

**SCaN** PROTECT

Willis

SECURITY, CYBER AND  
NETWORK INSURANCE

# SECURING YOUR FUTURE



**Businesses today rely heavily on computer networks. Using computers, and logging on to public and private networks has become second nature to us in our personal and professional lives, and our IT systems are central to our ability to do business.**

## **THE RISK**

We all constantly produce and save data, surf the net, upload content, and send emails daily. It is difficult to recall how we were ever able to manage without such technologies and the benefits they bring.

With all of the advances in technology, many companies struggle to secure networks, keep information confidential and avoid major issues.

Cyber risks are not limited to large E-commerce companies and those undertaking transactions over the internet. Any organisation that stores personal data, is reliant on computer or telephone networks, holds digital information or uses the internet can face these exposures.

### **ASK YOURSELF**

- How do I store confidential third-party information securely?
- How am I protected if a member of my staff decides to steal data, misuse information, commit fraud or just makes a mistake?
- What stops my business being hit like the bigger firms that I see in the press getting attacked?
- What are the most valuable things my business has? (customer data, intellectual property rights (IPR), reputation etc.)
- If I had a security breach tomorrow, how would I know and what would I do?
- Do I have appropriate coverage in place to handle unexpected downtime?
- Could I get all the data back if I lost a server, laptop, member of staff, filing cabinet etc?

# THE COST

## Cyber-crime costs GBP 27bn a year in the UK alone.

Hackers are increasingly targeting smaller, softer, less reactive targets since these provide a lower-risk alternative and since 2010 around 40% of all targeted attacks have been directed at small and medium enterprises (SME), compared to only 28% directed at large companies. Therefore it may be a costly mistake to believe you're fully covered by other insurances.

The gaps in more traditional insurance could include:

### PROPERTY

Property insurance is usually restricted to loss of physical property. By its nature, data is not necessarily a physical asset, and cannot be deemed to be covered under a traditional Property policy. Computer equipment and hardware is deemed to be physical property, however it is susceptible to specialist causes of damage (changes in temperature in a server room, loss of power, software related issues) which may not be covered by Property insurance.

#### SCaN PROTECT COVERS:

- Failure of Computer Hardware
- Loss of Data

### BUSINESS INTERRUPTION

To be indemnified under Business Interruption insurance, the damage must be physical. Traditional Business Interruption insurance will not uphold a claim where the interruption is due to the temperature of a server room, a software malfunction, virus or other unauthorised access. The more traditional Business Interruption insurance will also not respond to a loss of data resulting in a business interruption claim.

#### SCaN PROTECT COVERS:

- Business Income & Extra Expense

## THEFT

The theft of data is not covered under a standard Theft insurance. As in intangible asset, data is not seen to be an insurable loss under this specific type of cover. Generally, Theft insurance requires 'forced entry' to insure a loss, and as data can be stolen remotely, there will be no physical sign of an unauthorised incident. Theft insurance would usually exclude theft by an employee. If the insured were to take out 'Full Theft' cover, they take out the requirement for forced entry; however the intangible asset of data is not covered.

### SCaN PROTECT COVERS:

- Loss of Data
- Business Income & Extra Expense

## CRIME

The intention of Crime insurance is to cover theft of monies or tangible assets by employees; however data is not a tangible asset and would usually be excluded under Crime insurance. Even with a 'Computer Crime' extension, cover is normally restricted to the rectification costs only (i.e. restoration or recollection of data) with no consequential losses covered.

### SCaN PROTECT COVERS:

- Loss of Data
- Business Income & Extra Expense
- Privacy Breach Expenses

## TERRORISM

Terrorism insurance is related only to the extortion of physical assets, and physical damage thereof. The extortion of data, software and / or IT systems would not be covered under Terrorism insurance.

### SCaN PROTECT COVERS:

- Cyber Extortion Expenses

## PROFESSIONAL INDEMNITY / ERRORS & OMISSIONS

For a traditional Errors and Omissions (E&O) insurance to respond to a claim there must be some form of negligence on the insured's part. In relation to the insured's professional activities, they must be seen to have been negligent, and to have caused financial loss to a third party. Professional Indemnity insurance also excludes claims made as a result of criminal or deliberate acts of the insured or its employees.

### SCaN PROTECT COVERS:

- Disparagement, Plagiarism & Infringement
- Right to Privacy & Breach of Confidence
- Unauthorised Access & Virus Transmission
- Privacy Breach Expenses

## GENERAL LIABILITIES

General Liability insurance often excludes liability in relation to electronic data and usually excludes criminal or deliberate acts, and will not cover expenses, following a privacy breach.

### SCaN PROTECT COVERS:

- Disparagement, Plagiarism & Infringement
- Right to Privacy & Breach of Confidence
- Unauthorised Access & Virus Transmission

## HOW DO BREACHES OCCUR?



# THE SOLUTION

SCaN PROTECT can provide cover in 8 distinct but interrelated sections to YOU (1st Party Claims) and YOUR CLIENTS (3rd Party Claims). You can buy a combination of covers, so if a particular element does not apply to your business, you can simply leave it out...

- **Claims made by YOU (1st Party)**

1. Failure of Computer Hardware
2. Loss of Data
3. Business Income & Extra Expense

- **Claims made by YOUR CLIENTS (3rd Party)**

4. Disparagement, Plagiarism & Infringement
5. Right to Privacy & Breach of Confidence
6. Unauthorised Access & Virus Transmission

- **Additional Costs**

7. Cyber Extortion Expenses
8. Privacy Breach Expenses

# 24 HOUR ASSISTANCE

## EXPERT SUPPORT

We understand your business relies on effective, safe and secure information technology systems to succeed in today's competitive market. So any IT emergency, large or small that disrupts your IT systems will cost lost sales, lost production – or even lost reputation. That's why SCaN PROTECT gives you 24 hour assistance – delivered by some of the country's top legal, claims management, technical and data restoration experts.

## 24/7 EMERGENCY ASSISTANCE

Every SCaN PROTECT policyholder has access to a 24/7hour emergency helpline on: +44 (0)208 476 8603. As soon as you call, your emergency will be assessed, your insurance cover confirmed, and top experts put to work to resolve your emergency and restore your IT services.

The SCaN PROTECT 24 Hour Emergency Assistance service is delivered by Charles Taylor Adjusting, one of the world's leading international loss adjusters in close association with international law firm, Ince & Co. The team work with other leading industry experts to manage your claim, restore your systems and protect your business from further loss.

## HOW DOES IT WORK?

Every claim is different, so we don't offer a one size fits all service. Subject to your cover and limits of indemnity Charles Taylor Adjusting will package and manage an emergency assistance service to fit your needs. Here are just a few examples of how it could work for you.

- **Your IT network is lost through fire or theft or other incident:**

Technical teams will be on site as soon as possible, replacing hardware and rebuilding systems. You will be supported by the crisis management team and expert claims handlers to minimise the disruption to your operations.

- **A computer virus or cyber-attack disrupts your systems:**

Technical experts will investigate and appoint experts to restore your systems. The legal team will ensure that you have access to top lawyers to resolve any disputes and the claims management team will assist you 24/7 to get your business back up and running as quickly as possible.

- **A system failure leads to massive loss of customer data:**

Data restoration experts will immediately start work to rebuild your databases, while the crisis management experts and claims management teams will work closely with you to minimise loss and restore your operations. Any accusations of breach of privacy by your customers will be promptly managed by an expert legal team.

- **A computer hacker threatens to hold your business to ransom:**

Expert extortion management negotiators will take over the management of your case, supported by technical experts who will investigate and secure your systems against further attack.

# 1ST PARTY CLAIMS

## FAILURE OF COMPUTER HARDWARE

### THE COVER

This section provides cover for loss of, or damage to, computer hardware. Only restoration or replacement of physical property is covered under this section.

Hardware leased, rented, loaned to another is not covered, and the hardware must not be left in the open.

### CLAIM SCENARIO

The malfunction and failure of point-of-sale computer equipment meant that a retailer had to replace a large amount of hardware at their data centre at a significant cost.

## LOSS OF DATA

### THE COVER

This provides cover for costs incurred in connection with the loss or corruption of data, and the restoration of that data.

The causes of the data loss and/or corruption include:

- Network security breach, including hacking and Distributed Denial of Service (DDoS)
- Unauthorised use of the computer system
- Computer virus
- Accidental damage or destruction of data media
- Human error

### CLAIM SCENARIO

An engineering firm lost the potential revenue from a new innovation in propeller design, when the digital designs were stolen in a hack attack and the propeller was brought to market by another manufacturer.

## BUSINESS INCOME AND EXTRA EXPENSE

### THE COVER

A vital element, the Business Income and Extra Expense section helps the organisation to survive the impact of the loss of business income suffered due to the failure of computer systems.

### CLAIM SCENARIO

A software error and system malfunction leaves a City Council unable to issue traffic tickets. The estimated cost was GBP 1.5 million.

A supermarket chain suffers a system failure due to faulty hardware and data corruption. The Point of Sale system fails, as does the automatic stock ordering process, leaving the shelves empty and representing a major loss in revenue.



ONE PC IS AFFECTED BY CYBER-CRIME

# EVERY 4.5 SECONDS

WORLDWIDE.



# 3RD PARTY CLAIMS

## DISPARAGEMENT, PLAGIARISM AND INFRINGEMENT

### THE COVER

A company may become inadvertently liable to pay damages or incur costs where it is accused of one or more of the above activities, perpetrated through the use of their computer systems and websites.

### CLAIM SCENARIO

Company A pays Company B GBP 450,000 to settle an action relating to an email that incorrectly alleged Company B was about to be investigated by the Department of Trade and Industry.

An on-line retailer was sued for using a logo, images and product description without permission.

## RIGHT TO PRIVACY AND BREACH OF CONFIDENCE

### THE COVER

As more information is acquired and stored, breach of privacy or confidence is of increasing concern. This section provides protection against liability arising from such breaches.

Cover is included for:

- Invasion of privacy
- Infringement of data protection legislation
- Unauthorised use of confidential information

### CLAIM SCENARIO

A letting agent suffers a data breach and is being sued by tenants who have received letters in the name of the letting agent asking them to send rents to a new account.

A company employee of a printing firm sends a confidential price list from supplier A to supplier B allowing supplier B to target supplier A's clients offering lower prices.

## UNAUTHORISED ACCESS AND VIRUS TRANSMISSION

### THE COVER

A virus finding its way into your computer system can have a devastating effect. Similarly, the transmission of a virus to a third-party can have the same effect on their computer system.

In addition, companies who rely on your computer system to function for the continuance of their business can be severely affected should they be unable to access your computer system through a failure or denial of service attack.

### CLAIM SCENARIO

A manufacturer is unable to order parts from a key supplier as the supplier's extranet has suffered a denial of service attack. The manufacturer failed to complete orders on time.

A marketing company infected by a virus suffers a mail server failure after receiving an email containing a virus from a business associate.



HIGH-TECH CRIMINALS  
ARE RACKING UP OVER  
**100 ATTACKS  
PER SECOND**

WORLDWIDE.



# ADDITIONAL COSTS

## CYBER EXTORTION EXPENSES

### THE COVER

This section covers you in the event that your data, systems or other Cyber-related information are under threat of extortion.

Insurers may pay monies to:

- Terminate a Cyber-extortion threat
- Deal with or mitigate the threat

Details of this cover must be kept confidential and cooperation with law enforcement is essential.

### CLAIM SCENARIO

A “hactivist” group threatened an online aggregator with a Distributed Denial-of-Service (DDoS) attack unless payment was made.



## PRIVACY BREACH EXPENSES

### THE COVER

When a network or Cyber incident occurs, it can have a devastating effect on the reputation of the company and the confidence of its customers.

This section provides funds in the event of an incident to enable you to hire expert assistance to mitigate the effect of the incident.

In the event of a data breach the cost of notification of that breach to all relevant parties will also be covered.

Cover is provided for:

- Crisis management expenses
- Customer notification expenses
- Forensic costs
- Legal expenses
- PCI Security Standards Council fines

### CLAIM SCENARIO

An insurance broker writes to 51,000 UK customers after the loss of a back-up tape containing details on over 500,000 customers

**40%** OF ALL TARGETED ATTACKS HAVE BEEN DIRECTED  
AT SMALL AND MEDIUM-SIZED BUSINESSES

# FINEX GLOBAL

## **SPECIALIST KNOWLEDGE**

FINEX Global is a division of the leading global insurance broker Willis Ltd, with teams of experts providing specialist advice and services to our clients. Cyber issues are multi-disciplinary, spanning network security, online media, intellectual property, personal privacy, enabling technology, etc. Each component has its own risks and our approach produces a coordinated and comprehensive response.

## **EXCLUSIVE WORDING**

SCaN PROTECT is an exclusive wording to Willis that has been designed in conjunction with a major Cyber insurer - ACE European Group Limited.

We aim to provide our clients with a superior service, competitive premiums and Cyber insurance cover that goes beyond the 'off the shelf' policy typically offered to SMEs.

## **EXPERT CLAIMS TEAM**

With over 10 years experience dealing with Cyber insurance, our dedicated claims experts have in-depth knowledge of the claims process. We are committed to assisting our clients in getting their claim resolved promptly and with the minimum amount of disruption.

# NEXT STEPS

If you are concerned about Cyber risks, contact us and arrange an initial consultation to start mapping out your risks:

**Darryl Brophy**

T: +44 (0)1473 223819

E: [darryl.brophy@willis.com](mailto:darryl.brophy@willis.com)

**Gillian Gee**

T: +44 (0)1618 292648

E: [gillian.gee@willis.com](mailto:gillian.gee@willis.com)

**Martin Berry**

T: +44 (0)1473 223726

E: [martin.berry@willis.com](mailto:martin.berry@willis.com)

Statistics used on pages from Cyber Security & Information Assurance, 2011.

Statistics used on pages 5 & 7 are based on the 539 organisations responding to Information Security Breaches Survey 2010, PwC.

Statistic used on page 9 from Symantec's Threat Awareness Survey.

Willis Limited, Registered number: 181116 England and Wales.

Registered address: 51 Lime Street, London, EC3M 7DQ.

A Lloyd's Broker. Authorised and regulated by the Financial Conduct Authority.

10543/08/13