DataGuard Advantage

It’s not if, but when.

The ACE in your pack.

DataGuard Advantage

Are you ready?

When it comes to the risk of a major problem associated with computer hardware or data, it's not so much if, as when.

Information technology is so powerful and so ever-present in business life that we almost take it for granted. But we should remain vigilant about the risks it brings. From hardware failure to hacking to the possibility of defaming a rival, there are many threats that could result in financial loss or damaged reputation.

The cyber insurance provided by DataGuard Advantage provides essential peace of mind.

We no longer simply harness the power and exploit the potential of information technology – we actually depend on it. And because it is woven into the fabric of business life, it generates significant risk that brokers and their clients must address.

While a standard property and liability policy might cover IT risks, there is no guarantee that it will be sufficiently detailed and comprehensive. One potential issue with a standard policy is that it might exclude hardware and/or mobile devices. Or it might not cover business interruption caused by a virus, or fund increased cost of working while systems are down.

It might simply be that the standard policy limits are inadequate. Surveys suggest the cost of computer failure can run to £10,000 per hour or even £1m a day for big organisations. Limits are clearly worth a second look.

The more we embrace IT, the bigger and more complex the risks become. For example, a business might unwittingly infringe the intellectual property rights of others through online use of images and text, raising the possibility of intellectual litigation.

The loss of sensitive personal or business information is also becoming more prevalent and as companies hold more and more data this risk will become more relevant.

Tangled webs

An e-commerce platform is a must-have in many sectors, but what if a website crashes?

Sales will be lost as customers grow frustrated and turn to rivals. What if email goes down for any length of time? Routines would be crippled.

Then there are back-end processes: stock control is massively important, especially if just-in-time ordering is used. Delivery is likewise crucial. Retailers rely on point-of-sale systems – protracted downtime would damage income and reputation.

Every industry has its vulnerabilities. How would a hotel chain cope if its online booking and room management system was out of commission? What about a car-hire organisation suddenly unable to keep track of its vehicles? Any business running a helpdesk would suffer if it was unable to service customer enquiries.

Back to business

Whatever the danger, whatever the sector, all firms need to restore websites and communications networks swiftly so that they can return to "business as usual" and minimise any losses, be they financial or affecting market standing.

Specialist cover comes into play when IT staff do not have the skills to rebuild a system, obliging the user to bring in external contractors. Costly arrangements might also be needed to provide a temporary IT solution while facilities are restored.

Hack attack

Cyber fraud is the world's biggest type of fraudulent activity thanks to the value of the prize: credit card data that can be sold on through the criminal community. All companies, regardless of size and sector, are targets. There is also the threat of destructive malware, which is growing in potency and frequency of use. Symantec reports that a PC somewhere in the world is infected every 4.5 seconds. If – or rather when – a company is infected, it faces the risk of transmitting the virus onto a third party, precipitating a claim for damages.

Brokers and clients need to quantify the risks and consider whether a bespoke cyber risks solution is required. Any potential overlap between the firm's standard policy and the specialist cover can be avoided by choosing a cyber risks policy such as DataGuard Advantage, which allows the required cover to be selected from a menu.

Social notworking?

There is also the impact of social networking. A business may be happily uploading content and boosting its online presence, but can it be confident that all its online material is risk-free? What if employees and/or customers can add their own comments or other items? Can a site be policed?

Companies need to know if they are protected if something goes awry, such as when someone claims to have been defamed by content put out under the company's name.

> “a PC somewhere in the world is infected every 4.5 seconds. If – or rather when – a company is infected, it faces the risk of transmitting the virus onto a third party, precipitating a claim for damages…”

The DataGuard Advantage

DataGuard Advantage has six sections of cover to provide businesses with the flexibility to tailor the cover to their own needs:

- Computer hardware property cover
- Network restoration in the event of a loss of data, communications, applications, etc.
- Loss of business income and extra expense
- Liability in respect of disparagement, plagiarism and infringement through the use of the internet and email
- Liability in respect of data breaches, including costs associated with the notification of clients/customers post breach
- Transmission of a virus to a third-party and denial of access.

The ACE in your pack

Stability

We are a leading provider of insurance and reinsurance in Europe. Headquartered in London with a network of offices across 20 European countries, ACE Europe is part of The ACE Group of Companies, one of the world’s largest providers of property and casualty insurance, reinsurance and financial services. ACE European Group Ltd holds a financial strength credit rating of AA- (very strong) from Standard & Poor’s and A+ (superior) from AM Best.

Innovation

We offer a market-leading proposition for our customers with our extensive breadth and depth of organization, both in terms of products, geographic reach, underwriting and claims expertise and engineering capabilities. We pride ourselves on the quality and experience of our staff, who are specialists in their individual fields. Using this experience, we focus on products and services in market segments where this specialised knowledge creates a natural alliance and supports the key business goals of our customers.

Experience and expertise

ACE has a highly respected and knowledgeable underwriting team. We work with brokers and clients to provide a high quality insurance and claims service that is tailored to the needs of companies working across the commercial spectrum.

We are renowned in the insurance market for our major risk/multinational underwriting expertise. ACE is one of the very few insurers with the ability to underwrite and structure a global insurance programme, through the utilisation of its own offices worldwide and its global network of partner insurers.

DataGuard Advantage

Technical details

The policy provides cover for two main areas:

Traditional commercial property and casualty policies do not provide adequate protection against the new and emerging risks associated with computer systems and data storage.

ACE DataGuard Advantage provides the necessary additional protection to allow businesses to trade safely in today's inter-connected, always-on marketplace.

The cover provided by DataGuard Advantage addresses two key areas of concern:

First Party – cover for risks to the policyholder's own business and systems.

Third Party – cover against the risk that the policyholder may become liable to pay money to a third party as a result of storing or using data, or trading electronically.

DataGuard Advantage Product sheet

First Party

Hardware Cover

This section delivers comprehensive cover for physical loss or damage to computer hardware, including breakdown. A standard commercial combined policy will simply not provide the breadth or depth of specialist protection required.

Data cover

This provides cover for the costs incurred in connection with the loss of, or inability to access, data, or the corruption of data, as a result of:

- Network security breach
- Unauthorised use of the computer system by, for example, a disgruntled employee, an attack by hacker or a denial of service attack
- Computer virus
- Accidental damage or destruction of data media
- Human error
- Malfunction of the computer system
- Failure of utilities or other supply systems such as air conditioning
- Malfunction of peripherals and data transmission lines.

Crucially, cover includes the costs of restoration of any such data.

Business income and extra expense

This is vital. It helps a company to survive the impact of the loss of business income suffered due to a failure of their computer systems.

Crisis management and notification costs

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 optional extension to the policy provides funds, in the event of an incident, to enable the insured 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.

Cyber extortion costs

The policy can also be extended to include cyber extortion costs. This will pay for mitigation costs as well as any extortion demand itself.

Third Party

Disparagement, plagiarism and infringement

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

Rights to privacy or breach of confidence

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 and includes the loss of both personal consumer information and business confidential information.

Transmission of virus and denial of service

Computer viruses can have a devastating effect. The transmission of a virus to a third-party can have the same effect on their systems, triggering a claim for damages.

Additionally, companies that rely on your computer systems 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.

DataGuard Advantage covers the policyholder against costs and claims arising out of the contraction and/or transmission of a virus.

The above covers are not all automatic, and may have limits of liability and terms and conditions. They may attract an additional premium. Please contact your local ACE representative for full details. This information is descriptive only. The precise coverage afforded is subject to the terms and conditions of the policy as issued.

DataGuard Advantage

Retail clothing chain

Case study incident: Stock control system failure

Consequence:

Point-of-sale equipment stopped working. Unable to accept orders via website.

Impact:

Collapse of auto-ordering via point-of-sale tills resulted in popular items running short, with immediate and substantial negative effect on sales and, ultimately, reputation.

Policy Response:

DataGuard Advantage responded in several ways:

- funded cost of forensic investigation into cause of failure
- funded network restoration costs
- compensated for lost revenue
- funded increase cost of working from manual updating of stock system following full stock-take.

Charity

Case study incident: Website failure

Impact:

The charity relies heavily on donations made via its website, with the level of donations fluctuating according to the season, such as Christmas, or in connection with a sponsored event or advertising campaign. The website failure coincided with such an activity, severely compromising fund-raising activity and thus hindering its viability in terms of fulfilling its charitable aspirations and responsibilities.

Consequence:

Inability to accept online donations.

Policy Response:

DataGuard Advantage covered forensic investigation work into the cause of the failure and met restoration costs in full. It also covered the policyholder for loss of income and increased cost of working.

DataGuard Advantage

Engineering

Case study incident: Breach of commercial confidentiality

Consequence:

Legal action by a supplier.

Impact:

As part of tender for business, a supplier sent its price list to the policyholder, an engineering firm. This list was subsequently forwarded, inadvertently, to a rival of the original supplier. Once in possession of the list, the competitor was able to undercut the supplier's prices in order to win business. The supplier therefore brought legal proceedings for loss of future earnings against the engineering firm.

Policy Response:

DataGuard Advantage covered the policyholder's legal expenses and the cost of the settlement.

DataGuard Advantage

Clothing distribution warehouse

Case study incident: Stock control system malfunction

Consequence:

Programming error resulted in the distribution to stores of a limited range of garment sizes.

Impact:

Disruption of the distribution routine had a disproportionate impact on popular sizes, resulting in a dramatic reduction in sales.

Policy Response:

DataGuard Advantage covered the loss of income from the loss of sales.

DataGuard Advantage

Hotel sector

Case study incident: Back-end system failure

Consequence:

Check-in/check-out, billing, room management and staff coordination information became out-of-date and thus of no use.

Impact:

Without information to process customers, hotel reception became chaotic, incorrect bills were issued, income was impaired and business was lost.

Policy Response:

The hotel lacked cyber cover. DataGuard Advantage would have provided for lost revenue and funded increased cost of working.

DataGuard
Advantage

Online retailer

Case study incident: Website hosting failure

Consequence:

When equipment failed at the data centre hosting the retailer's website, the online sales function was unable to accept or process orders.

Policy Response:

DataGuard Advantage covered the loss of income from the loss of sales.

Impact:

Website downtime resulted in lost sales and revenue.

Add to Cart
X

DataGuard
Advantage

Office

Case study incident: Disparaging comment via email

Impact:

A seemingly throw-away comment within an internal email eventually formed part of a longer email thread that was distributed widely outside the business. It was eventually seen by a competitor who considered it to be disparaging and potentially damaging to its interests, and therefore legal proceedings were instigated. These resulted in the award of a £450,000 settlement.

Consequence:

Legal action by competitor.

Policy Response:

DataGuard Advantage covered the policyholder's legal expenses and the cost of the settlement.

DataGuard
Advantage

Glossary

Common terms used in cyber crime and IT insurance

Information technology and the world of cyber crime is packed full of “jargon”. Most people will understand a little of it; some will understand a lot of it; a few will understand most of it. Only specialists and nerds* will understand all of it.

This glossary has been put together to help the layman have some understanding of the terms or jargon most frequently encountered.

Words with an asterisk (*) beside them are defined within the glossary.

DataGuard Advantage Glossary of terms used in cyber crime and IT insurance

This glossary will help broaden understanding of the terms or jargon most frequently encountered in the world of cyber crime.

A

Adware
An unwelcome or malicious mini program that can infect the user's computer, causing unwanted "pop-up" adverts to appear.

Anti-virus software
Software that is specifically designed to protect computers against viruses.

B

Back door
A deliberate gap left in the security of a computer system, created by (crooked or criminal) programmers to enable them to access systems without detection.

Botnet
A network of computers used by criminals for purposes such as Denial of Access attacks.

C

Cloud
Ability to access computing resources, software and data as a service over the internet. The services can be scaled up and down as necessary with the user only paying for the services used.

Cookie
A package of data left on a user's computer when they visit an internet site or webpage. Cookies are usually legitimate and are used by an internet site to personalise it.

Cybercrime
Crime related to computers, internet and other information technologies.

D

Decrypt
Unscramble coded information.

Denial of Service (DOS)
A malicious attack which aims to cripple, or render a network or website inoperative. May be carried out by a botnet.

Digital signature
Acts as a guarantee that a computer file has not been tampered with or corrupted.

E

Encrypt
Encode information.

Ethernet
A wired system allowing computers to communicate with each other.

Extranet
Computer network where access is granted in a controlled manner to selected individuals/companies outside the company. It is often used to give access to business partners such as vendors and suppliers or other B2B relationships.

F

Firewall
Security software that limits access between a computer or network of computers and the internet. This helps to protect the network or computer from internet sites, hackers or malware which could infect them with viruses or other malware.

H

Hacker
A criminal who tries to breach the security of computer systems and networks. Hackers can perform targeted attacks where they select a specific organisation to attack or instigate random attacks using malware, which randomly attacks any system it can.

HTTP
Standard language used by computers to communicate over the internet.

HTTPS
Secure version of HTTP.

I

Instant Messaging
An alternative to email where responses can be instant and allow written "conversations" to take place. Often used by hackers to spread viruses and "worms".

IP address
A unique number given to each piece of equipment connected to a computer network, such as a PC, server, printer or scanner.

IP spoofing
A method a hacker uses to attack a network by forging an IP address.

L

Logic bomb
A malicious program, usually transmitted by email, that lies dormant and attacks when the infected computer or system meets certain criteria, for example when a specific date occurs or when a particular sequence of keystrokes is used.

M

Malware
Any software designed to cause damage or allow illegal access to a computer or network.

N

Nerd
An individual who is studious, usually young, often male and very well informed in computer matters. A nerd would not need a glossary like this.

P

Packet
Packets are used to move data around computer networks and the internet.

Phishing
A technique used by criminals to trick people into revealing information which would allow the criminal to steal their identity to gain access, for example, to their bank account. Phishing may take the form of an email purporting to be from the victim's bank or building society.

Pop-up
An unwelcome and unsolicited advert which "pops-up" in its own browser window. These can overwhelm a computer rendering it useless for accessing the internet. Pop-up infestations are usually a result of the actions of adware.

S

Self replicating code (or program)
A tiny program which, when activated, replicates itself. Each new copy is then able to again replicate itself and quickly clog-up entire networks. Worms are an example of this type of program. Viruses are also usually self replicating code that can, in addition, be extremely destructive.

Social engineering
A term describing the tricks used by hackers and virus writers to gain information or to trick users into activating viruses. Social engineering is also used to gain access to office buildings in order to steal items, documents, data, etc.

Spoofing
The act of pretending to be someone else while online or in an email. Hackers will steal email addresses and masquerade as someone else to gain information from unsuspecting recipients

Spyware
Software secreted onto a user's computer without their consent which tracks and reports their online usage. It may also track keystrokes, potentially revealing sensitive passwords and account numbers.

Strong passwords
Passwords containing "strong" features which would be considered almost impossible to guess. Strong features include:

1. Unusual "words"
2. Use of both upper and lower case
3. Use of symbols such as "!" or "?" or "&"
4. Use of numbers
5. Length of at least 8 digits.

T

Trojan horse
A piece of malicious software which enters the victim's computer embedded within genuine software, often spread as a seemingly innocent email attachment. Trojan horses can be destructive and difficult to extricate.

U

Upload
The transfer of information from the user's computer to any other computer or network.

V

Virus
A potentially destructive piece of self replicating code, which can deliver both a copy of itself and a destructive activity, such as wiping areas of the hard drive on a computer.

W

WiFi
A wireless system whereby computers communicate with each other. WiFi systems are vulnerable both from direct attack and from users connecting to "spoofed" WiFi networks. WiFi network security relies on strong and encrypted passwords.

Worm
A self-replicating program, which copies itself across a network, causing congestion and failure. Unlike viruses, worms do not require a host program to replicate, and they usually inhabit a network.

Z

Zombie
A computer that has been taken over by a malicious outside agency for its own purposes, usually as part of a network called a botnet. Zombies are harnessed to send out huge amounts of spurious emails or data packets in Denial Of Service attacks.

This glossary is intended to be for general informational purposes only and is not legal or professional advice. No ACE company shall be held responsible in any way for and specifically disclaims any liability arising out of or in any way connected to the information contained in this glossary. Any references to insurance policy provisions are not intended to amend or alter any insurance policy or contract.

Stability

We are a leading provider of insurance and reinsurance in Europe. Headquartered in London with a network of offices across 20 European countries, ACE Europe is part of The ACE Group of Companies, one of the world's largest providers of property and casualty insurance, reinsurance and financial services. ACE European Group Ltd holds a financial strength credit rating of AA- (very strong) from Standard & Poor's and A+ (superior) from AM Best.

Innovation

We provide a market-leading offering for customers with our extensive breadth and depth of organisation, in terms of products, geographic reach, underwriting and claims expertise and engineering capabilities. We pride ourselves on the quality and experience of our staff, who are specialists in their individual fields. Using this experience, we focus on products and services in market segments where this specialised knowledge creates a natural alliance and supports the key business goals of our customers.

Experience and expertise

ACE has a highly respected and knowledgeable underwriting team. We work with brokers and clients to provide a high quality insurance and claims service that is tailored to the needs of companies working across the commercial spectrum.

We are renowned in the insurance market for our major risk/ multinational underwriting expertise. ACE is one of the very few insurers with the ability to underwrite and structure a global insurance programme, through the utilisation of its own offices worldwide and its global network of partner insurers.

www.acegroup.com/uk

ACE European Group Ltd.

London
ACE Building
100 Leadenhall Street
London EC3A 3BP

+44 (0)20 7173 7000 tel
+44 (0)20 7173 7800 fax

www.acegroup.com/uk

Republic of Ireland
5 George's Dock
IFSC
Dublin 1

+353 (0) 1 440 1700 tel
+353 (0) 1 440 1701 fax

www.acegroup.ie

ACE European Group Limited is authorised and regulated by the Financial Services Authority in the United Kingdom and is regulated by the Central Bank of Ireland for conduct of business rules.

Published February 2012

Registered in England No.1112892
Registered in Ireland No.904967