The Callista Group

The commercial consequences of a phreaking attack.

BCL
DELIVERING DIGITAL EXCELLENCE

Caterham • Surrey • UK

This case study has been prepared by The Callista Group with the kind permission of BCL.

BCL's PABX reseller, maintainer and call air-time provider declined to be named in this case study and their identity has been withheld. For the purposes of this Case Study they have been referred to as X Ltd.

Case Study

A bit of background

A telephone system for any business is like oxygen - invisible but utterly vital. But it's also one of any company's most vulnerable assets because up until now there has been no effective means of securing it from hackers intent on routing their own illegal traffic through it.

Phreaking (or phone hacking, toll fraud, dial-though fraud) is not new. In the 1990s it was principally the domain of adolescents with a phone line and a keyboard looking for a bit of fun and making a couple of calls on someone else's tab to their friends in Wandsworth or Wellington – just because they could and just for a laugh. So far, so innocuous – but still illegal – and often these calls would go unnoticed amongst the vast number of calls in any month on a company's phone bill.

But phreaking in the 21st Century has gone from geek to something much more sinister and much more damaging. Today it's big business and organised crime often with links to terrorists intent on raising funds for their illicit activities and the victims of this fraud are their unwitting accomplices because they have to pay. As this Case Study demonstrates, when phreakers attack, the only winners are the phreakers themselves – and the telecommunications carriers who demand payment for the tidal wave of illegal call traffic phreakers generate at the victim's expense.

But no one – including PABX manufacturers and PABX resellers alike - wants to admit it's going on for fear of litigation from their customers for supplying telecommunications equipment which until now could at best only be secured via its own internal and very rudimentary security which as it turns out, can be breached by skilful phreakers in milliseconds. In short, useless. Insiders say that phreaking is the telecommunications industry's biggest secret, generating massive funding for the telecommunications bandits at the expense of their innocent victims who can sometimes face the very real threat of bankruptcy if they cannot pay. And it also creates massive and unexpected income for telecommunications carriers.

According to the Communications Fraud Control Association (CFCA) worldwide industry experts now estimate annual global telecommunications fraud losses to be in the range of USD72-80 billion – an increase of 34% from their survey five years ago.[1] Even more disconcerting, the CFCA maintains the UK is now one of the top five countries targeted by phreakers.

> *" The results of this survey confirm that telecom fraud is a more lucrative criminal business than we initially thought and that the problem is getting worse."*
>
> **John Frost, CFCA President**

In this Case Study the very real commercial consequences of a full-blown, professional and relentless phreaking attack on just one business in the UK is examined.

Setting the scene

BCL is an independent company of very longstanding which has supplied a wide range of business environments from home offices to large corporations with office automation products for 31 years. BCL purchases its call airtime from X Ltd, its PABX maintainer, a reseller of Siemens and Toshiba phone systems and a call air-time reseller of Opal, a British telecommunications carrier. X Ltd also supplied BCL's Siemens Hipath PABX. BCL has been a customer of X Ltd for five years and its average monthly phone bill is normally around £500 - £600. X Ltd has been a reseller of Opal's call air-time for 12 months.

This frightening story started to unfold one Monday evening in July 2009 when X Ltd was informed by Opal of "unusual call volumes" on BCL's lines via its Siemens HiPath PABX. Even more frightening, they said that this activity had been detected all through the previous weekend. X Ltd immediately examined BCL's phone records and determined that the calls had not been made as part of BCL's normal business activities and they were therefore identified as illegal calls.

X Ltd maintains it could not get remote access to BCL's PABX at that point so they placed an immediate block on BCL's lines preventing outbound international calls being made on them. They also maintain that they arranged to despatch one of their engineers to BCL's offices the next day. They claim they immediately informed Opal that the "unusual call volumes" they had detected more than two days earlier were the result of a phreaking attack on BCL. Opal allegedly responded dismissively to this and allegedly maintained it "was not their problem".

Two days later on Wednesday evening – and almost five days after this phreaking attack had begun and had been detected - BCL received an urgent telephone call from an X Ltd employee telling them that "unusual calling patterns" had been detected on their lines. At the time the cost of this unusual activity was estimated at £2,000. This total was revised by X Ltd over the next few days to an alarming £10,807.14 – ***more than 20 times the amount of BCL's usual monthly phone bill.***

What unfolded next

In the ensuing weeks significant correspondence passed between BCL and X Ltd both claiming the other was responsible. BCL claimed X Ltd was culpable because they not only supplied their Siemens HiPath PABX and had failed to secure it successfully from phreakers but also for waiting until the cost of the phreaking attack had mushroomed to more than £10,000 before alerting them to it.

X Ltd claimed BCL was at fault because the security of their PABX lay with them. Moreover, X Ltd claimed that they had installed BCL's Siemens HiPath PABX in "good faith" and to the exact specifications recommended to their engineers by Siemens at its accreditation courses but which had clearly not secured this now stricken PABX.

At no point was the PABX manufacturer, Siemens, contacted by either BCL or X Ltd for its opinion and advice on how to further secure BCL's PABX which had been secured according to Siemens's own specifications and which clearly had not worked and to let them know that the security they had recommended for their PABXs had been breached.

Opal - the carrier - demanded payment of the entire amount and claimed no responsibility at all. In their opinion if the calls were made through a private phone system, irrespective of whether these calls were authorised by the owner or not, the owner was responsible for payment. This is the universal view of telecommunications carriers everywhere.

> *" X Ltd said they had never heard of this type of hacking before but later at a meeting I had with them, they changed their story and their MD told me of a similar incidence elsewhere."*
>
> **Richard Shute, Director, BCL**

X Ltd locked down BCL's PABX so that in their opinion no further phreaking attempts could succeed. They started by blocking access to international outbound dialling since they had already ascertained that most of the previous illegal activity had been to these calling destinations and then monitored BCL's PABX daily. But as soon as international outbound calls were blocked via BCL's PABX, the phreakers immediately switched to routing their mobile outbound traffic through it. When X Ltd blocked access to these calls, the phreakers immediately changed tack again and began routing their calls to premium rate numbers through it.

It became very apparent that this was an organised and determined attack on BCL's PABX. As soon as changes were made in its programming to block the phreakers' access to international and mobile numbers, they immediately reacted to this and started channelling different call types through it which meant these hackers were effectively operating as a carrier and were able to react very quickly to any programming changes in BCL's PABX to maximise their access to it.

> *"These phreakers had perfect technical knowledge about how to control this PABX and they knew exactly what they were doing. We were shocked."*
>
> **Director, X Ltd**

Opal then demanded payment from X Ltd for the full amount of the phone bill rendered to them on BCL's behalf.

BCL called the Police to investigate the crime which had been perpetrated against them via their phone system and on investigation the Police discovered that ***the phreakers had gained access to BCL's Siemens HiPath via its password-protected voicemail ports***. After making some enquiries, the Police discovered other cases of similar fraud but they conceded the likelihood of tracing the perpetrators was remote.

> *"We welcomed the Police being called but we became totally disillusioned when they said they were unable to trace these hackers and that no further investigation would ensue."*
>
> **Director, X Ltd**

X Ltd for its part insisted that on installation of BCL's phone system, BCL's staff was directed on how to change the passwords on their Siemens HiPath voicemail boxes. BCL claims X Ltd's technicians did not do this but instead allegedly told them they could be changed "but no one ever does". X Ltd disputes its technicians made this claim.

In any event it was clear after the Police investigation that passwords, no matter how many times they were changed, would not have and could not have prevented this attack.

X Ltd then insisted on payment in full from BCL of the £10,807.14 phone bill and BCL consulted its lawyers – and its insurance company.

> *" Our insurance company declined to pay out claiming that we were responsible for the security of our PABX and our lawyers wouldn't accept our case unless they were 53% certain of winning and they said this was unlikely."*
>
> **Richard Shute, Director, BCL**

In the meantime and while the debate about culpability continued, BCL's PABX remained stricken with all international outbound dialling blocked and with only passwords on its voicemail ports which had already proved to be completely ineffective against phreakers intent on getting access.

Following a flurry of solicitor's letters between BCL and X Ltd in an attempt to settle this matter, X Ltd who had already agreed at their initial meeting with BCL to waive half the bill as a "gesture of goodwill", insisted BCL pay the remaining half of £5403.57 by the following Monday. BCL refused and X Ltd immediately disabled the ability for BCL to make any outbound calls of any type from their PABX. Moreover, X Ltd also threatened to disable BCL's ability to receive incoming calls if payment was not made. X Ltd maintains they only did this "as a last resort" and because they were under pressure from Opal (the carrier) to settle the entire outstanding phone bill.

> *"As a service provider we would not have been able to function at all had they done this and our customers would not have been able to receive the service from us they pay for. So in the interests of preserving our business and maintaining the ability to support our customers we had no choice but to pay - so we did. In return, X Ltd's only solution to prevent further phreaking attacks was to completely disable our ability to make outbound international calls and our voicemail ports remained protected only by passwords which had already proved completely ineffective against phreakers."*
>
> **Richard Shute, Director, BCL**

Shortly afterwards BCL contacted The Callista Group directly to enquire about Control Phreak, Callista's automatic PABX firewall to try to find a more satisfactory way to secure its PABX against fraud. X Ltd agreed this would be a good idea and at BCL's expense they arranged to install a LIM card into their Siemens HiPath so that the installation of Control Phreak could proceed.

Almost 10 months later Control Phreak was installed at BCL in April 2010 but in the meantime their only source of security was to essentially shut down significant functionality on their PABX and to rely again on ineffective password protection on its voicemail ports.

> *" We're appalled at the attitude of telecommunications carriers. They should be forced to stop hiding behind the data protection rules they use as an excuse for not tracing phreaked calls."*
>
> **Director, X Ltd**

In conclusion

This story highlights some very glaring deficiencies in the way PABX security is perceived and promoted by manufacturers, resellers and maintainers and as a result it is largely misunderstood by their customers who are the ultimate victims in the event of a phreaking attack. Despite claiming that their PABXs are and can be secured against crimes of this nature by the rudimentary security options all PABXs have, this is far from the truth and as this case study demonstrates, completely failed to keep BCL safe on any level from a phreaking attack.

The phreakers who struck BCL's PABX were clearly highly organised, highly skilled and highly determined and as soon as they knew the avenues open to them via this PABX were being systematically closed to them, they quickly reprogrammed it to route other call traffic through it. In this instance nothing could keep it safe - short of shutting down this PABX completely but this was not an option because it would have completely compromised BCL's business.

It also highlights where the lines of culpability should be drawn. Anyone who operates a business is responsible for the security of that business and all the equipment they run. However, PABX manufacturers and their resellers also have an obligation to make all of their customers aware of the security danger and to make them aware also of the limitations of the resident security in the devices they promote and sell – and that this will not keep them safe in the event of an assault by organised, professional hackers – or by any hackers.

But most of all it highlights that in any phreaking attack there are only ever two winners – the phreakers themselves and the telecommunications carriers who benefit significantly from the unexpected revenue generated for them globally by these telecommunications bandits. Meanwhile the PABX owner who is always an unwilling and an unwitting accomplice in these crimes will be expected to pay for it – and often the amount they have to pay is huge.

Had Control Phreak been installed at BCL when their Siemens was commissioned for them, this unfortunate and costly attack on them would have been thwarted automatically.

[1] CFCA 2009 Report