Cyber Insurance Application

Project Report

Dermot Berry

South East Technological University

17/04/2023

Supervisor – Dr Christopher Staff

Table of Contents

Introduction

Cyber Insurance has been expanding significantly in recent years since more attacks are happening more frequently, and the level of damage that occurred may leave businesses crippled by the repercussions of an attack. Most companies have experienced a cyber-attack in some shape or form. According to (GOMEZ PRIETO et al., 2023), 26% of the respondents had cyber insurance, while 74% didn't. The requirement/benefit of acquiring cyber insurance is expanding rapidly according to (NAIC, 2021) "Predictions indicate rates for cyber insurance buyers to increase by 15–50% overall in 2021". In 2021 (Balaban, 2021) states that "healthcare breaches reached 599 in 2020, a 55.1% spike compared to 2019".

The report entails the viability of my application for the cyber insurance industry, providing a secure web-based application, for Insurance providers to acquire instant results whether a potential customer is insurable or their risk is deemed too significant, by providing their answers to questions that are derived from multiple frameworks.

Description of the Project

The finished project is secure web-based application that users can complete a series of questions that will determine their overall risk, allowing the insurance company to determine if the potential client's risk is acceptable or too great. The application uses SQL databases for both the Users and the other database to store questions, scores, possible answers etc. The project has security such as input validation/sanitisation applied to pages that require user input. Depending on the selected options for each question a score is recorded. If the score does not meet certain criteria, the user is informed that insurance cannot be obtained as their cyber security posture does not meet the insurer's requirements.

Welcome page.

The welcome page doesn't allow users to create an account to login as the insurer may prefer to keep their information confidential. The site is hosted remotely which can be seen in the URL. See Fig 1.

Fig 1: Welcome page allowing user to login.

In Fig 2., the page only allows the user to perform one action with the application, preventing a threat actor from inputting malicious material.

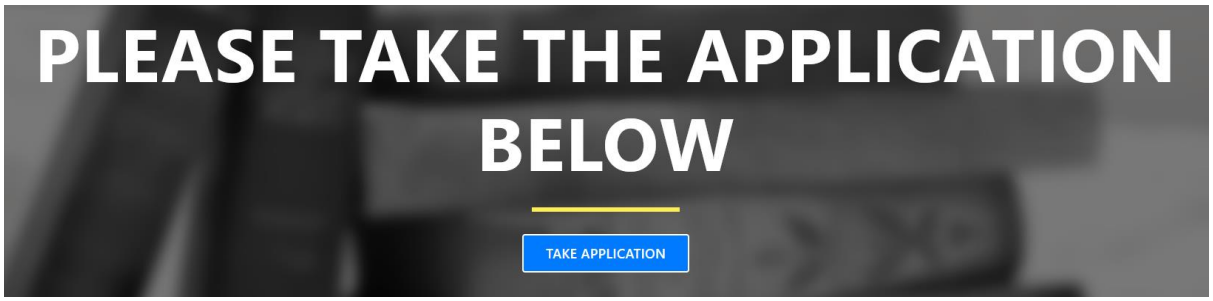


Fig 2: Application page, after the login is granted.

The application itself, only allowing the user to tick options, removing the need for an input field which may lead to an incident. Once the last question is completed the user moves to the score page. See Fig 3.

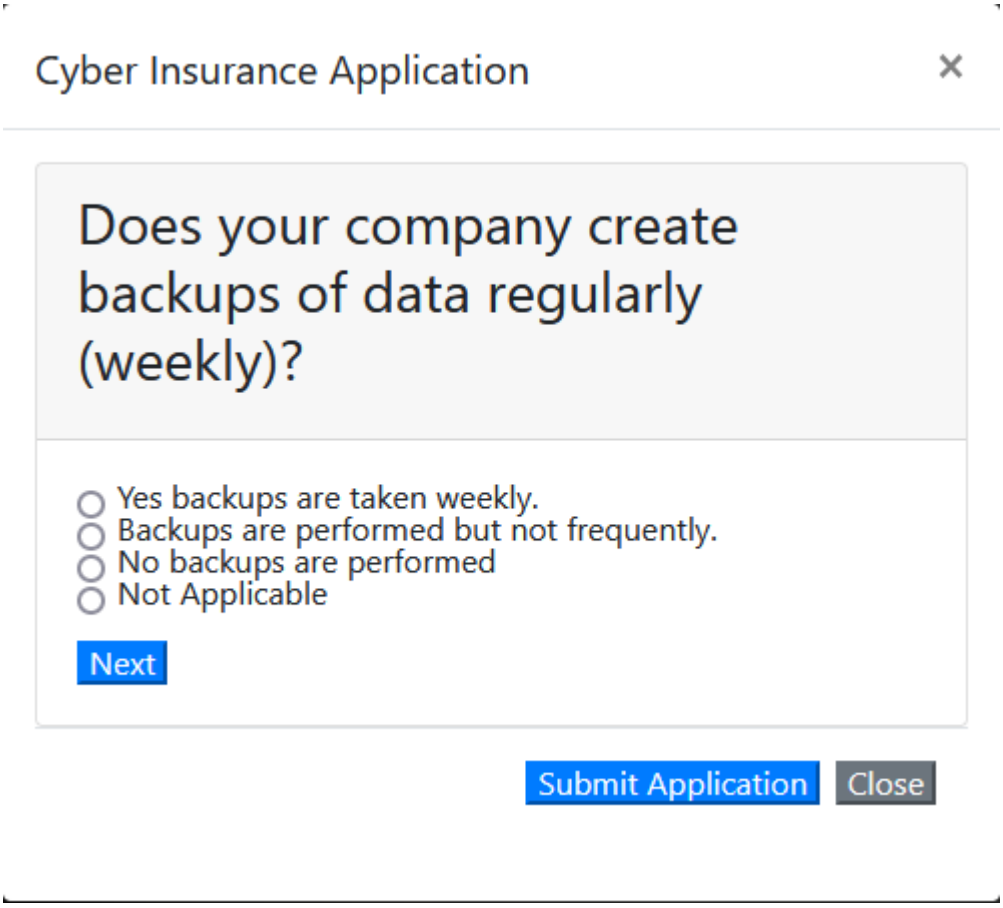


Figure 3: Application allowing the user to input tick box options only.

Fig 4 displays after the user has completed their assessment, the application can determine the score of the user for the insurance providers purpose to determine a premium. Also, if there are more than a certain number of controls missing the user is refused insurance automatically as their risk would be too high to insure.

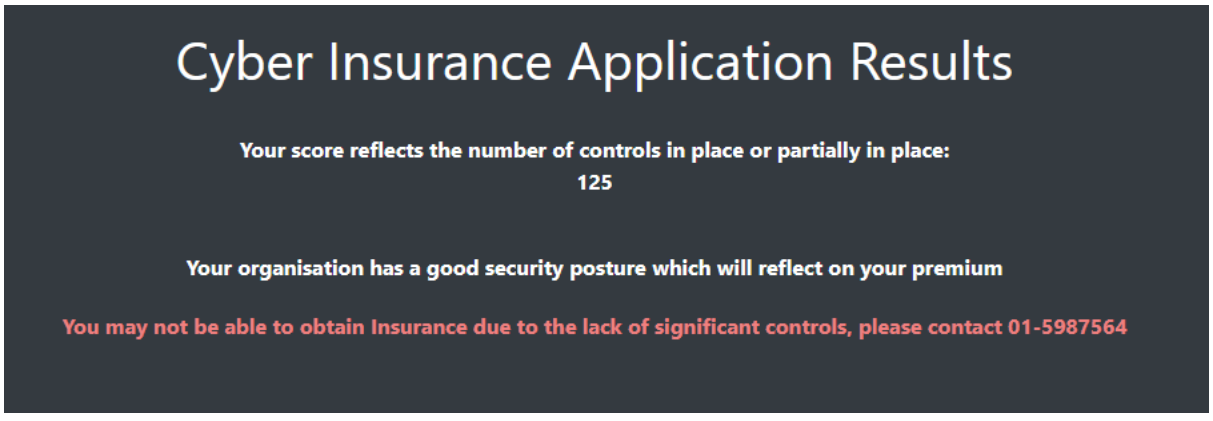


Fig 4: The score outcome of the user

General Issues

There were several issues that I didn't foresee. Many of the issues were overcome. However, there are several issues that remain.

Issues Encountered

Concept

After speaking with an auditor[1] who has experience in the insurance industry, it was disclosed that cyber insurance applications are not made public and the level of applications in the industry are more so paper/excel based. This meant that the application had to be made without any inspiration or knowledge as to how it should be presented to the user or its implementation. A secure web application is more suitable for this task as it can be accessed from anywhere, and results can be stored on a database to allow the insurer to check specific risks involved with a potential client with ease. A web-based application allows the calculations of risk immediately allowing insurers to save time and cost. Also, it gives a potential customer an indication that insurance can be obtained immediately.

Frameworks

There are various Frameworks that you can adhere to from a business perspective, however there are various frameworks to choose from. According (Cisternelli, 2022), the leading Cybersecurity Frameworks are NIST Framework and ISO 27001 & 27002. Most companies aim to adhere with one or more Frameworks with NIST being a popular Framework. I used NIST 800-53 and, ISO 27001 & ISO 27002 to choose the controls for the project. For most of the controls implemented in the application, I chose to find each control used across more than one framework. This pointed out that if a particular control was across multiple frameworks, it should be significant to the security posture of an organisation.

Vast number of controls

Considering NIST 800-53 has over 1000 controls, there was a significant amount of research needed pick suitable controls that would be valid in an insurance premium-determining application. This was a slow process, as I would read through ISO Frameworks also to determine if the control was used across more than one Framework. If the control was included in more than one framework it showed the specific control had to be of importance. This allowed me to include the control into my application by adapting the control into question for the user.

[1] Discussed cyber insurance to discover that cyber insurance applications mostly paper based and based at a high level. They wished to remain anonymous providing this information.

Time

The biggest issue was time constraints; finding these controls across multiple frameworks took a significant amount of time. The process of finding a particular control could take a minute or up to ten, depending on how much reading was involved before reaching a control with a significant risk associated with it. On average, it took around 6-8 minutes to choose a significant control. Once a control was selected, I would then search for the same control or control similar to the original control, and this part would take 50 - 60 minutes after reading through two ISO frameworks. After finding the particular control across more than one framework, I would create a risk matrix based on my opinion of the significance of the risk. The last step was to apply a risk methodology to validate the importance of a specific control. To determine the risk, I determined the strategic importance of each asset involved, the likelihood of the occurrence happening in a specific time frame, and the vulnerability of the business if an incident occurred. I aimed to get 200 or 300 controls assessed and have the risk methodology applied, however that did not happen as I did not have the time. In the end I assessed and applied the risk methodology to n controls.

Determining a Risk Methodology

In second year, I learned a significant amount about risk from our Incident handling and risk analysis module, a significant amount about qualitative and quantitative risk. Using knowledge gained from that module, I applied a Risk Matrix for each control for my application. Although I was asked by my supervisor on how I could back up my methodology with each risk matrix, I didn't understand that it would be my opinion to assess any risk, and I am no expert. After months I, too felt I did not justify my risk methodology even when pointed out by my supervisor. As the saying goes, "you can bring the horse to water, it doesn't mean it'll drink it." Approximately a week or two before my presentation, I realised I needed to add to my methodology, taking several factors to determine a risk score which would complement the risk matrices. The risk was assessed with a score as follows:

Strategic Importance * Vulnerability * Likelihood = Risk

Each of the conditions is given a score from 1 – 5. The result will determine the severity of the risk of each control implemented.

Hosting the application remotely

After implementing the project on localhost, I was advised that it would be a great feature to host it remotely. This was something I never done before, and it was daunting to say the least.

Another issue I had was that I didn't have an automated database and tables creation on my connection files, which would have been a nice feature. However, the tables are populated

with questions and answers, and I did not have the time to create automation for that as it would take too long.

Scoring System

The scoring system played a significant problem in the project. As I didn't have access to other scoring systems, I had to determine my own scoring system.

Security Aspect

Security plays a vital role in many applications that can be compromised in some form. I didn't know how I could keep the application as secure as possible throughout the application.

Issues Resolved

Concept

I resolved the issue of making an accurate application by defining questions that have significance from several Frameworks and applying a risk methodology to them, in turn assessing the risk of the user once completed. Industry feedback proved my application is similar to those in industry.

Frameworks

The Frameworks issue was resolved by taking questions from NIST and ISO Frameworks only as they are the most popular Frameworks that businesses try to obtain their standards.

Number of Controls

This issue could not be solved fully, as I simply did not have the time to research and assess each control that would be assessed. However, there are a significant number of controls assessed.

Time

Time was against me from the get-go, trying to research the project and be a part of the Irish wheelchair basketball team was demanding. With the number of controls in the Frameworks listed above, I would need a lot more time to assess over two hundred controls.

The Risk Methodology

I was able to determine a risk methodology for the application, to determine the severity of each control added to the app.

Hosting the app remotely

I was able to resolve this issue by enquiring with Catherine Moloney to figure out who to obtain a Blacknight account from. I was given an account from computer services, and then I had to figure out how to add my databases to their server. I found it difficult initially to add the databases. I was able to add both databases, one for users, and the other for the application details to keep them segregated (for security). After importing the databases, I was confused as to which database to link to Candept site. However, I realised that didn't matter from trial and error. I had setup my connection user and password which did not meet the criteria of the server's conditions, so I had to change the user and passwords on the databases to be accessible. Another issue was the actual questions wouldn't display to screen after getting it all to work. Later I found the issue was a small fix as a small piece of extra code was needed.

Scoring system

The scoring values were implemented by myself as I had no information as to how insurance companies would assess the risk of each control/question for their own determination. There is no affiliation with the score values.

However, after speaking with David Fortune[2], I realised that I should not give a potential client a score of ten for a particular control if it is not applicable to them. This made me re-assess how I approach the scoring. I changed the scoring system to negative mark all controls that were missing, partially in place, or not applicable, as if a company deems a control not applicable, that is incorrect. As the company is dealing with IT systems, data in some form, they should have the necessary controls that are asked in the application to ensure they are incident ready and have a good cyber security posture.

Possible Answer	**Original score weight**	**New score weight**
Yes, control is in place	10	10
The control is partially in place	5	5
No, control is not in place	0	-5
Not applicable	10	-5

Another problem which was an inconvenience was, when altering a score value for one control I managed to reset the whole table (of x controls) of its score to zero, which meant I had to enter all values again.

[2] Senior Security Consultant – all views are solely his own and not of his workplace.

Security

I proactively kept this in mind throughout the project. Since I could not find cyber insurance applications online, I adapted that approach throughout the application. I didn't add a registration page to the app as insurance companies in Ireland don't allow for the public to access these applications, whether paper or application based. On the login page I added parameterized queries, to prevent SQL injection. I also added session management and included an idle timeout function to the application. The login is the only page where a user can enter input, with the application page solely buttons and tick box input. This gives the user the least number of options when trying to expose the application. Usernames and passwords are hashed and salted to improve security.

Changes I would Make

If I were to make changes, it would be to attain cyber insurance applications in any form early on to see what detail is involved in the average application. I would have tried to reach out to experts earlier in my research as I would be able to get knowledge that would determine the accuracy of the application and the possibility of using their feedback openly with their permission. I would export databases regularly whenever significant changes are made to tables etc, as it prevents the loss of data and time required to fill tables. If I had the time to go back, I would try and get in contact with Insurance companies to try and establish a premium calculator which would allow the insurer to output the premium automatically on the website, or store their premium quotation online, allowing for a call-back scenario.

Accomplishments

I have created a secure web application with capabilities to perform multiple functionalities, the application would be able to send to users to receive an accurate representation of their cyber security posture. A list of accomplishments follows below.

Functionality	Description
Welcome page	A welcome page that allows the user to navigate to the login page
Login page	The login page is clear, allowing a user to log in and proceed to take the application
Assessment page	Once the user logins in they can begin to take the assessment

Score page	After completion of the application, the score is stored on the database and reflected to the user.
Logout page	Allows the user to logout
Admin Dashboard	Allows the admin to add, view users, and their score.

Functionality	**Description**
Display to the user, a welcome page, with a “login” button to allow the user to proceed through the application	The welcome page is basic functionality to stop unwanted traffic accessing the application. The login button allows the user to proceed and take the application.
Display to the user “Take Application” button	Allowing the user that has authenticated with the database to take the assessment.
Display to the user a frame that has multiple functionalities	The frame displays a question for the user to answer
Display to the user in the frame radio buttons that allow the user to select an option	with four options to choose from using radio buttons, the user can select an option that accurately depicts the state of that control.
Display to the user in the frame a “Next” button	The next button allows the user to move to the next available question once the current has been answered
Display to the user in the frame a “Submit Application” button that allows the user to complete the application	Whether if the user has completed all the questions or not it allows the user to complete the assessment. Once the user submits the application, it allows the user to navigate to the score page
Display to the user in the frame a “Close” button to allow the user to close the fame	Allows the user to close the frame if the application needs to be aborted for any reason
Display to the user a “score” webpage that allows for viewing their result	When the user has completed the application, their score, which is output to the screen, the page will determine and inform the user if their cyber security posture is suitable for insurance from the provider.
Display to the user “logout” button on the score page allowing the user to end session	After the user has seen their score and is finished, they can logout of the session

I gained countless knowledge from the respective frameworks that have given me knowledge of what is expected from a business standpoint to achieve a standard such as NIST 800-53 or ISO 27001 etc. I have assessed 60 controls for my project.

I learned how to host the application remotely using the University's facilities. I used knowledge gained from other modules that allowed me to create a significant website that has elements of security implemented to ensure the safety of the data of the user and the content from the organisation.

Industry Feedback

I managed to successfully get feedback from individuals from the IT sector, Senior Consultants, Risk managers, Compliance Manager, Head of Cyber etc. At the time my application was local based, so I was advised to enquire using a form online. After speaking with some past students and friends of mine, I was able to get in touch with experts in this field. Analysis of the expert feedback is below!

Response 1

The feedback below is from A Senior Security Consultant – David Fortune, the answers below are based on his opinion solely, and not of his workplace.

Respondent

2 | Anonymous | 75:58 Time to complete

1. **Would you mind sharing your name or if you prefer to keep it private, that's completely fine?**

   David Fortune - Senior Security Consultant - eir evo

2. **What risks concern you the most in terms of cyber threats?**

   Good question, but I am don't think it would be asked in a questionnaire for insurance. (I haven't seen anything like it anyway).

3. **If your company has been involved in an incident, how has it affected the company, policies etc, and how has it improved the overall cyber posture of the company?**

   I don't think companies would disclose if they have been breached (unless they're under some form of regulation - be it government oversight or central bank / public listed on stock exchange).

4. **What scope is there for coverage, i.e. what incidents would be covered under the insurance.**

   Coverage offerings are similar to any other insurance; it depends how much excess you're willing to pay and what type of "incidents" you want covered. Not all companies would have the same requirements. I would suggest asking something about how a company scopes their requirements.

5. **Are there any limits to cover, such as monetary limits on claims?**

Good question.

6. **What would you like to have added to an insurance premium? (what assets would you like to add to insurance that are not currently available).**

Good question.

7. **Can it be disclosed as to how your premium was calculated, e.g., size of company consideration, the industry they are in, past claims a factor in price.**

Good question and approach to it.

8. **Considering most companies that require cyber insurance are expanding annually, can a policy be automatically renewed?**

Insurance companies require a questionnaire to be completed annually that would detail any such changes that may impact the scope of insurance.

9. **How does your company value the premium you are given. Fair, or other?**

Good question, maybe offer some suggested "tick boxes" of answers - you would gather common data across different areas and get insight that could benefit the company using the application.

10. **If a claim has to be made, is the excess for claim high?**

Excess is scalable depending on the company's budget. You could drop the first part and just ask the simpler question

12. **Does your company create backups of data regularly, such as weekly?**

Good question. Suggest dropping "such as weekly" and ask the cadence of the backups.

13. **Is there Endpoint Security controls implemented?**

Good question.

14. **Does the organisation require third-party to access systems etc., is there an agreement in place?**

This question needs work - Suggest somehting like - "Does the company allow third-party access to systems?"

15. **If so are there NDAs in place?**

... this is the part 2 of the previous question. Good question.

16. **Upon Employee termination, is system access revoked, and is all security-related organisational system-related property retrieved?**

Good question.

17. **Is the company making employees aware of their cyber responsibilities through training etc.?**

Good question.

18. **Does the business take the necessary steps to destroy information that is no longer needed?**

Good question.

19. **Are you advising employees to take necessary actions and precautions to ensure the safety of confidential data?**

Good question, but the grammar should be addressed.

20. **Is data being recorded of deletion after removal? is removable data disabled to unauthorised users?**

2 Questions. Separate them.

21. **Is there assigned personnel (Manager) who is responsible for the security of assets and information who will communicate with the board/top management?**

2 Questions. Separate them.

22. **Is there a map of where data assets are stored or transmitted? Showing how identifiable data is being stored transmitted, disposed of etc. (life cycle)**

Good question - more privacy focused (an actual ask of GDPR).

23. **Are there controls in place that ensures the organisation is following standards, and procedures and data are maintained safely?**

Simply this question. Too wordy for a simple ask.

24. **Has the organisation a security and privacy plan in place? Have they provided an overview of the security and privacy requirements of the system? Including the risk for certain design and security decisions?**

Way too many asks here. Separate them and focus quesions on a single topic.

25. **Are there procedures in place to protect equipment that may be left unattended, such as computers, POS devices etc.?**

Good question. However, it could be worded a little clearer.

26. **Does the organisation identify critical assets to aid with a contingency plan? Has the organisation prioritized these assets so that the business can resume within a minimum time frame?**

Good question.

27. **Does the organisation perform a Root Cause Analysis of event?**

Good question. You could drop the second part allowing for more options to answer.

28. **Does the organisation have other security controls that may not be as secure as the primary security mechanisms however, that would enable business function to resume?**

This needs a reword to be a clearer ask.

29. **Does the organisation have an alternative storage site, such as Azure?**

Azure is a cloud computing service. OneDrive is a storage site. Azure is not seen as a storage facility.

30. **Is there an alternative site to carry out all processing for the organisation if the primary business premises are unavailable?**

Good question.

31. **Has the organisation the ability to recover the system to a known state after an incident or failure?**

You kind of asked this when you asked about backups. If you want to go deeper on backups, consider exactly what the asks are in both questions and ask them consequtively.

32. **Is all data backed up using a cryptographic function to prevent unauthorised viewing or altering of data?**

Good question. but, again... see above.

33. **Is there a control implemented to prevent any unauthorised changes to a system?**

This question is a little too vague - change controls can be technical (permissions) or administrative (policy).

34. **Does the organisation determine the potential security impacts before the live implementation of system changes?**

The essence of this question is good, it needs to be made a little clearer, though. Consider rewording.

35. **Does the cloud services provider adhere to regulatory controls?**

Companies don't tell cloud services where to store data - it is up to the customer to ensure the cloud provider offer data services in their regaulatory jurisdiction.

36. **Does the organisation implement the necessary statutory, and contractual controls?**

2 separate asks. Statutory are usually from a regulatory body or government. Contracts are between parties.

37. **Are the board involved in key decisions regarding cyber security?**

What is the question here?

38. **Does the company have an internal audit function?**

This question needs rewording. Is the ask about internal assessment/audit to find opportunities for improvement?

39. **Is there a baseline configuration of all systems developed, documented and maintained?**

Good question.

40. **Are controls in place to stop unauthorised changes to systems?**

Good question - but not sure it would be asked in such a way. Maybe ask - "Are controls in place to stop unauthorised changes to systems?".

41. **Has the company restrictions in place to prevent the unauthorised use of software? Ensuring the use of peer-to-peer file sharing is used in line with company policies.**

Again, controls in place to stop system changes like admin privilage requirements would stop this.

42. **Does the company have comprehensive logging and monitoring in place?**

Good question. Too wordy - simply ask does the company have comprehensive logging and monitoring in place. All event should be logged no matter the significance, as they could all add up for future investigation.

43. Can you provide feedback to the questions above as it helps me improve my application. **Thanks again - Dermot Berry** *

Overall, I think this has great potential. The best questions are always simple ones. Overly complicated or questions with 3 questions just lead to missing information. Ask all questions in their own question, maybe even something like Question 1a, 1b, 1c if they all fall in the same area - backups for example.

Following this response, other responses may share information from their current workplace, and it would be unethical of me to release their feedback/answers. However, I will include snippets below that I found interesting.

Other Responses (anonymised)

Person A

1. **Would you mind sharing your name or if you prefer to keep it private, that's completely fine?**

[redacted]

2. **What risks concern you the most in terms of cyber threats?**

Ransomware, Data Leakage, Phishing (email attacks),

3. **If your company has been involved in an incident, how has it affected the company, policies etc, and how has it improved the overall cyber posture of the company?**

The Company implemented [redacted] controls to close any security gaps as much as possible.

4. **What scope is there for coverage, i.e. what incidents would be covered under the insurance.**

Financial Loss

5. **Are there any limits to cover, such as monetary limits on claims?**

[redacted]

6. **What would you like to have added to an insurance premium? (what assets would you like to add to insurance that are not currently available).**

?

7. **Can it be disclosed as to how your premium was calculated, e.g., size of company consideration, the industry they are in, past claims a factor in price.**

I actually don't really know how the figure is calculated. We answer a load of questions and then they give us a figure. I'm guessing that depending on the answers to the questions they take a risk based approach and calculate the premium based on that eg. Are your backups tested regularly? If yes, premium reduces. If no it increases.

8. **Considering most companies that require cyber insurance are expanding annually, can a policy be automatically renewed?**

From my experience you must go through the same procedure every year. But if you're just being insured for a monetary value, eg 4 million, then if you attest to the same level of controls being in place then there should be no reason not to be automatically renewed.

9. **How does your company value the premium you are given. Fair, or other?**

Unfair. The price of premiums have sky rocketed in the last 5 years.

10. **If a claim has to be made, is the excess for claim high?**

I dont know.

12. **Does your company create backups of data regularly, such as weekly?**

Yes

13. **Is there Endpoint Security controls implemented?**

Yes

14. **Does the organisation require third-party to access systems etc., is there an agreement in place?**

Yes

15. **If so are there NDAs in place?**

Yes

16. **Upon Employee termination, is system access revoked, and is all security-related organisational system-related property retrieved?**

[redacted] There has been instances [redacted] revoked. [redacted] we do have a process to review access [redacted]

17. **Is the company making employees aware of their cyber responsibilities through training etc.?**

yes

18. **Does the business take the necessary steps to destroy information that is no longer needed?**

yes

19. **Are you advising employees to take necessary actions and precautions to ensure the safety of confidential data?**

yes

20. **Is data being recorded of deletion after removal? is removable data disabled to unauthorised users?**

?

21. **Is there assigned personnel (Manager) who is responsible for the security of assets and information who will communicate with the board/top management?**

[redacted]

22. **Is there a map of where data assets are stored or transmitted? Showing how identifiable data is being stored transmitted, disposed of etc. (life cycle)**

[redacted]

23. **Are there controls in place that ensures the organisation is following standards, and procedures and data are maintained safely?**

yes

24. **Has the organisation a security and privacy plan in place? Have they provided an overview of the security and privacy requirements of the system? Including the risk for certain design and security decisions?**

yes

25. **Are there procedures in place to protect equipment that may be left unattended, such as computers, POS devices etc.?**

26. **Does the organisation identify critical assets to aid with a contingency plan? Has the organisation prioritized these assets so that the business can resume within a minimum time frame?**

27. **Does the organisation perform a Root Cause Analysis of event?**

yes

28. **Does the organisation have other security controls that may not be as secure as the primary security mechanisms however, that would enable business function to resume?**

?

29. **Does the organisation have an alternative storage site, such as Azure?**

yes

30. **Is there an alternative site to carry out all processing for the organisation if the primary business premises are unavailable?**

yes

31. **Has the organisation the ability to recover the system to a known state after an incident or failure?**

yes

32. **Is all data backed up using a cryptographic function to prevent unauthorised viewing or altering of data?**

yes

33. **Is there a control implemented to prevent any unauthorised changes to a system?**

[redacted]

34. **Does the organisation determine the potential security impacts before the live implementation of system changes?**

somewhat

35. **Does the cloud services provider adhere to regulatory controls?**

yes

36. **Does the organisation implement the necessary statutory, and contractual controls?**

yes

37. **Are the board involved in key decisions regarding cyber security?**

yes

38. **Does the company have an internal audit function?**

yes

39. **Is there a baseline configuration of all systems developed, documented and maintained?**

40. **Are controls in place to stop unauthorised changes to systems?**

no

41. **Has the company restrictions in place to prevent the unauthorised use of software? Ensuring the use of peer-to-peer file sharing is used in line with company policies.**

somewhat

42. **Does the company have comprehensive logging and monitoring in place?**

no

43. Can you provide feedback to the questions above as it helps me improve my application. **Thanks again - Dermot Berry** *

Hi Dermot
It might be better to have a call sometime to discuss. Maybe you could ask my opinion on stuff or specific feedback on stuff. We could do a teams cal[redacted] email is [redacted]ie We could do something Friday or Monday if you want. My number is [redacted] as well.
Thanks
[redacted]

Person B

2. **What risks concern you the most in terms of cyber threats?**

Users, management not understanding the need for information asset protection, length of time for approvals for policies, standards, procedures, and controls.

3. **If your company has been involved in an incident, how has it affected the company, policies etc, and how has it improved the overall cyber posture of the company?**

No incidents We are a cybersecurity services provider, so we need to do continuous improvement and research to help all our clients.

4. **What scope is there for coverage, i.e. what incidents would be covered under the insurance.**

That is a tricky one. Stupid humans should never be covered. As long as an organization has a security policy architecture, controls implemented and tested regularly, and can prove what they have documented and how they are doing it and the staff know what is documented and follow the correct processes, then it should be covered under cyber insurance.

5. **Are there any limits to cover, such as monetary limits on claims?**

On the average with my dients I see million based on client size, products, and industry.

6. **What would you like to have added to an insurance premium? (what assets would you like to add to insurance that are not currently available).**

Nothing, when you have the right policy your physical and information assets will be covered.

7. **Can it be disclosed as to how your premium was calculated, e.g., size of company consideration, the industry they are in, past claims a factor in price.**

We have not had any claims over the las years, our policy is based on the limits that our clients normally request to cover any issues that came happen during their service.

8. **Considering most companies that require cyber insurance are expanding annually, can a policy be automatically renewed?**

No. An annual scope and risk assessment should be done before the renewal to ensure the organization continues to improve, tests and validates their own environment using standard processes on a regular basis.

9. **How does your company value the premium you are given. Fair, or other?**

For us our premium is fair.

10. **If a claim has to be made, is the excess for claim high?**

Not applicable and not sure I understand the question.

12. **Does your company create backups of data regularly, such as weekly?**

Backups are actually and are also covered by our so we have multiple layer backups separately segmented and protected.

13. **Is there Endpoint Security controls implemented?**

Yes, multiple in a layered defined t

14. **Does the organisation require third-party to access systems etc., is there an agreement in place?**

Third-party support vendors, no. Clients to their logs from our operations center, yes.

15. **If so are there NDAs in place?**

Most definitely, when we scope projects and discuss what a client wants, we put the NDA in place.

16. **Upon Employee termination, is system access revoked, and is all security-related organisational system-related property retrieved?**

Most definitely access is terminated immediately upon involuntary termination and [redacted] termination. [redacted]

17. **Is the company making employees aware of their cyber responsibilities through training etc.?**

Most definitely and they must sign an acknowledgement and our Employee Handbook upon new hire and annually, then reminded when they leave the organization.

18. **Does the business take the necessary steps to destroy information that is no longer needed?**

Yes, [redacted]

19. **Are you advising employees to take necessary actions and precautions to ensure the safety of confidential data?**

Yes, part of user awareness training and regular reminders throughout the year.

20. **Is data being recorded of deletion after removal? is removable data disabled to unauthorised users?**

Records that the deletion took place are done or a certificate of destruction if a device [redacted]

21. **Is there assigned personnel (Manager) who is responsible for the security of assets and information who will communicate with the board/top management?**

IT is in control of the assets, our [redacted] is responsible should an incident happen, and [redacted] is responsible for the annual testing and reviews. All information is reported to management which goes to the Board.

22. **Is there a map of where data assets are stored or transmitted? Showing how identifiable data is being stored transmitted, disposed of etc. (life cycle)**

[redacted] it is done by storage location or folder. The internal confidential is separate from all client information, and the personal information is separate from everything [redacted]

23. **Are there controls in place that ensures the organisation is following standards, and procedures and data are maintained safely?**

Yes, we have an annual [redacted] audit, an [redacted] risk assessment and control review, [redacted] vulnerability scanning, and ar[redacted] penetration test.

24. **Has the organisation a security and privacy plan in place? Have they provided an overview of the security and privacy requirements of the system? Including the risk for certain design and security decisions?**

Yes, the [redacted] team always asked about that and [redacted] is the owner of the security and privacy plans. The plans and programs provide detail and an overview for any client who asks can receive a copy and understand from a business viewpoint.

25. **Are there procedures in place to protect equipment that may be left unattended, such as computers, POS devices etc.?**

Yes, we have [redacted] technical policy for every device to protect all equipment.

26. **Does the organisation identify critical assets to aid with a contingency plan? Has the organisation prioritized these assets so that the business can resume within a minimum time frame?**

Yes, internally we are remote company and contingency [redacted] plans are in place. Yes on our client data storage because we support around the clock following the sun.

27. **Does the organisation perform a Root Cause Analysis of event?**

Yes, [redacted]

28. **Does the organisation have other security controls that may not be as secure as the primary security mechanisms however, that would enable business function to resume?**

Yes, because we are remote and some [redacted] o only [redacted] access is required from the remote laptops.

29. **Does the organisation have an alternative storage site, such as Azure?**

Yes.

30. **Is there an alternative site to carry out all processing for the organisation if the primary business premises are unavailable?**

We are 100% remote, so the alternative site is not required and we cross train in case someone on one of the team does not have Internet.

31. **Has the organisation the ability to recover the system to a known state after an incident or failure?**

Yes

32. **Is all data backed up using a cryptographic function to prevent unauthorised viewing or altering of data?**

Yes

33. **Is there a control implemented to prevent any unauthorised changes to a system?**

Yes. [redacted] monitoring.

34. **Does the organisation determine the potential security impacts before the live implementation of system changes?**

Yes, part of project management.

35. **Does the cloud services provider adhere to regulatory controls?**

36. **Does the organisation implement the necessary statutory, and contractual controls?**

Most definitely.

37. **Are the board involved in key decisions regarding cyber security?**

Yes.

38. **Does the company have an internal audit function?**

Yes, the [redacted]

39. **Is there a baseline configuration of all systems developed, documented and maintained?**

Yes.

40. **Are controls in place to stop unauthorised changes to systems?**

Yes.

41. **Has the company restrictions in place to prevent the unauthorised use of software? Ensuring the use of peer-to-peer file sharing is used in line with company policies.**

Yes, limited privileged access on the endpoints by users. Peer-to-peer file sharing is not permitted.

42. **Does the company have comprehensive logging and monitoring in place?**

Yes, our has a full runbook.

43. Can you provide feedback to the questions above as it helps me improve my application. **Thanks again - Dermot Berry** *

None.

Person C

2. **What risks concern you the most in terms of cyber threats?**

Loss of reputation, downtime, cost of outage, data privacy or customers and employees data.

3. **If your company has been involved in an incident, how has it affected the company, policies etc, and how has it improved the overall cyber posture of the company?**

Increased levels of security services in places. Staff are more aware. Training of staff is vital. Increased cyber insurance policy cover. Loss of income due to downtime. Loss of reputation. Cost to report and the resolve the issue. Loss of time dealing with the issue.

4. **What scope is there for coverage, i.e. what incidents would be covered under the insurance.**

Loss of income in the short and long term. Cost of reporting and resolving the issue. Cost of dealing with the issue from a PR perspective. Replacement of hardware. Use of a hotsite to move operations to.

5. **Are there any limits to cover, such as monetary limits on claims?**

Yes there are limits and also clauses in regards how far the cover will go if basic security is not in place.

6. **What would you like to have added to an insurance premium? (what assets would you like to add to insurance that are not currently available).**

Cost of professional services to recover and the investigate the issue. Cost of downtime. Assets = PCs laptops tablets network equipment and operational devices with hard drives.

7. **Can it be disclosed as to how your premium was calculated, e.g., size of company consideration, the industry they are in, past claims a factor in price.**

Size, amount of security services enabled. Type of data to be protected and company turnover.

8. **Considering most companies that require cyber insurance are expanding annually, can a policy be automatically renewed?**

No. Needs constant evaluation in line with new threats and security technologies in emerging. If we have more security then our risk goes down and the premium goes down also.

9. **How does your company value the premium you are given. Fair, or other?**

Fair.

10. **If a claim has to be made, is the excess for claim high?**

No.

42. **Does the company have comprehensive logging and monitoring in place?**

Yes

43. Can you provide feedback to the questions above as it helps me improve my application. **Thanks again - Dermot Berry** *

Ask if the company is aligned or accredited any ISO standards. Ask about encryption and two factor authentication to access company and third part SAS platforms. Backup of email platforms. Reporting on all platforms / audit logging. Good stuff. Well done. That's on the money.

The above answers from Person C were cut short, rather than taking up space on this document as Person C answered yes to every control question I had in the form.

Person D

2. **What risks concern you the most in terms of cyber threats?**

Business interruption due to cyber attacks and losing revenue due to an attack.

3. **If your company has been involved in an incident, how has it affected the company, policies etc, and how has it improved the overall cyber posture of the company?**

We have become more aware of possible threats. Re-training all staff to the dangers of phishing etc and key areas to look out for in the day to day running of the business.

4. **What scope is there for coverage, i.e. what incidents would be covered under the insurance.**

5. **Are there any limits to cover, such as monetary limits on claims?**

Yes. All claims have limits. Business interruption is based on the gross profit for the company over a 12/24/36 month period. For claims relating to customer compensation the limit is generally capped at €6.5million for public liability claims. However for more unique cyber requirements some companies will specifically build policies with dual underwriting. Essentially one company would cover a claim up to €6.5million and then a package will be drawn up with a second or even a third company to re-insure anything over the indemnity limit of €6.5million. These policies are generally significantly more expensive however and would be taken on by companies such as Lloyds of London.

6. **What would you like to have added to an insurance premium? (what assets would you like to add to insurance that are not currently available).**

The option to tailor make a product for smaller businesses rather than a "one size fits all" approach used by European companies.

7. **Can it be disclosed as to how your premium was calculated, e.g., size of company consideration, the industry they are in, past claims a factor in price.**

Generally daims factors are one of the main generators of insurance premium. This denotes a weakness in the company. If two claims for the same type of cyber attack are seen in the last 5 years am insurance company will request a third party to assess if that type of daim is likely to happen again. This is done at the businesses own cost and not the insurance company. It is possible to still get cover but an insurance company will add a memo to the policy excluding cover if they deem the company is at risk for another similar daim. The gross profit will also be taken in to consideration along with the business type and activity. If they use a third party vendor this can also cause in insurance company to increase the premium as the risk for an attack is greater.

8. **Considering most companies that require cyber insurance are expanding annually, can a policy be automatically renewed?**

All insurance policies can be auto renewed. It is up to the business to tell the company if there are any mid term amendments to be made (for example new employees). When renewal terms are issued the insurance will ask if there are any changes to be made.

9. **How does your company value the premium you are given. Fair, or other?**

More cover costs more money. If a policy covers all foreseeable claims then premium is generally not an issue. However to smaller businesses there can be push back on pricing offered. 90% of businesses will continue cover and pay premium once a thorough run through is done explaining all aspects of cover and risk.

10. **If a claim has to be made, is the excess for claim high?**

This varies greatly.The excess is generally between €500 and €1500 but can be greater depending on business activity.

All questions asked on the main survey were left blank and feedback is provided below.

43. Can you provide feedback to the questions above as it helps me improve my application. **Thanks again - Dermot Berry** *

Overall the questions generally follow along with the types of questions a customer would ask before inception of a policy and at renewal stage. As I work in the insurance space directly there are no questions induded that surprise me or that I haven't heard from a customer. The scope of the questions asked is also really broad which is great for a business. It asks the important questions and prompts really important information that a customer needs to know before investing in an insurance product. I feel like they are applicable to both small medium enterprises and more unique risks.

Person E

The feedback below for the application questions was left blank and feedback on those questions was provided in the last question.

2. **What risks concern you the most in terms of cyber threats?**

Business interruption due to cyber attacks and losing revenue due to an attack.

3. **If your company has been involved in an incident, how has it affected the company, policies etc, and how has it improved the overall cyber posture of the company?**

We have become more aware of possible threats. Re-training all staff to the dangers of phishing etc and key areas to look out for in the day to day running of the business.

4. **What scope is there for coverage, i.e. what incidents would be covered under the insurance.**

5. **Are there any limits to cover, such as monetary limits on claims?**

Yes. All claims have limits. Business interruption is based on the gross profit for the company over a 12/24/36 month period. For claims relating to customer compensation the limit is generally capped at €6.5million for public liability claims. However for more unique cyber requirements some companies will specifically build policies with dual underwriting. Essentially one company would cover a claim up to €6.5million and then a package will be drawn up with a second or even a third company to re-insure anything over the indemnity limit of €6.5million. These policies are generally significantly more expensive however and would be taken on by companies such as Lloyds of London.

6. **What would you like to have added to an insurance premium? (what assets would you like to add to insurance that are not currently available).**

The option to tailor make a product for smaller businesses rather than a "one size fits all" approach used by European companies.

7. **Can it be disclosed as to how your premium was calculated, e.g., size of company consideration, the industry they are in, past claims a factor in price.**

Generally daims factors are one of the main generators of insurance premium. This denotes a weakness in the company. If two claims for the same type of cyber attack are seen in the last 5 years am insurance company will request a third party to assess if that type of daim is likely to happen again. This is done at the businesses own cost and not the insurance company. It is possible to still get cover but an insurance company will add a memo to the policy excluding cover if they deem the company is at risk for another similar daim. The gross profit will also be taken in to consideration along with the business type and activity. If they use a third party vendor this can also cause in insurance company to increase the premium as the risk for an attack is greater.

8. **Considering most companies that require cyber insurance are expanding annually, can a policy be automatically renewed?**

All insurance policies can be auto renewed. It is up to the business to tell the company if there are any mid term amendments to be made (for example new employees). When renewal terms are issued the insurance will ask if there are any changes to be made.

9. **How does your company value the premium you are given. Fair, or other?**

More cover costs more money. If a policy covers all foreseeable claims then premium is generally not an issue. However to smaller businesses there can be push back on pricing offered. 90% of businesses will continue cover and pay premium once a thorough run through is done explaining all aspects of cover and risk.

10. **If a claim has to be made, is the excess for claim high?**

This varies greatly.The excess is generally between €500 and €1500 but can be greater depending on business activity.

43. Can you provide feedback to the questions above as it helps me improve my application. **Thanks again - Dermot Berry** *

Overall the questions generally follow along with the types of questions a customer would ask before inception of a policy and at renewal stage. As I work in the insurance space directly there are no questions induded that surprise me or that I haven't heard from a customer. The scope of the questions asked is also really broad which is great for a business. It asks the important questions and prompts really important information that a customer needs to know before investing in an insurance product. I feel like they are applicable to both small medium enterprises and more unique risks.

Analysis of user feedback

The feedback I have obtained comes from people who are in various areas of the I.T./Insurance Sectors. There are various opinions on certain elements of the application response and similarities in other areas.

When the users were asked “What risks concern you the most in terms of cyber threats?” there were a variety of responses, one user clearly stated Ransomware, Data Leakage, Phishing (email attacks), while others response was the loss of income, downtime, loss of reputation etc. I felt users who may deal operate from a technical standpoint deemed actual causes, where other users who are more so involved in the business side of their organisations are concerned about their downtime, financial loss. I found this interesting as it shows the different approaches to risk, one being preventative approach, while the other the reactive approach (concerned about the aftermath of a potential risk i.e., a phishing attack).

I believe my application is viable in the industry as there are significant similarities in the questions implemented. Although many questions were accurate, some of those questions were grouped together where they should be separated as they have significant importance that the user should answer separately. Some questions were not correctly asked, some were too complex or “wordy”.

Design Flaws/Differences

At the beginning of the project, I was focused on implementing an application that an organisation would require a third party to take in order to use or provide services for the organisation, as many organisations don't take any form of security assessment when dealing with a vendor. However, after researching this project, it was pointed out at my presentation by a supervisor that I should change my idea to assess businesses for cyber insurance. There is a significant difference in each project as my research was based on third parties and their security posture. The application is similar in some ways as it is based on whether a third-party/customer has certain controls in place. Both determine the risk that is involved with either obtaining a new third party for a vendor or insuring an organisation. However, most of the research before this is based on third-party risk.

I had plans to implement questions at random, so that each time the application is executed that it would display different questions. However, if the user is taking my application, it is better to have grouping of questions together. If the user needs to research controls, the next questions should be of similar type that allows the user to easily research all the same area before moving to the next, E.g., ask all human questions first, followed by data questions.

Additional Research

Additional research was required as the project is now aimed at a different target audience than the original idea. The research was required to determine the viability of a new project and its possible importance in the insurance industry.

There are differences in the current state of insurance applications in Ireland at present. Applications vary. However, most applications are excel based and/or basic regarding the questions asked.

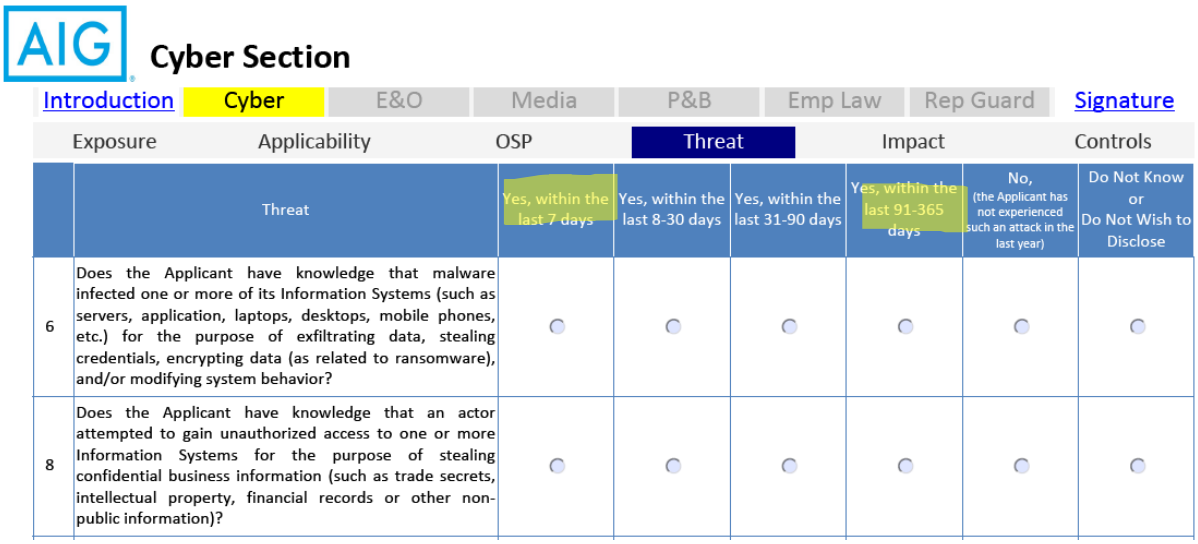
Analysis of current Cyber Insurance Applications

There are some cyber insurance applications which are available to potential customers immediately online however, most of those are from international insurance companies. Companies I have tried to perform an analysis of their applications are:

Insurance Provider	Online Availability
Sheridan Insurances	Not available
Brady Insurance	Not available
Arachas	Not available
Aon	Not available
AIG	Not available (American version available)
AnPost	Available for personal/family options
Techinsure.ie	Not available
OBF Insurance Group	Not available
OCI (O'Callaghan Insurances)	Not available
Chill Insurance	Not available
Brian Mullins (Brokers)	Not available
AXA	Not available
Liberty Group	Not available

From the list above Insurance providers, only two businesses can provide insurance online without having to request a call-back or an interaction of some form. It seems the insurance field in Ireland do not want to make their cyber insurance applications available for viewing from the public. While researching, I realised that AnPost can provide cyber insurance for personal or family options, and this may become an essential form of insurance in years to come. AIG Ireland also does not publish their application online. However, AIG USA did provide a cyber insurance application from July 2018, which is still available to view. This provided useful information as up until this point, I had no previous knowledge of what an application looked like, or what was being asked of the potential client. My only regret is not finding this application earlier in the project, as it would have helped guide me in relation to the types of questions asked in the industry.

The figure below shows how questions were asked on the AIG form. This was useful as it was similar in some sense to my own application. The selectable buttons represent the occurrence of a threat or breach of a specific control. This aligns with my risk methodology, the likelihood of an event happening is a factor is determining the risk of a particular control being breached or interrupted.



AIG **Cyber Section**

Introduction | Cyber | E&O | Media | P&B | Emp Law | Rep Guard | Signature

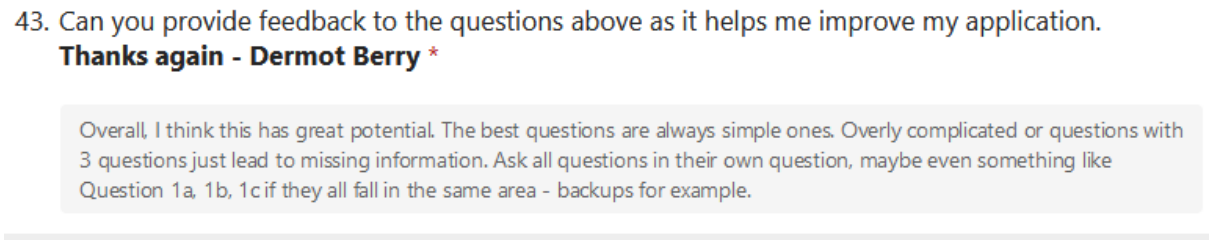
Exposure | Applicability | OSP | Threat | Impact | Controls

	Threat	Yes, within the last 7 days	Yes, within the last 8-30 days	Yes, within the last 31-90 days	Yes, within the last 91-365 days	No, (the Applicant has not experienced such an attack in the last year)	Do Not Know or Do Not Wish to Disclose
6	Does the Applicant have knowledge that malware infected one or more of its Information Systems (such as servers, application, laptops, desktops, mobile phones, etc.) for the purpose of exfiltrating data, stealing credentials, encrypting data (as related to ransomware), and/or modifying system behavior?	○	○	○	○	○	○
8	Does the Applicant have knowledge that an actor attempted to gain unauthorized access to one or more Information Systems for the purpose of stealing confidential business information (such as trade secrets, intellectual property, financial records or other non-public information)?	○	○	○	○	○	○

Fig 5: (AIG 2018) cyber application form

Industry Enquiries

As there were no insurance applications available to me from Ireland, I reached out to the industry in Ireland through various connections. I was able to obtain information which aided in my research and the accuracy of my project in comparison to those in the industry. The information gathered was tremendous, as it guided me on how I can improve the application and it is relevant to the current standards. I spoke with multiple experts in the field with varying positions. A Senior Security Consultant who has dealt with cyber insurance on numerous occasions. A representative in the Risk sector, a Compliance Manager the Head of Cyber Defences for a leading Irish Insurance provider and a commercial executive in a leading Irish Insurance broker. To be frank, I thought I wouldn't get any feedback on my application from anyone involved with insurance as it seems to be a closed-door setup, however, after receiving responses in my Microsoft forms, I was able to alter the application, fix mistakes made, move questions, separate them into separate questions etc. The feedback at the end was fantastic as I expected little feedback. Figures below are the final questions of each survey sent to experts.



43. Can you provide feedback to the questions above as it helps me improve my application.
Thanks again - Dermot Berry *

Overall, I think this has great potential. The best questions are always simple ones. Overly complicated or questions with 3 questions just lead to missing information. Ask all questions in their own question, maybe even something like Question 1a, 1b, 1c if they all fall in the same area - backups for example.

43. Can you provide feedback to the questions above as it helps me improve my application.
Thanks again - Dermot Berry *

Hi Dermot
It might be better to have a call sometime to discuss. Maybe you could ask my opinion on stuff or specific feedback

43. Can you provide feedback to the questions above as it helps me improve my application.
Thanks again - Dermot Berry *

Ask if the company is aligned or accredited any ISO standards. Ask about encryption and two factor authentication to access company and third part SAS platforms. Backup of email platforms. Reporting on all platforms / audit logging. Good stuff. Well done. That's on the money.

43. Can you provide feedback to the questions above as it helps me improve my application.
Thanks again - Dermot Berry *

None.

43. Can you provide feedback to the questions above as it helps me improve my application.
Thanks again - Dermot Berry *

Overall the questions generally follow along with the types of questions a customer would ask before inception of a policy and at renewal stage. As I work in the insurance space directly there are no questions induded that surprise me or that I haven't heard from a customer. The scope of the questions asked is also really broad which is great for a business. It asks the important questions and prompts really important information that a customer needs to know before investing in an insurance product. I feel like they are applicable to both small medium enterprises and more unique risks.

Learnings

Throughout the year I gained knowledge on various parts of the technical aspect of the project.

I learned how to host my project remotely rather than using a localhost server. I learned how to use Microsoft forms which allowed me to get feedback from experts in the industry. I also learned how to secure aspects of the application, such as implementing parameterised queries in input fields. I also implemented session tokens as another layer of security in the project. I learned how to design a better application using bootstrap. This allowed my website to present cleaner.

I acquired a lot of knowledge personally, the biggest being network amongst experts to acquire feedback with my project, it gave me the confidence to believe my application questions/layout is similar if not better to those in industry. I gained a significant amount of knowledge on risk and Insurance; the knowledge of risk was obtained by spending hours reading the various Frameworks listed to provide accurate questions for the application. I also learned how to accurately assign a risk score to controls using risk methodologies along with risk matrices. The main thing I learned was if I didn't sit down and keep on working away on the project, I would not be able to catch up.

Bibliography

(2018) *AIG*. Available at: https://www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/aig-usa-cyber-insurance-application.pdf.coredownload.pdf (Accessed: April 4, 2023).

Balaban, D. (2021) *Attacks on healthcare sector are on the rise*, *Forbes*. Forbes Magazine. Available at: https://www.forbes.com/sites/davidbalaban/2021/05/30/attacks-on-healthcare-sector-are-on-the-rise/?sh=4658c7dc264c. (Accessed: March 28, 2023).

Cisternelli, E. (2022) *7 cybersecurity frameworks that help reduce Cyber Risk*, *7 Cybersecurity Frameworks To Reduce Cyber Risk*. Available at: https://www.bitsight.com/blog/7-cybersecurity-frameworks-to-reduce-cyber-risk (Accessed: April 5, 2023).

Fig 5: (2018) *AIG*. Available at: https://www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/aig-usa-cyber-insurance-application.pdf.coredownload.pdf (Accessed: April 4, 2023).

GOMEZ PRIETO, J. *et al.* (2023) *Demand side of Cyber Insurance in the EU*, *ENISA*. Available at: https://www.enisa.europa.eu/publications/demand-side-of-cyber-insurance-in-the-eu (Accessed: March 28, 2023).

Report on the Cybersecurity Insurance Market (2021). Available at: https://www.insurancejournal.com/app/uploads/2021/11/NAIC-Cyber_Insurance-Report-2020.pdf (Accessed: March 28, 2023).

Acknowledgments

Firstly, I would like to thank Christopher Staff, my supervisor for his continuous guidance from day one. Chris has given me advise at any hour of the day, no matter how bad the questions.

I would like to thank my girlfriend Shauna, for her motivation to keep me going in college and her patience, waiting for me to finish college to get back into the working life, so we can move forward in our lives.

Thanks to my parents, who have been there since day one, helping me get back on my feet and telling me many times “hasn’t the years gone by so fast” & “you’re almost there”.

The experts I spoke to in industry, especially David Fortune who gave me fantastic feedback, without their input my project would only be a shot in the dark as to what is used in industry.

To my classmates, who I got to know in first year and then again in third year. We have been a tight knit group and it has been a pleasure to be able to stress about work all year round and their motivation to keep going.

Thanks to the Irish Wheelchair Basketball team for understanding and facilitating my absence early from trainings.

Declaration of Plagiarism

I declare, this document in this submission in its entirety is my own work except for where duty acknowledged. I have cited the sources of all the quotations, paragraphs, summaries of information, tables, diagrams, or other material. This includes software and other electronic media that is integral property rights may reside. I have provided the complete biography at the end of my document detailing all the works and resources used in the presentation of this submission. I am aware that failure to comply with the Institute's regulations governing plagiarism constitutes a serious offense.

Student:	Dermot Berry – C00242666
Supervisor:	Dr Christopher Staff
Institution:	South East Technological University
Title:	Cyber Insurance Application
Submission Date:	17/04/2023

Dermot Berry — 17/04/2023

Signature — Date