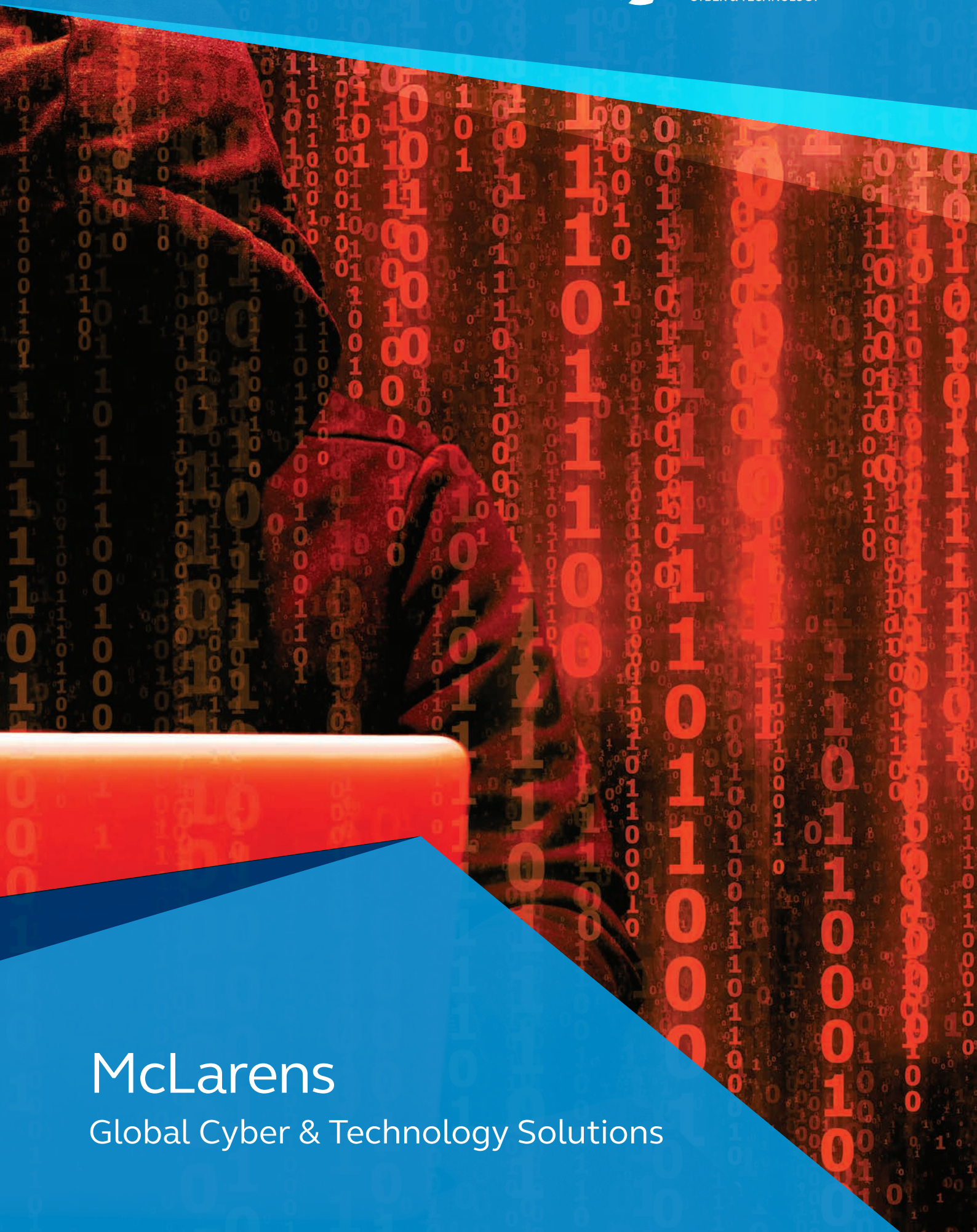
McLarens
CYBER & TECHNOLOGY



McLarens

Global Cyber & Technology Solutions

McLarens
Global

Borderless Cyber Crimes

In reality geographical borders for cyber criminals don't exist. Cyber incidents and attacks are occurring worldwide on a daily basis. McLarens has the global solutions for brokers, insurers, MGAs, and re-insurers requirements in this fast-moving and evolving market.

We have specialist cyber teams in multiple territories ready to react to that cyber incident whether it be localized to one area or affect a business on a global scale. From the United States to Australia, Asia to LatAm, Europe or the Middle East, McLarens has the expertise to react quickly and efficiently to our clients' requirements.

While offering truly global reach for cyber claims we realize that maintaining local and personal values in the claims process is vital to a successful outcome. Whether this be local or unique cultural difference, laws, or regulations we have the solutions for both global and local clients to deliver an outstanding professional claims services in the cyber arena.

In addition to cyber, we also have the expertise to manage claims involving highly complex equipment and systems utilizing computer technology. With McLarens' in-house expertise in all aspects of cyber and technology incidents, alongside our approved partners, we provide a solution tailored to your individual requirements.

Global Cyber Crime by the Numbers

In 2020 cyber crime cost the global economy **$945** billion*

By the end of 2021 a ransomware is predicted to attack a business **Every 11 seconds**

736,071,428 phishing web attacks occurred in the financial sector in 2020

As of 2020, the average cost of a data breach is **$3.86** million**

** 2021 Cyber Attack Statistics, Data, and Trends | Parachute (parachutetechs.com); ** (IBM)*

Our Expertise

Cyber

Cyber incidents by their nature require a specialist approach and solution. From global cyber incidents, to attacks on SMEs, to HNW clients being targeted, we have the people and processes in place to help get back on track. Our expertise includes:

- Banking scams
- Cyber business interruption
- Cyber crime
- Cyber liability – first and third-party
- Data breach
- Data corruption/data encryption
- Denial of service attacks
- Distributed denial of service attacks
- Mobile phone and telecoms scams
- Phishing/spear phishing attacks
- Ransomware/malware

Our Services

- Cyber crime investigation including potential recovery of funds
- Cyber liability investigation and defense
- Cyber quantum only services
- First response cyber services including 24/7 coverage
- Full cyber or hacking incident investigations and root cause analysis
- Identity theft investigation and assistance
- Pre-risk cyber services and post incident security audit including penetration testing
- Specialist cyber business interruption investigations, assessment and quantification services
- Telephone hacking/cloning investigations
- Virus removal and reinstatement of systems/data

Technology

With insurance policies now providing more specific and bespoke cover, there is an increasing need for specialists to deal with insurance claims. These claims can involve high value complex equipment which require the correct and timely consideration of both policy liability and quantum aspects. McLarens have technical knowledge and expertise in the following sectors:

- Building management systems
- CAD systems
- Digital printing
- Drones – both first and third party
- Electronic control systems
- Electronic equipment
- IT and computer equipment
- Media and post-production equipment
- Mobile communication equipment
- Robotics
- Security and monitoring equipment
- Smart networks
- Sound system networks
- Telecommunications equipment
- Television and sound equipment
- Videography and photography equipment

In addition to our in-house capabilities we also partner with external specialist including IT forensics and legal professionals to assist where required.

Our Services

- Full claims investigation and evaluation
- Industry leading experts in all technology fields
- Specialist partner services for root cause investigations and analysis
- Specification and procurement of specialist systems.

Coverage

Our global Cyber Solutions team for cyber and technology is headed by Nigel Collins, Technical Lead for Cyber & Technology, who also manages our suite of specialist supplier partners worldwide.

We have developed a global proposition and team to meet the requirements of insurers, brokers and businesses experiencing cyber or technology incidents in multiple territories and regions.

Nigel Collins, HNC Dip CII MBA
TECHNICAL LEAD – CYBER & TECHNOLOGY
+44 (0)7503 119 154
nigel.collins@mclarens.com

Asia
- China
- Hong Kong
- India
- Indonesia
- Japan
- Korea
- Malaysia
- Philippines
- Singapore
- Thailand
- Taiwan
- Vietnam

Australasia
- Brisbane
- Melbourne
- Perth
- Sydney
- New Zealand

Europe
- Belgium
- Denmark
- France
- Germany
- Italy
- Israel
- Netherlands
- Switzerland
- Spain

Latin America
- Brazil
- Colombia
- Mexico

Middle East & Africa
- Abu Dhabi
- South Africa

UK & Ireland
- Ireland
- United Kingdom

USA & Canada
- Atlanta
- Boston
- Chicago
- New York
- San Francisco
- Toronto

Case Study

Global Response With Local Knowledge

Situation: A global manufacturing company headquartered in Germany were targeted in a ransomware attack by a cyber-criminal gang. While they did react relatively quickly the scale of the attack was such that it proliferated extremely quickly. With the global footprint of the business and all facilities in multiple territories being connected to the head office in Germany this resulted in the ransomware spreading throughout the network on a global basis which completely disabled the business. From email communication, accounting functions, manufacturing, CAD, distributions and management of stock flows, all processes were completely disabled.

Scenario: In view of the global scale of the attack a truly global response was required. A global response was implemented with a management team put in place with specialist in the various regions affected mobilized to provide local assistance. Primary focus was on remediation within the German headquarter operations to allow facilities to be reinstated. Manufacturing processes were then prioritized with a global role out of systems to all areas. Less critical systems were then brought back online on a phased basis to complete the remediation process.

Outcome: Key to success for this incident was the collaborative approach and mobilization of the initial management team augmented by our local presence in the affected countries which brought together our global knowledge yet local accountability. This allowed the rebuilding process to be fast tracked getting the client back in business in a timely manner.

Notification of Loss

+44 (0)3309 122 241
Out of Hours: +44 (0)330 024 9955

cyber@mclarens.com

Contact

cyber@mclarens.com

www.mclarens.com

Connect

McLarens

@McLarensGlobal

McLarens

©2024 McLarens. All rights reserved