REMOVING SILOS TO PROTECT PROFITS

Aligning Network Security, Fraud Protection and Risk Management
**TABLE OF CONTENTS**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Three Disciplines, One Outcome</td>
<td>3</td>
</tr>
<tr>
<td>Aligning Our Efforts</td>
<td>5</td>
</tr>
<tr>
<td>Revenue Protection Processes</td>
<td>6</td>
</tr>
<tr>
<td>New Efficiency, Increased Security</td>
<td>6</td>
</tr>
</tbody>
</table>
A series of high profile network security attacks, compromising the personal data of millions of customers, has forced providers of communications and internet services to think again about data breaches.

The problem has multiple dimensions. Online services and communications networks are vulnerable to a whole range of threats from hackers and criminals. This makes it essential for you, as a service provider, to take as broad a view as possible of how you ensure the security of your network and the security of your customers.

An alignment of fraud protection, risk management and network security is needed. The business processes that support these elements are evolving fast and are becoming increasingly complex and inter-related. Developments associated with data analysis and business intelligence should be harnessed to promote multi-disciplinary revenue and customer protection. This requires an integrated approach that can align complementary techniques and activities including data capture, machine learning, analysis and workflow management in order to bring potentially separate processes into a single framework.

Instead of considering multiple, disparate processes and activities, each with its own specialist domain and systems, you can aim for seamless protection of the network. This will not only help assure the integrity and security of your network, it will improve revenue and margins and enhance the reputation of your business in the eyes of your customers and partners.

THREE DISCIPLINES, ONE OUTCOME

NETWORK SECURITY

The number and intensity of cyber-attacks has reached record levels. Led by a new generation of threats, these attacks are straining the structure of the Internet itself and are costing service providers not just time and money but also hard earned reputation and customer trust.

In this rapidly evolving threat environment, the ongoing challenge is to identify, deploy and manage the most advanced security procedures and solutions. Given the hundreds of malicious network attacks taking place every year, together with the increasing sophistication and scale of these attacks, this is not an easy task.

Network security protection is not a homogeneous discipline, and it can be broken down into different focus areas:

- **Network and data protection** – These are typically network security infrastructure elements such as malware protection, DDoS detection and mitigation, security event monitoring, firewall management, authentication processes and intrusion detection.

- **Vulnerability management** – These processes focus on detecting vulnerabilities in the network that can be exploited. This can also include the monitoring of traffic anomalies and cleaning data packets to pre-empt the launch of possible attacks.

While you may currently use in-house systems and procedures, there is an increasing trend towards use of cloud-based applications and managed service options which provide cost benefits and, more importantly, 24-hour resourcing and flexibility with which to monitor and secure your network.

FRAUD PROTECTION

Fraud protection should involve continuous monitoring of traffic and investigation of anomalies to provide incremental insight with every increase in the sophistication of attacks. While the types of fraud that are perpetrated against CSPs are broadly similar, each fraud technique is continually evolving. Fraud ranges from the very simple to the very complex, and includes everything from the level of street crime handset theft through cloning, account hacking, employee fraud, and highly sophisticated international and roaming frauds.
Communications fraud continues to be a serious issue. In its 2015 ‘Global Fraud Loss Survey’ The US based Communications Fraud Control Association (www.cfca.org) indicated that fraud cost telecom network operators up to $38.1 billion annually. This is estimated to represent just under 2% of total revenues.

While much focus of fraud management is on protecting the domestic network from fraud attacks, the reality is that a lot of loss-generating fraud takes place in the wholesale environment, using international voice termination and roaming as a means to perpetrate fraud. It should be additionally recognized that fraud attack patterns taking place in one part of the world have a habit of showing up in other places. There is definitely value in having an international dimension to fraud protection.

**PARTNER RISK MANAGEMENT**

While there is increasing service provider focus on internal security, it is evident that some companies pay rather less attention to the assessment of the security practices of their partners and supply chains. Partner risk management can logically be divided into two areas:

- **Customer risk** – The risk of providing a service to a third party needs to be considered. This includes requirements for financial checks, as well as scrutiny of the customer’s business model, line of credit and application of policies for high rate destination monitoring and blocking.

- **Supplier risk** – This requires due diligence, comprehensive pre-testing, analysis of rate sheets for premium rate or unallocated number ranges as well as application of a consistent risk calculation formula.

Partner risk management should be integrated as part of the triple axis of network security, fraud protection and risk management. But often there is pressure to circumvent policy and abbreviate due diligence in order to sign customers or bring onboard new suppliers.

Managing risk in the supply chain is an important component of network security, as network vulnerabilities can be exposed through third party activity, as well as fraud prevention.

For example, dealer fraud can be a significant issue. A dealer might establish fictional customer accounts, sell equipment and services to these phantom customers, then collect the sales commission and disconnect the account and cancel the ‘sale’ prior to the completion of your account update cycle.
ALIGNING OUR EFFORTS

There is both an opportunity and a need for better alignment between network security, fraud protection and risk management activities.

It is time to re-consider the compartmental approach to these related processes. This is less about BSS/OSS architecture and more about process alignment. In fact, with cloud-based applications and managed service options this does not necessarily have to concern in-house infrastructure at all. What it does imply is the orchestration of multiple data processing activities, including:

- **Security management**
- **Fraud protection**
- **Partner risk assessment**

These common functions can be identified, automated and connected for increased levels of security and protection.

Closer process alignment can present a common set of protection management processes and policies, letting you take a multi-dimensional approach to the protection of your network, your customers and your revenue and profit margins.

An integrated approach provides tangible cost benefits, in terms of process alignment and efficiency gains. Reconciliation, analysis, case management, reporting and dashboards can be shared functions. It is recognized that a DDoS attack is often a pre-cursor to a serious hack or fraud attack on a network, thus aligning network security and fraud traffic analysis in this example provides multi-layered protection for your business and your customers.
REVENUE PROTECTION PROCESSES

With the notion of such cross-functional revenue protection, your business benefits from the value of an integrated approach to protecting itself and implementing business process optimization. This leads to the ability to protect data, protect customers, increase revenue, enhance margins and minimize costs across multiple business areas.

To do this involves introducing a fourth element beyond network security, risk management and fraud protection. Using advanced business intelligence (BI) provides detailed analytical and investigative capabilities, linking and correlating information that is relevant for security, risk management and fraud protection.

Analytical capabilities augment operational BI by enabling the evaluation of events and trends at more discrete levels, detecting patterns and correlating information. An analysis-based approach ensures that you are taking a multi-dimensional view of your network operations to protect your business.

- **Network security** - understanding vulnerabilities and applying a policy-based approach to defend against them
- **Fraud protection** - taking a pro-active approach to understanding and responding to traffic abnormalities
- **Partner risk management** - building intelligence into the on-boarding process

NEW EFFICIENCY, INCREASED SECURITY

Network security, fraud protection and partner risk management have tended to be regarded as separate functions. Each area has its own processes, language and conventions. The alignment between these functions should not be sidestepped if you want to achieve optimal protection for your business.

Linking closely aligned processes, common data and business intelligence provides optimum use of resources and information to protect your business. There are common approaches, case management, process functions and information flows that are re-usable across these functions. When properly aligned these processes should be able to graduate towards a more predictive and pre-emptive approach to securing your network and preventing fraud.

Taken to the next logical step, such a platform can become the basis for business optimization activity, used to identify opportunities to enhance revenue, reduce cost, eliminate fraud and maximize profitability. The only obstacles concern process integration, organizational alignment and cross-department negotiation within your own organization. While this concept might represent a challenge to accepted practices, the opportunity is there now if you are willing to embrace new techniques to protect your business.