CryptClip

Here we present the business plan for our product, a cryptographic device we named *CryptClip*. We first introduce the market opportunity, explaining how our business will take advantage of it. We then describe concisely and precisely the company information, the market potential and target customers, and the financial phasing of the business.

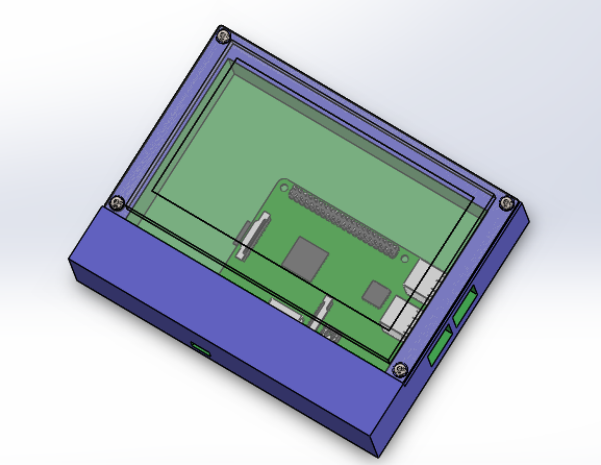


Figure 1: *Current CAD of the* CryptClip*, where LED screen is transparent. Empty areas shall be filled with battery pack.*

1 The need: A problem in security...

Privacy and data protection are fundamental issues for individuals, companies, and public institutions. However, the vast majority of available solutions to these problems are software-based, meaning that they rely on encryption techniques run by software installed on the devices used to exchange data. To cite a recent example, this week WhatsApp introduced end-to-end encryption on all the communications performed through its application (see **Table 1** for an analysis of the current competitive landscape). However this provides security only on the assumption of non-compromised devices. For example, they assume the absence of malware, operating system backdoors, and no user errors. In this sense, it is astonishing that today employees remain the most cited source of information-security compromise for companies [PWC], often as a consequence of vulnerabilities such as phishing. This issue is also captured by a survey we conducted showing that over 50 percent of the public are concerned about security both at work and home - this being an issue of acute importance when the same devices are used both in work and leisure.

2 ... and a *Solution*

We present a paradigm shift to the problem of data security, by **moving the core of the cryptographic power from the software to the hardware**. Such a solution allows for perfectly secure data transmission with immunity to all known attacks. This is achieved by introducing a separate cryptographic device used as a mobile phone or computer accessory, *CryptClip*. The device is user-friendly, it could for example replace the widely used mobile phone case, or it could be implemented on a power bank hence avoiding the obstacle of its portability.

The beauty of our product, *CryptClip*, lies in its ability to provide a simple security solution to all users of modern communication devices. The strategic vision of our security approach amounts to stopping personal communication devices, such as smart phones, from receiving any plain text (secret message) or encryption keys. *Instead*, and here comes the paradigm shift, the encryption (and decryption) of the secret messages happens inside CryptClip. In this way the communication device will always receive only securely encrypted information, such that an eavesdropper on the line, or an agent with backdoor access cannot expose your confidential information content.

3 Prototype V0.1

We have begun development of the first prototype. This combines a touchscreen LED display, and an

Figure 2: *Front/Back of current* CryptClip *prototype, not including battery.*

Competitive Landscape					
Company Name	**Product Type**	**Key Security Features**	**Security Rating**	**Price**	**Usability**
Telegram	Instant messenger	Optional end-to-end encrypted messaging with self-destruct timers	Low	Free	High
WhatsApp	Instant messenger	end-to-end encrypted	Low	Free	High
BlackBerry	Smart phones	Option of a secure workspace	High	Around US$600	Moderate
SpiderOak	Online backup and file hosting service	encrypted cloud storage and client-side encryption key creation	Moderate	Free	High
Crypt-Clip	Encryption device	Encrypted communication with secret key distribution	High	Around US$100	High

Table 1: *When looking at sales to the general public our main competitors would be* ***Telegram Messenger****,* ***WhatsApp****, and similar secure messaging apps based on 256-bit symmetric AES encryption, RSA 2048 encryption and DiffieHellman key exchange. [telecry]. These do not provide thorough security solutions and are susceptible to many attacks.*

off-the-shelf microcomputer to preform one-time-pad encryption on arbitrary files. The item also doubles as a powerbank when not in use. As the technology allows encryption of arbitrary data, encrypting live audio/video will not be a substantial challenge. We also implement Wegman-Carter authentication which ensures all messages are tamper-proof. Together with a one-time-pad, we achieve robust security. We intend to further add to the security of the devices by utilising the anonymous broadcasting techniques [AnomCom], which allow us to completely hide the identity of the message sender. Key distribution is currently achieved via a local share (physical contact of devices) - however implementation of a key distribution method is in process. No servers are used to transfer data, and no additional hardware is required except for the *CryptClip* and the user's phone/computer.

4 Financials

Current barriers for market entry facing *CryptClip* are the initial production of the device, preliminary funding for prototyping, and a sales strategy to enter the market with *foot-in-the-door* contacts. See **Figure 3** for details of company phasing.

4.1 Pricing

From the prototyping work to date we estimate costs at S$30 per unit. This leads to an initial sale price of $S\$60-100$ per unit. Survey results show a quarter of public would be initially prepared to pay over S$50. Although contract sales will require negotiation, we will aim for a pricing equivalent of S$80 per unit with the allowance of device support and exclusivity. This emphasises a need for a directed sales to a specific market.

4.2 Break-even point

Assuming a retail model, wherein devices are sold at S$80 per unit, with manufacturing cost at S$30, the total profit is S$50 per device. To achieve this the company will have at this point received approximately $S\$80,000$ funding. We would thus require an immediate sale of 1600 devices to break even. Alternately, to break even over the course of one year from product launch, we would require sales of 13,600 devices (this covers a burn rate at $S\$50,000$ pcm which equates to sale of just over 1100 devices per month).

From market research, we estimate potential sales of over 45,000 units in Singapore alone (10 percent of all members in finance, IT sector and healthcare). With value capture of just over 30 percent of the Singapore market alone we would achieve break-even. We estimate global potential for *CryptClip* at approximately 9mil units (again assuming 10 % of workers in Finance, I.T and healthcare require them), implying a revenue stream of $450mil.

5 Minimum viable business product

We strongly believe in the lean startup model of entrepreneurship, and wish to release a minimal viable

Potential Markets				
Market	**Example Market Size**	**Willingness/Need**	**Considerations**	**Priority**
Banking/Finance	• 4m (EU & US top 20) • 200k (Singapore)	• Fast adoption • Largest CySec losses • Large budget: $9.5bn/yr (US), up 14% worldwide.	• Large presence in S'pore. • Existing solutions, strong competition.	High
IT / Telecomms	• 3.9m (top 15 IT global) • 1.4m (top 10 Tel. global) • 125k (S'pore)	• Incidents/losses/budgets up 107%/33%/51%. • Respondents would pay S$72 average.	• Large market in S'pore. • Competition with in-house solutions.	Medium
Pharma/Biotech	• 890,000 (top 10 global) • 20k (Singapore)	• Incidents/budgets up 38%/13%. • Slow to address CySec.	• Most top 10 companies have presence in S'pore	Medium
Healthcare	• 500k health insurance companies, over 800k active doctors (US). • 12,000 doctors in S'pore. • 140k (healthcare general) S'pore.	• Slow to spend on CySec. • Losses up 4%, $10bn/yr global budget by 2020. • Respondents would pay S$75 average.	• Growing industry globally; large driver of IT growth. • S'pore is a global industry leader.	High

Table 2: *The following table shows example market size (estimates for selected geographical regions, in number of employees unless stated) and associated considerations for several key industries that are susceptible to being targeted for the theft of sensitive data (financial, personal, IP-related). Unless stated, monetary figures given are in US$, incidents/losses/budget figures refer to information/cyber-security (CySec), quoted increases are 2015 vs. 2014. 'Respondents' refers to those of our survey.*

product as soon as possible. for *CryptClip*. An initial product will only be able to perform the encryption of text (not live audio) and will require users to meet to share encryption keys. This may be initially inconvenient, however, it already overcomes all security issues regarding possible malware and back-doors on a user's phone or computer.

This early release will also allow us to identify any coding errors or prominent user issues. Due to decreased functionality, this minimal product is expected to retail at a lower price than those mentioned previously.

6 Target Markets

Table 2 summarises our market research and client priorities. We now briefly outline the major potential areas.

6.1 Finance

With regards to the banking industry, the PwC State of Information Security Survey reports that average information security spending is up 14% in the financial services sector, compared to last year [PWC], while the "Banking & Financial Services Cybersecurity: U.S. Market 2015-2020 Report", published by Homeland Security Research Corp., found that in 2015 spending by the industry in the U.S. alone totalled US$9.5bn - the largest non-government cybersecurity market. In Singapore, over 1200 financial institutions - including over 200 banks, 150 insurance entities, and 400 trading firms - have a presence [MAS, Trad], employing over 200,000 people and accounting for over 12% of the national GDP [ChNewsAsia]. Due to the large market, minimal bureaucracy, fast uptake of security tech and large budgets, we intend to make finance and banking a priority target.

6.2 I.P and I.T

Theft of IP and trade secrets by competitors is an increasing concern for companies in the R&D sphere. A 2013 report by The Commission on the Theft of American Intellectual Property concluded that IP theft costs the United States more than US$300bn per year [USIPcommision], while in 2011 a UK Cabinet Office report on the cost of cyber crime estimated that British companies lose £9.2bn (US$13bn) yearly for the same reason [UKcyber]. With respect to Singapore, a report prepared by the Center for Strategic and International Studies concluded that cyber

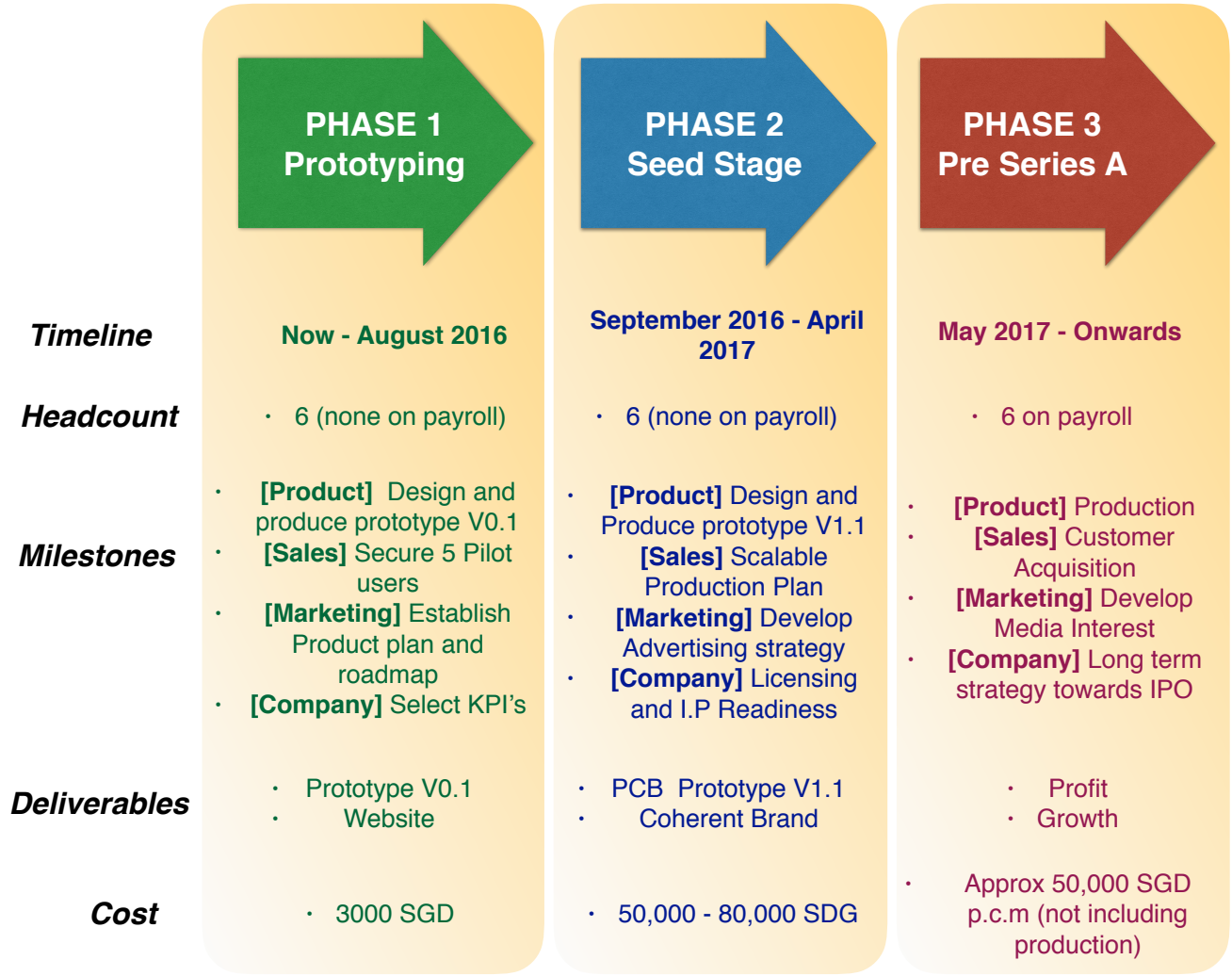


Figure 3: *Phasing of the company.*

crime in general costs the country S$1.25bn annually [SingaporeCyber]. A major industry in which IP security is an acute concern is pharmaceuticals and biotechnology sector.

6.3 Healthcare

Doctor-patient confidentiality is a key principle, backed up by law, in the healthcare industry. An increasing proportion of the interaction between patient and medical professional now takes place remotely, including appointments and diagnoses. Doctors and specialists may also confer with one another remotely, over unsecured communications channels. Healthcare payers and providers have increased their information security budgets by 79% over the past two years [PWC]. We therefore believe that there is significant potential for growth in data-sharing practices in this industry.

6.4 Government and Military

Secure communication is also paramount within the realms of government, police, military, and other state bodies. However, the time required to achieve a sale in these sectors will be significantly longer than in our primary targets. The uptake of technology that has not been designed in-house, or by existing trusted partners, requires a higher-level authorisation and more bureaucracy. These bodies are also reluctant to use technologies that are openly available on the market, an issue that would likely be particularly acute with the military. For these reasons, the government and military sectors are not currently within our target markets.

7 Sales process for acquiring a customer

We have several means of establishing awareness of *CryptClip* in our target markets: directly contacting managers (HR, department, branch) directly by phone/email/walk-ins; attending conferences, workshops, fairs and showcase events relevant to the target industries; participation in social/networking events attended by people from the target industries (e.g. meetup.com groups); participation in industry competitions (e.g. Accenture); leveraging the support of our institutions (SUTD, NUS) to connect with potential customers; using our own personal contacts, and those of our VC mentor. An advertising strategy will be prepared in future company phasing.

8 Use of proceeds

8.1 Website

A website will be the next requirement of the project, to easily promote *CryptClip*. This should include links to documents from the 10K, team description, and links to any news articles regarding the company. The website can be (mostly) made in house however-it may be beneficial to purchase a pre-made template, which then be altered cheaply. Ongoing costs for hosting may also be required. Business cards will also be required.

8.2 Accenture competition

Beginning in July, Singapore Accenture is beginning a competition to complete a finance related device. The invitation expressly encourages entries with providing security for mobiles. It may be ideal for us to enter as almost all documents for initial entry have already been prepared. Funds from the 10K would then be used to finance any expenditures involved with initial entrance .

8.3 Prototyping costs

This will encompass the remainder of expenses to complete designs of the device in phase 1 costs - mostly PCB design with a small fraction on improving casing for the current prototype for use in Accenture entry. The expect cost for completing this will exceed the total presented here and we will require further funding to complete this stage.

9 Team information and background

Our team are passionate about cryptography with relevant expertise in the fields of physics, cryptography (both classical and quantum), computing, and electronics.

Joshua Kettlewell - Ph.D. candidate, SUTD

Team lead. Responsible for accounting and purchasing, construction (both hardware and software) of a prototype, liaising with competition organisers. Master of Physics, University of Sheffield.

Dr. Tommaso Demarie - Post-doctoral research fellow, SUTD

Responsible for development of theory for the device and liaising with investors and venture capitalists. PhD in Quantum Information, Macquarie University.

Ewan Munro - Ph.D. candidate, NUS

Responsible for software and hardware development and device integration. MSc in Mathematical Physics, University of Edinburgh.

Ada Altybayeva - Undergraduate student, SUTDAda Altybayeva - Undergraduate student, SUTD

Development of aesthetic and ergonomic prototyping aswell as overseeing electronics of the device.

Zhikuan Zhao - Ph.D. candidate, SUTD

Research on commercial cryptographic techniques, and efficient implementation of key distribution. Master of Physics, University of Oxford.

Wei Pan - Ph.D. candidate, SUTD

Development of the code for the device. Bachelor of Engineering, University of Zhejiang.

CryptClip: March/April 2016 survey results

The goal of the survey was to acquire data to shape our market strategy.
Here we summarise the key findings from the data we collected.

Infographic:

93 *Respondents*

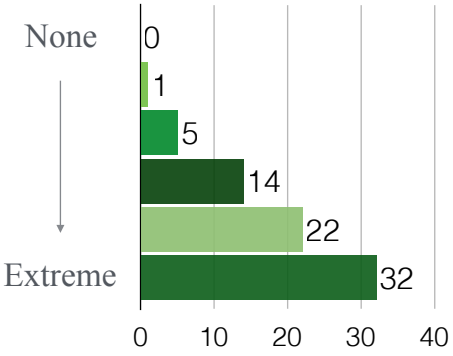
Main age group:
26 - 35 (60%)

Mostly
not students (90%)

Industries most represented

- IT industry (20%)
- Research and development (20%)
- Media and Arts (13%)

Level of distress if personal data were compromised
(74 responses)



Most important kind of information to exchange securely
(69 responses)

Email, instant messages

62%

PDF, word documents

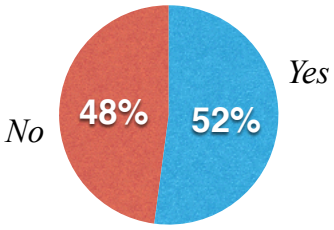
16%

Key questions:

Do you believe *secure communication* is an issue for either your work life and/or personal life? (93 responses)

- Both personal and work life (45%)
- Personal life only (20%)
- Work Life only (10%)
- I do not believe it is an issue (25%)

Do you use software of physical devices to protect the privacy of your communication? (71 responses)



How much are you willing to pay for a device like CryptClip that can keep your communications (calls, messages, file sharing, etc.) secure (72 responses):

- More than 50$ (25%)
- Between 20$ and 50$ (30%)
- Less than 20$ (30%)
- Would not buy it (15%)

References

[QCrypt] N. Gisin et al., *Quantum cryptography*, Rev. Mod. Phys. 74, 1, 2002.

[AppCrypt] B. Schneier, *Applied Cryptography: Protocols, Algorithms*, John Wiley & Sons, Inc. 1993

[AppleFBI] http://www.bbc.com/news/technology-35601035 *Apple v the FBI - a plain English guide*

[TelBR] http://www.bloomberg.com/news/articles/2016-02-23/telegram-surpasses-100 -million-users-backs-apple-on-encryption

[telecry] "FAQ for the Technically Inclined" Telegram. Retrieved 9 January 2016.

[wikiblackphone] https://en.wikipedia.org/wiki/Blackphone

[TelOpt] http://www.wired.co.uk/podcast/episode-256 Telegram's Pavel Durov: Podcast 256

[WAOpt] http://www.wired.co.uk/podcast/episode-162 Behind the scenes of WhatsApp: Podcast 162

[QuesLink] http://goo.gl/forms/gbspejiKUA Security device feedback

[PWC] http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html

[IDC] https://ncmedia.azureedge.net/ncmedia/2016/04/IDCNUSFinalResearch.pdf

[JPMorganNYtimes] http://dealbook.nytimes.com/2014/12/22/entry-point-of-jpmorgan-data-breach-is-identified

[JPMorganForbes] http://www.forbes.com/sites/stevemorgan/2016/01/30/why-j-p-morgan-chase-co-is-spending-a-half-billion-dollars-on-cybersecurity/

[JPMorganIBtimes] http://www.ibtimes.com/jp-morgan-chase-cyberattack-more-80-million-accounts-compromised-says-new-report-bank-1698834

[MAS] http://www.mas.gov.sg/

[Trad] http://www.iesingapore.gov.sg/

[ChNewsAsia] http://www.channelnewsasia.com/news/business/bank-jobs-in-singapore/

[USIPcommision] http://www.ipcommission.org/report/

[UKcyber] https://www.gov.uk/government/uploads/system/uploads/attachment/data/file/60943/the-cost-of-cyber-crime-full-report.pdf

[SingaporeCyber] http://csis.org/files/attachments/140609/rp/economic/impact/cybercrime/report.pdf

[Factsheet] https://www.ipos.gov.sg/IPforYou/ IP-forBusinesses/IPFactsheets.aspx

[DocSg] https://www.moh.gov.sg/

[lawSg] http://www.lawsociety.org.sg/

[AnomCom] Anonymous Broadcasting D. Chaum J. Cryptology1 1988