CYBER RESILIENCE

Cyber Recovery Retainer

Turn the Worst Week of the Year Into Lasting Security Improvement

Most organizations finish a breach with a forensic report and a remediation backlog. Few convert the incident into durable program maturity.

01 — THE CHALLENGE

Cyber incidents do not end when the forensic engagement closes. The following 90 days often determine whether the organization genuinely hardens or quietly returns to its previous operating state.

Many response partners leave after the active incident. The organization is left with remediation findings, an exhausted executive team, and no structured path to convert lessons learned into stronger controls and governance.

02 — WHY ARCTIQ

Arctiq's Cyber Recovery Retainer focuses on pre-incident readiness and post-incident transformation.

Before an incident, we help organizations prepare through breach scenario planning, executive pre-briefings, IR plan alignment, and tabletop history review. During an active incident, Arctiq supports the client's existing incident response partners, breach coach, and counsel-led response without disrupting qualified forensic or crisis-management teams.

> Where Arctiq leads is the structured 90-day transformation following the incident. If no incident occurs during the retainer year, capacity converts into a tabletop exercise, Defense Assessment, premium service, or workshops. Retainer capacity is never lost.

03 — ADVISORY CAPABILITIES

- Breach scenario and readiness planning
- Executive and board pre-briefings
- IR plan alignment
- Ransomware decision trees
- Cyber insurance and breach counsel escalation paths
- Post-incident lessons-learned synthesis
- Root-cause remediation planning
- Detection engineering against observed TTPs
- Identity and privileged access hardening
- Segmentation and resilience improvements
- Tabletop validation of rebuilt capabilities

RETAINER SCOPE: **Breach Readiness** · **90-Day Transformation** · **Insurer Coordination** · **Detection Engineering** · **Identity Hardening**

04 — BUSINESS OUTCOMES

Organizations gain:

- ✓ Greater readiness before an incident
- ✓ A structured 90-day post-incident improvement program
- ✓ Prioritized control and governance improvements
- ✓ Stronger identity, detection, and resilience capabilities
- ✓ Measurable security maturity following an incident
- ✓ Flexible retainer value even when no incident occurs

05 — WHY IT MATTERS

An incident should create more than a remediation backlog. Arctiq helps organizations convert hard-earned lessons into stronger governance, hardened controls, and lasting program maturity.

Discuss a recovery retainer →

www.arctiq.com