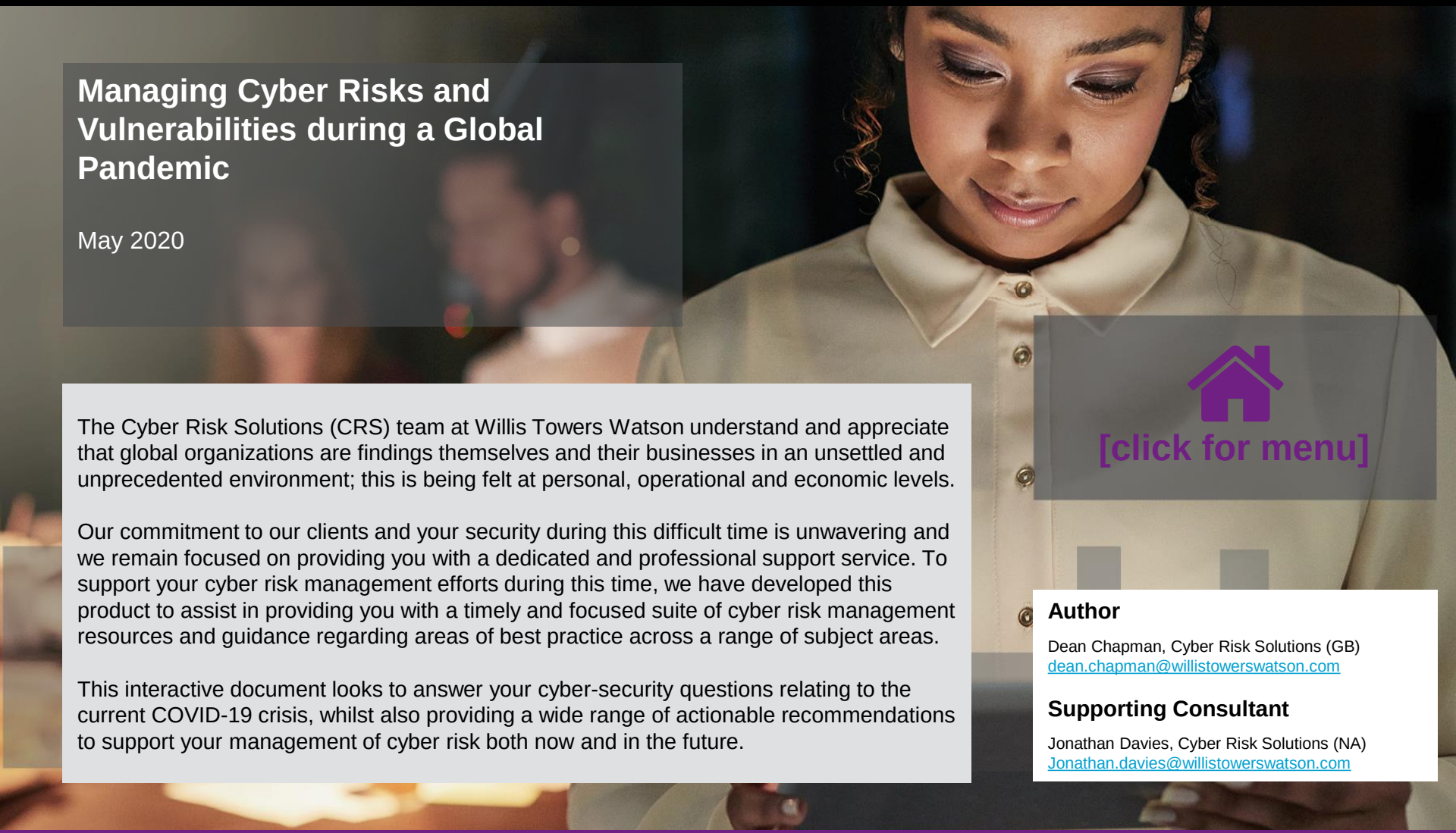
Decode Cyber Risk



Managing Cyber Risks and Vulnerabilities during a Global Pandemic

May 2020

[click for menu]

The Cyber Risk Solutions (CRS) team at Willis Towers Watson understand and appreciate that global organizations are findings themselves and their businesses in an unsettled and unprecedented environment; this is being felt at personal, operational and economic levels.

Our commitment to our clients and your security during this difficult time is unwavering and we remain focused on providing you with a dedicated and professional support service. To support your cyber risk management efforts during this time, we have developed this product to assist in providing you with a timely and focused suite of cyber risk management resources and guidance regarding areas of best practice across a range of subject areas.

This interactive document looks to answer your cyber-security questions relating to the current COVID-19 crisis, whilst also providing a wide range of actionable recommendations to support your management of cyber risk both now and in the future.

Author

Dean Chapman, Cyber Risk Solutions (GB)
dean.chapman@willistowerswatson.com

Supporting Consultant

Jonathan Davies, Cyber Risk Solutions (NA)
Jonathan.davies@willistowerswatson.com

© 2020 Willis Towers Watson. All rights reserved.

Willis Towers Watson

Managing Cyber Risk and Vulnerabilities during a Global Pandemic

Guidance and Best Practice

- Pandemic-related Cyber Updates
- Working From Home (WFH)
- Managing Cyber Incidents Remotely
- Data Security & Regulatory Compliance
- Managing People + Cyber Risk Culture
- Managing Third-Party Cyber Risk
- Business Continuity & Cyber Resilience

WTW Cyber Risk Solutions

- Cyber Mission and Values
- Cyber Risk Solutions
- Additional Cyber Risk Management Resources
- Contact Us
- Disclaimer

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has over 40,000 employees serving more than 140 countries. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas — the dynamic formula that drives business performance. Together, we unlock potential.

Willis Towers Watson offers insurance-related services through its appropriately licensed entities in each jurisdiction in which it operates, for example:
Willis Towers Watson North America, Inc in the United States
Willis Limited in the United Kingdom

FPS1130

© 2020 Willis Towers Watson. All rights reserved. Proprietary and Confidential. For Willis Towers Watson and Willis Towers Watson client use only.

Willis Towers Watson

Pandemic-related Cyber Updates

Current Trends / Situational Awareness

An increasing number of malicious cyber actors have looked to exploit the current COVID-19 pandemic for their own objectives. Global agencies have detected heightened nefarious cyber activity which has led to increased cyber threats to individuals and businesses. In particular, the surge in home / remote working has increased usage of potentially vulnerable services, such as Virtual Private Networks (VPN) and home WiFi networks; malicious actors know this and are actively looking to capitalise.

Advanced Persistent Threat (APT) groups are known to be targeting individuals, small and medium businesses as well as large organizations with predominantly Social Engineering attack techniques that once again look to capitalise on the global COVID-19 pandemic. Heightened Email Based Attack campaigns (such as Phishing) and increased Smishing (SMS based attacks) are common place. Individuals and organizations alike must apply the enhanced due care and attention to the cyber security of their workforce, their data, systems, networks and devices through this troubling time.

Additional Resources

GB - National Cyber Security Centre - link
US - Cybersecurity and Infrastructure Security Agency - link
Global – Infosecurity Magazine COVID-19 Blog - link

Questions for Global organizations

Q. Is your organization at risk during this crisis?

Hackers and malicious groups are indiscriminate. If they can observe financial or intellectual gain by targeting your people and your business then your organization is at risk. Malicious actors are targeting people and business right now with a high degree of success.

The global pandemic will undoubtedly be testing your organization in ways that it has never been tested before. Your success in navigating your business, your clients and your workforce through this time rests upon your ability to respond to the drastic change in working processes, as well as service delivery models, in an effective and timely manner.

Q. What areas should your organization focus on during this crisis?

This interactive document provides general guidance relating to those key areas, listed below, that we believe should be considered as priority security activities during this period. For more detailed guidance please do not hesitate to contact the Willis Towers Watson CRS Team.

- Working from Home / Remote Working
- Managing Cyber Incidents Remotely
- Data Security & Regulatory Compliance
- Managing People + Cyber Risk Culture
- Managing Third-Party Cyber Risk
- Business Continuity & Cyber Resilience

For further information or to discuss in detail please contact us.

© 2020 Willis Towers Watson. All rights reserved.

Working From Home

Current Trends / Situational Awareness

Due to the restrictions in place across most of the globe, a large number of organizations have been required to move their workforce to a predominantly remote (home) working environment.

Whilst Work From Home (WFH) is increasingly common, a vast majority of organizations have never before had to rely upon the continuity of their business operations to be delivered by a largely remote, home-based workforce.

Hackers and criminal groups are fully aware that a large number of global workforces are now working from home and that most are utilising a wide range of devices, systems and networks (including home Wi-Fi). As a result, organizations have had to adapt their operating and service delivery models at incredibly short notice.

The information (right) has been provided to assist your organization in identifying those key areas of risk (associated with home working) as well as offering a series of recommendations that aim to provide your business with a focus for best practice going forward during these difficult times.

Best Practice Guidance / Key Takeaways

The following recommendations have been provided for your consideration and possible onward management of cyber risk.

✓ **Infrastructure and Access Management**
Consider pressures on your information systems and infrastructure. Can it support widespread remote access? Consider which systems / applications are critical to business continuity, ensure they are supported whilst looking to 'close down' any less critical activities / apps etc.

✓ **Home Wi-Fi Networks**
Offer guidance and signposting to resources that support the securing of home Wi-Fi networks. Prioritize those individuals in 'close quarter' living environments, encourage changing of default passwords and utilisation of WPA2-AES security where possible.

✓ **System, Application and Browser Updates and Patching**
Is your organization applying updates / patches to business critical systems / applications? Ensure web / internet security updates are applied and consider blacklisting where possible. For home workers, encourage security updates / patches are applied to personal devices.

✓ **Reporting Suspicious Cyber Activity**
Communication, encouragement and ease of use are **key.** Reporting of suspected incidents or unusual cyber activity should be as seamless as possible, ideally using a single Point of Contact. Communicate the contact details and process widely to all parts of your business.

For further information or to discuss in detail please contact us.

© 2020 Willis Towers Watson. All rights reserved.

Managing Cyber Incidents Remotely

Current Trends / Situational Awareness

Due to the restrictions in place across most of the globe, a large number of organizations have been required to move their workforce to a largely remote (home) working footing. Whilst this may have some benefits to your organization, it does mean that a different approach to managing your enterprise cyber security will be required.

One area of your cyber security strategy that will require attention is likely to include the changes to the manner in which your organization detects, manages and responds to cyber security incidents.

With a demonstrable increase in global cyber attacks, your business must ensure your incident management and response processes are robust and take into account the new set of circumstances in which your organization may now be operating.

Taking immediate action to adapt to and overcome the challenges posed by remote working and implementing an effective remote IR strategy could just be the difference between successful containment and recovery or suffering a major incident.

Best Practice Guidance / Key Takeaways

The following recommendations have been provided for your consideration and possible onward management of cyber risk.

- **Review and Test your Incident Response (IR) Plan**
  Whilst most organizations possess an IR plan, it is highly unlikely that this plan would be been 'stress tested' in an environment such as the present one. Organizations should review and test incident plans to ensure it's applicability and efficacy in supporting new operating models (WFH and remote working etc.).
- **Communication is Key**
  Review and test existing security team communication channels, are these fit for purpose? We recommend developing a response call out 'tree' and ensure this is communicated to all key stakeholders and response plan participants.
- **Incident Response, Business Continuity and Disaster Recovery**
  In these unprecedented times, and whilst your IR plans are being reviewed, tested and enacted, the current climate could also act as a catalyst for the formal alignment and/or consolidation of your IR, BC and DR plans.
- **Keep it Simple for Employees > Incident Reporting**
  During this period of confusion and where operating processes are being adjusted to meet new working models, the reporting of suspect and real-time security incidents should be made as seamless and simple to follow as possible for your workforce.

For further information or to discuss in detail please contact us.

© 2020 Willis Towers Watson. All rights reserved.

Data Security & Regulatory Compliance

Current Trends / Situational Awareness

While it is widely acknowledged that these are difficult times for enforcing data security, data protection regulators worldwide have issued guidance to help organizations comply with their obligations under applicable data protection and ePrivacy laws.

Regulators are aware of the struggles organizations are facing and, in considering enforcement, will likely take into account the current health emergency. That said, organizations should remain vigilant and not use this as a reason to become complacent.

Global regulators have indicated that they are aware of the pressures facing organizations in the current environment. For example, the UK Information Commissioner's Office (ICO) has hinted that, whilst there is no extension of the statutory 30-day time limit for organizations to respond to data subject access requests, they will not rush to penalise organizations struggling to meet this limit.

The Global Privacy Assembly (GPA) has compiled the latest guidance and information from GPA members on data protection and COVID-19, which can be found within our additional resources page.

Best Practice Guidance / Key Takeaways

The following recommendations have been provided for your consideration and possible onward management of cyber risk.

- **No Respite from Data Protection Obligations**
  Organizations should ensure that they remain compliant with their obligations under applicable data protection and ePrivacy laws.

- **Policies and Procedures**
  Ensure your employees know what office policies extend into the home working environment and adjust procedures to account for remote working where applicable.

- **Enhanced Social Media Guidelines for Remote Workers**
  Employee posts on social media can pose a serious threat to your business and we recommend-reminding your employees of your social media policy. A **#mytemporaryoffice #socialdistancing** post on Facebook or Instagram may inadvertently disclose confidential or reputationally damaging information posing significant risk for the organization.

- **Communicating With Employees**
  In communicating with employees and other stakeholders, organizations should be aware of their legal obligations and risks in disclosing personal health data or other sensitive information.

For further information or to discuss in detail please contact us.

© 2020 Willis Towers Watson. All rights reserved.

Managing People + Cyber Risk Culture

Current Trends / Situational Awareness

It comes as no surprise to learn that malicious actors are using the current global crisis as the springboard for a new wave of heightened nefarious cyber activity.

Largely taking the form of an Email Based Attack (EBA) or via Smishing (SMS-based phishing), hackers are preying on people's worries and concerns of COVID-19 to achieve their sordid objectives. These are not particularly sophisticated attacks, however history shows us that Social Engineering is an effective, tried and tested technique that offers timely and financially lucrative return for very little investment (on the hackers part).

As with those other cyber security concerns organizations have at the current time, it is safe to assume that your 'Human Firewall' is the one likely to be most tested and the one that your business should be looking to strengthen wherever possible. A focus on people security enhancements during this period could well be the difference between your successful identification and containment of a security event or potentially suffering a major incident.

By exploiting high levels of individual and collective stress and anxiety that the current climate has presented, hackers know that targeting people, and therefore your business, might be easier than it typically would be (see also remote / home working).

Best Practice Guidance / Key Takeaways

The following recommendations have been provided for your consideration and possible onward management of cyber risk.

- **Communication is Crucial**
  Your employees are likely to be suffering from heightened levels of stress and anxiety associated with the current evolving situation. Businesses should be mindful of the mental health impact(s) on their workforce and, from a cybersecurity perspective, support and empower them whilst offering empathy and reassurance wherever possible.

- **Cyber Threat Awareness Updates**
  With heightened malicious activity observed globally, you should look to provide your workforce with an increased level of cyber threat situational awareness, focusing on current social engineering campaigns with support on how to confidently and effectively identify and report such incidents / suspect activity.

- **Home Working Support**
  Wherever possible, and if resources allow, your security teams could provide direct support to your workforce, paying particular attention to helping them secure home Wi-Fi networks, personal devices and online accounts etc.

- **Professional Development and Learning / Upskilling**
  Encourage, if possible, that your employees take part in opportunities for training / upskilling. There are a wide range of free training resources available online which can assist in keeping your workforce aware.

For further information or to discuss in detail please contact us.

© 2020 Willis Towers Watson. All rights reserved.

Managing Third-Party Cyber Risk

Current Trends / Situational Awareness

Given the current risk outlook, the need for enhanced due diligence in third-party, supply chain and vendor selection and management activities is critical. While travel bans and work from home policies prevent on-site evaluations, third-party risk must still be assessed and evaluated.

When engaging with third-parties, we recommend that the conversation start with empathy, as your point of contact may be feeling the pressure of this event at a personal level.

Valuable information to support vendor selection and management can be gained by reviewing the third-party's Incident Response Plan (IRP), Business Continuity Plan (BCP), and Information Security Policy. This also applies to existing third-parties upon which your business has critical dependencies. Remote work should not impact the completion and return of a custom security questionnaire so ask the questions that are important to your organization.

Remember, your third-parties and their subsequent third-parties are all likely to be feeling the strain of recent events, so keeping a regular, cordial dialog should assist in keeping you informed and ahead of any potential issues that may arise.

Best Practice Guidance / Key Takeaways

The following recommendations have been provided for your consideration and possible onward management of cyber risk.

Maintain the Practice of Supply Chain Risk Management
Consider replacing on-site evaluations with a thorough document review process focusing on:

- Incident Response Plan
- Business Continuity / Disaster Recovery Plan
- Information Security Policy (and sub-policies)
- Custom Security Survey Questionnaire

Stay in Close Contact with Existing Vendors
Identify the vendors your organization is operationally dependent on and maintain regular communications in order to stay ahead of potential supply chain issues.

Consider Supply Chain Interruption in your Incident Response Plan
During your next Incident Response Exercise, include a scenario relating to an interruption in the supply chain, and document lessons learned for inclusion in your IRP.

Establish Third-Party Time to Recover (or RTO) During Selection
Time to Recover (TTR) or Return to Operations (RTO) is measured by how long it takes for a supplier to recover its operations or relocate to an alternate site.

For further information or to discuss in detail please contact us.

© 2020 Willis Towers Watson. All rights reserved.

Business Continuity & Cyber Resilience

Current Trends / Situational Awareness

Global business continuity is currently being tested in conditions that are largely unprecedented.

Business continuity planning is designed to drive a business through temporary operational disruptions. The Business Continuity Plan (BCP) is an important tool for ensuring that an organization's core business functions are preserved both during and after an incident such as the coronavirus pandemic.

A BCP should outline the policies, procedures, and instructions an organization must follow in the face of such incidents, and is likely to be aligned with other policies such as an Incident Response Plan and Disaster Recovery Plan as part of a wider program of security and resilience.

Some industry regulatory authorities require license holders to maintain a Business Continuity Plan as part of the license holder's fiduciary duty to customers and may specify the issues that each plan is to address.

The austere situations that are likely to result in a BCP being activated bring with them added stress, increased responsibility, and considerable pressure to restore normal operations ASAP, so be sure to establish clear lines of communication and clearly assigned decision rights at the outset.

Best Practice Guidance / Key Takeaways

The following recommendations have been provided for your consideration and possible onward management of cyber risk.

Employee Health and Wellbeing
Establish a strategy that enables employees to function without endangering them. Ensure you have the tools, technology, capacity, and security measures in place to support a larger remote workforce. It may also be necessary to offer greater flexibility to normal working expectations.

Assemble a Business Continuity Team
Choose carefully who will be directly involved, from the plan's owner to those it affects. Appoint at least one person to devise a response strategy and coordinate pandemic readiness activities. Identify backup personnel in case some team members become unavailable. Be sure that senior leadership is visibly involved in the company's decision-making and assign clear decision rights to the appropriate team members.

Communication is Everything
Develop-a clear communication plan providing employees and customers with regular updates as well as actions taken. Take care to base your communications in verifiable news sources.

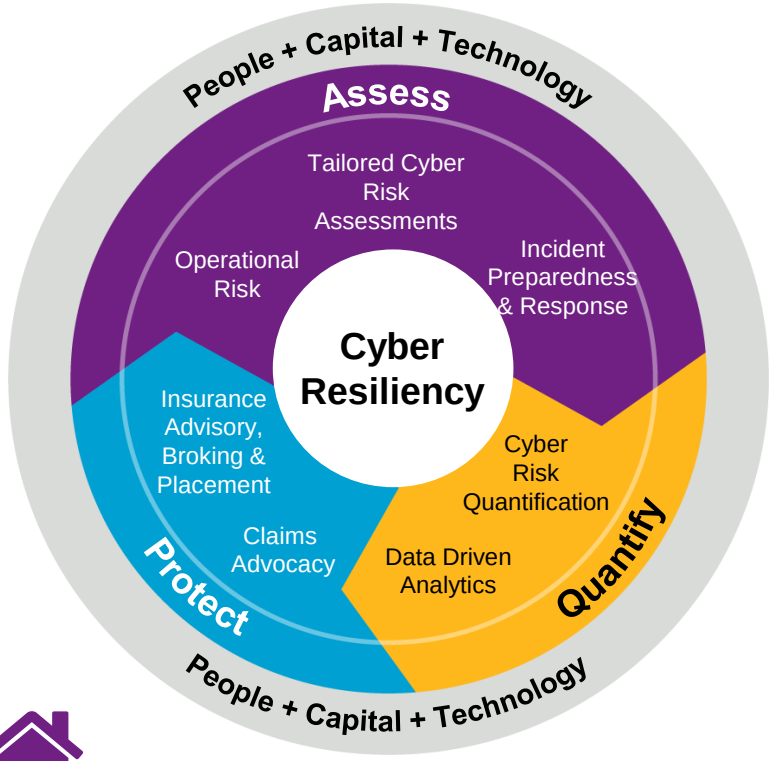
For further information or to discuss in detail please contact us.

© 2020 Willis Towers Watson. All rights reserved.

Cyber Mission and Values

Our holistic approach to cyber risk evaluates all threats - people, capital, technology - through three stages – Assess, Quantify, Protect - to ensure that our client is best prepared to protect and grow its business.

We are strategically positioned to identify and support growth opportunities across all segments through subject matter expertise, product development/enhancement, and partner relationships. Our claims- and culture-centric data allow us the opportunity to deploy innovative solutions to add new revenue streams and differentiate existing LoBs in the cyber risk management space.



Key offerings:

❑ **Insurance Placement**

- Insurance Advisory, Broking and Placement solutions and services designed to help clients mitigate the myriad of risks they are facing
- Claims Advocacy, including claims handling, loss mitigation, technical claims resolution, and risk control services

❑ **Integrated Cyber Risk Resiliency Solutions**

- The Cyber Risk Solutions Team offers tailored services that align cyber risk management with business objectives, support insurance goals and deliver cost effective Cyber Risk Resilience
- Cyber Quantified (CQ) proprietary analytical modeling to quantify the frequency and severity of privacy breaches and network outages
- Customized, cross functional enterprise cybersecurity review and assessment with our proprietary Cyber Risk Profile Diagnostic (CRPD).
- Customized consulting services focused on client needs, including:
Risk Assessment and Quantification	Incident Response Planning
Insurance and cybersecurity alignment	Operational Risk Analysis
Business Continuity Planning	Employee Training and Awareness

© 2020 Willis Towers Watson. All rights reserved. Proprietary and Confidential. For Willis Towers Watson and Willis Towers Watson client use only.

Cyber Risk Solutions Tailored Approach

Willis Towers Watson

Objectives

The Cyber Risk Solutions Team offers tailored services that support insurance goals, align cyber risk management with business objectives and deliver cost effective Cyber Risk Resilience.

Client Needs

Customized services can be provided in the following cyber risk areas:

- Insurance and organizational cybersecurity alignment
- Risk Assessment and Quantification
- Incident Response and Business Continuity Planning
- Operational Risk Analysis
- Employee Training and Awareness

Tailored Solutions

Taking into account client requirements, customized solutions can include:

- Cyber Risk Workshops, aligned with NIST or ISO frameworks
- Executive Workshops
- Incident Response and Business Continuity Plan Testing and Improvement
- Risk Quantification and Peer Benchmarking projects
- Cyber-security policy review and analysis
- Insurance Feasibility and Quantification

© 2019 Willis Towers Watson. All rights reserved. Proprietary and Confidential. For Willis Towers Watson and Willis Towers Watson client use only.

Additional Cyber Risk Management Resources

Willis Towers Watson

Working From Home (WFH)	GB – National Cyber Security Centre (NCSC) - link EU – European Union Agency for Cybersecurity - link Global – ComputerWeekly Remote Working Guidance - link
Managing Cyber Incidents Remotely	GB – National Cyber Security Centre (NSCS) - link US - Cybersecurity and Infrastructure Security Agency - link Global – Information Security Forum (ISF) - link
Data Security & Regulatory Compliance	Global – Global Privacy Assembly (COVID-19 Resources) - link Global – National Law Review (COVID-19 Data Protection) - link GB – Information Commissioners Office (ICO – COVID-19) - link
Managing People + Cyber Risk	Willis Towers Watson – Wellbeing during COVID-19 - link Global – Information Security Forum (ISF) - link SANS – Resources and Blog - link
Managing Third-Party Cyber Risk	Willis Towers Watson – Supply Chain Risk (Insights) - link Global – Information Security Forum (ISF) - link GB – National Cyber Security Centre (NCSC) - link
Business Continuity & Cyber Resilience	Willis Towers Watson – Business Continuity Management - link

© 2020 Willis Towers Watson. All rights reserved.

Contact Us – Cyber Risk Solutions

Willis Towers Watson

North America and Global

Dominic Keller
T: +1 415 806 2012
E: dominic.keller@willistowerswatson.com

Great Britain

Dean Chapman
T: +44 (0) 7920 211779
E: dean.chapman@willistowerswatson.com

Western Europe

Fernando Sevillano
T: +34 654 519 235
E: fernando.sevillano@willistowerswatson.com

© 2020 Willis Towers Watson. All rights reserved.

Disclaimer

The purpose of this document is to provide you with information and to assist you in your management of risks during the global COVID-19 crisis. It does not imply that no other risks or hazardous conditions exist.

Unless Willis Towers Watson provides express prior written consent; no part of this document should be reproduced, distributed or communicated to any third-party organization. This document, and any advice or recommendations contained herein are based upon conditions observed and information made available to us through a number of sources, and does not constitute legal, regulatory, tax or investment advice. The material contained herein is based upon information believed to be reliable; however no representation or warranty, expressed or implied, as to accuracy or completeness of such information is made and no liability is accepted for direct or indirect loss or damage of whatsoever nature arising out of the use or reading of all or any part of the information contained herein. Implementation of our advice or recommendations is the responsibility of the client organization.

This document is copyright protected and confidential between Willis Towers Watson and the party with whom it has been shared. Willis Towers Watson does not accept any liability if this document is used for an alternative purpose from which it is intended, nor to any third-party in respect of this document.

© 2020 Willis Towers Watson. All rights reserved.