BT Global Services

September
2010

Beyond. Security

How the cloud will (and won't) impact your organisation's security

Beyond. The cloud

1 Executive Summary

* This white paper is based on "IT Security: six things you need to know in 2010", first published by BT Global Services in February 2010

Everyone, it seems, is talking about the cloud. This white paper is one of a series that aims to move beyond the hype that currently surrounds the cloud.

This paper looks at security. It asks what are the most important security issues today? And how, if at all, will these be impacted by the cloud?

It looks at what a CEO should be asking his CIO about security to ensure his enterprise adopts cloud services appropriately and securely. While not all business processes and services will be ideal for migration to the cloud, and not all organisations will place the same value on the benefits the cloud delivers, the goal of improving organisational performance should not be limited by an irrational fear of the cloud.

Recent research from BT Global Services found that CEOs and CIOs are almost equally concerned about security in the cloud. For that reason, this paper offers practical guidance on the headline security issues and should be a vital desk companion to CEOs and CIOs looking to foster better understanding of how data and network security affects their organisation.

2 Introduction

Information security is one of the most critical issues facing any organisation today, be they a financial institution holding customers' banking details or a government body holding electoral, health, criminal, employment or immigration data. Too often an inability to translate the issue from a technical to a business one gets in the way. Vital facts are lost, as it were, in translation.

Add the cloud into the equation and this problem escalates, as hype trumps reality. Actually knowing the security issues inherent in cloud services, in order to overcome them, can be a challenge.

We offer a straightforward guide to the problem and the solutions available. BT Global Services has decades of experience helping major international organisations protect themselves and their customers from the ever-present threat of information loss or attack.

This paper is aimed at spreading just some of that experience around.

It looks at the following areas:

- Cybercrime
- Social media in the workplace
- Security in the cloud
- Enterprise cloud considerations

We hope it is useful and that you get in touch if you have any questions at all.

"We offer a straightforward guide to the problem and the solutions available."

3 Cyber crime

What's the problem?

Globalisation is leading to a new 'cyber cold war' between hackers and security professionals. It is a very modern battlefield, one that itself exists "in the cloud", with skirmishes being fought daily over data carried via the internet and networks.

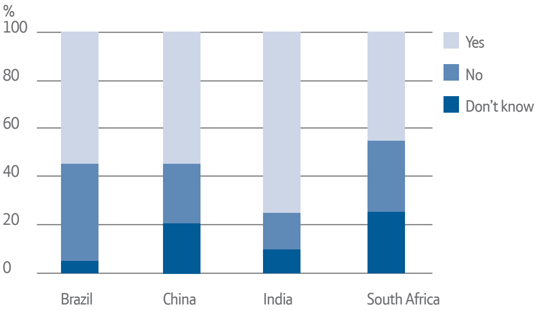
The war is escalating partly because globalisation has led to a single global network, and a patchwork of criminal justice regimes, some more susceptible than others to cyber-criminals and gangs.

The result is a very modern transmutation of the age-old phenomenon of "industrial espionage", which has been around since the dawn of commerce. Spying on, stealing or sabotaging the data of another organisation – be it a commercial enterprise or a national government – gives you anything from competitive advantage to economic and military superiority.

And there is a worrying acceptance of the problem. More than half of executives in developing regions themselves admit that the threat of international cyber-espionage, hacking or web fraud is more likely to come from a source located in a developing economy such as (but not limited to) Russia, India, Brazil or China.[1]

"Is cyber crime a real danger for this organisation?" CEO

Do you believe that the threat of international cyber-espionage (hacking, web fraud etc.) is more likely to come from a source located in a developing economy such as (but not limited to) Russia, India, Brazil or China?



Can we protect ourselves?

Questions are being asked in boardrooms: "can we truly protect ourselves against the next generation of hacking? Or is damage-limitation the best we can hope for?" Providing reassurance is a tricky thing, because companies involved in providing security solutions need to be transparent and responsible with their claims. So let us be very clear, here, from the outset: there is no easy panacea to this problem. There is no single product or service that can be plugged in and means your data is safe. It means companies need to sit up and take this problem seriously at a senior level and not relegate it to a nuts-and-bolts IT services issue.

[1] Datamonitor research commissioned by BT: Threatening Skies: Risk in the Global Economy, 2008

3

Yes, but don't expect technology to solve the problem on its own

Firstly, it is vital to recognise how the very nature of globalisation has altered the challenge. Once upon a time, a virus detection programme could easily check IP addresses linked to a PC or server, spot any beginning 85.xxx, recognise that this was going to China, for example, and block the address. Today, of course, most international companies will be sending and receiving legitimate data packets to and from China daily – suppliers' details, product data, order information. So modern software has to learn what activity is legitimate and what is not before it begins to run effectively. This is hugely powerful, but the understanding of the process is not always there. Too many organisations, erroneously, think they have this activity covered as soon as they've installed the new kit. Just because suspicious activity has not been detected does not mean that it's not going on.

The very language we use is also a problem. The term, "cyber-crime", leads us to forget that the data still starts and ends with a physical machine, and so the physical threat is frequently overlooked. You can have the best technology in the world, but it won't help if your office cleaners are easily able to smuggle information out of your building on a data stick.

Ultimately, what is needed is a combination of good corporate policy, married to effective technology. Far too often, we see one without the other and, in 2010, this is not good enough.

Practical advice

1. Check physical security. Ensure that your technology, facilities management and human resources departments, at the very least, are talking to each other. Any external suppliers with access to your building should be properly vetted.
2. Ensure you have the appropriate technology in place and that it is set up correctly: software-based anomaly detection, located in the network, coupled with solid firewalls at your data centre end.
3. Link this up with effective policy adherence – rigorous testing, monitoring, recording – such as is demanded by ISO 27001 (BS7799) the Information Security Management System ('ISMS')
4. Ensure that policy is in place for follow-through: detecting and countering an attack is one thing. You need to be able to trace it and build up the chain of evidence so that, should you ever need to take someone to court, there is a proper chain of evidence. This means your IT people need to be trained to log dates and times properly, and your legal department will need to be involved to ensure your policies adhere to privacy laws.

"It's a growing threat, and one we must confront" CIO

4

Social media in the workplace

What's the problem?

Social networking has been one of the most talked-about security topics of the past two or three years as cloud-based and often mobile services have allowed workers to circumvent security procedures and firewalls. As soon as it became apparent that people were using their work as well as their personal internet connections to log on to external sites to share information – and, potentially, data – organisations began voicing their concerns. The worry was, and still is, that sites such as Facebook and Twitter might at best reduce people's productivity and at worst pose a threat to information integrity.

The threat to information integrity is certainly not limited to third party social networks. Any cloud-based service or process makes it inherently easy to move proprietary information off the premises. In fact, in most cases, the bulk of the retrieval, manipulation and storage takes place outside the firewall. Yet, as many hackers will tell you, this is more of a psychological issue than anything else. From the outside, firewalls look the same, whether they are run by an enterprise IT team or a cloud service provider. And the cloud provider will tell you, for them this is a core operational issue, from the CEO down.

Of particular concern has been the theory that the incoming generation of employees, reared on the internet and potentially blasé about security, will pose a major challenge for management.

So, is there a risk?

This stems from a fear of the unknown. The generation currently entering the workforce uses a different vocabulary, follows a different culture, has different demands, demonstrates a high speed of learning and has different expectations. They push the boundaries of older management.

But is this a threat? The pace of change in terms of new media and social networking tools will frequently continue to outstrip our ability to check for technical security threats and counter them. The convergence of external and internal applications will proceed at pace and, certainly, the risk of data leakage is a very real one as people (of all generations, but particularly younger employees) increasingly blur the boundaries between their public/private and personal/professional lives.

That said, the longer organisations spend debating the threats, the higher the danger that they will fall behind the curve when it comes to exploiting opportunities

> **"Any cloud-based service or process makes it inherently easy to move proprietary information off the premises.**

4

Maybe, but the benefits outweigh the dangers

The social web is a driver of change. There are challenges – and solutions – for enabling cloud-based collaboration via social networking tools, using them safely in the workplace while demonstrating business value and creating an environment for young talent to grow and want to stay with your organisation.

At their heart, social networking sites are about collaboration and sharing ideas. Both of these things are the very lifeblood of innovation and organisations must find a way of embracing rather than banning them. And by placing their use within the bounds of corporate guidance and policy, people may become better users of these technologies, reducing the risk of information leaks via mistakes.

> **“Properly managed, these new ways of communicating present an opportunity”**
>
> CIO

Practical advice

1 Make the tools available. You can’t – or at least will find it increasingly difficult and counter-productive to – stop people using tools that they have grown up with, that are so ingrained into their way of life.

2 Divorce management issues from the equation. For example, worrying about whether employees will ‘waste time’ chatting on Facebook is only a modern incarnation of worrying if they’ll ‘waste time’ chatting at the water cooler. Motivating people and optimising productivity is a management issue, not a security one.

3 It is possible to make any web-based tool secure, with the right technology, the right training and the right level of awareness among the workforce. And so, again, education is key:

- Make your security policy on social networking usage relevant to your Generation Y employees. Listen to them, engage, and participate.
- Never say no! They will just go round you.
- Embrace the younger generation’s needs – it will accelerate innovation.
- As with any other application, layer up the technology to ensure that data is encrypted and secure, and that access controls to sensitive information are appropriate to the user.

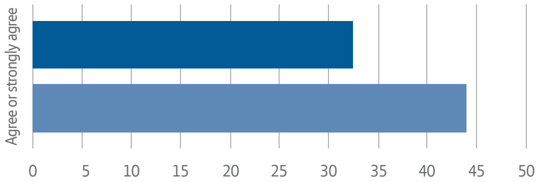
5 Security in the cloud

The delivery of services via the cloud has been one of the most talked-about subjects in IT circles, but it has now made it onto the boardroom agenda. Getting beyond the hype is particularly important, as business decisions may depend on a true grasp of the security issues associated with the cloud.

CIOs are responding to the growing awareness of the importance of the cloud. According to the Gartner Executive Programmes' 2010 CIO survey[2], the top three technology priorities cited by CIOs are virtualisation, cloud computing and web 2.0, while the top business priorities are business process improvement and reducing enterprise costs. In the current climate, the ability to deliver better IT services for less chimes with business leaders' own objectives. The idea of upgrading technology without significant capital expenditure is finding fans both among CIOs, but also CEOs and CFOs.

BT Global Services' recent Enterprise Intelligence research reveals an interesting disconnect between CIOs and CEOs, with nearly half CIOs (44%) saying they believe they deal with information that is too sensitive for the cloud, but only a third of senior executives saying the same. The implication is that it could be CEOs urging a move to the cloud in 2010, with CIOs offering a note of caution.

CIO caution: "Our information is too sensitive for the cloud"



Do cloud benefits outweigh risks?

Many of the risks associated with cloud services are grounded in who controls what. The ability, or lack thereof, to transfer control and risk relating to data to third parties is critical. Recent research by the EU Network and Information Security Agency (ENISA), to which a crack team of BT's security experts contributed, reveals that the biggest security concerns associated with the cloud are corporate data confidentiality, privacy and the integrity of services and/or data. These three issues are major 'deal-breakers', and if they cannot be addressed completely, enterprises will find it difficult to move to cloud architecture.

On the other hand, the benefits of moving to cloud architecture are potentially huge: significantly reduced capital expenditure and fixed costs; increased agility thanks to the rapid provisioning and de-provisioning of resource; faster return on investment thanks to pay-as-you-use commercial models; the availability of services to a mobile workforce; unlocking business opportunities by removing previous barriers to entry; theoretically more robust business continuity (see the next section for a more detailed discussion of business continuity in the cloud).

Cloud security requires strict policies and planning

Cloud services are extraordinarily diverse, and there can be no one-size-fits-all approach to security. Just look at the software-as-a-service offered by major names like Microsoft, Google and Salesforce.com, and compare them to infrastructure-as-a-service from Amazon, IBM or BT. These are very different propositions and require different security policies and controls.

[2] Inc. Press Release, "Gartner EXP Worldwide Survey of Nearly 1,600 CIOs Shows IT Budgets in 2010 to be at 2005 Levels", 19 January 2010

5

The solutions that are most likely to provide enterprise-level stability, security and usability will comprise federations of best-in-class solutions provided via a mixture of in-house 'private' clouds and third-party 'public' clouds. Such a 'hybrid' approach has the potential actually improve security, because cloud providers often invest significantly more in security expertise and processes. It's just important to know what, specifically, they offer. The best advice is to lock horns commercially with multiple cloud service providers and ensure your security policy and requirements are built into their offerings.

Practical advice

1. Research the market. All the providers of cloud services, whether delivering software, infrastructure or platform solutions offer different services with different service level agreements and security features. Selection of the right services is an essential first step.

2. Federated solutions may be more bespoke and robust. Using a selection of different services – including a self-managed private cloud – to build a bespoke solution can ensure cloud services are more aligned with your business needs. Increasingly, federation will become an essential part of building bespoke cloud services, meeting security and risk demands, adding transparency and increasingly providing secure collaboration between trusted parties.

3. Prepare for cloud culture. The automated interface of many cloud services can feel alien to IT departments used to dealing with people within supplier organisations. Procurement, legal or commercial teams can also find the pay-as-you-go contracting model of cloud services demanding. Take these teams with you if you opt to strategically source services from the public cloud, otherwise they may become strategic barriers.

4. Regularly seek independent audits of cloud operators' offerings, to ensure they are still the best in class and best fit for your needs

Legislation Covering Data

Data protection legislation often prevents the transfer of risk from one corporate entity to another. For example, both Sarbanes-Oxley and the UK's Data Protection Act require the company looking after data to remain entirely responsible for it. Legislation also presents jurisdictional challenges. For example, cloud providers are typically forced to locate data within a specific territory, usually the client's own country, which hinders the benefits and flexibility of their service offerings. Under such stringent conditions, the data-owning party would need so much control over how the data is stored and used, that the benefits of cloud storage of data or computing resource could be lost.

> **"The cloud can be safe, secure… and financially attractive"**
>
> CIO

6 Enterprise cloud use

Availability – at the heart of security

A sophisticated service that delivers significant value to its users remains worthless if it is not consistently available. When considering the security of cloud services, availability is one of the biggest single issues. There are multiple challenges here: how does cloud architecture impact availability levels during periods of normal service; how much can the cloud help or hinder availability when an organisation needs to rapidly scale up or down key services; and what impact does the cloud have on an organisation's business continuity strategy?

The bottom line for most organisations today is that non-availability of services costs money through impacted productivity and sales, lost customers and damaged reputation. The strategic challenge for cloud providers is how to transfer the risk of downtime from enterprises seeking to adopt cloud architecture. We have already shown that some risks cannot be transferred, for legislative reasons (see the previous section). But it is, theoretically at least, possible to offset some of the concerns of enterprises by committing to strict service level agreements.

How can we maintain service levels in the cloud?

This is where federators of cloud services can add value, not only by bolting together services to create bespoke solutions, but providing security wraps and service level guarantees that potentially exceed those of the third party cloud provider alone. The lessons learned in the design and deployment of high availability infrastructures is critically important for cloud providers, and there is evidence that some are not yet applying sound engineering design. Those with an infrastructure heritage are leading the way here.

While elasticity of service is one of the core features of cloud architecture, and scaling up and down does not affect availability, business continuity – in particular, disaster recovery – offers its own challenges in the cloud.

Under a traditional business continuity model, all data stored on dedicated – and probably self-managed – servers is routinely duplicated and stored on a mirror server at a distinct location, in case of a disaster. Under cloud architecture, however, the location of servers is not necessarily a fundamental aspect of service provision, which makes ensuring data is copied to a remote location a challenge. This is mitigated by the fact that, increasingly – mainly for reasons of data protection legislation – cloud providers' customers stipulate in which region or territory servers, and therefore data will be physically located.

> **"Can we guarantee our customers world-class service in the cloud?"**
>
> CEO

7 The BT offer

As the authority on enterprise security, BT's Managed Security Solutions assure customers' business continuity, improved compliance, and protection from financial loss. Leveraging our experienced professionals and state-of-the-art security solutions, BT delivers comprehensive protection and real economies of scale and efficiencies of cost.

BT's Managed Security Solutions Group's portfolio of managed security solutions provides customers with the industry's most complete, single-source enterprise security solution. Our rich heritage in Managed Security has earned us the trust of customers. Our foundation in real-time internal network and host-level protection is augmented by managed internal and external network protection services, including:

Managed Security Monitoring, powered by BT Counterpane

BT's managed security monitoring service combines a team of disciplined security experts, a rigorous process for incident detection and response, and best-of-breed technologies to provide information-driven organisations with immediate feedback regarding the efficacy of their network's security – in real-time. Our security monitoring is the business solution that empowers enterprises to reduce liability, improve information safety, and facilitate audits.

Device Management, powered by BT Counterpane

Device management focuses on proactively implementing configurations in the best interests of the customer so that devices are always providing maximum protection and surveillance. That's why BT's MSSG SLA offers unlimited changes to devices when they are initiated by BT. This includes new signatures and updates from the vendor and configuration changes BT MSSG recommends based on observations from hundreds of networks and thousands of devices around the world.

Managed Vulnerability Scanning, powered by BT Counterpane

BT MSSG offers two levels of Managed Vulnerability Scanning service to meet customer needs. BT partners with Qualys for service delivery.

- The Full Service option is for companies interested in leveraging BT's expertise and experience to manage their scans and tightly integrate it with BT's infrastructure. BT's scans can be scheduled to suit your needs on a weekly, monthly, or unlimited basis.
- The Self Service option is for companies preferring to self-administer their scans and wish to take advantage of additional features of the service, including asset classification and remediation management.

Both service options provide flexibility in scheduling scans and defining internal and external targets including address-specific or address-range coverage options, and conditional start-stop time boundaries. All scan reports are correlated across data from vendors as well as data from BT MSSG's proprietary correlation engine. Executive summaries and detailed scan reports are available 24x7 via the BT MSSG Portal.

Managed Log Retention, powered by BT Counterpane

Managed Log Retention frees customers from the log and security management burden while enabling them to achieve federal and industry compliance, reduce total cost of ownership, and benefit from best practice guidance on risk management with swift responses to security incidents, compliance inquiries, and internal threats.

> "Our security monitoring is the business solution that empowers enterprises to reduce liability, improve information safety, and facilitate audits."

7

Ethical Hacking

BT's Ethical Hacking services enable customers to protect their networks, information assets, and corporate reputations by identifying vulnerabilities before they can be exploited. Our security experts will identify vulnerabilities, provide recommendations to remediate identified issues, and help improve their security posture. BT proprietary testing methodologies and techniques yield high quality results that will help customers optimize their security infrastructure.

- Application Testing: Reviews the logic structure, code, methods of access and authentication mechanisms of your web-based applications
- Network Testing: Provides external and internal vulnerability and penetration assessments, VPN vulnerability and penetration tests and an analysis of VoIP within your environment
- Wireless Security: Identifies weaknesses and vulnerabilities specific to your wireless infrastructure
- System Hardening: Tests for over 1,000 network-level vulnerabilities within your current network configuration
- War Dialing: Identifies unauthorized modems that provide access to your network and then attempts to exploit your network through illicit devices

For more information on BT Managed Security Services and how they can make your organisation and your customers more secure and risk-resilient, please visit bt.com/globalservices or contact Ray Stanton (ray.stanton@bt.com)

The 'Beyond the Cloud' series of white papers examines in depth specific aspects of running an organisation, and show that, beyond the hype, cloud services have an important role to play. They should be seen as part of the solution to corporate challenges such as boosting productivity and efficiency, and meeting demands such as delivering better customer service and security.

The other papers in the series are:

- How the cloud will (and won't) make your customers happier
- How the cloud will (and won't) make your operations more efficient
- How the cloud will (and won't) make your people more productive

"The 'Beyond the Cloud' series of white papers should be seen as part of the solution to corporate challenges such as boosting productivity and efficiency, and meeting demands such as delivering better customer service and security."

Beyond.
The cloud

Offices worldwide

The services described in this publication are subject to availability and may be modified from time to time. Services and equipment are provided subject to British Telecommunications plc's respective standard conditions of contract. Nothing in this publication forms any part of any contract.

Registered office: 81 Newgate Street, London. EC1A 7AJ
Registered in England No. 1800000.