CYBER CRIME

islands
TRUST & CORPORATE

islands
TRUST & CORPORATE

A Top Down View Of Our Group In 2020

ISLANDS BY NUMBERS

83,500
ACTIVE POLICIES

96%
CLAIMS PAID

170,515
CALLS TAKEN (12 MONTHS)

7512
CLIENTS THROUGH OUR DOORS

97%
RENEWAL RATE

£42,000
SPONSORSHIPS IN CI

1978

The Islands Insurance Brokers Ltd Guernsey & Alderney is established

1987

NFU Mutual acquisition of the Group (consisting of MJ Touzel Insurance Brokers Ltd (Jersey) and Islands Insurance Brokers Ltd Guernsey & Alderney)

2016

Group rebrands as Islands

148
STAFF

3
OFFICES

NFU Mutual
DELEGATED AUTHORITY

islands
TRUST & CORPORATE

Manage Your Cyber Risk With Insurance That Has You Covered

CYBER CRIME INSURANCE

WHY YOU NEED IT

Cyber is one of the most frequently discussed topics across all types of business. The risk to large corporations is not something new; however, Cyber criminals are now frequently targeting SMEs. These risks are evolving fast and are often not fully understood. They are a concern for any business reliant on IT systems and on the use of personal or confidential data, irrespective of size or industry sector.

As soon as a cyber incident occurs, which can be triggered by an employee's inadvertent click of a link in an email, the company can be exposed to a severe reputational threat which will also affect the company financially.

A cyber policy should be more than just an insurance policy providing financial resources following a cyber breach. Perhaps even more importantly, it can provide access to specialist cyber responses and technical services, knowledge, and expertise to avert and mitigate the losses to the company.

This includes:

- Immediate access to specialist cyber response and technical services, such as IT forensic expertise, legal advice and public relations services following a cyber incident.
- Access to complimentary and discounted risk management services to assist companies avoid or minimise damage caused by cyber incidents.
- Indemnify the business in respect of claims by third parties, including regulators, arising from privacy or network breaches and intellectual property infringements. This can include defence and investigation costs and awards and damages.
- In respect of the business' own losses, the policy can cover costs incurred in notifying third parties of data breaches, reimburse costs incurred to recover lost data and restore computer systems, losses arising from extortion incidents (i.e. ransomware), theft of funds arising from cybercrime (i.e. social engineering) and loss of revenue to the business and increased costs incurred whilst the IT system is not operational, in addition to losses arising from reputational damage.

COVER AND BENEFITS

Incident Response Services - Provide immediate access to IT forensic expertise, legal advice and public relations services who will work with you from those first critical moments of an incident to avert or minimise the loss and reputational damage to your business and get you up and running as soon as possible.

Loss of Revenue - Whilst your computer system is not operational due to a cyber attack or privacy incident, a cyber policy can reimburse you for loss of profit and the additional costs incurred. Even once the incident has been resolved, the company may suffer further financial losses arising from subsequent reputational damage which can also be covered, helping to protect the company's future earnings.

Third Party Notification Costs - Where there has been a loss or disclosure of personal data, there may be a regulatory requirement to notify affected third parties of the incident, including a need to establish call centres, provide credit monitoring and identity monitoring, as well as other services which can be costly and can be covered under a cyber policy.

Third Party Allegations - Should a third party make an allegation against you arising from a data breach or unintentional transmission of malware to their computer system, the policy can defend you as well as settle a third party's costs and compensation awarded against you. Cover is also provided for regulatory investigations arising from a personal data breach, including settlement of insurable civil fines.

Computer System Damage - Where your computer system has been damaged or lost as a result of a cyber incident, a cyber policy can cover the costs incurred by the business to restore your computer system including your hardware, software and data.

Theft of Funds - Where there has been a theft of the company's funds, be this from a social engineering attack including the settlement of a fraudulent invoice, acting upon the instruction purporting to be from a senior executive or the unauthorised transfer from your bank account, a cybercrime policy can reimburse you for the lost amounts.

Extortion Cover - Where you are subject to a ransom demand arising from a threat to, or following the introduction of malware to your computer system, denying you access to your computer system or threatening to destroy or release confidential information, a cybercrime policy can reimburse you for the costs incurred, including the ransom paid.

Media Liability - Where there has been an allegation of defamation or breach of intellectual property rights against you arising from your media content, cover can be provided for your costs to defend and your liability for the claimant's costs and damages awarded.

Payment Card Industry Cover - Where there has been a breach of the Payment Card Industry Data Security Standards, the policy can cover the costs incurred, including fines.

Knowledgable Specialist Staff - Our expertise enables us to identify the key risks to your business and with our access to specialist cyber insurers, provide a cyber policy tailored to your needs.

UK CYBERSECURITY STATISTICS

What you need to know about the cyber world today
Information sourced from CSO | www.csoonline.com

88%
UK companies have suffered a data breach in the past 12 months

41%
UK consumers claim they won't return to a business post-breach

EVERY 19 SECONDS
A UK small business is successfully hacked

3/10
UK organisations state they've lost customers after data breach

£640,000
AVERAGE REMEDIATION COST AFTER SUCCESSFUL RANSOMWARE ATTACK

1/3
Of AIG's cyber insurance claims in EMEA 2018 were for Business E-Mail Compromise attacks

50%
Of cyberattacks in the UK **involve phishing** (that's 20% higher than global ave)

140,000
Number suggesting a skilled cyber security personnel shortage across EMEA

75%
Did you know? 75% of the UK data flows through the EU.

£183 MILLION
BIGGEST FINE ISSUED BY THE ICO

Check your mail
1/3722 e-mails in the UK is a phishing attempt. Almost 55% of all e-mail in the UK is spam.

Train, don't blame!
22% of UK org's do not provide employees with regular security awareness training for e-mail.

Support is at hand
There are an estimated 1,221 firms in the UK providing cyber security products and services. Talk to us, we can help.

CONTACT US

WILLIAM WOODFORD
SALES DIRECTOR
T: 01481 738040
M: 07781 135065
E: WILL.WOODFORD@ISLANDS.GG
W: TRUST.ISLANDS.INSURE

RICKARDT DE BEER
BUSINESS DEVELOPMENT
T: 01481 738036
M: 07839 726140
E: RICKARDT.DEBEER@ISLANDS.GG
W: TRUST.ISLANDS.INSURE

islands
TRUST & CORPORATE

Manage Your Cyber Risk With Insurance That Has You Covered

CYBER CRIME INSURANCE

WHY YOU NEED IT

Cyber is one of the most frequently discussed topics across all types of business. The risk to large corporations is not something new; however, Cyber criminals are now frequently targeting SMEs. These risks are evolving fast and are often not fully understood. They are a concern for any business reliant on IT systems and on the use of personal or confidential data, irrespective of size or industry sector.

As soon as a cyber incident occurs, which can be triggered by an employee's inadvertent click of a link in an email, the company can be exposed to a severe reputational threat which will also affect the company financially.

A cyber policy should be more than just an insurance policy providing financial resources following a cyber breach. Perhaps even more importantly, it can provide access to specialist cyber responses and technical services, knowledge, and expertise to avert and mitigate the losses to the company.

This includes:

- Immediate access to specialist cyber response and technical services, such as IT forensic expertise, legal advice and public relations services following a cyber incident.
- Access to complimentary and discounted risk management services to assist companies avoid or minimise damage caused by cyber incidents.
- Indemnify the business in respect of claims by third parties, including regulators, arising from privacy or network breaches and intellectual property infringements. This can include defence and investigation costs and awards and damages.
- In respect of the business' own losses, the policy can cover costs incurred in notifying third parties of data breaches, reimburse costs incurred to recover lost data and restore computer systems, losses arising from extortion incidents (i.e. ransomware), theft of funds arising from cybercrime (i.e. social engineering) and loss of revenue to the business and increased costs incurred whilst the IT system is not operational, in addition to losses arising from reputational damage.

COVER AND BENEFITS

Incident Response Services - Provide immediate access to IT forensic expertise, legal advice and public relations services who will work with you from those first critical moments of an incident to avert or minimise the loss and reputational damage to your business and get you up and running as soon as possible.

Loss of Revenue - Whilst your computer system is not operational due to a cyber attack or privacy incident, a cyber policy can reimburse you for loss of profit and the additional costs incurred. Even once the incident has been resolved, the company may suffer further financial losses arising from subsequent reputational damage which can also be covered, helping to protect the company's future earnings.

Third Party Notification Costs - Where there has been a loss or disclosure of personal data, there may be a regulatory requirement to notify affected third parties of the incident, including a need to establish call centres, provide credit monitoring and identity monitoring, as well as other services which can be costly and can be covered under a cyber policy.

Third Party Allegations - Should a third party make an allegation against you arising from a data breach or unintentional transmission of malware to their computer system, the policy can defend you as well as settle a third party's costs and compensation awarded against you. Cover is also provided for regulatory investigations arising from a personal data breach, including settlement of insurable civil fines.

Computer System Damage - Where your computer system has been damaged or lost as a result of a cyber incident, a cyber policy can cover the costs incurred by the business to restore your computer system including your hardware, software and data.

Theft of Funds - Where there has been a theft of the company's funds, be this from a social engineering attack including the settlement of a fraudulent invoice, acting upon the instruction purporting to be from a senior executive or the unauthorised transfer from your bank account, a cybercrime policy can reimburse you for the lost amounts.

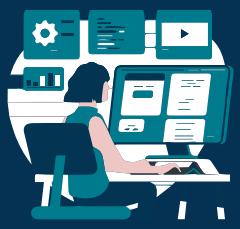
Extortion Cover - Where you are subject to a ransom demand arising from a threat to, or following the introduction of malware to your computer system, denying you access to your computer system or threatening to destroy or release confidential information, a cybercrime policy can reimburse you for the costs incurred, including the ransom paid.

Media Liability - Where there has been an allegation of defamation or breach of intellectual property rights against you arising from your media content, cover can be provided for your costs to defend and your liability for the claimant's costs and damages awarded.

Payment Card Industry Cover - Where there has been a breach of the Payment Card Industry Data Security Standards, the policy can cover the costs incurred, including fines.

Knowledgable Specialist Staff - Our expertise enables us to identify the key risks to your business and with our access to specialist cyber insurers, provide a cyber policy tailored to your needs.

DO YOU NEED CYBER CRIME INSURANCE?



Your business is dependent on a computer system to operate efficiently.

Its disablement would be detrimental to your ability to service your clients and generate income.

You pay and receive payment by electronic means and interception of payment instructions could result in loss of income to your business.

You hold personal / 3rd party confidential data.

Should it be captured and released into the public domain by accident or by criminal action it could negatively impact your reputation and future revenue.

Should a cyber or data breach occur such as a ransomware attack, you don't have access to the specific skills and expertise required to assist you in remedying the incident, minimising the disruption and damage to your business and importantly your clients.

You would value additional products and services that could support your company in building up your resilience to cyber or data breach incident.

CONTACT US

WILLIAM WOODFORD
SALES DIRECTOR
T: 01481 738040
M: 07781 135065
E: WILL.WOODFORD@ISLANDS.GG
W: TRUST.ISLANDS.INSURE

RICKARDT DE BEER
BUSINESS DEVELOPMENT
T: 01481 738036
M: 07839 726140
E: RICKARDT.DEBEER@ISLANDS.GG
W: TRUST.ISLANDS.INSURE

islands
TRUST & CORPORATE

Manage Your Cyber Risk With Insurance That Has You Covered

CYBER CRIME INSURANCE

WHY YOU NEED IT

Cyber is one of the most frequently discussed topics across all types of business. The risk to large corporations is not something new; however, Cyber criminals are now frequently targeting SMEs. These risks are evolving fast and are often not fully understood. They are a concern for any business reliant on IT systems and on the use of personal or confidential data, irrespective of size or industry sector.

As soon as a cyber incident occurs, which can be triggered by an employee's inadvertent click of a link in an email, the company can be exposed to a severe reputational threat which will also affect the company financially.

A cyber policy should be more than just an insurance policy providing financial resources following a cyber breach. Perhaps even more importantly, it can provide access to specialist cyber responses and technical services, knowledge, and expertise to avert and mitigate the losses to the company.

This includes:

- Immediate access to specialist cyber response and technical services, such as IT forensic expertise, legal advice and public relations services following a cyber incident.
- Access to complimentary and discounted risk management services to assist companies avoid or minimise damage caused by cyber incidents.
- Indemnify the business in respect of claims by third parties, including regulators, arising from privacy or network breaches and intellectual property infringements. This can include defence and investigation costs and awards and damages.
- In respect of the business' own losses, the policy can cover costs incurred in notifying third parties of data breaches, reimburse costs incurred to recover lost data and restore computer systems, losses arising from extortion incidents (i.e. ransomware), theft of funds arising from cybercrime (i.e. social engineering) and loss of revenue to the business and increased costs incurred whilst the IT system is not operational, in addition to losses arising from reputational damage.

COVER AND BENEFITS

Incident Response Services - Provide immediate access to IT forensic expertise, legal advice and public relations services who will work with you from those first critical moments of an incident to avert or minimise the loss and reputational damage to your business and get you up and running as soon as possible.

Loss of Revenue - Whilst your computer system is not operational due to a cyber attack or privacy incident, a cyber policy can reimburse you for loss of profit and the additional costs incurred. Even once the incident has been resolved, the company may suffer further financial losses arising from subsequent reputational damage which can also be covered, helping to protect the company's future earnings.

Third Party Notification Costs - Where there has been a loss or disclosure of personal data, there may be a regulatory requirement to notify affected third parties of the incident, including a need to establish call centres, provide credit monitoring and identity monitoring, as well as other services which can be costly and can be covered under a cyber policy.

Third Party Allegations - Should a third party make an allegation against you arising from a data breach or unintentional transmission of malware to their computer system, the policy can defend you as well as settle a third party's costs and compensation awarded against you. Cover is also provided for regulatory investigations arising from a personal data breach, including settlement of insurable civil fines.

Computer System Damage - Where your computer system has been damaged or lost as a result of a cyber incident, a cyber policy can cover the costs incurred by the business to restore your computer system including your hardware, software and data.

Theft of Funds - Where there has been a theft of the company's funds, be this from a social engineering attack including the settlement of a fraudulent invoice, acting upon the instruction purporting to be from a senior executive or the unauthorised transfer from your bank account, a cybercrime policy can reimburse you for the lost amounts.

Extortion Cover - Where you are subject to a ransom demand arising from a threat to, or following the introduction of malware to your computer system, denying you access to your computer system or threatening to destroy or release confidential information, a cybercrime policy can reimburse you for the costs incurred, including the ransom paid.

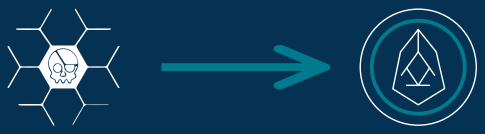
Media Liability - Where there has been an allegation of defamation or breach of intellectual property rights against you arising from your media content, cover can be provided for your costs to defend and your liability for the claimant's costs and damages awarded.

Payment Card Industry Cover - Where there has been a breach of the Payment Card Industry Data Security Standards, the policy can cover the costs incurred, including fines.

Knowledgable Specialist Staff - Our expertise enables us to identify the key risks to your business and with our access to specialist cyber insurers, provide a cyber policy tailored to your needs.

CYBER CRIME INSURANCE CLAIMS EXAMPLE

CRYPTOJACKING CAUSES CRASHES



WHAT IS IT?
Cryptocurrency mining is the method of verifying cryptocurrency transactions, instead of buying it, and getting a portion of the transaction in cryptocurrency.

For this you require massive computing power and Capital outlay.

Cryptojacking is when a large computing resource is hijacked. It is usually done in one of two ways:
- Downloaded via phishing e-mail with link or attachment;
- Malicious code on website or digital advert which contains the mining software and it works in the background while the visitor is online.

WHAT TYPICALLY HAPPENS?
These codes / attachments have a debilitating effect on the victim's networks.

Search rankings drop / visibility drops / fulfilments drop and these all result in a reduction in sales or productivity. You also cannot manually increase your search ranking because it is algorithmic by nature.

In this example, to mitigate Business Interruption, a third party who specialises in search engine optimisation needed to assist in boosting the ranking through an Ad Words campaign.

WHAT DOES THIS HIGHLIGHT?
- The impact of a cyber event can last much longer than you initially expect.
- Even after restoring systems, normality is not automatically guaranteed.
- Indemnity periods vary between policies. This incident clearly shows you might require full cover for the incident, the recovery, and the business interruption right up to the point until the client is in the same financial position as they were before the incident.

Source Cyber claims case study: Search engine setback | CFC Underwriting

CONTACT US

WILLIAM WOODFORD
SALES DIRECTOR
T: 01481 738040
M: 07781 135065
E: WILL.WOODFORD@ISLANDS.GG
W: TRUST.ISLANDS.INSURE

RICKARDT DE BEER
BUSINESS DEVELOPMENT
T: 01481 738036
M: 07839 726140
E: RICKARDT.DEBEER@ISLANDS.GG
W: TRUST.ISLANDS.INSURE