VOICE : FRAUD PROTECTION — RISK MANAGEMENT

MINIMISE RISK TO MAXIMISE YOUR PARTNERSHIP POTENTIAL

TAKE STEPS NOW TO MITIGATE THE RISK OF YOUR RELATIONSHIPS, AND SECURE YOUR BUSINESS LONG INTO THE FUTURE.

Navigating today's multifaceted communications landscape means working with more partners, across a wider range of services. And managing the risk associated with these relationships has never been more critical – or complex. How do you know, for example, a reseller incorporated in Gibraltar, with equipment in Liechtenstein and a bank account in Austria, can really offer below-market rates from A-Z?

That's where Tata Communications comes in. We have the experience, resources and industry credentials to manage all of your partner risk issues on your behalf. Leaving you free to forge the relationships that will build your business, secure in the knowledge that we've got your future covered.

You'll benefit from:

- Fast and seamless protection across all customer and supplier partnerships
- An easy, hassle-free managed services approach
- A team of highly-trained risk analysts, working round the clock to industry best practise
- Peace of mind at a fraction of the cost of allocating in-house resources

HAVE A SECURITY HEAVYWEIGHT IN YOUR CORNER

Tata Communications has extensive experience in the managed termination space, and more than 30 managed service agreements in place. Continuous training means our analysts are always on top of industry best practice. Addressing both customer and supplier risk, we provide the awareness to prevent any potential problems before they arise. And our extensive and ongoing testing enables you to establish and manage your partnerships in a way that best minimises your risk exposure.

HOW RISK-READY IS YOUR BUSINESS?

You can begin protecting your business today. Use the following checklist to kick-start your risk management policy. Then talk to us for more information about further securing your partnerships — and your future.

- Limit PSTN dialling to essential destinations
- Avoid routing plans which facilitate loop access to the PSTN via the PBX
- Enable call admission controls, for example maximum sessions and registration policies
- Disable non-essential port ranges
- Interconnect over a trusted interface when possible, such as TLS or IPSec
- Apply updates and patches on a regular basis
- Enable dynamic dialling rules if possible, for example enabling time of day and/or routing destination policies
- Secure your edge with an SBC on premise, or via a service provider like Tata Communications
- Limit access and call processing to known IP addresses
- Upgrade your devices using the latest stable release
- Change default passwords for all your devices – especially accounts with administrative privileges
- Use strong passwords with a combination of capital and lower case letters, numbers and symbols
- Put password expiry policies in place
- Establish account lockout policies to combat brute force and dictionary-based attacks
- Set up proper notification policies for locked-out accounts
- Block all 'lower' TCP ports (<1024) to public IPs
- Use non-standard ports for web-accessible interfaces, if they must be accessible from public IPs
- Block ICMP responses for mission-critical devices and only selectively allow ICMP responses to trusted IPs
- Use challenge-response authentication to encrypt communication to any web-based portals over public IP

OUR RISK MANAGEMENT SERVICES

Key features:

- New partner risk
- Due diligence processes
- Pre-testing of routes
- Auto-alert rules and notifications

For customers:

- High rate destination blocking and monitoring
- A-number/CLI management and blocking feature
- Portal variance reporting
- Customised auto alert rules and reports
- Capping feature

For suppliers:

- Supplier due diligence and on-boarding questionnaire
- 'Know your supplier' principal
- Elaborate pre-testing and 25+ point testing schedule
- Calculated risk, including anti-fraud and False Answer Supervision (FAS) amendment for new suppliers
- Analysis of supplier rate sheets, including check of Premium and Unallocated number ranges

- Understand the device you are running — for example, some SBCs allow end-point registration without a username or password as long as an extension is configured
- Block administration access from a public IP for VoIP devices
- Implement strong passwords and if you require public access, only allow it from specific IPs. Consider employing a jump-server architecture such as Citrix
- Enforce standards for voicemail passwords, including periodic password resets
- Disable PBX remote dialling and dial-through capabilities
- Allow only trusted IPs to send to default VoIP ports
- Require carrier authentication using prefixes that are at least six digits long — and change them on a regular basis
- Scan your network from a public IP to discover open ports and secure them
- Test your security measurements by trying to access your own network from a public IP
- Send VoIP calls to your own network to test its vulnerability
- Ignore, or block completely, messages from unknown IPs. Some devices will send 100 calls to an unauthorised IP, only to reject the call in a subsequent message. This only serves to inform an intruder that a VoIP device is available and listening