bsi.

...making excellence a habit.™

ISO/IEC 27018

Safeguarding Personal Information in the Cloud

Whitepaper

Summary

The protection of private information has never been a higher priority. Many national and international bodies, including the International Organization for Standardization (ISO), the US government and the European Union, are all taking steps to address this issue. One initiative they share in common is ISO/IEC 27018 and the additional controls that extend ISO/IEC 27001 to secure information held by Cloud Service Providers (CSPs). What specifically does ISO/IEC 27018 offer customers of cloud services, and why is it important?

The scale of data breaches

2,803,036
– every day

1,947
– every minute

116,793
– every hour

32
– every second

Potential exposure of personal data is at the top of the international agenda. The overwhelming number of high profile security breaches has focused people's attention on how their individual details need to be protected. If you look at the list of breaches and the number of people affected, you can see the scale of the problem: the US Office of Personnel Management data on over 21m government employees was stolen and the attack on the Carphone Warehouse in the UK affected more than 2m of their customers were affected. These represent just the tip of the iceberg of attacks over a three-month period in 2015. In fact, McAfee have estimated 800 million data records were lost in 2013[1].

Yet companies are spending even more on security. According to figures from Gartner, global IT security spending is set to reach $76.9 billion in 2015[2].

While the image of the socially misfit hacker resonates with many people; most attacks from outsiders are carried out by sophisticated criminal gangs or state-sponsored organizations, making it particularly difficult to take action against them. There's an more insidious risk, that of the insider who, deliberately or unintentionally, leaves a company open to attack. These are often more dangerous as they often go unreported or are covered up. According to research from PricewaterhouseCooper[3], 75% of organizations who suffer from security compromises committed by employees do not involve law enforcement nor bring any legal charges. This means that those organizations' customers are vulnerable, and any companies who hire those individuals in the future would be unaware of their past and may be open to further attacks.

It's little wonder that there's so much anxiety about how personal data is protected and, in particular, why there is so much fear about the cloud as well as why there's still a reticence to entrust data to CSPs.

It's for these reasons that the European Union, for example is looking at new regulations on Data Protection in an attempt to harmonize the legal situation across the continent. When it comes to Europe, there are a variety of local data protections laws, making it especially difficult for cloud providers to operate. The cloud crosses international borders, while the laws governing data security are primarily country specific.

[1] http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf [2] http://www.gartner.com/newsroom/id/2828722
[3] http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

Part of the issue also has been the way that organizations hold data – there's a legal separation when it comes to cloud providers. They hold data on behalf of their customers, yet the customer has the legal responsibility for what happens to that data.

This is where the fears about CSPs are really centred: all are happy to talk about their security expertise, the amount they spend on data protection and the physical barriers they put in place to prevent breaches, but there's an underlying anxiety as to whether the CSPs are going to treat confidential data in the same way as their customers would.

While the European Union is trying to introduce some coherence into the data protection arena, the US has to contend with a different situation.

In the States, there's no national law regulating how personal data is used. The different polices of the individual states can also cause a degree of confusion. This is exacerbated by various regulatory demands placed by different industries. All these factors combine to make formulating a coherent data policy rather difficult. In August 2015, in an effort to address this, the National Institute of Standards Technology advised Federal agencies to "use relevant international standards for cybersecurity, where effective and appropriate, in their mission and policymaking activities."[4] As agencies for the US government implement these standards, they will begin to demand their contractors and supply chains to also conform to the requirements of various standards.

ISO/IEC 27000

From an international perspective, ISO has developed a family of standards for information security which provides a framework for companies to develop processes and procedures to address information security concerns throughout an organization.

The leading standard in this group is ISO/IEC 27001, which is the most widely-recognized standard for protecting sensitive information from unintentional distribution and unauthorized access. With its 114 controls, ISO/IEC 27001 can mitigate risks involved with the collection, storage and dissemination of information by:

- Allowing organizations to comply with increased government regulation and tough industry specific requirements
- Providing the requirements for an effective information security management system
- Letting organizations grow knowing that all their confidential information will stay confidential

[4] http://csrc.nist.gov/publications/drafts/nistir-8074/nistir_8074_vol1_draft_report.pdf

The **ISO/IEC 27018** standard

ISO/IEC 27001 only goes so far. To allay the additional fears created by the cloud, ISO launched a new standard, ISO/IEC 27018, in the autumn of 2014. CSPs will want to adopt this standard to help reassure their customers about the security of their data. The new standard, which is an extension of ISO/IEC 27001 and ISO/IEC 27002 standards, provides guidance to organizations concerned about how their cloud providers are handing personally identifiable information (PII).

It's a bit of legal minefield for organizations and one of the reasons that the EU discussions have been so drawn out, however some legal definitions needed to be established first. Key among them is PII itself; this is the definition on which all discussions hang. PII has been defined as any information that (a) can be used to identify the PII principal to whom such information relates, or (b) might be directly or indirectly linked to a PII principal.

That, of course, raises another question, what is meant by a PII principal? This is a little trickier as some countries refer to this entity as the data subject. Likewise, there's some vagueness about the term PII controller, sometimes called a data controller, but the central point is that the PII controller is the person who determines the purposes for which that data is processed.

What does **ISO/IEC 27018** contain?

There are several guidelines within the standard. According to the ISO definition, these are:

- To help the public cloud service provider comply with applicable obligations when acting as a PII processor, whether such obligations fall on the PII processor directly or through contract
- To enable the public cloud PII processor to be transparent in relevant matters so that cloud service customers can select well-governed, cloud-based PII processing services
- To assist the cloud service customer and the public cloud PII processor in entering into a contractual agreement
- To provide cloud service customers with a mechanism for exercising audit and compliance rights and responsibilities in cases where individual cloud service customer audits of data hosted in a multi-party, virtualized server (cloud) environment might be impractical technically and might increase risks to those physical and logical network security controls in place

While these are the bare principles, if we look at the ramifications of what these mean and how they can help customers, then we can see that, for the first time, there's a real framework for handling personal data.

What ISO/IEC 27018 does is ensure that a cloud provider documents how personal data is handled, what procedures it has in place and how it reacts to customer requests. It can also assist in drawing up stronger contractual agreements.

It can help benefit the cloud provider too. The standard will help set out how CSPs can train staff about PII, set a documentation procedure in place and provide guidelines to follow. And ISO/IEC 27018 will also provide real transparency so personal data, and how it's handled, are not just afterthoughts.

There are three areas an organization needs to question when implementing the standard.

- Are there existing legal and statutory requirements that an organization must follow, including any industry-specific rules and regulations
- Does adherence of ISO/IEC 27018 entails additional risks to the organization, and
- Will the adoption of such a standard run counter to an organization's corporate policies and business culture?

Conclusion

There is little doubt that the cloud industry is in need of standardization to provide adequate and effective information security. According to a survey from TrustE, carried out at the end of 2014, 92% of British online users were worried about their privacy; that's an increase from 89% in 2013[5]. The biggest concern remains the possibility of companies collecting and sharing personal information. Increasingly, consumers are demanding companies become more transparent about the collection, use and protection of their online data.

The arrival of ISO/IEC 27018 helps to concentrate the industry's focus on providing increased security to protect PII. The standard is already being supported by some major cloud vendors: Microsoft has incorporated it into Azure , Office 365, Dynamics CRM and Global Foundation Services and both Amazon Web Services and Dropbox have also achieved certification to ISO/IEC 27018. Many more CSPs are expected to follow. Organizations will increasingly move information to the cloud to benefit from the greater flexibility of technology as well as the decreased demand on resources, but there will only be a high level of adoption when security, specifically privacy concerns, are answered.

The impending European regulation will ensure that a new approach to privacy will be the order of the day.

ISO/IEC 27018 will help to provide a set of guidelines for customers and cloud providers alike.

It won't be a substitute for national and international regulations, and its wide-scale adoption won't mean that providers would automatically follow legal demands, but it will be an important step along the way.

[5] https://www.truste.com/about-truste/press-room/british-customers-online-privacy-more-important/

Why BSI?

BSI has been at the forefront of information security standards since 1995, having produced the world's first standard standard, BS 7799, now ISO/IEC 27001, the world's most popular information security standard. And we haven't stopped there addressing the new emerging issues such as cyber and cloud security. That's why we're best placed to help you.

At BSI, we create excellence by driving the success of our clients through standards. We enable others to perform better, manage risk and achieve sustainable growth.

For over a century, our experts have been challenging mediocrity and complacency to help embed excellence into the way people and products work.
We make excellence a habit

Our products and services

We provide a unique combination of complementary products and services, managed through our three business streams; Knowledge, Assurance and Compliance.

Knowledge

BSI works with business experts, government bodies, trade associations and consumer groups to capture best practice and structure the knowledge all organizations need to succeed. The majority of the widely used and implemented international standards were originally shaped by BSI, for example ISO 14001, Environmental Management and ISO 9001 for Quality Management.

Assurance

Independent assessment of the conformity of a process or product to a particular standard ensures that our clients perform to a high level of excellence. We help our clients understand how they are performing, thereby identifying areas of improvement from within

Compliance

To experience real, long-term benefits, our clients need to ensure ongoing compliance to a standard so that it becomes an embedded habit. We train our clients to understand standards and how to implement them, as well as provide added value and differentiated management tools to facilitate the process of ongoing compliance.

To find out more visit: **bsigroup.com**

bsi.

bsigroup.com

BSI/UK/751/SC/1015/EN/BLD