



**CPP Group UK**

**Cyber**  
**“Prevention is better  
than cure”**



**Presenters: Michael Whitfield & Perry McShane**



**Chartered  
Insurance  
Institute**

## Welcome to CPP Group UK

> 9 Million customers

> 30 Years protecting customers

> 11 Countries worldwide

> 250 Business partners

> 1/24 One of only 24 FCA sandbox applications from cohort 1

> Tech Fostering a culture of innovation








## Learning objectives:

- 1. Consider the regulatory position regarding cyber risk and understand what the PRA advice means in practical terms
- 2. Gain an appreciation of the real life cyber risks that make SME easy targets
- 3. Gain an understanding of the types of products available in the market that can be used to safeguard against cyber risk as a preventative measure
- 4. Understand how brokers can show their value as a trusted expert advisor of choice for their SME clients
- 5. Understand the role of cyber insurance policies in the risk management and risk mitigation cycle.





## Who is this relevant for?

-  Commercial lines brokers and insurers
-  Financial services providers
-  Information security officers
-  Regulatory compliance teams and personnel
-  Providers / users of insurance affinity schemes



# In the press...it's everywhere



LIVE WEBINAR: RISK ASSESSMENT

## Inherent, Residual and Targeted Risk: What Risk Professionals Need to Know

19 JUNE 2019 10.00AM - 10.45AM BST

REGISTER NOW



### BEWARE OF 'SILENT' CYBER RISK

The UK's insurance regulator has warned insurance companies that they need to do more to reduce and manage their exposure to 'silent' – or non-affirmative cyber risk.

Non-affirmative cyber risk occurs when insurance policies are 'silent' on the matter, in that they don't explicitly either include or exclude it.

The shot across the bows from the Prudential Regulation Authority (PRA) follows its survey of insurance firms of various sizes, which found that although some work has been done to address the issue, more effort is needed in relation to businesses' non-affirmative cyber risk management, risk appetite and strategy.

Firms taking part in the survey generally agreed that a number of traditional lines of business have

### ABOUT ENTERPRISE RISK MAGAZINE



Enterprise Risk Magazine is the leading quarterly title for risk managers and enterprise risk, with a print circulation of over 5,500.

Enterprise Risk is published on behalf of the Institute of Risk Management (IRM). The majority of IRM members receive their copy of Enterprise Risk at



## Brokers reveal biggest challenges to selling cyber cover

By Clare Ruel | 20 June 2019

With the risk of cyber crime ever increasing and evolving, the threat to UK businesses remains high but cyber insurance uptake is still comparatively low compared to the US, *Insurance Times* looks at the challenges brokers face selling the product and how to overcome the problem

While 78% of brokers view cyber insurance as an area of growth for their business, two fifths (37%) admit to having never sold a cyber policy.

The biggest barrier highlighted by brokers was that 90% of their clients believe that they do not need cyber cover at all. [these findings were according to Ecclesiastical's recent research.](#)

## Hiscox creates Cyber Exposure Calculator

INSURER



Aara Syed  
@BrokerAara

17 Jun 2019



0 Comments



Hiscox has unveiled a Cyber Exposure Calculator, which it said will aid businesses estimate the possible financial impact they may suffer if they experienced a cyber attack.

The calculator is free to use and a firm can see its potential cyber exposure and the value of its data by selecting the country and sector in which it operates as well as its revenue.





### Insights

Hiscox has detailed that it worked with consultancies to develop the calculator and explained that it offers some insights into

# 1. The regulatory position – Challenge and Opportunity

**“Understand the regulatory position regarding cyber risk and understand what the PRA advice means in practical terms”**

The key points:

-  A number of traditional lines of business have exposure to non-affirmative cyber risk, with casualty, financial and motor lines among those noted to have the largest exposure. **The PRA is concerned about the potential prudential risk and urges firms to do more to assess their exposures**
-  As with any other insurance product, **cyber insurance policies** must **meet the demands** and needs of customers on an ongoing basis. There is an especial challenge in this area because the requirements change and develop on an almost daily basis
-  As cover widens, affirmative exposure increases. **Is premium income keeping up with that exposure** and is risk appetite and awareness clearly enough defined?
-  PRA concern is centered around prudential risk. Brokers and advisors have a **critically important** role to play in promoting risk mitigation strategies to their SME customers in order to control and limit ultimate insurance losses. **Therein lies an opportunity.**

According to the PRA's recent survey:

***"firms' stress test results suggest that a cyber event could have widespread impact on a number of different lines of business. Some firms assessed the potential risk of loss from cyber events as being comparable with major natural catastrophes in the US."***

## Quick Fact

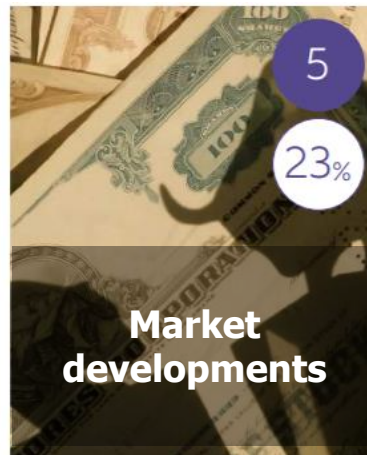
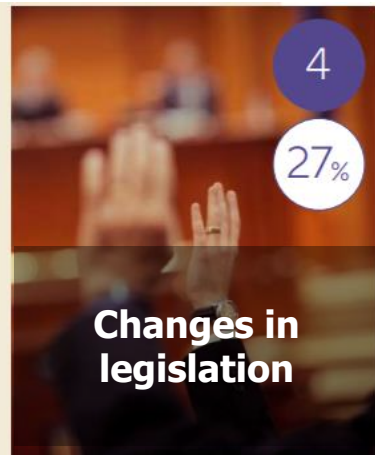
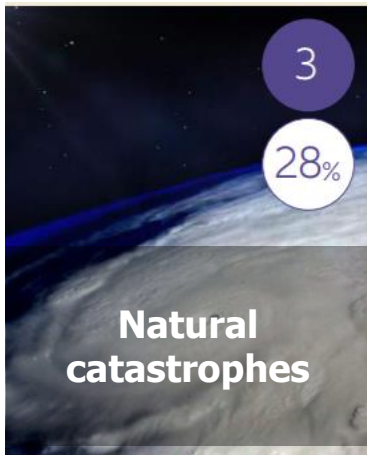
Non affirmative or silent cyber – is the latent, potentially unknown exposure in an insurer's portfolio created by a cyber risk which has not been explicitly excluded.

## 2. Firstly....what are the cyber risks

“Gain an appreciation of the real life cyber risks that make SME easy targets”



*“Business Interruption and cyber incidents are tied at the top ranking at 37% in the UK's biggest risks.”*



\* Source:

<https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2019.pdf>



## 2. Cyber hackers are not who you think they are...

### **Hacking is easy**

Communities, discussion groups and online walkthroughs are easy to find

**Hotel staff.** Do you leave your laptop in your hotel room? How do you know its not been compromised? This has happened!

### **Malware as a Service -**

Available on the Dark Web for a reasonable fee



### **The "dark" web is easily accessible.**

Cyber attacks can be mass produced and are easily accessible

### **Disgruntled employees are a risk!**

A threat actor can offer financial gain for minimal effort - i.e. plug this USB drive into the CEO's device and give it back to me tomorrow ;)

**Have you educated your team?** Threat actors will drop USB drives on purpose. Will a member of your team plug it into your network to help find the owner?



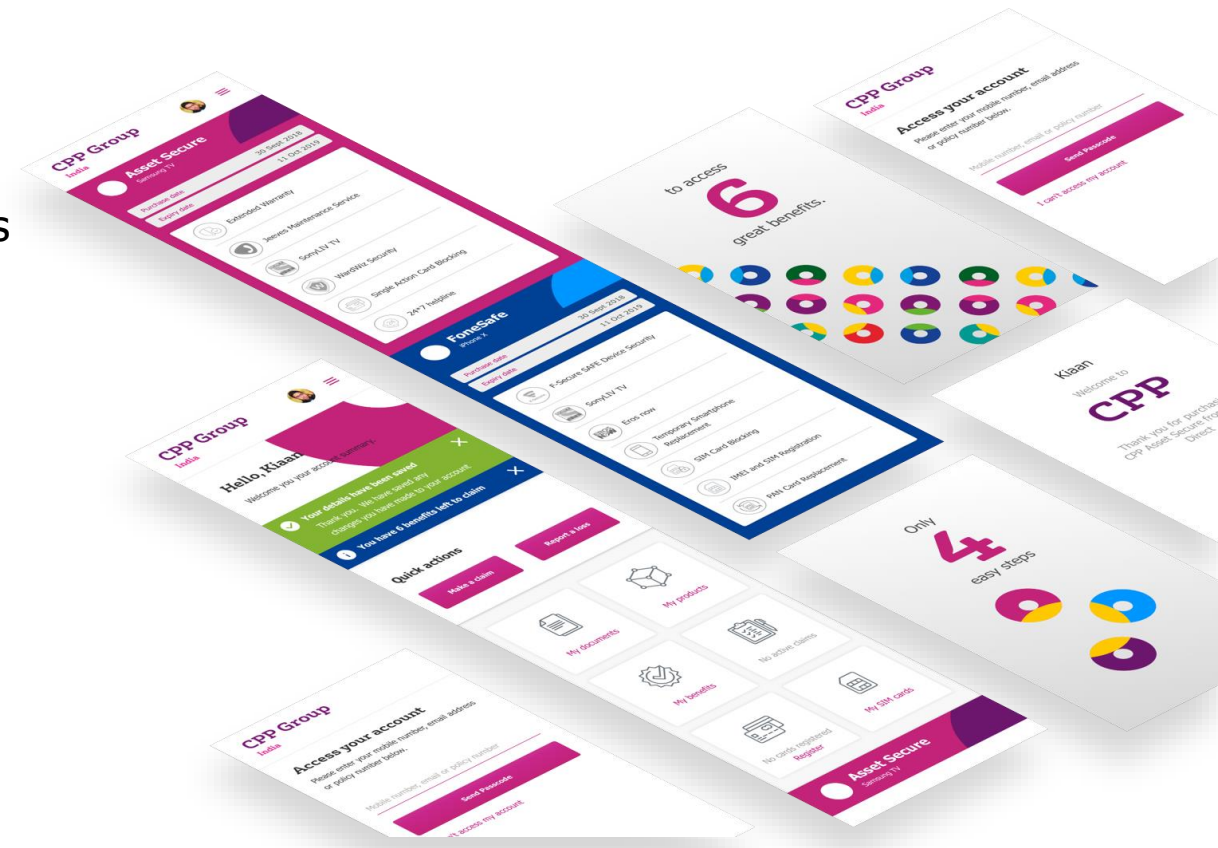
## 2. Some real world examples...Ransomware



## 2. Quantifying the risk...why specifically SMEs

- 16% of UK SMEs have suffered a cyber attack in the past 12 months...23% of London based SMEs
- That's almost 900,000 firms!
- More than 1 in 5 of those attacks cost the victim SME £20k, 11% over £50k\*
- The pace of increase in attacks is accelerating every month
- Ingenuity of attackers is increasing to stay ahead of attempts to curtail

\* Source: Zurich SME Risk Index.



## 2. Why SMEs are easy targets

### The risks for SMEs



**Being hacked**



**Business interruption**



**Losing revenue**



**Brand reputation damage**



**Losing customers**



**Personal liability and penalties**



**New laws & directives**



## 2. Why should SMEs care?

**“Gain an appreciation of the real life cyber risks that make SME easy targets”**

### Why should SME businesses care?

- Everyone is exposed, SMEs even more so
- The risk is real. It's everywhere and on the rise
- Traditional insurance products rarely provide sufficient cover – product design cannot keep up with the pace of the emerging threat

### Why should insurance advisors care on behalf of their clients?

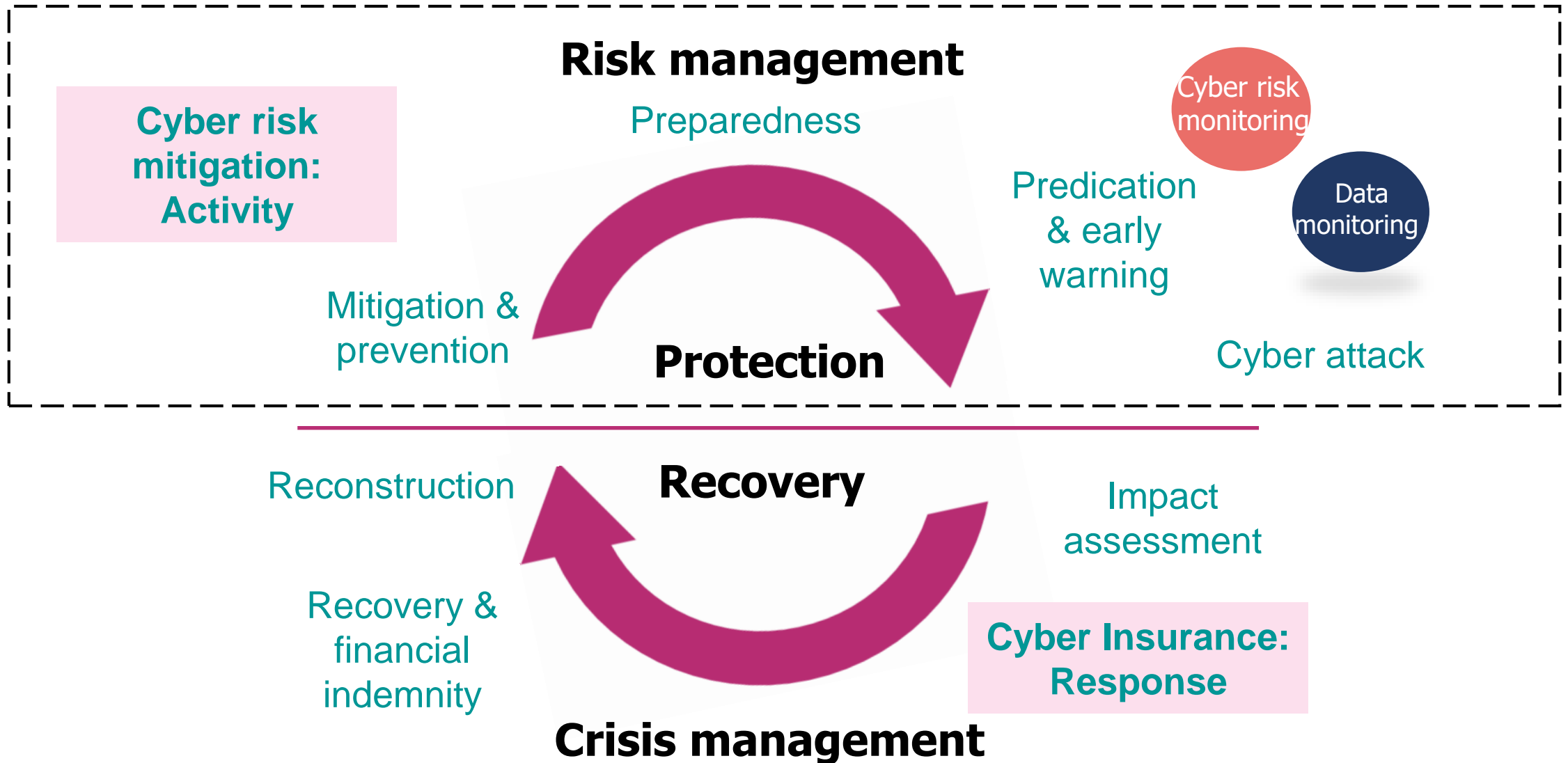
- Customers often think they have more cover than they actually do. This can lead to a false sense of security
- The fundamental problem is the failure of SMEs to realise that they need to 'prevent' as well as to 'cure'!

\* Source:  
<https://www.claimsmag.co.uk/2019/05/brokers-and-smes-far-apart-on-cyber-risks/14184>



### 3. Cyber risk mitigation – prevention IS better than cure

“Gain an understanding of the types of products available in the market that can be used to safe guard against cyber risk as a preventative measure”







## Quick Fact

Digital ecosystems provide the basis for a range of risk mitigation services that can prevent damage before it occurs. However, some of these tools involve opening up data to scrutiny and potential vulnerability in themselves...

### 3. Safeguarding against cyber risk

There are products available in the market that address the need for risk mitigation, e.g.

OWI

This data monitoring tool **detects if business data** has been compromised online and provides actionable steps on how to fix them

KYND

**There are tools to** help to monitor the level of IT risk using a businesses' website domain.



### 3. Safeguarding against cyber risk

#### How do data monitoring services work?



##### BUSINESS PROTECTION

This constantly monitors **SME business information** such as email address, bank account details, and payment card details.



##### HISTORICAL SCAN

After the SME business information is registered, it can run a historical scan against a database of **compromised data collected** since 2006.



##### RESULTS

The SME business will be alerted if **any information is found to be compromised** and what the level of risk is.



##### ACTION PLAN

The SME business will then receive a report with the **next steps to secure** the relevant details and limit the risk of them being compromised again in the future.



### 3. Safeguarding against cyber risk

How does this tool detect compromised data?



Dark Web webpages



Twitter Feeds



Sharing Networks



Compromised hosts



Command & control  
servers



**50,000** malware  
samples per day



Torrent sources



IRC channels

### 3. Safeguarding against cyber risk

#### How do cyber risk monitoring services work?



#### ASSESS

Cyber risk technology provides expert insight to the cyber risks an SME business may face by tracing what their domain is connected to



#### UNDERSTAND

Using a simple traffic light system, it can provide a risk report which highlights cyber areas an SME business could be exposed



#### FIX

If a part of the business is vulnerable, this tool will help the SME to take the next steps to stop potential cyber risks from turning into a real attack



#### MONITOR

It will monitor cyber risks and alerts the business to new ones if they arise





### 3. Cyber risk mitigation

Know your risks...audience profile



*Quick Fact*  
**If you registered by  
Wednesday 3<sup>rd</sup> July...  
your data is in here!**

an hour ago

SERVICE  
**Vulnerable Services**

This web server on [redacted] has a well-known and highly visible security vulnerability.

[Help](#) [+](#)

an hour ago

[redacted]  
**Domain Registration**

[redacted] does not match the domain [redacted]. This could be for a valid reason but it is best to check.

[Help](#) [+](#)

2 hours ago

[redacted]  
**Domain Registration**

KYND has connected [redacted] to your organisation.

[Help](#) [+](#)

## 4. Brokers as the trusted experts: Cyber Insurance

“Understand how brokers can show their value as a trusted expert advisor of choice for their SME clients”

of brokers have **never sold** a cyber insurance policy

**38%**

of brokers see cyber as an **area of growth** for their business

**78%**

A barrier to selling cyber is that 90% of **clients** believed that they **did not** need the **cover**

**90%**



**64%**

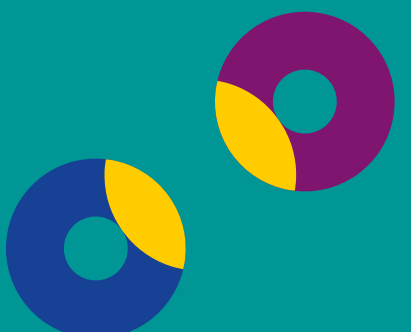
of brokers said they would like **more training** on cyber insurance & risk

**27%**

of brokers said they would **not feel confident** selling a cyber policy

**48%**

of UK businesses identified **one cyber attack** per month



“To remain competitive, insurance brokers have to be able to show their value as the trusted expert **advisor of choice** for their SME customers. If they fail to do so, they risk the core insurances that currently form the backbone of their income stream becoming vulnerable to those wishing to **commoditise** those products. It could also be argued that the provision of such advice lies in the very heart of a **broker’s professional responsibility**”



**How do you do this?**

\*Source <https://www.insuranceage.co.uk/broker/3898396/blog-brokers-need-to-seize-the-opportunities-in-cyber>



#### 4. Education...What we learned from speaking to SME businesses

**What do you use the internet for?**

"Online booking system which is cloud based, website, Facebook, Twitter & Pinterest"

**How concerned are you about cyber risk impacting your business?**

"Worried a little, not that much"

**What are your concerns if you suffer a cyber attack?**

"Hacker random, so we can't access customer details, fraud, competitors can see how we work"

**How concerned are you about cyber risk impacting your business?**

"Very concerned. Work with high profile retail payment systems, if we get hacked our customers wouldn't be able to take payments and would ruin our business and reputation"

**How would a cyber attack impact your business?**

"All my work is online, so I wouldn't be able to do business which would catastrophic and very embarrassing"

“

"No, I didn't know Cyber insurance existed"

**How protected are you against a cyber attack?**

"Not really at all, don't know how to do it and it's probably expensive for the amount of damage it could do."

**What are your concerns if you suffer a cyber attack?**

"Steal money and cause untold damage"

”

**Do you have cyber insurance?**

"No, I have insurance with xxxxx for public & employer's liability"

"Not for cyber but we should be covered under our PI?"

**How would a cyber attack impact your business?**

"It would really impact our business and it's a major concern at the moment. A cyber attack could give access to our customers systems, emails etc."



## 4. Some practical advice

### **Adopt plain language to explain cyber to SMEs**

Use language that the SME's staff and executives understand and relates to their day-to-day business activities.

### **Recruit champions**

Encourage the SME to appoint influential members of staff to champion cyber risk in the business.

### **Educate SMEs on their potential vulnerabilities**

Understand what data is valuable and why. Which elements of their systems are vulnerable to intruders etc

### **Adopt the right technology**

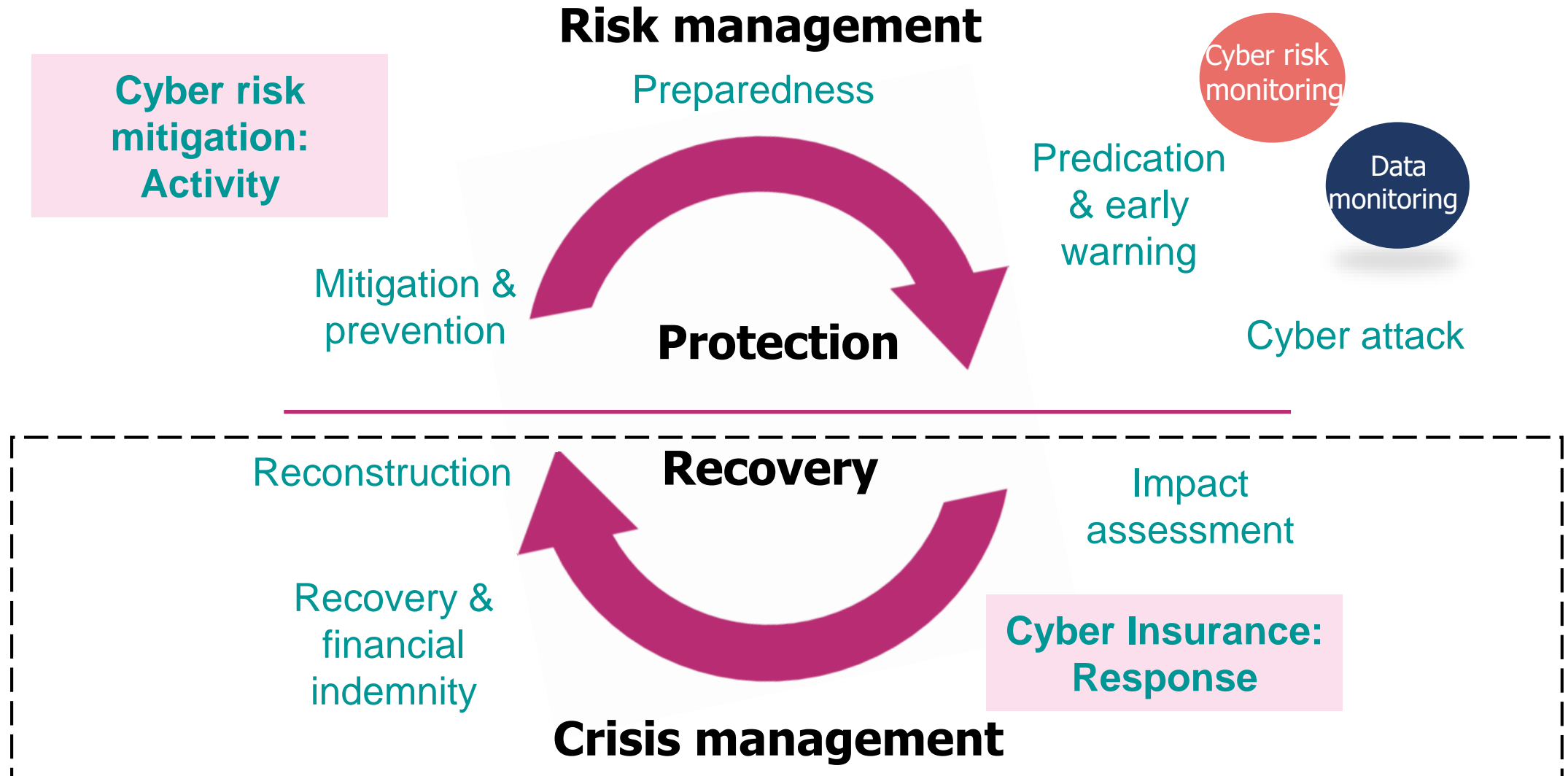
There is technology out there that can be easily implemented to help SMEs monitor and manage their cyber security

### **Education**

SMEs are highly vulnerable and the biggest problem is being ignorant to it. SMEs need to be aware of the threats they're exposed to and how they can detect suspicious activity. Poor password security, public wireless networks and suspicious emails are all examples where a cyber breach could occur.

## 5. Cyber Insurance policies

“Understand the role of cyber insurance policies in the risk management and risk mitigation cycle”





## 5. Cyber Insurance

### Specialist cyber insurance:



A range of sophisticated products are available in the market



Product designers & manufacturers are working hard to keep up with the increasing sophistication of the threats



There is more work to be done, but more flexible and more rapid delivery mechanisms are making relevant products available more quickly.

## More about us....

Our products and services keep people close to the things that are important to them. Whether it's personal possessions or digital identity we can help to keep them safe from harm, provide assistance to minimise inconvenience if things do get lost, broken or stolen - and help to put things back to the way they should be.



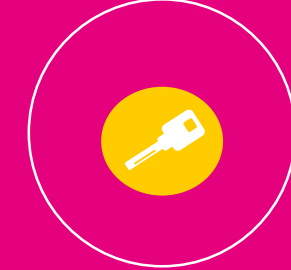
### For customers

We create and deliver **innovative products** that are designed to provide **peace of mind** for your customers by reducing the stresses of day-to-day life

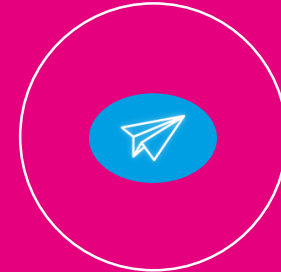


### For business partners

Our products are designed to **make your core products and services** better – adding critical value, revenue and differentiation, all with a fully managed customer experience



Basic Key Protection



Flight rescue



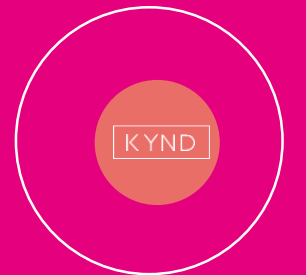
Cyber - Insurance



SmartKey Protection



Cyber - OwlDetect



Cyber - KYND

All of our products can be enriched with a wide range of relevant and useful benefits

## Re-capping our learning objectives & lessons:



1. Consider the regulatory position regarding cyber risk and understand what the PRA advice means in practical terms

→ The PRA's comments are ultimately designed to achieve better outcomes for end customers by ensuring that insurance firms are addressing potential prudential risks.



2. Gain an appreciation of the real life cyber risks that make SME easy targets

→ Advisors don't need to understand all the risks at a technical level, just be able to explain the key risks at a generic level.



3. Gain an understanding of the types of products available in the market that can be used to safeguard against cyber risk as a preventative measure

→ Digital ecosystems will provide the basis for a range of risk mitigation services that prevent damage before it occurs.







## Re-capping our learning objectives & lessons:



4. Understand how brokers can show their value as a trusted expert advisor of choice for their SME clients



Don't ignore the risk, you will be doing your clients a disservice. Seize the opportunity!

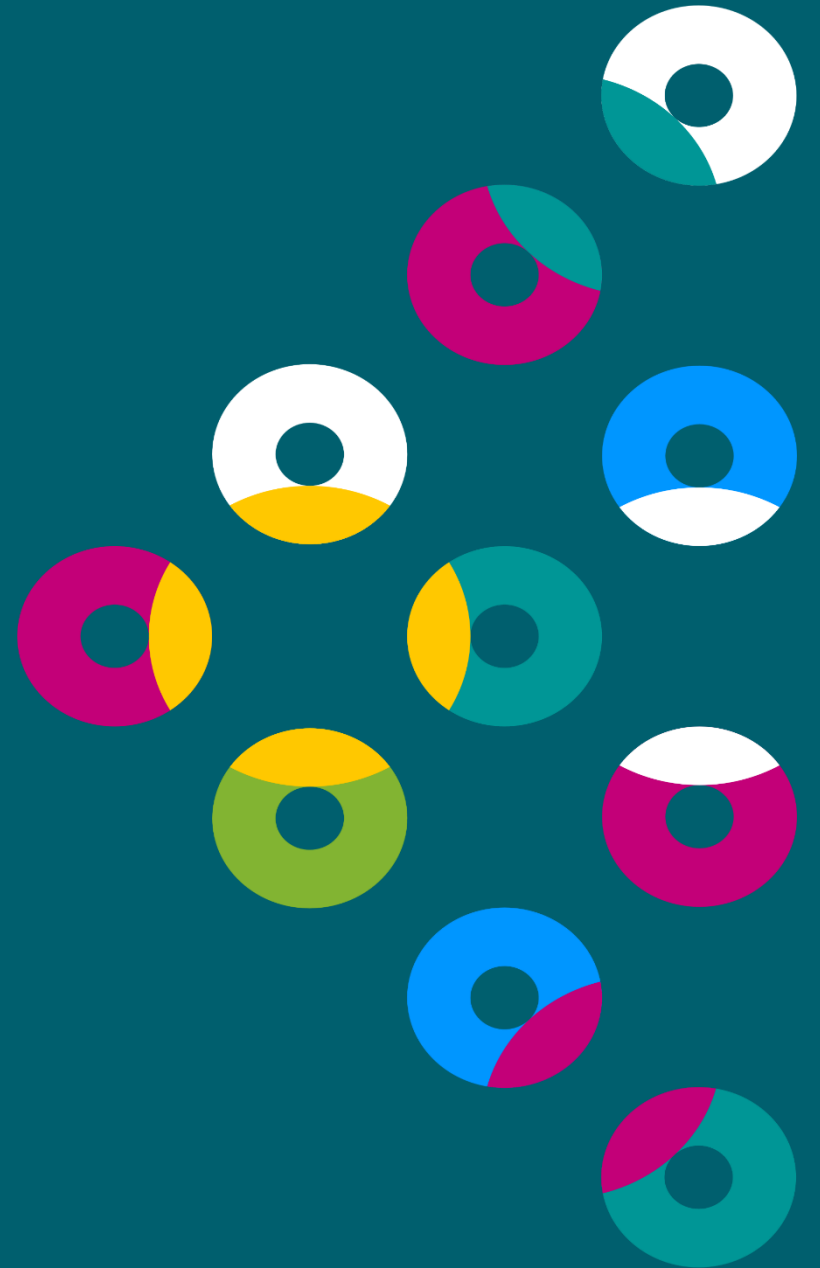


5. Understand the role of cyber insurance policies in the risk management and risk mitigation cycle.



Insurance policies generally provide 'after the event' assistance and indemnity. They are an important component in the risk mitigation toolkit, but are not the entire answer.

**THANK YOU**  
TIME FOR QUESTIONS





**Michael Whitfield**

**Managing Director**

**[michael.whitfield@cpp.co.uk](mailto:michael.whitfield@cpp.co.uk)**

**07860 255 260**



**Perry McShane**

**Sales Manager**

**[Perry.mcshane@cpp.co.uk](mailto:Perry.mcshane@cpp.co.uk)**

**07736 908 763**

**CPP Group UK**

**Inspiring Partnerships**

**[uk.cppgroup.com](http://uk.cppgroup.com)**