Featured in this issue:
Safe digital transformation for SMEs

Organisations are eagerly adopting digital transformation. Solutions such as containerisation and other cloud-based models allow greater flexibility while helping firms remain secure. These also address compliance and data sovereignty requirements, the need for greater business continuity in the event of a disaster (natural or otherwise) and improved accessibility to hardware and data. And for smaller firms, the assurance of colocolation and the flexibility of cloud infrastructure strikes a good balance for their IT needs, says Jack Bedell-Pearce of 4D Datacentres.  

Learning lessons from data breaches

Where money is spent, bad actors will follow. Data breaches involving e-commerce have now surpassed breaches at the point of sale and they’re becoming very expensive.

In spite of this, there remains an alarming lack of corporate self-awareness when it comes to cyber security.

Securing VoIP: encrypting today’s digital telephony systems

One persistent cyber security myth is that attacks only ever involve attackers exploiting system vulnerabilities and stealing personal data.

In fact, telecoms systems are equally susceptible to coming under attack. And as telephony is the beating heart of any business, it is essential that all businesses employ secure encryption as a part of their telecoms set-up. And there are three elements to this – awareness, education and action, argues Nick Claxson of Comtec.

China steps up hacking as US issues indictments

Cyber attacks emanating from China have allegedly ramped up in the past few months, while the US has hit back by issuing 10 indictments against Chinese citizens, two of them said to be intelligence agents.

According to the indictments unsealed by the US Department of Justice, intelligence officers Zha Rong and Chai Meng, supported by a team of hackers – Zhang Zhang-Gui, Liu Chunliang, Gao Hong Kun, Zhuang Xiaowei and Ma Zhiqi – carried out a campaign of attacks over five years, mainly targeting aerospace companies. The DOJ claims the accused were working for the Jiangsu Province Ministry of State Security (JSSD), headquartered in Nanjing, and stole information about key technology used in commercial aviation. This information, it’s claimed, was passed to
dent response team and employing end-to-end encryption. For a mega breach of a million customer records, this represents a $27m dollar cost savings per breach. The benefit of employing end-to-end encryption and establishing a response team is quite simple to calculate and can be thought of as the chance of any one organisation being breached in the next 12 months multiplied by the average number of breached records times the cost benefit for one breached record – or 50% x 25,000 x $27/record = $337,500. In this hypothetical scenario, the CSO now has an annual benefit of over $300,000 to justify a security investment.

In summary

The combination of spending money, combined with a ‘it won’t happen to us’ attitude, leads to a surprising lack of action. All three examples previously discussed involved significant gaps in personnel training, but it is the combination of investment in people and robust encryption that yields the greatest return on investment. Although a dual focused strategy of people and technology might seem obvious, it still isn’t to most corporations.

About the author

Steve Roberts is a former close protection and surveillance operative turned security consultant, advising businesses, government, police forces and other large organisations on matters of real-world security. He is also the founder of OSS Technology (http://onlinespyshop.co.uk), a commercial surveillance and counter-surveillance consultancy and retailer helping individuals and businesses negate sometimes sensitive issues. Roberts is a privacy advocate and believes that it’s a collective responsibility for us all to work towards the highest standards of personal, data and corporate privacy possible.

References


Securing VoIP: encrypting today’s digital telephony systems

Nick Claxson, Comtec

Cyber security is a topic on every organisation’s radar. It was only very recently that we heard about the catastrophic Dixons Carphone data breach, which involved 5.9 million card payments and the personal data records of 1.9 million people.1 And who can forget the infamous TalkTalk hack from 2015, in which the personal details of 157,000 customers were compromised?2 As a result of this breach, the company was hit with a record £400,000 fine.

These are just two of many examples of the damage that can be caused through cyber security negligence – both from a financial and a reputational perspective. The statistics surrounding this issue are staggering – cybercrime is set to cost businesses around $6 trillion globally by the year 2021.3 There are many myths and perceptions around the world of cyber security and cyber attacks. One particularly prevalent misconception, however, is that cyber attacks only ever involve attackers exploiting system vulnerabilities and stealing personal data. In fact, the truth is that telecoms systems are equally susceptible to coming under attack. It is therefore essential that all businesses employ secure encryption as a part of their telecoms set-up – it is just as important as anti-virus software and firewalls.
Success through telephony

Telephony is the beating heart of any business. It is an essential component of any effective communications system and is used for a variety of different purposes, whether it’s an informal chat between two colleagues or a confidential discussion between board members. However, much to the surprise of many, it is now just as open to being hacked as the rest of an organisation’s infrastructure.

“Businesses relied on ISDN for their telephony needs – a legacy method that allows voice services to be delivered across digital lines. Over time, this proved itself to be incredibly secure”

However, this has not always been true. Traditionally, businesses relied on ISDN for their telephony needs – a legacy method that allows voice services to be delivered across digital lines. Over time, this proved itself to be incredibly secure, leaving very little room for hackers to successfully exploit it.

Despite its security advantages, ISDN is now seen within the industry as a slow and antiquated technology, and plans are afoot to replace it with more modern alternatives over the coming years. BT, for example, has already announced plans to switch off its ISDN network entirely by 2025, replacing it with a fully IP-based system instead. Eventually, ISDN will be gone for good, which will consequently force engineers to train themselves in newer technologies.

Where IP falls short

The problem with operating via IP, however, is that it is essentially the exact opposite of ISDN. While it is indeed more agile and flexible – a major boon for any business – it also carries increased security risks, particularly when used for VoIP purposes.

The reason for this – or at least part of the reason – is our own comfort and familiarity with IP-based communications on a wider scale. When we send an email message to a colleague at work or chat to a family member living in another country using a VoIP service like Skype, the vast majority of us are only ever thinking about what it is we are saying, listening to, reading or otherwise. We are rarely thinking about how this information is being transmitted to the individual(s) on the other end of the line, and how likely it could be for those communications to be intercepted at any moment.

The inescapable truth is that every communication made over IP – including those that are voice-based – is at its purest form just a data packet. These packets vary drastically: they could be small or large and they could contain information that is either publicly available or highly sensitive and confidential. But there’s one thing that all packets have in common: each one is a potential target for hackers. This is why every single one needs to be protected with the same level of urgency that is usually reserved for wider security-related issues.

“By implementing comprehensive and sophisticated encryption technology, businesses can hide their phone systems from hackers entirely, making it considerably tougher for them to go ahead with their toll fraud plans”

While GDPR is by far the most talked-about regulation to impact data and IT infrastructure security, it is not the only one. Businesses also need to be paying close attention to the Payment Card Industry Data Security Standard (PCI DSS), which was set up to help businesses process card payments securely and reduce card fraud. While technically complex to implement, it is vital that any business processing card transactions is compliant. Similarly to the GDPR, anyone found not to be abiding by the rules can suffer serious consequences, including fines, litigation and reputational damage.

The recent arrival of these new regulations means there is officially no better time for businesses to adopt a self-policing policy that allows them to deal competent ly with any data-related issues before they become a much bigger problem. But quite how businesses actually tackle this problem is another thing entirely.

Peace of mind

Encryption is the ideal solution for businesses looking to strengthen their telephony security and ensure that all future VoIP efforts are secure. It essentially provides an
extra level of defence to your telecoms system that makes it far more difficult for any badly intentioned individuals to access the data packets that are travelling across the IP network. As well as providing peace of mind for businesses themselves, it can also play an important role in achieving and maintaining compliance with the regulations mentioned above.

If the encryption is strong enough, it can also protect businesses against toll fraud, which is an especially dangerous emerging form of cyber attack. In its purest form, toll fraud involves a hacker accessing a telephony system and using it to call premium rate numbers. This leaves the businesses themselves with huge phone bills, and often with no way to resolve the situation other than to pay.

However, by implementing comprehensive and sophisticated encryption technology, businesses can hide their phone systems from hackers entirely, making it considerably tougher for them to go ahead with their toll fraud plans.

**Conclusion**

While, as discussed, there are pros and cons associated with various methods of telephony, the benefits of embracing IP-based telephony over ISDN cannot be denied. IP is quicker, simpler to implement and maintain, and it allows businesses to operate via a unified IT infrastructure.

We cannot escape the security-related issues of IP, but we know that encryption technology can help any business to overcome these issues with relative ease. By embracing encryption, organisations across all sectors can operate with the same level of reassurance that they had become accustomed to in the ISDN days, without wondering when their company name might appear in the headlines with the words ‘cyber attack’ next to it.

There are three words that businesses should keep in mind when adopting encryption technology: awareness, education and action. It’s important to keep our eyes open to cyber security-related risks, educate our staff around what they can do to mitigate these risks and take appropriate action from a top level. These actions will often differ according to business or industry but if all businesses can take these steps, they can effectively avoid being caught out by hackers looking for new avenues of attack.

**About the author**

Nick Claxson is managing director of Comtec and is responsible for overseeing all management decision-making within the organisation. He has headed Comtec since its beginnings as an IT consultancy in the 1990s.

**References**


---

**Business continuity and disaster recovery – advice for best practice**

**Paul Timms, MCSA**

With downtime leading to reputational damage, lost trade and impact on long-term projects, organisations are starting to realise that continuity planning and disaster recovery are critical to success. Business continuity needs to be properly planned, tested and reviewed in order to be successful. For most businesses, planning for disaster recovery will raise more questions than answers to begin with: however by ensuring you do the hard work now you will save a lot of pain in the future.

**Risk appetite**

All businesses are different when it comes to risk. While some may view a ransomware attack as a minor inconvenience and deal with it by running on paper for a week while they rebuild systems, others view any downtime as unacceptable, with IT systems imperative to running their business.

The individual risk appetite of your organisation will have a significant impact on how you plan and prepare for business continuity. You will need to consider your sector, size and attitude towards downtime, versus cost and resources. Assessing this risk appetite will

---

**Business continuity and disaster recovery – advice for best practice**

**Paul Timms, MCSA**

With downtime leading to reputational damage, lost trade and impact on long-term projects, organisations are starting to realise that continuity planning and disaster recovery are critical to success. Business continuity needs to be properly planned, tested and reviewed in order to be successful. For most businesses, planning for disaster recovery will raise more questions than answers to begin with: however by ensuring you do the hard work now you will save a lot of pain in the future.

**Risk appetite**

All businesses are different when it comes to risk. While some may view a ransomware attack as a minor inconvenience and deal with it by running on paper for a week while they rebuild systems, others view any downtime as unacceptable, with IT systems imperative to running their business.

The individual risk appetite of your organisation will have a significant impact on how you plan and prepare for business continuity. You will need to consider your sector, size and attitude towards downtime, versus cost and resources. Assessing this risk appetite will

---

**Business continuity and disaster recovery – advice for best practice**

**Paul Timms, MCSA**

With downtime leading to reputational damage, lost trade and impact on long-term projects, organisations are starting to realise that continuity planning and disaster recovery are critical to success. Business continuity needs to be properly planned, tested and reviewed in order to be successful. For most businesses, planning for disaster recovery will raise more questions than answers to begin with: however by ensuring you do the hard work now you will save a lot of pain in the future.

**Risk appetite**

All businesses are different when it comes to risk. While some may view a ransomware attack as a minor inconvenience and deal with it by running on paper for a week while they rebuild systems, others view any downtime as unacceptable, with IT systems imperative to running their business.

The individual risk appetite of your organisation will have a significant impact on how you plan and prepare for business continuity. You will need to consider your sector, size and attitude towards downtime, versus cost and resources. Assessing this risk appetite will

---

**Business continuity and disaster recovery – advice for best practice**

**Paul Timms, MCSA**

With downtime leading to reputational damage, lost trade and impact on long-term projects, organisations are starting to realise that continuity planning and disaster recovery are critical to success. Business continuity needs to be properly planned, tested and reviewed in order to be successful. For most businesses, planning for disaster recovery will raise more questions than answers to begin with: however by ensuring you do the hard work now you will save a lot of pain in the future.

**Risk appetite**

All businesses are different when it comes to risk. While some may view a ransomware attack as a minor inconvenience and deal with it by running on paper for a week while they rebuild systems, others view any downtime as unacceptable, with IT systems imperative to running their business.

The individual risk appetite of your organisation will have a significant impact on how you plan and prepare for business continuity. You will need to consider your sector, size and attitude towards downtime, versus cost and resources. Assessing this risk appetite will

---

**Business continuity and disaster recovery – advice for best practice**

**Paul Timms, MCSA**

With downtime leading to reputational damage, lost trade and impact on long-term projects, organisations are starting to realise that continuity planning and disaster recovery are critical to success. Business continuity needs to be properly planned, tested and reviewed in order to be successful. For most businesses, planning for disaster recovery will raise more questions than answers to begin with: however by ensuring you do the hard work now you will save a lot of pain in the future.

**Risk appetite**

All businesses are different when it comes to risk. While some may view a ransomware attack as a minor inconvenience and deal with it by running on paper for a week while they rebuild systems, others view any downtime as unacceptable, with IT systems imperative to running their business.

The individual risk appetite of your organisation will have a significant impact on how you plan and prepare for business continuity. You will need to consider your sector, size and attitude towards downtime, versus cost and resources. Assessing this risk appetite will

---

**Business continuity and disaster recovery – advice for best practice**

**Paul Timms, MCSA**

With downtime leading to reputational damage, lost trade and impact on long-term projects, organisations are starting to realise that continuity planning and disaster recovery are critical to success. Business continuity needs to be properly planned, tested and reviewed in order to be successful. For most businesses, planning for disaster recovery will raise more questions than answers to begin with: however by ensuring you do the hard work now you will save a lot of pain in the future.

**Risk appetite**

All businesses are different when it comes to risk. While some may view a ransomware attack as a minor inconvenience and deal with it by running on paper for a week while they rebuild systems, others view any downtime as unacceptable, with IT systems imperative to running their business.

The individual risk appetite of your organisation will have a significant impact on how you plan and prepare for business continuity. You will need to consider your sector, size and attitude towards downtime, versus cost and resources. Assessing this risk appetite will

---

**Business continuity and disaster recovery – advice for best practice**

**Paul Timms, MCSA**

With downtime leading to reputational damage, lost trade and impact on long-term projects, organisations are starting to realise that continuity planning and disaster recovery are critical to success. Business continuity needs to be properly planned, tested and reviewed in order to be successful. For most businesses, planning for disaster recovery will raise more questions than answers to begin with: however by ensuring you do the hard work now you will save a lot of pain in the future.

**Risk appetite**

All businesses are different when it comes to risk. While some may view a ransomware attack as a minor inconvenience and deal with it by running on paper for a week while they rebuild systems, others view any downtime as unacceptable, with IT systems imperative to running their business.

The individual risk appetite of your organisation will have a significant impact on how you plan and prepare for business continuity. You will need to consider your sector, size and attitude towards downtime, versus cost and resources. Assessing this risk appetite will