A Business Plan for Data Security and Privacy Services

Wen Zeng[1], Abigail Smith[2], Moira Carroll-Mayer[2], Vasileios Germanos[2], Francois Siewe[2]
[1]School of Computer and Information Engineering, Shanghai Polytechnic University, Shanghai, China
Email: wen.zeng.wz@gmail.com
[2]School of Computer Science and Informatics, De Montfort University, Leicester, U.K.
Email: P2549817@my365.dmu.ac.uk, moiracaroll2000@yahoo.co.uk
vasileios.germanos@dmu.ac.uk, FSiewe@dmu.ac.uk

2024 IEEE/ACIS 24th International Conference on Computer and Information Science (ICIS) | 979-8-3503-7664-7/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICIS61260.2024.10778387

***Abstract*—Cyber Security Academic Startup Programme (CyberASAP) provides academics with the expertise, knowledge and training needed to convert their research into technologies, products and services. Due to the fast development of digital technologies, data security and privacy became an active research topic. However, we do not have business plan templates for data security and privacy. Therefore, it is necessary to develop a business plan for data security and privacy technologies, which can help the data security and privacy research out of the university lab and into the commercial market. In this study, technical and non-technical risks and related contingency plans will be addressed through consideration of risk management and secure system architecture.**

***Index Terms*—Business, commercial market, Cybersecurity, security industry, data security, privacy**

I. Introduction

A business plan is a key tool for planning and achieving positive outcomes using the business model [16]. It provides a picture of short to medium-term objectives and projected forecasts. It shows how you intend to implement it. It also provides details on key aspects of the intended operations on the governance, the particular service, the market, achieving sustainability, and social impact.

Cyber Security Academic Startup Programme (CyberASAP) has provided academics with the expertise, knowledge, and training needed to convert their research into products and services in the global economy since 2017 [4], [9]. CyberASAP is funded by the UK Department for Digital, Culture, Media and Sport and delivered by Innovate UK KTN and Innovate UK. Every year, CyberASAP invests up to £800,000 in innovation Cyber security projects coming from an academic research base. It creates a pipe to move great Cybersecurity ideas out of the university lab and into the commercial market [4], [9]. In this program, an important part is to developing an operational business plan in the field of Cybersecurity and Digital Forensics.

There are some Cybersecurity business plan templates, for example: [3], [8], [15], [18], [19], which can guide you on every stage of the business writing. However, as far as we know, there does not have any business plan templates for data security and privacy services.

In this study, we will develop a business plan in the fields of data security and privacy. Technical and non-technical risks and related contingency plans will be addressed through consideration of risk management and secure systems architecture.

This paper is organized as following: Section II is the basic concepts in this paper. Section III is the executive summary. In Section IV, the services will be listed which can help organizations improve their GDPR compliance position. In Section V, we will discuss the market; and then Section VI is the competitive analysis. Section VII and Section VIII are the personal plan and financial plan, respectively. In section IX, we will discuss the legal and ethics of starting a Cybersecurity company. Section X concludes the paper.

II. Preliminary Material

In order for commercial organizations to operate in a modern business environment, they must meet a series of data privacy and data protection-related ethical and legal requirements. One of the most recent paradigm shifts in these requirements was the adoption of the General Data Protection Regulation (GDPR) by the European Union (EU) on 14 April 2016, enforceable from 25 May 2018.

The GDPR itself represents an effort to harmonize data protection legislation across the EU, enhance privacy and data protections for consumers, and introduce stronger regimes of fines and penalties to punish breaches and non-compliance.

The GDPR is the culmination of popular, political, and consumer pressure which has developed in response to the growing use of data for commercial purposes. It also represents the most prominent set of controls in the world, and one of the strictest. It heralds, or in some cases directly prompted, other jurisdictions to make efforts to improve their data protection laws and motivated consumers to become more aware of the risks to their personal data, and rights they can exercise towards it [17].

A McKinsey survey in 2020 found that "Consumers trust companies that limit the use of personal data and respond

979-8-3503-7664-7/24/$31.00 ©2024 IEEE
Authorized licensed use limited to: De Montfort University. Downloaded on March 05,2025 at 10:29:37 UTC from IEEE Xplore. Restrictions apply.

quickly to hacks and breaches" [1]. The same survey found that 50% of consumers trust companies and brands that quickly react to hacks or breaches.

This motivated consumer basis, and wider political pressure, are not simply due to a changing cultural zeitgeist [14]. This changing attitude in both institutions and mass society is itself a rational response to the dramatic increase in threats to personal data in recent history. As personal data is processed in increasing quantities, potential attack vectors, and value of personal data (to various different types of malicious actors) have increased too. "Threat actors" who target information systems have grown, and indeed recent academic discussions suggest even the most pessimistic estimates on the proliferation of threat actors understate the problem [12]. Subsequently breaches of personal data have increased in both volume, depth, and cost – both economic and non-economic.

Data breaches are listed by the World Economic forum as one of the top 5 threats to global stability [20]. $5.52 is the average total cost of a breach at enterprises of more than 25,000 employees, compared to $2.64 million for organizations. The average total cost of a data breach has increased by 10% since 2014 [20], [21]. The number of data breaches has increased almost tenfold from 157 breaches in 2005 to 1497 breaches in 2019 [11].

In this context of a stricter legal framework, a more informed, more energetic consumer base, and a proliferation of motivated threat actors, organisations need to be able to provide consumers with greater clarity, security, and freedom over their own data. Organisational mechanisms are essential to provide the protections consumers need [10]. We can help by providing a full assessment, roadmap, and implementation service to ensure your organisation is doing everything it can to protect consumers' data, and become an industry leader in data privacy.

III. Executive Summary

We consider that Privacy Practice (PP) is a limited company which provides bespoke General Data Protection Regulation (GDPR) consultancy and training services to small and medium sized enterprises (SMEs).

The key objective of PP is to help clients achieve and maintain a stable GDPR compliance position. PP has a detailed understanding of data protection legislation and the consultants are able to translate complex legal requirements into digestible actions. It provides quality services and advice to the clients, building trust and confidence to unlock the value of data.

PP provides services across all industries. The consultants have specialised knowledge and expertise in the Healthcare and Life Science industries which will be the initial target market. The target audience to sell the services to are senior management in risk/compliance positions with budget to invest in consultancy services.

The business provides services to SMEs in the UK. The business need is justified by available quantitative and qualitative research. The development of this business plan has critically considered the relevant factors and regulatory environment to enhance the business idea and ensure maximum benefit for the clients.

The short-medium term objectives are to:

- Establish the company in the market and take on at least 5 clients in the first year of business.
- Increase the online presence by increasing website traffic by 50% before the end of the first year.

The long-term objective is to become the go-to privacy consultancy for SMEs. Privacy is a fast-paced, evolving topic, and we will be at the forefront of regulatory and market changes. Offerings will be tailored to the ever-changing privacy landscape to ensure that our services are relevant and desirable.

A. The Business

The GDPR came into force in May 2018. Although the regulation has been in place for almost three years, maintaining and establishing GDPR compliance remains a key challenge for organisations that process personal data of EU citizens.

PP provides bespoke GDPR consultancy and training services to support UK SMEs with privacy and GDPR compliance. SMEs do not have the same resources or in-house capabilities as larger enterprises, therefore, they rely more heavily on external support from consultants.

Market research by [5] noted that the demand for GDPR services is anticipated to increase significantly. There are a number of drivers for this increased demand, including:

- *Privacy regulation and enforcement:* A key driver for GDPR services remains compliance with GDPR and UK Data Protection Act (DPA) 2018. With increased fines from regulators, there will be increased awareness from organisations on the need to comply.
- *Significant incease of breach notifications:* [7] notes that for the period from 28 January 2020 to 27 January 2021, there were, on average, 331 breach notifications per day (a 19% increase on the previous year's daily average).
- *Increasingly digital world:* As noted by [6], organisations are becoming increasingly digital which means that the need for cyber and data security is at an all-time high.
- *Demand for transparency and trust from consumers:* Organisations that fail to protect data risk losing the trust of their customers. [2] found that over 50% of consumers would switch companies because of their data policies or data sharing practices.

PP will be set up as a limited company with one Director. Moreover, four additional consultants will be hired on 12-month contracts. The number of consultants beyond this will be determined as certainty of revenue stream becomes clearer.

IV. Services for Customers

PP will offer a catalogue of GDPR services to help organisations improve their GDPR compliance position. The following services will be offered:

- *Data Protection Impact Assessments (DPIA)* - PP will help to embed a privacy by design culture and DPIA

979-8-3503-7064-7/24/$31.00 ©2024 IEEE
Authorized licensed use limited to: De Montfort University. Downloaded on March 05,2025 at 10:29:37 UTC from IEEE Xplore. Restrictions apply.

process into organisations. It also undertake DPIA's to identify key privacy risks in new and existing data processing. The assessment will use a mix of document reviews, stakeholder interviews, and physical visits and inspections where necessary.
Benefit: Ensure compliance with Privacy by Design obligations of the GDPR.

- *GDPR Gap Analysis* – This involves mapping of an organisation's existing state against the proven GDPR compliance framework. The company will undertake a high-level analysis of an organisation's existing material to assess their privacy compliance maturity. Risk-based ratings and key recommendations will be provided for every area that is analysed.
  Benefit: Understand current level of GDPR compliance and create a roadmap for target compliance level.
- *GDPR Data Flow Mapping and Inventory* – PP supports organisations with their Article 30 GDPR obligations by documenting their processing activities in line with regulatory requirements.
  Benefit: Comply with Article 30 GDPR requirements.
- *Training, awareness and culture change* – PP offers a range of training packages to increase GDPR knowledge and awareness. This includes provision of "Fundamentals of GDPR" training, which can be delivered as classroom training or e-learning and can be tailored depending on business need. PP also deliver CIPP/E training and run awareness campaigns.
  Benefit: Demonstrate that employees receive appropriate training to better protect personal information and reduce the risk of data breaches.

Offerings are tailored to the ever-changing privacy landscape to ensure that clients receive relevant services that add-value to their business.

V. Marketing Analysis

PP has a particular focus on the healthcare and life sciences industries, because:

- The industries processes large volumes of "special category" personal data, such health data.
- There is interplay between GDPR and Clinical Trials Regulation.
- Development of digital health products is increasing.
- COVID-19 has increased the collection and use of health data.

This is the niche of PP, and organisations come to PP for the specialised knowledge in this area.

Attracting, retaining and growing clients is key. Thus, PP will:

- Target clients from existing professional network, based on 10 years industry experience in privacy and healthcare/life science industries.
- Attend networking events and conferences in the healthcare/life sciences and data privacy fields.
- Develop a company website with a strong brand. Write blogs to publish on the website, demonstrating expertise and driving traffic to the website.
- As the customer base develops, PP will include reviews and testimonials on the website to portray PP as a trusted brand.
- Invest into SEO advertising.
- Use social media to attract future business, including professional networks such as LinkedIn.

VI. Competitive Analysis

Market research by [13] suggests that the demand for GDPR services is set to grow by 24% by 2026. Notably, the SME segment is expected to record higher growth rate during the forecast period compared to the large enterprises.

In 2020, the GDPR services market was valued at $1,183.2 million. This is expected to rise to $4,364 million by 2026, at a Compound Annual Growth Rate of 24.3% over the forecast period 2021 – 2026. Therefore, as the demand for GDPR services is to increase there will become an increasing need for specialist services.

Another key market trend noted by [13] is that the healthcare and life sciences industry is to hold significant market share for a number of reasons, including increased use of Internet of Things ("IoT"). Additionally, Europe remains a region with strong growth as companies continue to comply with requirements of GDPR.

[13] notes that the GDPR services market is relatively fragmented, with many different businesses offering services to support organisations across almost all industries.

Established professional services firms, such as Deloitte, currently provide GDPR consultancy services. However, as industry leaders, these firms are instructed by large, sophisticated clients. By providing more competitive pricing, PP will be more desirable for SMEs.

Two consultancy firms targeting GDPR services to SMEs have been identified and evaluated below:

- *Privacy Helper:* This firm is well established in the market. It has transparent pricing structure, and offering highly competitive rates of £125 per hour + VAT. It offer extensive GDPR services, including gap analysis, training, audit and data breach support. It is advertising as UK's #1 privacy consultancy on their website. "Knowledge hub" on their website provides free guidance to organizations, such as "GDPR checklist for SMEs". However, it does not appear to provide industry specialisation. Quality of service/product may be questioned when looking at the highly competitive hourly rates. Only one office location (Bedford).
- *Evalian:* This firm is also well established in the market. It offers extensive GDPR services, and Cyber security consultancy services, such as ISO reviews and penetration testing. It published reviews from SMEs on their website. Offices in multiple locations. However, pricing are unknown. Working with organizations of all sizes across

Authorized licensed use limited to: De Montfort University. Downloaded on March 05,2025 at 10:29:37 UTC from IEEE Xplore. Restrictions apply.

multiple sections – may not be first choice if industry specialists are required.

Privacy Helper and Evalian are well-established in the market, and therefore have a reputational advantage. However, neither appear to be targeting any particular industry.

PP will target the health care and life sciences industries, and therefore some key wins in this would help to solidify PP's position in the market. PP will market itself as approachable and agile, which is a key differentiator from larger and more established consultancies.

There are three key business risks:

- The client is dissatisfied with the service that has been provided or with the quality of the deliverable, which could lead to the client claiming to have suffered financial loss as a result of the work. Example mitigation: Business insurance, quality review procedures, limited liability cap in contracts, tight wording in contracts.
- Losing or breaking a device that is vital to completing client work, for example, losing a laptop and all the files on it. Example mitigation: Back-up of all files, saving to the Cloud so files can be accessed using other devices.
- Employing too many consultants leading to under-utilisation and financial losses. Example mitigation: Employ consultants on 12-month contracts, monitoring of the pipeline.

VII. Personnel Plan

PP is reliant on attracting strong talent to lead its engagements. Consulting is widely recognised as a "people" business, and PP prides itself on having a strong team of qualified and experienced consultants with strong academic credentials.

PP will monitor the skills of the employees. Where there is a skills gap, PP will close this gap by training existing employees or hiring additional consultants. As a minimum, all employees hold the CIPP/E qualification and PP aims to attract consultants with the culture and career progression opportunities. Table I shows the employees in the PP.

VIII. Financial Plan

The start-up costs for PP have been estimated below. As the company will first operate remotely, there are no costs for rent or overheads. Table II is the list of startup expenses.

Finance manager will develop a comprehensive financial plan and detailed forecasts, cash flows and Profit and Loss projections. Table III is the summary statement.

PP will work with the clients to provide flexibility when it comes to pricing, offering time-based and fixed fee arrangements. The services are priced competitively and take into account the size and duration of the contract. Table IV shows the hourly rates which are used for provision of services.

Sales forecast: PP has estimated its sales forecast based on the charge-ability of its consultants. This has taken into account market fluctuations, quiet periods, and that consultants will not be 100% utilised. In a best-case scenario, consultants will charge 75% of their time to clients, and in a worst-case scenario, they will charge 25% of their time.

If 75% chargeable, the total monthly sales is £84,000, and the total annual sales is £1,008,000. See table V for more details.

If 25% chargeable, the total monthly sales is £28,000, and the total annual sales is £336,000. See table VI for more details.

IX. Legal and Ethics

PP complies with all legal obligations including:

- Registering with Companies House, HMRC, VAT.
- Companies Act 2006.
- Purchasing insurance policies, such as Employer's Liability Insurance.
- Filing a corporation tax return each year.
- Employment laws.
- Health and Safety laws.
- Data protection laws.

PP will hire an accountant to help with financial obligations, including annual filing of accounts and running of payroll. A solicitor will be engaged to support with legal obligations and to draft boiler plate contracts.

Professional indemnity insurance has been obtained to protect individuals in case a claim is made in relation to the advice PP has provided.

PP has developed internal documents including a company handbook, policies and procedures to guide our employees and instil confidence in the internal practices.

PP recognises that its reputation and success rests on the personal ethics of its employees. PP has a documented Code of Conduct which outlines our shared values and ethical principles. Additionally, PP is committed to making an impact in society by looking to provide pro-bono services to non-profit organisations in the longer term.

X. Conclusion

In this study, we developed a business plan for data security and privacy businesses. Technical and non-technical risks and related contingency plans were addressed through consideration of risk management and secure system architecture. Moreover, the market and the competitors were analysed. Personal plan and financial plan are provided. In addition, related legal and ethical obligations are considered.

References

[1] Venky Anant, Lisa Donchak, James Kaplan, and Henning Soller. The consumer-data opportunity and the privacy imperative. *New York: McKinsey and Company*, 2020.

[2] Cisco. Consumer privacy survey: The growing imperative of getting data privacy right. https://iapp.org/media/pdf/resource_center/cisco_consumer_privacy_survey_nov2019.pdf. Accessed: 2021-04-29.

[3] Compliance. Cybersecurity business plan. https://www.complianceforge.com/product/cybersecurity-business-plan/, note = Accessed: 2021-10-29.

[4] CyberASAP. Expert support to commercialise academic cyber security innovation. https://ktn-uk.org/programme/cyberasap/, note = Accessed: 2021-10-29.

[5] DataBridge. GDPR services market – global industry trends and forecast to 2027. https://www.databridgemarketresearch.com/reports/global-gdpr-services-market. Accessed: 2021-05-01.

979-8-3503-7064-7/24/$31.00 ©2024 IEEE Montfort University. Downloaded on March 05,2025 at 10:29:37 UTC from IEEE Xplore. Restrictions apply.

TABLE I
EMPLOYEES IN THE LIMITED COMPANY.

Employees	Number of employees	Contract	Salary
Consultant	2	12 months	£35,000
Senior Consultant	2	12 months	£42,000
Accountant	1	Monthly	£39.5 per month
Solicitor	Contracted as required	N/A	£N/A

TABLE II
STARTUP EXPENSES

Capital equipment list	Amount
Furniture	£0
IT equipment	£15,000
IT Software	£500
Stationery and office supplies	£200
Mobile phones	£1,000
Total	£16,700

Location and admin expenses	Amount
Rental	£0
Legal and accounting fees	£5,000
Prepaid insurance	£1,000
pre-opening salaries	£154,000
Total	£160,000

Advertising and promotional expenses	Amount
Advertising	£5,000
Travel/entertainment	£1,000
Other/additional categories	£0
Total	£6,000

Other expenses	Amount
Registering the business	£12
Trademarks/designs/patents	£5,000
Total	£5,012

TABLE III
SUMMARY STATEMENT

Source of capital	Totals
Owners' and other investments	£100,000
Bank loans	£300,000
Other loans	£0
Total	£400,000

Startup expenses	Totals
Building/real estate	£0
Leasehold improvements	£0
Capital equipment	£16,700
Location/administration expenses	£160,000
Opening inventory	£0
Advertising/promotional expenses	£6,000
Other expenses	£5,012
Contingency fund	£0
Working capital	£0
Total	£187,712

TABLE IV
HOURLY RATES

Role	Hourly rate (excluding VAT)
Consultant	£75
Senior consultant	£125
Director	£300

979-8-3503-7064-7/24/$31.00 ©2024 IEEE

Authorized licensed use limited to: De Montfort University. Downloaded on March 05,2025 at 10:29:37 UTC from IEEE Xplore. Restrictions apply.

TABLE V
SALES AND COST OF THE COMPANY.

Role	Hourly rate (excluding VAT)	Sales per week	Sales per month	Number of employees	Total cost per month
Consultant	£75	£2,250	£9,000	2	£18,000
Senior Consultant	£125	£3,750	£15,000	2	£30,000
Director	£300	£9,000	£36,000	1	£36,000

TABLE VI
SALES AND COST OF THE COMPANY.

Role	Hourly rate (excluding VAT)	Cost per week	Cost per month	Number of employees	Total cost per month
Consultant	£75	£750	£3,000	2	£6,000
Senior Consultant	£125	£1,250	£5,000	2	£10,000
Director	£300	£3,000	£12,000	1	£12,000

[6] Deloitte. Future of cyber. https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Risk/deloitte-IE-risk-future-of-cyber-v8.pdf . Accessed: 2021-04-29.

[7] DLAPiper. DLA piper gdpr fines and data breach survey. https://sweden.dlapiper.com/sites/default/files/node/field$_download/Data\%20Breach\%20Report\%202021.pdf. Accessed$: 2021−05−01.

[8] Shannon Flynn. Building a cybersecurity plan for a small business. https://www.score.org/blog/building-cybersecurity-plan-small-business, note = Accessed: 2021-10-29.

[9] GOV.UK. Cyber security academic startup accelerator programme year 5. https://apply-for-innovation-funding.service.gov.uk/competition/824/overview, note = Accessed: 2021-10-29.

[10] Stewart Hayes, Malcolm Shore, and Miles Jakeman. The changing face of cybersecurity. *ISACA Journal*, 6, 2012.

[11] Joseph Johnson. $u.s.$ data breaches and exposed records 2020. https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/, note = Accessed: 2021-04-29.

[12] Lennart Maschmeyer. A tale of two cybers - how threat reporting by cybersecurity firms systematically underrepresents threats to civil society. *Journal of Information Technology & Politics*, pages 1–20, 2021.

[13] MordorIntelligence. Gdpr services market – growth, trends, covid-19 impact, and forecasts. mordorintelligence.com. Accessed: 2021-04-29.

[14] Nathan Newman. The costs of lost privacy: Consumer harm and rising economic inequality in the age of google. *William Mitchell Law Review*, 2014.

[15] OGScaptial. Cyber security business plan sample. https://www.ogscapital.com/article/cyber-security-business-plan/, note = Accessed: 2021-10-29.

[16] John Palmer. The differences between a business plan & business model. https://smallbusiness.chron.com/differences-between-business-plan-business-model-4744.html, note = Accessed: 2021-10-29.

[17] Paul M. Schwartz. Global data privacy: The eu way. *94 New York University Law Review 771*, 2019.

[18] Ben Shabat. How to build a small business cyber security strategy. https://www.become.co/blog/small-business-cyber-security-plan/, note = Accessed: 2021-10-29.

[19] Upmetrics. Cyber security business plan. https://upmetrics.co/template/cyber-security-business-plan-example, note = Accessed: 2021-10-29.

[20] WorldEconomicForum. The global risks report. geneva. *World Economic Forum*, 2019.

[21] WorldEconomicForum. Cost of a breach report. *New York: IBM*, 2020.

979-8-3503-7064-7/24/$31.00 ©2024 IEEE Montfort University. Downloaded on March 05,2025 at 10:29:37 UTC from IEEE Xplore. Restrictions apply.