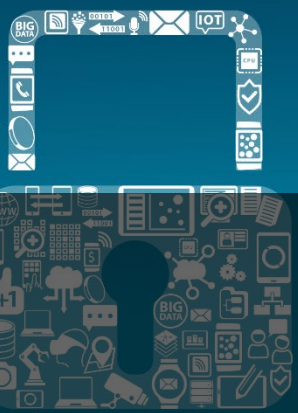

TOLLRING

COMBAT TELECOMS FRAUD:

DON'T JUST CAP IT, KILL IT!


BIG DATA
IOT
WWW
+1
BIG DATA

COMBAT TELECOMS FRAUD:
DON'T JUST CAP IT, KILL IT!

Toll fraud and phone hacking is a multi-billion-pound business for criminals, with monetary damages more than double that of credit card fraud. It is estimated that globally, phone fraud costs £25.5bn per year with the UK being the 3rd most targeted country. According to Action Fraud UK, the average PBX fraud between 2013 and 2016 cost £12,000 per business.

It is the responsibility of the entire industry to combat telecoms fraud. It destroys customer confidence, drives up churn and leads to bad debt. Not least, the income from telecoms fraud could be used to fund organised crime or even terrorism.

Service providers, telecoms manufacturers and their resellers need to take a proactive role in equipping end customers with the latest technologies and approaches to prevent call fraud, to ensure company policies are enforced and to achieve agreed levels of service.

FRAUD EXPOSURE

The rapid growth in Voice over IP (VoIP) services globally (valued at $83bn [2015], with expectations of growth to $140bn by 2021 (source: marketresearchstore.com), presents a major opportunity for crooks. As adoption of these cloud services continues to expand, fraudsters are taking advantage of these more open telephone networks.

The Communications Fraud Control Association (2015) identified the top methods for committing telecoms fraud as:

- US $3.93bn: PBX Hacking
- US $3.53bn: IP PBX Hacking
- US $3.77bn: Premium Rate Service
- US $5.97bn: Interconnect Bypass (e.g. SIM Boxes used as part of VoIP gateway installations)

And the top five countries where fraudulent calls terminate have been identified as Cuba, Somalia, Bosnia & Herzegovina, Estonia, and Latvia.

As criminals become more sophisticated, the types of fraud being perpetrated are increasingly difficult to detect and prevent. For example, fraudsters are starting to take smaller hits on a customer's system, known as 'pick-pocketing', so whilst a credit cap will provide a certain level of protection, these smaller crimes may go undetected but still manage to rack up significant costs.

WHO PAYS?

Regardless of whether customers are using analogue, digital or the latest IP based systems, fraudsters can hack in and gain access to a phone system and SIP trunks in seconds.

By the time the activity is discovered, the hacker is likely to have racked up thousands of pounds in fraudulent calls.

Many end users do not understand the risks and it is estimated that up to 85% of UK organisations may be vulnerable.

Importantly, the recent growth in cloud telephony has brought fraud and credit management to the fore. In the past, the customer was ultimately responsible for ensuring their premises-based PBX telephone system was secure and they largely took responsibility for the cost of fraudulent activities and bad debts.

However, with cloud telephony, the customer now expects resellers and service providers to guarantee fraud protection. In fact, if a provider cannot guarantee fraud protection, they may be unable to sell their services.

For smaller resellers, the cost of fraud can destroy their business. The income these resellers gain from cloud telephony comes in small breadcrumb payments over time.

If fraud happens, a huge chunk of money is required immediately and the reseller and service provider will need to pay; and it will be difficult to entice the customer to share in the costs.

This means service providers and resellers need to be more proactive in ensuring end customers are equipped to combat call fraud. It requires comprehensive and intelligent 'spot and block' capabilities in real-time across both hosted voice and SIP trunking platforms.

IMPROVING CREDIT MANAGEMENT

As a priority, providers and resellers need to consider the following aspects of credit management:

- The implementation of credit and spend-limit management tools can prevent customer bill shock, reduce bad debt and decrease customer churn.

- Providers and resellers need to introduce strict credit checking processes to mitigate risks. Credit checks are standard practice when a large capital outlay is involved, but the nature of cloud pay-monthly services has meant that credit checks have become less common practice, yet this is potentially offering customers an open-ended credit facility.

  For resellers, late payments can become bad debts, and result in increased churn. And churn in cloud telephony is already at about two per cent per month, double that of the mobile industry.

- Spend limits must be appropriate but It is not just about stopping people from making calls to expensive locations, it is also about ensuring normal business use does not rack up massive debts either.

INSIGHT FROM ANALYTICS

Fraud protection is a marvellous by-product of the wealth of analytics and big data that comes from cloud telephony. In addition to being able to see what is happening on a network relating to the performance of features or functions, this huge intelligence can be used to detect fraud.

We can now look at predictive analytics to see what can be done differently across the network to reduce fraud, rather than just relying on a fraud management system as the final gate keeper.

The best approach is to review real-time trends alongside predictive analytics, to eliminate fraud before or as it happens.

SOPHISTICATION BEHIND THE SCENES

As fraudsters become more sophisticated, credit blocking is insufficient to eliminate fraud before or as it happens.

Tollring recommends that calls should pass through multiple rigorous checks to combat fraudulent activity, for example:

- Continuous monitoring
- Real-time checks against a risk register
- Compliance with fraud rules and blacklisted destinations
- Capability to handle whitelist and greylist numbers to satisfy normal business usage
- Historical trend analysis and behavioural pattern monitoring
- Scalable credit management through multi-tier spend limits

The real-time element delivers the capability to 'stop a live call and block future attempts' with immediate effect. Alerts and notifications triggered when rules are breached enable different actions and alerts to be initiated depending on the nature and severity of the breach. Self-learning functionality and dynamic updates are the key to a future-proof solution.

THE VALUE OF FRAUD PROTECTION

For the communications carrier, service provider and reseller, fraud losses can substantially increase operating costs, so it is vital to invest in systems that protect online revenue flows and profit margins.

Improvements in fraud prevention increase customer lifetime value and reduce:

- Time spent handling customer bill shock / disputes
- Customer churn
- Late payment and bad debt
- Liability

For those in Sales and Account Management roles, the guarantee of fraud protection adds value through:

- Product differentiation for competitive advantage
- Increased customer satisfaction; less customer bill shock / disputes, more time up-selling
- Increased customer confidence with zero exposure
- Customer assurance of fraud protection without restriction
- Increased customer loyalty

Not least, preventing fraud is vital if providers and resellers want to protect their brand's reputation, since end customers tend to avoid firms that have suffered data breaches.

A study of over 3,000 adults from the UK, France and Germany found that 50% of consumers would not share data with or buy products from firms that have suffered a data breach.

The study undertaken by F5 Network also revealed that 61% of UK respondents thought firms were not doing enough to protect them from attack.

THE GLOBAL CHALLENGE

The intelligence gained from fraud and credit management worldwide is invaluable in the global fight against fraud. Fraudsters continually evolve their methods of attack so sharing intelligence will strengthen protection and maintain consistency. Fraud associations and trade bodies are the impartial parties that can assist this global challenge.

Alongside new Fraud and Credit Management tools within Tollring's iCall Suite analytics platform, Tollring has joined key players in the fight against fraud including the Internet Telephony Services Providers' Association (ITSPA), the Telecommunications UK Fraud Forum (TUFF) and the Association of Certified Fraud Examiners (ACFE).

These working groups deliver powerful ways to stay ahead of the latest trends in fraudulent activities and offer an opportunity to share best practice on a global scale.

THE EXAMPLE OF CALLJAM MALWARE; A CAUTIONARY TALE

A recently identified mobile malware named as “CallJam” repeatedly calls premium rate numbers once installed, racking up huge bills for the victim. The malware presents itself as a downloadable game in the official Google Play Store.

The unique threat of this malware is that it hides behind a downloadable game that is rated four-stars on the Google Play Store, encouraging people to download it. It is believed that as many as 500,000 people have downloaded the malicious app since it was first uploaded to the Google Play Store back in May 2016. (Source: National Fraud Intelligence Bureau, 2016).

Tollring’s multi-pronged approach would prevent this type of fraud by:

- Identifying that the call is to a premium rate number
- Identifying a change in call trend behaviour
- Using its real-time cost-rating engine, killing the active call and blocking repeat dialling

BT Wholesale Case Study

BT Wholesale launched its white-labelled fraud and credit management solution powered by Tollring in Q4/2016 and immediately found that fraudsters were using new, more intelligent methods to avoid being caught, such as regular smaller activities (pick-pocketing) to stay under the radar.

BT Wholesale works closely with Tollring to develop essential fraud rules in line with current trends on their network and to enable granular refining of the service.

"Intelligent analytics is the only way to stop the next type of fraud." *Dave Axam, Director Hosted Communications at BT Wholesale*

BT wholesale

For BTW alone, Tollring now monitors an estimated 400 new calls per/second (circa. 50,000 concurrent calls), mining this data to produce sophisticated business intelligence, facilitated by the cloud's infinite scalability.

BT Wholesale recently reported over 200% growth in the past 12 months in its Unified Communications hosted platform services, which is set to continue. The launch of this credit and fraud management solution is timely, in line with market growth, meeting the exact and current needs of its customers.

ABOUT TOLLRING

Tollring is taking major steps to not just reduce fraud in cloud telephony but to eliminate it.

Tollring is a market leading software developer providing data visualisation and business intelligence tools that help manage, understand and control a wide array of communications information, resources and assets.

With offices in the UK, the USA, India and Australia, Tollring specialises in business communications analytics, call recording solutions, telecoms expense management and fraud detection. Deployed as one single solution in the cloud, Tollring focuses on delivering the right information at the right time, accessible on any device.

Our innovative solutions are developed in-house and distributed via an extensive channel partner network to over 27,000 businesses globally.

Tollring prides itself in its high levels of technical capability and strives to deliver outstanding levels of support having been certified in quality standard ISO 9001 and ISO/IEC 27001 for Information Security Management.

TOLLRING

UK | USA | INDIA | AUSTRALIA

WWW.TOLLRING.COM


BIG DATA
IOT
WWW
+1
BIG DATA