ZDL GROUP

Incident Response Preparedness

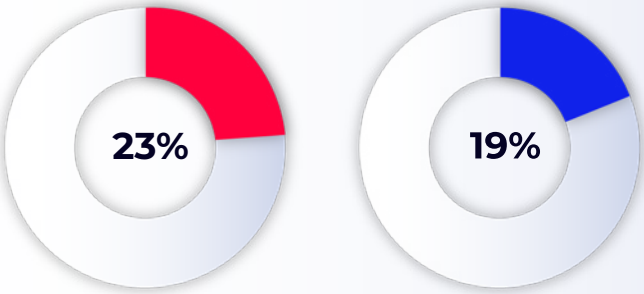
www.zdlgroup.com

Cyber Incident Prevention Planning, Support & Training

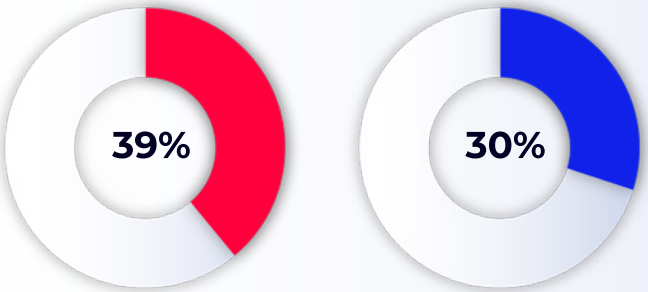
Incident Response Preparedness is designed to raise your organisation's resilience in the event of a crisis and/or breach to minimise the impact of an attack. Pre-Incident preparation is key and this is why we focus on Pre-Incident only services.

Assessing your capabilities for managing an incident, developing the right processes to put in place to manage, then training those with crucial roles to play before they happen, are core to the ZDL approach for Incident Management. From Policy and Plan reviews & creation to Runbook Crafting to Training and Desktop Simulations, preparing for the attack before it strikes protects business continuity and reduces the level of monetary damage that could occur.

Fewer than a quarter of businesses or charities have a formal cyber security strategy in place. [1]

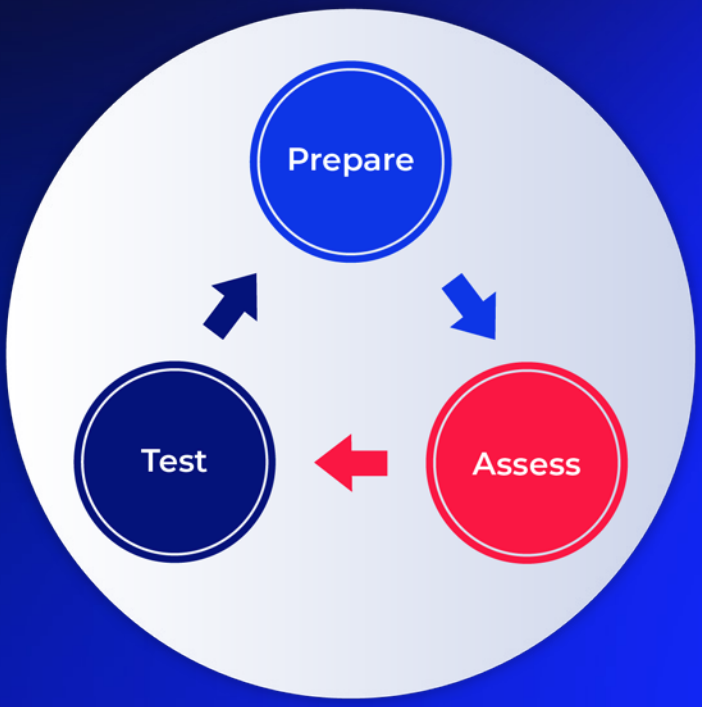


Around four in ten businesses and a three in ten charities report having any kind of cyber security breach or attack in the last 12 months. [1]



Prepare

Reduce the impact of an attack through training and response planning. Identify attack scenarios and define processes for response, tailored to your organisational needs. Train team members from across departments, from Security and IT to the Board & Communications, to work in a cohesive unit to help you protect your customers and financial and reputational position.



Test

The most effective way to understand if your organisation is prepared for a significant cyber incident is to regularly test your incident plan, runbooks, controls and how your teams respond through both desktop and technical incident simulations.

Assess

How ready is your organisation for an attack? Get attack-ready by assessing the process and response gaps in your business - before an attack happens. Ideally assessments should take place on an annual basis to accommodate for team and business structure changes.

Incident Response (IR) Preparedness Packages

Attackers are evolving tactics constantly and Incident Response Preparedness activities should be conducted every year to ensure you are ready for those perfect storms. For on-going resilience, our annual plans help businesses ensure that their incident planning and preparation stays current with changes in business strategy, departments, teams, and the latest threats.

We suggest three different levels of Packages but can of course create a Bespoke Package as well. Pricing is determined by many factors such as the size of organisation, number of participants in certain activities, the current cyber maturity of the business, existence of policies and/or Incident Response Plan etc...

Platinum

The Complete Package of Full Incident Response Preparedness through Reviews, Creation, Training and Desktop as well as Technical IR simulation, and Dark Web Analysis includes:

- IR Management Review – Policy/Plan Creation
- Runbook Review/Creation & Training
- First Responder Training
- Digital Forensics Fundamentals Training
- Desktop IR Scenario Training
- IR Capability Assessment
- Technical IR Simulation
- Open Source Intelligence (OSINT)/Cyber Threat

Gold

A Mid-Level Package to ensure more than the basics are covered includes:

- IR Management Review – Policy/Plan Creation
- Runbook Review/Creation & Training
- First Responder Training
- Digital Forensics Fundamentals
- Desktop IR Scenario Testing

Silver

Entry Level Package to get started with a Review, Policies and Training to include:

- IR Management Review – Policy/Plan Creation
- Runbook Review/Creation & Training

Maybe your organisation already has certain items in place?
We can create a Bespoke Pre-Breach Package that's right for you.

Delivering Excellence in Cyber Security

At ZDL, we believe that effective risk management requires a holistic 360° approach. We take a comprehensive view of our clients' cyber security risks and provide quality services to address those risks.

Our approach to Total Security Management helps make our clients' infrastructure, applications and data more secure in the face of a continually evolving Threat Landscape. Our aim is to build a partnership with our clients, built on a mutual respect and understanding of each other's businesses. We become a part of our clients' team, a valued partner; an intrinsic part of their business.

ZDL's 4 key service areas are designed to focus on our clients' cyber resilience journey. Our unique portfolio of services enables you to build an agile, responsive security infrastructure and strategy.

Our Services

Ethical Hacking

- Broad Security Review
- Red Teaming
- Security Audits
- Penetration Testing
- Cloud Security & Security Ops Testing
- Source Code Review/Coding Standards
- Social Engineering
- Physical Security

Training

- Security Awareness Programmes
- Secure Coding School for Developers
- Bespoke Senior Exec Security Training
- Runbook training/ Scenario Workshops
- Phishing & Resilience Programmes
- Physical Security Awareness
- Online Assessment / CBT Developer Training

Managed Services

- Supplier Evaluation Risk Management (VenDoor)
- Incident Response Preparedness
- Security Training for Developers - Annual Programme
- Managed Detection and Response (MDR)
- Virtual Information Security Manager
- OSINT/Threat Intelligence

Compliance

- Policy Review & Creation
- 360° Assessment
- PCI Remediation Support
- ISO/ NIST/EU GDPR Standards Agreement
- Business Continuity Management
- IR Management Review
- ISO Readiness Programmes
- Office365 Configuration Review

CONTACT US →

[1] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022

www.zdlgroup.com

London | Brighton | Manchester | USA