PBX Hacking takes a Toll on Business

ebook

FracTEL®
Telecom Perfected™

PBX Hacking Takes a Toll on Business

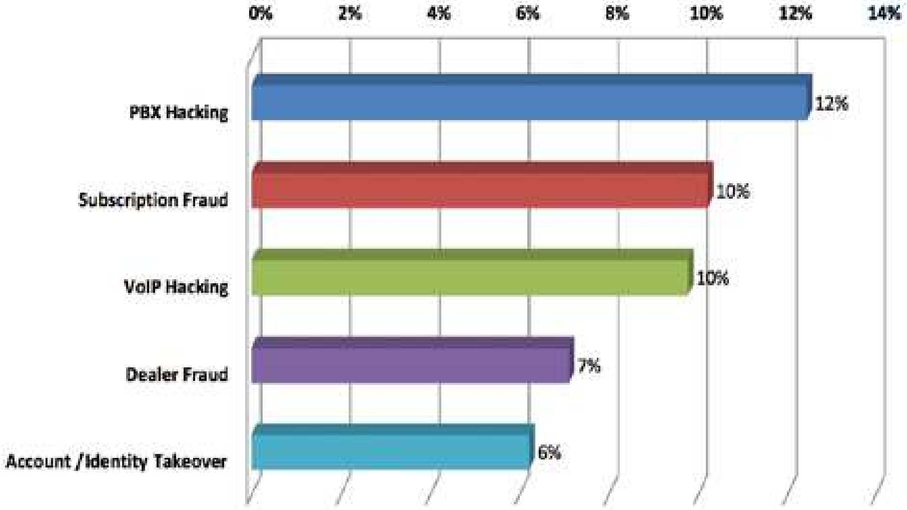
While developments in IP telecommunications technology have brought about many benefits for businesses, they have also been accompanied by an elevated frequency of PBX hacking and phone fraud. Individual hackers and highly organized criminals have increasingly been able to gain access and compromise phone and voicemail systems to steal business data or make expensive long distance calls. These threats and security issues can be highly consequential for any business operating a phone system. For businesses chartered with privacy requirements, the damage can be catastrophic.

In 2011, phone fraud occurring from compromised PBX systems was the single largest source of fraud loss for businesses.

While credit card fraud accounted for nearly $2.4 billion dollars in 2011, phone fraud more than doubled that, approaching nearly $5 billion dollars lost. By 2013, that amount increased to more than $25 billion. Businesses are at a huge risk when it comes to phone fraud, and the leading cause is unsecured and unmonitored PBX systems. Preventing fraud should be a priority for every business, but the challenge is tough to overcome. Evaluating the risks of fraud and taking the necessary precautions to prevent fraud are steps that every business should take.

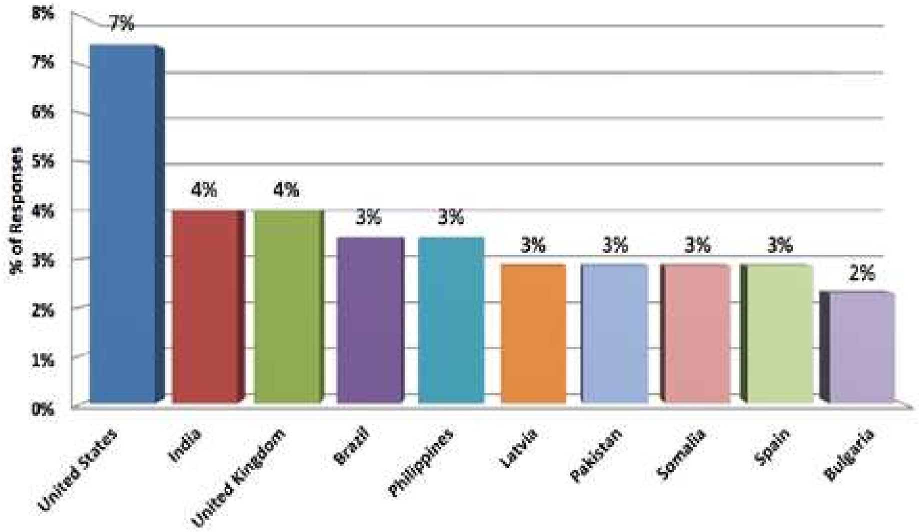
The average loss per phone fraud incident is between $10,000 and $80,000 dollars. For small businesses this can be devastating. Past performance is no way to adequately assess the threat that phone fraud poses for your business, as the technology and motivation to perpetrate fraud are relatively novel. If you have an IP phone system, it is almost certain that it is being probed for weakness constantly. It is important to keep in mind that without any kind of protection or insurance from phone fraud your company will be held fully responsible for any losses you experience. Court decisions

Top 5 Emerging Fraud Methods Globally



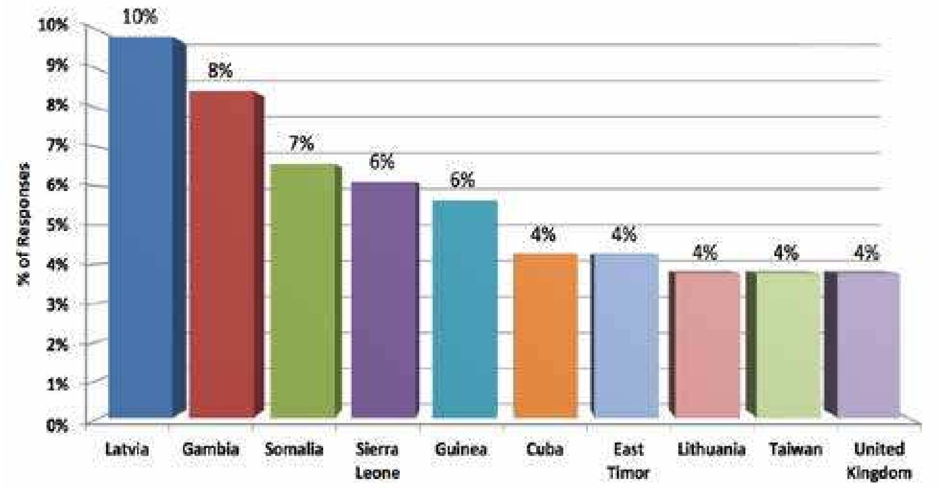
Top 10 Countries from which Fraudulent Calls Originate

Ten countries account for 35% of the originating global fraudulent calls



Top 10 Countries where Fraud Terminates

These top ten countries count for more than 40% of global fraudulent calls



have unambiguously decided that the responsibility falls on your business rather than your carrier or service provider. Since the carrier gets paid to provide these phone calls whether they are fraud or not, they are not necessarily financially incentivized to help you control the problem.

Victims of phone fraud aren't limited to bad neighborhoods or even urban/metropolitan areas. The internet makes it possible for bad actors on the other side of the world to perpetrate their crimes anywhere they find the opportunity. The hackers behind phone fraud search all over the world for potential targets, paying no mind to who or where they are. It is common for these villains to strike late at night or on weekends when their activity is least likely to impact service and be detected. Unfortunately, if they gain access to your system, they can make phone calls costing thousands of dollars in a matter of minutes. Even more unfortunately, the remote nature of the crime makes it almost impossible to catch and prosecute these bad guys.

How Do Hackers Profit?

Methods vary, but all create benefit for the thief at the expense of the business owner. Following are some of the methods that hackers use to monetize theft:

Outbound Calls

Access is used to make outbound calls to expensive "international premium rate" numbers for which the thief receives compensation. These numbers are analogous to "900" numbers in the US but are much more expensive for the caller and much more lucrative for the owner of the called number.

Calling Card

Access is sold, either directly or indirectly, to companies that provide calling card or call shop services, typically international calling to very expensive destinations.

Autodialers

Access is used by autodialers, making massive amounts of calls to facilitate telemarketing fraud or other illegal activity. This sort of fraud is often utilized by the hackers to support still more fraud, such as phishing (trying to scam individuals into giving social security or credit card information).

PBX hacking for the purpose of data theft can be even more expensive and damaging to a business. A surprising amount of proprietary data is typically stored in a phone system. For example, a modern PBX is likely to store some or all of the following: customer and/or employee contact information, call records, voicemails, and call recordings. For many businesses, loss or theft of this information could represent an existential threat. A compromise of privacy compliance can also result in massive fines. For example, the fine for a violation of HIPPA compliance can be up to $100,000 per incident. For many businesses, eavesdropping on calls should also be a major concern. While recent revelations regarding law enforcement eavesdropping have created a great deal of controversy, the use of similar technology by criminals represents a much higher potential for abuse and damage.

6 Tactics to Secure your Business Phone System

Being educated on the tactics of hackers is a valuable way to make sure your business isn't affected. Take note that one of the most common methods of obtaining credentials is social engineering (i.e. the company or an employee giving up valuable information as a result of being scammed). By recognizing the signs of a scam, businesses can often keep hackers away from their secure information. Improving PBX security takes many forms, the following are a few common steps:

Use Strong Passwords

This may seem like a no-brainer, but the lack of password protection is one of the biggest reasons people get hacked. Never leave a server or phone with a default password, and make sure that all equipment has strong passwords set - no exceptions. Secure and limit credential access to individuals with a need to know. The best PBX systems use secure provisioning files to completely obfuscate all device credentials.

Manage Extensions

The most common intrusion vector for phone fraud is hijacking a remote extension. If you have phones outside of your LAN, pay extra attention that they have strong credentials and restrict them to a static IP if possible. Always remove unused extensions from your system. If you use an Asterisk based system, programs like Fail2Ban can help detect and stop hijack attempts.

Move to the Cloud

Consider a cloud-based PBX solution that removes the premise PBX as an intrusion vector. This shifts responsibility for security of the biggest and hardest to protect component of the system to your phone provider.

Border Control

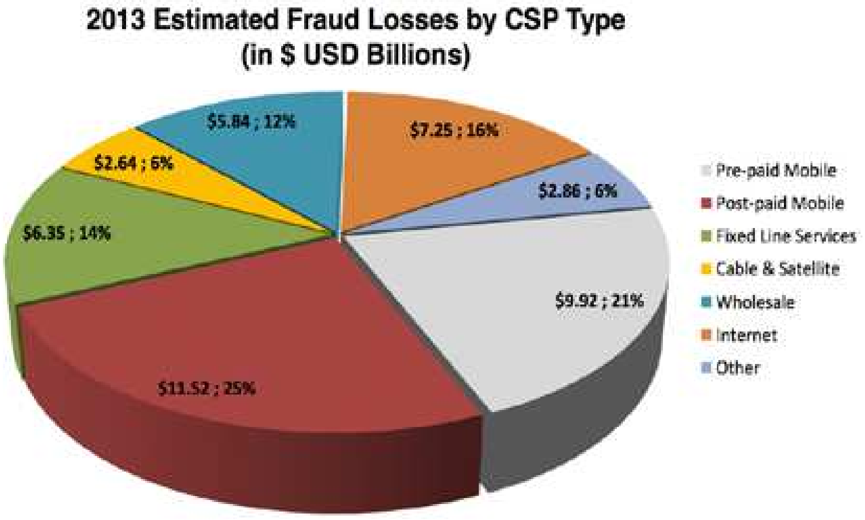
If you elect to use a premise PBX, use a capable firewall or session border controller (SBC) to restrict outside internet access to the minimum required for proper functionality. If the bad guys don’t know the PBX is there, they won’t try to get access. If possible, use IP peering as authentication to your provider. This is the form of authentication carriers use to talk to each other and has proven to be difficult to compromise.

AES Encryption

HIPPA Safe Harbor compliance requires that data be encrypted “in storage and in transport”. For phones, this should include AES encryption of signaling and media. Select a provider that can provide this.

International Calling Restrictions

If you do not need international calling, ask your provider to disable it. If you do need international calling, select a provider that can provide restrictions such as access codes, area restrictions, rate limits, credit limits, etc. These features can help limit the damage in the event you are somehow compromised.



Toll fraud and PBX hacking are a genuine threat to your business, but should not prevent you from taking advantage of the many benefits to be gained from IP-based communications.

Selecting the right provider can often give you all the protection you need. FracTEL®, a leading provider of communication solutions for business, has implemented an extensive 15 point fraud protection program, featuring an intelligent call monitoring system that provides automatic, real time notification of any suspicious activity. Their proprietary technology gives FracTEL the confidence to offer a $1,000,000 fraud insurance policy to users of their CloudPBX service.

Ask us about how
we've been perfecting a better
business phone system

FracTEL®
Telecom Perfected™

+1 (855) FRACTEL
372-2835

fractel.net

sales@fractel.net

Statistical information and charts taken from 2013 Global Fraud Survey from the Communications Fraud Control Association. www.cfca.org