American Land Title Association

Protect your property rights

Navigating Cyber Insurance

Presenter: Michael N. Russo, Jr., Esquire

Russo@CouncilBaradel.com

Copies: www.CouncilBaradel.com

April 2019

1800 M Street, NW, Suite 300S, Washington, D.C. 20036-5828 | P. 202.296.3671 | F. 202.223.5843 | homeclosing101.org

“THIS INSURANCE ISN’T AS SIMPLE AS TITLE INSURANCE”

American Land Title Association

Protect your property rights

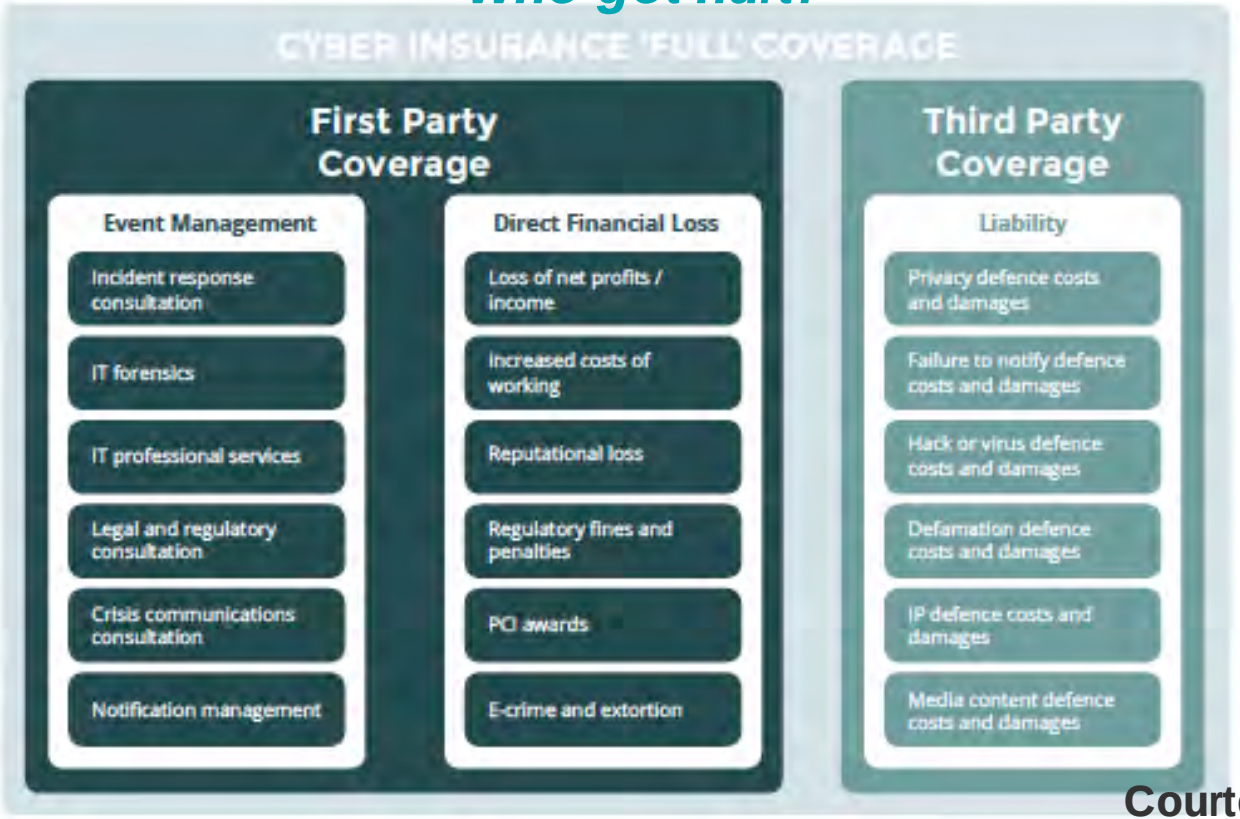
Insurance Conundrum

- “Occurrence” vs. “Claims Made”
- Non-Standard policies.
- **What** is a Claim?
- **How** to make a claim
- **What** to say.
- **Who** to direct claim to.
- **When** to make a claim

American Land Title Association
Protect your property rights

1st Party vs. 3rd Party

Who got hurt?



America
Title Ass
Protect your

Courtesy of Elmore Insurance Brokers

Making the Right Insurance Choice for Your Company.

- Evaluating risk
- Negotiating coverages and premiums
- Working through a broker
- Making your best case

Selecting the right broker

- Experience in the title industry
- Ability to negotiate coverage terms
- Determining coverage amounts
- Leveraging multiple policies
- American and European markets
- *Elmore Insurance Brokers - London*

UNDERSTAND
THE DIFFERENT TYPES OF INSURANCE POLICIES

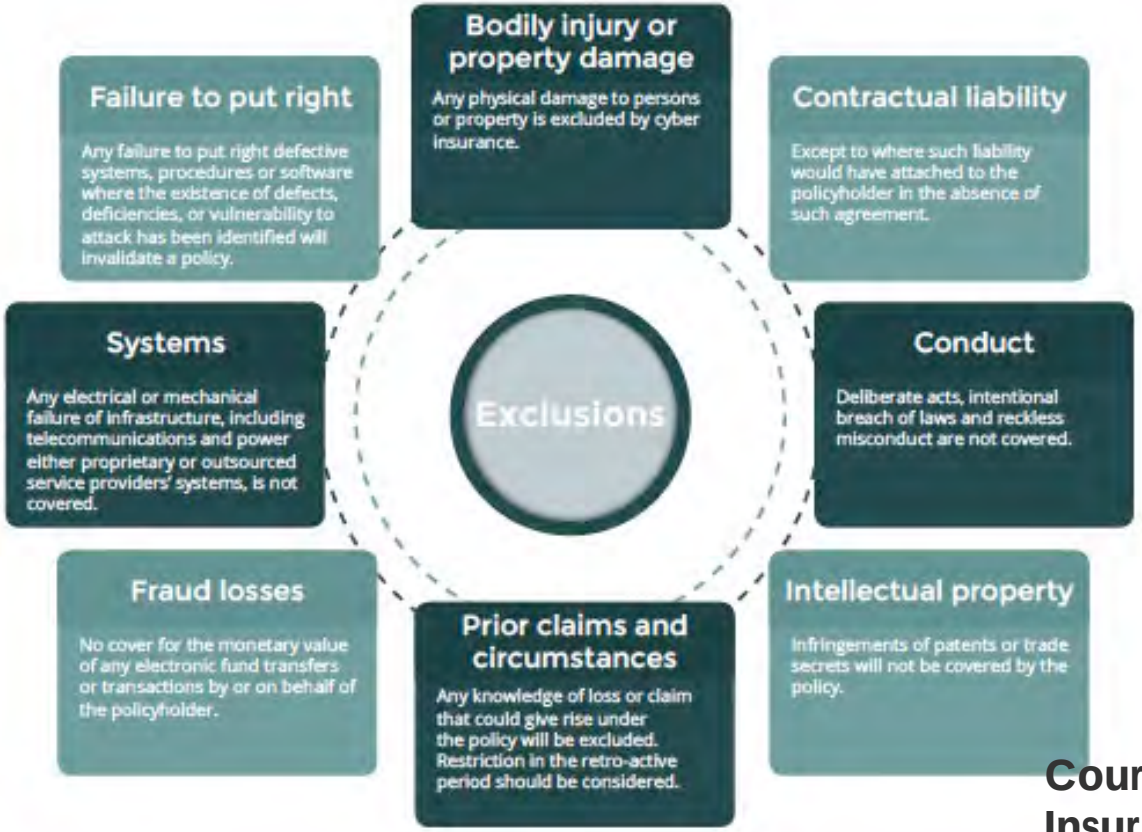
American Land
Title Association

Protect your property rights

Sources of Potential Coverage

- Errors and Omissions
- Fidelity
- Excess Policy
- Crime
- Cyber
- Social Engineering

Exclusions



American Land Title Associatio

Protect your property righ

Courtesy of Elmore Insurance Brokers

AREN'T THE "REGULAR GUYS" ENOUGH?

American Land Title Association

Protect your property rights

Errors & Omissions (E&O) Policy (3rd Party)

- Unintentional errors or omission of information
- Cyber Crime Endorsement
  - Limited Liability
  - Limited Coverage

Declarations Page

Item 7. Forms and Endorsements Effective at Inception:

Form Number	Form Title
MAN-RTP0013188-1801	Amend Defense & Settlement Endorsement II
RTP 101 (02/17)	Target Professional Liability Policy
RTP 624 (02/17)	Waiver Of Application
RTP 634 (02/17)	Amend Exclusion a. Claims Expense Reimbursement
RTP 648 (02/17)	Retroactive Date Per Insured
RTP 651 (02/17)	Disciplinary Proceeding Sublimit
RTP 652 (02/17)	Total Fungi Exclusion
RTP 653 (02/17)	Additional Insured - Vicarious Liability
RTP 663 (02/17)	Amend Subrogation
RTP 679 (02/17)	Defense Within Limits And Third Party Discrimination Exclusion
RTP 696 (02/17)	Social Engineering Exclusion
RTP 708 (02/17)	Real Estate Services

Social Engineering Exclusion

SOCIAL ENGINEERING EXCLUSION

It is agreed that:

1. Section **4. DEFINITIONS**, is amended by adding the following:

   "**Social Engineering**" means the **Insured's** reliance upon a deceptive misrepresentation, which the **Insured** believes to be genuine.

2. Section **5. EXCLUSIONS**, is amended by adding the following:

   - any actual or alleged loss of goods, money or securities resulting from **Social Engineering**.

Fidelity Bond (1st Party)

INSURING AGREEMENT

The Underwriter, in consideration of the payment of the premium, and subject to the Declarations made a part hereof, the General Agreements, Conditions and Limitations, and other terms of this Bond, agrees to indemnify the Insured against any loss of money or other property which the Insured shall sustain through any fraudulent or dishonest act or acts committed by any of the Employees, acting alone or in collusion with others, to an amount not exceeding in the aggregate the amount stated in Item 3 of the Declarations.

American Land Title Association

Protect your property rights

Excess or Umbrella Policy

- High liability amounts available
- Coverage terms
- Increases liability amounts
- Cost of single policy vs multiple using excess policies

American Land Title Association

Protect your property rights

THE “NEW GUYS”

American Land Title Association

Protect your property rights

Social Engineering Policy (1st & 3rd Party)

- Maximum Coverage $5,000,000
- Types of Policies
- Call-Back Policy
- No Call-Back Policy

American Land Title Association

Protect your property rights

Crime Policy (1st & 3rd Party)

- Covers Employee Dishonesty/Theft
- Covers Cyber Attack for Employees
- Data Breach Coverage
- Computer Systems Fraud Coverage
  - Callback Verification

Declarations Page

INSURING AGREEMENT	SINGLE LOSS LIMIT OF LIABILITY	SINGLE LOSS DEDUCTIBLE AMOUNT
A. Dishonesty	$5,000,000	$25,000
Trading Loss	Included	$25,000
Electronic Data Processing	Included	$25,000
B. On Premises	$5,000,000	$25,000
C. In Transit	$5,000,000	$25,000
D. Forgery or Alteration	$5,000,000	$25,000
E. Securities	$5,000,000	$25,000
F. Counterfeit Currency	$5,000,000	$25,000
G. Safe Deposit Box		
1. Liability of Depository	Not Covered	Not Covered
2. Loss of Customers' Property ☐ Money Included or ☐ Money Excluded	Not Covered	Not Covered
3. Combined total limit for Insurance Agreement ☐ Money Included or ☐ Money Excluded	Not Covered	Not Covered
H. Computer Systems Fraud	$5,000,000	$25,000
I. Data Processing Service Operations	Not Covered	Not Covered
J. Voice Initiated Transfer Fraud	$5,000,000	$25,000
K. Telefacsimile Transfer Fraud	$5,000,000	$25,000
L. Destruction of Data or Programs by Hacker	$5,000,000	$25,000
M. Destruction of Data or Programs by Virus	$5,000,000	$25,000
N. Telephone Toll Call Fraud	$5,000,000	$25,000
O. Unauthorized Home Banking Electronic Funds Transfer	$5,000,000	$25,000

Computer Systems Fraud Endorsement

1. **INSURING AGREEMENTS, SECTION (H) COMPUTER SYSTEMS FRAUD** is amended to add the following:

   FRAUDULENT ELECTRONIC COMMUNICATIONS

   The Insurer will pay for loss by the Insured resulting directly from the Insured, in good faith, having authorized or transferred, paid or delivered any funds, established any credit, debited any account or given any value in reliance upon a Fraudulent Electronic Communications Instruction through Email, Telefacsimile or Telephonic means received by the Insured provided that the Insured performed a Callback Verification with respect to such Fraudulent Electronic Communications Instruction.

Call-Back Verification

- Common Coverage
  - Coverage will not apply unless you have called an independently verified telephone number and confirmed that the wire instructions were valid.
- Negotiated Coverage
  - Callback verification is only required for the following situations
    - (a) use of new/different Customer escrow accounts;
    - (b) a Customer that has not previously worked with the Insured and is not on the Insured's ledger as a legitimate party to the escrow fund transaction; or
    - (c) a Customer that has requested a change to the escrow fund transaction from previously agreed upon instructions between the individual(s) or entity(ies) and the Insured.

Negotiated Language

- Commonly used language:
  - Loss by the insured resulting from the insured authorizing, delivering or transferring funds upon reliance on a fraudulent instruction provided that instruction purportedly came from an employee, a client or a vendor.
- Negotiated language:
  - Loss by the insured resulting from the insured authorizing, delivering or transferring funds upon reliance on a fraudulent instruction provided that instruction purportedly came from a legitimate party to the escrow transaction.

Cyber Policy (1st & 3rd Party)

- Protection from cyber and technology risks, such as:
  - loss of money due to fraudulent money transfers or phishing scams
  - extortion/ransom attacks
  - privacy breaches
  - computer viruses or hacking resulting in damage / disruption to computer systems

American Land Title Association
Protect your property rights

Fran Kelly Professional Liability, LLC
www.titleliability.com

What does it cover?

- Claims made by clients or employees
- Regulatory proceedings, fines and penalties relating to privacy laws
- Costs to notify affected individuals / provide credit monitoring to affected individuals
- Costs to restore data and computer programs damaged by hackers / viruses
- Business interruption and extra expense due to a breach
- Reimbursement of lost funds

INSURING CLAUSE 1: CYBER INCIDENT RESPONSE

SECTION A: INCIDENT RESPONSE COSTS

Limit of liability:	USD5,000,000	each and every claim
Deductible:	USD0	each and every claim

SECTION B: LEGAL AND REGULATORY COSTS

Limit of liability:	USD5,000,000	each and every claim
Deductible:	USD5,000	each and every claim

SECTION C: IT SECURITY AND FORENSIC COSTS

Limit of liability:	USD5,000,000	each and every claim
Deductible:	USD5,000	each and every claim

SECTION D: CRISIS COMMUNICATION COSTS

Limit of liability:	USD5,000,000	each and every claim
Deductible:	USD5,000	each and every claim

SECTION E: PRIVACY BREACH MANAGEMENT COSTS

Limit of liability:	USD5,000,000	each and every claim
Deductible:	USD5,000	each and every claim

SECTION F: THIRD PARTY PRIVACY BREACH MANAGEMENT COSTS

Limit of liability:	USD5,000,000	each and every claim
Deductible:	USD5,000	each and every claim

SECTION G: POST BREACH REMEDIATION COSTS

Limit of liability:	USD50,000	subject to a maximum of 10% of all sums we have paid as a direct result of the cyber event, each and every claim
Deductible:	USD5,000	each and every claim

INSURING CLAUSE 2: CYBER CRIME

SECTION A: FUNDS TRANSFER FRAUD

Limit of liability:	USD250,000	each and every claim
Deductible:	USD5,000	each and every claim

SECTION B: THEFT OF FUNDS HELD IN ESCROW

Limit of liability:	USD250,000	each and every claim
Deductible:	USD5,000	each and every claim

SECTION C: THEFT OF PERSONAL FUNDS

Limit of liability:	USD250,000	each and every claim
Deductible:	USD5,000	each and every claim

SECTION D: EXTORTION

Limit of liability:	USD5,000,000	each and every claim
Deductible:	USD5,000	each and every claim

SECTION E: CORPORATE IDENTITY THEFT

Limit of liability:	USD250,000	each and every claim
Deductible:	USD5,000	each and every claim

SECTION F: TELEPHONE HACKING

Limit of liability:	USD250,000	each and every claim
Deductible:	USD5,000	each and every claim

SECTION G: PHISHING

Limit of liability:	USD250,000	each and every claim
Deductible:	USD5,000	each and every claim

The Big Questions

There are a number of questions that can arise at this point, namely:

1. What types of insurance coverage is available?
2. Am I already covered?
3. What is typically excluded?
4. Which type of coverage is appropriate for the business?
5. Aligning risks with policy coverage
6. Should a stand-alone cyber insurance policy or a blended policy be purchased?
7. What type of post breach additional services are available to help manage a cyber-attack?

Courtesy of Elmore Insurance Brokers

(PLEASE DON'T JUST LEAVE ME STANDING UP HERE!)

American Land Title Association

Protect your property rights

Elmore
Insurance Brokers

What to Look for in a Cyber Insurance Policy

Elmore
Insurance Brokers

About the Author

Simon Gilbert, Founder and Managing Director of Elmore

Simon Gilbert has 15 years of experience working in the heart of the insurance industry throughout the world's leading business centres. Simon's appearance on **CCTV America** advising on cyber insurance and his expertise in this rapidly growing area of risk, coupled with more than a decade at the fore of the insurance industry make him a formidable force and partner in securing clients bespoke insurance for their needs.

Elmore
Insurance Brokers

About Elmore Insurance Brokers (Elmore)

Elmore is a City of London based brokerage firm with partnerships in place to offer world leading insurance and re-insurance for customers. Providing best value to clients is our cornerstone value, upheld by our promise to be forward-thinking specialists, providing a global perspective through our international network and advising on the risks of today for the challenges of tomorrow. We offer advisory, broking and claims management services under one roof, with particular expertise in the rapidly growing field of cyber insurance.

Elmore
Insurance Brokers

Introduction

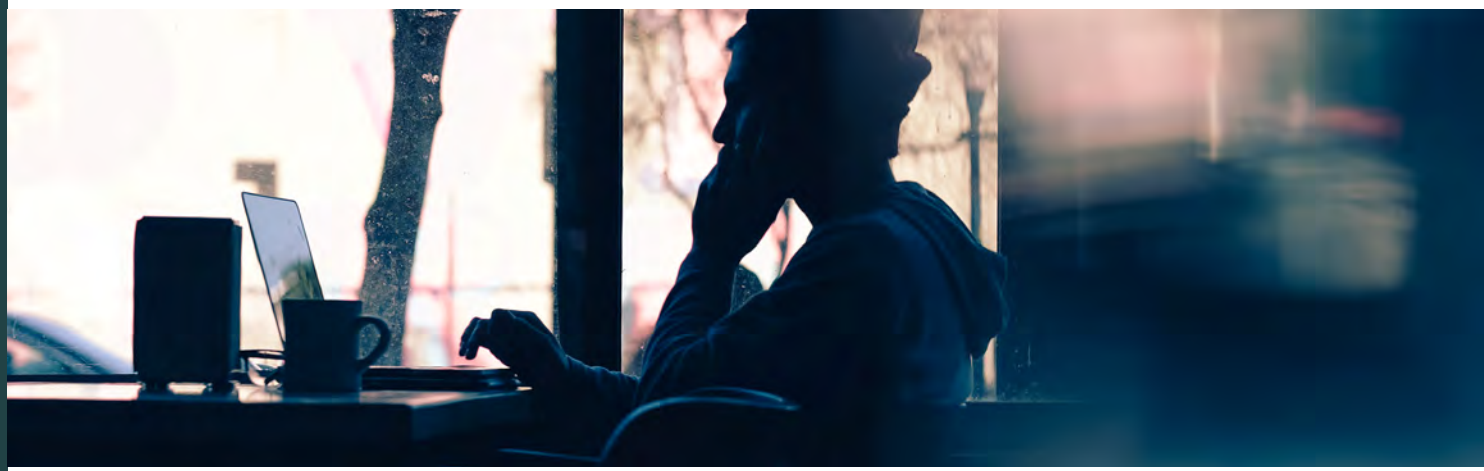
"Cyber security is now the third biggest risk faced by global business leaders." Lloyds Risk Index 2013, this was reiterated by Allianz Insurance stating "**Cyber Incidents were the third largest business risk for 2016**". Welcome to the third in our three part series of eGuides that addresses cyber risk and how to insure against it.

As the quotes above indicate, the risk of cyber-attack continues and with a changing regulatory landscape requiring companies to declare such attacks, the stakes are higher now than ever.

As companies embrace digital channels throughout every department and activity, this change brings with it inherent risks, and while systems and processes are built and put in place to mitigate these, there always remains the possibility of a loss event occurring.

In an increasingly connected world, this eGuide will address the role cyber insurance can take in managing the complex risks of a modern business. It will look at how organisations of all sizes can address the specific risk that is faced across all sectors, what risks cyber insurance can manage against and the role that a cyber insurance broker should be taking when it comes to helping to design a robust cyber insurance policy.

As major breaches continue to be publicised, the associated risks – and costs in responding to a breach – grow exponentially. This eGuide will also show the role that cyber insurance should take in managing those risks and reducing exposure to potentially crippling costs.



Elmore
Insurance Brokers

What A Cyber Insurance Policy Should Cover

The risks of cyber-attack are severe and growing all the time. With EU GDPR expected to add **even greater costs for an organisation to respond to a cyber attack**, it's important for organisations to transfer as much of that risk as possible away from themselves and onto the balance sheet of insurers.

But as with any insurance policy, it can be difficult to know what a business actually needs cover for and what a good policy looks like.

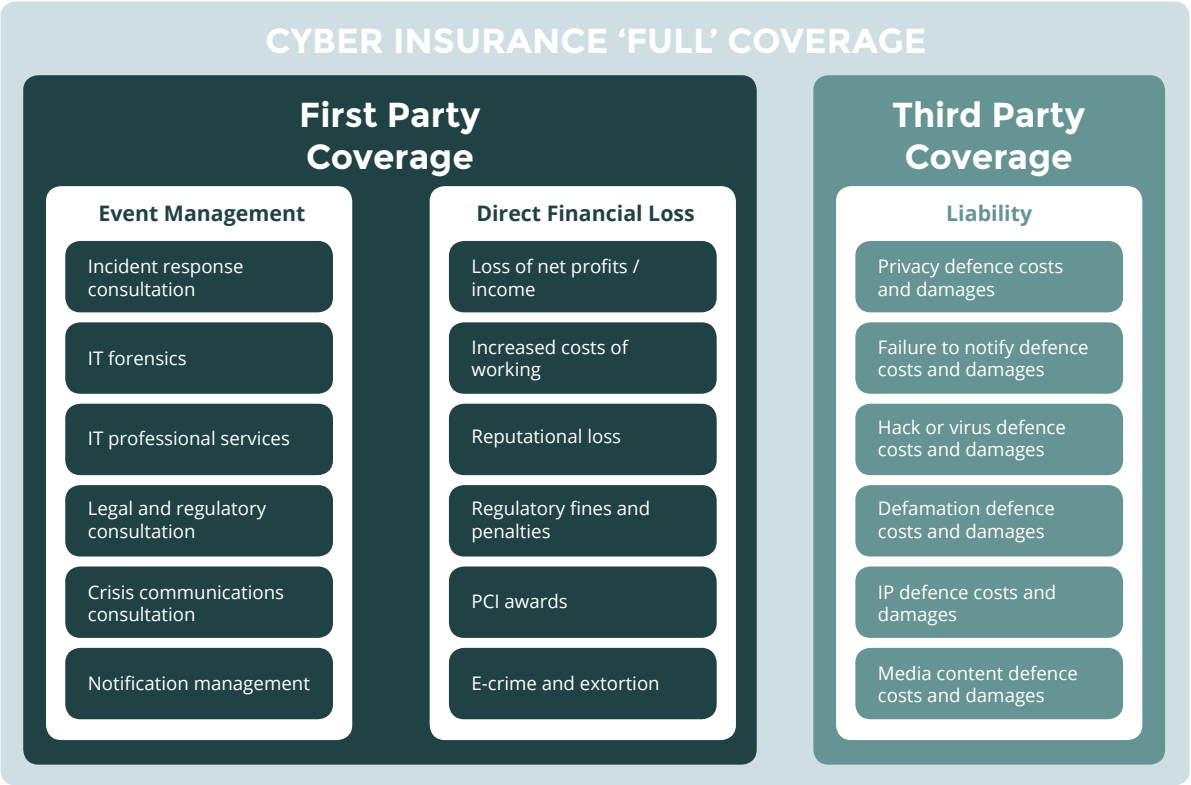
There are a number of questions that can arise at this point, namely:

1. What types of insurance coverage is available?
2. Am I already covered?
3. What is typically excluded?
4. Which type of coverage is appropriate for the business?
5. Aligning risks with policy coverage
6. Should a stand-alone cyber insurance policy or a blended policy be purchased?
7. What type of post breach additional services are available to help manage a cyber-attack?

Elmore
Insurance Brokers

1. What types of insurance coverage are available?

With no standardised terminology between insurers and brokers for cyber insurance, navigating policy coverage and its intent can be challenging. Having a cyber insurance broker on hand to guide across the different areas of coverage is important:



a) Event Management Costs

Following a data breach, businesses incur a range of costs or 'first party costs' in dealing with the aftermath including forensic investigation, public relations, customer notification, and credit monitoring. These costs are typically incurred by companies following a breach irrespective of whether a liability claim arises or not.

One of the key components of this coverage is notification. Companies that suffer a data breach may be required to notify a number of different stakeholders including their customers and/or employees whose personal information has been compromised, which can lead to significant expenses if large volumes are involved.

Regardless of the legal requirement it is good business practice to notify in the event of a breach to limit reputational damage.

Cover is provided for reasonable charges, costs, expenses and fees incurred by the policyholder with the insurers written consent within 24 months of the Insured first having knowledge of an actual or alleged unauthorised disclosure or loss of any Sensitive Personal Data (as defined in EU GDPR).

b) Digital Asset Replacement Expense Coverage

Costs to restore digital assets after a cyber event. The cover reimburses policyholders for the costs to restore the data or replicate it to the same level that it was prior to the breach. Although this used to be one of the key coverages its significance has been reduced over the years due to the enhanced sophistication of back up facilities

c) Non Physical Damage Business Interruption (NPDBI)

Loss in net profit/income that a firm is prevented from earning due to an outage to the Insured network or to the service providers computer system. Cover is also provided for interruption expenses including the increased costs in working during the downtime.

The trigger for the outage is usually a security failure (such as a cyber-attack) however it is possible to extend coverage to a system failure (such as a degradation of the network from any cause). The main buyers of NPDBI are normally those organisations that are network critical and their business depends on high levels of uptime.

Time retentions can vary from 6hr to 48hr depending on the risk and of course how much the policyholder wants to pay. The market norm is a 10 hour time retention which is the amount of time before policy coverage will trigger.

d) Customer Churn/Reputational Risk

This is an extension to the NPDBI coverage. It is standard for business interruption coverage to only cover the loss of net profit/income during the period of restoration. Once systems are restored back to the position prior to an event occurring then coverage will cease. However, following a large scale cyber event, there can be a fallout of customers known as 'customer churn' ultimately leading to a loss in net profits/ income for the months or even years after a major incident.

Those sectors where data integrity/service availability is a pillar of their organisation's offering will most likely be worse affected such an event and therefore this coverage will resonate most.

The use of monetary deductibles and policy limits can be more effective than time retentions and indemnity periods due to the time lag in customer churn scenarios. Following a cyber event it may take up to 72 hours for various stakeholders to become aware of the incident. Only after which point could the policyholder incur a drop in footfall. A 12 hour time retention which starts from the time of discovery of a cyber event would be eroded before costs actually incurred. It is therefore sensible to utilise a monetary deductible and indemnity period to avoid this situation.

e) Regulatory Proceeding Defence Costs

Coverage for the cost of reimbursement of all defence costs that a policyholder incurs following a formal investigation by a regulatory body concerning an actual or alleged unauthorised disclosure or loss of sensitive personal data which is either in the care, custody or control of the policyholder or a policyholder's service provider. For example following a data breach here in the UK the Information Commissioners office (ICO) will carry out an investigation to see if a business have breached the Data Protection Act 1998 (DPA). The costs of defending against the investigation will be covered under this section.

f) Payment Card Industry Data Security Standard (PCI DSS) Awards

The PCI DSS cover is for the awards which the policyholder has a contractual liability to pay to the card networks such as Visa and MasterCard following an actual or alleged unauthorised disclose or loss of card holder information. Where large limits are provided this module is often but not always sub-limited.

g) Cyber Extortion and Reward Payments Coverage

Costs to reimburse the insured for extortion payments and extortion expenses arising directly from a cyber extortion threat. Cyber extortion is a very real threat and is typical to take down a policyholder's network or to release sensitive personal data. Cover can also be provided for reward costs leading to the arrest of the hacker.

h) Cyber Crime

Cover for computer crime (actual theft of monies), id theft, telephone hacking, and phishing scams. It is possible to seek limited cover here for social engineering/ fake CEO Fraud, when the policyholder inadvertently acts upon fraudulent e-communications which purport to come from an authorized signatory but in fact have been sent by a fraudulent outside party. Insurers often sub-limit this coverage and more frequently are requiring a 'tested' process to be embedded in the policyholder controls in order to provide the coverage.

i) Cyber Terrorism

Cover provided under the heads of cover listed above where the act was committed by a cyber terrorist.

j) Security and Privacy Liability Coverage

Defence and settlement costs cover for legal actions brought by plaintiffs as a result of a breach of their sensitive personal data. This can sometimes be brought as a group action which looks to develop as an issue in the UK, in the years to come. Lawsuits can also come from banks themselves if they have incurred costs as a result of the breach. Insurers are yet to see any real case law for liability outside of the US for this section of coverage, however this is set to change as a result of the new EU data protection legislation as well as recent rulings in the UK such as the 2015 Google v Vidal-Hall decision concerning misuse of private information. Coverage is also provided here for the failure in not notifying customers as well as lability for the transfer of virus.

k) Internet Media Liability

Damages and defence costs the policyholder faces for infringing a third party's intellectual property rights in the publication of content in electronic or print media. Coverage is also provided for the actual or alleged libel, slander, disparagement of individual persons or organisations.

2. Am I already covered?

There is some confusion among buyers of insurance as to the difference between a General Liability, Professional Liability, Managerial Liability, Crime Insurance and Cyber Insurance policy. The differences between them are subtle and best considered in a gap analysis of coverage:

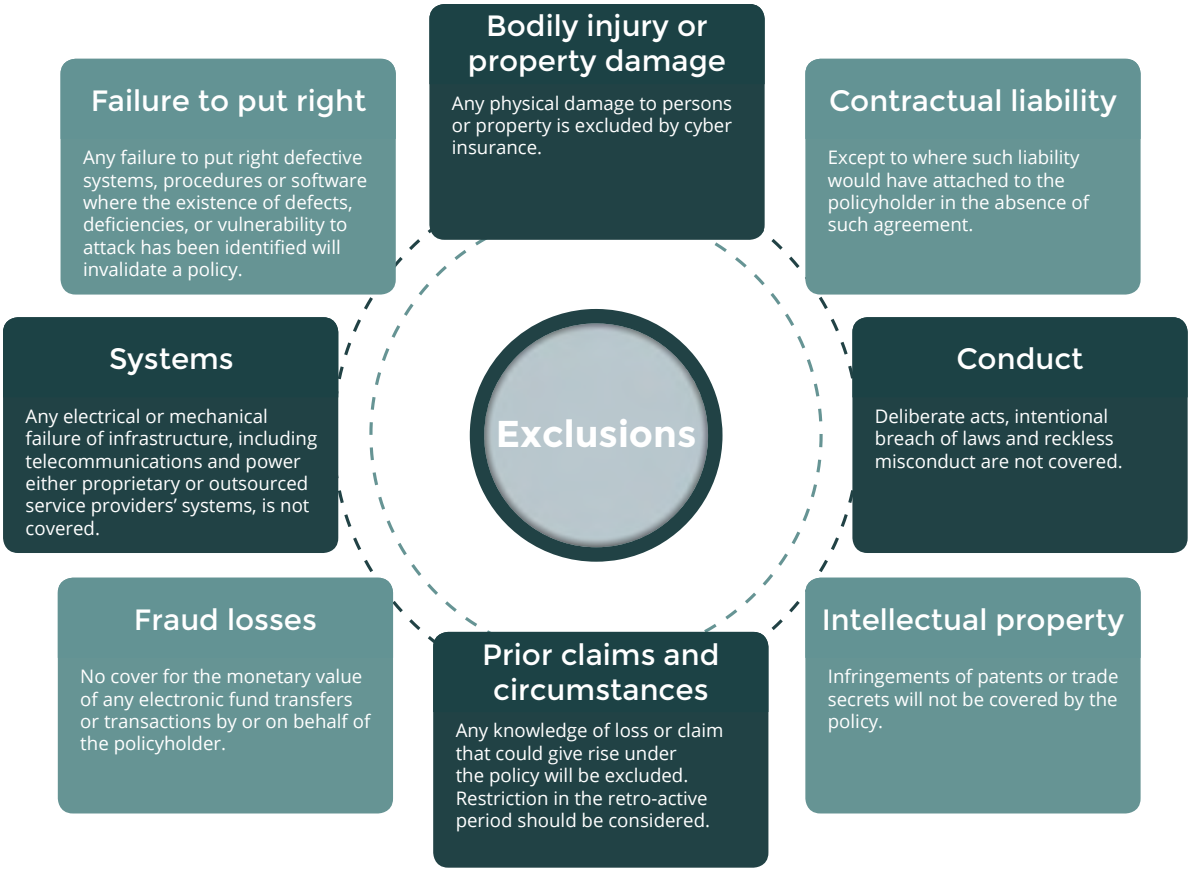
Elmore
Insurance Brokers

Scenario	General Liability	Professional Liability	Managerial Liability	Crime Insurance	Cyber Insurance
Loss to property causing physical damage from natural perils					
Business interruption caused by physical damage					
Injury to employees during working hours	✓				
Injury to 3rd party on premises	✓				
Wrongful professional act causing claim by 3rd party		✓			✓
Mitigation costs to reduce impact of wrongful professional act		✓			✓
Wrongful managerial act causing claim against directors/officers			✓		
Mitigation costs to reduce impact of wrongful managerial act			✓		
Direct financial loss caused by dishonest acts of employees				✓	
Direct financial loss from 3rd party crime including computer crime				✓	
Loss from cyber extortion and fraudulent e-communications				✓	✓
Costs for an IT forensic firm to undertake investigation of loss				✓	✓
Legal and regulatory costs to defend against 3rd party claim		✓	✓	✓	✓
Crisis communication costs and expenses			✓		✓
Non-physical damage business interruption from cyber attack					✓
Fines and Penalties by regulators (where insurable by law)			✓		✓
Liability to customers from breach of privacy/confidentiality		✓	✓		✓
Liability to 3rd parties from transfer of virus		✓	✓		✓
Liability to 3rd parties from digital media and web-site content		✓	✓		✓

Elmore
Insurance Brokers

3. What is typically excluded?

Like any insurance policy, there will be areas the policy won't cover. It's important to note these not only when making a claim, but when designing a company's policies and procedures to ensure the validity of any claim when it is made. These exclusions include:



Elmore
Insurance Brokers

4. What type of coverage is appropriate for the business?

A first step in insuring against potential threats is to assess the exposure across all parts of the business, using industry accreditations (such as Cyber Essentials or ISO 27001) as baselines can assist this process. If a business does not have the skills in-house, there are many specialist information security consultants able to help provide a comprehensive evaluation of a business, which will highlight areas of risk, make recommendations, prioritise actions and help build a strategic roadmap for continuous risk management.

A full risk management review can show critical gaps in operational control that need immediate attention. And a list of summary recommendations would give a timeline for carrying out any remedial actions required. By engaging with insurers at this point, it shows a firm is serious about actively mitigating and managing its risks. Something Insurers, look to reward in enhanced coverage or improved premiums.

It is important to understand that it is not one size fits all – not every firm has the same cyber exposures. It is therefore essential that a business works with an experienced cyber insurance broker so that policy coverage is tailored specifically for its needs.

In such a technical and ever changing area, it's important that a broker brings expert advice to ensure that a level of cover sufficient for an individual organisation is arranged and is most likely to pay out in the event of a potentially costly attack.

A good cyber insurance broker should be able to work with an organisation to map these risks out so that it can be decided whether they should be managed with insurance or managed with internal policies and procedures.

This should be done in two ways:

Risks to the Company

What systems are being used?

What security is in place?

What level of training is being received by staff?

What processes and policies are in place to safeguard systems?

How much personal /card data is being held?

Is the business network critical?

How resilient is the network?

What are the backup facilities?

How tried and tested is the BCP/ DRP/IRP?

Risks to the Sector

What is the value of data on the black market?

Is it a politically sensitive sector?

Is the sector heavily attacked?

What is the average cost of an attack?

Is it an environmentally sensitive sector?

The type of cover peers are purchasing?

What level of cover are peers buying?

Are regulations changing for sector?

Do cyber insurers see sector as high risk?

Is coverage specific to sector risks?

Once the risks within the sector and the company have been mapped, it will be easier to know which specific areas should be covered by a policy. This is often presented as a gap analysis of activity and risks mapped to likelihood of a claim under specific parts of coverage. The broker will need industry focused expertise combined with sound technical knowledge of the insurance product, ideally having real claims handling experience.

Elmore
Insurance Brokers

5. Aligning Risks with Policy Coverage

Once the sector/business specific risks have been mapped out, these should be aligned with any existing coverage that is in place. The broker should be able to review the documentation of existing policies and identify where specific risks are already covered by insurance and where there are gaps in policies in regard to cyber.

The broker will then be able to create either a stand-alone cyber insurance policy that is relevant to any exposed risks, or a blended policy that has cyber sitting right at the center of the cover.

Understanding how different insurance policies work together to provide a complete cover is an essential requirement of a Cyber Insurance Broker and one that will help to get good coverage and good value.

Elmore
Insurance Brokers

6. Should a stand-alone cyber insurance policy or a blended policy be purchased?

There are generally two ways of approaching cyber insurance, either as a stand-alone policy or as part of a wider blended policy such as Professional Indemnity or Crime Insurance with cyber extensions.

The key to understanding which approach is right for a business is analysing the risk profile first. If a business is high risk in terms of cyber (is network critical or holds large volumes of data) then a stand-alone policy would be most appropriate to ensure the widest cover possible. If however the cyber risk is incidental then a business may look to have an extension to a Professional Indemnity policy or a blended policy.

The other consideration is around limit of indemnity. If a firm buys a blended policy it needs to ensure enough limit available e.g. do they want their Professional Indemnity limit eroding the cyber limit and vice versa?

As a rule, stand-alone policies or blended policies that are designed by a specialist Cyber Insurance Broker will give a more relevant level of cover with terms and conditions that are in line and suitable for an organisation's needs.

Elmore
Insurance Brokers

7. What type of post breach additional services are required to manage a cyber event?

When purchasing a cyber insurance policy careful consideration should be given to what specialist breach response services are provided. Having the right team of experts in place to manage the breach is absolutely key in keeping costs down and managing reputation.

A comprehensive solution will incorporate an integrated breach response service that can be accessed via an online portal or via a 24/7 hotline. This will be a one stop shop for all breach needs including IT Forensic, IT Professional Services, Legal, Regulatory, PR and Credit monitoring services. After calling the hotline policyholders should have their own designated breach coach guiding them through every step of the way and bringing on the necessary expertise as and when needed. Benefits of using post breach additional services include:

- The breach is contained and handled in a cost efficient manner.
- Compromised data is identified and notification of data subjects are made.
- Credit and web monitoring is made available.
- Regulators are informed and kept up to date.
- PR issues are dealt with both internally and externally with the media.
- Costs are monitored and tracked throughout the process.

Elmore
Insurance Brokers

Summary and Takeaways

The level of cyber risk that companies face is significant, and growing all the time. With new legislation set to be enacted in the form of the **GDPR in 2018 and the revised DPA 98 perhaps sooner**, organisations will be forced to pay even bigger costs in the form of fines and reputational damage if they are hit by a cyber-attack. As a result companies are increasingly turning to cyber insurance to help manage and transfer this risk.

When buying cyber insurance, it's important that organisations understand the specific risk faced by them as a company but also the wider sector. By using a cyber insurance broker that can map those risks and manage the wider policies to ensure these risks are sufficiently managed through insurance.

Takeaways

- The risks of cyber attack are growing – as are the costs. Understanding the GDPR legislation and the changing DPA is critical for all companies
- Cyber insurance should be bought from a broker that has expertise in cyber. The broker will need to review existing policies and find any gaps where coverage doesn't currently exist
- A blend of insurance policies such as Professional Indemnity Insurance together with Cyber Insurance can be used to achieve a suitable level of coverage
- Ensure that the cyber insurer provides comprehensive post breach services

Elmore
Insurance Brokers

Do your existing insurance policies cover you in the event of a cyber-attack? Take our Silent Review today and our consultants will analyse your policies and identify any areas where you are critically exposed.

CLAIM YOUR FREE SILENT REVIEW TODAY