bsi.

...making excellence a habit.™

ISO/IEC 27018

Safeguarding Personal Information in the Cloud

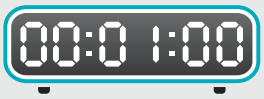
Whitepaper

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 the international standard ISO/IEC 27018.

The scale of data breaches[1]

3,046,456
– every day



2,116
– every minute

126,936
– every hour

35
– every second

ISO/IEC 27018 is a code of practice for protecting personally identifiable information in public cloud services. It's structured as an extension to the widely used and respected ISO/IEC 27002 code of practice for information security controls. So what specifically does ISO/IEC 27018 offer customers of cloud services and why is it important?

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 had data on over 21m government employees stolen and the attack on Carphone Warehouse in the UK affected more than 2m of their customers. These represent just the tip of the iceberg of attacks over a three-month period in 2015. In fact, according to Breach Level Index $707.5 million data records were breached in 2015[1].

Yet companies are spending even more on security. According to figures from IDC, global IT security spending is set to reach $101.6 billion by 2020[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 a more insidious risk, that of the insider who, deliberately or unintentionally, leaves a company open to attack.

Internal threats are often more dangerous as they often go unreported or are covered up. According to research from PricewaterhouseCoopers[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, opening themselves up for attack.

With identify theft accounting for 64% of data breaches in the first half of 2016[1], 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 use of cloud computing and entrusting data to Cloud Service Providers (CSPs).

It's for these reasons that the European Union, for example has implemented new regulations on Data Protection (the General Data Protection Regulation or GDPR) in an attempt to harmonize the legal situation across the continent. When it comes to Europe, there are a variety of country-specific

[1] http://breachlevelindex.com
[2] http://www.computing.co.uk/ctg/news/2474455/global-it-security-spending-to-top-usd100bn-by-2020
[3] http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf

data protection laws, making it especially difficult for cloud service providers to operate. Cloud computing crosses international borders, while the laws governing data security are primarily country specific.

Part of the issue has also been the way that organizations hold data – there's a legal separation when it comes to cloud service 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 CSPs 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 personal and confidential data in the same way their customers would.

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

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

ISO/IEC 27000

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

The leading standard in this group is ISO/IEC 27001, which is the most widely-recognized standard for protecting sensitive information against unintentional distribution and unauthorized access. With its 114 controls, ISO/IEC 27001 and the closely related ISO/IEC 27002 can mitigate the risks involved with the collection, storage and dissemination of information by:

- Providing the requirements for an effective information security management system
- Allowing organizations to comply with increased government regulation and tough industry-specific requirements
- 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 deal with the additional concerns associated with the processing of personal data using cloud computing, ISO created a new standard, ISO/IEC 27018, in the autumn of 2014. CSPs are adopting this standard to help reassure their customers about the security of their data. An extension of ISO/IEC 27001 and ISO/IEC 27002, ISO/IEC 27018 provides guidance to organizations concerned about how their cloud providers are handing personally identifiable information (PII).

It's a bit of a legal minefield for organizations and one of the reasons that the EU GDPR took so long to agree, however some 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 or organization who determines the purposes for which the personal data is collected and processed.

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

There are several objectives within the standard. According to the ISO text, 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 in public cloud services.

ISO/IEC 27018 takes the extensive set of security controls described in ISO/IEC 27002 as a base and then extends them in two ways. First, existing security controls are extended in a number of areas to deal with dividing responsibilities between the cloud service customer and the cloud service provider. Second, a new set of security controls are added, to reflect the privacy principles defined in the ISO/IEC 29100 privacy framework standard.

Examples of extended security controls include:

- Requirements for the encryption of PII - in motion, when stored and also on any removable physical media
- The deletion of PII within a specified period once the data is no longer required
- That PII is processed only for the purposes expressly stated in the cloud service agreement
- To cooperate in dealing with the rights of PII principals in inspecting and correcting their PII, something that is mandated by many regulations

ISO/IEC 27018 ensures that a cloud service provider has appropriate procedures in place for handling PII. It can also assist in drawing up stronger cloud service agreements. The standard sets out how CSPs can train staff about PII, what documentation procedures are required and provides guidelines to follow.

ISO/IEC 27018 aims to provide real transparency for the cloud service customer so that the customer has a clear understanding of what the cloud service provider is doing with respect to the security and protection of personal data.

There are three areas where an organization needs to pay particular attention 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 entail additional risks to the organization
- Will the adoption of the standard require changes to the 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 2015 survey from TrustE, 92% of British online users were worried about their privacy[6]. The biggest concern is users not knowing how the personal information collected about them online is used and the possibility of companies sharing personal information. Increasingly, consumers are demanding companies become more transparent about the collection, use and protection of their online data.

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 providers: Microsoft Azure, IBM Softlayer, Google Apps for Work, Amazon Web Services and Dropbox have all achieved certification to ISO/IEC 27018. Many more CSPs are expected to follow. Organizations will increasingly move information and processing to cloud services 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 addressed.

The European GDPR ensures that a new approach to privacy will be the order of the day.

ISO/IEC 27018 helps to provide a set of guidelines for achieving appropriate protection of PII for customers and cloud service providers alike.

ISO/IEC 27018 isn't a substitute for national and international regulations, and its wide-scale adoption won't mean that providers would automatically follow legal demands, but it is an important step along the way.

[6] 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 help organizations to embed resilience, helping them to grow sustainably, adapt to change, and prosper for the long term. We make excellence a habit.

For over a century our experts have been challenging mediocrity and complacency to help embed excellence into the way people and products work. With 80,000 clients in 182 countries, BSI is an organization whose standards inspire excellence across the globe.

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

The core of our business centres on the knowledge that we create and impart to our clients. In the standards arena we continue to build our reputation as an expert body, bringing together experts from industry to shape standards at local, regional and international levels. In fact, BSI originally created eight of the world's top ten management system standards.

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 train our clients in world-class implementation and auditing techniques to ensure they maximize the benefits of our standards.

Compliance

To experience real, long-term benefits, our clients need to ensure ongoing compliance to a regulation, market need or standard so that it becomes an embedded habit. We provide a range of services and differentiated management tools which help facilitate this process.

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

bsi.

bsigroup.com