VoIPstudio White Paper

Ensuring the security of your VoIP service.
Why it matters and how to achieve it

Ensuring the security of your VoIP service

Introduction

Hosted VoIP is now mainstream and will soon be the dominant means of enabling effective business communications. According to data from Cavell Group, a consultancy firm, we are moving towards a tipping point in hosted telephony: the ongoing decline in on-premises solutions, such as PBXs, is about to be overtaken by the growing market penetration of hosted services around the world[1].

Thanks to advances in network speeds and their reliability to carry voice and business data over the same lines, as well as improved connectivity of a range of devices, cloud-based VoIP services will soon replace traditional on-premise solutions in the enterprise. Put simply, hosted VoIP is now mainstream and is set to become the dominant means of enabling effective business communications.

For example, according to Cavell Group, strong growth over the last 6 months has brought the UK hosted VoIP market to over 3 million users, making the UK the leader in Europe in terms of numbers of Hosted VoIP users.

Strong market growth predicted

The research collected from 94 UK services providers confirms that the market has grown 11% in that period with a million further users connected in the last seven calendar quarters. A remarkable increase given that the first 1 million users took 3 years to achieve.

But it is not just the UK showing significant growth in the hosted VoIP market. France, Netherlands and Germany each now have between 1 million and 1.5 million seats. Cavell predicts the total European market to grow by more than 17 million users over the next 5 years at a CAGR of just under 25%.

Meanwhile, research from market analyst house IHS Markit shows that a decline in on-premises PBX licenses caused an 8% drop in the total global market in 2017, compared to 2016, to $5.7 billion. Total PBX lines were down 9% year-on-year in 2017, with every segment taking a hit.

Author of the report, and senior research director for VoIP, UC and IMS at IHS Markit, Diane Myers, blames the fact that businesses have been holding off on upgrades and new purchases, and that the on-going move to cloud services is having an impact on the market.

It's not just a sign of lowered spending either. According to IHS Markit, enterprise spending is healthy, but businesses are giving low priority to telephony upgrades and expansion on the premises side – which strongly suggests that they are shifting resources towards cloud deployments.

TOTAL EUROPEAN MARKET
FOR **HOSTED VOIP**
WILL GROW BY MORE THAN
17 MILLION
USERS OVER THE NEXT 5 YEARS
AT A **CAGR OF JUST UNDER 25%**

1. https://www.cavellgroup.com/cavellvoice/cloud-communications-starting-to-bite-into-traditional-operators-revenues/

The benefits of VoIP

There are clear reasons why enterprises are increasingly looking to hosted telephony solutions, as they offer multiple benefits. Of course, many companies and users are attracted by lower cost. Cloud services reduce CAPEX – the cost of purchasing, installing or upgrading a traditional PBX system is far greater than installing a hosted VoIP system. In fact, extending or upgrading legacy hardware to modernise services, for example, often costs more than a complete new deployment of VoIP.

Lower cost, richer features

At the same time, many VoIP solutions offer a free or inclusive call package, which reduces OPEX. Hosted solutions require no maintenance or upgrades, and usually offer free technology upgrade roadmaps, which are the responsibility of the provider.

Indeed, cloud-hosted solutions offer the latest technology, updated constantly, at no additional cost to the customer. They offer inclusive services such as conference calls, instant messaging and mobile communications, while remote workers are able to conference call from other locations at no additional cost. Messages can be broadcast to groups, while some VoIP services can also transcribe voicemails and send them via email to ensure that messages or calls are not missed.

Other inclusive services might include call hunting, single number, virtual receptionist, in-browser IM, and allow deskphones and softphones to be used simultaneously.

Many businesses, such as inbound and outbound contact centres, need to scale communications systems rapidly according to peak demands. As VoIP services are device independent, and simple to use, they allow enterprises to add and remove lines and users quickly and easily, according to capacity demands. Of course, it also removes the need to pay for redundant capacity, compared to traditional systems. In such platforms, lines are often purchased on a ‘just in case’ basis, but only used during periods of peak activity.

Efficiency and productivity enhancements

Other benefits to business might include consolidation of costs, as other services are migrated to the cloud, while ‘aaS’ models offer greater cost savings and business process streamlining. VoIP solutions can also be integrated easily and seamlessly with existing hosted CRM systems, resulting in improved customer services and call handling, as well as the option for ‘upselling’ or prospecting.

However, the biggest benefit to enterprises is that hosted VoIP can significantly boost employee productivity and efficiency, while providing business flexibility and agility, in addition to the lower cost of ownership.

“Cloud hosted solutions...offer inclusive services such as conference calls, instant messaging and mobile communications, while remote workers are able to conference call from other locations at no additional cost. Messages can be broadcast to groups, while some VoIP services can also transcribe voicemails and send them via email to ensure that messages or calls are not missed.”

The challenge of security for VoIP

Perhaps one of the biggest challenges holding business back when it comes to migrating to hosted solutions, however, is the perception of security vulnerability. In general, the costs associated with protecting and defending against attacks and vulnerabilities have risen for all enterprises, in line with the frequency of such attacks.

VoIP is no different and can also be vulnerable. VoIP phones rely on Internet connections, which means that potential security issues cannot be overlooked. The cost of recovery after any security incident can be high, so a VoIP service that is not inherently secure is a false economy – unfortunately, not all hosted VoIP solutions are as secure as others.

What are the security requirements for VoIP?

To be secure, a VoIP solution needs to protect against a number of threats and vulnerabilities. These range from privacy policy and data vulnerabilities to technical threats in the network and in data centres. For example, many attacks focus on VoIP operating systems, internet protocols, the interfaces of VoIP hard phones and device-based softphones – all of which are vulnerable to unauthorised access, viruses and worms. In addition, denial-of-service (DoS) attacks can bring down entire systems.

Generally, VoIP security threats can be broken down into 3 broad areas:

1. Can anyone hack into my call?;
2. Are my networks and devices safe?; and,
3. Can someone else hack into, and use, my account?

More specifically, just some of the threats that VoIP solutions need to secure against include, but are not limited to:

- Phishing attacks – where businesses or employees are tricked into giving out confidential information.
- Denial of service attacks
- ID spoofing or 'masquerading' – hackers make calls and change caller ID information.
- Call hijacking – calls are routed to different locations or are "listened in" to by individuals outside of the business.
- Service theft – whereby hackers break into business or employee accounts and route the service elsewhere, while locking the paying user out of their account.
- Malware – hackers download spam or malware onto on-premise devices via the VoIP software.

Security is as essential for VoIP services as it is for any other enterprise application, with the costs associated with a cyber-attack growing each year.

For example, a recent report from Accenture found that businesses face an average of 130 security breaches per year, and that the average cost associated with resolving such an event for companies of all sizes is $8.74 million in the UK, and a staggering $18.25 million in the US[2].

Of course, these are not all attacks on VoIP services and systems, but according to a report from IBM's Security Intelligence Group, 51% of all security events analysed in 2016 involved attacks that used the VoIP protocol Session Initiation Protocol (SIP)[3].

It's an easy extrapolation to understand the costs that can be associated with VoIP attacks – certainly in the millions of dollars range.

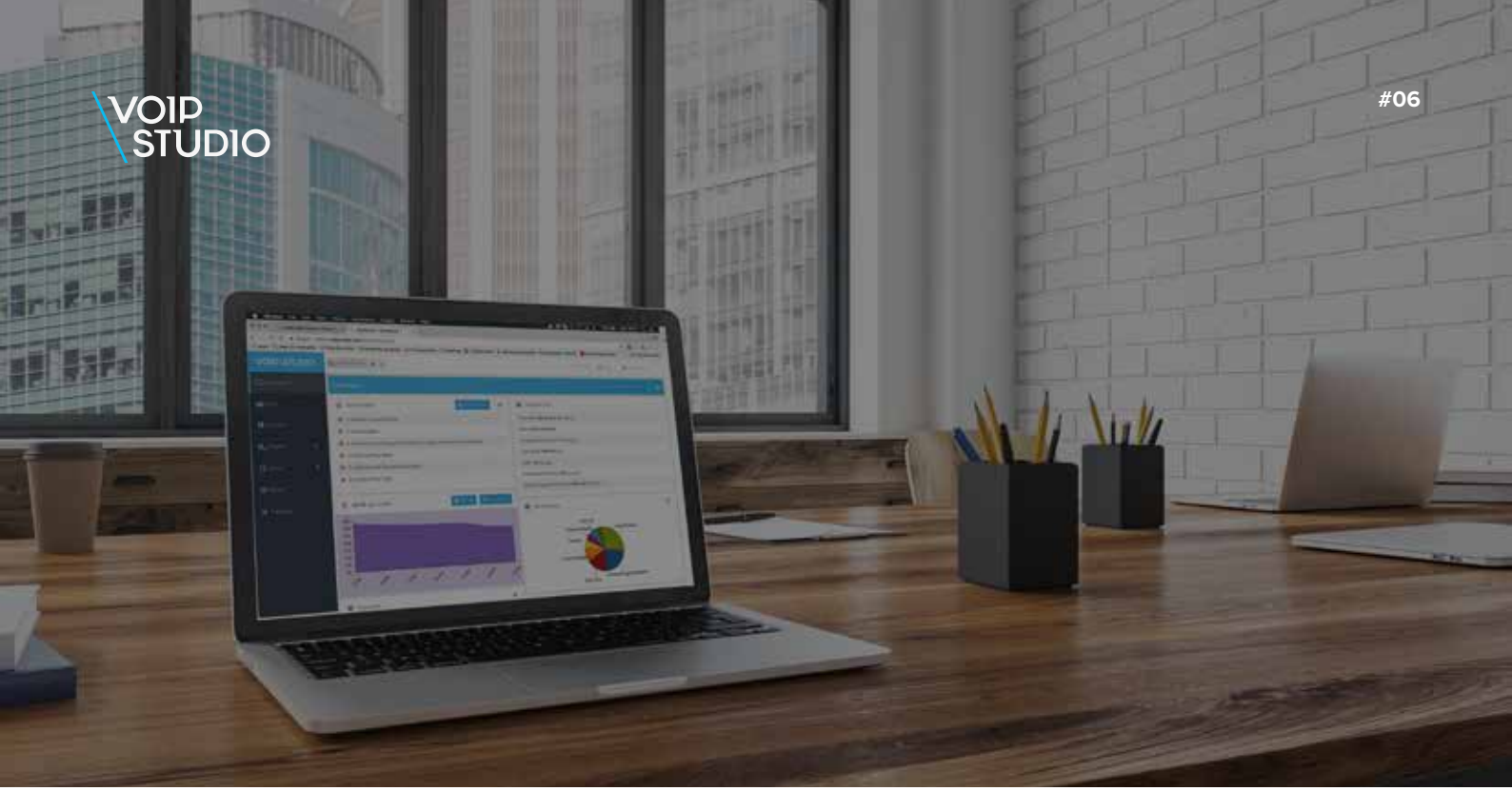
As a result, security needs to be a key selection criterion when choosing a hosted VoIP solution. What factors matter for ensuring the security of VoIP solutions?

VoIP security brings its own set of challenges in addition to the existing security problems of data networks. As well as vulnerabilities in the data centre – as for any data-based application – VoIP security threats extend to softphones and mobile clients, as well as to remote sites and often to temporary workers and contractors, which brings its own set of challenges that boil down to employee negligence.

As such, VoIP security requires a layered approach that includes data, devices, networks, applications and people.

2. https://www.accenture.com/t20171006T095146Z__w__/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50

3.. https://securityintelligence.com/hello-youve-been-compromised-upward-attack-trend-targeting-voip-protocol-sip/



The VoIPstudio solution

VoIPstudio is a cloud-hosted communications platform based on solid infrastructure that's designed to enable flexible yet secure connections between users, wherever they are. Security sits at the heart of our solution, and we adopt a multi-faceted approach towards ensuring our customers' security and peace of mind. We are dedicated to providing a resilient, secure service, and as such we adhere to all the major compliance requirements and regulations. We perform regular testing, scanning and audits on our infrastructure, and provide our customers with transparent information with regards to our security and privacy policies.

We also ensure that our network, systems, and applications are fully protected. For example, all connectivity to our networks or servers hosting customer data is defended with security mechanisms such as IPsec, Transport Layer Security (TLS), and Tunnelled Transport Layer Security (TTLS) – all of which provide strong encryption and authentication over VoIP networks.

However, technical capabilities, while necessary, are not sufficient. VoIP security requires cultural practices and clear supporting processes. Security starts at home, so we ensure that all of our employees adhere to company-defined processes and audit trails to ensure account integrity and to ensure there is no unauthorised access to data. We perform monthly security scans, and conduct a regular infrastructure audit for PCI compliance, which is performed by an external party. We continually perform vulnerability testing against threat and attack vectors to detect any security vulnerabilities in payment processes, to avoid ransomware, and other threats.

All of this has resulted in the creation of the following key security and compliance monitoring standards and procedures:

- Defined and documented organizational security standards and procedures.
- All employees and contractors required to sign a confidentiality agreement.
- Background checks for all employees that have access to customer data.
- Restricted access to only those employees that need to manage customer data or manage servers hosting customer data.
- Process for the timely removal of access to customer data from any employee or contractor that leaves the company or who no longer requires access.
- Continuous staff training on all internal security policies and general security awareness.

VoIPstudio is also certified by the UK Government Ombudsman, under the Information Commissioner Office and meets the upcoming requirements of the EU General Data Protection Regulation (GDPR), meaning that our customers can rest assured we adopt and meet not just current requirements, but also regulations as they evolve.

Data centres, encryption and hosting

Security also requires a robust system and operations. All calls made over VoIPstudio are routed via three data centres in the UK, US and Japan, which not only ensures better routing of calls but, but also provides a robust network with instant disaster recovery in the event of any unforeseen event so that your business can continue to operate.

All of our data centres are ISO 27001 certified, which ensures the highest possible standards of data security. In addition, all of our physical storage devices employ the highest standards of data encryption, using AES-256 to encrypt data. We also use TLS-encrypted SIP signalling and ZRTP for encrypted WebRTC voice streams.

All customer data is compartmentalised to prevent unauthorised access to the data of other customers. Individual data is also protected by 'hardened' passwords that are 'rotated' on a 90-day basis.

The physical security of our data centres that host the servers containing customer data is also assured. In order to ensure upmost security, all our data centres meet the following requirements:

- Rooms are secured by at least two access mechanisms (e.g., building key- card, man traps, security guard, and computer room badge-in).
- Only authorized employees are allowed physical access to the servers hosting customer data.
- 24/7 security at each data centre.
- All backups of customer data are either stored on-site with controlled access or at a secure vendor controlled location.
- The site supports additional levels of protection such as uninterruptible power and re suppression.
- Failed storage components in the data centre undergo an MoD-approved "erase" or "wipe" procedure (if functionally possible) prior to destruction.

We also have formal security policies and procedures in place for dealing with viruses, malware and related threats should such attacks occur. Anti-virus software programs are active on all Windows-based machines in our centres, and these systems have automated periodic full scans and use updated virus signature files.

User Management and Integrity

We also ensure that we protect the confidentiality, integrity, and availability of customer data. For example, each user is assigned a unique ID, and access to data in the VoIPstudio database has permission-based controls restricting access to authorised customer users only, as determined by each customer data owner.

Any change of user login status is also logged – these logs are treated as confidential information, and access to these reports can be restricted using the permission system. VoIPstudio also supports 256-bit SSL encryption between each component of the communications path for the transmission of confidential data, personal data, or authentication information, adding a further layer of protection.By implementing such a broad security strategy, VoIPstudio enables end-to-end security from human access to data centre integrity right through to strong technical controls and technologies throughout our network, ensuring that our customers can rest assured that we are dedicated to guaranteeing the security of our VoIP communications solution.

Conclusion

Hosted VoIP solutions are becoming the dominant means of enabling business communications. But, like every other enterprise application (hosted or on-premise), they need to deal with a growing number of security threats and vulnerabilities. Hosted VoIP is vulnerable to attack, which can lead to significant distress and, of course, costs. These must be avoided.

Choosing a hosted VoIP solution that can protect against all of these threats is paramount, and is not something that is guaranteed by all providers. A professional, enterprise-grade solution must provide the security guarantees and protection that businesses need.

VoIPstudio gives you peace of mind by ensuring protection against most human and technical threats, while still offering outstanding value for money. Security is integral to the VoIPstudio vision, meaning that you can rest assured your business communications are secure, protected and that the service is wholly reliable. It not only allows businesses to use their security budget more effectively, but it also makes your life simpler.

Footnotes

1. https://www.cavellgroup.com/cavellvoice/cloud-communications-starting-to-bite-into-traditional-operators-revenues/
2. https://www.accenture.com/t20171006T095146Z__w__/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50
3. https://securityintelligence.com/hello-youve-been-compromised-upward-attack-trend-targeting-voip-protocol-sip/