Praxonomy Blog
EMPOWERING BOARDS

Data Security — A Note On Standards And Certifications

Written by Steve Schecter on August 28, 2019

INTRODUCTION

What is the value of data to your business?

Whether it's a close look at the steps your company follows to create products, details of confidential discussions between senior management and clients, or board-level plans for the company's future, how much damage would result from a leak, theft or other loss of key company data?

And in light of the potentially serious consequences, how far would you go to protect that data?

The growth of Software as a Service (SaaS) makes the question more complex. SaaS providers like Microsoft, Oracle, Salesforce, Google, Sage, Praxonomy and many other companies routinely handle business-critical data. This means that your software vendors now manage much of your data, not you. How can you be certain that your data stays secure and what should you ask your SaaS vendors about data privacy and security?

There are too many topics to include in a single post but one essential question to ask any vendor is: **"What certifications do you have and can I see them?"**

There are a number of industry-standard, globally recognized certifications that provide assurances that vendors follow best practice or at least "commercially reasonable" good practice guidelines for security and quality management. Any good SaaS vendor should be willing to disclose its certifications to a prospective client.

But which certifications should you look for? And what do the different certifications mean? A look at two of the major security certifications follows.

ISO/IEC 27001

The gold standard when it comes to standards would include just about anything from the International Organization for Standardization, aka ISO, headquartered in Geneva, Switzerland, with members from 164 countries contributing to its more than 22,000 published standards which cover almost all aspects of manufacturing work and technology development and provision.

One ISO standard you should become familiar with is ISO/IEC 27001, which lays out requirements for an Information Security Management System. It details best practices for the secure management of data and covers the process from end to end, including the hiring and training of staff who may have access to confidential information; password or other credentialing use; data storage procedures; encryption strategies; back-up, restore and disaster recovery policies; physical access to premises; server configuration and updates; vulnerability and penetration testing, as well as many other areas.

When a company is ISO/IEC 27001 certified, it means that the company has passed a stringent audit by an independent third party. The certification, if granted (many companies fail), shows that the company complies with all major requirements, has written policies covering all aspects of the ISO/IEC 27001 standard and can prove that staff are properly trained in the standard (and all of its related policies and procedures) and that the standard is consistently followed, and that means by everybody, from new hires all the way up to the CEO and the board.

Furthermore, such certification is not a one-time event. Companies that wish to maintain their ISO/

IEC 27001 certifications must submit to annual audits conducted by independent, ISO-accredited organizations. This is in addition to the companies' ongoing production of non-conformance, corrective action and preventive action reports and a cycle of internal audits and general "fit-for-purpose" policy, procedure and detailed work instruction reviews.

Praxonomy achieved its ISO/IEC 27001 certification after an audit by the British Standards Institute, an organization founded in 1901 and accredited by more than 20 international standardization bodies in the EU, the US, China and Japan, including the ISO. Praxonomy proudly displays its ISO/IEC 27001 certificate on its website. Though by no means the company's only security initiative (process and policies are only one aspect of a comprehensive security framework), it is your assurance that Praxonomy adheres to global best practices for data management and security.

SOC / SSAE

Now that you have one assurance that your software provider is following best security practices, you have to go further. Your data will likely be residing in a third-party data center because SaaS vendors generally buy data center services from companies that specialize in data center and related service operations.

How can you be sure that the vendor's data center is secure? The answer is that the data center should be able to provide its own ISO/IEC 27001 certification, or at least a SOC 2 Report. Ideally, a data center that provides anything more than co-location services should hold both certifications.

The System and Organization Controls (SOC) report, also referred to as a Statement on Standards for Attestation Engagements No. 16 (SSAE-16), was formerly called the Statement on Auditing Standards No. 70 (SAS 70). Developed and administered by the American Institute of Certified Public Accountants (AICPA), SOC does have an international equivalent, the International Standard on Assurance Engagements (ISAE) 3402. Nevertheless, it is very much an American standard.

There are various "levels" to this standard. A SOC 1 Report refers to the controls an organization has in place to cover financial reporting. A SOC 2 Report relates to data and process issues. A SOC 3 Report usually indicates vendor compliance in respect to one or more SOC 2 topics but does not disclose testing methodology or details of vendor-specific results.

American companies that fall under Sarbanes-Oxley Act (SOX) rules often ask technology vendors for SOC reports. Though similar, SOX and SOC are different.

SOX is a law that requires (mostly) big American companies to keep certain types of records and disclose risk management and financial information to regulators and the public.

SOC is an accountant's report on a company's internal controls and is designed to examine the company's data security policies, warrant the effectiveness and efficiency of its operations model and thus bolster stakeholder confidence.

For our purposes, the important SOC standard is the SOC 2 Report. This is based on the Trust Service Criteria and provides details for controls in the critical areas of Security, Availability, Processing Integrity, Confidentiality and Privacy. Under "Security" the report specifies that "Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives." This is a good start.

Note that your SaaS provider may not be legally authorized to share its data center service provider's SOC 2 Report with you. Some data centers do provide this report directly from their websites but many do not. Your SaaS provider may have to introduce you to relevant contacts at its data center services provider and let you ask for certification proof on your own.

IN CONCLUSION

Before you commit to a SaaS provider, your due diligence should include an investigation of its track record on data security. Globally recognized third-party certifications such as ISO/IEC 27001 and SOC 2 are crucial parts of such an investigation. In

fact, these reports should cornerstone your review process.

Keep in mind however that ISO/IEC 27001 is an international "best practice" audit certification whereas the SOC 2 Report is an American "good practices" framework. Though the two certifications examine overlapping security issues, the certifications are not the same and do not necessarily carry the same weight.

Also keep in mind that some SaaS providers mislead prospective clients by noting that their data center service providers are ISO/IEC 27001 or SOC 2 Report certified while not mentioning the fact that they themselves are not certified to any standard. So read the fine print. It matters.

Praxonomy recommends that you ask your SaaS provider to provide proof of the following:

1. The SaaS provider's own ISO/IEC 27001 certification,
2. Its Data Center ISO/IEC 27001 certification or current SOC 2 Report (preferably both),
3. Its GDPR compliance and privacy policy documentation,
4. Up to date transparency reports such as warrant canaries (this means that the vendor discloses law enforcement or other government agency requests as well as court orders for client data), its responses to those requests and orders and any related transparency policy documentation — good vendors will also include disclosures on data breaches, if any,
5. Third-party badges or seals in respect to data privacy practices and compliance (such as Verasafe or TRUSTe),
6. Periodic third-party reports relating to system penetration and vulnerability testing,
7. Clear and comprehensive data privacy and data security terms and conditions in its user contracts, and
8. Its own data security whitepapers, including software architecture descriptions.

If your SaaS vendor can give you these things, then the vendor is probably taking its data security responsibilities seriously.

ABOUT THE AUTHOR

Steve Schechter has more than 30 years of IT management experience with Barclays Bank, Merrill Lynch, Warner Bros. and others. He has focused on cloud operations and governance for the past seven years and is currently the Director of Cloud Services at Velocity Technology in Hong Kong.