A Risk Management Framework for Penetration Testing of Global Banking & Finance Networks VoIP Protocols

Yogesh Malhotra, PhD

www.yogeshmalhotra.com

Griffiss Cyberspace, Global Risk Management Network, LLC
306 Market St., Griffiss Air Force Base, Rome, NY 13441, U.S.A.
www.FinRM.org

May 8, 2014

According to computer scientists at Columbia University, "A vulnerability inside all current Cisco IP phones allows hackers to take complete control of the devices… It's relatively easy to penetrate any corporate phone system, any government phone system…" reported IEEE Spectrum article. Multiple news sources and blog 'Cisco Phone Hack' of computer security expert Bruce Schneier noted: "All current Cisco IP phones, including the ones seen on desks in the White House and aboard Air Force One, have a vulnerability that allows hackers to take complete control of the devices."

ABSTRACT

Voice over Internet Protocol based networks have been gaining central prominence in global banking and finance industry over the past decade. In recent years, they have been considered a primary avenue for costs optimization and revenue maximization by global banks thus fuelling exponential growth based upon worldwide adoption. Despite central role both technologically and economically, sparse attention has been given to critical vulnerabilities described as the 'weakest link' in global banking and finance networks and the 'soft targets' in the underbelly of global banking and finance. This article's focus is on addressing these critical gaps in global banking and finance practices and key industry frameworks underlying prudent risk management and information assurance practices for global banking and finance.

General Terms

Banking & Finance, Risk Management, Compliance, Controls, Call Centers, Network Computing, Network Protocols, Voice over Internet Protocol, VoIP, Cybersecurity, Penetration Testing, Vulnerability Analysis, Threat Assessment, Stress Testing, Systems Auditing, Regulatory Compliance.

1. INTRODUCTION

According to computer scientists at Columbia University, "A vulnerability inside all current Cisco IP phones allows hackers to take complete control of the devices… It's relatively easy to penetrate any corporate phone system, any government phone system…" [7] (emphasis added) reported a recent *IEEE Spectrum* article. Multiple news sources and blog 'Cisco Phone Hack' of computer security expert Bruce Schneier noted [27]: "All current Cisco IP phones, including the ones seen on desks in the White House and aboard Air Force One, have a vulnerability that allows hackers to take complete control of the devices." Researchers shared that they could remotely compromise VoIP phones over Internet, those phones could attack and infect other phones as well as other connected devices on shared networks. They noted that critical functions and infrastructure capabilities of the U.S. federal government, global banking and finance, and many large enterprises rely upon such VoIP network devices and protocols.

Despite emerging critical risks and vulnerabilities of VoIP networks, a recent Gallup survey noted that bank call centers – with VoIP networks as their primary backbones are the next key for revenue growth for global and regional banks searching for avenues for optimizing costs and increasing profits [8]. Cap Gemini Banking report *Trends in Retail Banking Channels: Improving Client Service and Operating Costs* of 2012 [5] notes that the call center, also known as phone banking, represented the second highest increase in transaction volumes for 2008-11 after

the Web for the same time period. Multiple industry reports on Banking and Finance [1, 2, 3, 24] observe that VoIP networks call center and phone banking represent key investments and financial transaction infrastructures for both global and regional banks.

Given increasing reliance of global banking and finance firms on the VoIP networks and associated VoIP network protocols, it is critical to analyze associated risks, threats, and vulnerabilities. Furthermore, it is equally important to understand how corporate risk management and systems and network level risk management frameworks take those risks, threats, and vulnerabilities into consideration. Such analyses are important for ensuring that the real or potential risks are recognized as well as audited and accounted for what they are. These analyses are all the more important given characterization by banking and finance industry related recent press reports of VoIP call centers as the "weakest link in banks' security chain" [16] and as "soft targets" [26].

2. RELATED RESEARCH

Even though call centers are experiencing heavy growth in global banking and finance in recent years, their role in the industry has been recognized for over 15 years or so. Since 'early era' of commercial Internet and Voice over Internet Protocol, four most

important application areas of call centers in finance included: Retail Banking, Retail Brokerage, Credit Card Operations, and Insurance [19]. Examples of recent VoIP implementations at big banks include the 2005-2006 VoIP rollout planned to span 180,000 phones with one-third each in retail, enterprise, and contact center operations for the Bank of America [11].

A review of existing penetration testing frameworks in practice based on industry practices research conducted at different levels of analysis yields some interesting findings [18]. The industry practices research survey found that diverse penetration testing frameworks exist at three different levels of analysis: Networks Protocols and Network Analysis Tools Frameworks; Systems and Networks Infrastructure Frameworks; and, Risk Management and Controls Policy Frameworks [18]. Other than a few computing and automation focused articles related research of published articles archives such as IEEE and ACM however show sparse focus on those penetration testing frameworks prevalent in industry practices [12, 34]. Formal research on frameworks to bridge the three levels applied in practice seems non-existent.

Related to the level of Networks Protocols and Network Analysis Tools Frameworks, there are multiple published academic research papers with focus on specific VoIP protocols. Many of them deal with the shared concerns about ensuring anonymity, security, confidentiality, and privacy of VoIP communications without degrading bandwidth performance and quality of service typically measured in terms of latency, jitter and packet loss; vulnerabilities and threats related to specific protocols, potential attack vectors and their remediation [29]. Just like other globally connected, decentralized, distributed, flexible, and inclusive internet-enabled innovative technologies, however, VoIP suffers from similar security threats, vulnerabilities, and exploits [30]. Security and encryption of VoIP communications, particularly for the session initialization using SIP, and Quality of Service (QoS) are key matters of ongoing concern [25]. Even in absence of source voice samples, techniques such as hidden Markov models (HMM) can be used for deciphering VoIP messages based on correlations between phenomes and the length of codec output packets [33]. VoIP communications are also susceptible to remote attackers not in the path of VoIP traffic who can conduct attacks such as man-in-the-middle (MITM) [36]. Proposed remediation measures include VPN solutions for secure VoIP transmission without compromising performance, QoS, or effective bandwidth, and, low latency networks capable of providing strong privacy protection for VoIP calls [35].

3. RISK MANAGEMENT FRAMEWORKS

3.1 Pen Testing Frameworks in Practice

A recent review of existing penetration testing frameworks in practice found that penetration testing frameworks exist at three different levels of analysis as shown in Fig. 1: Networks Protocols and Network Analysis Tools Frameworks (NPNATF); Systems and Networks Infrastructure Frameworks (SNIF); and, Risk Management and Controls Policy Frameworks (RMCPF) [18]. In the above scheme, RMCPF typically represent overarching enterprise level frameworks of corporate risk management and corporate compliance. They may encompass and relate to SNIF at the lower level of systems and networks related risk management, controls, and, regulatory compliance. SNIF may further encompass and relate to NPNATF at a still lower level.

Figure 1. Three Levels of Pen Test Frameworks in Practice.
Source: Malhotra, Y. *A Framework for Penetration Testing & Security of Network Protocols for Global Banking & Finance Call Centers*. Global Risk Management Network, LLC. 2014.

The intent of the industry practices research was to analyze three key issues related to VoIP networks and related infrastructures: what are the specific VoIP related issues that intersect across the 3 levels of analysis; how the 3 levels relate to each other in various aspects in their focus on VoIP; and, how the 3 levels need to address VoIP risk concerns spanning multiple levels.

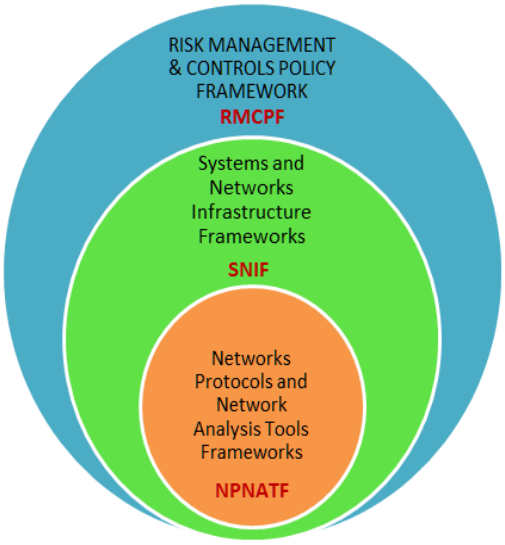

Figure 2. Proposed Risk Management Framework.

3.2 Risk Management Framework Needed

It is important to recognize why the above three levels need to be understood in an integrated manner and why penetration testing needs to be viewed within an overall risk management framework as depicted in Fig. 2. First, there is an ongoing debate among various proponents of risk management with different views of how and what pen testing should focus on at different levels of analysis. Some may argue that it is not the 'same as' vulnerability assessment, while others may contrarily see the two as serving complementary purpose [17]. Second, the objective of penetration testing can be better understood and executed within the risk management framework in terms of what is considered important

and gets required resources and sponsors. Third, integrating both penetration testing within the overall risk management framework and controls policy level framework serves most important twofold purpose. It connects the executive level risk management concerns to the pen testing team level concerns thereby ensuring two most critical 'levers'. It ensures that executives responsible for corporate policy level risk management controls and compliance become more cognizant of how policy gets implemented in reality. It also ensures that that the pen testing team is aware of how their contributions fit in the overall value delivered to the enterprise in terms of identifying, mitigating, transferring, and/or accepting risk and ensuring compliance at systems and networks level *as well as* at overall corporate level.

3.2.1 Making Penetration Testing Worth It

The above three issues bolstering the recommended framework address two key related questions: *Is pen testing worth it*? And, *if it is, then how to ensure that it is done right*? Paraphrasing Bruce Schneier [28] from his blog 'Is Penetration Testing worth It': Security consists of detection, protection, and response and all three are needed for good security. However, before you can do a good job with any of them, you must assess your security. And done right, penetration testing is a key component of security assessment. The proposed framework resolves some such dilemmas about pen testing as noted by Schneier [28]: "It's going to be expensive, and you'll get a thick report when the testing is done... And that's the real problem. You really don't want a thick report documenting all the ways your network is insecure. You don't have the budget to fix them all, so the document will sit around waiting to make someone look bad. Or, even worse, it'll be discovered in a breach lawsuit. And if you're not going to fix all the uncovered vulnerabilities, there's no point uncovering them."

The framework proposed above connects top level sponsorship and support for pen testing thus alleviating the problems outlined by Schneier while ensuring the accountability of the pen testing functions at different levels to overall corporate risk management, compliance and controls policy. It also addresses related concerns underscored by Schneier about the two reasons why you might want to conduct a penetration test: "One, you want to know whether certain vulnerability is present because you're going to fix it if it is. And two, you need a big, scary report to persuade your boss to spend more money." By ensuring that top management, business and technology managers and the pen test teams recognize that they are *all* addressing the *same mission* of the enterprise, the framework also resolves the above problem.

The survey of the penetration testing framework, frameworks of controls and compliance at systems and network levels, and frameworks of overall enterprise level risk management and compliance practices establishes the need for spanning existing gaps to better serve the enterprise risk management concerns. The research findings of practice at the three levels of analysis are reviewed below to examine some of the critical gaps and how they can be spanned for effective and efficient risk management.

3.3 Networks Protocols & Tools Frameworks

Networks Protocols and Network Analysis Tools Frameworks (NPNATF) are defined as the frameworks that are at the actual hands-on and / or automated pen testing process wherein specific network analysis tools are used for various network analysis activities related to both vulnerability assessment *and* penetration testing. As understood popularly, a penetration test simulates the actual attack from a malicious attacker which could be *anyone*. In reality, such attacks from anyone out there are what enterprises *must* need to prepare for even if they like the phrase vulnerability assessment over penetration testing. From those developing industry leading tools advancing both vulnerability analysis and penetration testing, listed below are couple of important lessons from the trenches [emphasis added]. "When it comes to security, *the best defense is offense*; you need to test the effectiveness of your own security practices before a real intruder does it for you" says HD Moore, Chief Architect for Metasploit [14]. Specific to VoIP, the renowned firm CodenomiCon, an industry leader in pen testing and known for having given t-shirts that say 'GO HACK YOURSELF', notes [emphasis added]: 'The best defense against VoIP vulnerabilities is a great proactive offense. You must test your software before *some else* does.' Given an external focus, major Big-4 firms with other global firms as clients also define pen testing similarly as an attempt to gain access to a client's network, systems, and data by simulating various threat groups including hackers, unethical competitors, and disgruntled employees. At the level of network protocols and tools framework, industry practice survey reveals two different sets of frameworks. One set of frameworks serve as an overall scheme within which various *phases* of actual penetration testing, vulnerability analysis, stress testing, security auditing, etc. are conducted. Other set of frameworks are Swiss-knife like tool kits that are actually deployed to execute the procedures within the specific phases of penetration testing and vulnerability analysis with aid of specific tools and techniques for identifying and exploiting vulnerabilities.

NPNATF thus exist at two levels of granularity: first is the top level drill-down scheme to guide the application and use of specific steps, procedures, techniques, and tools in the pen testing process, and, second is the specific technique and tool kits that are mapped on to the top level framework to actually do pen testing. These layers, particularly, the tools and techniques layer seems to be most advanced in terms of the sophistication as well as the granularity of level at which VoIP specific vulnerabilities, threats, and attacks are identified as well as executed.

3.3.1 Pen Test Overall Scheme Frameworks

3.3.1.1 Penetration Testing Execution Standard

A key overall scheme framework for networks and systems focused penetration testing and security vulnerability analysis is the Penetration Testing Execution Standard accessible at www.pentest-standard.org. It identifies the goal of the standard in providing both businesses and security service providers with a "common language and scope for performing penetration testing (i.e. Security evaluations)." Their overall scheme of defining pen testing into specific sections such as Pre-engagement Interactions, Intelligence Gathering, Threat Modeling, Vulnerability Analysis, Exploitation, Post Exploitation, and, Reporting is more or less reflective of industry practices at the NPNATF level of analysis. In some schemes at higher levels such as SNIF and RMCPF we shall see later, some of these phases are merged and re-named. The specific depth of procedures and techniques is very extensive as one will find from their freely accessible Web site and perhaps offers in public domain the most comprehensive structured NPNATF overall scheme framework that others in the same

category try to emulate. In assessing where VoIP security fits within the above framework, it is observed that: (a) VoIP mapping is an activity within Active Footprinting within Internal Footprinting within Footprinting within Intelligence Gathering section. (b) VoIP is also a subset of Voice Network Scanners within Automated within Active within Testing within Vulnerability Analysis section. Some sections and related activities may not specifically list VoIP but they are in fact significantly used in VoIP security testing. Examples include tools for network auditing, password decryption, or denial of service attacks that may be used with VoIP protocols or with other network protocols. This is where technical knowledge of specific penetration testing techniques and network protocols is helpful. Examples of such activities include MITM (man-in-the-middle attack such as using Wireshark and Cain and Abel) or Phishing within Indirect Attack within Exploitation – which is in fact done as Vishing given focus on Voice-mail phishing. (c) VoIP is also an activity under Audio Capture within Pillaging within Post-Exploitation. The overall scheme serves as a guide for conducting penetration tests and writing the pen test reports for clients.

3.3.2 Pen Test Tools & Techniques Frameworks

It is at the level of Pen Test Tools & Techniques Frameworks where actual pen testing is implemented and executed with the aid of specific pen test tool kit frameworks such as the open source Metasploit Framework and probably lesser known proprietary counterparts such as Immunity's Canvas and Core Security's Core Impact Pro. The proprietary tools may provide more specialized services and quicker updates whereas open source Metasploit Framework enjoys all benefits that go with a widely adopted, used, and tested open source toolkit framework. Since the proprietary versions are powered by most of the same features as those in open source framework, it is descriptive of general understanding of other similar toolkit frameworks as well.

3.3.2.1 Metasploit and Kali Pen Test Frameworks

Metasploit Framework described as a tool for penetration testing for risk validation and developing and executing exploit code against remote targets, can probably be best appreciated by doing actual pen testing using the industry bible on the topic, *Metasploit: The Penetration Tester's Guide* [14]. Of course, to fully harness the power of the framework toolkit, you need specifically equipped virtual machines (VM) such as Kali (docs.kali.org/general-use/starting-metasploit-framework-in-kali) or Backtrack (backtracktutorials.com/metasploit-tutorial/) on your darknet as well as an assortment of other tools such as NMap [21] and Wireshark [6], to name two of perhaps hundreds of such tools. The framework was created by the same authors who also provide its online summary version as a free self-guided review at: www.offensive-security.com/metasploit-unleashed/. A VM such as Kali would show the toolkit framework mapped broadly on to the overall scheme frameworks discussed earlier. For instance, the opening menu of Kali Linux shows sections such as Information Gathering, Vulnerability Analysis, Web Applications, Password Attacks, Wireless Attacks, Exploitation Tools, Sniffing/Spoofing, Maintaining Access, Reverse Engineering, Stress Testing, Hardware Hacking, Forensics, Reporting Tools, and System Services. To see where VoIP specific exploits, vulnerabilities, and attack tools can be found, one needs to drill down from the top menu. Within Information Gathering, one will find Telephony Analysis and VoIP Analysis; within Sniffing/Spoofing are found the subsections Voice and Surveillance and VoIP Tools many of which can be used from within the framework or as independent installations on Kali; in the section Stress Testing is VoIP Stress Testing. As noted earlier, there are many, many other non-specific tools that can be used with VoIP specific analysis and attacks such as OS Backdoors and Tunneling Tools within Maintaining Access, and, Offline Attacks within the Password Attacks section.

Besides specific and non-specific tools and techniques within the Metasploit Framework and Kali Linux toolkits, there are a couple of VoIP specific frameworks available in the form of books published by industry penetration testers. Developers of these VoIP toolkit frameworks are among VoIP pen testing specialists who have been active in both building and testing pen testing tools many of which are integrated into tool kit frameworks.

3.3.2.2 Hacking VoIP & Securing VoIP Frameworks

Based upon the book of the same name, *Hacking VoIP* [9] is a published VoIP pen testing toolkit and VoIP auditing framework written by active practitioners and founders who started out around Silicon Valley. This framework focuses on specific VoIP protocol levels vulnerabilities, threats, and attacks for SIP, RTP, H.323, and IAX2 besides VoIP infrastructure attacks, and, securing VoIP. It also contains a template for Auditing VoIP for Security with specific illustrative tests that can serve as a starting point for developing enterprise or division specific VoIP auditing frameworks. The other VoIP pen testing specific framework published by industry practitioners affiliated with the Finnish firm CodenomiCon is titled *Securing VoIP Networks: Threats, Vulnerabilities, and Countermeasures* [31]. Even though there are several other VoIP pen testing books, it seems relevant to highlight *Securing VoIP* given its additional focus on Risk Management and Controls Policy Frameworks (RMCPF) including VoIP Networks Security Controls, Security Policy, and Compliance. It is interesting to observe that similar in-built focus on risk management, controls, and compliance is also observed elsewhere in the applied context of enterprise level IT risk management practices among some European firms. The above 'anchors' or 'hooks' related to RMCPF seem relevant for firms interested in bridging the existing disconnects for developing a coherent, efficient, and effective pen testing, security, and risk management framework discussed earlier and depicted in Fig. 2.

The above two frameworks can be effectively used in conjunction with the other toolkit frameworks described next. In addition to above VoIP specific frameworks, additional VoIP related pen test interfaces are visible across higher level NPNATF frameworks such as OWASP within Web Application Penetration Testing.

3.4 Systems and Networks Level Frameworks

This SNIF framework layer at the next level above NPNATF also has its focus on penetration testing and vulnerability testing besides auditing and risk management. However, at this specific level the focus of most procedures and techniques is at the systems and networks level rather than at the more granular level of telecom network protocols such as VoIP and associated protocols such as SIP, RTP, and, H.323 where key vulnerabilities exist and are exploited. System Development Life Cycle (SDLC) framework such as OWASP discussed next falls in this category.

3.4.1 Systems & Networks Overall Scheme Frameworks

3.4.1.1 OWASP Application Security Standard

Evolving from the background of System Development Life Cycle (SDLC) testing, OWASP, acronym for Open Web Security Application Project, is a pen test overall scheme. It is accessible at www.owasp.org and includes some higher level features of the Pen Test Tools & Techniques Framework similar to Metasploit. It contains specific categories such as Application Security Verification Standard Project. OWASP defines application security activities as key practices performed during the software development lifecycle in order to reduce risk or increase assurance in an application. The OWASP Testing Framework consists of the following phases just like the pentest-standard and provides specific application security guidelines for each phase.

Phase 1: Before Development Begins
Phase 1A: Review Policies and Standards
Phase 1B: Develop Measurement and Metrics Criteria
Phase 2: During Definition and Design
Phase 2A: Review Security Requirements
Phase 2B: Review Design and Architecture
Phase 2C: Create and Review UML Models
Phase 2D: Create and Review Threat Models
Phase 3: During Development
Phase 3A: Code Walkthroughs
Phase 3B: Code Reviews
Phase 4: During Deployment
Phase 4A: Application Penetration Testing
Phase 4B: Configuration Management Testing
Phase 5: Maintenance and Operations
Phase 5A: Conduct Operational Management Reviews
Phase 5B: Conduct Periodic Health Checks
Phase 5C: Ensure Change Verification

3.4.1.2 Overall Scheme & Enterprise Frameworks

The overall scheme frameworks including the two discussed above were compared against enterprise frameworks used by Big-4 firms such as E&Y and PwC for their clients to determine two things. First, how the specific enterprise pentesting frameworks compare with the overall scheme frameworks; and, second, where are the specific concerns about VoIP networks addressed therein and to what level and depth of analysis, diagnosis, and remediation. Recognizing increasingly central role of broadband in powering enterprise networks at all levels – VoIP backbones in telecom companies, VoIP in LAN, VoIP in WAN/VPN, VoIP in last-mile QoS secured networks, and VoIP over public Internet – above enterprise frameworks recognize important role of VoIP, PBXs, & Voicemail. Enterprise frameworks seem to have many sections mirroring the NPNATF Overall Scheme Frameworks, however level of specificity for VoIP security seemed at more general SNIF level with sparse focus at NPNATF Pen Test Tools & Techniques level discussed next. This point is important given that dominant set of network protocols central to vulnerabilities, threats, and attacks in case of VoIP networks include a quite different set such as SIP, RTP, H.323, and, IAX [located between the TCP/UDP layers and user application layers in the network protocols stack] with associated vulnerability analysis and pen testing attack, diagnosis, and remediation tools and techniques. The above enterprise frameworks clearly recognize however that risk management is 'imperative' given that there will *always* be known and unknown [including zero-day] vulnerabilities. Many such vulnerabilities are often at the network protocol level and hence can be best addressed at the more granular NPNATF level. Hence, for effective risk management, it is all the more imperative to understand the key linkages between SNIF and NPNATF. It can be asserted that SNIF level frameworks, particularly in case of NPNATF, are only as effective as the *precision* in identifying and remediating related threats, vulnerabilities, and risks.

However, for either of SNIF and NPNATF to have real teeth and real resources for them to have the needed effect, they need to be effectively linked and related to the top level RMCPF.

3.5 Risk Management Controls Frameworks

It is at the corporate risk management, corporate controls, and corporate policy level where the top executives typically focus and delegate specific execution of risk, controls, and compliance policies to divisional business and technology managers. Hence, it is the level that is most concerned about regulatory compliance. It seems however most removed from where nuts, bolts, and screws actually make the real work happen in terms of vulnerability assessment, penetration testing [and stress testing] of systems at their most vulnerable levels which is at the level of specific network protocol levels. For instance, anyone keeping up with the headlines generated by the recent 'heart bleed'[1] zero-day 'bug' or the prior zero-day 'bugs' that impacted Apple's all platforms [10], desktop and mobile, may probably have observed terms such as SSL/TLS that are the names of network protocols active between Layer 5 and Layer 6 of the OSI network protocol stack. *This is the level of network protocols, such as the above security protocols, where most critical threats and vulnerabilities exist and where real countermeasures need to be in place*. Regardless, the RMCPF is perhaps equally critical, as *real compliance* of risk management controls at the NPNATF level critically and vitally depends upon adequate support, sponsorship, and funding at the executive levels which control budgetary and manpower allocations. There are three types of regulatory frameworks that are apparent at this level that are seemingly more visible to the C-suite and the top executives. Examples of such business and IT frameworks relevant to VoIP pen testing are discussed below.

3.5.1 Payment Card Industry Banking Frameworks

The first type of regulatory compliance frameworks for pen testing that banks need to follow are those governed by specific industry associations and organizations founded and managed by the banking industry such as Payment Card Industry Data Security Standards (PCI DSS) (www.pcisecuritystandards.org). For instance, PCI Requirements and Security Assessment Procedures ver. 3.0 of November 2013 [22] lists the following Detailed PCI DSS Requirements and Security Assessment Procedures: Build and Maintain a Secure Network and Systems, Protect Cardholder Data, Maintain a Vulnerability Management Program, Implement Strong Access Control Measures, Regularly Monitor and Test Networks, and Maintain an Information Security Policy. Related Requirements for each of the procedures are consistently at a very high level policy, controls, and compliance focus with no specific granular focus on specific systems and networks level, say, as compared with the System Audit & Control Frameworks discussed below. Similarly, PCI Protecting Telephone-based

[1] https://en.wikipedia.org/wiki/Heartbleed

Payment Card Data criteria attribute increasingly greater card fraud to the VoIP and phone enabled channels consistent with industry trends reviewed here [23]. Similarly, specific procedures for VoIP recordings and transmissions are at high granularity relevant to applications usage and interface level issues with broad focused recommendations such as 'proper use encryption and authentication' in transmission of data. At least at the top level visible for the above standard, specifics about quality or robustness of encryption or authentication schemes such as encryption key length, encryption and hashing schemes, and random or non-random salt requirements are found to be sparse.

3.5.2 IT Systems Banking Audit & Control Frameworks

The second type of regulatory compliance frameworks for pen testing that banks need to follow are those by business focused professional organizations and associations known for developing, upgrading, and sustaining professional practice standards. In case of information systems focused governance, risk management, controls, and compliance policy focused standards, ISACA (www.isaca.org) is one example. With its focus on internal controls and governance frameworks such as COSO and COBIT, ISACA recognizes importance of integrating controls frameworks with general audit and assurance frameworks as well as IT audit and assurance frameworks. ISACA recognizes VoIP as a 'primary component' of enterprise communications. ISACA standards also explicitly recognize the inordinate vulnerability of the VoIP networks while strongly recommending separation of voice and data networks so that if one of them is compromised it may not lead to partial or complete loss of *both* critical functions.

Given their focus on both business and technology aspects of VoIP[2], ISACA Controls Framework seems to be one possible bridge that can span RMCPF VoIP and SNIF and NPNATF [13]. Recognizing that VoIP server is an architecture that supports and drives business processes, ISACA specifies the primary COBIT processes associated with VoIP implementation in the following terms: Define the Information Architecture, Communicate Management Aims and Direction, Identify Automated Solutions, Acquire and Maintain Technology Infrastructure, Ensure Systems Security, Manage the Configuration, Manage Data, Monitor and Evaluate Internal Control, Ensure Compliance with External Requirements, and Provide IT Governance. Its VoIP Threat Taxonomy goes into quite granular aspects of VoIP specific vulnerabilities and potential attacks at a level comparable to NPNATF. Hence, it offers a potential 'bridge' to link the RMCPF with NPNATF level pen testing, auditing, and security criteria. ISACA VoIP Audit/Assurance Program templates currently focus primarily on access control, authentication, and encryption with specifications such as the use of specific encryption algorithms and encryption protocols for VoIP. These templates can be certainly improved by additional criteria from its VoIP Threat Taxonomy based upon specifics informed by NPNATF.

3.5.3 SANS Financial Services Regulatory Frameworks

The third type of regulatory compliance frameworks for pen testing that banks need to follow are those developed by IT focused professional organizations and associations known for developing, upgrading, and sustaining professional practice standards. In the case of IT systems focused governance, risk management and controls related standards, training, and certifications, SANS (www.sans.org) is one such example. A SANS report on *Penetration Testing in the Financial Services Industry* [20] refers to the PCI DSS Standards discussed above in addition to Unified Compliance Framework (UCF) and FFIEC IT Examination Handbook (ithandbook.ffiec.gov). The UCF site describes itself as the only industry-vetted compliance database framework covering regulations for Information Technology, Physical Security, and Records Management. FFIEC is the U.S. government interagency body that prescribes uniform principles, standards, and report forms for the federal examination of financial institutions by federal financial regulatory agencies that include the US Fed Board of Governors and FDIC. Typical to penetration testing focus at the NPNATF, the SANS financial industry standard also prescribes vulnerability assessment grids with risk ratings, vulnerability status, and vulnerability ratings that are also reviewed in the later discussion.

3.6 Proposed Risk Management Framework

Earlier, the two key questions motivating the debate about pen testing and vulnerability analysis were shared: Is pen testing worth it? And, if it is, then how to ensure that it is done right? Re-framing the above questions is important as the worth of penetration testing can't be assessed without recognizing its relevance and worth to enterprise risk management, controls, and compliance. Perhaps, more relevant and useful questions may be framed as: *How can pen testing and vulnerability analysis effectively contribute to the execution of enterprise level risk management, controls, and compliance policies? How can enterprise level risk management, controls, and compliance policies ensure that pen testing and vulnerability are accountable to enterprise risk management execution?* Relating the two levels, RMCPF and NPNATF, with SNIF as the 'binding glue' between the two, is critical. While bridging the disconnects between the three levels – *risk management policy*, *systems and network infrastructure controls*, and *vulnerability analysis and threat assessment* such as at the level of specific protocols associated with VoIP – the proposed framework is also intended to resolve the dilemmas about pen testing discussed earlier.

VoIP related new threat vectors increase the risk to enterprise networks because not only is VoIP vulnerable to IP related data network security risks but it is also vulnerable to emerging and relatively untested protocols associated with VoIP. Banking and Financial Services regulatory guidelines such as Gramm-Leach-Bliley (GLB) Act require financial institutions to have a policy in place to protect the information from foreseeable threats in security and data integrity. Given the context of risk management, controls, and compliance policy and frameworks discussed above, regulatory compliance can benefit from adapting the proposed framework to institution's specific needs. The integration across [the three levels of] vulnerability analysis and penetration testing embedded within overall systems and networks controls and overarching risk management and compliance framework can facilitate such context-sensitive adaptation. For instance, from perspective of auditing such as the ISACA framework, vulnerability assessment and penetration testing can be embedded within IT audit framework of assessment of the adequacy of internal controls for effective risk management and compliance.

[2] http://m.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Voice-over-Internet-Protocol-VoIP-Audit-Assurance-Program.aspx

The proposed risk management framework described here identified the three levels of vulnerability analysis and penetration testing activities evident in industry practices and relevant industry standards and frameworks. It also offered specific examples of actionable frameworks that are already being used successfully across diverse enterprises. In addition, it offered specific examples of technical implementation frameworks that are crucial for risk management based upon effective threat analysis, vulnerability assessment, and penetration testing for hardening the systems and networks. By adopting and integrating the three levels of specific frameworks discussed herein [and other similar frameworks], any financial institution, whether global or regional, can develop, maintain, improve, and sustain its enterprise risk management and compliance frameworks.

At the specific level of vulnerability assessment and penetration testing, the question may be asked if the organization must pen test every application. If it is required for regulatory compliance and effective risk management, then probably it must be done. That being said, it is even more so critical to identify the most critical vulnerabilities that are relevant to the enterprise portfolio of networks, systems, services, and applications. Many such industry databases that rank and rate specific vulnerabilities based upon severity and threat level are accessible online. OWASP maintains Top-10 vulnerability lists in multiple threat categories and SANS offers a Top-20 and Top-10 lists of security controls and vulnerabilities such as those specific to UNIX and Windows systems. Industry standard practices such as A-B-C analysis can be used to identify the specific vulnerabilities that have the greatest potential implications in terms of effect on networks and systems, and, business impact in terms of criticality and vitality of specific services and functions. In addition, further investigation into specific Common Vulnerabilities and Exposures (CVEs) can be done by reviewing dozens of archival databases such as those maintained by NIST (nvd.nist.gov) and MITRE (cve.mitre.org).

Having defined the need for an integrated adaptive overarching risk management framework for the 3-levels at which vulnerability analysis and penetration testing are implemented, it needs to be recognized that there is probably no ‘one size fits all’ solution. Some organizations may be more adept at technical network protocols and networks analysis levels and may need to better link their current practices to systems and network level controls and enterprise level risk management and compliance. Others may have well developed enterprise level risk management and compliance frameworks and systems and network level controls and may have to refine how vulnerability analysis and penetration testing can dovetail into them to enable better execution and improved performance at all levels. Similarly, depending upon diverse industry contexts such as banking and finance, and, healthcare systems, some may perceive greater risk in external-facing systems, networks, applications, and services, while others may focus on most critical information such as in credit card processing or electronic medical records processing.

4. FUTURE WORK

The proposed framework seems to be the first of its kind based upon research specifically focused on banking and financial services risk management, controls, and compliance framework. Even though the utility of the framework was illustrated in the context of VoIP systems, networks, applications, and services, it can be extended to other banking and financial services systems and network protocols as well. In addition, even though the framework is developed and illustrated in the context of banking and finance, it can also be easily extended to other industries such as healthcare. The key distinction will be in terms of industry specific analysis of relevant risk management, compliance, and controls frameworks and how they can benefit from the other two levels that share many common characteristics across industries.

Besides research focused extension of the frameworks, additional future work is foreseen in terms of development of specific technologies such as enabling automation at the three levels discussed in the article as well as the integration of such technological capabilities across the three levels of frameworks.

5. CONCLUSION

VoIP based networks are a primary avenue for costs optimization and revenue maximization in the global banking and financial services industry. Despite their key strategic role as enablers of revenue growth and customer satisfaction, such VoIP networks are described as the ‘weakest link’ and ‘soft targets’ in global banking and finance networks. To remedy the above situation, the risk management framework proposed herein addresses critical gaps in industry frameworks of prudent risk management and information assurance practices for global banking and finance. Based upon research on industry practices and frameworks on vulnerability analysis and penetration testing activities, the proposed risk management framework identified three levels at which such activities are evident. Enterprise risk management and regulatory compliance by banking and financial services institutions can benefit from adopting and adapting the proposed framework to fit the specific institution’s specific context and needs. Such context-sensitive adaptation can be enabled by integration across vulnerability analysis and penetration testing embedded within overall systems and networks controls framework and overarching risk management framework.

The proposed framework bridges the gaps between corporate strategic policy, controls, and compliance frameworks; systems and networks controls; and, network protocol and network analysis level vulnerability analysis and penetration testing. It reframes the debate on the question: ‘Is pen testing worth it?’ by grounding it in the context of risk management and asking: How can pen testing and vulnerability analysis effectively contribute to the execution of enterprise level risk management, controls, and compliance policies? How can enterprise level risk management, controls, and compliance policies ensure that pen testing and vulnerability assessment are accountable to enterprise risk management execution? While bridging disconnects across risk management policy, systems and network infrastructure controls, and vulnerability analysis and threat assessment such as at the level of VoIP specific network protocols the proposed framework also resolves the multiple dilemmas evident in industry debates about pen testing.

REFERENCES

[1] Accenture. *Banking 2016: Accelerating growth and optimizing costs in distribution and marketing*. Accenture. 2012.

[2] Accenture. *The Next-Generation Insurance Contact Center: Driving the Efficient Growth Agenda*. Accenture. 2011.

[3] Bain & Company, Inc. *Customer Loyalty in Retail Banking*. Bain & Company, Inc. Global Edition 2012.

[4] Booz & Company Inc. *Redefining the Mission for Banks' Call Centers Cut Costs, Grow Sales, or Both*. strategy+business. Booz & Company Inc. 2008.

[5] Cap Gemini. *Trends in Retail Banking Channels: Improving Client Service and Operating Costs*. Cap Gemini. 2012.

[6] Chappell, L. *Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide*. 2nd ed. Laura Chappell University, 2012.

[7] Choi, C.Q. *Cisco IP Phones Vulnerable*. IEEE Spectrum, (December 18, 2012).

[8] Clayton, Lee. *Bank Call Centers May Be the Key to Revenue Growth*. The Gallup Blog. September 20, 2013.

[9] Dwivedi, H. *Hacking VoIP: Protocols, Attacks, and Countermeasures*. No Starch Press, 2009.

[10] Goodin, D. *Extremely critical crypto flaw in iOS may also affect fully patched Macs*. Ars Technica. Feb 22, 2014.

[11] Hamblen, M. *Q&A: Bank of America's Massive VoIP Rollout Detailed*. Computerworld. November 17, 2006.

[12] Hudic, A. ; Zechner, L. ; Islam, S. ; Krieg, C. ; Weippl, E.R.; Winkler, S. ; Hable, R. Towards a Unified Penetration Testing Taxonomy. In *Proceedings of the International Conference on Social Computing (SocialCom): Privacy, Security, Risk and Trust (PASSAT)*, 2012, 811 - 812.

[13] ISACA. *Voice-over Internet Protocol (VoIP) Audit/Assurance Program*. ISACA. 2012.

[14] Kennedy, D., Gorman, J., Kearns, D., and, Aharoni, M. *Metasploit: The Penetration Tester's Guide*. No Starch Press. 2011.

[15] Kindervag, John. *How to avoid VoIP security risks: Forrester's six-step process*. Sep. 30, 2011. Forrester Research, Inc.

[16] Kitten, T. *New wave of Call Center Fraud: Criminals Enhance Telephony Scams to Fool Employees*. Bank Info Security, April 5, 2013.

[17] Lopez, Ernest & Linton, Matt. *Penetration Testing and Vulnerability Assessment*. NASA Ames Research Center. August 17, 2010.

[18] Malhotra, Y. *A Framework for Penetration Testing & Security of Network Protocols for Global Banking & Finance Call Centers*. Global Risk Management Network, LLC. 2014.

[19] Melnick, E.L., Nayyer, P.R., Pinedo, M.L., Seshadri, S. (Eds.). *Creating Value in Financial Services: Strategies, Operations and Technologies*. Springer, 2000.

[20] Olson, Christopher. *Penetration Testing in the Financial Services Industry*. SANS Institute. 2010.

[21] Paulino, C. Pale. Nmap 6: *Network exploration and security auditing Cookbook*. Packt Publishing. 2012.

[22] PCI Security Standards Council. *Payment Card Industry Data Security Standard (PCI DSS), Version 2.0, Information Supplement: Protecting Telephone-based Payment Card Data*. March 2011.

[23] PCI Security Standards Council. *Requirements and Security Assessment Procedures*, Version 3.0. November 2013.

[24] PwC. *When the Growing Gets Tough: How Retail Banks Can Thrive in a Disruptive, Mobile, Regulated World*. PwC's Financial Services Institute (FSI). 2011.

[25] Radman, P., Singh, J., Domingo-Prieto M., Arnedo-Moreno, J., Talevski, A. VoIP: Making Secure Calls and Maintaining High Call Quality. In *Proceedings Mobile Multimedia Security*, (Paris, France, 8-10 November, 2010), 56-62.

[26] Ryan, P. *As Fraud Increases, Call Centers Become Key Security Battleground for Banks*. Bank Innovation. January 9, 2013.

[27] Schneier, B. *Schneier on Security, Cisco Phone Hack*. WWW: www.schneier.com/blog. March 12, 2013.

[28] Schneier, B. *Schneier on Security, Is Penetration Testing Worth it?* WWW: www.schneier.com/blog. May 5, 2007.

[29] Shen, C., Nahum, E., Schulzrinne, H., and Wright, C. P. *The Impact of TLS on SIP Server Performance: Measurement and Modeling*. IEEE/ACM Transactions on Networking, *20*, 4, (August 2012), 1217-1230.

[30] Sicker, D. C. and Lookabaugh, T. *Security, Not an Afterthought*. Queue (ACM), (September 2004), 57-64.

[31] Thermos, P., and Takanen, A. *Securing VoIP Networks: Threats, Vulnerabilities, and Countermeasures*. Addison-Wesley Professional, 2007.

[32] Williams, Jeff. *Beyond Penetration Tests: Tips to Improve Application Security*. BankInfo Security. January 24, 2012

[33] Wright, C. V., Ballard, L., Coull, S., Monrose, F., Masson, G. *Uncovering Spoken Phrases in Encrypted Voice over IP Conversations*. ACM Transactions on Information and System Security, *13*, 4, (December 2010).

[34] Xiong, P. and Peyton, L. A model-driven penetration test framework for Web applications. In *Proceedings of the International Conference on Privacy Security and Trust (PST)*, 2010, 173 - 180.

[35] Zhang, G., and Berthold, S. Hidden VoIP Calling Records from Networking Intermediaries. In *Proceedings of Principles, Systems and Applications of IP Telecommunications*, pp. 12-21, 2010.

[36] Zhang, R., Wang, X., Farley, R., Yang, X., Jiang, X. On the feasibility of launching the man-in-the-middle attacks on VoIP from remote attackers. In *Proceedings of the ACM Symposium on Information, Computer and Communications Security*, (Sydney, NSW, Australia, March 10-12, 2009), 2009, 61-69.