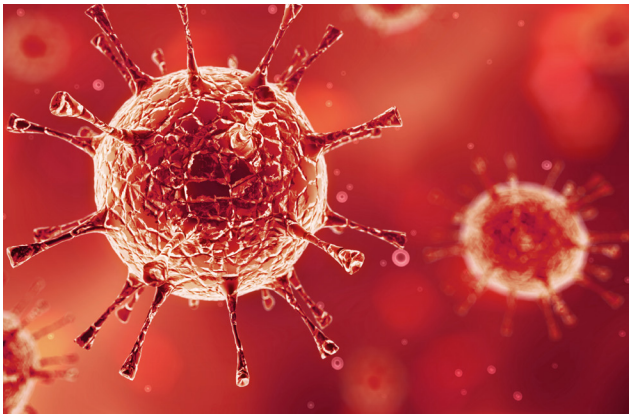
MARSH JLT SPECIALTY

INSIGHTS | MARCH 2020

COVID-19: Implications for Cyber, Media, and Tech E&O Coverage

Risks and challenges may emerge with the adoption of social distancing and stay-at-home protocols to reduce COVID-19's adverse effects. With employees, students, patients, and others asked to function remotely under stressful circumstances, and infrastructure pushed to handle more activity, organisations must consider how their cyber risk profiles may be affected.



The biggest challenge is migrating from a physical presence to a virtual one. Once organisations acknowledge this challenge, they must take appropriate action to mitigate potential risks – for example, by reinforcing employee and other users' awareness of cyber threats, boosting and supporting technology systems, and reviewing insurance coverages with an eye toward potential losses under cyber, media, and technology errors and omissions (E&O) policies.

Awareness and Vigilance

Increased remote working is presenting more opportunities for cyber-attackers, and organisations just starting to use remote desktop protocols for work may be more susceptible to a cyber-attack. For instance, individuals may log in remotely from home networks that use less secure hardware.

Cyber actors have already taken advantage of people seeking information on the pandemic. COVID-19 is increasing the occurrence of phishing and "social engineering" events, with information about the virus used as the hook.

Remote working also increases the risk of relaxed privacy policies and procedures. To facilitate working from home, employees may remove printed files from the workplace, or transfer personally identifiable information to unsecured or unencrypted storage or personal devices – potentially exposing the information to a breach by unauthorised users or improper use and disposal.

Organisations should proactively remind employees that good digital hygiene is even more critical when connecting to networks remotely. The burden may fall on employees at home to conduct activities such as patching and updating systems, logging out when not working or using networks, physically securing computers, following proper procedures about handling private data, and using robust passwords for devices and home Wi-Fi.

MARSH

Demands on IT Resources

Organisations also need to maintain a heightened state of cybersecurity, including testing system preparedness for inevitable operational disruption. IT information security teams are now being called upon to handle problems arising from a suddenly and greatly increased remote workforce.

Demand on web communication tools will increase, which may reduce system availability. System outages or degradation will interrupt operations, causing loss of revenue and additional expense.

Insurance Considerations

Insurance coverage for privacy breaches, security incidents, and technology outages is already available. In fact, a typical cyber policy provides various loss prevention and mitigation services that can be accessed both before and after an event. Several insurers are also proactively reaching out to policyholders when they become aware of potential threats or exploitable vulnerabilities. However, with the unprecedented number of people "social distancing", the rapid rise of remote connectivity will likely create new vectors for cyber claims, particularly under three distinct coverages:

Cyber.

Technology errors and omissions.

Media liability.

Some of the COVID-19 pandemic's unique circumstances may limit or challenge the responsiveness of these policies.

Cyber Coverage

Most cyber insurance policies include a broad array of coverages relevant to the current environment. These include network security liability, privacy liability, security response and forensic costs, data recovery and restoration, ransom event costs, reputational harm, network business interruption and associated expense, system failure, contingent business interruption, and privacy regulatory defence.

In some situations, however, coverage may not apply. Cyber insurance policies typically include:

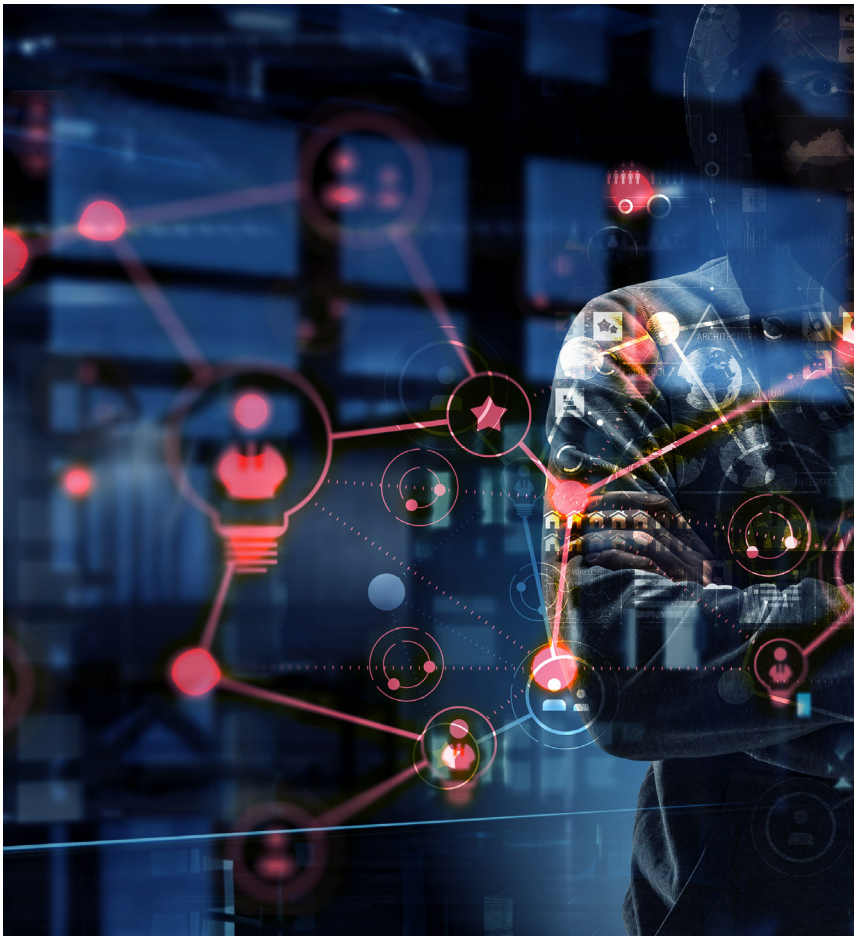
- **Infrastructure exclusions.** Policies typically exclude coverage for failure of power, utility, mechanical, or telecommunications (including internet) infrastructure or services not under the insured's direct operational control.
- **Voluntary shutdown coverage limitations.** Coverage may only apply to voluntary shutdowns to prevent the spread of malware or limit damage – and not to shutdowns intended to improve network access or functionality.
- **Limitations in computer system or network definitions.** Policyholders should review key definitions and whether they affect coverage for owned, operated, or leased systems and those operated by third parties.
- **Limitations in system failure definitions.** Some policies may require a human or programming "error", proof of testing or patches, or proof of system use prior to failure in order to trigger coverage.

Demand on web communication tools will increase, which may reduce system availability. System outages or degradation will interrupt operations, causing loss of revenue and additional expense.

Technology (E&O) Coverage

Technology E&O policies include coverage for wrongful acts in the delivery of technology services, or failure of technology products to work or perform intended functions that are potentially relevant to current conditions. Coverage may not apply, however, in certain circumstances because of a policy's:

- **Technology products and services or wrongful act definitions.** Wrongful acts may only be covered when technology products or services are offered "for a fee", or provided or designed for use in conjunction with a service. Some policies only cover the negligent rendering of service but not the "failure to render".
- **Deceptive business practices, antitrust, and consumer protection exclusions.** Policies may exclude coverage when goods or services fail to conform with represented quality or performance.
- **Bodily injury/property damage exclusions.** Most E&O policies cover third-party resultant financial loss, under the premise that third-party bodily injury and property damage claims will be first addressed by casualty programmes, and only trigger E&O coverage after casualty coverage has been exhausted.
- **Governmental action exclusions.** A tech E&O policy may preclude claims from governmental agencies unless in the direct capacity as a customer.
- **Trading losses or loss of money exclusions.** Claims for trading losses, change in the value of accounts, and transfer of money are typically excluded.
- **Over-redemption or coupon exclusions.** Promotional games, price discounts, coupons, or other considerations given in excess of a contract's value are typically excluded.



Media Liability Coverage

Media liability policies include coverage for a wide range of acts related to the creation or display of media material (for example, information, sounds, images, and graphics). Typical media liability coverages include defamation or product disparagement, infliction of emotional distress, misappropriation of names or likenesses, privacy rights violations, and infringement of copyrights or domain names, and plagiarism.

But losses and damages incurred may not be covered under some circumstances. Media policies typically include:

- **Deceptive business practices, antitrust, and consumer protection exclusions.** Policies may exclude coverage for goods or services failing to conform with any represented quality or performance.
- **Bodily injury/property damage exclusions.** Coverage may include emotional distress but not claims of actual physical harm to persons.
- **Governmental action exclusions.** Media policies may preclude claims from governmental agencies unless in their direct capacity as customers.
- **Media coverage for non-media entities.** Coverage may be tied to online media only or in connection with delivery of professional services.

NEED FOR POLICY COVERAGE REVIEWS

As the pandemic continues, risk professionals should work with their insurance advisers to carefully review policy language to refresh their awareness of what is and is not covered, and act as necessary to ensure that coverage will be triggered in the event of a loss.

For more information on the cyber risks and coverage implications of the COVID-19 pandemic, visit www.marsh.com or email:

SARAH STEPHENS
Head of Cyber, International
Cyber, Media & Technology Practice Leader, UK FINPRO
+44 (0)7508 051080
sarah.stephens@marsh.com

BRIAN WARSZONA
UK Cyber Growth Leader
Cyber, Media & Technology Practice Leader, UK FINPRO
+44 (0) 7392 123570
brian.warszona@marsh.com

Insurance Brokers
Chartered