

https://dspace.org/

A distributor of security and home automation devices that use the internet of things

Mutinelli, Ingo

2018
https://hdl.handle.net/10539/31123

Downloaded from a DSpace repository. https://dspace.org/

A Distributor of Security and Home Automation Devices that use the Internet of Things

Ingo Mutinelli

712576

A Business Venture Proposal submitted to the Faculty of Commerce, Law and Management, University of the Witwatersrand, in partial fulfilment of the requirements for the degree of Master of Business Administration

Johannesburg, [2018]

DECLARATION

I, Ingo Arnold Mutinelli, declare that this Business Venture Proposal is my own work, except as indicated in the references and acknowledgements. It is submitted in partial fulfilment of the requirements for the degree of Master of Business Administration in the Graduate School of Business Administration, University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination in this or any other university.

(Ingo Arnold Mutinelli)

Signed at ……

On the …….. day of …… 20…..

ACKNOWLEDGEMENTS

I would like to thank the following people: My wife Natalie who put no pressure on me and assisted where she could throughout the process of completing this work – not to mention the not so insignificant task of handling our two boys and going through the lonely nights while I worked. I also need to thank Jurgen Gnoinski for his guidance as my supervisor, Anthony Stacey for his pearls of wisdom and commitment to us MBAs by offering up his time for boot camp. Lastly, all my colleagues at Elvey Security Technologies, especially my previous CEO Jack Edery, for allowing me to subject myself to the MBA programme, and my current CEO Gary Lowe, who not only added to this work by going through my interview process but also showed patience during this MBA when the business could have used my undivided attention rather than sharing it.

I also thank all the companies that responded to my surveys and questionnaires as well as those individuals that I interviewed to get the information necessary to substantiate my Business Venture Proposal.

I will always appreciate the effort and trust Elvey Security Technologies has shown me in allowing me to access company data and to use it in the compilation of this body of work.

This document was edited by Kathryn C. Sole (PhD) of Kathryn C. Sole Consulting, Johannesburg.

SUPPLEMENTARY INFORMATION

Supervisor:	Jurgen Gnoinski
Word count †:	13 876
Supplementary files:	Interview Questionnaire
	Survey Questions
	Recurring Revenue Contract
	IoT Storey Board
	Income Statement
	Detailed Marketing Budget
	Installation cost research

† Including Executive Summary, References, and Appendices.

Table of Contents

DECLARATION ii

ACKNOWLEDGEMENTS iii

SUPPLEMENTARY INFORMATION iv

EXECUTIVE SUMMARY .....

1. Business Problem 1

1.1. ENVIRONMENTAL ANALYSIS 1

1.2. PROBLEM ANALYSIS 2

2 Business Opportunity 8

2.1 DATA COLLECTION 9

2.1.1 SURVEY OF SECURITY COMPANIES AND INDEPENDENT INSTALLERS 10

2.1.2 ONE-ON-ONE INTERVIEWS WITH DISTRIBUTORS 12

2.1.3 NEW AND EXISTING HOMES 14

2.1.4 ALARMS BEING MONITORED IN SOUTH AFRICA 14

2.1.5 INTERNET OF THINGS RETAIL SOLUTIONS 15

2.2 MARKET RESEARCH 16

2.2.1 POTENTIAL MONTHLY RECURRING AND ONCE-OFF INCOME 16

2.3 DIFFERENT BUSINESS MODELS 17

3 Business Venture Options 0

3.1 ASSUMPTIONS 0

3.2 OPTION 1: RECURRING REVENUE SHARE – EXISTING CUSTOMERS 0

3.2.1 DESCRIPTION 0

3.2.2 MONTHLY SUBSCRIPTION TO SECURITY COMPANY OR INDEPENDENT INSTALLER 1

3.2.3 BASIC PACKAGE PRICING 2

3.2.4 PROBLEM STATEMENT 3

3.2.5 SOLUTION 3

3.2.6 TARGET MARKET 3

3.2.7 OFFERING 4

3.2.8 EXAMPLE OF BUSINESS CASE 4

3.2.9 RELATIONSHIPS BETWEEN ELVEY SECURITY TECHNOLOGIES, DSC, AND SECURENET 4

3.2.10 CUSTOMER JOURNEY 5

3.2.11 BENEFITS, GOALS, AND MEASUREMENT CRITERIA 5

3.2.12 COSTS AND FUNDING PLAN 7

3.2.13 BREAK-EVEN ANALYSIS 9

3.2.14 RISKS AND ISSUES 10

3.3 OPTION 2: DIRECT MODEL – INSURERS AND TELECOMMUNICATIONS COMPANIES 13

3.3.1 DESCRIPTION 13

3.3.2 BENEFITS 14
3.3.3 BASIC PACKAGE PRICING 14
3.3.4 RISKS AND ISSUES 16
3.4 RECOMMENDED OPTION 17

4 Implementation Approach 18

4.1 BUSINESS STRUCTURE 18
4.2 BUSINESS PLANNING AND EXECUTION 18

5 Conclusion 20

Appendices 21

References and Sources 22

EXECUTIVE SUMMARY

Integration, Intelligence, and the Internet of Things within the Security Industry. This is a Business Venture Proposal for a bolt-on business to Elvey Security Technologies, an existing company distributing security products to installers of such products. Context is provided explaining the company, where and how it operates, and the industry within which it currently operates. A link between Elvey Security Technologies and the new Business Venture offers synergies and opportunities that will benefit the new entity in the short term and the business as a whole in the long term.

An analysis of technology in the security industry, as well as the relatively new Internet of Things (IoT) technology and devices, is provided. The Proposal refers predominantly to the residential market (not commercial/industrial companies and businesses) because this is the key target market for the new business. The current status of the security industry is discussed and how the IoT is shaping its current and future prospects. The end-user of the technology is analysed as the driver to making the technology and related services necessary and of a potentially lucrative industry.

Studies and market research performed by large corporations and consultancies are offered as support for the Business Venture. Trends and spend on IoT devices and services are briefly introduced to underpin the opportunity. Interviews and surveys are conducted with other distributors and customers (installers of security systems) within the security industry. Market research on related IoT in the retail sector also presented.

Market analysis from a segmentation of the prospective customer base and route to market, as well as from active competitors, is given. The value proposition is evaluated in relation to proposed cost structure, recurring revenue streams, and resource requirements to prove sustainability of the business and how it will evolve within this fast-paced environment. Future plans for later sustainability of the Business Venture are also presented.

Business models employed by distributors and suppliers of technology are challenged by the current problems being experienced and changes that have been introduced within the security technology industry. New ways of creating revenue streams through the use of IoT are introduced. These proposed new revenue streams are a departure from the conventional business model and are accompanied by market research and case studies in which these

models work well and have been successful. The associated risks and their required mitigation actions are described.

The need for not only the technology and applications, but also the back-end services that will be provided by the business, is demonstrated. Discussion is presented on how these needs are currently met and, more importantly, how they are not being met and plans to address the deficiencies. A live case study is provided to articulate the Business Venture in action.

Keywords: i**ntegration, intelligence, Internet of Things, security industry, bolt-on business, residential, end-user, technology, distributor, installer, recurring revenue, sustainability, application, back-end service**

1. Business Problem

1.1. Environmental Analysis

The technologies sold into the commercial, industrial, and residential markets to secure people and property fall into four main categories: Surveillance (closed-circuit television (CCTV)), Intrusion (alarms), Access Control, and Fire (detection and suppression). The evolution of these products over the last two decades has moved from stand-alone analogue technologies towards a space where integration and interoperability between categories, digital, intellectual property (IP), open platforms, and, more recently, the Internet of Things (IoT) have changed the landscape. As customer needs and knowledge of technology have evolved and improved, so has the supporting infrastructure, in terms of fibre-to-the-home and GSM (Global System for Mobile Communications, originally Groupe Spécial Mobile) networks that are able to deliver data services, which, as little as five years ago, were out of reach to middle-class consumers.

For companies selling and installing security technologies, this change has come quickly as the technology has evolved. These companies have had to keep abreast of international trends and, more importantly, be in a position to address the growing market of those consumers who are using it in other forms, such as smart phone and tablet applications, home entertainment, and home automation. With the traditional home alarm, a customer had to arm or disarm from a key pad at their front door and any problems were notified by a telephone call from the associated security company. Today, by using the Internet and linked applications (apps), the end-user knows when there is a problem at their home at the same time as the security company is notified. These technologies have the added features of home-automation devices (such as lights, locks, and gate openers) and viewing cameras to see what is happening in real time. End-users can even reduce energy emissions and costs by controlling geysers and air conditioners through their IoT devices (products like *Google Nest*). Improved and more technology and services for an ever-increasing consumer base means greater possible revenue for companies involved in this industry.

Today's users have become more technologically sophisticated ("tech savvy") and, as technology advances are made, so too do users become more informed because information is more readily available. The days are past when technology was beyond the comprehension of the user and the seller was able to push products onto an uninformed user. The information

age and the Internet have changed the ways in which the consumer consumes information and, more importantly, the speed at which this information is consumed.

Many manufacturers of complex security systems (such as Bosch www.boschsecurity.com , BIS Surveillance and Kedakom en.kedacom.com) have designed their technology and operating systems so that they work optimally only when used in conjunction with their own devices. For instance, if a client were to procure a Bosch IP (Internet protocol) camera and use it with a Bosch NVR (network video recorder), they would be able to use the functions (video analytics) built into the camera, such as detection and counting of loitering, directional flow of traffic, or people. These features and seamless operation between devices are extremely stable and powerful to the end-user. However, using a camera from a different manufacturer on a Bosch NVR would limit some of its features due to missing streams from the camera. Chinese manufacturers like HIK Vision and Dahua Technologies have, however, built and copied technology for many years and, in so doing, have created an environment in which different manufacturers' products work seamlessly with each other, although reliability is still an issue at times. This interoperability and integrated approach is growing across all markets: closed systems, like those of Bosch, whilst still popular, are being caught up and overtaken in the market by systems that offer interoperability and integration.

1.2. Problem Analysis

In light of the above overview of technology evolution in the security industry, an alarm system that is operated by a home or business owner is considered. This is usually activated using a key pad, typically situated at an entrance for easy arming or disarming when arriving or leaving the premises. These alarms are generally grudge purchases, precipitated by an unfortunate event such as a burglary, or a forced purchase from an insurer that dictates that a security system be in place for certain cover to provided. Alarms are stand-alone systems, which, until recently, did not integrate with other technologies. Home automation is usually considered out of reach for most consumers due to the considerable costs that could be added to an alarm system to make it more appealing, such as addition of indoor and outdoor cameras. However, through the new technological world of interoperability and the connected home (Internet and IoT), previously prohibitive costs have become more accessible: remotely activating an alarm on a device of the user's choice through an application is only one of myriad capabilities that are now be readily achieved.

In addition to the technological advances discussed above, there is a significant drive towards self-monitored alarms. Four main reasons are responsible for this trend:

1. Many new homes are being built in complexes or estates, which usually have access security at the entrance, perimeter security (such as electric fencing and cameras), as well as roaming guards, making the environment relatively safe;
2. There is a general mistrust of security companies who regularly have response officers that are involved in the crimes being committed;
3. The cost of monthly services from security companies;
4. The capability for interoperability between solutions (surveillance, alarm, home automation).

Keeping the above points in mind, many alarm security companies no longer have the ability to gain entry to a home in a complex. Other legally limiting factors have also come to the fore for security companies, including health and safety legislation that protects staff, liability claims against damage to property caused by an officer climbing over a boundary wall, and wrongful shootings. Alarm security companies are today hesitant to allow response officers to gain entry to premises on which an alarm has been activated. Many end-users are now questioning the need for an alarm company to monitor their system.

Given the recent more-widespread availability of fibre optic to the home, combined with access to technology advancements in home installations that are readily available on user devices, security self-monitoring becomes a serious value proposition. The larger alarm manufacturers have begun making products outside of their traditional security profile: they offer integrated communication modes, such as GPRS (general packet radio service) (via a SIM (subscriber identity module) card), Ethernet (via IP), and Wifi (wireless local area networking). This means that a user can interact with their system from anywhere in the world, provided that they can access the Internet from a device (telephone, tablet, or computer). Taking it one step further, devices can now be wirelessly added to an alarm system using mesh technologies, such as Zigbee and ZWave. Such devices include light dimmers and switches that can activate items in the home, such as geysers and pool pumps. Water sensors, smoke detectors, temperature sensors, movement sensors, and already-mainstream indoor and outdoor cameras are now easily added to the system, enabling a visual account of an incident or situation (verification) and real-time viewing of the premises and the people in it.

Elvey Security Technologies Security Technologies (Elvey Security Technologies) has been a supplier of security technology (Access Control, CCTV, Fire and Intrusion products) for over seventy years. Its existing business is as a distributor to installers of security solutions to the residential and commercial/industrial sectors. These installers vary from one-man businesses to regional and national security companies and companies that specialize in integrated specialist solutions. Elvey Security Technologies makes its profits through a margin on the various products (in the four verticals listed above) that it sells.

With the introduction and development of the IoT, a recurring business opportunity exists to couple the products that Elvey Security Technologies sells to back-end services that can be offered though applications and remote operations. This opportunity is conceptualised as combining the manufactured hardware (the current product) with developed software (the so-called back-end) that enables the interoperability of many different pieces of hardware onto a single platform driven from a central point, such as a smart phone. This interoperability and back-end cannot exist without the hardware and *vice versa*, but the key component to seamless integration of all the components is the associated data network. The data and commands that travel along these networks give the user the ability to switch devices, monitor alarm systems, receive push notifications, and pro-actively manage risks and energy consumption on a single platform. It is here that a distributor that owns the value chain – that of supplying product to the installer and maintaining this relationship through training, technical support, and warranties on hardware – can begin to share in the recurring-revenue model that back-end solutions offer.

Simply put, the distributor's value proposition is that stock is kept, distributed, and supported around the country. For the specific case of Elvey Security Technologies, this is done through a well-resourced network of branches (20) in South Africa and Sub-Saharan Africa and a customer base of installers (approximately 3000). Trading accounts or terms are provided and long-term relationships are built. These offer the back-end/software developer of interoperable services/applications a vast pre-existing network (and the substantial savings that accrue from not having to develop this capability). In return for this network, the distributor of the hardware supply and support would share revenues.

Recent tough economic conditions have seen end-users trying to bypass the distributor to obtain better pricing and manufacturers entering markets in an effort to directly influence them. This has put the distributor in a precarious situation and resulted in dwindling profits: the power to drive the market is increasing held by a manufacturer that often does not have

the interests of the market or customer at heart. The distributor is currently in a situation in which it is essential to find a part of the value chain that it can control. The IoT, with the associated interoperability of products and their back-end services and applications, is one area of market demand in which the distributor can control the manufacturers' products.

Given the current challenges faced by distributors, the resultant opportunities that arise through this business model-using commercially viable IoT devices, interoperability of disciplines (alarm, home automation, and video), and their integration onto a single user-driven platform—makes this concept extremely attractive. The market landscape of distributors is changing in this industry: pursuing this new business model (back-end services through an application) to run in conjunction with the current model (distribution) offers mutual synergism (sales of the back-end applications are dependent on hardware sales and *vice versa*).

Within the context of this Business Venture Proposal, the challenge is that Elvey Security Technologies is a distributor of hardware (Intrusion, Surveillance, Access Control, and Fire products). Changing the existing business model to include recurring revenue by making available an application that enables back-end services is new territory for the business. To unpack this further, one needs to be cognisant of the fact that offering a product to the market is one thing: the work required to ensure that the product is supported is the most important component of the value chain. Critical success components for a distributor to make a product available that is supplied to installers and used by the general public (home and business owners) include services such as stocking the correct quantity, being able to train customers on correct use of the product, and providing technical support for the product in the market. These are Elvey Security Technologies's core competencies. Elvey Security Technologies does not have experience in linking software, applications, communications, and networks to the product. This Business Venture is therefore proposed as a "bolt-on" to the existing business, but inherently separate with its own specialised human resources.

A second problem to overcome may be the perception by the general market that Elvey Security Technologies's entrance (through the bolt-on business) into the recurring revenue market, by offering self-monitoring services through an application and dedicated network, will be encroaching on their customers' core business. In effect, it may be perceived that Elvey Security Technologies is now openly competing with its own customers. Elvey Security Technologies's customer base buys security equipment, installs it in residential and commercial/industrial premises, and attaches communication devices to monitor these

security installations. Signals from the device triggered by a security event are sent to the control room of the security company, which responds by sending out armed response services and alerting the owner or designated key holder. A monthly fee is charged for this service; this is the core of the security provider's revenue generation. This recurring revenue is at risk as end-users increasingly prefer self-monitoring systems. With Elvey Security Technologies changing the flow of this recurring revenue stream from the monitoring company to itself, the perception in the market place will be that Elvey Security Technologies is competing with their customers. The result may be a boycott of Elvey Security Technologies products (which are the core of the Elvey Security Technologies business). For example, Elvey Security Technologies have 8 x (Texecom, ADI, IDS, Regal, Sensor, Reditron, Gallagher, Pinsec) multi branch national distributors of security products as competitors that customers can go to that offer similar products. The key to addressing this risk is a revenue-share component with the installer to ensure that the installer also obtains value in offering this solution to a market that wants to self-monitor.

The various drivers of change are indicated in the matrix shown in Table 1. Other key driving forces include:

- Disruptive innovation with respect to both products and competitor business models: products will become commoditised, whereas the services and apps behind them will become the factor that cements the customer relationship;
- Changes in the long-term growth rate of the industry, which is dependent on the local, regional, and global economies;
- Emerging new Internet capabilities and applications, i.e., IoT technologies;
- Changes in who buys a product and how they use it, i.e., changes in traditional channels as the end-user buys directly from the manufacturer;
- Diffusion of technical knowledge across firms and countries, resulting in increased competition between manufacturers;
- Changing attitudes, lifestyles, and societal concerns that are associated with technologically sophisticated end-users;
- Advances in technology, including examples in which alarms become less attractive as do-it-yourself (DIY) application-based products grow;
- Changes in social and demographic patterns, such as questioning the need to purchase an alarm when living in a high-security complex.

Table 1. Drivers of changes in distributorship in the security industry.

Key driver for change	**Trends affecting the industry now**	**Trends affecting the industry in about five years**	**Industry success factors at present and in the future**
1 Technology advances	**1** The Internet of Things	**1** This will continue to evolve at a fast pace that cannot be forecast or predicted	**1** Current – not fully understood Future – product cannot be sold without a service component
2 Tech-savvy end-users	**2** Customers want more than just security	**2** Connected devices will become standard.	**2** Current – customers know what they want Future – customers will demand what they can get
3 Exclusivity under threat	**3** Competitors are gaining access to exclusive brands	**3** Manufacturers will continue to search for wider market penetration	**3** Current – focused distribution Future – commoditisation of products with an emphasis on supporting services (apps)
4 Route to market changes	**4** Competitors are innovating in how they access the customer	**4** On-line ordering supplemented by pin-point deliveries	**4** Current – national supply chain Future – Speed and availability of product above all; remote access of services
5 Economic pressures	**5** Price pressures are making value-add distribution more difficult to justify	**5** High-end, high-margin products will become commoditised and services will become standard	**5** Current – premium products still corner some markets Future – product price becomes secondary to supporting services (apps)

2 Business Opportunity

The business opportunity is conceptualised in terms of the following scenario from the point of view of the end-user:

> *"Imagine that your alarm system is also a home automation system that can be remotely accessed (through an application downloaded from the Apple iStore or Android Play Store) to arm or disarm it, switch on lights, turn off the geyser to save electricity, or view footage from cameras linked to the system. Furthermore, your system will alert you and send push notifications and photographs when the alarm goes off or a family member gets home and disarms the system. Water sensors will alert you when they sense water in the drip tray of your geyser long before it bursts. Smoke sensors will alert you well in time before your house burns down."*

Such a system offers the end-user the power of professional security as well as home automation, all run by the user in real time with visual bi-directional voice. The capability to sense water leakage or fire smoke opens up immense possibilities for insurance companies and banks that pay out large sums in claims after the fact. These products make it possible to proactively manage the home and limit risk. Insurers can also collect valuable data from their customers to assist in creating new business models and developing future products.

To ensure seamless integration of this new suite of products, the effectiveness of the network and its up time is critically important. The system cannot operate in an off-line state: if the network is down, so too will be the remote operation of the system because the application cannot be accessed. The application facilitates the interoperability of the different devices and technologies. Managing this comprises the services component of the business model. The application provides push notifications and direct operation for the end-user. The "stickiness" that moves this offering from a grudge alarm purchase to a "cool" lifestyle piece of technology has an associated monthly cost because a service is purchased. Once the technology has been sold—either directly, rented out, or provided on a plan—the scale-up from alarm operation via the mobile application to basic home automation to video-on-demand creates a recurring revenue model.

As a distributor in the security sector, Elvey Security Technologies has always made products available to installation companies that offer security services to the commercial/industrial and residential markets. Security is a lucrative market in South Africa, so customers (security

companies and installers) have a wide range of products to choose from; maintaining loyalty and return is a challenge for distributors. With the evolution of the IoT and the ubiquitous App world, the opportunity to link products and services becomes extremely attractive: without the product, the services would not operate; without the services, the distributor sells only product and the threat of substitution or change to another similar product is ever-present. This Business Venture Proposal is for the distributor to host the IoT services (the Application) that makes the interoperability and integration between technologies possible, thereby adding a services component to the value proposition whereby the end-user interacts directly with the technology.

Elvey Security Technologies's core business is as a distributor selling product to installers of security technology. It is an exciting prospect to take advantage of the advantages of services, applications, and IoT, and the recurring or annuity income model of this business opportunity. Controlling the product, distribution, and back-end Application that brings all the technology together (to give the user the experience and interaction that they require) opens up recurring revenue streams and encompasses the entire value chain.

In practice, a back-to-back agreement with the Application developer will be signed by Elvey Security Technologies, which specifies an agreed distribution price for the services/Application. This, in effect, means that the distributor will supply both the product and the back-end services and application. The installer and distributor enter an agreement in which every implementation that the installer sells or installs attracts a monthly revenue stream that is shared between the two parties. Furthermore, telecommunications companies are interested in this technology because it requires data to operate, which is one of their main products. Insurers are also interested in this technology because it can provide forewarning and possible reduction of impending claims through products like smoke and water sensors. Such technology would also give both telecommunications companies and insurers the opportunity to utilise the large volumes of data generated to detect patterns and trends in their customer behaviour by monitoring how they interact with their systems.

2.1 Data Collection

To substantiate the premises, assumptions, and some pricing components for the Business Venture, various studies were conducted by direct market research and direct investigation (surveys and interviews).

The population size for the market research was the number of security companies currently on Elvey Security Technologies's vendor list, i.e., the sample was approximately 1600 out of 3000 listed customers (about 1600 customers make a purchase each month). Market research surveys generally work better when the sample size is large (SurveyMonkey, undated). The number of registered security companies increased by 6.1% from 8195 to 8692 in 2016 (Private Security Industry Regulatory Authority, 2016). Of these, more than 50% are guarding companies that do not typically purchase technology, but instead provide physical guards as their core business. Moreover, the initial target market for the Business Venture is existing Elvey Security Technologies customers that have profiles on Elvey Security Technologies's enterprise resource planning (ERP) system, 30-day accounts, and a relationship with the business through its branch network of 20 outlets. A suitable sample size was selected using the SurveyMonkey sample size calculator (SurveyMonkey, undated). Strict parameters from confidence and margin-of-error perspectives were selected due to the specific nature of the survey questions and the professionalism of the respondents. For a population size of 1600, confidence level of 85%, and margin of error of 15%, the calculated sample size was 23.

2.1.1 Survey of security companies and independent installers

The survey attempted to ascertain and understand how security companies are preparing for the IoT trend and what opportunities are seen. Furthermore, the survey attempted to gauge to what extent the respondents have put a business model together to take advantage of any perceived IoT opportunities.

It was also important to determine whether respondents would see distributors as a competitor if they entered into a recurring-revenue model, similar to that of security companies , because this is a critical risk to the proposed Business Venture. If a respondent (as an independent installer or representing a security company) viewed a revenue-share model as an opportunity, it was important to ascertain how they would view such a model with a distributor. Details of the customer survey and responses are provided in Appendix A.

From the 33 companies that took part in the survey questions below, the following summarised responses were offered.

1. Do you see the residential alarm market moving away from the traditional form of monitoring home alarms in favour of self-monitoring?
   42% Yes; 42% No; 16% abstained

YES 14/NO 14 (5 no answer)

2. Is the end-user demanding more control from their alarm systems with added features, such as applications, home automation, and video verification?
   76% Yes; 3% No; 21% abstained

YES 25/NO 1 (7 no answer)

3. Do you feel that the new IoT technology available today is able to replace the traditional "professional" security system?
   36% Yes; 36% No; 28% abstained

YES 12/NO 12 (9 no answer)

4. Are you actively looking to offer these solutions to your customers in the short term (within six months or less)?
   55% Yes: 27% No; 18% abstained

YES 18/NO 9 (6 no answer)

5. If a distributor were to offer a comprehensive IoT solution and fully support the hardware and back-end solution (through applications and services), would you be interested?
   79% Yes; 6% No; 15% abstained

YES 26/NO 2 (6 no answer)

6. If distributors were to charge a monthly recurring fee for the above (Q5) services,would you still be interested?
   52% Yes; 21% No; 27% abstained

YES 17/NO 7 (9 no answer)

7. Do you see the opportunity for a revenue-share model to capture this new customer base that wants to self-monitor through an application using IoT devices?
   67% Yes; 9% No; 24% abstained

YES 22/NO 3 (8 no answer)

8. What would a fair monthly price point be for an application that offered push notification, video verification, and home automation with server support and full redundancy?
   Of 22 respondents (67%), the average monthly price was R 132.57 (sum of prices provided: R 2,916.50). On removing one outlier that lay between R 500.00 and R 1,500.00, the average monthly price was R 87.11 (sum of 21 remaining prices: R 1,916.50)

Values provided (in ZAR): 100–150; 200+; 35; 50; 50–75; 50; 75; 500–1500; 150; 99; 250–350; 120; 150; 0; 150–250; 50–100; 0; 0; 0; 0; 0; 150. The zero values represent those of respondents who believed that the solution should be free.

9. Are there any comments that you would like to add regarding IoT, application-based self-monitoring, and the connected home or business?

Network/coverage; free apps are available; this needs to offer more value; must work consistently; quick consistent network; easy and scalable solution; liability mitigation; tech/app must be impressive; offering must be clear; customers still don't see the value of features and benefits so these will have to be made clear; consistent system uptime is a must.

2.1.2 One-on-one interviews with distributors

A one-on-one interview process was conducted with competitors to Elvey Security Technologies as well as with manufacturers that are entering the South African market in competition to their distributors. The respondents represented Forbatt, Reditron, and Tyco three major safety and secuirty companies operating in South Africa. An interview was also conducted with the Chief Executive Officer (CEO) of Elvey Security Technologies. All interviews sought to ascertain how distributors/manufacturers see the IoT trend affecting their business and how they are preparing to take advantage of these opportunities? Details of the survey and responses are provided in Appendix B. Responses from these companies are summarised as follows:

10. Do you see the residential market moving away from the traditional monitoring of home alarms?

Yes, a definite move is happening. Back-end services are, however, not 100% there yet. Armed response is also still something that is required due to our [South African] crime.

11. Is the end-user demanding more control from their alarm systems with added features, such as applications, home automation, video verification?

Yes, but such technologies are not yet fully understood by the end-user.

12. Do you feel that the new IoT technology is able to replace legacy professional security systems?

Not entirely: professional security in South Africa remains in demand from end-users and so professional systems will always be required due to the high crime rate.

13. Are you actively looking to offer these solutions in the short term (within six months or less)?

Yes, we already are. The biggest push from us is, however, customer engagement and education because the technology already exists.

14. Do you believe that a distributor is able to offer a comprehensive IoT solution and fully support the hardware and back-end solution (application and services)?

A mixed response was received from the respondents: 50% believe that the distributor is able to do so if correctly resourced; 50% responded saying that the distributor will always need the manufacturer.

15. Do you think that installers and installation companies would be prepared to pay a monthly recurring fee if distributors were to charge for the above (Q5) services?

25% responded no; 50% responded yes; 25% responded that the security company may decide to offer these services themselves, so the proposition needs to be sufficiently powerful to keep the installer interested – strong features and a lucrative revenue share are imperative.

16. Do you see the opportunity for a revenue-share model to capture this new customer base interested in IoT self-monitored systems?

Revenue share is the way in which to keep the new customer base interested: yes.

17. What would a fair monthly price point be for server, application, and back-end services on a revenue-share basis?

Dependent on services offered and back-end features: between R 100 and R 500 per month.

2.1.3 New and existing homes

Data collection using editorials, Statistics South Africa, and the Internet was undertaken to illustrate the end-user market size (home owners), estimate how many new security installations can take place, and to gauge the size of the potential retrofit market in terms of existing security systems that end-users may wish to upgrade to IoT-ready products to access the features and benefits of self-monitoring capabilities.

There are about 15.6 million households in South Africa at present (approximately 11 million brick houses or apartments (Statistics South Africa, 2016). The number of households is growing faster than the population, so between 38% and 46% of households live in homes that have been built since 1994. "Since 1994 the private sector in the bigger municipalities has constructed 1.625 million residential buildings" (Schussler, Smith, C. 2016, 22 February *Home Ownership in SA: Facts Tell a Different Story*).

2.1.4 Alarms being monitored in South Africa

Security companies use monitoring software in their control rooms to manage the signals that come in from communication devices, such as radio transmitters and GSM communicators. Internationally designed control-room software products are available, but the majority (85%, Grahame Clarke owner of Oryx Listener www.oryxsystems.co.za the largest supplier of security control room software in S.A) are designed and developed locally for the South African context. Three South African products are dominant: *Listener*, *Watch Manager*, and *Execuguard*. Of these, *Listener* is used by 70% of security companies that offer monitoring and response as a service.

The owner of Oryx, that designed the *Listener* control room monitoring software, was interviewed to understand the relationships between the number of monitored alarms in existing houses compared with those in new houses being built. The interview also focussed on determining current attrition rates (end-users that cancel services from their service providers)

and information regarding self-monitored alarms currently on offer. The Oryx platform is managed by the company on behalf of security companies, so Oryx has access to some 80% of available data, thereby offering an accurate assessment for this analysis. A direct interview with Graham Clarke (owner of Oryx *Listener*) provided the following data:

- Oryx monitors some 1 million sites in South Africa;
- their monitoring software is used in approximately 500 control rooms in South Africa;
- the number of sites has decreased over the past three years (1.1 million sites were monitored three years ago).

Some of the reasons offered for the drop in number of sites monitored included:

- affordability;
- a greater number of people living in complexes compared with free-standing homes;
- estates and complexes manage their own security.

To compensate for this stagnation and drop in control-room-connected homes, security companies are offering more services to households than in the past and are charging for these extra services. Services include chaperone services, medical and more recently monitoring of specifics like borehole levels, pool/fish pond pumps and refrigeration

2.1.5 Internet of Things retail solutions

Based on research carried out for other markets and the models adopted by Samsung and ADT (Wieczner, J. (2015, 29 October) in the United States of America (USA), the South African retail security sector was examined to understand whether opportunity was perceived regarding the IoT and, if so, how this was being addressed (see Incredible Connection appendix). Specifically, the activities of the retailers DionWired (www.dionwired.co.za) and Incredible Connection (www.incredible.co.za) with respect to IoT were of interest: their approaches vis-à-vis hardware and the attached services and their views on whether the recurring revenue portion of the solution was something that they could capitalize on were interrogated.

DionWired is an electronic technology retailer and part of the Massmart Group. DionWired does not currently offer IoT devices for home automation, security, or surveillance. Although stores stock many electronic household appliances and office equipment, there were no products that offer the solutions discussed in this Business Venture Proposal.

Incredible Connection is an electronic technology retailer that is part of the JG Group owned by Steinhoff (www.steinhoffinternational.com). All stores visited stocked IoT devices for home automation and surveillance. In December 2017, a Smart Plug with application sold for R 799.00 and an indoor camera sold for R 1,699.00. The so-called "nanny cam" was not included in this research because it is categorised as a DIY item, rather than as professional security as were most of the other products (www.incredible.co.za/departments/security). The Smart Plug and indoor camera both worked on a standalone basis with a free application but were not part of an integrated solution. There was no main hub or control-panel solution offering an integrated, interoperable solution bringing together the elements of Alarm, Surveillance, and Home Automation in a single application.

All products were sold on a DIY basis, with a toll-free number for telephonic technical support. No on-site technical support is available; the hosted services on the free application are generic and not encrypted or supported locally. Pricing on the Smart Plug is similar, albeit cheaper, compared with the professional version offered in our Business Venture. The indoor camera is significantly cheaper but is a stand-alone unit (not part of a security and home automation ecosystem) and there is no outdoor version available, which severely limits the requirements of most surveillance systems that offer outdoor protection.

The only advantage of these retail offerings is that of price for the indoor camera, which will only be attractive to those consumers looking for a "quick fix". From an opportunity perspective, this large electronic retailer is stocking IoT devices for a demand that is clearly present: large multinational public companies do not stock products that do not sell and a due diligence will have been performed prior to stocking of these items.

2.2 Market Research

2.2.1 Potential monthly recurring and once-off income

Various national security companies were telephonically contacted to determine general market prices for alarms, home automation, and CCTV systems. General monthly monitoring and armed response pricing for domestic/residential alarms and monthly data charges for applications were also investigated.

An average monthly monitoring fee of R 500.00 was calculated from a cross-section of thirty security providers located in Johannesburg, Durban, Cape Town, and Port Elizabeth. Prices

ranged from R 150.00 to R 990.00. Some companies are also already making use of basic panic applications that are driven through a smart phone and include in these monthly monitoring and armed response fees.

These data enabled an understanding of current price points for monitored alarm systems and data and application charges to gauge whether the proposed revenue-share model would work for Elvey Security Technologies using the proposed back-end and application. This market intelligence and the survey results discussed earlier indicated that there was potential opportunity for this model, so this pricing was used in the models described in Chapter 3.

2.3 Different business models

The four business models considered for the monetisation of inrenet based opportunities are those of outright purchase, rent-to-own, and monthly subscription.

Various markets employ a recurring revenue-share model with outright purchase of equipment. For example, cellular telephone shops share in recurring revenue with telecommunications providers, such as MTN and Vodacom, by selling cellular phones with SIM cards.

The telecommunications industry also uses a model of recurring revenue share with an additional monthly contribution to offset equipment costs, where, for example, contracts that include more data and higher monthly premiums will attract free phones.

The business automation industry often employs a model of recurring revenue share and rental of equipment, where office equipment (such as photocopiers, printers) is rented to the end-user. The company installing the copier links it to a network (normally fibre) and then shares recurring revenue with the network provider (fibre-to-the-home/business companies).

A direct model of revenue sharing through the sale of recurring services is also employed by technology providers, such as telecommunications companies, and insurers.

These four models are all able to be implemented in Option 1 of the Business Venture Proposal (Section 3.2) with the fourth model applicable to Option 2 (Section 3.3).

3 Business Venture Options

Two Business Venture Proposals are considered: Option 1 is based on a recurring revenue-sharing scheme with existing customers; Option 2 is based on a recurring revenue-sharing scheme with existing customers in addition to partnerships with telecommunications companies with respect to data consumption and with insurers with respect to potential for claims reductions.

3.1 Assumptions

Both Options 1 and Option 2 are based on the following assumptions, which were valid as at December 2017:

- the exchange rate was set at a forward rate of ZAR 14.00/USD;
- all prices exclude value-added tax (VAT) that is levied in South Africa;
- the product suite is based on the DSC range of alarm equipment (www.dsc.com), resolution cameras, Fibaro ZWave home automation devices (www.fibaro.com), and the Securenet (www.securenettech.com) back-end application and services;
- all current agency agreements with Elvey Security Technologies on the above manufacturers' products are intact and ongoing;
- all costs were assumed for the bolt-on Business Venture joining the Elvey Security Technologies head office environment as a standalone business within the group;
- networking costs and server hosting costs at Vodacom Business Centre remain constant and within a 10% price point at the date of last quotation (December 2017).

3.2 Option 1: Recurring Revenue Share – Existing Customers

3.2.1 Description

Elvey Security Technologies's IoT division (the new bolt-on Business Venture) supplies IoT products to a security company or independent installer. The products include a control panel that is the main brain of the system and allows for the connection of IoT devices to the Cloud and is operated through an application. The devices include typical alarm products (passive infrared detectors (PIRs) and door and window contacts), flood and smoke detectors, ZWave

devices to drive lights, air conditioners, geysers, and cameras for video verification and live-streaming with bidirectional audio capability. The hardware is driven through the application. The end-user has full functionality and receives push notification from all devices.

The security company or independent installer pays a recurring monthly fee for the application, server and network maintenance and uptime, as well as any updates and/or software fixes that may be required. These are provided by Elvey Security Technologies's IoT bolt-on business. The end-user pays a marked-up monthly fee to the security company or independent installer for the services and receives information from the hardware through the application.

A simulated Proposal, prepared using the Business Venture described above, is presented below. The Potential Customer is the Elvey Security Technologies customer (security company or independent installer). The Potential Customer's customer is the end-user. All indicated pricing is what Elvey Security Technologies's Potential Customer would pay for the services and hardware. Securenet is the back-end application-and-services component of the solution: this is a separate product that is designed and developed by Securenet in the USA.

3.2.2 Monthly subscription to security company or independent installer

Table 2 shows pricing to the Potential Customer. The approximate selling price of the application to the end-user is R 100.00 per month. All selling prices are calculated at a 40% margin. This has been calculated based on the break even analysis and the market potential as researched for this proposal.

Table 2: Component pricing for Option 1.

Stock-keeping unit	Stock-keeping unit description	Potential Customer price (R)
Complete Interactive Residential	Dual Path IP only - Includes Zwave	52.00
Video	Includes up to 4 cameras 250 events - IP only	52.00
Video Plus	Includes up to 8 cameras 500 events - IP only	91.00
Complete Interactive Residential Plus	Dual Path GSM plus IP - Includes Zwave	99.00
Portal Branding	Branding and background customization	*123,000.00

2 Way Voice	Two-way voice service	31.00

*This cost will be waived for commitment to the proposal by the customer. These services will effectively be given for free.

3.2.3 Basic package pricing

Total kit price: R 7,335.00

- 1 x Panel (WiFi + 3G)
- 2 x Passive infrared detectors
- 2 x Door/window contacts
- 2 x Remote key fobs

Individual item prices:

- Panel R 6,200.00
- Passive infrared detector R 498.00
- Door/window contact R 535.00
- Remote key fob R 327.00
- Flood sensor R 1,087.00
- Smoke sensor R 1,188.00
- Indoor camera R 2,351.00
- Outdoor camera R 3528.00
- ZWave device R 808.00

Data usage and throughput:

Full-resolution (720p high-resolution video format) streaming at 2048 kB/s is assumed.

SMS (short message service) and email notifications are assumed to use less than 5 MB if the system communicates ten times per day using GPRS or Ethernet via push notification and video clips on event.

This data throughput calculation is important because it gives the end-user an indication of the costs involved with communication either through a SIM card or IP connection. Using GPRS (SIM card) as the communication format means that an R 80.00 pay-as-you-go SIM will easily cover normal communications of the control panel, video verification, and home automation. This does, however, exclude video streaming: this is entirely up to the end-user with respect to how often and for how long they view footage from the system cameras. This means that the

end-user is responsible for ensuring that they have enough available data for their viewing preferences.

3.2.4 Problem statement

IoT technology has progressed to the point that it is no longer out of reach to the general market (residential and commercial/industrial). The ability to transfer data and communicate through effective networks means that cost-effective solutions are available to better secure properties and people. Users' lifestyles can also be improved (through an application) by remotely operating lights, opening automatic door locks, and switching devices like geysers for energy management. Proactive management of impending risks can be managed using smoke detectors and flood sensors. A site's environment and activity can be remotely viewed using real-time video and by receiving push notifications. Trend analysis shows that self-monitoring is a growing phenomenon in the residential market, especially in gated communities, apartments, and homes with younger technologically sophisticated consumers. Results of the surveys conducted for this Proposal are available as Appendixes A and B.

3.2.5 Solution

A control panel (central hub) manages the ecosystem from a central point in the home or business to integrate elements of security, remote home automation, and video-verification technologies. The system employs a professional alarm system that has additional integrated technology (ZWave, WiFi, or GSM) that allows for home automation, visual verification, and proactive energy and risk management. These products offer a strong self-monitoring component through interoperable, integrated back-end services and applications.

3.2.6 Target market

The target market is the Elvey Security Technologies customer (professional security companies and independent installers) that installs security systems in the residential and commercial/industrial sectors. These installers have access to their own existing customer bases as well as to new market entrants looking for technology to be installed on their premises. Elvey Security Technologies currently has approximately 3000 security companies as customers. This database will be made available to the new Business Venture to mine for suitable partners.

3.2.7 Offering

The offering includes the following:

- DSC IoTega alarm system (includes GSM, Wifi, radio frequency (RF), and Zwave)
- RF 433 MHz or 868 MHz devices
    - Passive infrared detectors
    - Door/window sensors
    - Panic buttons
    - Smoke detector
    - Flood sensor
    - Indoor/outdoor camera
- Securenet back-end application
- ZWave devices
    - Plug
    - Light switch/dimmer
    - Switch

3.2.8 Example of business case

The IoT has progressed to where technology is readily available to offer the consumer an alarm system with home automation and video verification. This technology integrates seamlessly onto a single platform that the user has the power to interrogate and drive and from which push notifications are received. This functionality is available through an IP and/or GPRS network. In addition to the data-usage opportunity, there is the advantage of the customer's engagement on the platform by driving the system and its devices to enjoy lifestyle benefits, such as home automation, energy management, and video-on-demand and/or video verification on event through the main control panel of a professional security system. This scaleable solution will be offered to the growing market of consumers who are beginning to demand these solutions.

3.2.9 Relationships between Elvey Security Technologies, DSC, and Securenet

Elvey Security Technologies is the distributor of DSC equipment and registered vendor for the Securenet back-end solution that works with the DSC IoTega. Securenet is a USA-designed product with offices in the USA and Australia and worldwide representation through distributors. Elvey Security Technologies stocks and supports DSC and Securenet products in South Africa and Sub-Saharan Africa on a revenue-share model with Securenet. The

agreements that Elvey Security Technologies has in place with DSC and Securenet are such that, besides the direct support offered by Elvey Security Technologies, further support – if needed – is offered by the manufacturer to ensure that all customer requirements are met.

3.2.10 Customer journey

The Potential Customer's customer would purchase the package (equipment) from the Potential Customer with full access to the back-end services and application based on the specific plan selected by the end-user (see Table 2).

Once the Potential Customer's customer has purchased the equipment and chosen the plan, the installation will be carried out by the Elvey Security Technologies-trained Potential Customer. Once the installation is complete and payment has been made, the on-line services will commence on the Engagement-of-Services command. These services can be turned on or off during the course of the contract by the Potential Customer, should their customer default.

The end-user then has the use of the system and all its features directly on the panel's key pad or remotely through mobile devices (smart phone, tablet, lap top) through the application. The system can be added to or upgraded at any time and the end-user can purchase more devices to grow the system as and when required.

The trained installer will offer all technical support and any product replacements will be done by the installer. Elvey Security Technologies will warrant all equipment and, on a swap-out basis, ensure that the customer has the least possible system downtime. Elvey Security Technologies will hold all necessary stock for its Potential Customer and its partners to ensure that new installations, system add-on requirements, and damaged or faulty devices can be supplied at all times.

3.2.11 Benefits, goals, and measurement criteria

As a distributor of security products, Elvey Security Technologies has been representing international and local brands for over 70 years. The role of the distributor is to stock, market, make available, and support the products that the manufacturers award on an agreement basis. The agreements generally have exit clauses and manufacturers are known to award multiple agencies or even trade directly in competition to their distributors. Coupled to the fact that there are many brands, manufacturers, and distributors from which security

companies can choose makes distribution a difficult business. A distributor starts from a zero base each month: it is here that the key advantage presents itself in introducing this proposed Business Venture. The recurring component of the business model creates a passive revenue stream that grows in a compound manner. There is an evergreen period, after which all revenue is pure profit; the back-end services and application also feed product sales. Table 3 summarises the potential benefits.

Table 3: Potential financial benefits of Option 1.

Category	Benefit	Value per month
Financial	• New revenue generated from the sale of equipment at a 40% margin – based on estimated number of kits sold per month – market appetite • Recurring monthly contracts are attached in direct relation to panels sold – same as estimated number of kits sold per month • Compound growth on all recurring contracts sold	R 7,335.00 R 84.00
Operational	• As recurring contracts grow past the initial stage where costs are covered, the evergreen stage follows	Current margin on recurring services is 25%
Market	• Increased market awareness • New markets for greenfields/blue ocean sites • Additional competitive advantage • Decreased threat of substitution due to recurring contracts (12 to 24 months) locking in end-users • Alarm, video, and home automation services effectively lock in the end-user	100% Difficult to change lifestyle
Customer	• Improved customer satisfaction • Increased customer retention – "stickiness" of the services • Greater customer loyalty	100% Revenue-share model makes money for the customer

Staff	• Increased staff satisfaction – new commission structure based on recurring monthly revenue • Improved organisational culture • Better staff retention	100% A successful business has the propensity to improve morale. A new business that starts off well builds good morale and staff retention.

3.2.12 Costs and funding plan

The proposed Business Venture is based on a bolt-on business to the existing business of Elvey Security Technologies. Elvey Security Technologies has a head office with 20 branches around South Africa, as well as in Botswana and Namibia (each branch has administration and stores with the relevant staff complements). There are clear efficiencies and immediate savings that are available to the bolt-on business because it will reside at Elvey Security Technologies's head office in Greenstone, Johannesburg, and make use of warehouse space at the head office and in each store around the country. Existing networks will be used for telephony and information technology (IT); common staff, such as pickers, packers, receptionists, debtors, and procurement, will be utilised. The hardware solution is, in most cases, already purchased by Elvey Security Technologies for their core business function and the initial targeted customer base is already Elvey Security Technologies customers, so these core functions are already sufficiently resourced and will not need to be supplemented in the short term (12 to 18 months).

Extra resources will be required in terms of specific billing personnel that understand monthly recurring billing. Investment in a recurring billing system is required. One software engineer is required to handle the server and ensure that the back-end services run smoothly. There will be an element of outsourcing: the server will be housed at Vodacom Business Centre to ensure 24-hour uptime and clean power, as per their contractual commitments. Four dedicated sales personnel who understand applications, IoT devices, and how recurring contracts work will be required.

The business costs are summarised in Table 4. An income statement is available as Appendix C.

Additional capital will be required to purchase servers. A server that will be housed in the Vodacom Business Centre will be acquired. A second server will be in place for redundancy to ensure that switchover is possible should any failure occur on the part of the primary server.

The servers will have the software loaded to run the application and all related services, such as alarm control, video verification, home automation, and the installer configuration tool.

A second server to run the APN (access point name) that will also be housed at the Vodacom Business Centre will be required. An APN is the gateway between a GSM, GPRS, 3G (third generation), or 4G (fourth generation) mobile network and the Internet. A mobile device making a data connection must be configured with an APN to link to the carrier. In this context, the panel will have a dual SIM card that will roam between the Vodacom and MTN networks, depending on which signal is the strongest, to ensure maximum uptime and connection to the application from a mobile device. A private APN simply means that the devices will link to the carrier on their own streams (not the public APN), which means less data traffic and reduced chance of failed signals and communication between devices. The associated capital costs are shown in Table 5.

Table 4: Business costs associated with Option 1.

Category	Cost	Value	Budgeted
People	• Salaries of sales staff (x 4) • Salaries of billing personnel (x 1) • Salary of software engineer (x 1) • Commission	R 90,000.00 R 20,000.00 R 35,000.00 R 20,000.00	Yes Yes Yes No – approximate
Physical	• Office and warehouse rental • Tools (computers, phones, etc.) • Depreciation • Consumables	R 59,000.00 R 10,700.00 R 4,500.00 R 3,500.00	Yes Yes Yes Yes
Marketing	• Advertising / branding • Promotional material • Advertising in journals and publications • Launches and exhibitions	R 6,667.00 R 5,000.00 R 8,334.00 R 8,334.00	Yes Yes Yes Yes
Network	• Costs to run the network – APN • Cost to house the server in Vodacom Business Centre * SIM card to be added to all GPRS configuration panel kits (not IP-based)	R 3,000.00 R 7,100.00 *R 8.00 per SIM	Yes Yes
TOTAL PER MONTH		**R 275,135.00**	Yes

Table 5: Estimated capital costs associated with Option 1.

Funding source	Amount	Notes
Elvey Security Technologies	R 500,000	A server (plus redundancy) to be housed at Vodacom Business Centre
Elvey Security Technologies	R 100,000	APN server
Elvey Security Technologies	R 1,650,810	Start-up cost, based on estimated man hours
TOTAL CAPITAL COST	**R 2,250,810**	

These assets will be depreciated over five years using the straight-line depreciation method:

Purchase cost – estimated salvage value = Depreciable asset cost;

Five-year useful life = 20% depreciation rate per year;

20% depreciation rate x depreciable asset cost = annual depreciation.

Capital cost (R 2,250,810) – R 337,622 (15% salvage value after five years) = R 1,913,189. Annual depreciation at 20% (five-year useful life) = R 382,638 or R 31,886 per month. It is unorthodox to depreciate the start-up costs (R 1,650,810): this should be considered as a loan that will be repaid to Elvey Security Technologies for the first six months during which the business will start up. At a monthly cost of about R 275,000 to run this bolt-on Business Venture (Table 4), these start-up costs will provide for an approximate six-month period to attain the critical mass required to sustain the business.

3.2.13 Break-even analysis

The break-even analysis was undertaken using sales as the baseline to cover cost. The formula used was Fixed Cost divided by Contribution Margin Percentage (FC/Contribution margin %). A variable costing system was not employed because most costs are fixed, as shown in Tables 3 and 4. There are too many individual products to use units (FC/Contribution per unit) and the calculation becomes too complex. Once the break-even point is calculated from a sales perspective, a rough estimate of the number of panel kits that need to be sold can be calculated.

Individual items over and above the kits (alarm devices, cameras, and home automation devices) are add-on products that are nearly impossible to forecast because the base kit should cover 80% of likely purchases (the kit composition will cover the average home/apartment). The remaining 20% of sales arising from additions to the base kit will largely

be dependent on the individual and their personal site situation. These sales will also be made up of add-on purchases to systems already installed because these are fully scaleable and upgradeable at a later stage. The break-even analysis is presented in Table 6.

Elvey Security Technologies currently sells approximately 2000 alarm control panels per month. Based on the study conducted in which 33 independent installers and professional security companies were surveyed (see Chapter 2), the move to self-monitored systems is already underway in South Africa. For the business to sustain itself and make the sales necessary to break even, a reasonable time will be required to reach these levels. This cost has been factored into the cost structure as the capital cost (CAPEX) item **Start-up Costs – TIME** (Table 4). Revenue generated over and above equipment sales, through the accumulation of monthly recurring revenues, needs to be factored into the calculation: this is accounted for in Table 3 (Financial).

Table 6: Break-even analysis for Option 1.

Item	40% margin	25% margin
Fixed costs	R 275,135 (excluding R 20,000 commission)	
Contribution margin	40%	25%
Total sales required to breakeven per month	R 687,838	R 1,100,540

3.2.14 Risks and issues

One of the main risks to the Business Venture is the reputational risk that Elvey Security Technologies may suffer once this bolt-on business starts achieving success. Traditional business models have distributors supplying product as their core business and security companies monitoring and responding to the security systems that they install. The distributor's main revenue stream comes from the margin on products sold; the security company makes its main revenue from monthly recurring revenue. In this Business Venture, a distributor of equipment will be offering a platform on which end-users will be able to self-monitor and, in effect, will no longer require the services of the security company. The need to install the equipment nevertheless remains (it cannot be done as a DIY project).

A risk exists that the developer of the back-end services and application (which allows the user to interrogate their alarm system, view live video streams, and connect their home through IoT devices) integrates their software to work with multiple hardware manufacturers. The developer controls the hardware through their own services and data centres and effectively owns the back-end that makes this concept possible. A distributor would be at risk by being in a position where a market is built on a product controlled by an external entity: this is why this business model requires the services to be internally hosted.

Another closely related risk is that of Elvey Security Technologies being new to software development and applications. Understanding the supply chain and customer base is a clear strength of the existing Elvey Security Technologies business; understanding the development of services and how resource-hungry that will be to the business is not fully understand. Support is a critical area and differentiator for this Business Venture: although Elvey Security Technologies has the internal IP to provide support and training on the supplied hardware, the new business needs to ensure 100% uptime of the services, provide skills to fix bugs, and, in time, develop the product to a point where the application and back-end services are wholly owned and controlled by the business. Hardware and software that is manufactured in Europe and the USA is meant for those markets; slight modifications to suit the Southern African conditions may not function entirely correctly. Idiosyncrasies, such as communication formats and fire walls, need to be understood.

A final risk is that of legislation and approvals requirements. ICASA (Independent Communications Authority of South Africa) must authorise all wireless technologies. Plug types (European, USA, South African) and power-supply regulations are governed by SAIDSA (South African Intruder Detection Services Association). Waiting for such approvals or for manufacturers to change the specification on a power supply or plug type can delay implementation.

Potential risks are summarised in Table 7.

Table 7: Potential risks associated with Option 1.

Description	Likelihood	Impact	Mitigating actions
Reputational risk	High	High	Ensure that marketing is through channels that keep customers at the forefront: they need to sell to the end user Market the revenue-share concept effectively

			to ensure that the customer base views this as an added source of revenue
Inability to recruit correct software engineer	Low	Low	Outsource to specialised companies with the required skill set
Technology solution is unable to deliver required results	Low	High	Product design to be tendered on a PoC (percentage of completion) basis to ensure that it works in the required environment
Approval delays and incorrect product makeup	Medium	Medium	Ensure timeous applications for all approvals Technical team to work directly with the manufacturer to understand product makeup and compatibility within the South African context

To mitigate the high-priority risks listed in Table 7, it will be important to ensure a list of prioritized issues that can be implemented and enable working towards addressing those key risks. Table 8 identifies the key risks and their resolution actions.

Table 8: Key risks and resolution actions for Option 1.

Description	Priority	Resolution actions
Message to the market regarding the new product offering (hardware and software) and the revenue-share component	High	Training of internal staff to ensure that everyone is clear on the strategy and that communication to customers is not ambiguous or contradictory Customer seminars outlining the strategy and benefits to them of using a recurring revenue-share model
Technology unable to deliver proposed features and benefits	High	Proof-of-concept sites to be identified and used as incubators to find product weaknesses: these can then be used as reference sites once they are up and running smoothly Rigorous bench tests and simulations to be performed on the product to ensure robustness
Regulatory approval	Low	Application to ICASA has been submitted and feedback is awaited Early approvals have been sought to ensure that the implementation is not delayed

3.3 Option 2: Direct Model – Insurers and Telecommunications Companies

3.3.1 Description

Some 44% of insurers across the world are looking at digital initiatives. The South African medical insurance company Discovery (www.discovery.co.za) is a stand-out innovator in their use of technology and the IoT. Furthermore, 31% of insurers worldwide are planning to work with start-ups from outside of the insurance industry to enable better services and gain more information from their client base (Jubraj, Watson, & Tottman, 2017). The concept of *Insurtech* refers to the use of technology innovations designed to optimise savings and efficiencies from the current insurance industry model.

According to James Dalton, Director of General Insurance Policy at the Association of British Insurers (Association of British Insurers, 2017), Insurtech is significantly benefitting the insurance industry; this is now spilling over into other industries, including that of telecommunications. There has been a fundamental shift in the relationship between traditional industries and markets and a number of new and emerging technology companies. Insurers recognize the benefits of collaborating and investing with these companies for example, Discovery has just purchased a technology business to take advantage of retaining that IP in-house McKinsey and Company, Adrian Gore (How Discovery Keeps Innovating; May 2015). Technology businesses like Elvey Security Technologies are not aiming to become insurers or telecommunications businesses themselves, given the significant regulatory and capital barriers; however, by adding clever IoT devices with interactive customisable applications to their offerings, a positive interdependence between the two industries can be enabled. With the above in mind, a potential market beckons that distributors have never directly targeted – that of insurance and telecommunications companies.

The costs of the business model remain the same as those of Option 1, so a cost analysis does not form part of the below discussion. For details, the break even analysis and cost break down should be consulted.

3.3.2 Benefits

There are clear benefits that accrue from dealing with insurers and telecommunications companies. The main benefit arises from the sheer scale of potential customers that can be tapped into from their existing bases. This access to scale does, however, come at a cost: all margins will drop by 15 percentage points to approximately 25% when dealing direct. The kit makeup and stock-keeping units (SKU) on services do, however, remain the same. The customer prices under this scenario are presented in Table 8.

Table 8: Component pricing for Option 2.

SKU	SKU description	Potential Customer price
Complete Interactive Residential	Dual Path IP only - includes Zwave	R 45.00
Video	Includes up to 4 cameras 250 events - IP only	R 45.00
Video Plus	Includes up to 8 cameras 500 events - IP only	R 78.00
Complete Interactive Residential Plus	Dual Path GSM plus IP - Includes Zwave	R 84.00
Portal Branding	Branding and background customization	*R 123,000.00
2 Way Voice	Two-way voice service	R 27.00

*This cost will be waived for commitment to the proposal and, in this case, is more critical because the target customers are significantly more brand-conscious than independent installers: their brand appears on all products, services, and marketing, regardless whether these products and services are outsourced.

3.3.3 Basic Package Pricing

Total kit price: R 7,335.00

- 1 x Panel (WiFi + 3G)
- 2 x Passive infrared detectors
- 2 x Door/window contacts

Individual Item Prices:

- Panel R 5,278.00
- Passive infrared detector R 423.00
- Door/window contact R 455.00
- Remote key fob R 278.00
- Flood sensor R 924.00
- Smoke sensor R 1,010.00
- Indoor camera R 1,999.00
- Outdoor camera R 2,999.00
- ZWave devices R 687.00

Installation:

- General wireless installation – panel, 2 magnetic contacts, 2 panic buttons (fully wireless or self-contained) is between R 1,500.00 and R 2,000.00;
- Basic call-out fee is between R 350.00 and R 480.00 – for fault finding;
- Hourly labour rate is between R 400.00 and R 500.00 – for upgrades.

Data Usage and Through Put:

Full-resolution (720p high-resolution video format) streaming at 2048 kB/s is assumed.

SMS and email notifications are expected to use less than 5 MB if the system communicates ten times per day using GPRS or Ethernet via push notification and video clips on event.

In this context, the customer (telecommunications company or insurer) will offer a package that includes all data through the data package purchased when buying a SIM package, fibre connection, or insurance plan. The telecommunications company is looking for innovative ways in which to entice customers to their network and use their data services: the connected home uses data and offers a novel way in which to engage with their customer and have that customer continually make use of their services as a lifestyle tool, which thereby becomes “sticky”. The insurance company is looking into these solutions for slightly different reasons. Besides the obvious “sticky” lifestyle benefits that increase customer engagement and retention, insurers are looking at ways to mitigate risk. With the addition of smoke and flood sensors on an IoT platform, customers can be incentivised to install these lifestyle enhancers and get early warnings of fires, burst geysers, and other leaks that constitute major risk KPMG Business Unusual (May 2016). The insurer benefits from an engaged customer base and a reducing claim risk, which equate to millions of rands in extra revenue and savings, respectively.

3.3.4 Risks and Issues

Table 9 summarises the risks associated with Option 2. Similar risks and issues to those of Option 1 (Table 7) are listed, with two key differences, as discussed in Table 10. This does not mean that the two common risks are not important, but rather that their resolutions are the same and it is unnecessary to repeat them.

Table 9: Risks and mitigating actions for Option 2.

Description	Likelihood	Impact	Mitigating actions
Reputational risk of being seen to be competing with our customer by entering the recurring revenue market	High	High	Ensure that installer providing the installation to the end-user is a *bona fide* installer and independent of Elvey Security Technologies. Market the revenue-share concept effectively to ensure that the customer base understands that this added source of revenue is for the installer and that while Elvey Security Technologies (bolt-on Business Venture) is attracting direct business, the channel is still benefitting (installation and recurring revenues)
Insurers and telecommunications companies are large enough to learn the business of importing equipment, distribution, and software, following Discovery's model of vertically integration, and in so doing cut out Elvey Security Technologies	High	High	Elvey Security Technologies must own the back-end solution and software. Whilst Elvey Security Technologies (bolt-on Business Venture) will initially be selling on a platform, in time Elvey Security Technologies will need to develop its own platform so that it does not risk being bypassed. Owning the platform will give Elvey Security Technologies the power to develop bespoke solutions that cannot easily be replaced and to remain relevant as owners of the platform – besides the obvious advantage of making more money by not having to share revenues
Technology solution is unable to deliver required results	Low	High	Product to be tendered on a PoC basis to ensure that it works in the required environment
Approval delays and incorrect product makeup	Medium	Medium	Ensure timeous applications for all approvals Technical team to work directly with the manufacturer to understand product make-up and compatibility within the South African

			context

Table 10: Key risks and resolution actions for Option 2.

Description	Priority	Resolution actions
Message to the market regarding the new product offering (hardware and software) and the revenue share component	High	Standard agreements are to be drawn up between the installer (independent installer/security company) and Elvey Security Technologies, **AS WELL AS** the telecommunications com[pany or insurer to ensure no confusion regarding Elvey Security Technologies's respect for the channel, i.e., working with its core customer base and not cutting them out
Threat of substitution and being cut out by the telecommunications company or insurer	High	A specialist (budget provision is made for a software engineer) must be hired to ensure that Elvey Security Technologies (new bolt-on Business Venture) can start to develop its own back-end services and application to reduce the risk of substitution or being cut out by the current revenue-share company (Securenet)

3.4 Recommended Option

Both options are recommended and both options are able to be implemented simultaneously. It will, in fact, be critical to implement both approaches simultaneously to ensure that the required sales are achieved within the budgeted time (six months). It is critical to the sustainability of the business to reach the break-even point within this period.

4 Implementation Approach

4.1 Business Structure

The business structure is described in Figure 1.

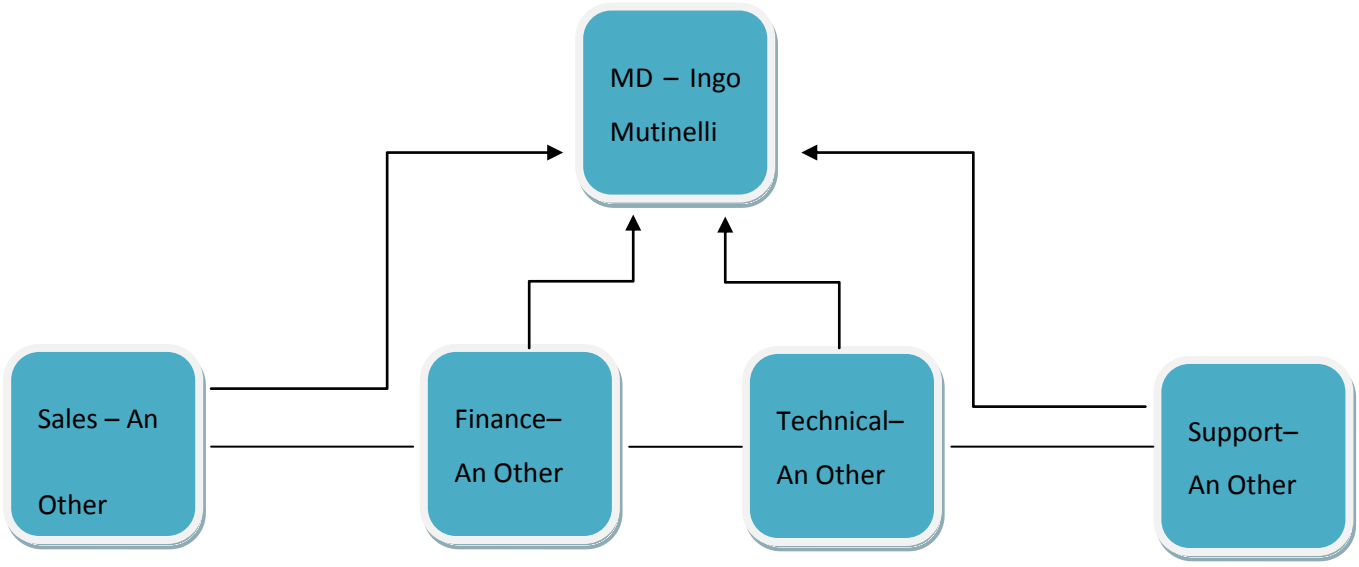


Figure 1: Proposed structure of Elvey Security Technologies bolt-on Business Venture.

Once all staff are in place and the back-end infrastructure is complete from the perspective of software services, network, and server planning, execution can take place. The most critical item of this business model is the back-end services and application that bring all components (alarm, surveillance, IoT devices, and home automation) to a single point of control: the application.

4.2 Business Planning and Execution

It is important to set the sales plan from the beginning. Because this Business Venture is new, the sales strategy will be set by the Managing Director (MD). The following key areas will be set out for the execution of the business plan.

Targeted customers: Elvey Security Technologies's base of 3000 customers will be assessed by branch and region. There are 20 Elvey Security Technologies branches and each branch serves a region (for example, the Boksburg branch serves the East Rand, the Roodepoort branch serves the West Rand). Each has a portfolio of customers that buy from that branch and are

registered via a specific branch code. The database of customers will be contacted via electronic mailer to ascertain willingness to be contacted by the new Elvey Security Technologies bolt-on business dealing specifically with IoT devices and a recurring revenue-share model. A 90% interest rate is anticipated (90% of survey respondents responded positively to IoT, a growing self-monitoring market, and revenue-share models (see Section 2.1.1). This does not mean that 90% of the 3000 customers on Elvey Security Technologies's books will be targeted: the full data base comprises poor-paying customers, businesses that have closed in the past six months, and businesses specifically focused on commercial industrial projects (not the residential market).

Call plan: A national call plan will outline proposed customer visits, identification of decision makers within the businesses, and current product range being used by the company.

Marketing plan: A marketing plan, outlining our Core Activities, Marketing Objectives, Marketing Mix, Products/Services, Place, Promotions and Prices, will be communicated. Detail of the marketing plan is provided in Appendix D. Budget has been set aside for marketing activities to bring the solution to market. The main activity will be road shows in the various regions where customers will be invited to a breakfast and the technology will be showcased by way of presentation. International manufacturers will present the technology and the bolt-on Business Venture will present the services and revenue-share model to the delegates.

Operational Plan: All physical stock required, as set out in Sections * and *, is imported. The following process applies:

- Once an order is placed with supplier, DSV (www.dsv.com) will receive a copy of the order with the supplier contact details (in this case, it will be DSC Canada);
- DSV advises the originating office of the new order and contact is made with the supplier to finalise cargo readiness date;
- Communication is forwarded to Elvey Security Technologies to advise when the container will be ready for packing;
- DSV will arrange booking with the shipping line for place of origin;
- Sailing details are forwarded to Elvey Security Technologies, showing ETD (estimated time of departure) and ETA (estimated time of arrival);
- Export clearance is carried out at the origin.
- Once the vessel sails, DSV is to forward pre-alert Elvey Security Technologies for processing of clearing instructions;

- Shipment documents (completed clearing instructions and packing list, commercial invoice, and bills of lading) are scanned and sent to DS SA.
- DSV SA requires clearing instruction from Elvey Security Technologies to start clearing process at least seven working days before the vessel arrives in Durban;
- Customs clearance is done via EDI (electronic data interchange), duties and VAT are brought to account with SARS (South African Revenue Service) and are paid on behalf of DSV clients by EDI;
- Original bills of lading, if required, must be submitted to DSV prior to vessel arrival in Durban;
- Once released from customs, the cargo is processed and DSV will obtain release forms from shipping line;
- Once released from the shipping line, DSV will forward transport instructions to the transporter to uplift the container from the terminal;
- On vessel arrival at the port, the container is off-loaded and either railed or road-freighted to Johannesburg.
- File to be invoiced by DSV on or before delivery.

5 Conclusion

This Business Venture Proposal has been researched from a live environment through the resources available to me as a direct operator in the Security industry. The comments and deductions made are based on more than 20 years experience in the Security industry. Outside of my own experience supporting research into the market size and future trends at a time when our industries (and others) are in a state of change due to exciting new IoT technology has been provided.

Cost analysis and break even analysis have been provided as well as operational processes and consideration on how to address this growing market have been offered. Further to that the key advantage of bolting this business into a profitable Publically Listed business (Elvey Security Technologies) mitigates many risks such as financial, reputational and first mover risks that start ups need to contend with.

It is with this in mind that this Business Venture Proposal should be seen as a viable proposition that has every chance of succeeding. I thank the reader for her attention and look forward to comments.

Appendices

Documentation in support of this Business Venture is appended as follows:

- Customer survey (Appendix A);
- Distributor interview (Appendix B);
- Income statement (Appendix C);
- Detailed marketing budget (Appendix D);
- IoT story board (Appendix E);
- Installation cost research (Appendix F)
- Hosting and maintenance contract for recurring revenue model (Appendix G).

References and Sources

Bentley, C. (ed.) (undated). The Manufacturer Industry 4.0 UK Readiness Report (pp. 1–16). The Manufacturer In Association with Oracle, United Kingdom. Retrieved 2nd February, 2018, from;
https://www.oracle.com/webfolder/s/delivery_production/docs/FY16h1/doc19/ Industry-Report.pdf

Dahua Technology (2017, 4 October). *Dahua Technology Creates a More Connected World with HDCVI-IoT* Retrieved 2nd February, 2018, from;
http://me.dahuasecurity.com/me/news/dahua-technology-creates-a-more-connected-world-with-hdcvi-iot-1341.html
International Institute for Analytics (2015). *Discussion Summary: The Internet of Things: Opportunities and Applications across Industries* (December 2015 Interview Featuring: Jason Mann, Director, Industry Product Management, SAS) (pp. 1 –8). Retrieved 2nd February, 2018, from;
https://www.sas.com/content/dam/SAS/en_us/doc/research2/iia-Internet-of-things-108110.pdf

Ironpaper (2016). *Internet of Things Market Statistics – 2016* Retrieved 2nd February, 2018, from;
http://www.ironpaper.com/webintel/articles/Internet-of-things-market-statistics/

Jubraj, R., Watson, S. and Tottman, S. (2017). The Rise of Insuretech. Accenture, United Kingdom. Retrieved 2nd February, 2018, from;
http://fintechinnovationlab.com/wp-content/uploads/2017/05/the-rise-of-insurtech.pdf

Meola, A. (2016, 22 May). *People Buy Smart Home Products for this One Main Reason* Retrieved 2nd February, 2018, from;
http://www.businessinsider.com/home-security-is-number-one-driver-of-smart-home-adoption-2016-4/?r=AU&IR=T

Private Security Industry Regulatory Authority (2016). Annual Report 2015/2016 (pp. 1–162). Centurion, South Africa. Retrieved 2nd February, 2018, from;

http://www.psira.co.za/psira/images/Documents/Publications/Annual_Reports/PSIRAAnnualReport2015-16.pdf

Reagan, C. (2017, 19 September). *Best Buy CEO sees 'Growth Opportunities' Ahead, Wall Street isn't Buying It* Retrieved 2nd February, 2018, from;
https://www.cnbc.com/2017/09/19/best-buy-ceo-weve-fixed-what-was-broken-now-focus-is-on-growth.html

Smith, C. (2016, 22 February). *Home Ownership in SA: Facts Tell a Different Story* Retrieved 2nd February, 2018, from;
https://www.fin24.com/Economy/kill-dangerous-property-nationalisation-slogans-with-facts-economist-20160222

Statistics South Africa (2016). General Household Survey 2016, Statistical Release P0318 (pp. 1–185). Pretoria, South Africa. Retrieved 2nd February, 2018, from;
http://www.statssa.gov.za/publications/P0318/P03182016.pdf

SurveyMonkey (undated). *Sample Size Calculator* Retrieved 2nd February, 2018, from; https://www.surveymonkey.com/mp/sample-size-calculator/

Wieczner, J. (2015, 29 October). *Best Buy CEO on How to Lead a Corporate Turnaround (Without Making Employees Hate You)* Retrieved 2nd February, 2018, from; http://fortune.com/2015/10/29/best-buy-ceo-turnaround-tips/

Bosch Security solutions product overview, from;
https://www.boschsecurity.com/xc/en/software-and-services/management-software/bis/

Kedacom Surveillance product overview, from;
https://en.kedacom.com/

Discovery – how our business works, from;
https://www.discovery.co.za/corporate/how-our-business-works

Keynote Address by James Dalton (22 June 2017) to the Verisk Risk Symposium, from;
https://www.abi.org.uk/search/?q=insuretech

McKinsey and Company, Adrian Gore How Discovery Keeps Innovating (May 2015), from;
https://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/how-discovery-keeps-innovating

KPMG Business Unusual (May 2016), from;
https://assets.kpmg.com/content/dam/kpmg/pdf/2016/07/2016-Insurance-Survey-v2.pdf

The Connected Home, from;
https://nest.com/