



Cyber Response Solutions

Industry-leading full service incident management to fit your unique needs

IDX clients benefit from our comprehensive, end-to-end management of preparing, containing, and responding to any type and size of cyber attack. With one seamless, full service team, IDX eliminates the need to patch together multiple vendors, providing services that cover the full spectrum of needs around incident readiness and response.

Incident Readiness Services

As cyber threats are increasing in frequency and complexity, incidents can have devastating effects to an organization's bottom line and reputation. Organizations need to be prepared to respond quickly and effectively to reduce the impact of incidents, while enhancing stakeholder confidence, regulatory compliance, and overall security posture.

INCIDENT READINESS SERVICES

- Threat Hunt (TH)
- Tabletop Exercise (TTX)
- Incident Response Capabilities Assessment (IRCA)
- Ransomware Readiness Assessment (RRA)
- Malware Analysis (MA)
- Purple Team Exercise (PTE)
- Intelligent Pen Testing (IPT)

DARK OPS ENGAGEMENTS

- Dark Web Investigation
- Digital Asset Inquiry, Transaction, and Recovery
- Ransomware Data Download, Defusing, & Delivery
- (with optional data mining)

ON-DEMAND INVESTIGATIONS

- Executive Threat Assessment
- Person of Interest Investigation
- Background Check Investigation
- Attack Surface Assessment
- Phishing Kit Analysis
- Supply Chain & Third-Party Risk Assessment
- Industry Threat Landscape

EXECUTIVE & EMPLOYEE PROTECTION

- PII Removal
- PII Removal + Social Media + Dark Web + Physical Security

THREAT INTELLIGENCE

- Deep & Dark Web / Identity & Fraud / Network & Vulnerability
- Raw or Finished





Incident Response Services

Security incidents cost an organization time, money, reputation, and customers. A swift response is critical in minimizing the impact, protecting customer trust, maintaining business continuity, and meeting regulatory compliance. Our team of experts mobilizes efficiently and timely to mitigate the damages caused by a cyber attack.

DIGITAL FORENSICS & INCIDENT RESPONSE (DFIR)

Investigations with Remediation

- Business Email Compromise (BEC)
- Ransomware and/or Data Extortion
- Advanced Persistent Threat & Insider Threat
- Phishing & Malware
- DoS, DDoS & Supply Chain Attack

Threat Actor Communications

- Payment Negotiation & Facilitation (no payment transfer)
- Leaked Data Recovery & Decryptor Testing

Data Recovery & Restoration

- Full Disk Decryption
- Cloud and/or On-Premises
- Virtual and/or On-Site Support

DOMAIN TAKEDOWNS & RECOVERY

- Domain Takedown and/or Hijacking Recovery
- ZeroFox Global Disruption Network (GDN) Add-On
- Uniform Domain-Name Dispute-Resolution Policy (UDRP)

DEEP, DARK WEB, & DOMAIN MONITORING

- Post-Ransomware Monitoring for Exfiltrated Data
- Monitoring of Ransomware Leak Site
- Data Breach Class Actions - Named Plaintiffs
- Attacker Chatter, Phishing & Ransomware Staging

DATA MINING & REVIEW

Structured and/or Unstructured Data Processing

- Bulk ingestion and summary reporting

Phase I - Data Mining & E-Discovery

- Bulk data processing and reporting
- Search term analysis and reporting (PII; PHI; PCI; Custom)

Phase II - Data Review

- Offshore manual review with onshore project management & quality control -OR-
- Full onshore manual review, project management & quality control

Phase III - Consolidated Entity List Creation

- Includes complete document mapping & geo summaries
- Filterable for quick breach notification list creation

Phase IV - Reporting, Portal Access & Data Deletion

- Fully customizable timelines

Phase V - Identity Validation & Advanced Address Lookup

- Verify or update PII (including date of death)
- Update or complete best mailing address

BREACH NOTIFICATION, CALL CENTER & IDENTITY PROTECTION

Fully Managed, Supported, & Serviced

- Dedicated project manager coordinates and ensures a successful "go-live"
- Dedicated client success manager provides support through the entire event

Notification Support (US & International)

- Address cleanup, updating & validation (CASS + NCOA)
- Advanced address lookup (optional)
- Mailhouse fulfillment (letters & envelopes)
- First-class postal delivery & returned mail handling
- Email delivery
- Custom enrollment website
- Fully customizable reporting and remailing options

FAQ Call Center Support (US & International)

- Toll-Free, 9am-9pm ET + 24/7 availability
- Custom FAQ scripts
- Language/translation support as-needed

Identity Protection Services (US & International)

- 1 or 3 bureau credit monitoring (US, Canada, Australia, & UK)
- Cyberscan dark web monitoring (global)
- Account takeover & compromised credentials (global)
- Protection and monitoring for minors (excluding credit monitoring)
- Up to \$1M in identity theft insurance policy (US & Canada only)



IDX is a leading provider of identity protection and cyber response services for companies and individuals throughout the U.S. We combine consumer-centric software and concierge-style professional services in serving organizations across government, healthcare, commercial enterprises, financial institutions, and higher education.



**Have questions?
We'd like to help.**

 855-HELP-IDX

 response@idx.us