Incident Response Tabletop Exercise

Bishop Fox Incident Response Tabletop Exercises enables your organization to accurately evaluate incident response readiness by immersing your key stakeholders in realistic and customized threat scenarios designed specifically for your business.

EXPERT DEVELOPMENT & GUIDANCE

Put your Incident Response Plan to the Test

While most organizations now have some form of incident response plan in place, the effectiveness of these plans are often unknown. Bishop Fox Incident Response Tabletop Exercises enable your organization to accurately evaluate incident response readiness by immersing participants in realistic and customized threat scenarios.

Bishop Fox’s world-class Red Team works closely with your organization to develop scenarios in line with trends in the threat landscape and industry-specific risks, ensuring a realistic and relevant test of your incident response plans. We leverage our extensive experience working with clients across many industries, to facilitate a collaborative process that encourages stakeholder participation and delivers an accurate assessment of your readiness, identifying any critical gaps in your strategy.

KEY OUTCOMES

- Enhanced Incident Preparedness
- Informed Decision-Making
- Objective Evaluation
- Compliance Documentation
- Time & Cost Efficiency
- Engagement & Collaboration

HOW IT WORKS

Incident Response Tabletop Exercise Workflow

1. Planning & Preparation
   - Customer provides IR process & procedures documentation
   - Discovery & scenario development meetings
   - Tabletop exercise development & approval
   - Engagement scheduling

2. Facilitation
   - Tabletop exercise
   - Debriefing
   - Anonymous post-exercise survey

3. Reporting
   - Report
   - Cyber IR Readiness score
   - Post-engagement meeting
   - Recommendations
Impactful Insights to Evolve Your Strategy

Tailor-made to Your Objectives

Bishop Fox offers a “building block” approach to red team services that can include an IR Tabletop Exercise and any combination of the following methodologies:

<table>
<thead>
<tr>
<th>Assessment Knowledge Types:</th>
<th>Methodologies:</th>
<th>Example:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Knowledge</td>
<td>External Breach Red Team</td>
<td>Ransomware Readiness</td>
</tr>
<tr>
<td>Partial Knowledge</td>
<td>Physical Breach Red Team</td>
<td>Purple Team</td>
</tr>
<tr>
<td>Zero Knowledge</td>
<td>Continuous1</td>
<td>Red Team Program Build</td>
</tr>
<tr>
<td></td>
<td>Tabletop Exercise</td>
<td></td>
</tr>
</tbody>
</table>

1 (Multi-phase Red Team, Purple Team, Ransomware Readiness)

CLIENT SATISFACTION

6000+ Offensive Security Projects Delivered

1000+ Global Customers Protected

81 Net Promoter Score

16+ Years of Experience

Trusted By Industry Leading Organizations

Amazon  EQUIFAX  SONOS

August  CHANGE Healthcare  Google

Recognized as a Leader in Offensive Security

About Bishop Fox

Bishop Fox is the leading authority in offensive security, providing solutions ranging from continuous penetration testing, red teaming, and attack surface management to product, cloud, and application security assessments. We've worked with more than 25% of the Fortune 100, half of the Fortune 10, eight of the top 10 global technology companies, and all of the top global media companies to improve their security. Our Cosmos platform, service innovation, and culture of excellence continue to gather accolades from industry award programs including Fast Company, Inc., SC Media, and others, and our offerings are consistently ranked as "world class" in customer experience surveys. We've been actively contributing to and supporting the security community for almost two decades and have published more than 16 open-source tools and 50 security advisories in the last five years.

Learn more at bishopfox.com
Follow us on @