



GENLIB

SPECIALISED INSURANCE & INNOVATIVE SOLUTIONS
FOR BROKERS
FSP 35482

CYBER RISKS / E-RISK

Insurer:	Certain underwriters at Lloyd's
UMA:	Camargue Underwriting Managers (Pty) Ltd
FSP No.:	6344
Approved Lloyd's Cover holder: PIN	107824DRW

SUMMARY

Please note that this document is not a substitute for the policy wording and some technical accuracy has been forfeited for that sake of easy reading.

Why has cyber risks insurance become necessary?

The incredible pace of growth in technology worldwide has produced a society which has become totally dependent on technology. This has caused a greater connectivity between people and organisations than has ever existed in human history. Unfortunately, this has brought with it new risks which traditional insurance is ill-equipped to cope with. These risks include viruses, hacking attacks, liability arising out of online publishing and cyber-crime; to name but a few.

Cyber risks insurance has been designed to address these new and unusual threats faced by organisations operating in a high-tech world.

Overview of the Camargue Cyber Risks Policy - The scope of cover under the policy includes:

- Liability and own damage risks which arise out of operating a computer network.
- Liability arising from on-line publishing (such as a web site) as well as from traditional media such as brochures can also be covered.
- An option which provides professional indemnity cover appropriate to technology companies.
- It not only covers the Insured's liabilities to others; it also provides a form of specialised business interruption cover which covers the Insured's loss of income arising out of computer down-time. In addition, the actual cost of recovering lost data is also covered.

The cover provided by the policy is found in **7 insuring agreements** which are summarised in the table below. **The client can select any combination of these.** Insuring Agreements 1 & 2 apply are for **Tech PI (Professional Indemnity)** and apply to IT companies only. These companies may also select to add Insuring Agreements 3,4,5,6,7.

All other companies may only select from Insuring Agreements 3,4,5,6,7.

INSURING AGREEMENT	BRIEF DESCRIPTION
1. (Technology) Professional Services (Tech PI only)	this provides technology-based companies with cover arising out of negligence in their work.
2. Multimedia Liability (With Tech PI only)	any loss arising out of any physical and/or electronic publication. This cover is usually given with PI insurance and therefore is only available to clients who take section 1 to prevent a duplication of cover given on the Insured's PI policy.
3. (Network) Security & Privacy Liability	any loss arising from the Insured's negligence in preventing a computer security breach.
4. Data Recovery & Loss of Business Income	a form of business interruption cover for disruption resulting from the downtime of the Insured's network. It also covers the cost of restoring the Insured's lost data.
5. Privacy Regulatory Defence & Penalties	any loss/claim arising out of the Insured not complying with laws relating to privacy which are insurable by law.
6. Crisis Management Costs, Customer Notification Expenses, and Customer Support and Credit Monitoring Expenses	this cover mitigates the potential damage to the Insured's brand (own damage) and liability arising out of compliance with privacy legislation such as notification costs.
7. Data Extortion	any loss/claim arising from ransomware where the Insured's systems are affected.

It is likely that a claim/circumstance could trigger different sections of a cyber policy. For example, should the client suffer a ransomware event where their systems are locked, data is encrypted and/or data is stolen. This could trigger Section 4 | Data recovery and loss of income, Section 5 | Privacy regulatory defence and penalties, Section 6 | Crisis management costs and Section 7 | Data extortion.

It is important to note the difference between a Cyber and Commercial Crime policy. A Cyber policy relates to a data loss whereas a Commercial Crime policy relates to the theft of funds.

Hacking of a bank account for financial gain only will be covered under a Commercial Crime policy whereas hacking a system to obtain a set of data or locking user out of a system would be covered under a Cyber policy.

A **Commercial Crime** policy provides cover 4 areas of coverage:

1. **Employee Dishonesty:** Any loss of money and/or property belonging to the insured directly from any dishonest or fraudulent act of an employees.
2. **Computer Fraud:** The insured is hacked and the hacker gains access to their banking profile and transfers the insured's funds out to themselves. Alternatively, the insured is hacked, and the hacker makes use of a computer virus which introduces a malicious code causing the insured to pay out money to the hacker. It is important to note that it is the insured's own computer network which has been hacked. There must be a direct financial loss.
3. **Extortion:** The insured (CFO, finance team member) receives a threat from someone threatening to hurt a family member, for example, unless they pay a certain amount of money.
4. **Fraudulent Transfer Instruction:** The insured normally give instructions to the bank to pay his client but this time, a third party give the bank instructions as if he is the insured. The bank falls for this and transfers the insured's funds out to the client (actually the third-party fraudster). Although it can be argued that the bank is liable for their negligence in processing instructions from an illegitimate party, the client can claim back from the Crime policy, and we subrogate against the bank/their insurers.

It is important to note that the above does not provide cover for when the employee is tricked into paying a fraudulent invoice/instruction. The insured's financial institution needs to be tricked by the third party, not the other way around, see below screenshot:

The sections below provide a more detailed explanation of the cover provided by these insuring agreements.

1) Insuring Agreement 1 – (Technology) Professional Services

Technology Professional Services means **your** business services, which are performed for and on behalf of **your** clients or customers in the ordinary course of **your** business. Such services include, but are not limited to, the design or sale of any products relating to the provision information technology services, data processing services, installation of products, design, development, integration, or configuration of a electronic communication network or any aspect thereof, web design and content delivery, and **technology professional services** stated in the **schedule**.

This Insuring Agreement 1 relates to Tech PI (Professional Indemnity) and is applicable only to those companies whose business is described by the definition of Technology Professional Services.

This section covers liability arising out of the Insured providing a business service to its customers.

❖ **Covers a pure economic loss liability caused by negligence and**

- Arising out of the Insured's ordinary business services performed for customers; and
- Includes design, sale, installation, development of IT products and services.
- Example: The insured underestimated the client's internet traffic and as a result specified an inadequate system causing the client to suffer a loss of business.

❖ **Defamation, product disparagement**

- Defamation example: An agent of the bank's outsourced call centre calls the bank's customer a crook. The customer sues the bank for defamation and the bank in turn sues the call centre. If the call centre was the insured, then they would need Professional Services cover.

❖ **Copyright infringement**

- Example: The broker's IT developer builds a program partly using code belonging to someone else. The owner of that code could sue the broker for copyright infringement and also stop them from using that program. The broker would then sue the IT developer and the IT developer's policy would respond.

2) Insuring Agreement 2 – Multimedia Liability

This insuring agreement relates to Tech PI (Professional Indemnity) and is only provided with Insurer Agreement 1.

This section covers the Insured's liability arising out of any physical or electronic publication. Unlike the E&O section, which covers liability caused by work done for a customer's benefit, this section covers the Insured's liability arising out of its own internet, marketing, and advertising activities.

❖ **Defamation, product disparagement**

- Example: "Our product is the only product in the market which has passed the 24-hour reliability test." A competitor may dispute this showing that their product also passed the 24-hour reliability test. They might then sue the Insured, claiming that the untruthful information on the brochure has unjustly enriched the Insured at the competitor's expense.

❖ **Invasion of Privacy**

Legally, an invasion of privacy may include any of the following:

➤ Publication of private facts

- Example: When a plumber publicized his skill in sorting out the on-going cockroach infestation problems at the local Big-M Restaurant, the restaurant suffered a loss of income.

- Example: A case study illustrating cost savings shows the customer in a bad light. Although names have been removed it is still possible for people to establish who the customer is.
- Includes the release of employee information
- Example: As part of a misguided PR campaign the company releases the following statement “Our equity policy ensures we give priority to employing HIV+ people.” As a result of this, the company’s employees feel aggrieved as the general public now considers them “infected”.

➤ Placing a person in a false light

Thabo’s butchery publishes a flyer advertising their monthly special on pork chops. The graphic work is done by his teenage daughter who ‘Photoshops’ the image of an actress so that it appears she is participating in the butchery. Later, the actress’ lawyers bring an action of defamation against the butchery because she is a vegetarian and does not want to be associated with a butchery.

➤ Unauthorised appropriation of a person’s name or likeness

Example: An IT company’s web site listed its customers. One of the customers, GreenBank, acted against them claiming that the IT company is unlawfully trading off the GreenBank brand by suggesting that this reputable bank has found the IT company a worthy trading partner.

➤ Intrusion into a person’s sphere

Example: The Insured’s HR manager bugged the office to determine if the sexual harassment charges against the CEO were valid.

➤ The collection of personal data

While studying his psychology qualification, the Insured’s manager secretly collects data related to the employees eating, social and hygiene habits.

❖ **Plagiarism; dilution or infringement of copyright, domain, or slogan**

Example: Wimpie’s Plumbers hires a school kid to build his website for R700. He later discovers that the pretty face on his web site was that of Kim Kardashian and her lawyers now want compensation for the use of her image.

❖ **General negligence in the release of multimedia content**

Example: The Insured forgot to tell the PR company that it did not succeed in getting James Bond to endorse its products. As a result, misleading advertising was released into the market.

3) Insuring Agreement 3 – (Network) Security and Privacy Liability

Covers the Insured’s liability arising out of its negligence in preventing a security breach or a privacy breach (hacker attack), resulting in:

❖ **Alteration, copying, theft, destruction, or unauthorised disclosure of data**

- Includes the loss or unauthorised disclosure of customer or employee information
- ID theft (including phishing)

❖ **Allowing the Insured's network to participate in an attack on a third party's computers**

- Example: Denial of access attack – using your system to flood the victim's system with data requests causing the victim's system to cease functioning
- Example: Allowing your system to spread a computer virus

❖ **Breach of privacy regulations**

- Includes negligently failing to disclose a breach in terms of laws and regulations

4) Insuring Agreement 4 – Data Recovery and Loss of Business Income

Covers the Insured's "own damage" monetary loss caused by a security breach, virus, human error causing data loss, accidental hardware destruction or a programming error. The cover applies regardless of whether the act was committed by an employee or a third party.

Cover under this insuring agreement includes:

❖ **Loss of income (before income tax) or the on-going operating expenses**

- This form of business interruption cover does not require any physical damage to machinery
- Is subject to a waiting period (this is often 24 to 48 hours)
- Example: down time arising out of an oversight during software testing

❖ **The costs to restore data and programs**

❖ **Claims preparation costs (this includes the cost of a forensic investigation)**

❖ **Increased cost of working**

- Example: the cost of hiring external equipment, alternative premises and even staff overtime pay incurred in order to rectify the situation

❖ **Public relations costs**

5) Insuring Agreement 5 – Privacy Regulatory Defence and Penalties

This section covers damages and defence costs for which the insured becomes liable as a result of a civil regulatory action. This action would be caused by a security breach or privacy breach.

- Includes cover for civil penalties and fines if they are insurable by law

6) Insuring Agreement 6 – Crisis Management Costs, Customer Notification, Support and Credit Monitoring Services

Following a security breach, the company will pay:

- Cost of employing a public relations consultant to mitigate brand damage if the security breach was publicized in the media

- PR, advertising, and related expenses required to comply with a mandatory customer notification following the compromise of personal info
- Customer support activities such as credit file monitoring and ID theft education

7) Insuring Agreement 7 – Data Extortion

The company will reimburse the Insured in respect of:

- Extortion money paid to terminate a threat of corruption or damage to programmes and information held on a computer network
- Other related expenditure, such hiring a consultant to establish if the threat is for real



Significant Policy Exclusions

The following list highlights some of the policy's exclusions:

❖ Reasonable foreseeability

- There is no cover for liability arising out of acts which the insured could reasonably have foreseen would lead to a claim.

❖ Third Party infrastructure failure

- There is no cover for liability arising out of the failure of third-party equipment which is not under the Insured's control. This applies to both electrical and mechanical failures.
- Example: liability caused by an Eskom power failure.
- Remember: this exclusion also applies to damage which is caused by a power spike.

❖ Gradual deterioration

- The policy excludes losses arising out of progressive or gradual deterioration.
- Example: There is no cover for a loss which could have been prevented by properly maintaining the computers and other equipment.

❖ Costing

- There is no cover for liability arising out of incorrect or inadequate price or cost estimates or product descriptions.

❖ Liability arising out of ceasing to provide a product or service

- Example: The Insured decides to stop providing technical support for an old product. As a result, these old machines stop working and the customers suffer a financial loss. There would be no cover if they sued the Insured for this financial loss.

❖ Liability arising out of gambling, prizes, coupons, pornography, alcohol, tobacco, drugs, etc. is expressly excluded Unfair competition. There is no cover for liability arising out of:

- anti-competitive behaviour
- violating a restraint of trade
- deceptive trade practices

❖ FICA violations

- There is no cover for liability arising out of a violation of the Prevention of Corrupt Activities Act of the Financial Intelligence Centre Act.
 - This exclusion applies to the Privacy Regulatory Defence and Penalties.
- ❖ **Government**
- There is no cover under the Professional Services section for claims brought against the Insured by any government - in its capacity as a customer - if the claim arises out of a violation of the Prevention of Corrupt Activities Act of the Financial Intelligence Centre Act
- ❖ **Bodily injury**
- Injury includes death and sickness
 - Mental anguish is covered if it results from the trauma of a breach of privacy and the like.
- ❖ **Property Damage**
- There is no cover for loss, destruction, and corruption of tangible property. This exclusion does not apply to data which is not tangible property.
- ❖ **Fire & perils**
- There is no cover for liability arising out of fire, flood, earthquake, etc.
 - However, if the fire & perils event causes an insured event (such as the loss of data) then there would be cover for the insured event.
 - Example: This exclusion would not apply if the tsunami destroyed the Insured's data centre as well as the back-up site.
 - Remember: There is no cover for the hardware itself, only the data and the consequential loss are covered.
- ❖ **Assumed liability**
- There is no cover if the Insured takes over someone else's liability (unless the Insured would have been liable anyway).
- ❖ **Beta Testing**
- There is no cover for any loss of data and income arising out of using programs which are not production ready.
- ❖ **Unlicensed programs**
- There is no cover for wilful acts such as knowingly using unlicensed programs.



Claims Made

The policy is issued on a claims-made basis which means that:

- The event causing the claim must occur after the Retroactive Date but before expiry of the policy
- The Insured must become aware of the possibility of a claim during the period of insurance. The Insured must immediately notify the Insurers if they become aware of a possible claim.



Risk Management Services included in the Policy cover:

M³

In line with Camargue's M3 philosophy of **managing, mitigating** and **migrating** critical business risks, policyholders across all product lines insured through Camargue Underwriting Managers (Pty) Ltd may access the below risk management services.

#	Service	Service Provider	Benefit to Client
1	Private Arbitration	Tokiso Dispute Settlement	Alternative options to costly litigation in commercial and employment disputes
2	Cyber Vulnerability Scan (CVS)	Cyber Safe Consultants	Automated vulnerability assessment. Click here to find out more.
3	Crisis Communication & Public Relations	PR Expert / Rianette Cyber Wellness	Public relations support and media disaster management
4	Legal Support	Everingham Attorneys	Contract vetting and management
5	Telephonic Services	Legalex (Pty) Ltd	Legal support on most commercial legal matters
6	Brit Data Safe	ePlace Solutions Inc.	<ul style="list-style-type: none">• Phishing Simulation• Online Training• Training Coordinator• Unlimited Advice – cybersecurity, compliance issues, technical questions• Securityvue Cyber Scan• Knowledge Center• News and Alerts

More About Brit Data Safe

Brit DataSafe is a suite of risk management tools and services to proactively manage cyber exposure for the evolving world of data protection and privacy risk, providing the ability to respond quickly and effectively in the event of a data breach. The Brit DataSafe platform is provided by ePlace on behalf of Brit Insurance, who are a capacity provider to Camargue Underwriting Managers. There is no additional cost for the use of the platform.

Training Coordinator

Finding the time to implement cybersecurity training across your organization can be a challenge. The Training Coordinator can do it for you! The Training Coordinator will send training instructions, track course assignments and deliver a completion report for compliance and regulatory purposes.

Phishing Simulations

Work with our Training Coordinator who can deploy a simulated phishing campaign on your employees. We will send phishing emails to your employees to help identify those susceptible to phishing attacks. Results are delivered to you and our Training Coordinator can help implement online training courses to educate the susceptible employees.

Online Training

Human error is the biggest risk to cybersecurity. Training and educating employees are paramount to ensure security of business systems. Through 15 online training modules covering breaches, phishing, ransomware, data security, safeguarding information, and more, you've taken a step towards cyber protection.

Unlimited Advice

Contact us to review your cybersecurity posture, compliance issues, or technical questions. Our team of privacy attorneys and technical experts will help you address any question you have, big or small.

SecurityVue Cyber Scan

Use this report to identify areas of cybersecurity risk based on multiple vulnerability scans of your public facing systems and applications. The report also includes results from over 100 malware and blacklist database lookups. To get a report, reach out to our experts who can run the scan of your public facing systems and applications and provide you with guidance to address the identified risks.

Knowledge Center

Save time with self-service, 24/7, online access to sample data security policies, procedures, and agreements, incident response planning materials, risk assessment tools, vendor management resources, step-by-step compliance guidance, and more.

News and Alerts

Stay up to date with the latest risks and solutions with our monthly newsletter, poster reminders, training emails, and cyber alerts when needed.

For more information

Contact the Experts at cyberteam@eplaceinc.com

Register and Login

Go to DataSafe.BritInsurance.com

Click "Register" link at the center of the page and follow the registration instructions.

Your Sign-Up Code is your policy number.