

# **Investigation into VoIP Communications fraud and TDoS attacks and solutions required for the corporate environment**

*Paul Carroll*

A dissertation submitted to the University of Dublin in partial fulfilment of the requirements for the degree of MSc in Management of Information Systems

***08 June 2018***

Jun-18

---

## Declaration

I declare that the work described in this dissertation is, except where otherwise stated, entirely my own work, and has not been submitted as an exercise for a degree at this or any other university. I further declare that this research has been carried out in full compliance with the ethical research requirements of the School of Computer Science and Statistics.

Signed:

A handwritten signature in black ink, reading "Paul Cornell", enclosed in a thin blue rectangular border.

8 June 2018

Jun-18

---

## Permission to lend and/or copy

I agree that the School of Computer Science and Statistics, Trinity College may lend or copy this dissertation upon request.

Signed:

A handwritten signature in black ink, reading "Paul Cornell", enclosed in a thin blue rectangular border.

8 June 2018

Jun-18

---

## **Acknowledgements**

I would like to thank my partner, Charmaine and my daughters, Amy, Sarah and Rachel for all their support, inspiration and understanding, without them this dissertation would not have been possible.

Special thanks to my tutor, Aideen Keaney, for all her generous support and expert guidance in helping me complete this dissertation.

I am also very grateful to all my friends and colleagues whom were gracious with their time and lending me their support on this journey.

Lastly I would like to dedicate this dissertation in memory of my father.

## Abstract

Voice Over Internet Protocol (VoIP) systems continue to disrupt and alter traditional telecommunications technologies, whilst increasingly converging with a multitude of heterogeneous computing platforms and systems across both commercial and consumer domains. With internet connected devices now almost ubiquitous, VoIP is becoming an increasingly popular technology for both business organisations and end consumers. Park (2009, p. xvii) suggests that *'Voice over Internet Protocol (VoIP) has been popular in the telecommunications world since its emergence in the late 90s, as a new technology transporting multimedia over the IP network, and that today people commonly make phone calls with IP phone or client software (such as Skype or iChat) on their computer or send instant messages to their friends'*. Organisations continue to integrate voice and data as this convergence offers greater flexibility and the potential for cost savings such as utilising shared infrastructure to deliver voice and data communication services to end users. Flanagan (2012, p.1) contends that *'Packet voice, Voice over IP and Unified Communications (UC) technologies are remaking telephony in a fundamental way that hasn't been seen since the 1960s'*

This research began with an in-depth review of VoIP and UC technologies including a detailed overview of their key features, advantages and disadvantages and known vulnerabilities and security risks. This included a detailed analysis of the known vulnerabilities and security risks that these technologies present to organisations whilst exploring several potential solutions and risk mitigation strategies for same. The research highlighted the growing trend of VoIP and the move towards UC technologies, a trend reflected in 2018 where four out of the top five UC vendors are cloud/software companies as opposed to traditional telecoms providers.

The research findings highlighted in the Literature Review and subsequent Findings and Analysis chapters demonstrated that VoIP and Unified Communications are complex technologies which are fast becoming standard communication systems in today's modern organisations. Following comprehensive qualitative research conducted with leading subject matter experts from Information Security and Telecommunications industries, it was confirmed that as these technologies continue to converge with existing data networks and computing platforms they are susceptible to many forms of cybercrime namely, toll fraud, data breaches and denial of service attacks. International Revenue Share Fraud (IRSF), Premium Rate Fraud and Wangiri call back schemes were identified as the most common and serious types of toll fraud due to the potential financial impact these can have on an organisation.

The majority of the academic literature was in general agreement regarding the numerous types of security vulnerabilities and risks associated with VoIP and Unified Communications implementations. Similarly, there was also a general consensus amongst all interviewees that VoIP and Unified Communications fraud was a real threat and growing concern for today's organisations. The new GDPR legislation which came into effect in the EU on the 25<sup>th</sup> May 2018 was also specifically called out as a key concern and security driver for all interview participants, all of whom unanimously agreed that VoIP security was very much a GDPR issue today.

The findings from this research will be of practical benefit to anyone working with or planning to implement VoIP or UC technologies in their corporate environments.

## Table of Contents

<b>1</b>	<b>INTRODUCTION</b>	<b>1</b>
1.1	IP TELECOMMUNICATIONS HISTORY	1
1.2	GLOBAL VOIP MARKET SIZE WORLDWIDE BY REGION 2014-2024	2
1.3	MAIN VOIP / UC VENDORS	3
1.4	CLOUD VS ON PREMISE VOIP/UC SOLUTIONS	5
1.5	RESEARCH OBJECTIVES	6
1.6	SCOPE OF THE STUDY	7
1.7	BENEFICIARIES OF STUDY	7
1.8	CHAPTER ROADMAP	8
1.9	RESEARCH TIMEFRAME	8
<b>2</b>	<b>LITERATURE REVIEW</b>	<b>9</b>
2.1	INTRODUCTION	9
2.2	VOIP OVERVIEW	9
2.3	MAIN COMPONENTS OF VOIP	11
2.4	KEY FEATURES OF VOIP SOFTWARE	12
2.5	VOIP BENEFITS AND DISADVANTAGES	13
2.6	VOIP VULNERABILITIES	14
2.7	SOURCES OF VOIP VULNERABILITY	15
2.8	VOIP VULNERABILITY COMPONENTS	16
2.9	VOIP THREAT TAXONOMY	16
2.10	TDoS, VOIP HACKING AND TOLL FRAUD	24
2.11	VOIP / UC SECURITY ATTACKS	25
2.12	VISUALISING THE ART OF MOBILE FRAUD	27
2.13	GENERAL DATA PROTECTION REGULATION	28
2.14	LEGAL RAMIFICATIONS	28
2.15	RISK MITIGATION STRATEGIES	29
2.16	SUMMARY OF RISK MITIGATION STRATEGIES	38
2.17	SUMMARY OF THE FINDINGS OF THE LITERATURE REVIEW	39
<b>3</b>	<b>METHODOLOGY AND FIELDWORK</b>	<b>40</b>
3.1	INTRODUCTION	40
3.2	RESEARCH PHILOSOPHY	40
3.3	RESEARCH STRATEGY	41
3.4	INTERVIEW METHODOLOGY	42
3.5	LESSONS LEARNT	48
<b>4</b>	<b>FINDINGS AND ANALYSIS</b>	<b>49</b>
4.1	INTRODUCTION	49
4.2	INTERVIEW FINDINGS	49
4.3	DATA AND THEME PRESENTATION	51
4.4	SUMMARY	62
<b>5</b>	<b>CONCLUSION AND FUTURE WORK</b>	<b>64</b>
5.1	INTRODUCTION	64
5.2	CONCLUSIONS	64

Jun-18

---

5.3	GENERALISABILITY OF FINDINGS .....	64
5.4	LIMITATIONS OF RESEARCH AND FUTURE WORK .....	65
5.5	SUMMARY .....	66
<b>6</b>	<b>REFERENCES .....</b>	<b>67</b>
6.1	NEWS ARTICLES / BLOGS / SURVEYS.....	70
<b>7</b>	<b>APPENDICES .....</b>	<b>72</b>
7.1	APPENDIX A. INFORMATION SHEET FOR INTERVIEW PARTICIPANTS.....	72
7.2	APPENDIX B. INFORMED CONSENT FORM FOR INTERVIEW PARTICIPANTS .....	73
7.3	APPENDIX C. INTERVIEW QUESTIONS .....	75
7.4	APPENDIX D. SAMPLES FROM TRANSCRIBED INTERVIEWS .....	76

Jun-18

---

## List of Tables

Table 1.	Interview Questions	46
Table 2.	Interviewee Profile	50



## List of Figures and Charts

Figure 1.	Global VoIP market size worldwide by region 2014-2024	2
Figure 2.	2017 Gartner Magic Quadrant for Unified Communications	4
Figure 3.	Biggest UC Vendors in 2018	5
Figure 4.	Sample SIP session	10
Figure 5.	The major components of VoIP	11
Figure 6.	Features of VoIP software	12
Figure 7.	VoIP Benefits and Disadvantages	13
Figure 8.	Sources of VoIP Vulnerability	15
Figure 9.	VoIP Vulnerability Components	16
Figure 10.	Call volumes during a TDoS attack	21
Figure 11.	2017 Global Fraud Loss Survey, Fraud Method Definitions	23
Figure 12.	2017 Global Fraud Loss Survey, Fraud Type Definitions	23
Figure 13.	The SecureLogix Anatomy of Automated TDoS	24
Figure 14.	Bypassing firewall filters by using VLAN hopping	24
Figure 15.	Visualising the Art of Mobile Fraud	27
Figure 16.	Cisco Security Control Framework (SCF) Model	34
Figure 17.	NSIT Cybersecurity Framework Core	35
Figure 18.	NSIT Cybersecurity Framework Core Activities	36
Figure 19.	Benefits of Implementing an Information Security Management	38
Figure 20.	Qualitative Data Tag Cloud	49
Chart 1.	How widespread is the use of VoIP technologies in workplaces	51
Chart 2.	Organisations moving to Unified Communications solutions	52
Chart 3.	What do you know about communications fraud	54
Chart 4.	Concerns about communications fraud	54
Chart 5.	Biggest challenges or concerns in relation to Information Security	55
Chart 6.	Is communications fraud a board level concern	57
Chart 7.	How highly do you rate privacy as a communications issue	58
Chart 8.	Experienced any type of communications fraud or security breach	59
Chart 9.	Risk Mitigation Strategies	61

Jun-18

---

## Abbreviations

ACK	Acknowledge
CIO	Chief Information Officer
CSP	Communications Services Provider
DOS	Denial of Service
DDOS	Distributed Denial of Service
DPC	Data Protection Commissioner
ICO	Independent Commissioners Office
ICT	Information Communications Technology
IP	Internet Protocol
MSSP	Managed Security Service Providers
PABX	Private Automated Branch Exchange
PBX	Private Branch Exchange
POTS	Plain Old Telephone Service
PSTN	Public Switched Telephone Network
SBC	Session Border Control
SIP	Session Initiation Protocol
SOC	Security Operations Centre
SYN	Synchronize
TCP	Transmission Control Protocol
TDoS	Telephony Denial of Service
UC	Unified Communications
UCaaS	Unified Communications as a Service
VoIP	Voice Over Internet Protocol

## 1 Introduction

This chapter introduces the topic of IP communications and provides a brief overview of the key technologies underpinning and contributing to modern telecommunications networks. It describes how Voice over Internet Protocol (VoIP) and Unified Communications (UC) are becoming ever more popular as a modern means of communication for voice and messaging applications. The chapter concludes by presenting the research objectives, scope and beneficiaries of the study.

### 1.1 IP Telecommunications History

Early telecommunications technology evolved from traditional rudimentary analog systems in the 1960s known as Plain Old Telephone Service (POTS) and Public Switched Telephone Networks (PSTN), to digital telephone networks known as Private Branched Exchanges (PBX). This evolution continues today with the migration of legacy analog and digital telecommunications to modern on premise and cloud-based internet protocols, including the unified convergence with computer networks. *'Voice over Internet Protocol (VoIP) has been popular in the telecommunications world since its emergence in the late 90s, as a new technology transporting multimedia over the IP network, and that today people commonly make phone calls with IP phone or client software (such as Skype or iChat) on their computer or send instant messages to their friends'* (Park 2009, p. xvii).

According to Flanagan (2012, p.1) *'Packet voice, Voice over IP and Unified Communications (UC) technologies are remaking telephony in a fundamental way that hasn't been seen since the 1960s'*. Unified Communications is a term used to describe the growing popularity of converged communications e.g. telephony, video conference calling, messaging, client applications etc. This term is often used interchangeably with Unified Communication Solutions (UC Solutions). In contrast, VoIP is an IP telephony service and thus essentially classed as separate product, however VoIP is a default element of Unified Communications given voice it is an integral component of any such Unified Communications solution.

Gartner (2017) states that *'All Unified Communications (UC) solutions are intended principally to improve user productivity and enhance business processes that relate to communications and collaboration'* Gartner defines UC solutions — equipment, software and services — as offerings that facilitate the use of multiple enterprise communications methods to achieve those aims. UC solutions integrate communications channels (media), networks and systems, as well as IT business applications and, in some cases, consumer applications and devices. (Gartner 2017)

Unified Communications are an attractive proposition for today's organisations as UC solutions present opportunities for organisations to reduce costs by enabling the consolidation of communications infrastructure such as phone, faxes, email, and video conferencing facilities. Tipping (2014, p.5) mentions *that 'one of the many benefits of an IP-based UC system is that it can be widely distributed across internal and external IP networks, greatly improving communications and collaboration. This allows employees to stay connected when geographically distant from the office, whether on business travel or working from home. This type of platform also allows companies to reduce their costs, deliver high quality voice and video, and enable more features; but it does come with some risk'*. There are unfortunately

some risks involved with Unified Communications. For example, Tipping (2014, p.5) states that the distributed and heterogeneous nature of Unified Communications which traverse disparate public and private networks results in the creation of many entry points for IP based attacks.

Therefore, organisations should approach VoIP cautiously when considering deploying a VoIP solution on their networks due to the serious security issues that can arise from integrating many network elements with voice and existing data networks. These security issues are often compounded by the fact that many traditional security devices such as firewalls and encryption protocols are not adequately equipped to protect VoIP services or networks from sophisticated threats (Park 2009). This shall be discussed in further detail in the following chapter (Literature Review).

### 1.2 Global VoIP market size worldwide by region 2014-2024

According to Ameri Research, the global Voice over Internet Protocol (VoIP) market was valued at \$43.3 billion in 2016 and is forecast to grow at a robust compound annual growth rate of 10.2% between 2017 and 2024, culminating to global revenues of \$93.9 billion by 2024. (Ameri Research 2017, Online)

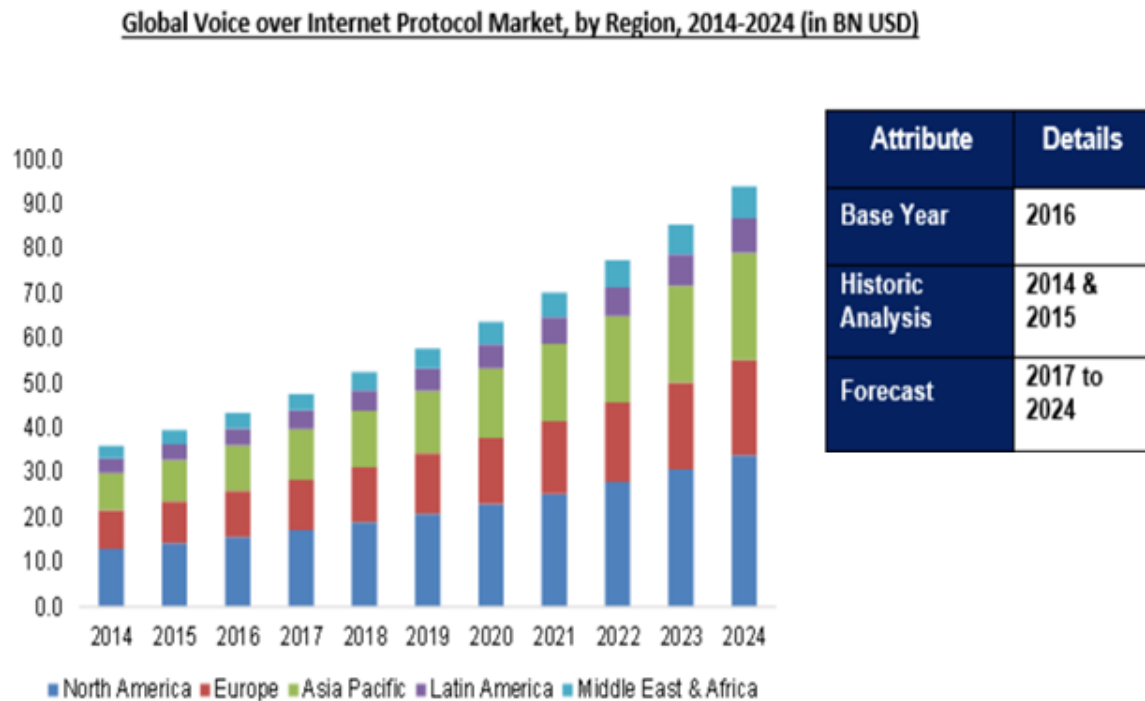


Figure 1. Global VoIP market size worldwide by region 2014-2024 (Ameri Research 2017, Online)

Figure 1 shows the estimated size of the global Voice-over-IP (VoIP) market worldwide and its forecasted growth by region, from 2014 to 2024. Ameri Research is a US based market research company. The above data is based on secondary sources and was also gathered by quantitative research which sampled a large number of industry players.

### 1.3 Main VoIP / UC Vendors

The following section outlines the current market leading vendors in VoIP and Unified Communications solutions. As the emphasis of this research is the corporate environment, this section only looks at on premise (solutions installed on customer sites/infrastructure) and cloud-based services.

#### 1.3.1 On premise UC solutions providers

Gartner state that *'UC applications are increasingly being integrated with, or offered in concert with, collaboration applications to form Unified Communications and collaboration (UCC) solutions. In some cases, they are being integrated with business applications and workflows, or are being targeted at vertical user groups.'* (Gartner 2017)

It is useful to divide UC into six broad communication product areas:

1. **Telephony** — This area includes fixed, mobile and soft telephony, as well as the evolution of PBXs and IP PBXs. This category includes options for voice and video that bypass traditional connectivity methods such as direct internet-based connections.
2. **Meeting solutions** — This area includes multiparty voice (audio) conferencing, videoconferencing, web conferencing (including document- and application-sharing capabilities), and various forms of unified meeting capabilities and infrastructure
3. **Messaging** — This area includes email, which has become an indispensable business tool, voice mail and various approaches to unified messaging (UM).
4. **Presence and instant messaging (IM)** — IM enables individuals to send textual and other information to individuals or groups in real time. Presence services enable individuals to see the status of other people and resources.
5. **Clients** — Unified clients enable access to multiple communication functions from a consistent interface. They may take different forms, including thick desktop clients, thin browser clients and clients for mobile devices (such as smartphones and tablets), as well as specialized clients embedded in business applications.
6. **Communications-enabled business processes** — The ability to integrate a UC solution with other business and communications applications creates significant value for users. An example is the integration of UC with field service or purchasing applications.

The above list is sourced from Gartner's Magic Quadrant for Unified Communications (Gartner 2017)

### Gartner Magic Quadrant for Unified Communications



Source: Gartner (July 2017)

Figure 2. Gartner Magic Quadrant for Unified Communications (Gartner 2017)

Figure 2 shows the key players in the Unified Communications market (for on premise solutions) and categorises these into four distinct categories. These are:

*Leaders* – recognised as having a full UC product/service offering and demonstrated success in the market

*Challengers* – have UC product/service capabilities with potential to become market leaders but may lack experience in certain areas or markets

*Visionaries* – offer alternative approaches to UC but are limited by experience and/or capabilities to deliver and compete against market leaders

*Niche Players* – specialise in specific areas of UC but lack full product/service offerings and market reach

### 1.3.2 Cloud based UC solutions providers

Cloud based Unified Communication solutions are commonly known as *Unified Communications as a Service (UCaaS)*. The following graph shows the top 5 UC vendors in the market by gross income as opposed to profit. It should be noted that these earnings are the vendors gross income, not just the earnings from UC products or services. That said, the graph below highlights that 4 out of the top 5 vendors are cloud/software companies as opposed to traditional telecoms providers and this can be viewed as an indication of the increasing trend of voice communications convergence with IP networks indicating a shift from traditional telecoms providers to pure software/cloud-based providers.

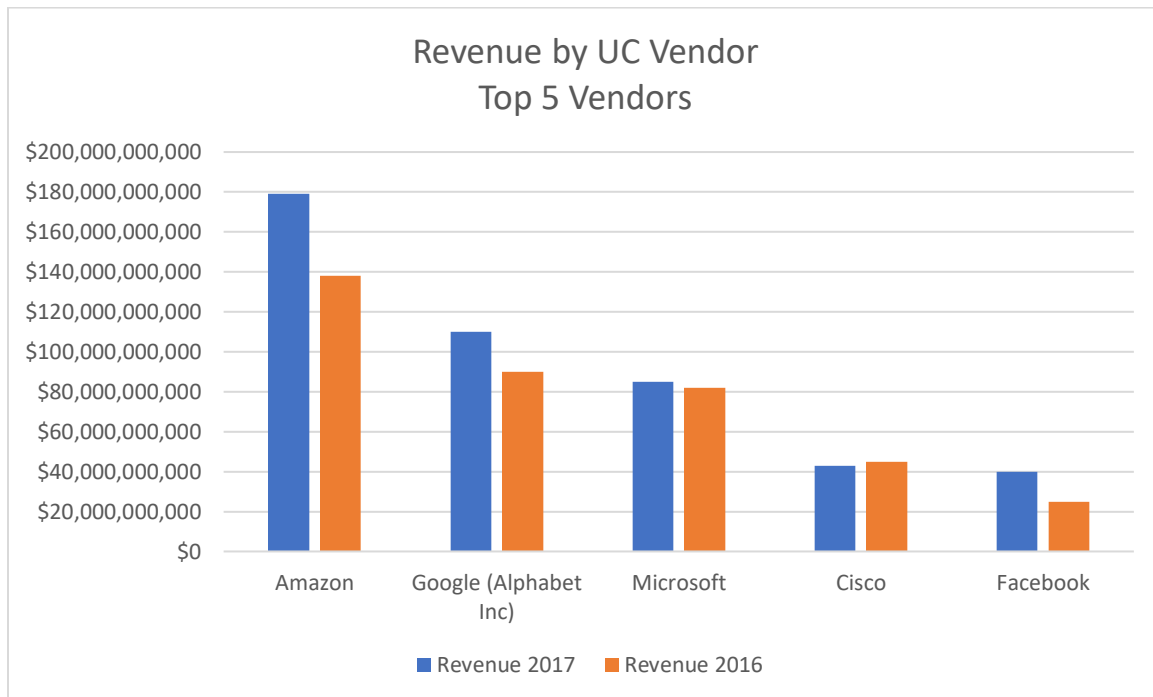


Figure 3. Biggest UC Vendors in 2018 (UCToday.com 2018, Online)

## 1.4 Cloud vs On Premise VoIP/UC Solutions

The advent of increasingly converged IP communications and how these services are implemented presents today's organisations with many options in terms of how they wish to design and implement their IP communications within their organisation. The most common deployment approaches organisations can choose from are as follows:

### 1.4.1 On Premise

On premise VoIP or UC solutions involve deploying the chosen VoIP or UC solutions on the organisations own systems infrastructure and network. This approach is often found in larger enterprises that already have a significant ICT infrastructure in place and the relevant support teams to manage these systems. Going with an on premise solution enables an organisation greater control of how the system is deployed in terms of solution design and configuration. Organisations with stringent security requirements or concerns tend to favour on premise solutions for the reasons described above. However, these solutions are more expensive in terms of capital and operational expenditure due to the financial overhead associated with

procuring the required hardware and software and the resources (IT support) needed to run and maintain these systems.

#### *1.4.2 Cloud Solutions*

VoIP and UC solutions in the cloud are delivered by a managed service on infrastructure hosted in the vendor/service providers data centre. This type of service offering is common with smaller organisations as it enables organisations to get up and running on a VoIP or UC solution quickly and cost effectively, as all hardware, software and systems management is essentially outsourced to the managed service provided via the cloud. The only infrastructure required by the organisation is reliable internet connectivity to access the cloud services. Whilst this flexibility provides many tangible benefits for an organisation as outlined above, careful consideration should be given if security is a key requirement or concern given many cloud offerings are delivered via multi-tenant environments meaning the underlying networks and infrastructure are essentially shared with many other customers across a common platform.

#### *1.4.3 Hybrid Solution (On premise + Cloud)*

This approach offers the best of both worlds for organisations as it combines the flexibility of cloud based services with the assurance and resilience of an on-premise solution. This approach is often utilised by small to medium sized enterprises (SME's), right up to larger organisations that may already have significant on-premise VoIP or UC implementations but wish to harness the benefits of cloud services for their own particular business or end user requirements. Organisations that chose to take this approach still need to consider prudent security measures given that the hybrid approach involves connecting an organisations private network with a public cloud service. That said, many of today's cloud service providers have security built into their service offerings to ensure customer communications are appropriately secured. This is usually achieved in the form of securing customer endpoints with end-end encryption and setting up Virtual Private Networks (VPN's) between the customers network and the cloud service providers network to create a secure tunnel for communications.

### **1.5 Research Objectives**

The aim of this research is to understand what security concerns organisations face when securing their Voice Over IP (VoIP) communications infrastructure and what solutions exist to mitigate such concerns. It shall also look at the increasing growth in VoIP and Unified Communications and the level of risk posed to these technologies by two of the most common threat vectors that exist today, these are communications toll fraud and telephony denial of service (TDoS) attacks.

This dissertation will examine the current global market for secure VoIP communications and ascertain the current level of threats and risks to communications integrity including possible solutions and risk mitigation strategies for same. The study aims to answer the following research questions,

1. Gain an understanding of the size of VoIP communications market globally
2. Gain an understanding of how serious Toll Fraud and TDoS are in industry today
3. Gain an understanding of the organisational impacts of Toll Fraud and TDoS



4. Ascertain what the typical organisational security posture is regarding VoIP communications and security
5. Ascertain if Fraud and TDoS is seen as a Board level problem

### **1.6 Scope of the Study**

This study looks at the current security posture of VoIP technologies and Unified Communications systems in today's corporate environment and the security challenges associated with same. While the research will cover Unified Communications in general, it is intended to focus on VoIP communications in particular and the security threats posed by Toll Fraud and TDoS in the context of an organisations corporate environments.

### **1.7 Beneficiaries of Study**

This study is aimed at ICT professionals with responsibility for managing corporate IT and Unified Communications systems. It is envisaged Chief Information Officers, Product Managers, IT Managers and Systems Administrator's would also gain an improved understanding of the following,

1. How pervasive Toll Fraud and Telephony Denial of Service (TDoS) attacks are in today's modern forms of voice over IP (VoIP) communications.
2. How popular corporate VoIP systems and applications can be compromised for criminal gain and malicious intent.
3. The security implications for converged communications and potential impacts on the corporate environment.
4. Real life examples and case studies of Toll Fraud and TDoS attacks on institutions and commercial enterprises including how and why these occur.
5. What are the ethical and legal implications of compromised Unified Communications solutions and services.

## **1.8 Chapter Roadmap**

The purpose of this section is to provide the reader with a clear roadmap of how this dissertation is structured including a description of the key chapters contained within.

### *Chapter I: Introduction*

This chapter provides an overview and background on the chosen topic, research question and intended target audience including a chapter roadmap describing how this dissertation paper is structured.

### *Chapter II: Literature Review*

This chapter describes what VoIP technology and Unified Communications are, how these are used today, and the security challenges and risks associated with their usage. This chapter looks at the current research and publications from leading experts in the marketplace and academic sources while providing a review and summary of this data.

### *Chapter III: Methodology and Fieldwork*

This chapter outlines the methodology used to undertake this study while acknowledging any strengths and weakness with the chosen approach and the rationale for same.

### *Chapter IV: Findings and Analysis*

This chapter outlines the results of the study obtained via primary and secondary research, and from interviews with the selected subject matter experts on the chosen topic, which are comprised of ICT professionals working in the relevant industry fields i.e. ICT, Information Security and Telecommunications.

### *Chapter V: Conclusions and Future Work*

This chapter provides a discussion of the research question and related key objectives including an outline of the key security issues and concerns pertaining to current and future developments of VoIP technologies for both consumer and business applications.

## **1.9 Research Timeframe**

This research study was conducted between October 2017 and May 2018. The Literature Review was completed between October 2017 and March 2018. Approval for the semi-structured interviews was granted by the TCD Research Ethics committee in March 2018. Semi structured interviews were conducted in March and April 2018. The analysis of the data was conducted from April 2018 to May 2018.

## 2 Literature Review

### 2.1 Introduction

The purpose of this dissertation is to ascertain how prevalent fraudulent and malicious activities are regarding VoIP and Unified Communications technologies in the Information and Communications Technology (ICT) sector. It is therefore necessary to gain an understanding of the size and scope of the problem while identifying possible solutions and mitigation strategies for businesses and its end users. This chapter describes what VoIP and Unified Communications are and looks at the current vulnerabilities and previous security issues with these technologies as context for the research question. Legal and data protection implications for VoIP and Unified Communications shall also be explored given the timely introduction of new EU legal directives on data protection in the form of General Data Protection Regulation (GDPR), which will come into force on the 25th May 2018. The migration of modern telecommunications to cloud based internet protocols and their convergence with computer networks presents many risks and challenges for organisations in today's marketplace. Researchers contend that these risks are expected to worsen as this VoIP and Unified Communications migration trend continues. This is mainly due to the lack of strong built in security mechanisms and the use of open standards in existing IP-based networks. (Akhga and Arabnia 2014, p. 359). These risks and challenges will be discussed in further detail in section 2.6 *VoIP Vulnerabilities*.

At its most basic, the 3 main uses for VoIP irrespective of business or consumer context is typically,

1. Computer to Computer calls
2. IP phone to IP phone (aka Softphones)
3. IP phone to PC to PSTN

### 2.2 VoIP Overview

#### 2.2.1 What is VoIP

VoIP is a technology based on Internet Protocol (IP) that enables voice communications over traditional computing systems and software applications. Popular messaging applications such as Skype, WhatsApp, Viber all run over VoIP technology. These applications are used in both consumer and business contexts. VoIP is also commonly defined as:

*'VoIP enables the users to use the Internet as the transmission medium for voice communication'* (Singh, H. P., et al. 2014, p.336)

In parallel to using IP protocols to transfer voice and data, VoIP technologies also require underlying signalling protocols for effective end to end communications management. Whilst there are numerous signalling protocols in existence today, the Signal Initiation Protocol (SIP) is one of the most common protocols used today due to its low overhead and simple implementation. SIP is *'also the latest version of signalling*

and has dominated development work since about 2000' (Flanagan 2012, p.78). One definition of SIP is:

*'an application-layer control (signalling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences.'* (Rosenberg, J., et al. 2002. p.9)

A more recent definition by Ghafarian et al. (2016) describes SIP as *'an application-layer signalling text-based protocol used for establishing or terminating a session between two or more partners using VoIP system'*. (Ghafarian et al. 2016. p.1032)

Akhga and Arabnia (2014, p. 360) mention that *'Session Initiation Protocol (SIP) has rapidly gained widespread acceptance as the signalling protocol of choice for fixed and mobile Internet multimedia and telephone services. SIP is an application layer control protocol that allows users to create, modify, and terminate sessions with one or more participants. It can be used to create two-party, multiparty, and multicast sessions that include Internet telephone calls, multimedia distribution, and multimedia conferences'*.

### 2.2.2 Sample SIP Session

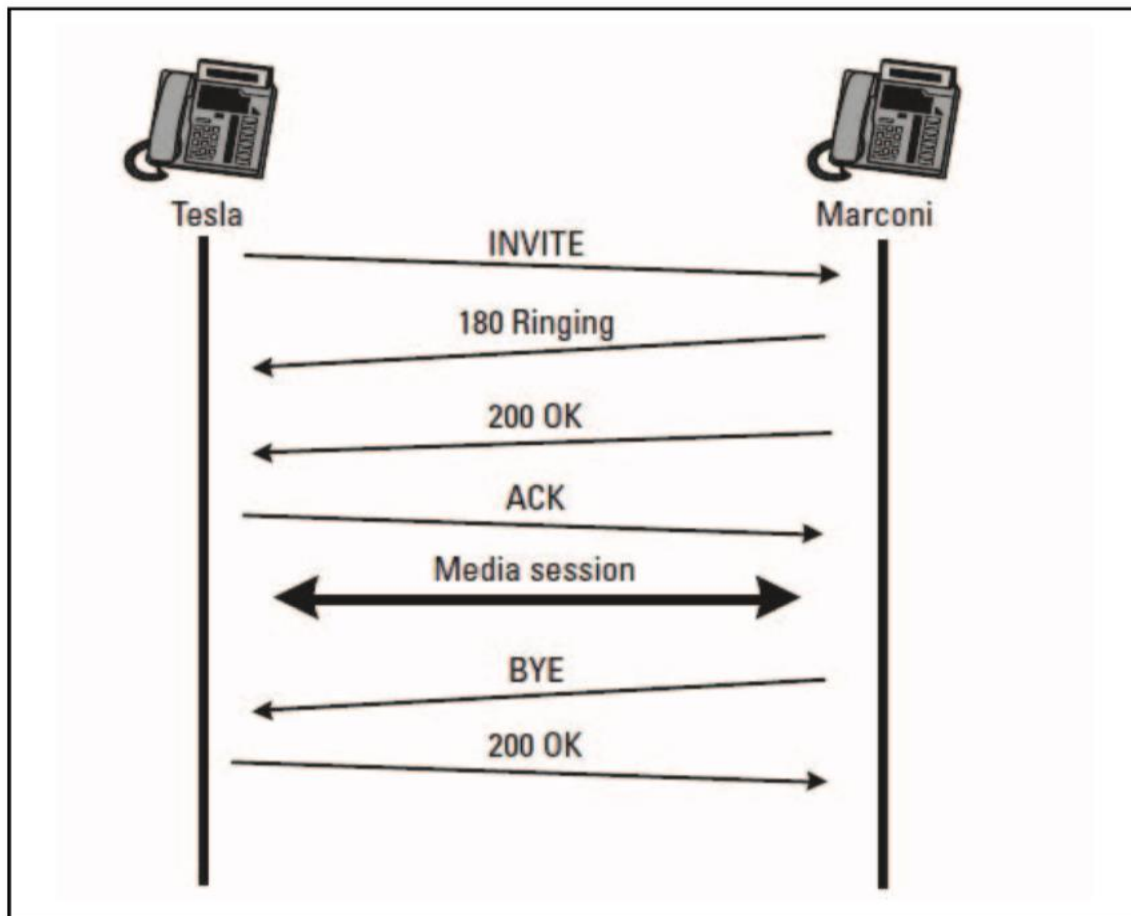


Figure 4. Sample SIP session (adapted from Ghafarian et al. (2016). "An Empirical Study of Denial of Service (DoS) against VoIP.).

Ghafarian et al. (2016. p.1032) mentions that, 'According to RFC 3261 [14] there are six types of SIP messages: INVITE, ACK, BYE, CANCEL, REGISTER, and OPTIONS. Figure 3 illustrates a sample of SIP INVITE request. The INVITE contains the details of the type of session that is requested. It could be a simple voice session, a multimedia session such as a video conference, or a gaming session.' (Ghafarian et al. 2016. p.1032)

In figure 4 above 'Tesla sends an INVITE message to the Proxy Server. The server in turn either sends it directly to Marconi or checks the database for the next hop. Once the request reaches the destination, the equipment rings and Marconi sends 200 ok indicating that the acceptance of the call and the session initiation is then finalized by Tesla sending an ACK message back to Marconi. After finishing the session, Marconi ends it by sending a BYE message to Tesla.' (Ghafarian et al. 2016. p.1032)

### 2.3 Main Components of VoIP

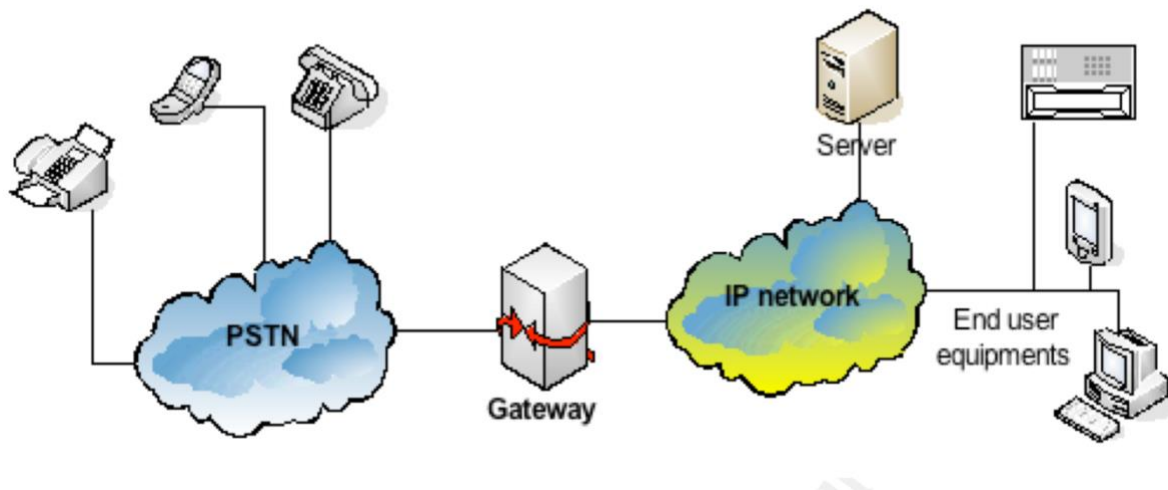


Figure 5. The major components of VoIP (Xin, J. 2007. p.7)

The figure above shows the main components that comprise of a basic VoIP solution, these are described as follows,

- An end user desk or soft (IP) phone or workstation running VoIP software (Cisco, Skype etc.)
- A Public Switched Telephone Network (PSTN) which is a switching network enabling users to make calls
- A VoIP Gateway which is a device that acts as a bridge between conventional telephone networks and VoIP telephone networks

## 2.4 Key Features of VoIP software

The following table summarises the key features of some common VoIP software on the market today.

Features of VoIP software.

VoIP software	Protocol support	Encryption	Other capabilities	License
Skype	Proprietary P2P protocol	Yes	Conferencing, video, file transfer, voicemail, Skype to phone, phone to Skype, additional P2P extensions (games, whiteboard, etc.); depending on the platform	Freeware/closed proprietary
Gizmo	SIP, extensible messaging and presence protocol (XMPP)	Secure real-time transport protocol (or SRTP)	Record calls, forward calls, MSN IM, windows live talk, Google Talk, Talk with Yahoo, Messenger, XMPP	Freeware/closed proprietary
GoogleTalk	Extensible messaging and presence protocol (XMPP)	ZRTP (Z-real-time transport protocol)	Video, chat, file transfer, voicemail, mail via "GMail Integration"	Closed proprietary
Cisco IP communicator	Skinny call control protocol (SCCP or skinny), SIP, trivial file transfer protocol (TFTP)	Secure real-time transport protocol (or SRTP)	Call recording, silent monitoring, multiple lines and directory numbers, configurable speed dial, calling name and number display, call waiting, call forward, call transfer, three-way calling (conference), call park, call pickup	Closed proprietary
KPhone	Session traversal utilities for NAT (STUN), SIP, name authority pointer (NAPTR)	Secure real-time transport protocol (or SRTP)	Video, voice, IM, external sessions, IPv6 support for UDP	GPL/free software
Vbuzzer	SIP	Transport layer security (TLS)	IM (MSN), voicemail, personalized voice greeting	Freeware/closed proprietary
X-Lite	SIP, STUN, interactive connectivity establishment (ICE)	No	IM, single login account, for Windows and Mac also conferencing, video and SIMPLE based presence	Freeware/closed proprietary
Yahoo! Messenger	SIP (using TLS) and RTP (media)	Unknown	Video, file transfer, PC to phone, phone to PC	Freeware/closed proprietary
Phoner	SIP, telephony application programming interface (tapi), common ISDN application programming interface (CAPI)	TLS, SRTP, ZRTP	Conferencing, call redirection, call recording	Freeware/closed proprietary
Bria	SIP/SIMPLE, XMPP, STUN, ICE	TLS, SRTP	Voice and HD (1280 × 720p) video calling; multiple account integration; address book support (Mac and Windows); company chat rooms; USB support; troubleshooting assistant; workgroups; call recording and conferencing	Proprietary
iCall	SIP, (AOL instant messenger), AIM, ICQ, extensible messaging and presence protocol (XMPP)	TLS, ZRTP	Video, file transfer, PC to phone, phone to PC, IM (MSN, AIM, ICQ, Yahoo!, XMPP, Google Talk), voicemail	Freeware/closed proprietary
PhonerLite	SIP	TLS, SRTP, ZRTP	Conferencing, call redirection, call recording	Freeware/closed proprietary
3CX phone system	SIP	TLS, SRTP	Voice and video IP telephony, voice and videoconferencing, voice mail and instant messaging	Proprietary

Figure 6. Features of VoIP software (Singh, H. P., et al. 2014. p.371)

## 2.5 VoIP Benefits and Disadvantages

The following table summarises the key benefits and disadvantages associated with the use of VoIP software.

BENEFIT		DISADVANTAGE	
TYPE	DESCRIPTION	TYPE	DESCRIPTION
Cost savings	This is the most attractive feature of VoIP. This is due to voice traversing over the Internet or private networks, hence call charges for long distance/international calls are significantly reduced	Complicated Service / Network Architecture	Integration with rich media services (voice, video, IM presence) make it difficult to design the service and network architecture due to the plethora of different devices and protocols to support
Rich Media Service	Presence awareness (online, offline, busy) and ability to integrate with other media types e.g. instant message, video call, file transfer	Interoperability issues between different protocols, applications or products	VoIP vendor proprietary standards and protocols can differ and therefore create challenges with interoperability
Phone portability	No longer tied to a dedicated line like legacy phones, VoIP enables the user to use the same number anywhere as long as they have an IP connection	Quality of Service (QoS) issues	Ensuring QoS can be difficult due to the volatile nature of IP packets travelling over multiple disparate networks
Integration & Collaboration	VoIP protocols can integrate with many applications such as email, web and social networks	Security Issues	VoIP traffic can traverse public (open) networks and comprise of many network elements therefore posing significant risks to security
User Control Interface	Most VoIP applications provide users with feature rich customisations and personalisation	Emergency calls	Due to the flexibility and transient nature of VoIP it can be difficult to provision VoIP with emergency services like 911

Figure 7. VoIP Benefits and Disadvantages (adapted from Park 2009, pp. 6-9).

## 2.6 VoIP Vulnerabilities

The previous section explored the many advantages and disadvantages of using VoIP communications. This section looks at the many different vulnerabilities of VoIP and describes in detail the various methods of how VoIP communications security can be compromised.

Ghafarian et al. (2016, p. 1031) mentions that VoIP has become more widespread due to its low cost but also warns that the underlying open source signaling protocols such as Session Initiated Protocol (SIP) which transmit messages in unencrypted clear text can make VoIP prone to attack. Common attacks against SIP include eavesdropping, connection hijacking, call fraud and DoS attack.

Cadet and Fokum (2016, p.2) suggest that the deployment of VoIP is very complex since the application can work over the global Internet or corporate networks and that VoIP depends on many Internet technologies and protocols that are not designed with security in mind. This can result in VoIP technology being compromised by subverting many of these elements. Akhga and Arabnia (2014, p. 359) also suggest that *'the problem of detecting fraud in telecom in general and in Voice over IP (VoIP) in particular is very difficult'*. This is primarily due to the sheer volume of VoIP traffic generated on the network and the plethora of different and ever changing fraud methods and attack vectors available to malicious actors. In order to proactively identify and mitigate fraudulent activity every event and VoIP packet on the network must be inspected to ascertain and distinguish between genuine (aka valid) and fraudulent or malicious traffic.

Park (2009, p.15) describes two main types or categories of VoIP vulnerabilities, the first coming from the underlying network infrastructure that VoIP applications reside on i.e. network, operating systems and web servers. The other type of vulnerability comes from the VoIP protocol and associated devices such as the IP phone, voice gateways, media controllers and signalling controllers.

Peter Cox, CEO of UM Labs R&D, a pioneer and leader of security software services for real-time communications, suggested the following when describing VoIP vulnerability during a webinar on VoIP Security: Threats & Trends in 2009:

*'VoIP applications and protocols suffer from a broader range of vulnerabilities than IP applications, those applications have a higher potential impact, and a successful attack have a higher and more immediate cost.'* (Peter Cox 2009, Online)

This is because common IP applications such as web and email are normally secured with standard security protocols such Hyper Text Transfer Protocol Secure (HTTPS) and Secure Socket Layer (SSL) to encrypt communications transmission. In contrast, VoIP communication is more complex to secure given the many protocols it relies on i.e. SIP, H.323 etc.

Flanagan (2012, p.175) also mentions that *'as part of a data network, VoIP servers may succumb to a denial of service attack, eavesdropping and data theft. Examination of the vulnerabilities in a VoIP system confirms that it has many more potential problems than a circuit switched PBX. To protect the system, prevent fraud, and ensure availability of phone service a VoIP solution must include a serious concern for security.'* Flanagan further postulates that *'implementing a VoIP or UC system that communicates with locations outside its offices on the Internet opens an organisation to many potential violations of HIPPA,*



*Sarbanes-Oxley, credit card, and other regulations that may carry significant penalties as well as embarrassment at disclosure of customers data loss* (Flanagan 2012, p.175).

The following diagrams in figures 8 and 9 present a high-level overview of the main characteristics, components and sources of VoIP vulnerabilities.

### 2.7 Sources of VoIP Vulnerability

The following diagram depicts the main characteristics and sources of VoIP vulnerabilities.

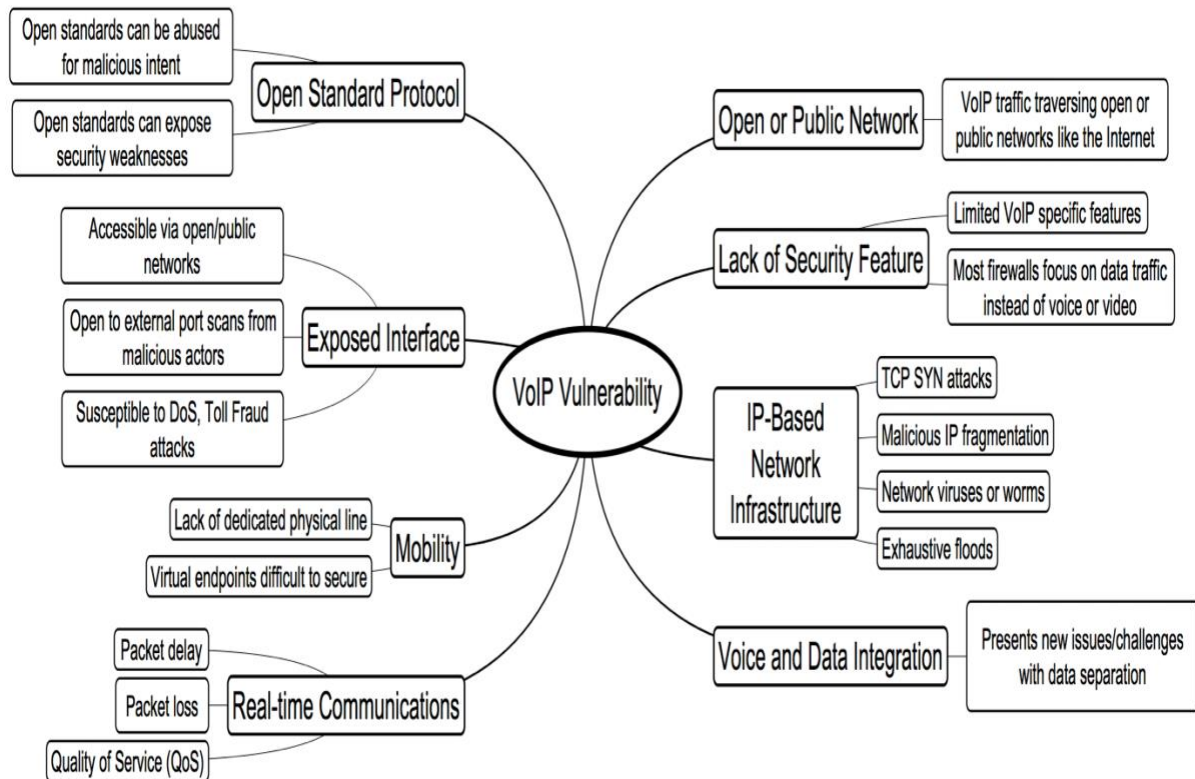


Figure 8. Sources of VoIP Vulnerability (adapted from Park 2009, pp. 10-11).

Figure 8 above is a graphical representation of the main characteristics and sources of known VoIP vulnerabilities broken out into the primary and secondary threat categories. It provides a holistic overview of the many attack vectors and methods available to a malicious actor to gain access to a VoIP system and compromise communications integrity. This holistic view can act as a useful reference for system administrators and solutions architects when designing and implementing a VoIP solution with security in mind.

## 2.8 VoIP Vulnerability Components

The following diagram depicts the main components in VoIP and their vulnerabilities.

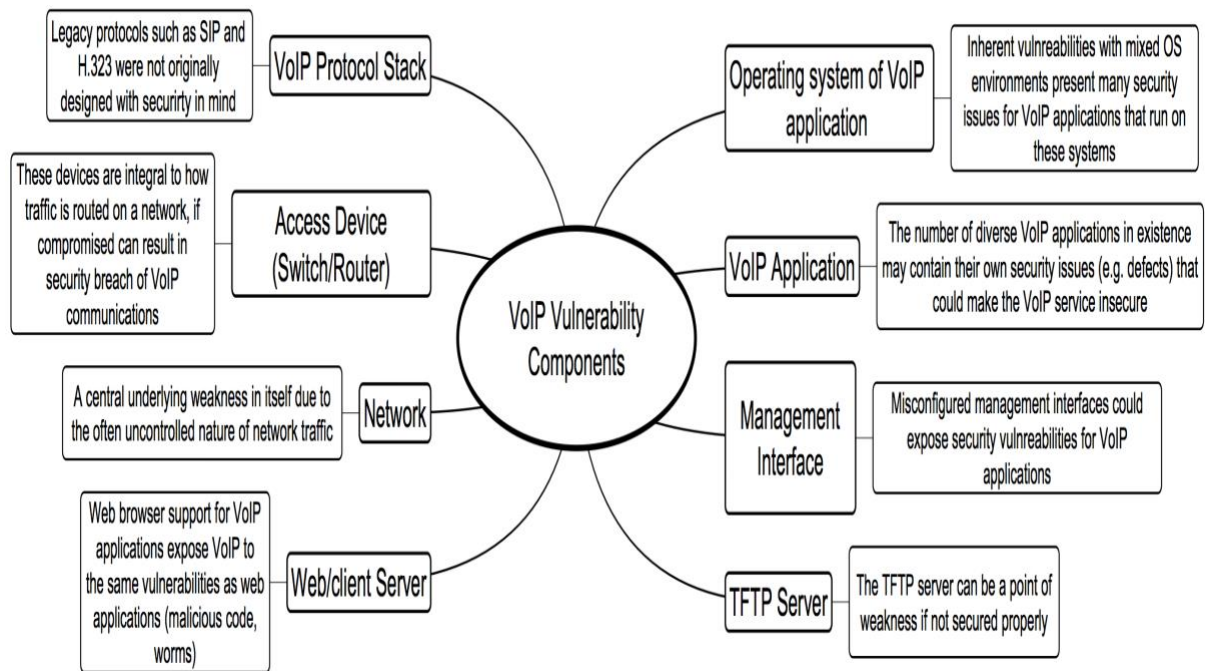


Figure 9. VoIP Vulnerability Components (adapted from Park 2009, pp. 12-13).

Figure 9 above is a graphical representation of the main components and dependencies that make up a standard VoIP solution and how these can be exposed to known vulnerabilities as highlighted in the previous section. In line with the previous section this figure is broken out into the primary and secondary vulnerability component categories. It provides a holistic overview of the many attack vectors and methods available to a malicious actor to gain access to a VoIP system and compromise communications integrity. This is a useful reference for system administrators and solutions architects when designing and implementing a VoIP solution with security in mind. It highlights the key network and application infrastructure that should be fully assessed and hardened from a security perspective.

## 2.9 VoIP Threat Taxonomy

The purpose of the VoIP Threat Taxonomy is to provide a high-level summary of the threats, measures and impact analysis whilst identifying possible mitigation strategies for same. It is not intended to be an exhaustive list of current and potential threats.

Park (2009) proposes categorising VoIP threats into the following key categories,

- Threats against **availability**
- Threats against **confidentiality**
- Threats against **integrity**
- Threats against **social context**

### 2.9.1 Threats against availability

These types of threats aim to disrupt the availability of a VoIP service which is typically expected to be available 24/7. *That is, the threat is aiming at VoIP service interruption, typically, in the form of DoS* (Park 2009, p.43). The typical threats against availability are as follows,

**Call flooding:** a common form of denial of service where an attacker floods valid or invalid heavy traffic to a target system.

**Malformed messages:** is when an attacker creates and sends malformed messages to the target server or client for the purpose of service interruption.

**Spoofed messages:** is when an attacker inserts fake (spoofed) messages into a certain VoIP session to interrupt the service or insert them to steal the session. The typical examples are “call teardown” and “toll fraud”.

**Call hijacking:** this can occur when some transactions between a VoIP endpoint and the network are taken over by an attacker.

**Server impersonating:** is when a VoIP client sends a request message to a server in the target domain for registration, call setup or routing.

**Quality of Service (QoS) abuse:** is where an attacker intervenes in the negotiation of media sessions between VoIP endpoints to deliberately degrade and abuse quality of service.

(Park 2009, pp. 20-30)

### 2.9.2 Threats against confidentiality

These types of threats relate to unauthorised access and capture of VoIP service credentials for subsequent unauthorised connections or other deceptive practices. The typical threats against confidentiality are as follows,

**Eavesdropping media:** two methods which are typically used by an attacker in VoIP is media packet sniffing (in the same broadcasting domain or media path as the target user) and compromising access devices (e.g. network switch).

**Call pattern tracking:** is the unauthorised analysis of VoIP traffic from or to any specific nodes or network so that an attacker may find a potential target device, access information (IP/port), protocol, or vulnerability of network.

**Data mining:** pertains to unauthorised collection of unique identifiers e.g. user name, password, phone number etc. and is often used for toll fraud and spam calls.

**Reconstruction:** means any unauthorised reconstruction of voice, video, fax, text or presence information after capturing the signals of media between parties. This method can be used for future attacks or deceptive practices.

(Park 2009, pp. 30-34)

### 2.9.3 Threats against integrity

These types of threats are aimed at undermining the integrity of a VoIP service thereby resulting in severe service impact. The typical threats against integrity are as follows,

**Message integrity (message alteration):** is the threat that an attacker intercepts messages in the middle of communication entities and alters certain information to reroute the call, change information or interrupt the service.

**Media integrity (media alteration):** is the threat that an attacker intercepts media in the middle of communication entities and alters media information to inject unauthorised media, degrade the QoS, or delete certain information.

(Park 2009, pp. 34-38)

### 2.9.4 Threats against social context

These types of threats tend to focus on manipulating the social context between communication parties so that an attacker can misrepresent himself as a trusted entity and convey false information to the target user (victim). The typical threats against the social context are as follows,

**Misrepresentation:** is the intentional presentation of a false identity, authority, rights, or content as if it were true so that the target user (victim) or system may be deceived by the false information.

**Call Spam (SPIT):** often referred to as spam over IP Telephony (SPIT) and is defined as a bulk unsolicited set of session-initiated attempts (e.g. INVITE requests), attempting to establish a voice or video communications session.

**Phishing:** is an illegal attempt to obtain somebody's personal information e.g. ID, password, credit card information etc. by posing as a trust entity in the communication. In VoIP, phishing is typically happening through voice or IM communication, and voice phishing is sometimes called vishing.

(Park 2009, pp. 38-43)

It should be noted that this VoIP Threat Taxonomy was first drafted back in 2005 by The Voice over IP Security Alliance (VOIPSA), an open, vendor-neutral organization. VOIPSA is made up of VoIP and information security companies, organizations, and individuals that have a desire to participate in project releases, strategy and other decisions. VOIPSA aims to fill the void of VoIP security related resources through a unique collaboration of VoIP and Information Security vendors, providers, and thought leaders.

This Taxonomy defines the many potential security threats to VoIP deployments, services, and end users.

Other VoIP researchers and authors such as Park (2009) have adopted many of the fundamental principles of this taxonomy to draft and build on their security publications and recommendations regarding VoIP communications security. Whilst this taxonomy is almost 10 years old and does not appear to have received many revisions since its initial publication in 2005, many of the threats and fundamental principles set out in the taxonomy are still

relevant to modern VoIP communications today and thus this taxonomy has contributed to developing security frameworks and best practice recommendations for VoIP communications security.

As per the research question, the primary VoIP threats this research study will focus on are Telephony Denial of Service (TDoS) and Toll Fraud. The rationale for focusing exclusively on TDoS and Toll Fraud is that these are the most common and high profile types of attacks targeting VoIP communications, examples of which will be discussed in further detail later in this chapter in section 2.11 *VoIP / UC Security Attacks*. The VoIP Threat Taxonomy categorises TDoS and Toll Fraud under the following headings,

#### Threats against *availability*

**Call flooding:** a common form of denial of service where an attacker floods valid or invalid heavy traffic to a target system. This is a primary method for TDoS / DDoS attacks which are specifically aimed at overwhelming a system to the point where it is no longer able to service requests, thereby essentially rendering the system or service unavailable for genuine traffic / service requests.

**Spoofed messages:** is when an attacker inserts fake (spoofed) messages into a certain VoIP session to interrupt the service or to steal the session. The typical examples are “call teardown” and “toll fraud”. This is a primary method for Toll Fraud attacks thereby enabling a malicious actor to generate revenue from fraudulent toll fraud calls.

#### Threats against *confidentiality*

**Data mining:** pertains to the unauthorised collection of unique identifiers e.g. user name, password, phone number etc. and is often used for toll fraud and spam calls. This is where a malicious actor can combine multiple methods i.e. *data mining + spoofed messages* to increase their potential of launching a successful toll fraud attack with the aim of generating revenue for the attacker.

Distributed Denial of Service (DDoS) in general will be covered in detail as DDoS and TDoS attacks share many of the same attack vectors, characteristics and objectives. TDoS and DDoS are effectively the same thing, the only difference being TDoS targets telephony/communications systems whereas DDoS mainly targets data networks and public facing systems like websites. These are described and discussed in further detail later in this chapter.

#### 2.9.5 *What is TDoS*

Telephony Denial of Service (TDoS) is a form of Denial of Service that specifically targets voice communications systems with the explicit intent of rendering communications systems incapacitated by overwhelming the system with floods of consecutive requests. It is also commonly defined as a Denial of Service attack:

*‘Denial-of-service (DoS) attacks aim to reduce the quality of the phone system, even to the extent of preventing users from making and receiving calls. Like DoS attacks on data networks, email systems or corporate websites, the perpetrators aim to flood voice services with unnecessary traffic’.* (Stanton R. 2006. p.12)

The Boston Regional Intelligence Center (BRIC), a law enforcement activity within the metropolitan Boston Homeland Security region, define TDoS as, *'TDoS attack results from the intentional generation of illegitimate phone traffic targeting a victim's phone systems. In many cases, the perpetrators of TDoS attacks leverage Voice Over Internet Protocol (VoIP) telephone equipment. TDoS attacks have the potential to significantly disrupt legitimate telephone call volume and as a result impact continuity of operations.'* (Mark Collier's VoIP/UC Security Blog 2013, Online).

It is mentioned that *'TDoS attacks generally employ fewer resources than the DoS attacks that are designed to cripple IT systems such as networks, servers, and software. At its most basic, all that a TDoS attack requires is an automated phone dialer that calls a target phone number and hangs up — over and over. That very simple concept can stop anyone else from getting through the line.'* (sTechAdvisory 2016, Online)

The practice of using automated phone dialers in a TDoS attack is commonly referred to as *Robocalling*, this essentially involves using an auto dialler to generate unsolicited calls to a target system with the intent of overwhelming the system (Simpson 2017).

Simpson's warnings regarding the potential threats TDoS can pose to emergencies services are not unwarranted, given that the City of Boston in the U.S. posted a public Cyber Threat Bulletin regarding a Telephony Denial-Of-Service Attack in one of its hospitals on 14<sup>th</sup> May 2013 (Mark Collier's VoIP/UC Security Blog 2013, Online).

Park (2012, p.128) also mentions that Denial-of-Service (DoS) attacks are the most common threat in VoIP networks due to the many different methods, attack vectors and sources an attack which can manifest on a target system. This is discussed in further detail in the following section.

### 2.9.6 Types of DDoS attacks

TDoS / DDoS attacks can take many different forms and use varying methodologies. Arbor Networks, a US company which provides network security and network monitoring solutions suggests the following as the most common DDoS methodologies in use today.

#### Volumetric Attacks

The primary objective of volumetric attacks is to consume the bandwidth of the target network/service and/or the link between this and other connected networks (i.e. internet). This is purely about congesting network bandwidth.

#### TCP State-Exhaustion Attacks

TCP state exhaustion attacks are primarily aimed at knocking out key network infrastructure such as core routers, firewalls and application servers thereby rendering network connections and services unusable.

#### Application-Layer Attacks

These types of attacks specifically target applications such as website or backend applications or databases with the intent of over exercising those application functions or services. These attacks are the most sophisticated and stealthy attacks because they can be very effective with as few as one attacking machine generating traffic at a low rate. This makes these attacks very difficult to proactively detect with traditional flow-based monitoring solutions. (Arbor Networks 2016, Online)

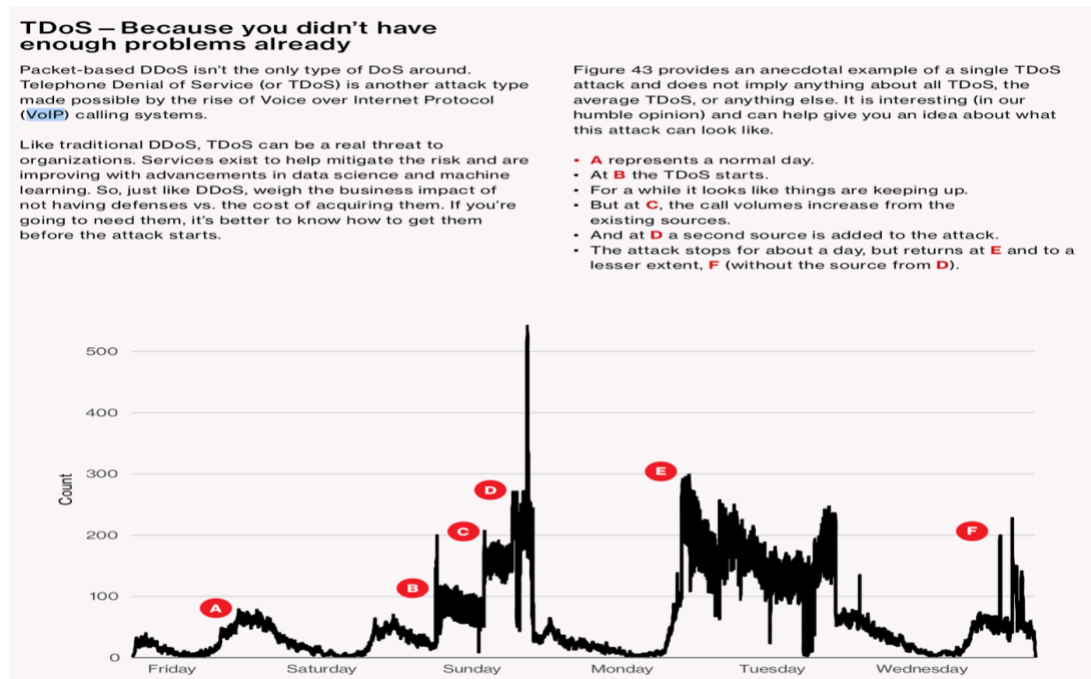


Figure 10. Call volumes during a TDoS attack (Verizon DBIR 2017, Online)

Figure 10. above depicts sharp rise in call volumes as a result of a malicious TDoS attack as denoted in a recent report on Data Breach Investigations by the US telecoms operator Verizon (Verizon DBIR 2017, Online).

### 2.9.7 What is Toll Fraud

Toll Fraud involves the unauthorised access and control of a telecoms system or service to avoid paying for telephone calls and/or for monetary gain. This essentially refers to the generation of a series of calls from a compromised host (victim) to premium high rate phone numbers. This type of fraud is also commonly referred to as International Revenue Share Fraud (IRSF) and Premium Revenue Share Fraud (PRSF).

*'This fraud involves artificially inflating traffic to a premium rate number.'* (Howells, I. et al. 2016. p.39)

The Communications Fraud Control Association (CFCA), a not for profit organisation working to combat communications fraud, define communications fraud as 'the use of telecommunications products or services with no intention of payment'. (CFCA 2017, Online). Fraud can also be described as an *'activity that leads to obtaining financial advantage or causing loss by implicit or explicit deception'* (Akhga and Arabnia 2014, p. 359).

Park (2009, p.26) suggests that Toll Fraud is one of the most common threats these days and one particularly associated with long distance and international calls.

In the context of Toll Fraud techniques, it is mentioned that *'the most common threat to VoIP systems is a hacker technique called "SIP Toll Fraud". Using this technique, a hacker (usually located in a region where law enforcement is lax) connects via the Internet to a VoIP PBX system (or to a SIP provider such as Vodacom) and "guesses" at a user code and password in order to successfully register as a remote extension. If the hacker is successful in registering, he can then make telephone calls as though he were actually inside the company premises. This hack does not give the hacker access to company data or anything else very useful, other than the ability to run up expensive telephone bills at the company's expense. The hacker will often make repeated calls to premium service numbers (again in countries where law enforcement is difficult)'*. (VBX Telecom 2013, Online). This type of fraud can enable an outside party access to a VoIP system with a PSTN connection to place calls to anywhere in the world. (Flanagan 2012, p.179).


There are two important distinctions that must be understood when discussing fraud: fraud methods and fraud types,

### 2.9.8 Fraud Methods

The CFCA describe fraud methods as 'how an attacker accesses the network or service to enable revenue to gain from an attack' (<http://www.cfca.org/fraudlosssurvey>, 2017, p.11)

The following provides a summary overview of the most common fraud methods found in 2017





## 2017 Survey

### Fraud Method Definitions:

Fraud Method	Description
Abuse of network, device or configuration weakness	Exploitation of a configuration weakness to gain access to a network or device; Includes VoIP equipment such as a modem or router.
Abuse of Service Terms and Conditions	Violation of the carrier's service terms and conditions or acceptable use policy.
Account Takeover	Manipulation and utilization of existing customer account in order to gain devices or service
Brand Name / Logo Abuse	Acquisition and use of a company's logo without permission
Clip-on Fraud	Stealing service by attaching wires to another customer's phone equipment
Dealer Fraud	All types of fraud conducted by indirect and 3rd party dealers
IMEI Reprogramming	Changing the IMEI of a handset to hide the true origination or identity of a caller
Internal Fraud / Employee Theft	Theft of service or equipment by employees; Also includes abuse of company's credit and adjustment policy
Mobile Malware	Compromised Mobile Applications
PBX Hacking	Compromised PBX systems used to make calls
IP PBX Hacking	Compromised IP PBX used to make fraudulent calls
Phishing / Pharming	Theft of personal info or credentials via hacking, phishing, vishing, etc...
Pre-Paid Equipment & Services	All types of fraud and abuse involving pre-paid equipment and services
Robocalling	Use of computerized auto-dialers to deliver pre-recorded messages to perpetrate fraud.
Signalling Manipulation	Manipulation of the SIP or SS7 signaling message to hide the true origination or identity of a caller
SIM Cloning	Duplicated SIM card used to charge phone calls back to the original SIM card
SMS Faking or Spoofing	Manipulation of the ANI to hide the true origination or identity of SMS or MMS
Social Engineering	Manipulation of an employee or customer to unintentionally give out important information
Spoofing (IP or CLI/ANI)	Manipulation of the IP address/CLI/ANI to hide someone's true origination or identity
Subscription Fraud (Application)	Creation of false details to gain access to goods and services with no intention to pay
Subscription Fraud (Credit Muling/Proxy)	Utilization of real identity details (with authorisation for payment) to obtain goods and services with no intention to pay
Subscription Fraud (Identify)	Utilization of a real identify without the owners knowledge to obtain goods and services with no intention to pay
Voicemail Hacking (Not associated with PBX Hacking)	Compromised voicemail system used to make calls
Wangiri (Call Back Schemes)	Call back fraud schemes
Payment Fraud	Utilization of stolen credit cards, debit cards or counterfeit checks in order to obtain service


**COMMUNICATIONS FRAUD CONTROL ASSOCIATION** 27

Figure 11. "2017 Global Fraud Loss Survey, Fraud Method Definitions" (CFCA 2017, Online)

### 2.9.9 Fraud Types

The CFCA describe fraud types as 'how an attacker uses the network or service to generate revenue from an attack' (<http://www.cfca.org>, 2017, p.11).

The following provides a summary overview of the most common fraud types found in 2017



## 2017 Survey

### Fraud Type Definitions:

Fraud Type	Description
Arbitrage	Exploitation of the differences in rates between different countries
Cable or Satellite	Signal theft or retransmission from a cable or satellite provider
Commissions Fraud	Schemes used by dealers to collect additional commissions and spiffs
Denial of Service (DoS) and Distributed Denial of Service (DDoS)	An explicit attempt to make a machine or network resource unavailable to the users of a service
Domestic Revenue Share (DRSF)	Abuse of Carrier Interconnect agreements through such things as Traffic Pumping, Switch Access Stimulation, 8yy Dip Pumping and CNAM Revenue pumping schemes
Device / Hardware Reselling	Resold equipment such as handsets, tablets, IPTV devices, routers...
Friendly Fraud	Utilization of Charge Backs, Returned Checks, Card Holder Not Present, etc... to perpetuate services
Interconnect Bypass (e.g. SIM box)	Unauthorized insertion of traffic onto another carrier's network. This includes Interconnect Fraud and GSM Gateway Fraud or SIM Boxing.
International Revenue Share Fraud (IRSF)	Artificial inflation of traffic terminating to international revenue share providers
Premium Rate Service	Artificial inflation of traffic terminating to premium service providers
Private Use	Use of a service neither directly nor indirectly paid for without rendering some kind of financial compensation
Service Reselling (e.g. Call Sell)	Resale of stolen phone services
Theft / Compromise of data (e.g. logins)	Includes such things as the acquisition of personal information or intellectual property
Theft / Stolen Goods	Equipment Theft
Theft of Content	Stealing content such as ringtones, games, or applications
Wholesale Fraud	Exploitation of wholesale interconnect agreements

**COMMUNICATIONS FRAUD CONTROL ASSOCIATION** 28

Figure 12. "2017 Global Fraud Loss Survey, Fraud Type Definitions" (CFCA 2017, Online)

The most common and serious fraud methods and fraud types classified under the umbrella term "Toll Fraud" are namely PBX, IP PBX hacking and Wangiri (call back schemes) which

are the most frequent methods used to conduct fraud types like International Revenue Sharing Fraud (IRSF) and Premium Rate Service Fraud. The primary reasons why these are so serious is due the financial losses that can be incurred by an organisation if their communications systems are compromised to conduct fraudulent calls to premium rate numbers. This is discussed in further detail in sections 2.11 *VoIP / UC Security Attacks* and 4.3.4 *Organisational Impacts of VoIP / UC Security Vulnerabilities*.

## 2.10 TDoS, VoIP Hacking and Toll Fraud

The following diagrams are simple depictions of TDoS, VoIP hacking and Toll Fraud examples.

*Anatomy of Automated TDoS*

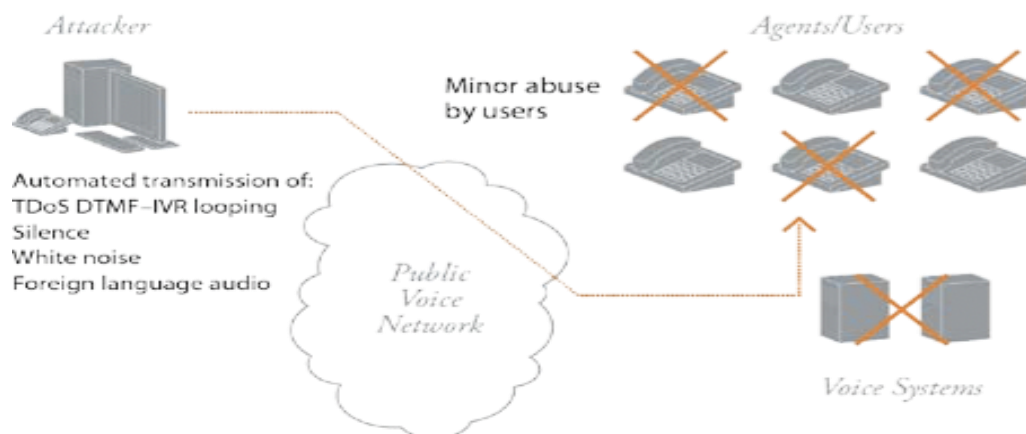


Figure 13. The SecureLogix Anatomy of Automated TDoS (SecureLogix Corporation 2017, Online)

Figure 13 above is a simple depiction as to how an attacker can utilise many forms of voice data (audio, white noise) to flood a VoIP system in a method attack method known as 'call pumping' (SecureLogix Corporation 2017, Online).

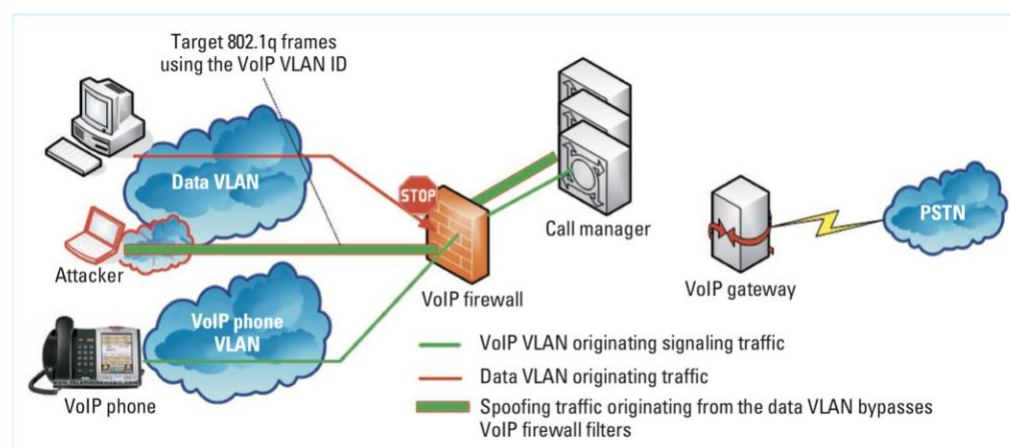


Figure 14. Bypassing firewall filters by using VLAN hopping, attackers can get past VoIP firewalls. (Thermos, P. 2009)

Figure 14 above depicts how an attacker can conceivably bypass common security firewalls by spoofing the mac address (unique identifier of a device) of another VoIP phone thereby

“impersonating” a genuine (aka valid) user thus enabling the attacker access into the VoIP infrastructure. (Thermos, P. 2009)

## **2.11 VoIP / UC Security Attacks**

The following outlines several real-life examples of recent publicly reported security attacks and attempted fraud in relation to denial of service and voice communications fraud.

### **German ISP Deutsche Telekom (2017)**

In 2017 the German ISP Deutsche Telekom was taken offline by a distributed denial of service attack that impacted close to 1 million customers on Deutsche Telekom’s network. A 29-year old British man who is only identified as “Daniel K.” was arrested Feb. 22 by the British National Crime Agency at the request of Germany’s Federal Criminal Police Office. Daniel K. pleaded guilty to masterminding the attacks that used Mirai malware to hijack routers, surveillance cameras and baby monitors and carry out denial of service attacks. (Threatpost.com 2017, Online)

### **Wangiri Phone Scam in Ireland (2017)**

Many of Ireland’s leading telecom operators experienced an unprecedented surge in the number of Wangiri premium rate call fraud in Q4 of 2017. The Irish Independent reported, “It would appear that all Irish mobile number ranges have undergone an unprecedented attack from this in recent weeks,” said a spokeswoman for Three, Ireland’s second largest operator. The scam is known as a ‘Wangiri’ call, because the mobile phone typically rings just once or twice. The scammers hope that people will automatically call back without looking too closely at the number. “The longer someone stays on the phone the higher the charge will be,” said a spokeswoman for Eir, previously known as Meteor. “This scam is a telecoms industry-wide problem.” (Irish Independent 2017, Online). Such was the extent of this scam, Ireland’s Commission for Communications Regulation (ComReg) was compelled to issue a consumer information bulletin on Scam Call Information advising consumers to be vigilant of scam calls (ComReg 2017).

### **Boston Globe hit by denial of service attacks (2017)**

In 2017 the Boston Globe was hit with a sustained DDoS attack which used a botnet to take down many of The Boston Globe’s website and internal systems. ‘As of Thursday afternoon, nobody knew who attacked the Globe network or why. Many DDoS attackers are never identified. Wade Sendall, the Globe’s vice president of information technology, said the first attack came around 3 p.m. Wednesday. “We think it was a probe,” he said, aimed at testing the Globe network’s defences and figuring out the best ways to get past them. Even so, the probe repeatedly disrupted the newspaper’s telephones and the editing system used to prepare content for print and online editions. The attacks resumed around 11 a.m. Thursday, making it impossible for many Globe employees to do their jobs and rendering bostonglobe.com inaccessible for many readers. By mid-afternoon, Globe technicians and specialists from the company’s Internet provider had set up effective defences’ (The Boston Globe 2017, Online). While there was no indication this was a DDoS attack specifically aimed the Globe’s telephony/communications systems (i.e. TDoS), it’s a prime example of how a typical DDoS attack can disrupt an organisations communications infrastructure.

### **How a Dorm Room Minecraft Scam Brought Down the Internet (2016)**

2016 saw one of the most sophisticated and severe denial of service attacks that resulted in significant widespread impact to internet traffic. Originally, prosecutors said, the defendants hadn't intended to bring down the internet—they had been trying to gain an advantage in the computer game Minecraft by knocking out traffic to popular Minecraft servers and stealing customers from the competition. The DDoS attack in question later became known as the Mirai botnet attack. Wikipedia define a botnet as 'a number of Internet-connected devices, each of which is running one or more bots. Botnets can be used to perform distributed denial-of-service attack (DDoS attack), steal data, send spam, and allows the attacker to access the device and its connection. The owner can control the botnet using command and control (C&C) software. The word "botnet" is a combination of the words "robot" and "network". The term is usually used with a negative or malicious connotation.' (Wikipedia 2018, Online). 'Mirai shocked the internet—and its own creators, according to the FBI—with its power as it grew. Researchers later determined that it infected nearly 65,000 devices in its first 20 hours, doubling in size every 76 minutes, and ultimately built a sustained strength of between 200,000 and 300,000 infections' (Wired 2017, Online).

### **Europol Dismantle Serious Cybercriminal Group (2015)**

In 2015 the European Union law enforcement agency (Europol) helped Spanish police dismantle a serious cybercriminal group operating a large scale international revenue share fraud (IRSF). IRSF is a form of toll fraud where criminals generate malicious calls to premium rate numbers for illegal revenue generations. Europol issued a press release which stated, 'Europol has supported Spanish police\* in an operation codenamed Walker, to take down a serious cybercriminal group during a coordinated action in Barcelona. With on-the-spot support from Europol, the action in Spain on 6 July resulted in the arrest of nine suspects, the dismantling of a sophisticated illegal call centre, six house searches and the seizure of numerous pieces of evidence; over 100 mobiles phones and stolen SIM cards, more than EUR 10,000 in cash, credit cards, computer equipment and other devices were taken away for further forensic examination.' (Europol 2015, Online). Europol confirmed that 'The aim of this investigation was to target the cybercriminals and their accomplices who were involved in large scale telecommunication fraud as well as channelling and cashing-out the proceeds of their crimes. The criminals made fraudulent phone calls to premium service numbers set up and managed by other members of the criminal group based outside the EU. Each cybercriminal had their specialty and the group was involved in receiving mobile phones stolen from tourists in Spain, then harvesting and misusing the foreign mobile numbers (until they were blocked by the telecom operators in their countries), before then sending the money earned abroad.' (Europol 2015, Online).

### **Callback Scheme Used in International Revenue Share Fraud (2014)**

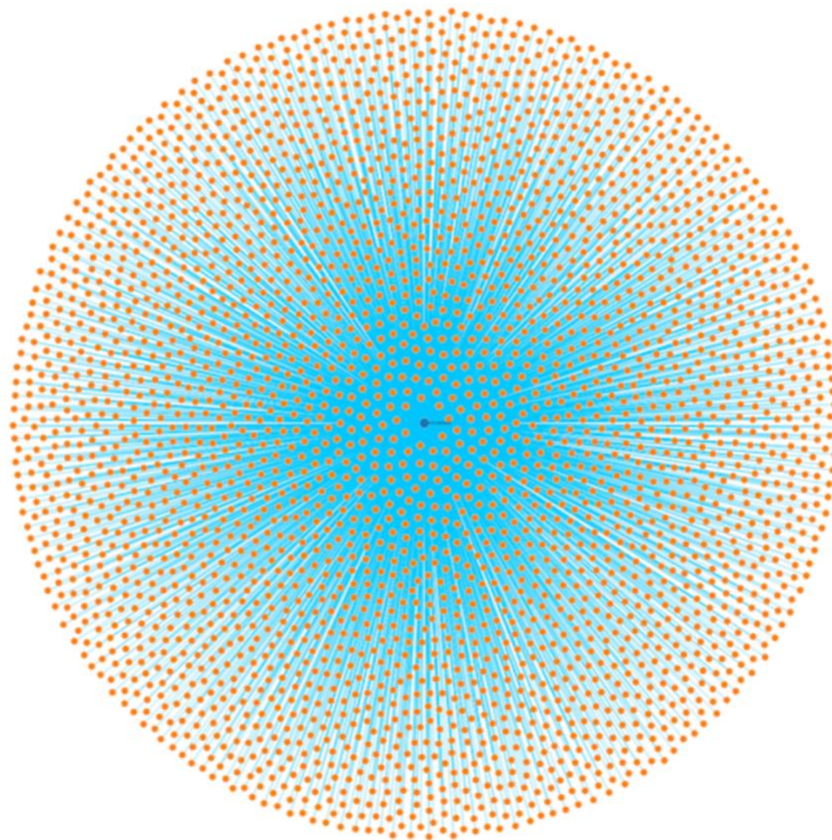
In another example of growth in International Revenue Share Fraud (IRSF), The Federal Bureau of Investigations (FBI) in the United States where compelled to issue a public service announcement in 2014 warning the public of the growing threat posed by IRSF. In their public service announcement, they stated, 'Telephone companies in the United States are seeing missed calls used to enable International Revenue Share Fraud (IRSF). Fraudsters are using call generators with automated spoofing capabilities to place calls to a large volume of US cell phone numbers. The calls typically ring once. The number displayed on the recipient's caller

ID is a high cost international number, usually located in the Caribbean. The recipient calls the number back and is greeted with a message designed to keep them on the line, such as “Hello, you have reached the operator, please hold.” The longer the caller stays on the line, the more revenue fraudsters generate.’ (FBI 2014, Online).

This type of attack was prevalent in Ireland last year (2017) with the Irish Times reporting that ‘Thousands of phone users across all the Irish mobile networks targeted in a telephone scam which sees fraudsters dialling from numbers in Liberia and Chad and immediately disconnecting in the hope those who are targeted will call back.’ (The Irish Times, 2018). This researcher has had previous first hand personal experience of a number of these types of fraudulent calls to his personal mobile phone.

## 2.12 Visualising the Art of Mobile Fraud

The following graph is an example of how big data can be used to present a visualisation of a mobile fraud attack. The attack in this example uses a fraud method known as the *Wangiri* fraud and is used in conjunction with the fraud type known as international share fraud.



**A Wangiri Attack: Blue Lines Are Calls from a Single Number in Cuba to Brazil**

Figure 15. Visualising the Art of Mobile Fraud Howells et al. (2016) p.14

Figure 15 above is a graphical representation of a *Wangiri* attack which shows how one malicious number in Cuba (the attacker) can generate malicious calls to thousands of target numbers (potential victims) in Brazil via a Robodialer as described earlier in this chapter.

Argyle Data Inc. describe a *Wangiri* attack as '*based on volume and probability. A robo-dialer calls thousands of numbers, hanging up after just one ring to show as a missed call, with the goal of getting unsuspecting victims to call the number back. In the case of international revenue share fraud, the calls come from a foreign country that has high connection fees.*' (Howells et al. 2016, p. 15).

## **2.13 General Data Protection Regulation**

The General Data Protection Regulation (GDPR) will come into force on the 25th May 2018, replacing the existing data protection framework under the EU Data Protection Directive.

The Irish Data Protection Commissioner (DPC) states that '*GDPR emphasises transparency, security and accountability by data controllers and processors, while at the same time standardising and strengthening the right of European citizens to data privacy.*' (DPC 2018)

GDPR will have significant implications for both individuals and organisations regarding an individual's rights in relation to how their personal data is stored and managed by organisations, and the new legislation an organisation is expected to abide by when processing personal data.

The DPC define personal data as '*any information that can identify an individual person. This includes a name, an ID number, location data (for example, location data collected by a mobile phone) or a postal address, online browsing history, images or anything relating to the physical, physiological, genetic, mental, economic, cultural or social identity of a person.*' (DPC 2018)

### **2.13.1 Individuals**

The Irish Data Protection Commissioner outlines the following benefits and rights an individual of an EU state will be entitled when GDPR comes into effect in relation to how businesses and organisations store and manage personal data, '*the General Data Protection Regulation (GDPR) will give greater control to individuals over their personal data by setting out additional and more clearly defined rights for individuals whose personal data is collected and processed by organisations and businesses.*' (DPC 2018)

### **2.13.2 Organisations**

The Irish Data Protection Commissioner outlines the following implications GDPR is expected to have for businesses and organisations in terms of how they manage and process data, '*the General Data Protection Regulation (GDPR) very significantly increases the obligations and responsibilities for organisations and businesses in how they collect, use and protect personal data. At the centre of the new law is the requirement for organisations and businesses to be fully transparent about how they are using and safeguarding personal data, and to be able to demonstrate accountability for their data processing activities.*' (DPC 2018)

## **2.14 Legal Ramifications**

There are significant legal ramifications for organisations and businesses that breach the new GDPR laws, '*the Data Protection Commissioner is being given more robust powers to impose very substantial sanctions including the power to impose fines. Under the new law, the DPC*

*will be able to fine organisations up to €20 million (or 4% of total global turnover) for the most serious infringements.’ (DPC 2018)*

#### *2.14.1 How does GDPR impact VoIP or Unified Communications?*

Whilst GDPR is primarily focused on the protection of personal data and the IT systems and processes associated with same, many modern VoIP and Unified Communication systems rely on their own proprietary databases which retain basic user information such as name, phone number and ID’s. Therefore, this information is susceptible to the same security and data protection risks as traditional computer systems if not properly secured and controlled. Call recording and voicemail (i.e. where personal details are captured) are forms of data processing and will result in significant changes for any organisation that uses these methods of processing and collecting of personal data. Under the new GDPR rules, organisations wishing to continue the practice of call recording or using voicemail to capture personal data will need to justify legality and demonstrate the purpose fulfils six key legal principles of GDPR.

1. The people involved in the call have given consent to be recorded
2. Recording is necessary for the fulfilment of a contract
3. Recording is necessary for fulfilling a legal requirement
4. Recording is necessary to protect the interests of one or more participants
5. Recording is in the public interest, or necessary for the exercise of official authority
6. Recording is in the legitimate interests of the recorder, unless those interests are overridden by the interests of the participants in the call

(ICO 2018)

The introduction of GDPR also presents opportunities for organisations to review their security posture and specifically VoIP and Unified Communications infrastructure to ensure adequate protection is in place for mandatory GDPR compliance. Tony Friar, Chief Technical Officer of Velona Systems, an Irish based start-up that provides security software for internet telephony, recently stated that *‘presently Service Providers are focused on the IT side of GDPR with less emphasis on the voice side. This brings real opportunities for those Service Providers who are first-to-market with GDPR solutions for VoIP. By implementing GDPR solutions at both the Access and Core Network layers, Service Providers not only better meet GDPR compliance requirements but can also reassure their customers that their privacy is protected. This can be a significant competitive advantage, which over time will become a basic requirement as the impact of GDPR on voice becomes widely known and enforced.’* (Velona Systems 2018)

### **2.15 Risk Mitigation Strategies**

Further to the VoIP vulnerabilities and fraudulent activities discussed earlier in this Literature Review, Akhga and Arabnia (2014) mention that *‘the diversity of fraud activities in telecommunications in general and in VoIP in particular has made the detection of such misbehaviours a difficult task. Most of the telecom operators and VoIP providers currently rely on simple rule-based systems for reviewing customers activities. The rule-based system defines fraud patterns as rules. The rules might consist of one or more conditions. If all the conditions are met, an alarm is produced. These rules are usually developed as a result of investigations of past fraudulent activities. In addition, they tend to be very basic, consisting of a simple threshold conditions on some feature of the service subscription’* Akhga and Arabnia

(2014, p. 362). This approach is reactionary in design i.e. in response to a prior fraudulent event or activity, therefore it is not a very effective means of preventing fraud attacks as these attack vectors can take many different forms, which can easily evade a rule-based system if a rule does not exist for a specific attack type in the first place.

### 2.15.1 Big Data and Artificial Intelligence (AI)

Research from Howells et al. (2016) would suggest they also share this view as they mention *'this is how most fraud management systems operate today, detecting known, old types of fraud and failing to detect new variants or combinations of fraud'* (Howells et al. 2016. p.37).

There is limited literature available examining the real time detection of VoIP related attacks, one such paper from Akbar and Farooq (2014) titled "*Securing SIP-based VoIP infrastructure against flooding attacks and Spam Over IP Telephony*", looked at an accurate and real-time attack classification system that detects: (1) application layer SIP flood attacks that result in denial of service (DoS) and distributed DoS attacks (DDoS), and (2) Spam over Internet Telephony (SPIT). Whilst there are obvious benefits to early accurate detection and alerting of potential attacks (e.g. quicker response time, ability to minimise impact of an attack etc.), it is essentially one (albeit important) element of security defence and not a holistic end-end solution. It should also be noted that Akbar and Farooq's research and related experiments were conducted in a laboratory environment as opposed to a real live network environment.

In contrast, research from Howells et al. (2016) looked at a more holistic approach and put forward the idea of utilising big data and machine learning (AI) that encompasses multiple data sources from VoIP communications events such as VoIP data packets and subscriber billing data to proactively identify and combat communications fraud in a real-time and automated fashion. (Howells, I. et al. 2016. p.4). Their research is based on the premise that current communications fraud prevention methods are predominately reactive (after the fraud has occurred) and dependant on a multitude of manual activities using many disparate systems to identify and remediate communications fraud. Howells et al. (2016) argue that this approach is no longer viable or scalable as voice communications continue to converge with data networks coupled with the increasingly sophisticated and innovative methods criminals continue to develop to carry out their fraudulent activities.

Research from Dakur and Dakur (2014) in their paper "*Eavesdropping and Interception Security Hole and Its solution over VoIP Service*" also took a broader (albeit high level) approach to securing VoIP services at the network and application layer using techniques such as account authorisation and authentication, physical network segregation, use of encryption and network packet inspection and filtering. They also suggested the following precautions/steps that should be regularly employed in order to deter VoIP hackers.

- It is always advised to ensure that the VoIP network is detached from the data network, which helps reduce the exposure of malicious threats to the VoIP network by exposing only a smaller surface of the network
- It is helpful to use authentication to check if the incoming connections from outside are real
- Use encryption so that if at all the VoIP packets are compromised, it would be difficult to decrypt them



- Intrusion detection systems (IDS) are very useful which could be used along with firewalls that have specific support for VoIP applications
- Have a determined strategy to implement a layered security approach for confirming authorization, authentication, and Transport Layer Security

Dakur and Dakur (2014, p. 4)

### 2.15.2 VoIP Security Best Practices

Following on from the practical tips from Dakur and Dakur (2014) above, there are several common recommended best practices that can be considered when it comes to securing VoIP communications. These are described in further detail as follows,

#### 1. Infrastructure Operating System Hardening / Patching and Anti-Virus Protection

Implementing a standardised security hardening and patching policy across all underlying network, infrastructure and application systems supporting Voice and Data communications is a prudent and highly recommended standard in terms of industry best practice for ICT security. Xin (2007) and Persky (2007) also highlight this type of approach as a minimum countermeasure to mitigate disruptions to essential systems supporting VoIP communications. Cisco, a leading vendor in IP telephony also advocate similar best practices and recommendations for their customers in terms of securing their own IP telephony solutions (Cisco Press, 2012)

#### 2. Ensure appropriate network separation of Voice and Data networks and use of firewalls

Network separation and firewall implementations have long been a common basic standard in design and build of voice and data communication networks. The most basic function of a firewall is to protect the perimeter of a network and ensure only approved traffic is permitted in and out of a network. That said, a firewall is only as good and effective if it is a) configured properly and b) constantly monitored (real-time log analysis) and maintained (updated with latest security patches, firewall rules/policies continually reviewed and assessed for threats). While network segregation and the use of firewalls can go a long way to securing voice and data communications, researchers such as Flanagan (2012) and Park (2009) advise that these approaches are not completely fool proof and should be considered as mandatory elements that comprise of an overall security strategy. For example, many common firewalls are not exclusively designed with VoIP security in mind and lack the granular features to inspect VoIP packets such as SIP traffic and identify potential fraudulent traffic patterns etc.

#### 3. Implement appropriate Intrusion Detection and Prevention Systems

Intrusion Detection/Prevention Systems (IDS/IPS) have become more common in recent years as organisations seek to secure their voice and data networks and applications continue to converge. IDS/IPS devices are usually deployed in front and/or behind the perimeter firewalls on a network and have much more sophisticated packet inspection features to identify and block suspected malicious network traffic. Research from Cadet and Fokum (2016) in their paper "*Coping with denial-of-service attacks on the IP telephony system*" looked at using an open source IPS system called Snort to

test the effectiveness of an IPS system in mitigating denial of service attacks on a IP telephony system. Whilst their experiments were carried out in a test environment their results indicated that the use of IDS/IPS systems can enable VoIP providers and organizations to build effective IPS without incurring maintenance fees or software licenses from any commercial proprietary alternative IPS solutions.

4. Utilise strong Authentication, Authorisation and Encryption throughout the network

Xin (2007) and Persky (2007) advocate strong authentication coupled with strict physical and logical security schemes for controlling access to VoIP systems as key contributory factors to ensuring appropriate VoIP security. Cisco also advocate similar best practices in terms of securing IP telephony solutions which they recommend to their end customers. (Cisco Press, 2012).

5. Implement a Session Border Control (SBC)

Many organisations using VoIP as their primary means of voice communications are advised to implement a dedicated Session Border Controller (SBC) server or device to protect and secure VoIP communication protocols such as SIP. SBC's are usually deployed on the edge of a network similar to that of a firewall and monitor incoming and outgoing SIP traffic. Research from Tipping (2014) in his paper "*The rising threats from Voice over IP*" states that '*these devices protect against DoS and DDoS attacks, provide media and signalling encryption, and black, white and grey listings, ensuring no one can see past the 'front door' to gain information*' (Tipping 2014, p.6). He also states that by deploying an SBC an organisation can cost effectively secure voice and data communications thereby reducing the risk of potential data breach.

6. Verify your VoIP provider (if using a managed service/Cloud based solution)

Outsourcing VoIP communications to a managed service provider or cloud based solution is becoming an increasingly attractive proposition for many organisations such as small to medium enterprises (SME's) given the many benefits with this approach (cost effective, less management overhead etc.). Irrespective of how the VoIP service is delivered (i.e. cloud/managed service or on premise), the same security risks and challenges exists. It is therefore imperative for organisations adopting a cloud/managed service VoIP solution that they chose their vendor wisely and exercise the proper due diligence to confirm the vendor has the appropriate measures in place to ensure the VoIP service is delivered securely. German (2017) recommends organisations to request their vendors to share the relevant details on how they ensure secure VoIP communications and ascertain how often these systems and updated to ensure the business is protected from the latest threats (German 2017, p.15).

While the above practical tips from Dakur and Dakur (2014) combined with the VoIP security best practices are prudent and worthy considerations for anyone using or seeking to implement a secure VoIP solution, they can be somewhat rudimentary and often disjointed in

design (if not implemented correctly in holistic fashion) and often do not fully consider the rather broad and complex nature of Information Security in its entirety.

To properly develop and implement a truly end-end holistic security solution or strategy that encompasses people, process and technology, organisations often seek to embed a recognised information security framework, methodology and/or set of international recognised security standards into their organisation. Such frameworks would not only encompass the practical technology and procedural VoIP security recommendations outlined above but would also ensure a structured methodology for the design and implementation of a comprehensive security strategy to secure VoIP communications. This layered security approach that implements security controls in a holistic manner across multiple underlying network, infrastructure and application layers ensures a solid foundation for building secure and robust IP telephony solutions (Cisco Press 2012).

### 2.15.3 Cybersecurity Models, Standards and Frameworks

The following section outlines some of the common internationally recognised frameworks, methodologies and standards for developing a mature information security strategy. Whilst these frameworks and models are generally implemented by larger and more mature organisations due to the significant undertaking such an endeavour mandates, many of the core principles that carry over from the various frameworks and models can and should be employed by any organisation concerned about securing their data and communications network. It should also be noted that the following security models and frameworks are agnostic to any specific type of technology or system, however the standards and recommendations set out in each framework are entirely applicable to developing a comprehensive multipronged approach to designing, building and implementing a secure VoIP communications network.

#### **Cisco Security Control Framework (SCF) Model**

Developed by Cisco Systems, Inc. an American multinational technology conglomerate and one of the world's largest networking and communications providers. Cisco define the Cisco Security Control Framework (SCF) model as '*a structure of security objectives and supporting security actions to organize security controls. The Cisco SCF model is based on proven industry best practices and security architecture principles, and the vast practical experience of Cisco engineers in designing, implementing, assessing, and managing service provider, enterprise, and small and medium-sized business (SMB) infrastructures. Using the Cisco SCF model, organizations can align security requirements and controls into logical groups to facilitate the understanding and communication of the control architecture for their IT infrastructure*'. (Cisco 2009, Online)

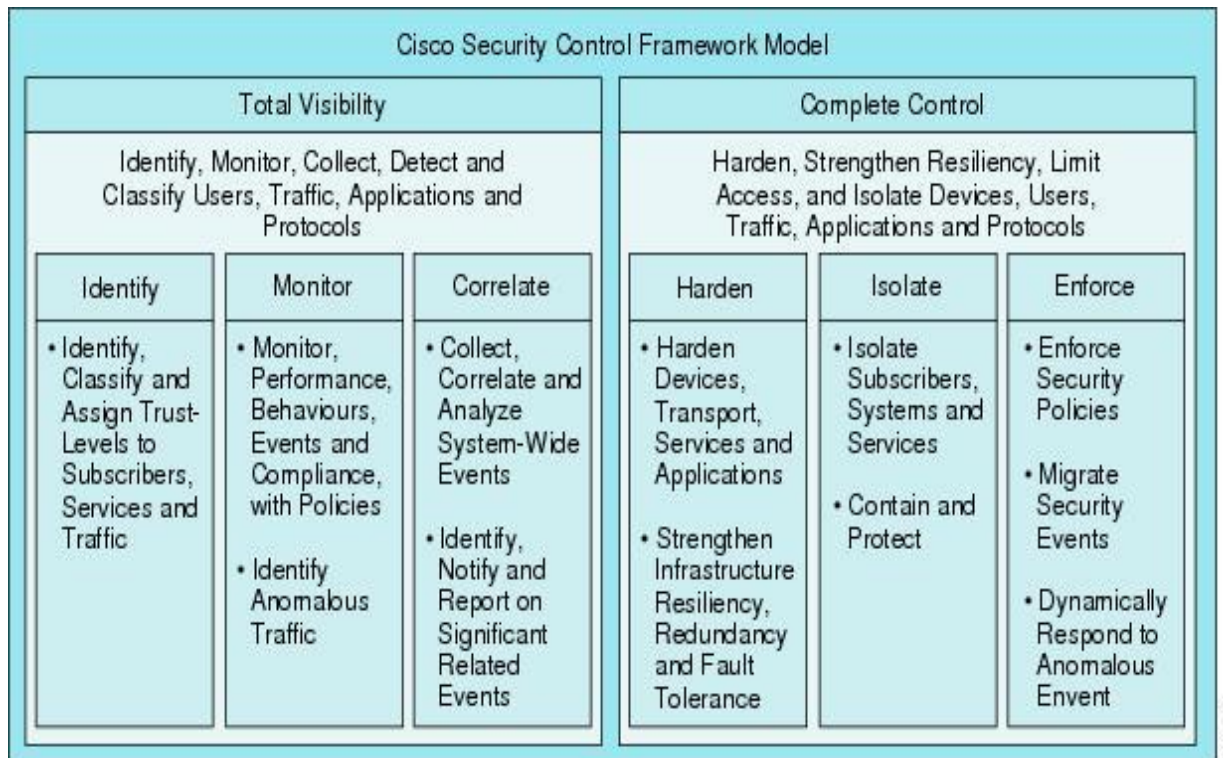


Figure 16. Cisco Security Control Framework (SCF) Model (Cisco 2009, Online)

The organization of the Cisco SCF model is designed to increase the focus on three primary goals related to the security of the IT infrastructure and assets. These goals are as follows:

- Protect the IT infrastructure
- Protect the IT assets using network-based controls
- Mitigate and respond to security incidents using network-based controls

The design of the Cisco SCF (see Figure 16) model brings together the regulation and standards based requirements with fundamental architectural principles, industry best practices, and a wide breadth of engineering experience from inside and outside of Cisco. The result is a vendor-agnostic model that supports the organization and definition of control sets to meet each organization's specific objectives. (Cisco 2009, Online)

## National Institute of Standards and Technology (NIST) Cybersecurity Framework



Figure 17. NSIT Cybersecurity Framework Core (NIST 2018, Online).

This framework was conceived following a Cybersecurity executive order issued by President Obama of the United States in 2013 and called for the Federal government and its agencies to lead the fight against cyber criminals. It was *'created through collaboration between industry and government, the voluntary framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk'* (NIST 2018, Online). It is envisaged this voluntary framework will guide organisations on how best to develop their cybersecurity strategy and help organisations to better understand, manage, and reduce its cybersecurity risks. NIST have also reported that *'Organizations are using the Framework in a variety of ways. Many have found it helpful in raising awareness and communicating with stakeholders within their organization, including executive leadership. The Framework is also improving communications across organizations, allowing cybersecurity expectations to be shared with business partners, suppliers, and among sectors. By mapping the Framework to current cybersecurity management approaches, organizations are learning and showing how they match up with the Framework's standards, guidelines, best practices. Some parties are using the Framework to reconcile and de-conflict internal policy with legislation, regulation, and industry best practice. The Framework is also being used as a strategic planning tool to assess risks and current practices.'* (NIST 2018, Online). Whilst the NIST Cybersecurity Framework was initially developed for the United States, the basic principles of the framework are country and organisationally agnostic, and also cooperate with the International Organization for Standardization, on Information Security and Risk management standards.

Function	Category	ID
<b>Identify</b>	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
<b>Protect</b>	Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
<b>Detect</b>	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
<b>Respond</b>	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
<b>Recover</b>	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Figure 18. NSIT Cybersecurity Framework Core Activities (NIST 2018, Online).

Figure 18 above outlines the desired cybersecurity activities and outcomes organized into categories and aligned to Informative References. NIST works with the Framework community to create and maintain a catalogue of Informative References (References). References are citations of detailed cybersecurity documents to any combination of Functions, Categories, and Subcategories within the Framework. References show how to use a given cybersecurity document in coordination with the Framework for the purposes of cybersecurity risk management (NIST 2018). It is envisaged that the core 5 functions can extend beyond security and also cover the wider scope of risk management in general.

### Zero Trust Model

The Zero Trust Model (also known as Zero Trust Network) is a relatively new concept created in 2010 by John Kindervag, who at the time was a principal analyst at Forrester Research Inc. Kindervag ‘a 25-year veteran of the high-tech world is recognised as the leading expert in the areas of wireless security, intrusion detection and prevention, and voice over IP hacking. During John’s tenure at Forrester he developed Forrester’s Zero Trust model of information security’ (NIST 2018, Online). The key premise of the Zero Trust Model is to eliminate the concept of “trusted” networks and assume the default position that ALL network traffic is untrusted irrespective of its origin (i.e. internal private networks and open/public networks). ‘Zero Trust takes into account the possibility of threats coming from internal as well as external sources and protects the organization from both types of threats. Cybersecurity must fully integrate with an organization’s network because organizations must contend with malicious

*insiders who are often in positions of "trust."* (NIST 2018, Online). The Zero Trust Model has three key concepts,

1. **Ensure all resources are accessed securely regardless of location:** Assume that all traffic is threat traffic until your team verifies that the traffic is authorized, inspected, and secured. In real-world situations, this will often necessitate using encrypted tunnels for accessing data on both internal and external networks. Cybercriminals can easily detect unencrypted data; thus, Zero Trust demands that security professionals protect internal data from insider abuse in the same manner as they protect external data on the public Internet.
2. **Adopt a least privilege strategy and strictly enforce access control:** When we properly implement and enforce access control, by default we help eliminate the human temptation for people to access restricted resources. Today, role-based access control (RBAC) is a standard technology supported by network access control and infrastructure software, identity and access management systems, and many applications. Zero Trust does not explicitly define RBAC as the preferred access control methodology. Other technologies and methodologies will evolve over time. What is important is the concept of minimal privileges and strict access control.
3. **Inspect and Log all traffic:** In Zero Trust, someone will assert their identity and then we will allow them access to a particular resource based upon that assertion. We will restrict users only to the resources they need to perform their job, and instead of trusting users to do the right thing, we verify that they are doing the right thing. In short, Zero Trust flips the mantra "trust but verify" into "verify and never trust." Zero Trust advocates two methods of gaining network traffic visibility: inspection and logging. Many security professionals do log internal network traffic, but that approach is passive and does not provide the real-time protection capabilities necessary in this new threat environment. Zero Trust promotes the idea that you must inspect traffic as well as log it. In order to do so, network analysis and visibility (NAV) tools are required to provide scalable and non-disruptive situational awareness. NAV is not a single tool, but a collection of tools that have similar functionality. These NAV tools include network discovery tools for finding and tracking assets, flow data analysis tools to analyse traffic patterns and user behaviour, packet capture and analysis tools that function like a network DVR, network metadata analysis tools to provide streamlined packet analysis, and network forensics tools to assist with incident response and criminal investigations.

(Source: NIST 2018, Online)

## **ISO 27001**

ISO 27001 is the international standard that provides the specification and requirements for implementing an Information Security Management Systems (ISMS). The International Organisation for Standards (ISO) define ISMS as *'a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process. It can help small, medium and large businesses in any sector keep information assets secure'* (ISO 2018, Online). ISO 27001 is an internationally recognised security standard that many organisations seek to implement and certify in to adhere to best practices and reassure their customers that security is taken

seriously and safeguarded accordingly. A 2016 ISO survey of management system standard certifications highlighted a 21% increase (from 2015-2016) in organisations certifying in the ISO 27001 standard.

The following depicts an overview of the key benefits for an organisation that adopts and implements an ISO 27001 ISMS,








By implementing an ISMS certified to ISO 27001, your organisation can:	
	<p><b>Win new business and retain your existing customers</b></p> <p>Not only does ISO 27001 certification help you to demonstrate good security practices, thereby improving working relationships and retaining existing clients, but also gives you a proven marketing edge against your competitors, putting you alongside the likes of Google, Microsoft and Verizon.</p>
	<p><b>Avoid the financial penalties and losses associated with data breaches</b></p> <p>The average cost of a data breach is estimated at \$3.79 million (€3.16 million), according to IBM. ISO 27001 is the accepted global benchmark for the effective management of information assets, enabling organisations to avoid costly penalties due to non-compliance with data protection requirements and financial losses due to data breaches.</p>
	<p><b>Protect and enhance your reputation</b></p> <p>Cyber attacks are increasing in volume and strength daily, and the financial and reputational damage caused by an ineffectual information security posture can be fatal. Implementing an ISO 27001-certified ISMS helps to protect your organisation against such threats and demonstrates that you have taken the necessary steps to protect your business.</p>
	<p><b>Comply with business, legal, contractual and regulatory requirements</b></p> <p>The Standard is designed to ensure the selection of adequate and proportionate security controls that help to protect information in line with increasingly rigid regulatory requirements such as the General Data Protection Regulation (GDPR), the Network and Information Systems (NIS) Directive and other cyber security laws.</p>
	<p><b>Improve structure and focus</b></p> <p>When a business grows rapidly, it doesn't take long before there is confusion about who is responsible for which information assets. The Standard helps businesses become more productive by clearly setting out information risk responsibilities.</p>
	<p><b>Reduce the need for frequent audits</b></p> <p>By providing a globally accepted indication of security effectiveness, ISO 27001 certification negates the need for repeated customer audits, reducing the number of external customer audit days.</p>
	<p><b>Obtain an independent opinion about your security posture</b></p> <p>Accredited certification to ISO 27001 involves undertaking regular reviews and internal audits of the ISMS to ensure its continual improvement. An external auditor will also review the ISMS at specific intervals to establish whether the controls are working as intended. This independent assessment provides an expert opinion of whether the ISMS is functioning properly and provides the level of security needed to protect the organisation's information.</p>

Figure 19. Benefits of Implementing an Information Security Management System (ISMS), (itgovernance.eu 2018, Online)

## 2.16 Summary of Risk Mitigation Strategies

The previous section outlined several risk mitigation strategies that should be considered in order to properly secure an organisations VoIP communications infrastructure. Whilst the above set of recommendations all have equal merit in their own right, it is the view of this researcher to follow a layered security approach that implements security controls in a holistic manner across multiple underlying network, infrastructure and application layers in parallel to utilising a security framework such the Zero Trust Model. The VoIP Security Best Practices recommendations set out in section 2.15.2 supplemented by a security framework like the Zero Trust Model should be strongly considered as mandatory options for designing a secure



VoIP / UC solution. This would then help ensure a solid foundation for building a secure and robust IP telephony solution for an organisation.

## **2.17 Summary of the Findings of the Literature Review**

The objective for this research question is to ascertain how prevalent fraudulent and malicious activities are regarding VoIP technologies in the Information and Communications Technology (ICT) sector and understand the size and scope of the problem while identifying solutions and possible mitigation strategies for organisations and its end users. The Literature Review findings highlighted several known vulnerabilities in VoIP and Unified Communications, whilst evidence collected from the research in the Literature Review confirms that the increasing use of VoIP and convergence of Unified Communications presents many security challenges for today's organisations. Toll Fraud in the form of International Revenue Sharing Fraud (IRSF) was found to be a common communications fraud, this was particularly prevalent in the form of widespread spate of Wangiri premium rate calls which targeted all major mobile telecoms operators and their customers in Ireland for several months in 2017 / 2018. Distributed denial of service (DDoS) attacks were also found to be common forms of attacks aimed and disrupting key communications networks and IT systems, examples of which were outlined in section 2.11 *VoIP / UC Security Attacks*.

### 3 Methodology and Fieldwork

#### 3.1 Introduction

This section provides a detailed overview of the chosen research methodology undertaken in response to the research question in this study. It outlines the key drivers and rationale behind the chosen methodologies while highlighting any potential constraints or shortcomings with the chosen methodologies.

This research utilises primary and secondary research methodologies, semi-structured interviews will be used for the primary research. Aspects of the interview design and execution are discussed later in this chapter. The relevance of the interview design, implementation, ethical considerations and compliance are also discussed.

#### 3.2 Research Philosophy

Saunders, Lewis and Thornhill (2012) define research philosophy as an *"overarching term relating to the development of knowledge and the nature of that knowledge."* (Saunders et al. 2012, p.127).

There are several common research philosophies to be considered by the researcher when designing a research approach for their specific research question and related topics. These are generally known as Positivism, Realism, Interpretivism and Pragmatism.

Positivism is associated with the natural sciences which have developed from engagement with the world in which data were collected and observations made prior to hypotheses being formulated and tested (Saunders et al. 2012, p.135). Brinkmann and Kvale (2009, p.58) suggest positivists have *'contributed to moving social research beyond myth and common sense as a result of their emphasis on using and reporting transparent methods for arriving at scientific data opens the possibility of intersubjective control and critiques of research findings, counteracting subjective and ideological bias in research.'* The data collection most commonly used in a positivist philosophy tends to be highly structured, consisting of large samples of quantitative and/or qualitative measurements (Saunders et al. 2012, p.136). In the context of qualitative research, Silverman (2006, p.118) states *that 'positivism interview data have the potential to give access to the 'facts' about the world. The primary use is to generate data which is valid and reliable, independently of the research setting'.*

Saunders et al (2012, p.136) state that. There are two types of realism, direct and critical. Direct realism states that what we experience through our senses portrays the world accurately e.g. what you see is what you get. In contrast, critical realism argues that what we experience are sensations, meaning the images of the things in the real world, not the things directly. Saunders et al (2012, p.136) argue that the critical realist's view of a constantly changing social world is more aligned with business and management research objectives which are primarily concerned with understanding the rationale for phenomena as a precursor to recommending change.

Interpretivism is primarily concerned with understanding the differences and significance between the roles of humans and objects in the context of how these differences impact on

how research is conducted and interpreted. Saunders et al. (2012, p.137) state it is '*crucial to the interpretivist philosophy is that the researcher has to adopt an empathetic stance*'. The challenge here is to enter the social world of our research subjects and understand the world from their point of view. The data collected is typically qualitative in nature comprising of in-depth investigations using smaller sample sizes. Rubin & Rubin (2005, p. 20) state *that 'the interpretive constructionist approach guides observational and in-depth interviewing and argue that for many research problems, this paradigm is more appropriate'*. The interpretive constructionist theory is primarily concerned with how people view objects or events and the meaning they attribute as the important factor (Rubin & Rubin, 2005, p. 27).

Pragmatism asserts that concepts are only relevant where they support action (Kelemen and Rumens 2008). Pragmatists acknowledge that there are many different ways of interpreting the world and undertaking research, that no single point of view can ever give the entire picture and that there may be multiple realities (Saunders et al. 2012, p.143). Pragmatism emphasizes the primacy of practice and the use-value of ideas and theories produced by researchers (Brinkmann and Kvale, 2009, p.51). This suggests that a pragmatist researcher will employ many different external objective and subjective views, multiple method designs, quantitative and qualitative that best enables answering their research question.

### 3.3 Research Strategy

The research strategy outlines the methods for how research data will be collected and analysed for this research study. Saunders et al (2012, p.169) suggest that there are many ways to collect and analyse data depending on whether the chosen research method is quantitative, qualitative or mixed methods and as such, case studies, surveys, questionnaires, experiments, and interviews are applicable for use. The data collected can be categorised as either quantitative or qualitative. Quantitative data relates to quantifying numerical data while qualitative data relates to qualifying non-numerical data.

In the context of Information Systems research, Galliers (1992) puts forward the idea of using research "approaches" as opposed to traditional "methods" when conducting research and argues that approaches are a more generic concept than methods as they may employ many different methods or techniques. Galliers (1992) further proposes splitting these approaches into two main categories in the context of scientific and interpretivist philosophies and states that,

*'Scientific approaches may be defined as those that have arisen from the scientific tradition – characterized by repeatability, reductionism and refutability (cf. Checkland 1981) – and which assume that observations of the phenomena under investigation can be made objectively and rigorously (cf. Klein & Lyytinen 1985)'* (Galliers 1992, p.148).

Galliers (1992) also puts forward the idea that subjective/argumentative research (a category of Interpretivist approaches), tends to be a freer flowing and more creative process, that in the right hands (of a skilled researcher) can be very valuable in building and testing theories. The strength of this approach '*lies in its creation of new insights and ideas whereas the weakness arises from the unstructured, subjective nature of the process*' (Galliers 1992, p.157). In the context of choosing an information systems research approach, he states that, 'survey, descriptive/argumentative and action research approaches appear to have the widest applicability in information systems research' (Galliers 1992, p.161).

Whilst an action research approach would be suitable, it was not possible to follow this approach given the time constraints and access needed to organisations. Therefore an interpretivist research philosophy was chosen for this research study with qualitative data collected from semi-structured interviews with subject matter experts in the relevant fields. This method was chosen as its semi-structured nature provides the researcher with greater flexibility and scope to explore and compare findings from each interview conducted, whilst gaining a deeper understanding of data compared to that of data collected via surveys. The absence of any prescribed set of interview rules presents the interviewer with greater opportunities to construct and conduct the interview based on the key skills and knowledge.

Galliers (1992) highlights that the number of variables involved in surveying, coupled with limitations regarding understanding the underlying causes/process, and potential for bias in survey respondents and the researcher as key weaknesses associated with conducting surveys. It was envisaged that constructing and conducting an appropriate survey would present challenges gaining access to sufficient sample size of industry experts. There is also a limit to the number of questions that any survey questionnaire can contain if the goodwill of the respondent is not presumed to be too much (Saunders et al. (2012, p.178). It is for these reasons why surveys were discounted from the chosen research methodology in favour of semi-structured interviews which are deemed more appropriate for this research study, for the reasons outlined above.

### **3.4 Interview Methodology**

Saunders et al. (2012, p.388) state that *'The research interview is a purposeful conversation between two or more people, requiring the interviewer to establish rapport, to ask concise and unambiguous questions, to which the interviewee is willing to respond, and to listen attentively'*. Responsive interviewing, a term coined, and a model developed by Rubin & Rubin (2005) is a particular interview model based on the premise of recognising the interviewer and interviewee as human beings with emotions, personalities, interests and experiences where a relationship is formed during the interview that creates an ethical obligation for the interviewer. Rubin & Rubin (2005, p. 30) state that *'The goal of this type of research model is to generate depth in understanding, rather than breadth while keeping the interview design relatively flexible throughout'*.

It is mentioned that *'in a qualitative research interview, knowledge is produced socially in the interaction of interviewer and interviewee'* (Brinkmann and Kvale, 2009, p.82). Silverman (2006, p.113) states that *'one of the strengths of qualitative research is its ability to access directly what happens in the world, i.e. to examine what people actually do in real life rather than asking them to comment on it'*.

There are a number of predominant interview typologies to be considered by the researcher, these are structured interviews, semi-structured interviews and unstructured interviews. Structured interviews use questionnaires based on a pre-defined set of questions and thus generally tend to pertain to quantifiable data and as such is referred to as quantitative interviews. In contrast, semi-structured interviews tend to be based on a list of themes or set of key questions which can be unstructured and in-depth by design. Semi-structured interviews tend to be exploratory by design and support open discussion and conversation flow, thus they can be referred to as qualitative interviews. Unstructured interviews are conducted in a formal setting in that the interviewer and interviewee have agreed a time and

place to conduct the interview, however the questions tend to be open-ended and express little control over interviewees responses. In an unstructured interview the interviewer looks to build rapport with the interviewee allowing the interviewee to express themselves in their own way thus promoting a freer flowing discussion.

In the context of structuring interview questions, Brinkmann and Kvale (2009) highlight the importance of Thematizing the interview study which refers to *the 'formulation of research questions and theoretical clarification of the theme investigated'* (p.105). The premise here is essentially centred around the *why, what and how* of the interview:

- *Why*: clarifying the purpose of the study
- *What*: obtaining the pre-knowledge of the subject matter to be investigated
- *How*: becoming familiar with the different techniques of interviewing and analysing, and deciding which to apply in order to obtain the intended knowledge

(Brinkmann and Kvale, 2009, p.105)

Brinkmann and Kvale (2009, p.131) also go on to highlight that *'the more spontaneous the interview procedure, the more likely one is to obtain unprompted, lively, and expected answers from the interviewees. And on the other hand, the more structured the interview is, the easier the later conceptual structuring of the analysis will be'*.

In developing this view further, Brinkmann and Kvale (2009, p.99) postulate *'that the better the preparation for an interview, the higher the quality of the knowledge produced in the interview interaction, and the more the post interview treatment of the interviews will be facilitated'*.

Comprehensive secondary research on the research question subject matter was conducted to gain a better understanding of the subject matter in question. This consisted of reviewing many academic journals, related industry whitepapers and publications from subject matter experts and authors such as Flanagan (2012), Park (2009) and Thermos (2009). This then aided the researcher in forming several views and questions regarding the research topic and thus identifying the relevant questions that would ultimately form the interview questionnaire.

In preparation for carrying out the live interviews for this dissertation paper, this researcher studied the relevant literature from the publications of Brinkmann and Kvale (2009), Saunders et al (2012) and Rubin and Rubin (2005) to aid in the creation of a research and interview methodology design. Considerable emphasis was then placed on the interview design in terms of defining the appropriate interview questions for the planned semi-structured interviews. The researcher then conducted two pilot interviews to trial the interview process to ensure the interviews could be conducted within the target window of c. 30 mins and that all questions could be delivered and answered within that timeframe.

In designing an effective approach for planning and executing an interview process, Brinkmann and Kvale (2009, p. 99) suggest that *'the open nature associated with research interviewing presents the researcher with advantages and disadvantages due to the lack of formal standards, rules and procedures in the interview investigation'*. To address these challenges, Brinkmann and Kvale (2009) propose a sequential set of guidelines to assist the researcher throughout the interview journey from conceptual idea to final report, whilst

minimising any potential hardships arising from the process for the researcher. They refer to this process as the,

#### Seven Stages of an Interview Inquiry

- *Thematizing*. Formulate the purpose of an investigation and the conception of the theme to be investigated before the interviews start. The *why* and the *what* of the investigation should be clarified before the question of *how* method – is posed.
- *Designing*. Plan the design of the study, taking into consideration all seven stages of the investigation, before interviewing. Designing the study is undertaken with the regard to obtaining the intended *knowledge* and taking into account the *moral* implications of the study.
- *Interviewing*. Conduct the interviews based on an interview guide and with a reflective approach to the knowledge sought and the interpersonal relation of the interview situation.
- *Transcribing*. Prepare the interview material for analysis, which generally includes a transcription from oral speech to written text.
- *Analyzing*. Decide, on the basis of the purpose and topic of the investigation and of the nature of the interview material, which modes of analysis are appropriate for the interviews.
- *Verifying*. Ascertain the validity, reliability, and generalizability of the interview findings. Reliability refers to how consistent the results are, and validity means whether an interview study investigates what is intended to be investigated.
- *Reporting*. Communicate the findings of the study and the methods applied in a form that lives up to scientific criteria, takes the ethical aspects of the investigation into consideration, and results in a readable product.

(Brinkmann and Kvale, 2009, p.102).

#### 3.4.1 *Thematizing*

The primary objective of the interview was to speak with subject matter experts and industry professionals with experience of VoIP and Unified Communications technology.

The researcher also had a basic understanding of each interviewee's background given some were existing professional contacts and the remaining interviewee's contacts were established via mutual professional networks.

#### 3.4.2 *Designing*

A number of elements of the overall interview approach needed to be considered to ensure the interview process was executed in a consistent manner. The following describes the key elements which were considered.

#### ***Ethical Issues***

Brinkmann and Kvale (2009, p.63) suggest that an interview inquiry is a moral enterprise and that ethical problems arise throughout the entire interview process due to complexities of "researching private lives and placing accounts into the public arena" (Birch et al. 2002, p.1).

The following key concerns pertaining to ethics that the researcher focused on were as follows,

- Confidentiality and Anonymity - All interview participants identities had to be protected therefore all interview results were anonymised to ensure the interviewee and/or any organisation could not be identified including ensuring any potentially sensitive information was not disclosed.

To mitigate any potential conflict with ethical concerns and prevent any potential harm to the interviewee (Brinkmann and Kvale, 2009, p.173), ethics approval was required from Trinity College Ethics Committee before conducting any primary research via semi structured interviews. A mandatory comprehensive ethics proposal was required to be submitted to the Ethics Committee detailing the research background, rationale, methodologies, strategy and details pertaining to participant consent in advance of any primary research being conducted. This also included confirmation of the intended interview participants and outlining a detailed description of interview questions that would be used during the interview process. See Appendix C and D for further details on the interview process.

### **Recruitment Strategy**

*'Most management and organisational researchers suggest that you are more likely to gain access where you are able to use existing contacts'* (Buchanan et al. 1988; Easterby-Smith et al. 2008; Johnson 1975) (Saunders et al. 2012 p.219). This was the primary recruitment strategy for this research and was employed exclusively throughout the design and execution of the interview process.

Saunders et al (2012, p.260) state that it is impractical for a researcher to collect data from an entire population for all research questions hence the need to select a sample size. There are several practical reasons for using samples, namely the issue of gaining access to interviewees, time constraints and the ability for the researcher to collect more detailed information due to collecting data from fewer resources.

Purposive sampling requires the researcher to use their own judgement when selecting cases that best enables them to answer their research question(s) and is often used when working with small sample sizes. (Saunders et al (2012, p.287).

### **3.4.3 Interviewing**

The interview process consisted of semi-structured interviews with participants from across the Information Security, ICT and Telecommunications industry. It was envisaged that valuable and practical insight could be derived from interviews with industry professionals and subject matter experts in the fields of Information Security, ICT and Telecommunications.

Ten interview candidates were identified to participate in the interview process. Approx. one third of the interview candidates consisted of current or ex work colleagues with the remainder made up from professionals working in the above industry sectors. Direct contact (in person, phone/email) was made to known contacts (colleagues), while new contacts were established by way of introduction from existing professional contacts and formal requests for participation via networks such as LinkedIn and other relevant channels (social media, professional bodies etc.). Interviews were conducted with individuals working as professional consultants, subject matter experts and/or contractors in the above industries at a suitable time and location as agreed with each interviewee.

An interview information and informed consent sheet were issued to every candidate in advance of the interview to ensure the appropriate expectations were set and relevant consent acquired accordingly. This was also a mandatory requirement to ensure compliance with Trinity College Dublin ethics standards.

Table 1 below outlines the list of questions that were presented to all interview participants.

1. In your opinion, how widespread is the use of VoIP technologies in workplaces?
2. In your experience, what are the primary communications tools most commonly found in organisations today?
3. In your opinion, do you believe organisations are increasingly moving to Unified Communications solutions?
4. In your experience, what are the typical infrastructure configurations for voice/Unified Communications solutions in workplaces (e.g. hosted, on premise or hybrid solutions etc.)
5. What do you know about communications fraud?
6. How concerned are you about communications fraud and its potential to impact in the workplace?
7. In your opinion, what are your biggest challenges or concerns in relation to Information Security?
8. Have you ever experienced any type of communications fraud or security breach?
9. What type of risk mitigation would you implement to protect organisations from cybercrime?
10. Do you use encryption to secure your communications infrastructure?
11. Do you audit your IT systems to identify anomalies / potential fraud?
12. In your experience, what % of IT budgets are allocated to security?
13. Do you believe communications fraud is a board level concern in modern organisations today?
14. In your experience, how highly do organisations rate privacy as a communications issue?
15. Do you believe real time VoIP security is a GDPR issue?
16. Have you ever experienced any type of DDoS attack?

Table 1. Interview Questions.

#### 3.4.4 Transcribing

All interviewees gave their consent to have their interviews recorded. Each interview was conducted and transcribed in line with (Brinkmann and Kvale, 2009) quality criteria for an interview. The criteria were as follows,

- The extent of spontaneous, rich, specific, and relevant answers from the interviewee
- The extent of short interviewer questions and longer interviewee answers
- The degree to which the interviewer follows up and clarifies the meanings of the relevant aspects of the answers
- To a large extent, the interview being interpreted throughout the interview
- The interviewer attempting to verify his or her interpretations of the subject's answers of the course of the interview



- The interview being 'self-reported', a self-reliant story that hardly requires additional explanations

(Brinkmann and Kvale, 2009, p.164).

Interview data was then anonymised and transcribed for analysis.

#### 3.4.5 Analysing

As suggested by Brinkmann and Kvale (2009) the researcher may read through his or her interviews again and again to reflect on theory and highlight specific themes of interest and understand interpretations. This was an essential requirement for the research in order to understand the data, draw conclusions and ultimately answer the research questions and key research objectives.

All interview transcripts were continuously reviewed in detail and consolidated into a master spreadsheet to help with categorising data for more detailed analysis and reporting.

Software was also used to supplement the data analysis process and identify any trends or recurring themes that were common amongst several interview transcripts.

#### 3.4.6 Verifying

The verification and reporting of interview findings is an ethical responsibility for the researcher (Brinkmann and Kvale, 2009, p.63). *'A common critique of research interviews is that their findings are not valid because the subject's reports may be false'*. (Brinkmann and Kvale, 2009, p.252). It was therefore imperative that the interviewer consider these key points throughout the interview process, to ensure a consistent protocol was followed when conducting all interviews so that findings could be more easily verified. A pragmatic validation approach was used throughout the interview process where interviewees were probed with follow up questions or prompts for further clarification where required so that their answers were clearly understood and validated. The interviewer used probing questions such as "why is that?" and "is that true?". As suggested by Brinkmann and Kvale (2009, p.256), *'pragmatic validation is verification in the literal sense – "to make true". To pragmatists, truth is whatever assists us to take actions that produce the desired results.'*

#### 3.4.7 Reporting

*'Working toward the final report from the start of an interview inquiry may contribute to a readable report of methodologically well-substantiated and interesting findings.'* (Brinkmann and Kvale, 2009, p.275). Consideration was therefore given to ensure all quotations were contextualised and interviewee identities remained anonymised. Interviewer style, tone and awareness for the readers ability to consume and understand the end report were also considered as important factors in the compilation of the final report.

### 3.5 Lessons Learnt

The following section summaries the key lessons learnt during the course of this research interview process.

Interview design and in particular question selection was an important part of the overall interview process in order to ensure maximum value and quality of data was derived from each interview. A total of 16 questions were chosen for the designated list of questions to be presented to each interviewee. In hindsight, it would have been more efficient for the interview process to reduce the list of questions down to 10-12 core questions and omit any closed-end questions. For example, 5 out of 9 interviews answered the following question,

*Do you audit your IT systems to identify anomalies / potential fraud?*

with a simple yes or no answer and thus limited the amount of quality answers and valuable data that could have been gathered if the question was rephrased to be more specific and open ended.

Conducting trial runs of the interview process in advance of the real interviews proved invaluable as it allowed the interviewer to practice forming a natural interview style whilst testing that all questions could be asked and answered satisfactorily in the targeted interview window of 30 minutes. This trial process also enabled the interviewer to test the relevant audio recording technology which would be used to record the live interviews with each interview participant who gave their consent for their interviews to be recorded.

Whilst the majority of interviews were conducted in person which was the obvious preference for the interviewer in terms of building rapport with the interviewee and also availing of the opportunity to pick up on any nonverbal cues (e.g. body language and facial expressions) during the interview, five out of nine interviews needed to be conducted by phone and Skype due to participants availability and geographic location. It was therefore imperative that a reliable and quality phone line be used to conduct remote interviews. This did not present as an issue in the main with exception to one interview which was conducted with an interviewee based in Dubai, United Arab Emirates. This particular interview was a challenge to schedule and conduct for several reasons, namely due the time difference between Dublin and Dubai and the fact that web traffic and VoIP communications were heavily monitored and controlled by the state in Dubai, coupled with poor quality telecommunications networks in that region. This interview was eventually conducted via a conference call utility that was setup by the interviewer which enabled the interviewee to dial into and join a call, however the quality of the call was poor overall due to the interviewee's connection as his end which resulted in several minutes of the interview being completely incomprehensible due the intermittent breakup of the line and overall poor call quality.

## 4 Findings and Analysis

### 4.1 Introduction

The following chapter analysed the qualitative data from the nine interviews which were conducted with participants working in ICT, Information Security and Telecommunications industries. The interviewees consisted of IP telephony and Unified Communications solution designers, service providers, administrators and product owners. The following section will analyse key themes identified during the interview process. These are discussed under the headings of technology adoption, security awareness and education, organisational impact of VoIP security vulnerabilities and legal considerations that have implications in relation to VoIP security.

### 4.2 Interview Findings

#### 4.2.1 Introduction

The following tag cloud represents the frequency of words used by interviewees and displays them graphically. These key words define the context for the subsequent analysis.



Figure 20. Qualitative Data Tag Cloud

The qualitative data tag cloud in Figure 20 above represents the most common recurring words highlighted in the primary research that was derived from the interview process. Qualitative data tag clouds are useful for highlighting specific keywords or phrases from interview transcripts and can help identify trends or patterns in interviewee feedback.

#### 4.2.2 The Interviews

A total of nine interviews were conducted during this research study out of a sample size of ten interview candidates targeted. One interview candidate did not respond to a request for interview, it should be noted this candidate was contacted via a direct message on LinkedIn which could have been a factor in their failure to respond to the interview request.

The nine interviewees that participated in one-one semi-structured qualitative interviews were specifically selected from a diverse range of backgrounds, experience and industries in order to cover as many viewpoints as possible. The interviewees represented CEO's, CTO's, IT Managers, Information Security Professionals, Systems Administrators, Network Engineers, IP Telephony Solution and Product Owners. All interviewees had varying degrees of experience with VoIP and Unified Communications ranging from subject matter expertise to comprehensive professional experience in end consumer or managed service provider contexts in both domestic and international organisations.

The organisations that the interviewees represented are summarised in the following table:

No:	Interviewee ID	Interviewee Background
1	INT01-JD	CEO and cofounder of an Irish based start-up that provides security software for internet telephony. This company has developed security solutions specifically aimed at mitigating toll fraud and TDoS attacks
2	INT02-PD	Chief Information Security Officer with the largest dedicated Information Security organisation in Ireland, providing a complete set of Information Security services, products and solutions targeting the Irish and UK markets
3	INT03-OB	IT Systems Lead with a leading Irish wholesale telecoms provider with hands on experience in systems administration of corporate VoIP and UC solutions
4	INT04-KM	Senior network engineer recognised as a VoIP subject matter expert working for an international telecoms operator
5	INT05-AC	IT Manager with a leading Irish wholesale telecoms provider responsible for the delivery and management of the organisations IT and systems estate
6	INT06-ND	Telecoms network engineer managing the telecoms and communications services for one of Irelands largest utilities company
7	INT07-NOC	Distinguished engineer working for a global leader in VoIP and Unified Communications
8	INT08-JS	Renowned cyber security expert and seasoned ICT international speaker currently working for one of the world's largest leading global information and communications technology (ICT) solutions providers
9	INT09-KE	VoIP/UC solutions pre sales engineer with an international telecoms operator

Table 2. Interviewee Profile

### 4.3 Data and Theme Presentation

#### 4.3.1 VoIP Technology Adoption

This section provides greater insight in the research question and helps answer one of the primary research objectives that sought to understand how widely adopted VoIP and Unified Communications are in today's modern organisations. All nine interview participants were asked this question and every participant confirmed that VoIP technology was currently being used in their respective organisations with varying degrees of usage, ranging from becoming more widespread to VoIP being the default standard communications technology within the workplace. These measurements were grouped as follows,

Classification	Usage Measurement
Standard	75% - 100%
Very widespread	50% - 75%
Widespread	25% - 50%
Becoming more widespread	0% - 25%

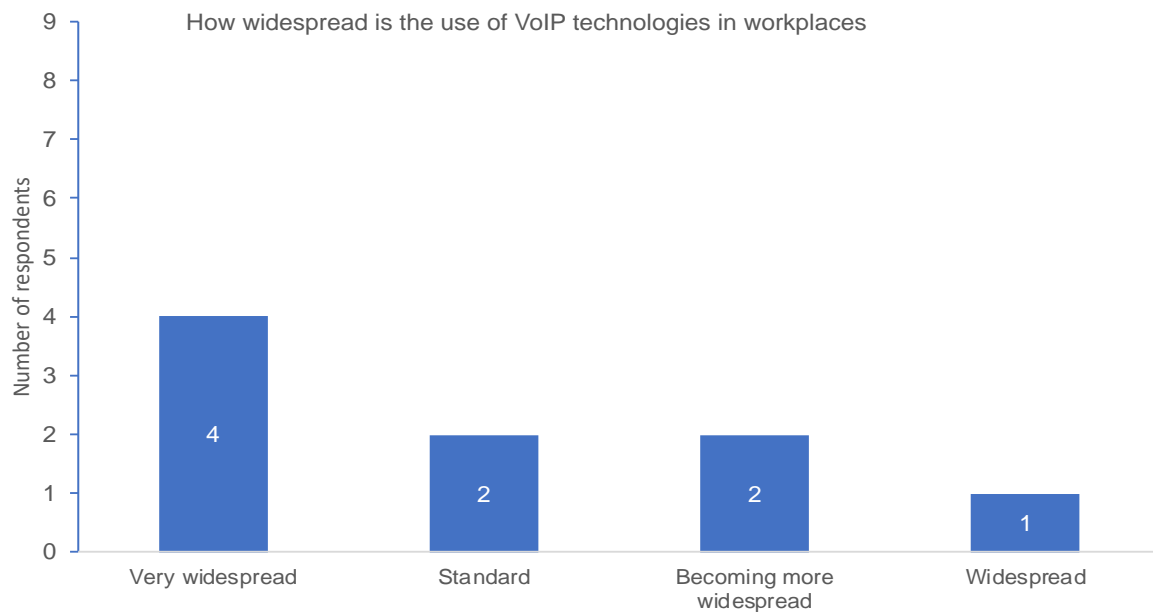


Chart 1. How widespread is the use of VoIP technologies in workplaces

All interview participants agreed that VoIP and elements of Unified Communications were becoming more mainstream forms of applications and communication methods in their respective organisations and that of their respective customer organisations. The most common VoIP and Unified Communications applications interviewees reported as typically found and used in their organisations was Microsoft's Skype for Business, which is an Instant Messenger application typically bundled with the Microsoft Office365 suite of office productivity and collaboration tools. Interviewees also reported that organisations were becoming more reliant on Skype for conducting voice and video conferencing meetings which are two core features of VoIP and Unified Communications systems. One interviewee commented,

*“Yes there would be calls, there will be meetings conducted over Skype as well even interviews, so would presentations be conducted over Skype, screen sharing and remote assistance as well at times.”*

Another interviewee commented,

*“yes still the telephony end is normally maybe in our case it’s Cisco based telephony, but we use Microsoft Skype for Business.”*

Two interview participants did highlight the view that full IP telephony adoption was *“not there yet”*. One CEO and business owner commented,

*“In my opinion it’s probably still not at 50%, but it is growing very rapidly so the legacy systems which is basically a phone on the desk is being replaced by phones on laptops, using things like Skype for Business and IP phones which are connected either to a cloud, hosted PBX or an on-premise PBX”*

In contrast to the previous comment, another interviewee commented,

*“So the good old reliable tel-set (desk phone) hasn’t gone away so the piece of plastic on your desk with the receiver that’s not going away anytime soon, I think much and all as a lot of companies like the savings on the cost etc, and it’s not going away!”*

Participants were also asked for their views on whether they believed organisations were moving towards unified communications.



Chart 2. Organisations moving to Unified Communications solutions

Whilst the overriding consensus derived from the interview process showed a positive trend in the adoption of VoIP and Unified Communications technology, several interviewees did comment and allude to some potential barriers of entry for some organisations in terms of their take up of VoIP technology. These were smaller organisations which may not possess or need a modern IT or communications infrastructure to successfully run their business operations. Budgetary constraints and a lack of appropriate underlying network connectivity requirements (i.e. high speed broadband) was also mooted as likely barriers for entry. One interviewee commented,

*“In my view it’s for in inverted commas, ‘rich organisations’ but it’s an expensive style of technology. So if you are in a small enterprise you are unlikely to be able to afford it, you are probably going to be buying a solution in from someone else.”*

Another interviewee commented,

*“Lots of talk and not a lot of action! Because what it boils down to is money and UC at the moment is while there is a lot of talk about it there is not a lot of uptake because people are deciding on whether to go hybrid, cloud or on premise and this is stopping its uptake”*

Whilst another interviewee commented,

*“The only reason I believe in Ireland having spoken to quite a few managed service providers (MSP's) is the lack of high quality broadband. That’s the only blocker to a more accelerated roll out.”*

#### 4.3.2 Security Awareness and User Education

This section emerged as a direct result of several security related questions presented to interview participants during the interview process. All interviewees were presented with several questions tailored to gauge an understanding as to their current level of knowledge pertaining to VoIP security issues, and that of general IT security in the context of IP telephony communications. It was envisaged that some of the interview participants would possess a rudimentary level of understanding and awareness of VoIP security and communications fraud given their backgrounds and professional experience in IT and telecoms industries.

The interviewees were first presented with the following leading security related question pertaining to communications fraud,

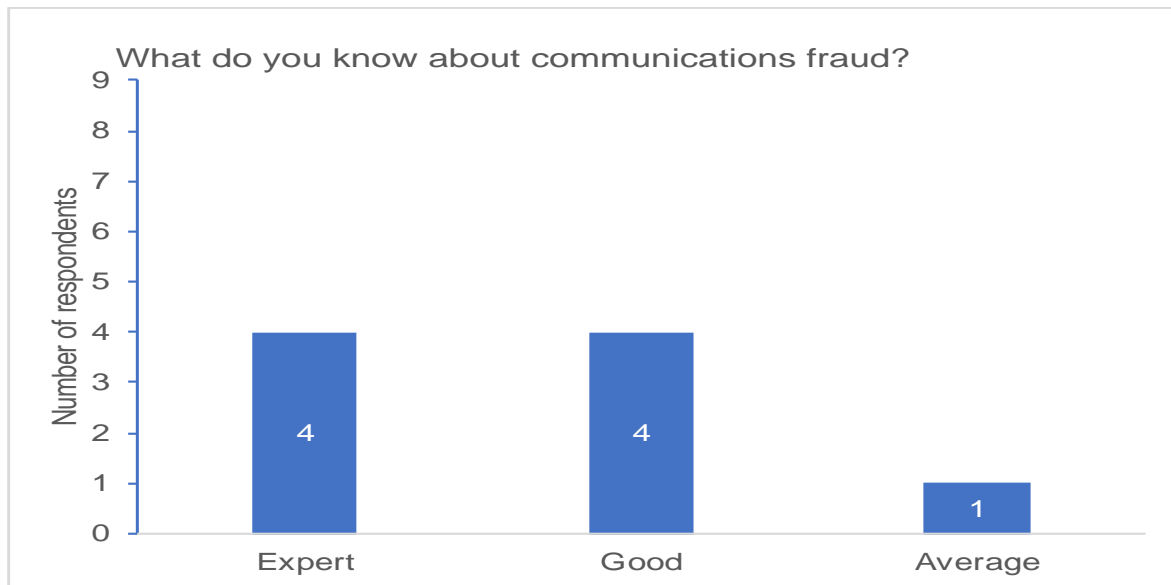


Chart 3. What do you know about communications fraud

As expected, the majority of the interview participants had detailed knowledge of communications fraud. Three ratings of *Expert*, *Good* and *Average* were defined, and subsequent percentiles assigned to each interviewee and category based on the level of detail in the corresponding answers from each interviewee. Respondents that answered this question in great technical detail were assigned an *Expert* rating, respondents that demonstrated a general understanding of fraud were assigned a *Good* rating whilst the remainder of respondents that could not demonstrate a strong technical understanding of communications fraud but knew that it existed were assigned an *Average* rating.

The next question presented to the interviewees remained focused on communications fraud and aimed to gain an understanding from the interviewees in terms of their level of concern about communications fraud and its potential impact on the workplace.

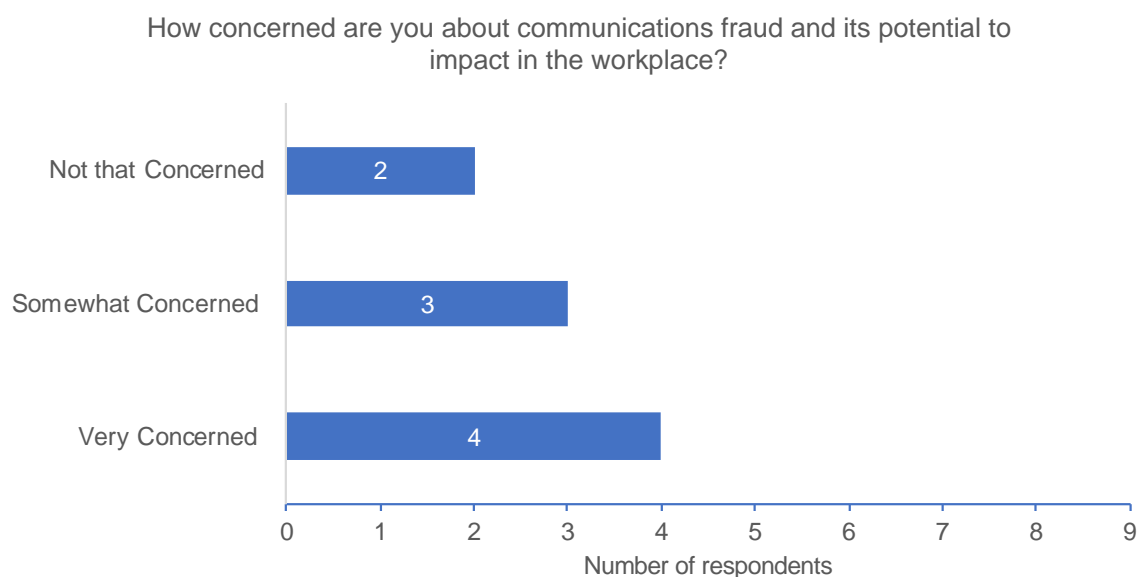


Chart 4. Concerns about communications fraud



Almost half (44%) of the interviewees confirmed they were very concerned about communications fraud and its potential to impact the workplace. Once interviewee whom is recognised as a subject matter expert on IP telephony and currently works for an international telecoms operator commented,

*“Communications fraud just like IT hacking, it’s probably on the increase. And it’s very important that we put systems in place to limit this”*

Another interviewee commented,

*“Pretty concerned because of our customers, it’s going to cost our customers money and the last thing we want is someone being able to take advantage of our equipment to steal money from our customers that’s not acceptable”*

In contrast, two interviewees (22%) stated they were not that concerned about communications fraud. One interviewee stated this was due to this not being an issue in their daily work as their company had *“dedicated security teams to manage those types of risks”*. The other interviewee stated they *“weren’t as concerned about communications fraud as they probably should be as they were a small company that opted to outsource their VoIP system to a 3<sup>rd</sup> party managed service provider”*. This interviewee also noted that they did plan to follow up with their VoIP provider to ask them how secure their system was and understand what security measures they had in place to mitigate risk and prevent communications fraud.

The third security related question presented to all interview participants sought to understand their views on what their biggest security challenges or concerns were in relation to Information Security.

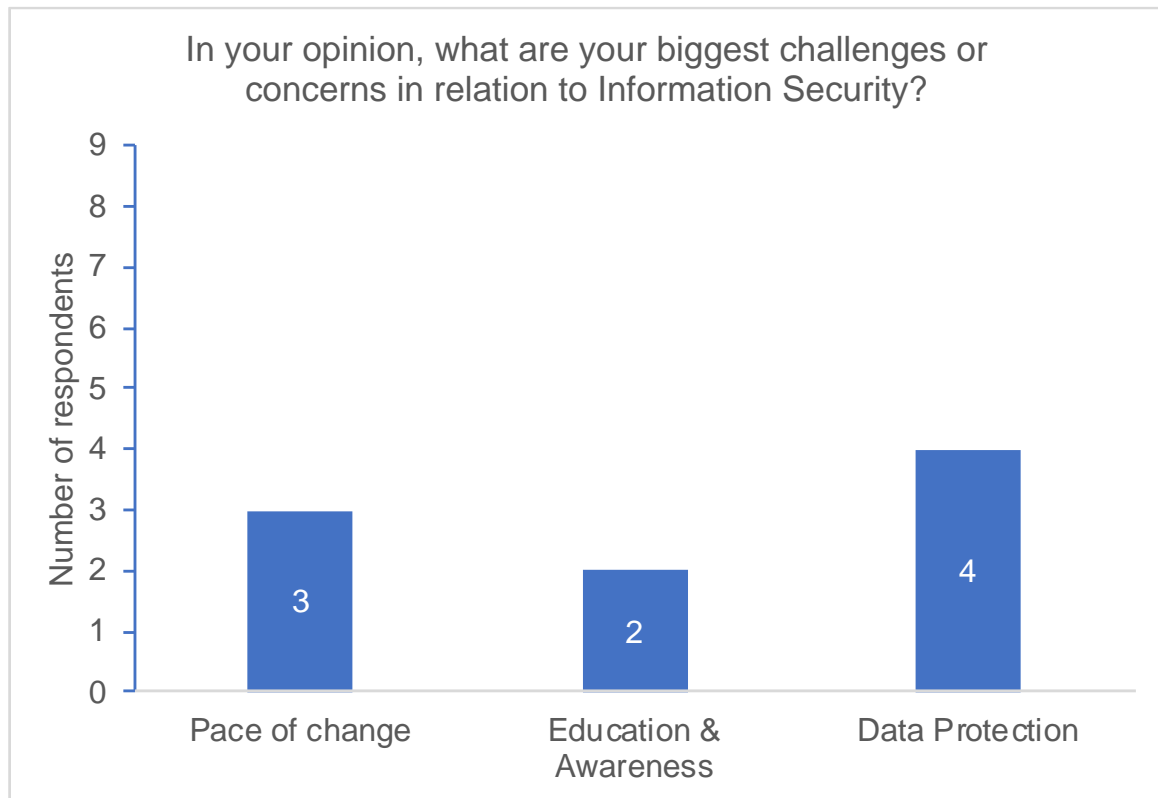


Chart 5. Biggest challenges or concerns in relation to Information Security

Chart 5 above summarises all interviewee responses into 3 main issues or concerns. The most pressing concern for almost half of all interview participants (4 out of 9) was *data protection* and securing sensitive company and customer (personal data) information. The data also confirmed that the new GDPR legislation on data protection was very prevalent and as such featured heavily as a primary driver or underlying concern in many of the interviewee responses to this question. Closely following data protection as the primary concern was the *pace of change* in terms of technology development and rate of security vulnerabilities and threats. One interviewee commented,

*“I think the biggest challenge is the pace of change. So the criminals are getting smarter and changing all the time, the attacks are changing. It’s ransomware probably in the last twelve months, it’s going to be something else next”*

Whilst another commented,

*“Yeah the biggest concern is keeping up with technology and keeping up with the threat”*

Probably the most despairing and concerning comment in response to this question came from one interviewee whom is recognised as a renowned cyber security expert currently working for one of the world’s largest telecoms manufacturers who commented,

*“Information Security today the way it is it’s losing the battle because the fraudsters/criminals are better organised, exchange information faster, invest in finding new exploits. The average organisation cannot afford to have a 24/7 monitoring of their IT systems let alone on their communication system”*

The third category identified as a primary IT security challenge or concern for two interview participants was centred around general security awareness and education particularly with end users of technology. This was based on the notion of the human as the weakest link in the chain given their susceptibility to every day social engineering techniques such as phishing and toll fraud like Wangiri premium rate calls. One interviewee commented,

*“The biggest problems we have is awareness, constant awareness.”*

Whilst another interviewee commented,

*“So, for me from a security perspective our end users are our softest targets and our most dangerous component on the whole network”*

Interview participants were also asked for their views as to whether they believed communications fraud was a board level problem for modern organisations today. Figure 26 below summarises the interviewee’s responses.

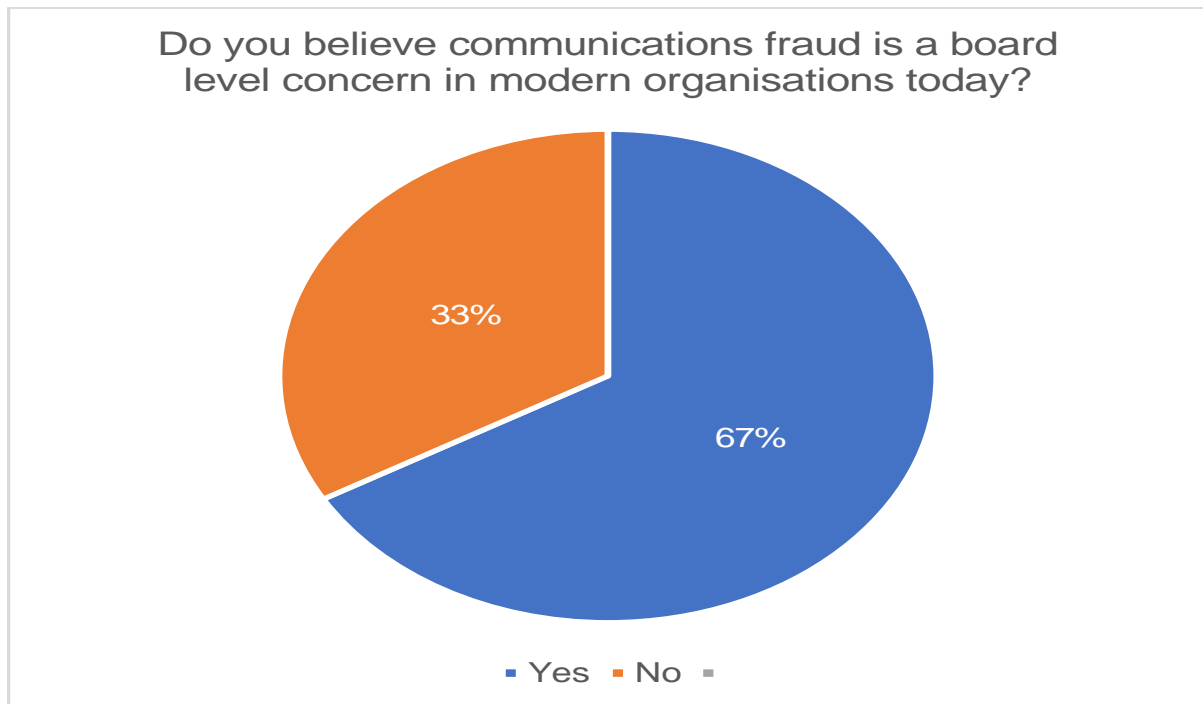


Chart 6. Is communications fraud a board level concern

As chart 6 above highlights, two thirds of all interview participants believed communications fraud was now a board level concern for today's modern organisations. GDPR was again also a present underlying contributory factor for 33% of interview participants whom responded yes to this particular question. Some interviewees commented,

*"Actually it's starting to get there. Simply because of the financial penalty with GDPR"*

Another interviewee commented,

*"Yes, I think so, because communications are an integral part of an organisations tools and asset"*

Whilst another interviewee commented,

*"Absolutely, they've got to, it's linked to GDPR as that's going to start the conversation isn't it"*

In contrast to the above comments, the remaining 33% of interviewees did not prescribe to this view nor did they believe communications fraud was a board level concern for most of today's modern organisations. One interviewee commented,

*"I think communications fraud isn't a big board level concern but the whole privacy where you're breached and people's, your customers' records or anything to do with your customers is put in peril, is a massive problem for companies now"*

Whilst another interviewee commented,

*"I don't think it's actually been managed into the board to say, look these are the risks and probably...I don't think anybody really has a formula really to put a value against those risks at the minute"*

### 4.3.3 Legislative and Compliance Implications for VoIP (e.g. GDPR)

Consistent with the views highlighted in section 2.14 of the Literature Review on the legal ramifications for VoIP security, compliance and data protection was a consistent recurring theme highlighted throughout the interview process. The new GDPR legislation which came into effect in the EU on the 25<sup>th</sup> May 2018 was specifically called out as a key concern and security driver for all interview participants. Interview participants were asked for their views on whether they believed real-time VoIP security was a GDPR issue. Interestingly, all nine interviewees agreed that VoIP was a GDPR issue. One interviewee commented,

*“Oh, absolutely. Yeah it is. Absolutely. Right. Both from a live communication, from the intelligence you would pick up from a conversation, the voicemail, the video conferencing or teleconferencing and the information you can glean from that. Those three, for any of the GDPR analysis that I’ve done on companies, those three are all on the radar”*

Another interviewee commented,

*“Of course, it is, because in the VoIP system a lot of information is captured which will fall under the GDPR rule, (e.g. call logs, user data etc.)”*

Interview participants were also asked for their views on how highly do organisations rate privacy as a communications issue. Chart 7 below summarises the interviewees responses to this question.

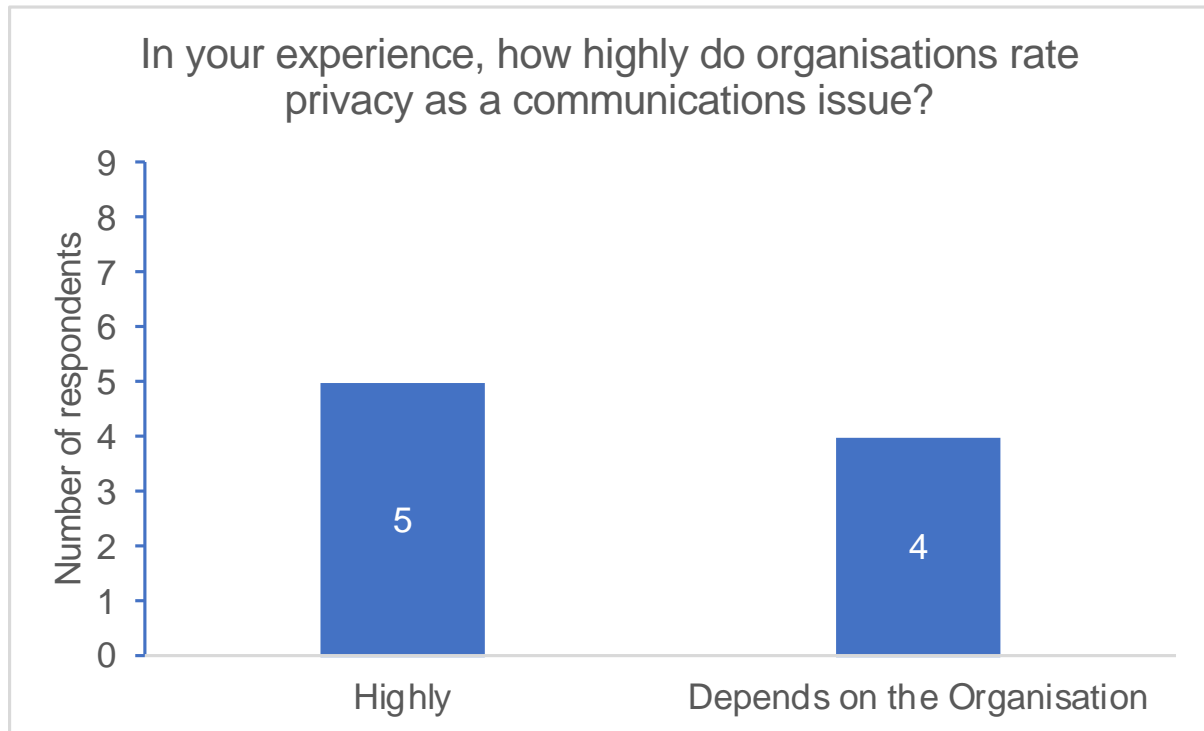


Chart 7. How highly do organisations rate privacy as a communications issue

The results from the interviewees corresponding responses were somewhat mixed but ultimately split between two main responses. That is, 56% of all participants believed privacy

was highly rated as communications issue whereas the remaining 44% believed that this was very much dependant on the organisation and various other factors such as the nature and type of organisation and whether they relied on or processing large amounts of sensitive commercial or customer information as part of their normal business operations. One interviewee commented,

*“This is a tricky one, right so, with GDPR coming in now we are talking about that actually is important. Historically it would have been more about secrecy of critical business information. So, at an executive level the general security posture would be more important than specifically privacy of information. I think the data protection commission and the EU have turned that on its head a little bit by putting a monetary value against personal information.”*

GDPR was again also a presented as an underlying contributory factor for 33% of interview participants whom responded with *high* as their answer to this particular question.

#### 4.3.4 Organisational Impacts of VoIP / UC Security Vulnerabilities

This theme provides greater insight into the research question and helps answer two of the primary research objectives that sought to gain a better understanding of how serious Toll Fraud and TDoS are in industry today, as well as the organisational impact from these two predominant VoIP security risks. Consistent with views and findings covered in the Literature Review, the data derived from the interview process confirmed that VoIP and Unified Communications security vulnerabilities and the impact these can have on an organisation is a real threat to organisations using these technologies today. Interview participants were asked two key questions to ascertain if they had ever suffered any type of communications fraud or security breach including if they had ever suffered or experienced a distributed denial of service (DDoS) attack on their organisations systems. Chart 8 below summarises the interviewees responses to this question.

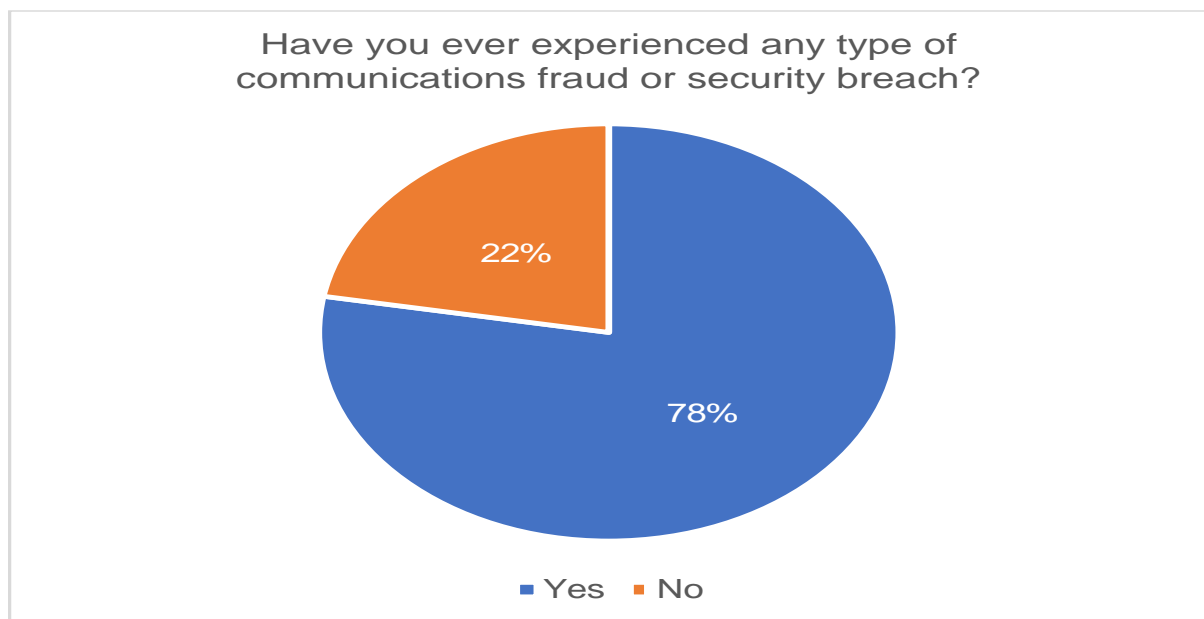


Chart 8. Experienced any type of communications fraud or security breach

The data confirmed that a significant 78% of interview participants (7 out of 9) experienced some form of communications fraud or security breach in their professional experiences. The level and variety of attacks and security issues was quite broad and ranged from ransomware attacks, phishing, SMS subscription fraud to attempted toll fraud in the form of Wangiri premium rate call attacks. The most disturbing and severe communications fraud experienced by one interviewee was a SIP hack, which is a form of international revenue share fraud (aka Toll Fraud) that resulted in a £30,000 financial loss for the interviewee in question and subsequently put him out of business. The disturbing element to this specific example (aside from the very real financial, business and personal detriment) was that this interviewee was actually proficient in IP telephony, availed of the best technology systems available and implemented the appropriate security measures yet he still fell victim to this form of communications fraud which had dire consequences for the him and his livelihood.

The second question presented to all interview participants sought to ascertain if they had ever experienced any type of DDoS attack. Whilst the results to this question were not as significant as the previous question, slightly less than half of all interview participants (44%) confirmed they had not experienced any form of denial of service attack in their professional experience. In contrast, 56% of interviewees confirmed they had experienced some form of DDoS attack in their professional experiences. One interviewee confirmed one case (that of a customer site) where their telephony system came under a Telephony Denial of Service (TDoS) attack. Therefore, the majority of DDoS attacks reported by the 56% of interviewees were those that involved the more traditional types of DDoS aimed at public facing websites or systems.

It was not possible to infer from the data a definitive conclusion or specific rationale as to the reason for such a low volume of confirmed TDoS attacks that specifically targeted a VoIP or Unified Communications system. This could be due to a number of factors such as the small sample size used for the interview process, the interviewees lack of awareness of any previous attacks or if this was due to some of the risk mitigation strategies that some of the interviewees had implemented in their systems to prevent these types of attacks from occurring. These risk mitigation strategies are discussed in further detail in the next section below.

#### *4.3.5 Security Posture and Potential Risk Mitigation Strategies*

The final theme identified from the interview findings centred around general organisational security posture and risk mitigation strategies, and thus provides greater insight into the research question which helps to answer one of the primary research objectives that sought to ascertain what the typical organisational security posture is regarding VoIP communications and security.

Almost all interviewees (89%) confirmed that they routinely audit their organisations key systems as part of security measures to identify and mitigate fraud. These were typically in the form of periodic manual and automated checks ranging from weekly, monthly and annual audits. One interviewee stated that they currently didn't have an auditing process in place but recognised that this was a gap they needed to address. Another interviewee confirmed that his organisation had a dedicated security team in place to manage all aspects of systems security including routine auditing and proactive risk management.

Interviewees were also asked if they used any type of encryption to secure their organisations communications infrastructure. Interestingly, all nine interviewees confirmed that they currently use various types of encryption technology to secure their communications infrastructure and network in general. The most common forms of encryption used were typically secure Virtual Private Networks (VPN's) used to setup a secure connection (tunnel) between a client endpoint (e.g. user/device) and a server endpoint (e.g. VoIP service).

Interviewees also stated that the Hypertext Transfer Protocol Secure (HTTPS) protocol was also widely used for standard web communications which can complement the built in security protocols found within common VoIP applications. For example, Microsoft's Skype for Business application which is fast becoming ubiquitous in the corporate environment uses its own proprietary secure protocols TLS (Transport Layer Security) and MTLs (Mutual Transport Layer Security) to secure Skype communications over the internet.

The final security related question presented to interviewees sought to understand their recommendations regarding what type of risk mitigation they would implement to protect organisations from cybercrime. The results from this question were quite broad and somewhat mixed, however there were some commonalities identified in the responses. Chart 9 below summarises the interviewees responses to this question,

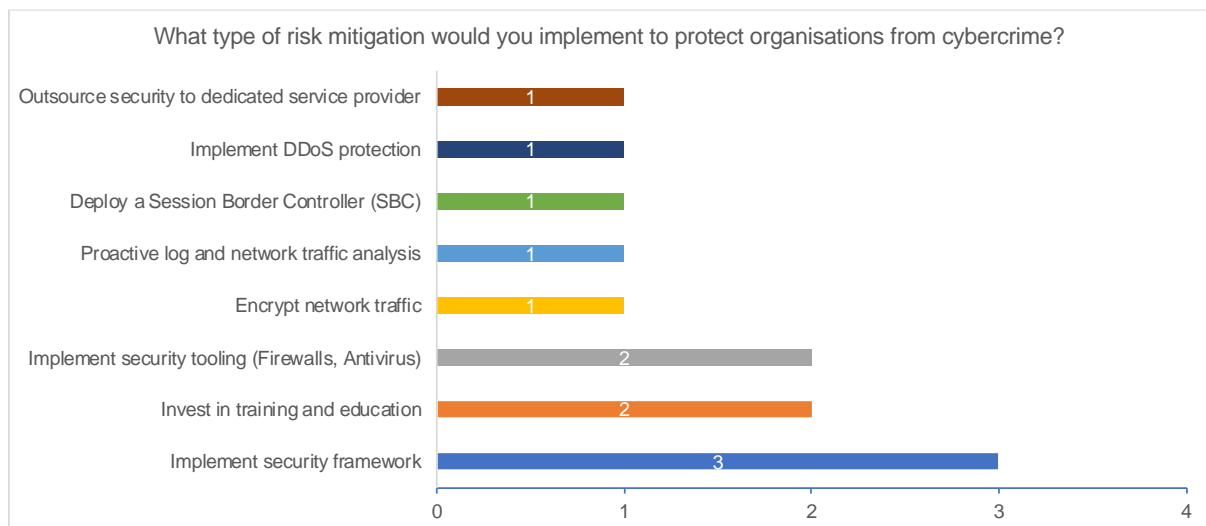


Chart 9. Risk Mitigation Strategies

Chart 9 above highlights the main risk mitigation recommendations identified in the interviewees responses. Several interviewees suggested multiple recommendations from the above figure. Consistent with the views highlighted in section 2.15.3 of the Literature Review on *Cybersecurity Models, Standards and Frameworks*, 33% of all participants recommended that an industry recognised security standard or framework be implemented as a holistic or layered approach to security that encompasses people, processes and technology. 22% of interview participants recommended implementing the appropriate security tooling (e.g. Firewall and Antivirus systems) and investing in the appropriate training and education for all users in terms of security awareness and risk management. Interestingly, only one interviewee confirmed that they had implemented designated Session Border Controller's (SBC's) to help secure and protect their organisations VoIP communications infrastructure.

#### 4.4 Summary

The interview process sought to gain further insight into the research question and ultimately answer the following primary research objectives,

*Gain an understanding of how serious Toll Fraud and TDoS are in industry today*

It was demonstrated that Toll Fraud and to a lesser extent TDoS are very real and serious risks to organisations communications infrastructure today. The evidence from the Literature Review and subsequent subject matter expert interviews conducted for primary research confirmed that there are many forms of Toll Fraud in existence today. The data also showed evidence of real life examples or recent toll fraud attacks such as International Revenue Share Fraud which was most prominent in the form of Wangiri premium rate calls which were widespread in Ireland in 2017. In terms of TDoS attacks, the Literature Review highlighted that many VoIP and Unified Communications systems are susceptible to this form of denial of service attack, however the evidence from the qualitative research indicated this was not as common as Toll Fraud, nor was it as common as the other form of traditional distributed denial of service (DDoS) attacks which are typically aimed at disrupting public facing systems or websites and as such much more frequent than TDoS.

*Gain an understanding of the organisational impacts of Toll Fraud and TDoS*

Consistent with the findings from the Literature Review and subsequent interview process carried out for primary research, the data confirms that Toll Fraud and TDoS can and does have serious implications for an organisations communications infrastructure if the appropriate security measures are not implemented correctly. The potential organisational impacts were evident in the real life examples of Toll Fraud and TDoS documented in section 2.11 *VoIP / UC Security Attacks*. This was also consistent with feedback from the interview process which confirmed that many interview participants had experienced various types of Toll Fraud and TDoS in their professional and personal experiences. The data also indicated that the level of severity in terms of organisational impact varied greatly from minimal disruption and inconvenience to significant financial, personal and business detriment.

*Ascertain what the typical organisational security posture is regarding VoIP communications and security*

The research confirmed that there was no one standard or uniform approach to an organisations security posture. The data collected indicated that how an organisation approached their VoIP communications and general IT security as a whole varied greatly from organisation to organisation. The data suggested that there are a multitude of factors for an organisation to consider which can influence how they approach implementing an information security strategy. Factors such as the nature of business operations, data processing requirements (e.g. personal data), technology adoption and financial considerations played a role in shaping an organisations general security posture. The research did however highlight several commonalities in terms of elements of standard security defences which are often present in many modern organisations today. These were typically in the form of implementing standard security tooling such as physical hardware and software devices such as firewalls to protect the network perimeter, antivirus protection and use of various different encryption technologies to protect data and secure network/communications traffic.



*Ascertain if Fraud and TDoS is seen as a Board level problem*

The research suggests that the risks posed by potential Fraud and TDoS (by way of the more common DDoS style attack) are often not very visible at board level (unless there has been a significant security breach resulting in data/financial loss or public brand damage). In contrast, the findings from the primary research and the corresponding feedback from more than half of all interview participants suggested that these risks were starting to become more of a board concern in today's organisations. The general consensus for 67% of interview participants was that legal and mandatory data protection requirements in the form of new GDPR compliance was clearly evident as a key underlying factor in driving more security awareness at board level.

*Ascertain what legal and compliance implications exist for VoIP Security*

The research demonstrated that the new EU directive on data protection laws (GDPR) which came into effective on the 25<sup>th</sup> May 2018 featured heavily in the data collected from the interview process. All interview participants universally agreed that real-time VoIP security was now a GDPR issue and as such GDPR was a key influencer in terms of IT security strategy as well as raising VoIP communications security awareness at a board level in organisations today. The research also highlighted that GDPR has fundamentally changed the security narrative and how organisations view data and the means in which data is processed and secured across the relevant information systems. In the context of VoIP and Unified Communications systems, GDPR obligations essentially instils an onus on an organisation to review their communications systems to ensure they are appropriately secured to protect any personally information which may be contained in those systems (e.g. user id, name, phone number etc.).

## **5 Conclusion and Future Work**

### **5.1 Introduction**

The objective of the research was to understand the risks posed to organisations by VoIP communications fraud and TDoS attacks and ascertain what possible solutions and mitigation strategies might exist for same. This chapter concludes this research, demonstrates that the research question has been answered, identifies the key findings and also acknowledges the limitations of the research and highlights options for potential further research in this area.

### **5.2 Conclusions**

The Literature Review looked at VoIP and Unified Communications technology in detail and explored several known vulnerabilities and security risks related to these technologies, which were then reviewed in detail to ascertain what conclusions were drawn from the associated research. The majority of academics were in general agreement regarding the numerous types of security vulnerabilities and risks associated with VoIP and Unified Communications implementations. Similarly, there was also a general consensus amongst all interviewees that VoIP and Unified Communications fraud was a real threat and growing concern for today's organisations.

The Literature Review also highlighted a common trend amongst many of the academic research publications reviewed for this dissertation, which showed that much of the academic research on VoIP and Unified Communications security focused heavily on the technical aspects of such issues and the proposed solutions or mitigation strategies. It was also noted that the majority of the academic research was either theoretical and that the related experiments were carried out in controlled lab environments.

The Literature Review highlighted several approaches that could be used to ascertain the level of communications fraud such as implementing the relevant security tooling and processes to identify and mitigate fraudulent activity on a VoIP system, in parallel to conducting continuous monitoring and auditing of all relevant networks, systems and data related to VoIP communications. The research also demonstrated that a well-designed and executed qualitative research study can prove beneficial to ascertaining the level of communications fraud and its potential impact on an organisation. However, it must be acknowledged that the level of success in terms of collecting valuable data is not just dependant on a well-designed and executed qualitative research study, it is also very much dependant on access to quality primary and secondary research sources. Specifically, the data and subsequent findings derived from subject matter experts during the interview process proved invaluable and helped validate much of the academic and non-academic research for this study.

### **5.3 Generalisability of Findings**

The interview process carried out as part of primary research for this dissertation interviewed professionals from Information Technology and Telecommunications industries. Although care was taken to include a broad selection of organisations, caution has to be exercised in extending these findings to all organisations. However the findings in relation to VoIP security vulnerabilities, communications fraud and potential risk mitigation strategies are useful and

should have relevance for any organisation seeking to implement VoIP and Unified Communications technology.

#### **5.4 Limitations of Research and Future Work**

The availability of up to date peer reviewed academic research on VoIP and Unified Communications security was somewhat limited and in many cases these publications were almost ten years old. This therefore resulted in a reliance on published reports and whitepapers from relevant industry vendors and research advisory companies. These sources were viewed objectively and the authors own particular vested interests and/or agendas were considered.

Due to time constraints and the general availability of suitably qualified candidates to participate in the interview process, a small sample size of nine participants were interviewed in total. The majority of participants were confined to the local Irish market, although several worked for international or global organisations. One interviewee was based abroad working for a global ICT company in the United Arab Emirates.

The sample of interview participants was predominately limited to Information Technology (IT) and Telecommunications industries. Further research could be carried out with non IT / Telecommunications industries, in particular contact/call centres would have also been ideal interview candidates as these organisations rely heavily on sophisticated telecommunications systems many of which have embraced VoIP and Unified Communications technologies to support their core business operations.

Due to the sensitive nature of the research question and communications fraud in particular, it was difficult to ascertain the true level of toll fraud and its financial impact on organisations. Whilst there are many publications from market research advisory companies such as Gartner and relevant industry bodies such as the CFCA on the financial cost pertaining to communications fraud, it must be noted that these are merely estimates and that detailed insight into the how these entities conducted the necessary background research was often difficult to ascertain or clarify.

Although several interviewees were forthcoming about their experiences with communications fraud, one interviewee claimed he was put out of business due to a €30K toll fraud. Another interviewee confirmed they also had a similar experience with toll fraud albeit not as severe as the previous example.

As previously stated, the research study focused on academic literature spanning a ten year period from 2007 to 2017. It also included primary and secondary present day literature from leading industry vendors and research advisories companies, coupled with primary research derived from expert interviews with specially selected subject matter experts from a diverse range of ICT and information security backgrounds. Given the rather broad timeframe used for the scope of this research study and considering the rapid pace of technology innovation and advancement, it would be prudent to have further research conducted to test the findings in this study and ascertain if and how new developments and advancements in technology impact studies of this nature. For example, what role could Artificial Intelligence play in mitigating the VoIP security vulnerabilities and risks associated with communications fraud highlighted in this research study.

## **5.5 Summary**

The objective of this research was to investigate VoIP Communications fraud and TDoS attacks and look at potential solutions and mitigation strategies required for the converged marketplace today.

This research demonstrated that VoIP and Unified Communications are complex technologies which are fast becoming standard communication systems in today's modern organisations. It was also confirmed that these technologies are continuing to converge with existing data networks and computing platforms and as such are susceptible to many forms of common cybercrime namely, toll fraud, data breaches and denial of service attacks.

The typical security posture of an organisation using VoIP or Unified Communication systems varied greatly from organisation to organisation and was influenced by many factors such as size and type of organisation, technology adoption, cost and data protection requirements. GDPR which came into effect on the 25<sup>th</sup> May 2018 essentially forces organisations to review and scrutinise their security policies and associated business processes to ensure all personal data of their employees and customers is adequately protected at all times. Given the substantial legal implications and financial penalties for organisations that fail to comply with GDPR legislation, it is envisaged that this will be a primary driver for raising general security awareness and risk at board level for all systems (data and voice) that retain or process any sensitive personal data.

## 6 References

Akbar, M. A. and M. Farooq (2014). "Securing SIP-based VoIP infrastructure against flooding attacks and Spam Over IP Telephony." *Knowledge and Information Systems* 38(2): 491-510. © Springer-Verlag London 2012

Babak Akhgar, Hamid R. Arabnia (2014) *Emerging trends in ICT security*. Waltham, MA: Morgan Kaufmann/Elsevier

Brinkmann, S. Kvale, S. (2009) *InterViews: learning the craft of qualitative research interviewing, 2<sup>nd</sup> Edition*. Sage Publications Inc.

Cadet, F. and D. T. Fokum (2016). *Coping with denial-of-service attacks on the IP telephony system*. SoutheastCon 2016.

Cisco (2009) *Cisco Security Control Framework (SCF) Model* Available at: <https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/CiscoSCF.html> [Accessed: 07/04/2018]

Data Protection Commissioner (DPC) (2018) *General Data Protection Regulation* Available at: <https://www.dataprotection.ie/docs/GDPR/1623.htm> [Accessed: 07/03/2018]

Data Protection Commissioner (DPC) (2018) *GDPR* Available at: <http://gdprandyou.ie> [Accessed: 07/03/2018]

Dakur, A. and S. Dakur (2014). *Eavesdropping and interception security hole and its solution over VoIP service*. 2014 IEEE Global Conference on Wireless Computing & Networking (GCWCN) DOI. 10.1109/GCWCN.2014.7030837

Flanagan, A. W. (2012). *VoIP and Unified Communications, Internet Telephony and the Future Voice Network*. John Wiley & Sons, Inc.

GALLIERS, R. D. (1992). *Information Systems Research: Issues, Methods and Practical Guidelines*. Oxford: Blackwell Scientific Publications.

Gartner *Magic Quadrant for Unified Communications*: Available at: <https://www.gartner.com/doc/reprints?id=1-46VDGVD&ct=170719&st=sb> [Accessed: 07/01/2018]

German, P. (2017). "Is your Session Border Controller providing a false sense of security?" *Network Security* 2017(1): 14-16. Available at: <https://www.sciencedirect.com/science/article/pii/S1353485817300077?via%3Dihub> [Accessed: 13/05/2018]

Ghafarian A., Seno, S. A. H., Dehghani, M. (2016). "An empirical study of security of VoIP system." *SAI Computing Conference* 2016 July 13-15, 2016 | London, UK <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7556105> Available at: [Accessed: 30/09/2017]

Howells, I., Scharf-Katz, V., Stapleton, P. (2016) "Fighting Future Fraud, A Strategy for Using Big Data, Machine Learning, and Data Lakes to Fight Mobile Communications Fraud"

Available at: <https://www.argyledata.com/files/FightingFutureFraud-eBook.pdf> [Accessed: 02/12/17]

International Organisation for Standardisation (ISO) *ISO/IEC 27000 family - Information security management systems* Available at: <https://www.iso.org/isoiec-27001-information-security.html> [Accessed: 07/04/2018]

Information Commissioners Office (ICO) (2018) *Guide to the General Data Protection Regulation (GDPR)* Available at: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr> [Accessed: 15/03/2018]

IT Governance (2018) *The Benefits of Implementing an Information Security Management System (ISMS)* Available at: <https://www.itgovernance.eu/isms-benefits> [Accessed: 07/04/2018]

Kvale, S. Brinkmann, S. (2009) *InterViews: learning the craft of qualitative research interviewing, 2<sup>nd</sup> Edition*. Sage Publications

Park, P. (2009) *Voice over IP Security* Cisco Press

Persky, D. (2007). "VoIP Security Vulnerabilities." SANS Institute InfoSec Reading Room. Available at: <https://www.sans.org/reading-room/whitepapers/VoIP/VoIP-security-vulnerabilities-2036> [Accessed: 26/11/17]

Rosenberg, J, Schulzrinne, H, Camarillo, G, Johnston, A, Peterson, J, Sparks, R, Handley, M, Schooler, E. (2002) RFC 3261 *SIP: session initiation protocol*. Available at: <https://www.rfc-editor.org/rfc/pdf/rfc3261.txt.pdf> [Accessed: 09/12/17]

Rubin, H, Rubin, I. (2005) *Qualitative Interviewing: The Art of Hearing Data Second Edition* Sage Publications, Inc.

Saunders, M, Lewis, P, Thornhill, A (2012) *Research Methods for Business Students, 6<sup>th</sup> Edition*. Financial Times Prentice Hall

SecureLogix Corporation (2017) *The Telephony Denial of Service (TDoS) Threat - TDoS White Paper*. Available at: <https://securelogix.com/resources/collection/whitepaper/telephony-denial-of-service-TDoS> [Accessed: 18/11/2017]

Singh, H. P., Singh, S., Singh, J., Khan, S. A. (2014). "VoIP: State of art for global connectivity—A critical review." *Journal of Network and Computer Applications* 37(Supplement C): 365-379. Available at: <http://www.sciencedirect.com/science/article/pii/S1084804513000647> [Accessed: 03/12/17]

SILVERMAN, D. 2006. *Interpreting Qualitative Data Third Edition: Methods for Analyzing Talk, Text and Interaction*. London, Sage.

Simpson, D. (2017). *FCC White Paper - Cybersecurity Risk Reduction*. P. S. H. S. Bureau and F. C. Commission, Federal Communications Commission (FCC). Available at: [http://transition.fcc.gov/Daily\\_Releases/Daily\\_Business/2017/db0118/DOC-343096A1.pdf](http://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0118/DOC-343096A1.pdf) [Accessed: 24/03/18]

Stanton R. *Secure VoIP—an achievable goal*. *Computer Fraud & Security* 2006. Available at: <http://www.sciencedirect.com/science/article/pii/S1361372306703335> [Accessed: 03/12/17]

Tipping, D. (2014). "The rising threats from Voice over IP." *Network Security* 2014(12): 5-6.

The Communications Fraud Control Association (CFCA), "2017 Global Fraud Loss Survey" Available at: <http://www.cfca.org/fraudlosssurvey> [Accessed 02/12/17]

The National Institute of Standards and Technology (NIST) (2018) *Cybersecurity Framework*. Available at: <https://www.nist.gov/cyberframework/new-framework#background> [Accessed: 07/04/18]

The National Institute of Standards and Technology (NIST) (2018) *Developing a Framework to Improve Critical Infrastructure Cybersecurity* Available at: [https://www.nist.gov/sites/default/files/documents/2017/06/05/040813\\_forrester\\_research.pdf](https://www.nist.gov/sites/default/files/documents/2017/06/05/040813_forrester_research.pdf) [Accessed: 14/04/18]

Thermos, P. (2009). "Evaluating the Security of Enterprise VoIP Networks." *IT Professional* 11(3): 30-36. Available at: <http://ieeexplore.ieee.org/document/4983398> [Accessed: 25/11/2017]

Velona Systems Ltd. (2018) *GDPR & VoIP - Burden or Opportunity?* Available at: <https://www.velonasystems.com/wp-content/uploads/2018/02/GDPR-and-VoIP-Problem-or-Opportunity-Velona-WP.pdf> [Accessed: 18/03/2018]

Verizon (2018) *Data Breach Investigations Report (DBIR) 2017* Available at: <http://www.verizonenterprise.com/verizon-insights-lab/data-breach-digest/2017> [Accessed: 24/03/2018]

VoIPSA (2015) *VoIP Security and Privacy Threat Taxonomy*: Available at: <http://www.VoIPsa.org/Activities/taxonomy.php> [Accessed: 10/10/2017]

Xin, J. (2007). "Security Issues and Countermeasure for VoIP" SANS Institute InfoSec Reading Room. Available at: <https://www.sans.org/reading-room/whitepapers/voip/security-issues-countermeasure-voip-1701> [Accessed: 07/05/18]

## 6.1 News Articles / Blogs / Surveys

Arbor Networks (2016) *Worldwide Infrastructure Security Report* Available at: [https://pages.arbornetworks.com/rs/082-KNA-087/images/12th\\_Worldwide\\_Infrastructure\\_Security\\_Report.pdf](https://pages.arbornetworks.com/rs/082-KNA-087/images/12th_Worldwide_Infrastructure_Security_Report.pdf) [Accessed: 31/03/18]

Ameri Research Inc. (2017) *Voice Over Internet Protocol (VoIP) Market Outlook To 2024*: Available at: <https://www.ameriresearch.com/product/voice-internet-protocol-voip-market-outlook-2024-key-access-type-categories-phone-phone-computer-computer-computer-phone-medium-mobile-fixed-user-type-domestic-corporate> [Accessed: 10/02/18]

Comreg *Scam Call Information* (2017) Available at: <https://www.comreg.ie/scam-calls-information/> [Accessed: 05/05/2018]

Europol (2015) *EUROPOL SUPPORTS SPANISH POLICE TO DISMANTLE SERIOUS CYBERCRIMINAL GROUP* Available at: <https://www.europol.europa.eu/newsroom/news/europol-supports-spanish-police-to-dismantle-serious-cybercriminal-group> [Accessed: 24/03/2018]

FBI Public Service Announcement (2014) *CALLBACK SCHEME USED IN INTERNATIONAL REVENUE SHARE FRAUD*: Available at: <https://www.ic3.gov/media/2014/140213.aspx> [Accessed: 16/12/2017]

FBI Public Service Announcement (2014) *PHISHING ATTACKS ON TELECOMMUNICATION CUSTOMERS RESULTING IN ACCOUNT TAKEOVERS CONTINUE*: Available at: <https://www.ic3.gov/media/2014/140428.aspx> [Accessed: 16/12/2017]

Independent.ie (2017) *'Wangiri' phone scam sweeping across Ireland is 'unprecedented' say operators* Available at: <https://www.independent.ie/business/technology/wangiri-phone-scam-sweeping-across-ireland-is-unprecedented-say-operators-36240323.html> [Accessed: 24/03/2018]

Mark Collier's VoIP/UC Security Blog (2013) *The Surging Threat of Telephony Denial of Service Attacks*: Available at: <http://VoIPsecurityblog.typepad.com/files/TDoS%5fpaper%5f4-11-13.pdf>

Mark Collier's VoIP/UC Security Blog (2013) *Cyber Threat Bulletin Boston Hospital Telephony Denial-Of-Service Attack 14 May 2013* Available at: <http://voipsecurityblog.typepad.com/files/cyber-threat-bulletin-13-06-boston-hospital-telephony-denial-of-service-attack.pdf> [Accessed: 14/04/2018]

Peter Cox, CEO | UM Labs (2009) *VoIP Security: Threats & Trends* Available at: [https://www.brighttalk.com/webcast/574/3832?utm\\_campaign=share\\_send\\_to\\_friend&utm\\_medium=email&utm\\_source=brighttalk-transact&utm\\_content=title](https://www.brighttalk.com/webcast/574/3832?utm_campaign=share_send_to_friend&utm_medium=email&utm_source=brighttalk-transact&utm_content=title) [Accessed: 17/02/2018]

The Irish Times (2017) *Wangiri fraud: What happens when you return a missed call from an unusual number?* Available at: <https://www.irishtimes.com/news/ireland/irish-news/wangiri-fraud-what-happens-when-you-return-a-missed-call-from-an-unusual-number-1.3260810> [Accessed: 18/03/2018]

Threatpost.com (2017) *Hacker Admits to Mirai Attack Against Deutsche Telekom* Available at: <https://threatpost.com/hacker-admits-to-mirai-attack-against-deutsche-telekom/127001/> [Accessed: 24/03/2018]



Techadvisory.org (2016) *TDoS: an attack on VoIP systems*: Available at: <http://www.techadvisory.org/2016/10/TDoS-an-attack-on-VoIP-systems/> [Accessed: 18/11/2017]

The Boston Globe (2017) *Boston Globe hit by denial of service attacks* Available at: <https://www.bostonglobe.com/business/2017/11/09/boston-globe-hit-denial-service-attacks/yS2mI5DJwDAuRnqxqzVKsl/story.html> [Accessed: 31/03/2018]

UCToday.com (2018) *Who's BIG in Unified Communications this Year?* Available at: <https://www.uctoday.com/news/marketplace/unified-comms-ones-to-watch/> [Accessed: 19/03/2018]

VBX Telecom (2013) *What is SIP Toll Fraud?* Available at: <http://vbx.co.za/what-is-sip-toll-fraud/#.Wn7XLWacZ25> [Accessed: 10/02/2018]

Wikipedia (2018) *Botnet* Available at: <https://en.wikipedia.org/wiki/Botnet> [Accessed: 31/03/2018]

Wired (2017) *How a Dorm Room Minecraft Scam Brought Down the Internet* Available at: <https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/> [Accessed: 31/03/2018]

## 7 Appendices

### 7.1 Appendix A. Information Sheet for Interview Participants

**Researcher:** Paul Carroll

[carrolp8@tcd.ie](mailto:carrolp8@tcd.ie)

086 819 8267

You are invited to take part in a research study. Before deciding whether or not to participate, it is important to understand why the research is being done and what it will entail. Please take time to read the following information carefully.

#### **BACKGROUND OF RESEARCH**

This research seeks to understand the current market state for Voice Over IP (VoIP) communications converged security solutions, and whether any such solutions adequately protect organisations against the threat from telephony toll fraud and denial of service (TDoS) attacks.

#### **PROCEDURE FOR THIS INTERVIEW**

If you agree to participate, this will require taking part in a short interview lasting 30 minutes which will also be recorded to capture your views on the security concerns regarding VoIP communications. The data collected will then be analysed and interpreted.

The following points should be noted about the interview:

- Your participation is voluntary and anonymous;
- You have the right to withdraw from the interview at any time during the process without penalty;
- You may refuse to answer a question without penalty;
- The interview process should take approximately 30 minutes;
- In order to accurately record the answers to the interview questions I will ask your permission to audio record the interview. However if this is not agreeable to you, I will take written notes which you will be asked to initial and date on completion of the interview.

#### **PUBLICATION**

The lead researcher (Paul Carroll) is a senior ICT professional currently working in the Telecommunications industry with a particular interest in information security. The sole purpose of this project is research necessary for preparing an MSc dissertation.

#### **ANONYMITY**

The information you provide will not be used for any commercial purposes. The information you provide will not be discussed with any other interviewee. The anonymity of the respondent will be maintained in the analysis, publication and presentation of the resulting data and findings.

#### **DIRECT QUOTATIONS**

The researcher may contact the interviewee at a later stage to clarify the contextual appropriateness of any direct quotations used in the final document.

## 7.2 Appendix B. Informed Consent Form for Interview Participants

Researcher: Paul Carroll

[carrolp8@tcd.ie](mailto:carrolp8@tcd.ie)

086 819 8267

I am 18 years or older and am competent to provide consent.

I have read, or had read to me, a document providing information about this research and this consent form. I have had the opportunity to ask questions and all my questions have been answered to my satisfaction and understand the description of the research that is being provided to me.

I agree that my data is used for scientific purposes and I have no objection that my data is published in scientific publications in a way that does not reveal my identity.

I understand that if I make illicit activities known, these will be reported to appropriate authorities.

I understand that I may stop electronic recordings at any time, and that I may at any time, even subsequent to my participation have such recordings destroyed (except in situations such as above).

I understand that, subject to the constraints above, no recordings will be replayed in any public forum or made available to any audience other than the current researchers/research team.

I freely and voluntarily agree to be part of this research study, though without prejudice to my legal and ethical rights.

I understand that I may refuse to answer any question and that I may withdraw at any time without penalty.

I understand that my participation is fully anonymous and that no personal details about me will be recorded.

*Please tick box*

I agree to the interview being audio recorded

Yes  No

I agree to the use of anonymised quotes in publication

Yes  No

I have received a copy of this agreement

Yes  No

**PARTICIPANT'S NAME (PRINTED):**

\_\_\_\_\_

**PARTICIPANT'S SIGNATURE:**

\_\_\_\_\_ Date: \_\_\_\_/\_\_\_\_/\_\_\_\_

**Statement of investigator's responsibility:** I have explained the nature and purpose of this research study, the procedures to be undertaken and any risks that may be involved. I have offered to answer any questions and fully answered such questions. I believe that the participant understands my explanation and has freely given informed consent.

**RESEARCHER'S CONTACT DETAILS:** Paul Carroll Phone: 086 819 8267

email: [carrolp8@tcd.ie](mailto:carrolp8@tcd.ie)

### 7.3 Appendix C. Interview Questions

1. In your opinion, how widespread is the use of VoIP technologies in workplaces?
2. In your experience, what are the primary communications tools most commonly found in organisations today?
3. In your opinion, do you believe organisations are increasingly moving to Unified Communications solutions?
4. In your experience, what are the typical infrastructure configurations for voice/Unified Communications solutions in workplaces (e.g. hosted, on premise or hybrid solutions etc.)
5. What do you know about communications fraud?
6. How concerned are you about communications fraud and its potential to impact in the workplace?
7. In your opinion, what are your biggest challenges or concerns in relation to Information Security?
8. Have you ever experienced any type of communications fraud or security breach?
9. What type of risk mitigation would you implement to protect organisations from cybercrime?
10. Do you use encryption to secure your communications infrastructure?
11. Do you audit your IT systems to identify anomalies / potential fraud?
12. In your experience, what % of IT budgets are allocated to security?
13. Do you believe communications fraud is a board level concern in modern organisations today?
14. In your experience, how highly do organisations rate privacy as a communications issue?
15. Do you believe real time VoIP security is a GDPR issue?
16. Have you ever experienced any type of DDoS attack?

#### 7.4 Appendix D. Samples from Transcribed Interviews

Interviewer	In your opinion, how widespread is the use of VoIP technologies in workplaces?
Participant	<i>"In my opinion it is becoming bigger, you can see in large organisations that they are trying to get away from the tradition PABX because of the cost of maintaining the equipment it's easier to virtualise the technology and provide I guess messaging along with a voice solution, soft phones you can go from your traditional desk top and take that phone and phone number with you on your mobile and whatever."</i>
Interviewer	What do you know about communications fraud?
Participant	<i>"Communications very wide topic, tremendous amount of fraud in VoIP and is quite sophisticated, revenue assurance, software pre-configured to check for known fraud types, companies that don't respond to the threat can go bankrupt, fraction of margins are small (on call rates) but money is made on volume. VoIP / telephony are heterogenous system."</i>
Interviewer	How concerned are you about communications fraud and its potential to impact your organisation?
Participant	<i>"If not implemented properly it could be open to phone calls been tapped, it could be opened to abuse, if it's not locked down properly, people can abuse it by say for instance a call of redirection or...or you are making calls to premium numbers.."</i>
Interviewer	In your opinion, what are your biggest challenges or concerns in relation to Information Security?
Participant	<i>"The biggest could be data protection, make sure all the company data, all the documents created within the company are kept secure online and offline as well."</i>
Interviewer	Have you ever experienced any type of communications fraud or security breach?
Participant	<i>"Yeah so, we have had we have had attempts at toll fraud and like everybody in Ireland over the last 6 months you know we would have had 50% of our mobile phone subscriptions attempted with the premium rate calls from Sierra Leone or Chad or wherever."</i>
Interviewer	What type of risk mitigation have you implemented to protect your organisation from cybercrime?
Participant	<i>"Implementation of a security metric (risk management system), need to model the security threat, it can come from firmware of a phone, screen overlay, Facebook/google collecting data and selling it. It's not about having zero risk but understanding what's an acceptable level of risk. Understand sources of risk and implement controls to manage those risks."</i>