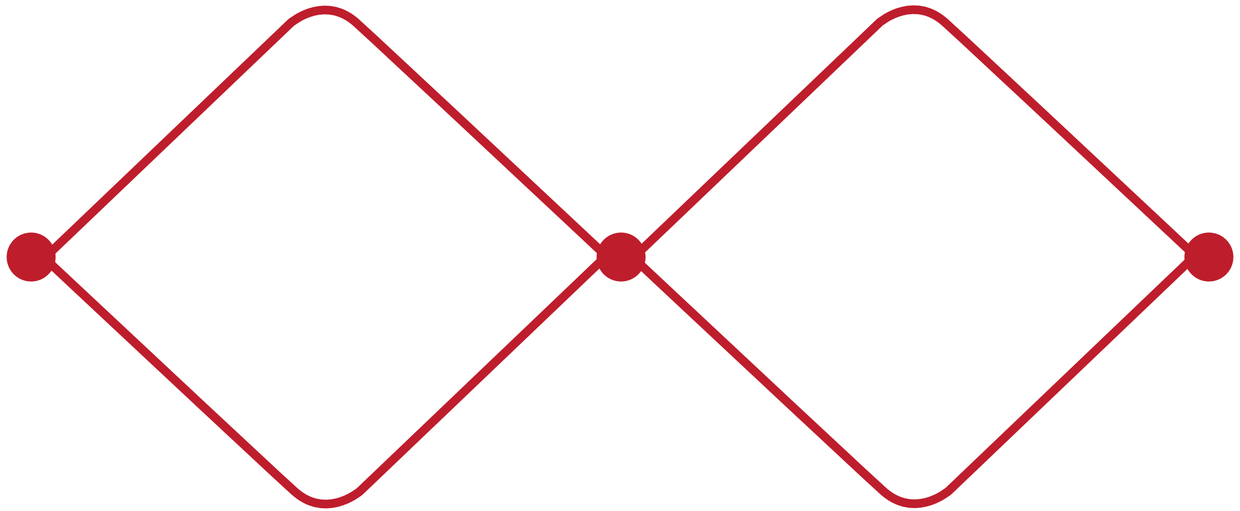
SANITAS
DATA SECURITY

Design Directions: Findings & Recommendations

Douglas Pflug Joe Lincoln Shiyu Ma Karla Henriquez

DESIGN PROCESS



Discover Define Develop Deliver

DESIGN PROCESS

The Double Diamond design process was used to provide structure to the project. It was introduced in 2003 by the Design Council as a graphical way to represent the design process. It is split into four phases:

DISCOVER
This stage of the process is for learning about the subject matter and surrounding information. The is focused on research and observation. This can be user and market research but also includes specific data concerning the client, systems and manufacturing.

DEFINE
The second stage is to define the brief. Using the data discovered in stage one the designer suggests a series of opportunities that can be tackled and developed using design methods. These are then analyzed and consolidated into the final brief.

DEVELOP
The third stage is aimed at ideation of initial concepts and the progression of these. Design methods and co-design techniques are used to produce developed concepts then these are analyzed to form the final concept.

DELIVER
The final stage of the process is for the development of the final idea. This consists of further co-design, testing and refinement.

CUSTOMER JOURNEY MAP

Stickdorn and Schneider (2011) thinks that Customer journey map is used to visualization of a service's experience. The whole customer journey map explains service interaction happened in touchpoint and accompanying emotion (ibid). He also suggests that we can find their process of service delivering and find their inner motivation and needs (ibid). In our project, a customer journey map was used to map each stage of customer's interaction. From this the attitude and needs of the customer will be determined and any opportunities and insights will be noted.

COMPETITOR ANALYSIS

Oxford reference define competitor analysis as a way to "analysis of competitors' strengths and weaknesses, strategies, assumptions, resources, and market positioning from all available sources of information, in order to identify suitable market strategies." In our project, a competitor analysis is used to identify close competition for the company and identifies similarities and differences in their services. Through competitor analysis, we identity some new service opportunities that Sanitas can develop in the future, such us membership program, packages, service aftercare.

OFFERING MAP

Servicedesigntool (n.d) suggests that the an offering map aim at describing what the service offers to the users through detailed ways. This instrument could support the elaboration of the service idea as well the development of some specific solutions. It could be a tool for the implementation of the concept but also for the communication of the service to the final user. In our project, we use offering map to visualize the offering services that are provided by Sanitas and to show how customer know their offering.

WHO IS SANITAS?

MARK PEGRAM

Began as a software engineer.
20 years experience in defense, IT and manufacturing.
Experienced project manager.

RIC DERBYSHIRE

Qualified in Computer Science and Cyber Security.
Focus on Penetration testing and hacking methods.

MIKE WATKINS

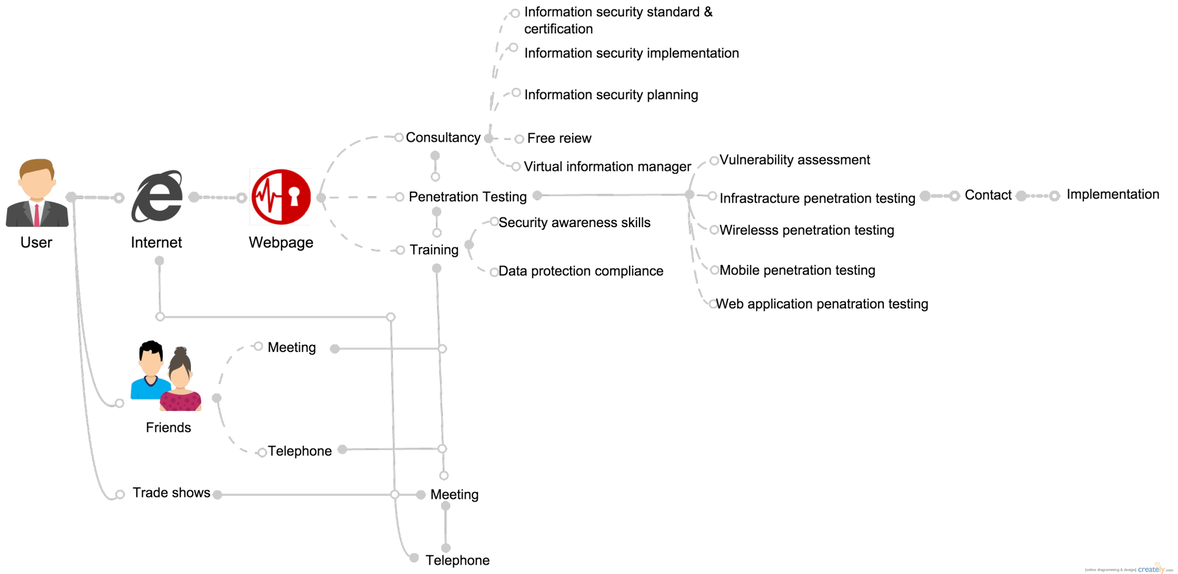
20 years experience in the IT sector.
Has an interest in Android app development.

Sanitas was founded by Mark Pegram, Ric Derbyshire and Mike Watkins. They met whilst studying the MSc in Cyber Security at Lancaster University. They soon discovered that they had a shared belief that IT security isn't just about having the right technology in place; having the right organisational attitude and behaviour is equally as important. They also believe that all aspects of information governance must be considered. They formed Sanitas Data Security with the intention of getting their belief across to UK organisations in need of data security guidance and support.

Meeting all the necessary UK data security laws and your industry-specific regulations can be a daunting and overwhelming prospect – that's where they come in. They offer a range of services including consultancy, penetration testing, training and research to ensure you meet all the necessary legislative and regulatory data security requirements.

They have a network of partners who complement and work alongside them to ensure they deliver a complete data security solution for their clients.
Sanitas pride themselves on delivering a high quality, personal service. They do this by taking the time to get to know the client and understand the clients data security and organisational needs before offering the ideal proposal to fit the requirements.

DISCOVER OFFERING MAP



OFFERINGS DISCOVER

PENETRATION TESTING

Penetration testing is an important step for developing any safe products and systems. On the one hand, penetration testing can scan vulnerability of systems or an operational site. On the other hand, penetration testing also stresses the implementation and design of a product or a system

(Linde, 1975) suggests that penetration testing tend to follows two approaches, which includes flaw hypothesis and attack tree. The flaw hypothesis approach is a flaw as a demonstrated undocumented capability, which can be exploited to violate some aspect of the security policy. When testers generate hypothesis flaws, they often complete background research at first. While, the attack tree is aim for penetration testing where there is less background information about system to be tested. The basic idea of the attack tree is a top-down approach which breakdown structure from the familiar tree representation of a logical proposition.

WHAT IS DATA SECURITY

Data security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites. Data security also protects data from corruption. Data security covers a lot of aspects of data infrastructures that may be technical and organizational, including procedures, policies, physical access.
‘We know how to secure our homes, offices and cars. We know what precautions to take while walking, shopping or doing business. We know which neighbourhoods to stay out of. We teach our children what to do, and we have a well-developed police and justice system that deal with miscreants. Although the police and justice system are coming to grips with the digital world, the criminals have successfully adapted their modus operandi for cyber space’ (Calder, 2005)

DATA SECURITY THREATS

There are many possibilities to cause security threat. To begin with, the damaged hard disk drive can lead to the loss of data. Also, hackers and malicious softwares, will also damage computer systems and destructs companies’ data. In addition, there is some operational error which should blame for the loss of data. ‘Hardware components can contain hidden backdoors, which can be enabled with catastrophic effects or for
Ill-gotten profit. These backdoors can be inserted by a malicious insider on the design team or a third-party IP provider’ (Sethumadhavan, 2011)

TRAINING

High rate of cyber-attacks is partly due to lack of data security awareness. Training focuses on protecting from hackers and from negligent behaviour. As many hacking attempts occur from disgruntled employees care must be taken so that there is internal security measures as well as external. Internal hackers can use their skills to do more hidden, but more critical damage to company. (Information technology security) so, positive and well- trained members of staff are an important part of making sure safe environment of data security. (Calder, 2005)

The systematic training can help company to minimise the possibility of security risks by increasing employees’ security awareness and skills, and use the act to protect their company from the damage of the attack. Data security is the degree of understanding of importance of information security and their capability to protect the organization’s data and networks. However, “ the three main barriers to information security awareness are: (1) general security awareness, (2) employees’ computer skills, and (3) organizational budgets “.

DISCOVER BLUEPRINT

The process blueprint maps all the interactions between the customer and Sanitas, the reason for these interactions, the attitudes and emotions of the client and this graph also maps potential opportunities for improvement of the interactions. The graph also shows the back stage causation. This mapping of the interactions was very useful in understanding the process which Sanitas and the customer undertakes and crucially could expose any points where there were opportunities to either make the process more efficient or perhaps more effective in regards to the customer's needs. To create the blueprint, information was gathered from meetings with Sanitas and through research on Sanitas.

Opportunities revealed during this method were:
Sanitas need to promote the need for their services instead of just what there services achieve.
Promotion of bespoke branding may generate more clients specific to that style of service.

- Sanitas need to promote the need for their services instead of just what there services achieve.
- Promotion of bespoke branding may generate more clients' specific to that style of service.
- Need to simplify and optimise the enquiry process.
- Possibility of selecting services through the grade of certification required.
- Methods implemented to persuade customers to purchase services after evaluation.
- Methods to generate repeats sales or additional services.

DISCOVER SWOT ANALYSIS

STRENGTHS

- Less outsourcing
- Certified
- Bespoke service
- Specialist knowledge
- Professional service

WEAKNESSES

- Small company size
- Specific client base
- No after sales service
- Limited marketing and advertisement

SWOT

OPPORTUNITIES

- After sales plan
- Improve brand awarness
- Optimise customer experience
- Improve communication with clients IT

THREATS

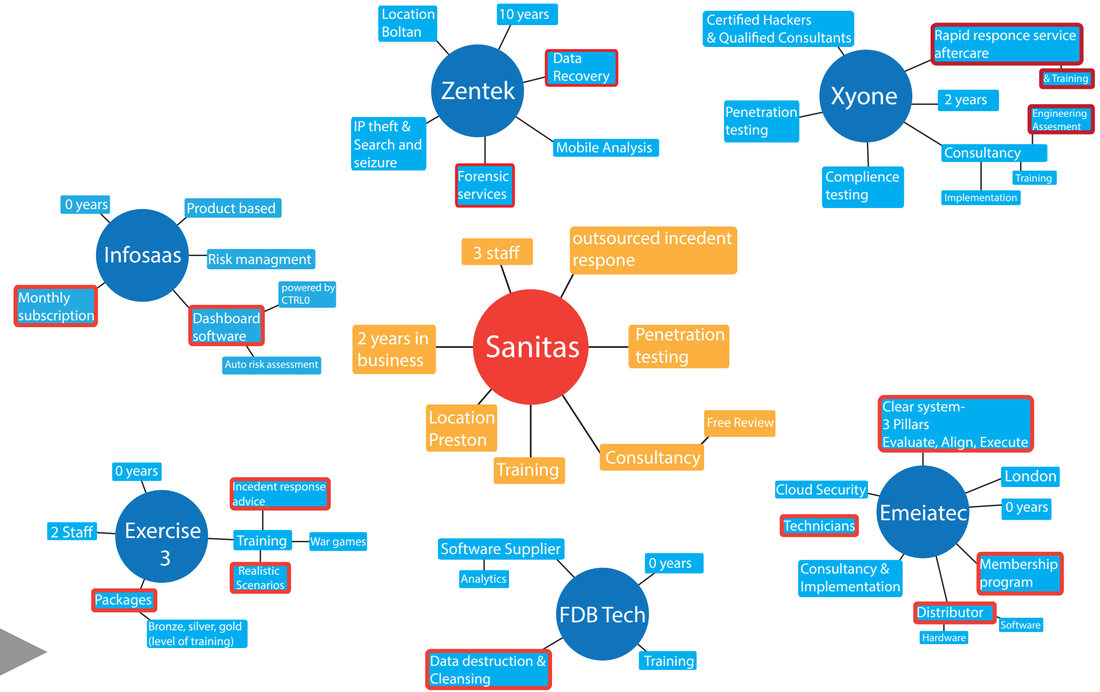
- Competitiors out sourcing resources
- Trend of automisation

COMPETITOR ANALYSIS

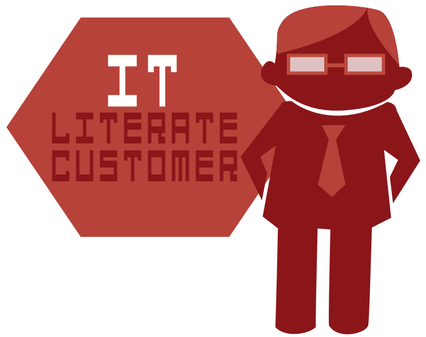
A competitor analysis was undertaken with focus on companies listed by (ukcybersecurityforum.com). This was to understand the differences in companies and to highlight opportunities for improvements and changes to Sanitas' services or client interactions. Some business's models were to unlike from that of Sanitas to make direct comparisons such as Xyone, which while offering similar services to Sanitas was found to outsource all of their services. The differences of interest and opportunities are highlighted in red on the competitor analysis:

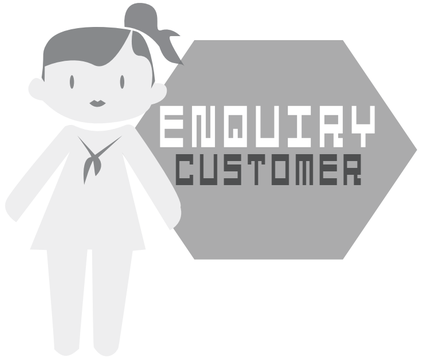
- Sanitas had expressed interest in developing a virtual security manager, which is a software solution. Infosaas offers a similar product and it was interesting to note that it is purchased with a monthly subscription.
- There were differences in the methods that services were offered. Emeiatec work using a monthly subscription, which Sanitas had noted as a possibility during initial interviews and Exercise3 split their services into graded packages of bronze, silver and gold, which Sanitas explained in further interviews that this had been attempted and hadn't been successful.
- Opportunities for additional services were Xyone's Rapid Response service that acts like an emergency service for security systems. However it was noted that this would not be possible with Sanitas' current four-employee structure. FDB Tech offers data destruction services that could be an opportunity for Sanitas and similar to Emeiatec they offer software sales as an additional revenue stream.
- A revue of Emeiatec revealed the opportunity to improve Sanitas' service framework. They use a very minimal 3-part system, Evaluate, Align, and Execute. This could provide clarity for the client.

COMPETITOR ANALYSIS DISCOVER



EXTREME USERS





It is essential to interact with the user in any research phase of a design project. Sanitas works with very large companies and other companies which they couldn't even disclose the names of. Due to the potential tarnishing of Sanitas' credibility it was decided that the customers could not be interacted with. This meant that to compensate for this we had to learn about the customers in other ways such as through meetings with Sanitas and secondary research. We found that Sanitas' clients fit into two groups. These two groups are the IT literate customer who potentially works for a larger company with an in house it department. The other is the business professional who doesn't quite know what they want but they know the desired end point, ie Cyber Essentials certification. It was found that each of these customers take a different journey to enquire with Sanitas and undergo the implementation slightly differently as well. The i.t literate customer doesn't need as much background infrastructure to enquire with Sanitas. The i.t literate customer may browse the website to check the offerings they provide but mostly only need the website for Sanitas' contact details. The i.t illiterate customer takes much longer looking at the website, potentially comparing Sanitas with other Data security companies before making a decision to contact Sanitas.

At the halfway stage of the project it was important to clearly define what opportunities discovered during the first half were going to be focused on. Sanitas had provided two options during the initial brief but had explained that these were open to interpretation and change depending on how the project developed.

OPTION 1

To focus on the Information Security Design and Implementation, and Penetration testing services. To improve services and client interaction, develop a more concise process and develop methods that allow less knowledgeable client to understand services.

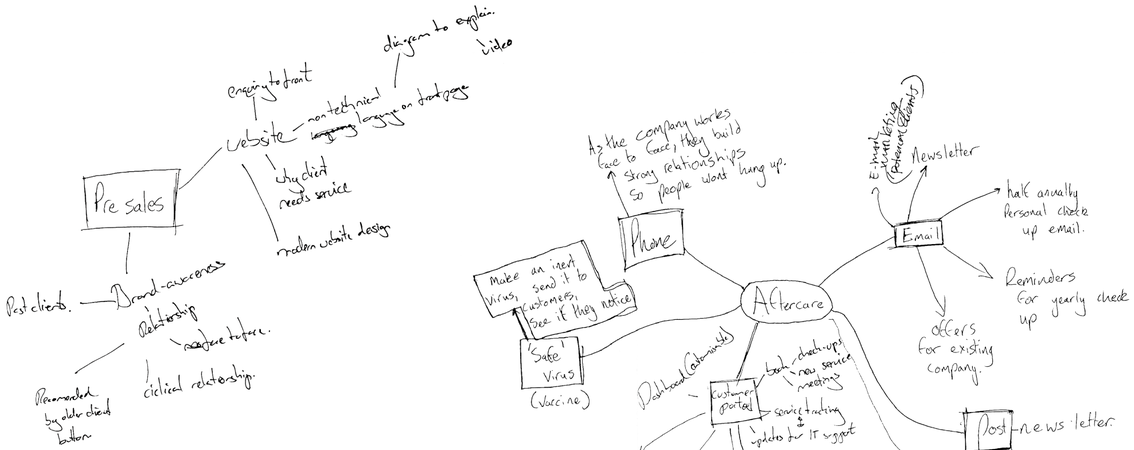
OPTION 2

To design a Virtual Security Manager. A software based information security system.

DEFINED BRIEF

While both options were interesting it was thought that due to limitations with both there might need to be an adapted brief to allow the group to progress. The Virtual Security Manager option was not taken beyond initial brainstorming as it was felt that it didn't suit a service design project structure or outcomes. Focus was given to option one however during research it was found that due to the inability to contact Sanitas' clients, the inability to shadow Sanitas and a universal defined implementation structure suited for the services there was very little room for progression.

It was decided to develop recommendations for presales and aftersales activities as these had little development and provided room for improvement and implementation.


Pre sales
Website
non-technical
language on front page
diagram to explain.
Video
engaging to front
stuck client
needs service
modern website design
Past clients.
Brand-awareness
Relationship
nurture before.
Recommended by older client base
cyclical relationships
As the company works face to face, they build strong relationships so people won't hang up.
Phone
Make an alert Virus, send it to customers, See if they notice
Safe Virus
(Vaccine)
Aftercare
Dashboard (automated)
Customer portal
book check-ups
new service
meeting
service testing
updates for IT support
NEW CLIENT "one" ID. GRAPHIC
Training PDFs
collecting info.
Email
Newsletter
E-mail (Existing clients) (Potential clients)
mail annually personal check up email.
Reminders for yearly check up
offers for existing company.
Post
news letter
E-mail
mail annually Vulnerability test.


IT PROFESIONAL IDEAL JOURNEY
GO ON WEBSITE
SEE REQUIRED SERVICES
RING OR E-MAIL SANITAS
NEEDS
EASY TO FIND WEBSITE
EASY TO FIND INFORMATION
QUICK RESPONSE
EMOTIONS
CONFIDENT THROUGH RECOMMENDATIONS
IMPRESSED BY RELATIVE INFORMATION
RELIEF

USER JOURNEY 2

IDEATION

The development stage of the process began with simple ideation using data gathered during the discovery stage and structure and focus provided during the define stage.
Mind maps focused on presales and aftersales separately generated opportunities for further development.

OPPORTUNITIES FOR PRESALES HIGHLIGHTED WERE:

- Optimising the website to generate more online enquiries by both extreme user demographics and how to promote services better.
- Improve company image and awareness through its website and other activities. This included optimising the webpage so it appears higher on search engine searches and how to stand out from competitors.

OPPORTUNITIES FOR AFTERSALES WERE:

- Aftersales contact. How could Sanitas extend the relationship with the client through communication and promotion? Initial ideas were newsletters, phone calls and emails.
- A ‘safe’ virus to check that all implemented systems and training were working to the correct standard.
- Customer portal. It is intended that this would be useful during the development and implementation but would also extend the relationship with customer.

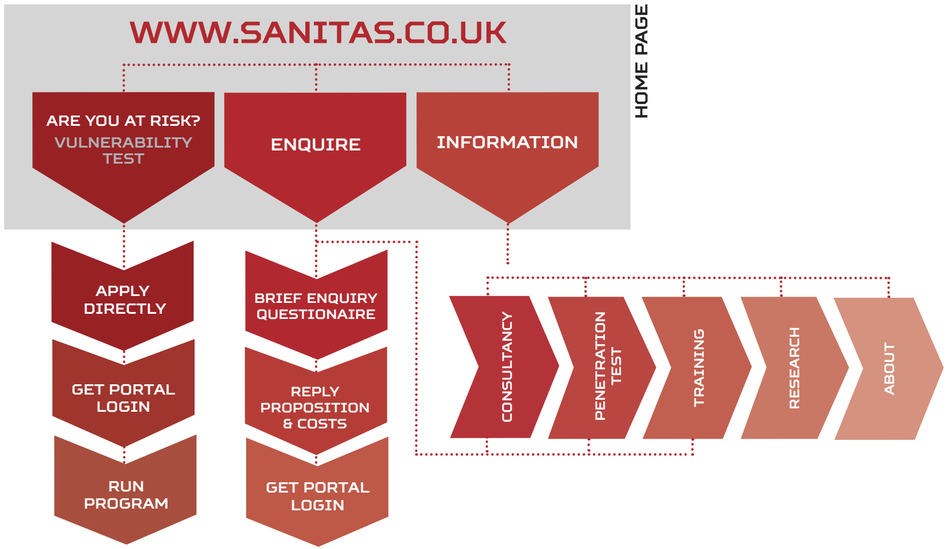
IDEAL USER JOURNEY MAPS

The group developed user journey maps with the focus of showing what was perceived through the research to be the ideal user journey for both extreme users. This would provide insights in how to optimise the presales and aftersales.

INSIGHTS WERE:

- Making the website easier to find.
- Providing the correct information clearly and when relevant for each extreme user.
- Provide separate paths through the website for each extreme user.
- Making enquiries a priority on the website.
- Quick response. A portal system was highlighted to provide consistent communication.
- Bespoke and well-managed aftercare, especially for the unknowledgeable demographic.

WEBSITE MAP



WEBSITE MAP

The website map represents the basic structure for a customer journey through the website. The grey rectangle represents the simplified vision for the front page. This has been designed to give focus too what has been perceived from the research as being the main tasks.
The enquiry option has been moved to the front and centre of the first page to signify that this is the function of the website and would generate more enquiries. This is to provide a more direct path for the unknowledgeable client by bypassing the technical information that they may not understand or have time to understand.
The information path is aimed at those who do have time or the technically literate client who wishes to conduct research into the business before enquiry or knows their requirements and just wishes to see if Sanitas could provide this.
It was highlighted during the research that a reason for the lack of sales is that the client sometimes does not realise the need for the services, as they do not believe that there is a problem. It was decided to promote the risks to encourage the client to purchase additional services. To do this a fix priced service, the vulnerability test would be conducted. The fixed price would encourage uncertain customers to purchase in contrast to the unknown costs of further services. It is a low cost and low effort service on Sanitas' part and would generate more clients.

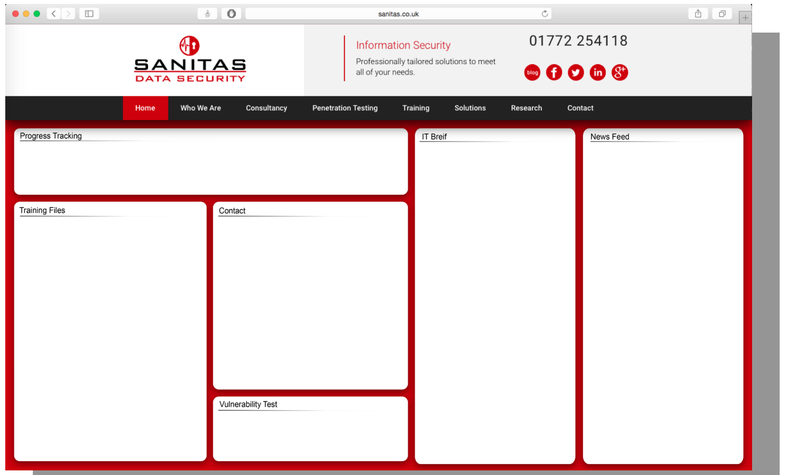
WEBSITE RECOMMENDATIONS

- During the research it was found that many information security companies talk in technical language on the website. For Sanitas to stand out it is suggested to take inspiration from lifestyle company branding and talk to the customer on the website like person to person. This would allow the company to be more approachable and would improve its bespoke brand image.
- The website should be optimised to suit the users goals and provide focus to these tasks over the company service offering. This streamlines the process and would generate more enquiries through the website.
- The British government is now asking all companies that work in contact with it to have Cyber Essentials security certificates so this is an opportunity to promote this on the front page of the website.

The Sanitas website is hard to find through search engines. To improve the visibility of the website it is recommended to use Search Engine Optimisation (SEO). This is using keywords in the website so it appears higher on a search engines findings. Using Google adwords the following phrases were highlighted:

- Security penetration testing
- Penetration testing
- Security testing
- Web security testing
- Information security courses
- Supply chain security
- Pen test training
- Penetration testing training
- Security chain
- What is penetration testing

CUSTOMER PORTAL



The Customer Portal is intended to improve Sanitas' services and relationship with the client. The visual shows a simple mock up of what this may look like. It is a modular design so that it can be tailored to the individual client to retain the brands bespoke identity. It also allows the sale of further services but as the customer must have a login it retains its exclusivity.

PROCESS TRACKING

Allows the client to view the progress of the service from purchase to implementation. This is to improve communication and relationship.

TRAINING FILES

Sanitas' training service consists in part of PDF files and presentations. This area could allow the client to download them after purchase for reminders or training new staff. Sanitas could also offer the sale of additional files or 'toolkits' in this area as a new revenue stream.

VULNERABILITY TEST

Once the client has purchased a vulnerability test from the website they are given a portal login. This module allows them to download any necessary software and record the results, which will also be forwarded to Sanitas.

CONTACT

A module to streamline contact with Sanitas to book services, meetings or check-ups. This frees up time for Sanitas to spend time on other things.

IT BRIEF

This module is aimed at improving communication with the clients IT support company. The client can allow the IT Company to access this communication thread.

NEWS FEED

A module that contains the companies newsletter highlighting risks and services. This is aimed at generating more sales and brand awareness.

CUSTOMER PORTAL

The customer portal is useful in aftercare techniques as it extends the relationship with client also providing them with a way to contact Sanitas. Promotes the sale of additional services.

NEWSLETTER/EMAIL

This aftersales method is aimed at generating company reputation, brand awareness and repeat sales. Recommendations for this method are:

- Speak to the reader like a person to promote bespoke branding.
- Aim information at the current risks and how Sanitas' services can protect against these.
- Promote new services.
- Use a client case study as promotional material. Possible limitation to this is that the clients IT support would prefer not to have flaws exposed but this could be solved by removing names and sensitive information.

PERSONAL CORRESPONDENCE

A more time consuming but beneficial method of communicating and promotion would be physical meetings and phone calls. This would be under the premise of checking if the implemented systems or training was working effectively. The aim the of this form of communication is to promote the bespoke branding of Sanitas and to generate more sales through clients that prefer this treatment.

DEVELOPMENT LIMITATIONS

The biggest limitation in the development phase was the fact that Sanitas' customers could not be studied. It is the most basic knowledge that in any design process the first step is to fully understand the customer through ethnographic and anthropometric research. In service design this is no different, the design must revolve around the customer. Secondly, immersive research into Sanitas as a company was not possible as they interact with the client mostly over the phone or by email for the enquiry, then face to face later on. Again, due to the fact the clients couldn't be studied meant that the service couldn't be witnessed but instead Sanitas has to explain the process afterwards. There is a difference between witnessing something yourself and somebody telling you about it, which meant the design process was hampered a great deal.

IMPLEMENTATION LIMITATIONS

The main limitation for the implementation was that in order for the company to grow they would need to implement what was recommended, but some of the recommendations will not be as necessary now as they will when they increase the flow of customers at a later date. This may seem counterintuitive to undertake recommendations at some cost and time which won't see a return on this investment until the future, but potentially the gain in customers would be worth the effort now. Another possible limitation in the implementation stage is that if the website is tailored too much for the i.t illiterate customer, it may look unprofessional to the i.t literate customer. If the website is too technical though, the I.t illiterate customer may feel out of their depth and look elsewhere.

THE BRAND AWARENESS WILL BE INCREASED BY:

- Higher ranked and easier to find website through search engines.
- Optimised website

THE BRAND LIFESTYLE WILL BE PROMOTED BY:

- Customer Portal.
- Aftercare newsletter.
- Optimised, customer focused website.

COMMUNICATION WITH CLIENTS AND I.T PROVIDER ACHIEVED BY:

- Customer portal

OPTIMISING THE WEBSITE FOR EXTREME USERS TO HELP GENERATE MORE ENQUIRIES BY:

- Giving the option to quickly skim information and enquire quickly for the i.t literate customers and making the website more interactive and thought provoking for the i.t illiterate customers.
- The customers will feel that Sanitas have really made an effort to understand their needs and this will pay off through word of mouth advertisement.

BETTER CUSTOMER RELATIONSHIP TO GENERATE REPEAT SALES BY:

- Aftercare newsletter
- Personal check-up from Sanitas

SPEED UP ENQUIRY PROCESS BY:

- Making the website more efficient for each customer will be a bi-product of optimising the website for them.

Brown Tim, (2009), Change by Design: How Design Thinking Transforms Organizations and Inspires Innovation, HarperCollins e-books, United Kingdom.

Calder, A. (2005) A Business Guide to Information Security. How to protect your company's IT assets, reduce risks and understand the law, London: Kogan Page Limited.

Design Council ,(2015), official website, design methods section, Available at: http://www.designcouncil.org.uk/news-opinion/introducing-design-methods

Doswell, B. and Watson, D.L. (2002) A Guide to Information Security Management, New York: Palgrave Macmillan Ltd.

Doyle, C. (Ed.). (2011). A dictionary of marketing. Oxford University Press.

Fischer, R.J. and Janoski, R. (2006) Loss Prevention and Security Procedures. Practical Applications for Contemporary Problems, UK: Butterworth-Heinemann.

Hunter, R. (2002) World without Secrets. Business, Crime, and Privacy in the Age of Ubiquitous Computing, New York; John Wiley and Sons Inc.

Parker, D.B. (1983) Fighting Computer Crime, New York: Charles Scribner's Sons.

Parker, D.B. (1998) Fighting Computer Crime. A New Framework for protecting Information, New York: John Wiley & Sons, Inc.

Parliamentary Office of Science and Technology (2006) Postnote October 2006 Number 271 Computer Crime, London: Parliamentary Copyright.

Sangiorgi, D. (2009). Building up a Framework for service design research, Conference Proceedings of the 8th European Academy Of Design Conference, Aberdeen, Scotland

Sangiorgi, D. (2011). Transformative services and transformation design. International Journal of Design, 5(2), 29-40.

Services design Tools, (2009), Official website, Tool blue print section, Available at: http://www.servicedesigntools.org/tools/35

Stanford Design School, (2015), Official Website, Design methods - Extreme User section,

Available at:
http://dschool.stanford.edu/wp-content/themes/dschool/method-cards/extreme-users.pdf

Stickdorn, M., & Schneider, J. (2011). This is service design thinking: Basics, tools, cases. Wiley.

Strebe, M. (2004) Network Security Foundations. Technology Fundamentals for IT Success, U.S.A: Sybex Inc.

The Audit Commission (2005) ICT Fraud and Abuse 2004 – Public Sector Update June 2005, Wetherby: Audit Commission Publications.

Ukcybersecurityforum.com,. 'Companies In North West Cluster'. N.p., 2015. Web. 23 Mar. 2015.

Vellani, K. (2007) Strategic Security Management. A Risk assessment Guide for Decision Makers, Oxford: Butterworth – Heinemann Ltd.

W.Hamlen Kevin, Thuraisingham Bhavani, (2012), Data security services, solutions and standards for outsourcing, The University of Texas at Dallas, United States.

Wollacott, P. (2007) Unknown threats lurking inside and out, as cited in Media Planet - Information Security – A Special Report about Keeping your Business Data Safe, London: The Times, March 27 2007 edition.