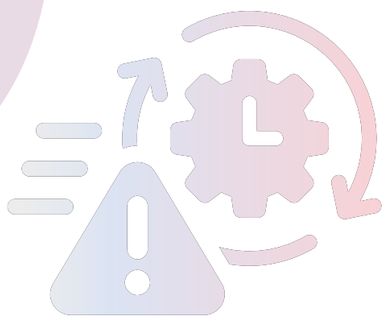
Incident Response Readiness That Reduces Risk

A Strategic Briefing for CISOs, CTOs, Legal Counsel, Risk Officers, and Crisis Management Leads. Fast, tested incident response reduces breach impact, cost, and regulatory risk.

CREST Registered Region - Global

VA PEN TEST

certin Empanelled



Incident Response Services

What the Data Says About Incident Response Speed

Real differences in outcomes between prepared and unprepared organizations.

$1.49M

Average Savings Per Breach

For organizations with tested IR plans vs. those without (IBM). Preparation pays back within the first avoided incident.

258

Days Average Dwell Time

Average time to identify and contain a breach without dedicated response capability. With a tested IR plan, organizations reduce this to weeks.

77%

Untested IR Plans

Percentage of organizations that have not tested their incident response plan. Most boards are discovering this gap before — not during — on incident.

$4.88M

Global Average Breach Cost

Healthcare: $7.42M to $9.77M.
US-based: $9.36M to $10.22M.
Costs rise sharply with every additional day of dwell time. (IBM)

Containment Cost: Early vs. Late Response

Response speed directly correlates with breach cost.

200 Days

Breaches contained under 200 days average significantly lower cost vs. those over 200 days (IBM).

$5.46M

Average breach cost when dwell time exceeds 200 days.

4-Hour

SI.A for Briskinfosec retainer clients — the window separating a contained incident from a cascading crisis.

6-Hour

CERT-IN mandatory breach notification window for indian organizations.

Key Insight

The consistent pattern: organizations without tested IR plans extend dwell time, lose forensic evidence, miss regulatory notification windows, and face higher insurance scrutiny. **The cost difference between prepared and unprepared is not marginal. It is foundational.**

Five Leadership Assumptions That Delay Incident Response

These are not misconceptions to correct.
They are reasonable assumptions that need updated context.

WHAT YOU THINK	THE REALITY
01 **"We can handle an incident with our existing IT team."** This is a common starting point, and it makes sense given that IT manages most day–to–day security operations.	Cyber incident response requires digital forensics, maiware analysis, evidence preservation, and regulatory compliance that are distinct from IT work. Organizations using IT teams for IR consistently extend dwell time and miss key indicators of compromise.
02 **"We will call a response firm when we need one. We do not need a retainer."** This is a practical position, and one many CFOs take during budget planning.	During an active incident, IR firms prioritize retainer clients. Organizations without pre–established agreements join a queue. A 4–hour SLA response requires a retainer relationship, not a cold call during a crisis.
03 **"Our cyber insurance covers all IR costs, so we do not need to plan."** Insurance is an important part of the risk picture, and worth understanding precisely.	Cyber insurance covers costs of an approved, documented response. Coverage depends on meeting notification timelines, using approved firms, and maintaining chain of custody. Organizations without IR plans often void key provisions.
04 **"Shutting down all systems immediately is the right first response."** This feels like the safest action under pressure, and it is how most untrained teams respond.	Immediate shutdown destroys volatile memory evidence — running processes, network connections, and encryption keys critical to understanding the full attack. Proper containment preserves evidence while limiting attacker movement.
05 **"Once the ransomware is removed, we are safe."** This is a logical assumption ofter a visible threat has been addressed and systems are restored.	Ransomware is typically the final stage of a multi–week intrusion. Initial access vectors and persistence mechanisms may still be active. Without a full compromise assessment, re–infection risk remains high.

Building an Effective Incident Response Framework

A structured approach ensures faster containment, regulatory compliance, and reduced impact.

Regulatory Notification Timelines

CERT-IN (India)

6 Hours

Mandatory reporting for significant cyber incidents under the IT Act, 2000 and CERT-In Directions.

GDPR (EU)

72 Hours

Personal data breach must be reported to the supervisory authority within 72 hours of awareness.

SEBI (India)

6 Hours

Cyber incidents impacting stack exchanges, clearing corporations, and market infrastructure.

DORA (EU)

4 Hours

ICT-related incidents must be reported to the competent authority without unreasonable delay.

The Six Phases of Incident Response

Based on NIST 800-61 Rev. 2 Framework

01 Preparation

Establish policies, assign roles, conduct training, and ensure the right tools, playbooks, and partnerships are in place.

02 Detection & Analysis

Identify suspicious activity early through monitoring, alerting, and threat intelligence correlation.

03 Containment

Limit the impact by isolating offected systems and stopping the spread while preserving critical evidence.

04 Eradication

Remove the roat couse of the incident, including malware, persistence mechanisms, and attacker access.

05 Recovery

Restore systems and operations in a secure monner with proper validation and monitoring.

06 Lessons Learned

Conduct a past-incident review to document findings, improve controls, and strengthen future readiness.

Why It Matters

Clear timelines and a tested response fromework enable organizations to oct decisively, meet regulatory obligations, preserve evidence, and minimize business disruption.

From Reactive Response to Operational Readiness

A mature incident response capability strengthens compliance, reduces risk, and improves organizational resilience.

Key Regulatory Frameworks

CERT-IN (India)

6-hour reporting for significant cyber incidents.

Mandatory under IT Act, 2000 and CERT-In Directions.

GDPR (EU)

72-hour notification for personal data breaches.

Applies to all organizations handling EU citizen data, worldwide.

SEBI (India)

6-hour reporting for cyber incidents.

Applies to stock exchanges, clearing corporations, and market infrastructure.

DORA (EU)

4-hour reporting for ICT-related incidents.

Applies to financial entities and their critical third parties.

Current State vs. Future State

Current State		Future State
Unplanned and reactive	→	Proactive and prepared
High dwell time (months)	→	Low dwell time (days/weeks)
Higher breach costs	→	Reduced breach costs
Regulatory penalties	→	Regulatory compliance
Reputational damage	→	Stakeholder confidence
Operational disruption	→	Business continuity

Business Impact: The Value of Being Prepared

$1.49M

Average Savings Per Breach

Organizations with tested IR plans save an average of $1.49M per breach compared to those without (IBM).

EUR 20M

Potential GDPR Fine Exposure

Violations can result in fines up to EUR 2BM or 4% of global annual turnover, whichever is higher.

22 Days → 4–6 Days

Faster Recovery with IR Readiness

Prepared organizations recover in 4–6 days vs. 22 days for those without a plan.

31%

Less Likely to Lose Customers

Strong incident response reduces customer attrition by up to 31% after an incident.

Key Takeaway

Preparedness is not just about compliance — it is a strategic advantage that reduces cost, builds trust, and ensures business continuity.

What Proactive Incident Response Protects

Incidents are inevitable, but their impact is not.
Prepared organizations protect what matters most.

01

Financial Impact

Reduce breach costs and avoid unnecessary expenses.

$1.49M

Average Savings Per Breach

Organizations with tested IR plans save an average of $1.49M per breach compared to those without. (IBM)

02

Compliance Impact

Meet regulatory obligations and avoid severe penaities.

EUR 20M

Potential GDPR Fine Exposure

Non-compliance can result in fines up to EUR 20M or 4% of global annual turnover, whichever is higher.

03

Operational Recovery

Minimize downtime and restore operations faster.

22 Days → 4–6 Days

Faster Recovery with IR Readiness

Prepared organizations recover in 4–6 days vs. 22 days for those without a plan.

04

Customer Trust

Maintain confidence and strengthen brand reputation.

31%

Less Likely to Lose Customers

Strong incident response reduces customer attrition by up to 31% after an incident.

05

Business Continuity

Ensure critical business functions continue with minimal disruption.

Stronger Resilience

A tested response capability ensures business continuity, safeguards revenue, and protects long-term growth.

Bottom Line

A proactive incident response program does more than contain incidents — it protects your business, people, and future.

What a Cybersecurity Incident Response Partner Should Deliver

The right partner brings the capability, speed, and experience to contain incidents and strengthen your resilience.

Capability	Briskinfosec Advantage	Typical Service Providers
Response SLA	**4-Hour SLA for retainer clients** Ensures faster containment and reduced impact.	**8–24 hours or best effort** Slower response increases dwell time and damage.
Forensics & Investigation	Advanced digital forensics, malware analysis, and evidence preservation with certified experts.	Limited forensics capability or reliance on third parties.
Regulatory Coverage	Expertise across CERT-In, QDPR, SEBI, DORA, HIPAA, PCI DSS, ISO 27001, and more.	Limited regulatory knowledge and narrow compliance focus.
Insurance Support	Pre-approved by leading insurers with experience in claim support and documentation.	Limited or no insurance coordination and support.
Post-incident Support	Lessons learned, gap analysis, and roadmap to improve future incident readiness.	Incident closure only, no long-term improvement focus.
Accreditations	**CREST Approved, CERT-In Empanelled, ISO 27001:2022 Certified GCFA | GCFE | GNFA Certified Team**	Limited certifications and credentials.
End-to-End Capability	From preparation to recovery — complete incident lifecycle support.	Partial services across the incident lifecycle.

Our Accreditations

- **CREST** Approved
- **CERT-IN** Empanelled
- ISO 27001:2022 Certified
- **GCFA \| GCFE \| GNFA** Certified Team

Proven Impact. Trusted by Global Organizations.

- **540+** Clients — Across 20+ countries
- **4,800+** Security Assessments — Delivered globally
- **0%** Client Breach Rate — Post-engagement
- **99.8%** Compliance Rate — Across 50+ frameworks

Why It Matters

Choosing the right incident response partner reduces risk, ensures compliance, and builds long-term organizational resilience.

What Happens Next?

Client Breaches
Post-assessment security record

Start With Zero Commitment

Understanding your unique security challenges begins with a conversation. We offer a no-obligation consultation to assess your current posture and identify immediate risk areas.

Our Team Holds Industry-Leading Certifications

We invest heavily in our team's continuous education because the threat landscape never stops evolving. Neither do we.

OSCP | OSWE | CISSP | CISA | CEH

CREST Accredited
Internationally certified penetration testing excellence

CERT-IN Empanelled
Government-recognized trusted cybersecurity assessment provider

ISO 27001 : 2022 Certified
Our own security practices are independently audited and verified annually

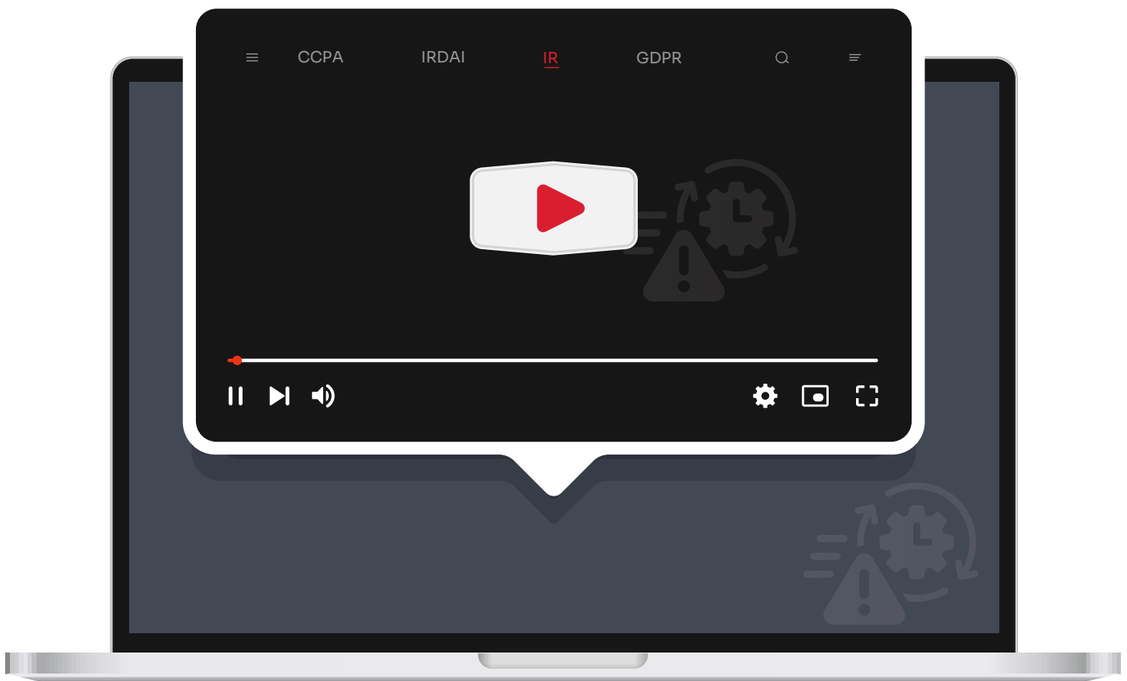
25+
Countries Client Portfolio

67%
Logic flaws missed by bots

98%
Client retention

640+
Successful Customers

5600+
Delivered in 24 countries



Reach us for FREE

consultation

Book Now

sales@briskinfosec.com
www.briskinfosec.com

Our Geographical Presence India UAE