Introducing Cyber 360

MARKEL

Welcome to Markel!

As a Markel policyholder you get more than just indemnity from us. We have designed Cyber 360 to safeguard your business before, during and after a cyberattack, and we do more than just protect and promise to pay.

Cyber is in our DNA.

Markel has been underwriting cyber liability insurance for more than 40 years. While the nomenclature has changed—"unauthorized computer access" insurance is now "cyber" and "electronic pirates" are now called "hackers"—our commitment to protecting you has never wavered.

As a policyholder you now have access to specialist resources and tools which will enable you to improve your cyber risk management and safeguard your business, all at no additional cost.
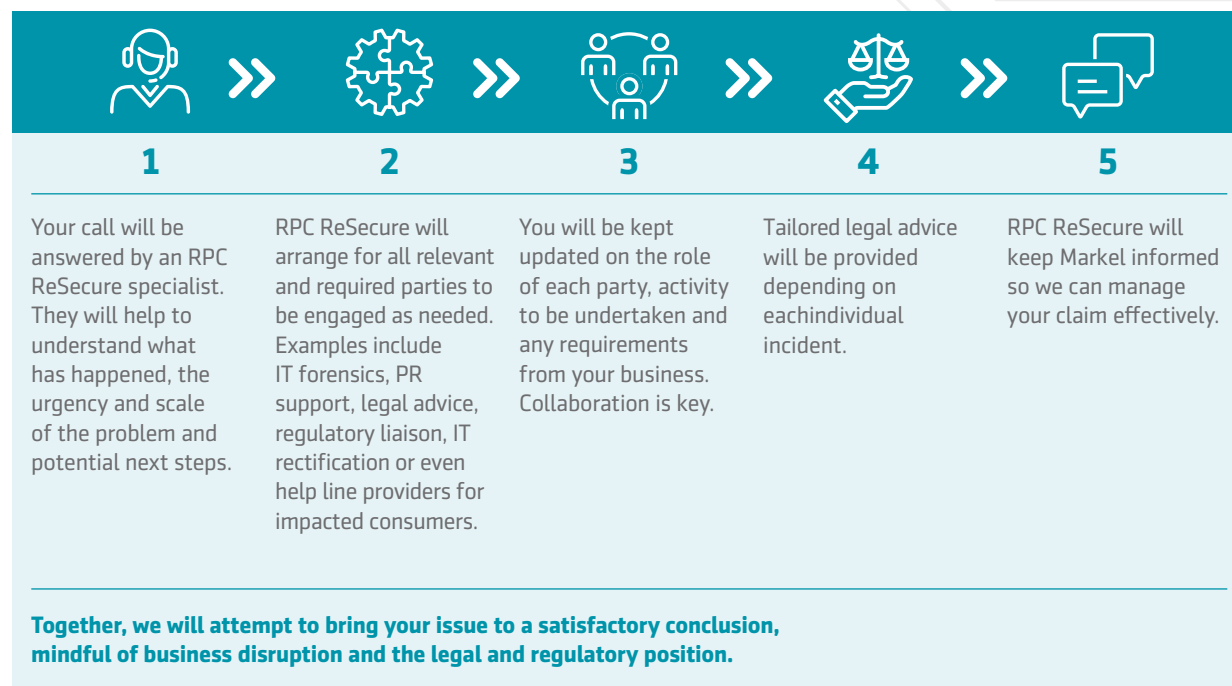
RPC ReSecure: Your tailored 24/7 incident breach response

We take claims very seriously. When your business is at risk, you might not know what to do or who to turn to— that's why we partner with RPC ReSecure who provides one of the leading cyber incident response services.

The incident response hotline is available 24/7 and ensures that when things go wrong, you will always have access to the support and advice you need. Additional experts such as IT forensic providers are ready and primed to help you in your hour of need.

For more information on the RPC ReSecure service, please click the graphic below.

How the process works

1	2	3	4	5
Your call will be answered by an RPC ReSecure specialist. They will help to understand what has happened, the urgency and scale of the problem and potential next steps.	RPC ReSecure will arrange for all relevant and required parties to be engaged as needed. Examples include IT forensics, PR support, legal advice, regulatory liaison, IT rectification or even help line providers for impacted consumers.	You will be kept updated on the role of each party, activity to be undertaken and any requirements from your business. Collaboration is key.	Tailored legal advice will be provided depending on eachindividual incident.	RPC ReSecure will keep Markel informed so we can manage your claim effectively.

Together, we will attempt to bring your issue to a satisfactory conclusion, mindful of business disruption and the legal and regulatory position.

Introducing NetDiligence® eRiskHub®

As part of the Cyber 360 policyholder benefits, you will have free access to the NetDiligence® eRiskHub® which is an online cyber risk management portal with tools and information to enhance the protection of your business. The hub also provides content bespoke by geographical area as we recognise what is relevant to an American business might not be to a European one.
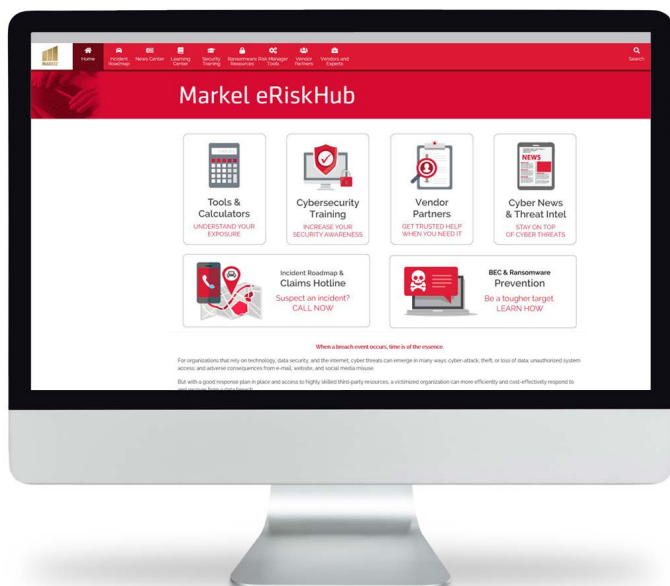
About NetDiligence®

NetDiligence® specialises in cyber risk readiness and response services. With more than 18 years of experience in cyber, NetDiligence is an award-winning provider of cyber risk management software and services to the insurance industry, including QuietAudit® risk assessments, the eRiskHub® cyber risk management portal and Breach Plan Connect® software-as-a-service (SaaS) to help policyholders with data breach response planning. NetDiligence publishes an annual Cyber Claims Study and hosts annual Cyber Risk Summits in Philadelphia, Santa Monica, Toronto, London and Bermuda. For more information, visit netdiligence.com.

If you haven't been into the Markel eRiskHub before or if it has been a while, now is a great time to check out all the cyber resources brought to you by Markel.

Key Features

Incident roadmap
Suggested steps to take following a network or data breach incident, free consultation with a Breach Coach® and access to a breach response team.

Ransomware resources
A guide on must-have ransomware safeguards, a ransomware stress test, a mock ransomware exercise, and a Markel-exclusive business e-mail compromise (BEC) and ransomware self-assessment survey that can help you reduce your exposure to BEC, ransomware and other exploit threats.

Risk manager tools
Cost calculators, research tools for causes of incidents and cyber claims payouts and sample policies, including one for remote working.

News center
Cyber news feeds, threat intelligence and security, legal and compliance blogs.

Cybersecurity awareness
Resources for ongoing employee education, including general security awareness, anti-phishing and IP/ trade secrets.

Ransomware stress test
An online self-assessment and remediation tool that measures an organization's susceptibility and ability to respond to a ransomware attack. Not only will this tool help identify areas of vulnerability, it will also provide feedback to help shore up those areas that need it.

Must-have ransomware safeguards
This NetDiligence guide outlines safeguards that are necessary to help any organization minimize the risk of a ransomware attack.

Ransomware mock breach exercise
This interactive game (eriskhub.com/markel) involves a simulated ransomware attack. As the event unfolds, the company's incident response team discusses the situation and the next-step actions available to them. Play along and make decisions regarding the company's system restoration, negotiation, payment, legal ramifications, notification, public relations and more.

Ransomware by the numbers
Aggregated ransomware attack statistics such as average ransoms paid, data recovery rates and network attach vectors. The tool is updated quarterly with the latest statistics from real ransomware events.

Remote working cybersecurity policy
More employees are working from home today than ever. A solid remote working policy is a must-have for any organization in this work environment. This downloadable template allows for the quick creation of a robust remote working security policy.

Improve your defences against the most prolific cyber threats

Cyber threats change regularly, and yesterday's concerns will be different to tomorrow's.

Currently the world is grappling with ransomware and business e-mail compromise (BEC) cyber threats. The eRiskHub portal contains resources to help with the most prominent cyber threats.

Ransomeware Stress Test by Tetra Defense
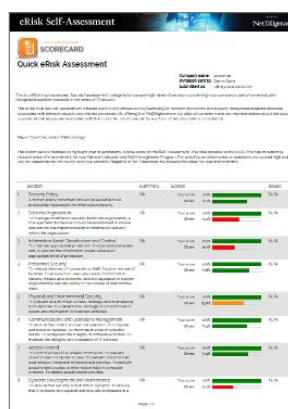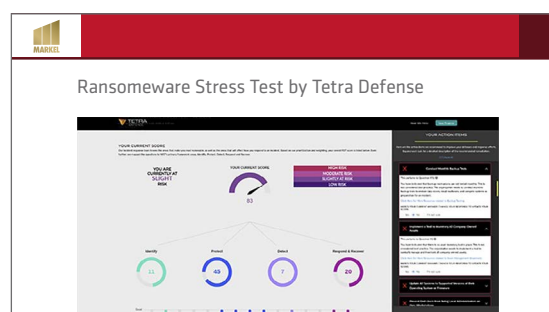
Through our partnership with NetDiligence, Cyber 360 policyholders also get free access to the QuietAudit tool.

Using this tool, you are able to self-assess your controls and protections to mitigate these significant cyber threats.

QuietAudit will provide you with a score reflecting your current risk management status, as well as a benchmark score of others in a similar industry to your own. QuietAudit will recommend and suggest further steps you can take to further improve your posture.

As the threats evolve, so too will the support, advice and resources we provide you.

We call it #PerformanceFreed.

During 2020, ransomware and business e-mail compromise accounted for a significant proportion of cyber incidents, hence why QuietAudit can really help your business move forward.

Meet the team

Scott Bailey
Divisional Managing Director, Cyber
scott.bailey@markel.com

Chris Burgess
Senior Underwriter & Head of Cyber
chris.burgess@markel.com

Tom Fassnidge
Claims Manager, Management
Liability, Cyber & PACE
tom.fassnidge@markel.com

Pushpa Sriwignarajah
Senior Underwriter, Cyber
pushpa.sriwignarajah@markel.com

Fred Pugh
Underwriter, Cyber
fred.pugh@markel.com

Rachel Gwilt
Senior Claims Adjuster
Rachel.Gwilt@markel.com

Charlotte Nicholls
Assistant Underwriter, Cyber
charlotte.nicholls@markel.com

James Loraine
Underwriting Assistant, Cyber
james.loraine@markel.com

Harry Barnes-King
Claims Adjuster
Harry.Barnes-King@markel.com

MARKEL®