Cyber incident readiness & response retainer

Helping you plan for and respond to cyber attacks

Boards, regulators, customers and investors recognise that cyber attacks present a significant threat. Their scale and sophistication is constantly evolving, and keeping pace with the techniques and procedures used by attackers can feel like an impossible task.

Having the right preparation and expert guidance ready to support your team provides confidence that cyber incidents need not turn into cyber crises.

More than a technical response

We understand that incidents require more than technical expertise. The rapid rise in destructive ransomware attacks demands experts in readiness, crisis recovery of IT operations, and executive-level technical incident management to deliver an effective response.

That's why our Incident Response capability includes PwC experts from legal, crisis management and public & media relations, to help you handle each component of a complex response.

We approach your response holistically to provide decision makers with a single view of facts with developments, risks and recommendations. This ensures that your entire business, not just your IT departments, emerge from incidents stronger and more resilient.

PwC can support your executive team in response to cyber incidents

- Stakeholder engagement
- Government and regulatory affairs
- Business continuity
- Communications
- Legal advice

The right preparation

We believe that ‘readiness’ is critical to help respond to an incident. Our retainer service is designed to prepare you and your teams for an incident long before it happens. When it does happen, our team will mobilise rapidly to help you respond – executing the process that we have designed and practiced with you.

Our readiness services cover both technical and non-technical aspects of the response process and include workshops, training and simulation activities to address gaps in systems and processes. We can help you develop truly cross functional incident response governance, with plans and strategies across technical cyber security, regulatory, law enforcement and media relations.

Our incident response capablity

650+

Digital forensics, incident response & threat research staff globally

600+

Incident response cases per year

40

Countries across our incident response network

Why PwC

We help our clients respond to incidents of any scale and sophistication. We have extensive experience responding to attacks involving ransomware gangs, cyber crime, insiders, and state affiliated threat actors.

We have worked closely with law enforcement and the New Zealand Government on sensitive incidents. Our Incident Response team hold NZ Government clearances enabling them to investigate compromises of sensitive IT systems.

Our legal practitioners have worked closely with NZ and international regulatory bodies for our clients. We understand the legal risks associated with an incident, including regulator breach reporting, cyber insurance and third party exposure.

What's included

- Access to a 24x7 incident hotline
- Onboarding workshop to understand your existing incident response processes, your IT systems and your core 3rd party suppliers
- Onsite support in New Zealand and around the world
- Custom Service Level Agreements to suit your business requirements
- Prepaid hours to use on any of our incident readiness & response services
- If these options do not fit your unique needs, we can provide you with a tailored retainer solution

Each tier includes the services listed above and a our silver and gold tiers include a set amount of prepaid hours to be used on our core digital forensics and incident response (DFIR) services, readiness services, cyber threat services or legal services.

Silver
40 hours

Gold
80 hours

Prepaid hours can be used on our core digital forensics and incident response (DFIR) services, readiness services, cyber threat services or legal services.

PwC incident readiness & response services

- Root cause analysis & post-incident reviews
- Incident containment
- Dark web monitoring
- Malware reverse engineering
- Intrusion detection & log analysis
- Forensic acquisition
- Incident playbook development
- Forensic readiness
- Game of Threats™
- First responder training
- Ransomware readiness assessment
- Crisis and incident simulations
- Threat hunting
- Threat intelligence
- Threat assessments and profiling
- Red teaming
- Penetration testing
- Architecture review
- Regulatory advice for notifiable data breaches
- External communications
- Engagement and management of foreign legal counsel*
- Cyber insurance policy assistance
- Advice regarding impacted supply, customer and other arrangements

*Does not include foreign legal assistance.

Key

- DFIR services
- Readiness services
- Cyber threat services
- Legal services

What PwC incident response looks like

Tailored reporting

From detailed technical analysis to executive-level briefings, to ensure every stakeholder understands the incident and the resulting impact.

Tool-agnostic incident response

We will work with your existing teams, systems and tools to respond to any incident.

A global footprint to match yours

Our global network of firms means we can respond to incidents wherever you operate.

Incidents of any size

We can help you respond to any incident, whether it's a large-scale ransomware attack, or a sensitive insider threat.

Backed by leading global threat intelligence

Our expert incident response and threat intelligence teams have years of experience identifying and responding to a range of incidents on some of the world's most sensitive networks.

Assistance with communications

We can help translate technical detail into business and risk language for communication with customers, regulators, and internal stakeholders such as business unit leaders and affected employees.

Helping a large corporation recover from a ransomware attack

Incident response

PwC established a 24x7 response team, working with the client's internal teams and vendors to contain, eradicate and recover from the attack.
PwC leveraged its global network to deliver 24-hour incident response support, which involved forensic acquisition and imaging, malware analysis and root cause analysis and investigation.

Legal support

PwC provided a team of legal specialists to assist the client in responding to legal challenges arising from the ransomware incident, including cyber insurance, regulatory notifications across the globe and other related legislative requirements.

Executive support

PwC also provided executive-level briefings and updates on the progress of the investigation.

System recovery assistance

PwC provided strategic and technical support in securely recovering impacted systems post-incident. PwC technical resources performed vulnerability assessments and malware scans to ensure that client systems were safely recovered.

Craig Maskell
Partner
Cyber
+64 21 915 380
craig.a.maskell@pwc.com

Tum Meksikarin
Associate Director
Cyber
+64 22 163 1992
tum.x.meksikarin@pwc.com

www.pwc.co.nz/services/cyber-security