In the ever-evolving technological landscape in which we live, our lives are dominated by technology. The development and widespread usage of the internet also means that more and more aspects of our daily, personal and business lives are moving online. We are all constantly producing and saving data, uploading content, and sending and receiving email traffic. The creation of this digital world has brought about a by-product – Cyber Risk.
WHAT ARE THE RISKS?

FIRST PARTY NETWORK LOSS
I.T. networks are at the heart of all companies. Degradation or failure of these systems could halt day-to-day operations and cost companies a significant amount due to lost revenue. System interruption can result from computer attacks, operational and administrative errors and virus transmission.

THE COST
- Loss of business income
- Costs to restore the network
- Costs to replicate/replace lost data
- Increased cost of working

PRIVACY BREACH AND SECURITY LIABILITY
In the age of ‘Big Data’, companies collect and store data to help improve the customer experience, but a side-effect of this data acquisition is the creation and storage of attractive and valuable data, which can be of huge interest to financially motivated hackers. Data comes in two distinct categories – Commercial Sensitive Data and Personal Identifiable Information.

THE COST
- 3rd Party damages
- Regulatory fines and penalties
- PR costs
- Costs to notify affected individuals
- Identity Theft monitoring costs
- Forensics costs
- Legal fees

REPUTATION
A company’s reputation is vital to attracting and maintaining clients. Mitigating cyber risks and being prepared to deal with cyber incidents is important to avoid any reputational harm.

THE COST
- Loss in sales revenue
- PR costs

TERRORISM
Over the years many aspects of life have gone online and terrorism attacks are no different. Cyber extortion is on the increase and companies are beginning to realise that their data can be extremely valuable to both themselves and to cyber criminals.

THE COST
- Extortion expenses
- PR costs
- Legal fees
WHAT DOES CYBER INSURANCE COVER?

Insurance coverage has been developed to address the challenges faced by business’ increased dependence on IT networks, third party IT and business processing providers. The cover has also been designed to address the risks that come with the abundance of digital assets and private data which companies collect and store.

At Willis, we work with our clients to help them understand their specific cyber risks. Willis then works with key cyber insurers to create tailor-made policies including cover for the identified risk exposures and filling in any gaps in current insurance policies. The standard covers that Willis manuscript includes the following:

FIRST PARTY NETWORK LOSS

— **Damage to Digital Assets**: Costs to recollect recreate and reconstitute the digital assets of an insured which is damaged or lost, altered, corrupted, distorted or stolen and any other costs to prevent, minimise or mitigate any further damage.

— **Non-Physical Business Interruption and Increased Cost of Working**: Income loss and interruption expenses incurred by the insured during the period of restoring the network directly as a result of the total or partial interruption, degradation in service or failure of the computer network.

PRIVACY AND SECURITY LIABILITY

— **Third Party and Employee Privacy liability**: Damages and legal fees as a result of a privacy breach or breach of confidence.

— **Security Liability**: Third party damages and legal fees as a result of unauthorised use, unauthorised access, transmission of a virus, denial of service attacks and other computer crime.
**MEDIA LIABILITY**

- **Multi-Media Liability:** Damages and legal fees as a result of a wrongful act in the course of publishing content in electronic or print media, including online social media platforms.

**PRIVACY REGULATION DEFENCE, AWARDS AND FINES**

- **Privacy Regulatory Investigation and Defence:** Expenses resulting from investigation, adjustment, defence and appeal of regulatory proceedings.
- **Privacy Regulatory Fines and Penalties:** Where insurable by law.
- **Payment Card Industry Fines:** Where PCI Data Security Standards are breached (please note that this cover is provided where relevant).

**CRISIS MANAGEMENT AND REPUTATIONAL EXPENSES**

- Costs to employ specialist forensic experts and solicitors to investigate and respond to a privacy breach or system failure.
- Costs to notify victims of privacy breaches and provide them with identity theft assistance and costs for PR related services to mitigate reputational harm.

**CYBER EXTORTION**

- Costs to engage crisis management experts
- Costs to pay ransoms if this is deemed to be necessary
**ARE MY CYBER RISKS COVERED BY OTHER INSURANCES?**

<table>
<thead>
<tr>
<th>CRIME/BANKERS BLANKET BOND</th>
<th>GENERAL LIABILITY</th>
<th>KIDNAP AND RANSOM</th>
<th>PROFESSIONAL LIABILITY</th>
<th>PROPERTY/BUSINESS INTERRUPTION</th>
<th>CYBER</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FIRST PARTY CYBER LOSSES</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Interruption due to:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&gt;&gt; Computer Crime</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>&gt;&gt; Employee Sabotage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>&gt;&gt; Operational Errors and Administrative Mistakes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>&gt;&gt; Cyber Terrorism</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Restoration, Recollection, Recreation of Digital Assets due to:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>&gt;&gt; Computer Crime</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>&gt;&gt; Employee Sabotage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>&gt;&gt; Operational Errors and Administrative Mistakes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>&gt;&gt; Accidental Damage to Hardware</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td><strong>DATA PRIVACY AND SECURITY THIRD PARTY LOSSES</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Breach of Sensitive Third Party Information</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Data Breach Caused by a Third Party Outsourcer</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Corruption of Third Party Data by Malicious Code</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Distributed Denial of Service or Malicious Code Delivered via your Network</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Corruption or Deletion of Third Party Data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Lost/Stolen Laptop or Hardware Containing Sensitive Third Party Data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Data Breach due to a Security Breach</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Intellectual Property Infringement, Plagiarism and Defamation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td><strong>DATA PRIVACY AND SECURITY FIRST PARTY LOSSES</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Protection Fines and Penalties</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Data Protection Investigation and Defence Expenses</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Public Relations Costs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Data Protection Legal Expenses</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Data Breach Notification Expenses</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Credit/Identity Theft Monitoring Expenses</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>

Please note standard policy wordings have been considered, not considering endorsements that may be obtained. For true comparison of policies individual policies and facts of claims would be required.
“As Companies begin to rely more heavily on sophisticated and intelligent technology solutions, they run into difficulty if and when that technology becomes unavailable for any reason.”
MISCONCEPTIONS OF CYBER INSURANCE

“CYBER INSURANCE IS INSURANCE FOR COMPANIES WHO SELL PRODUCTS OVER THE INTERNET.”

Cyber risks are faced not only by e-commerce companies and those undertaking transactions over the internet but also by those companies that collect and store personal and corporate sensitive data or are reliant on computer or telephone networks and data for their daily operations.

“WE DO NOT OPERATE IN TERRITORIES WITH PRIVACY LAWS MANDATING NOTIFICATION OF A DATA BREACH; THEREFORE WE DON’T NEED TO BUY CYBER INSURANCE”

Whilst it is true that you do not need to notify victims of a data breach in the absence of privacy laws mandating this requirement, it is however recommended by many privacy regulators to do so as part of best practise processes. In addition, this can avoid or mitigate any reputational harm. Furthermore, various territories worldwide have draft legislation that will soon be implemented enforcing companies to notify victims of data breaches.

“WE HAVE THE BEST I.T. SECURITY MONEY CAN BUY - WE WILL NEVER BE HACKED”

Whilst financially motivated hackers look for the “open doors”, those hackers who are ideologically motivated are far more persistent in penetrating a computer network.

In addition, computer networks are only able to complete the functions which they are programmed to do; it is us humans who are often the weakest link.

“CONFIDENTIAL INFORMATION ABOUT MY IT NETWORK IS REQUIRED TO GET A CYBER QUOTE”

Like you, the underwriters are concerned about the breach of any of your information. Keep in mind that a breach of your information could adversely affect them from a loss perspective.

Therefore information required by the underwriters is generally limited to a simple proposal form, however in some cases a teleconference may be necessary to expand on complex cases.
HOW CYBER INSURANCE RESPONDS

NETWORK DOWNTIME – DENIAL OF SERVICE
A Distributed Denial of Service attack brought down an e-commerce platform for 48 hours.

Covered Costs
— Loss of income
— Increased cost of working

NETWORK DOWNTIME – OUTSOURCERS’ ERROR
An IT outsourcer failed to provide the backup network of a retailer, resulting in a failure of their online shopping website and payment network.

Covered Costs
— Loss of income
— Increased cost of working

“PERSONAL IDENTIFIABLE INFORMATION” DATA BREACH
An e-mail server and external hard drive containing personally identifiable customer information was stolen while in the custody of a 3rd Party outsourcer.

Covered Costs
— Legal fees
— PR costs
— Forensics costs
— Costs to notify affected individual

PRIVACY REGULATORY INVESTIGATION
As a result of a privacy breach of their clients’ credit card details, a company was investigated by the local privacy regulator and was fined for breaching data protection legislation.

Covered Costs
— Legal fees
— Costs associated with the investigation
— Fines, where insurable by law

MEDIA LIABILITY
An employee posted a libellous statement about a competitor on their company Facebook page.

Covered Costs
— 3rd Party damages
— Legal fees

CYBER EXTORTION
A hacker threatened to take down a company’s network unless they pay them a ransom.

Covered Costs
— Extortion ransom
— Extortion expenses
WE HAVE SPECIALIST KNOWLEDGE
With our specialist knowledge in the sector, we are able to design innovative programmes that specifically reflect the needs of our cyber clients. For our clients the benefits are simple – expert advice ensuring the ultimate in cost-effective programme design.

WE TAKE A CONSULTATIVE APPROACH
We fully analyse your cyber exposures before proposing the most appropriate cyber risk-transfer solutions for your business.

WE UNDERTAKE CYBER RISK MANAGEMENT & ANALYTICS
We can establish your cyber risk profile utilising cyber assessment tools. This will allow you to take the appropriate actions to better protect your company’s computer network resource and information assets in order to mitigate potential cyber risks.

WE UTILISE OUR MARKET LEVERAGE
Willis has excellent market leverage due to the significant amount of premium that our cyber team places in to the market.

WE USE THE WILLIS “ONE FLAG” APPROACH
Willis’ expertise in all our offices around the world is available to you – essential for international companies who need to comply with the various international data protection laws.

WE UNDERTAKE DEDICATED CLAIMS HANDLING
We have been in the cyber market for over 10 years and our claims team have developed insightful experience in how best to deal with your cyber claim to get it resolved.

WE PROVIDE CYBER RISK UPDATES
Our clients are kept up-to-date with the latest cyber trends via bulletins, seminars and workshops.

To learn more about your business’ cyber risks or to approach us to act as your insurance broker, please contact:

Jasper Goring
T: +44 (0)20 3124 7147
E: Jasper.Goring@willis.com