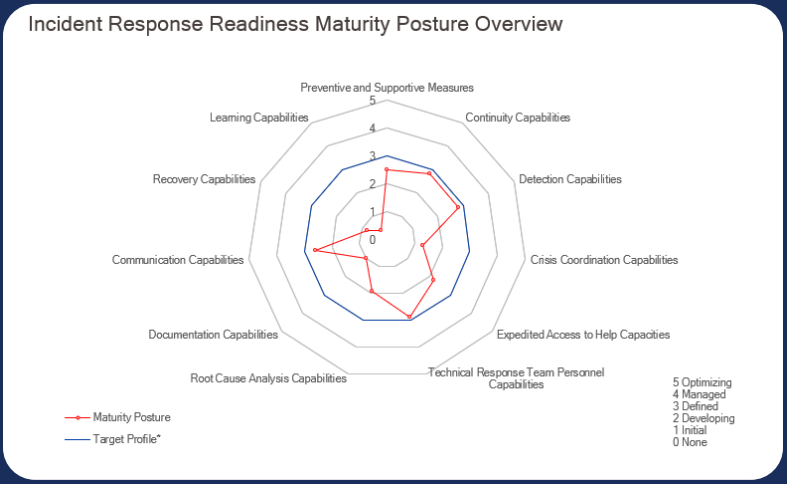
## UNDERSTANDING MATURITY POSTURE

**GoSecure BRA participants get a detailed profile with scores for each of the 11 Critical Concepts from 0—5 (None to Optimizing). The Capability Maturity Model Integration (CMMI) used for scoring is internationally recognized and easy to understand at all levels of an organization.**

**Organizations will identify a target for each aspect of their breach readiness as part of the assessment.**

**This can help teams:**

- **Evaluate current state**
- **Test if improvement efforts have made an impact**
- **Make the case for a bigger allocation of resources in an area for potential improvement**




## GOSECURE TABLETOP EXERCISES

The key to minimizing, containing and recovering swiftly from a ransomware or other attack is preparation. How can an organization evaluate the ability of their people, processes, policies and tools in place under pressure as a real-world major incident unfolds? **GoSecure Tabletop Exercises** offer an opportunity to assess response and recovery capabilities in a safe but realistic environment.

### What are GoSecure Tabletop Exercises (TTE)?

- Custom designed major incidents or crises where key participants (IT/Security, Executive, Operations, HR, Marketing, etc.) engage in role playing to test the organization's ability to respond and recover—as well as learn from the event.

### Who should engage in a TTE?

- GoSecure recommends TTE for clients who have completed a BRA and want to test associated improvements.
- Organizations who want to test team communication, collaboration and decision-making in a real-world, major incident scenario should consider a TTE.
- Many organizations need to complete an annual TTE for compliance or cyberinsurance requirements.

### How does GoSecure design the TTE?

- Each incident scenario is tailored to the client industry, geography, technology, personnel, etc.
- GoSecure will collect available documents such as the Incident Response Plan, Business Continuity Plan and Disaster Recovery Plan—as well as interview the IT team to determine the best weaknesses and flaws to exploit in the exercise and challenge participants.

### What results should an organization expect from a TTE?

- The GoSecure approach includes facilitated discussions throughout the exercise and a lessons learned session when the theoretical incident is resolved.
- After the session, clients get a report with improvement recommendations—as well as minutes and a recording of the session.

GoSecure

### LEARN MORE

www.gosecure.net/breach-readiness-services

### CONTACT US

www.gosecure.net/sales-contact

1-855-893-5428

### ABOUT GOSECURE

GoSecure is a recognized cybersecurity leader and innovator, pioneering the integration of endpoint, network, and email threat detection into a single Managed Detection and Response service. The GoSecure Titan platform delivers predictive multi-vector detection, prevention, and response to counter modern cyber threats. Titan MDR is designed to detect and respond in less than 15 minutes, delivering rapid response and active mitigation services that directly touch the customers' network and endpoints. For over 10 years, GoSecure has been helping customers better understand their security gaps and improve their organizational risk and security maturity through MDR and Advisory Services solutions delivered by one of the most trusted, skilled and experienced teams in the industry.

To learn more, please visit: https://www.gosecure.net.