INFORMATION SECURITY AND THE SUPPLY CHAIN

By Paul Traill,
Senior Information Security Consultant
PGI

As a best practice, being able to address security requirements with your critical service providers is included in all of the major cyber security standards consistently referenced today (see Table 1).

Why is this?

Well, it is a recognition that organisations do not work in a vacuum. They are not air tight entities and many businesses provide access to their systems or networks for other third-party companies; or they share data with them. This is to facilitate business justifiable needs. Typically, this can include the provision of essential goods and services. For example, vendor support and maintenance of systems; outsourced infrastructure, such as data centre hosting; or use of outside expertise for marketing, sales, or recruitment.

Where third-parties have access to your systems or they are being provided with your data (which could include confidential customer data) there is a risk. This risk is manifestly related to potential data breaches, and the impact it would have on your own organisation; which could result in:

- Potential financial liabilities (e.g. regulatory fines)
- Litigation
- Loss of reputation, and damage to the brand
- Loss of customers.

You may be assured that within your own organisation you have the lid firmly locked down on this security box. You have up to date security policies, standards, and procedures in place; they have been communicated effectively across the work place; you have skilled staff assigned to specific security roles and responsibilities; you have robust and compliant response and recovery processes; physical and technical security controls are well established, and so on. But what about that critical third-party supplier? Do they have the same level of security controls in place? Could they be the weak link where a data breach is waiting to happen?

Table 1: Security/Data Protection Standards and Supplier Assurance

Standard or Regulation	Description	Clause
ISO 27001:2013	International Standard for Managing Information Security Management Systems	A.15 Supplier Relationships
ISO27036:2014	Information Security for Supplier Relationships (Parts 1 – 4)	The Whole Standard
PCI DSS v3.2	Payment Card Industry, Data Security Standard	Requirement 12.8
ISF SOGP	Information Security Forum Standard of Good Practice	CF16 External Supplier Management (2011 Version)
IASME	The Standard for Information Assurance for Small and Medium-sized Enterprises	4.7 Operations and Management
CobiT	Control Objectives for Information and Related Technology	DS2 Manage Third-Party Services (v4.1 Reference)
GDPR	General Data Protection Regulation	Article 28 – Processor Article 32 – Security of Processing

According to the Ponemon Institute's benchmark study in 2017, data breaches caused by third parties are on the rise (7% annual increase), and at least 56% of respondents had experienced a breach from this source.

So, what can you do to mitigate this risk?

Measures that should be applied largely boil down into 3 key areas:

- Due diligence on any perspective business partner before you partner with them (Table 2, #1)
- Contractual agreements, completed during onboarding processes (Table 2, #2)
- Reviews carried out on a regular and ongoing basis (Table 2, #3).

#	Standard	Sub-clause	Description
1	PCI DSS v3.2 Requirement 12.8	12.8.3	Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.
2	ISO 27001:2013 A.15 Supplier Relationships	15.1.2 Addressing security within supplier agreements	All relevant information security requirements should be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organisation's information.
3	ISO 27001:2013 A.15 Supplier Relationships	15.2.1 Monitoring and review of supplier services	Organisations should regularly monitor, review and audit supplier service delivery.

Let's have a closer look at what these good practices can look like.

Due Diligence

Standard procurement practices dictate that an invitation to tender (ITT) or a request for proposal (RFP) exercise is carried out to acquire responses from candidate service providers. As part of this process, a relationship assessment (or due diligence review) should take place to check details of provider history, any previous and current business arrangements or disputes, demonstrable levels of maturity and underlying infrastructure. Most importantly, in relation to this article's focus, information security-related questions should be included at this stage as well, to ascertain the supplier's initial stance and degree of commitment to information security.

For example, you could enquire do they have any ratified security certifications in good standing? Do they have a dedicated security manager and / or security team in place? Do they have a documented security strategy and / or security architecture framework? How many security incidents have they managed in the last 5 years?

The earlier you can embed security considerations into a process the more beneficial and cost effective it is to the company, and what is to come next. This is similar to best practice activities in a Systems Development Life-Cycle (SDLC), where a security risk assessment is carried out in the discovery and design phases, rather than just before a new application is launched into a production environment. It's a bit too late by then to consider security implications for the first time (and very costly to unpick).

Contracts

What needs to be in place between you and the third party is a set of mutually agreed and legally enforceable terms to safeguard your business. This type of agreement typically will cover a wide range of subjects, depending upon the type of relationship being entered into. It is critical, however, that this must include security-related stipulations.

Depending upon the size (and negotiating weight) of each party the contract template may be proposed by your organisation or the other third-party. Either way, here are some critical subjects that need to be included:

- Roles and responsibilities; including single point of contact (preferably knowledgeable) to be able to respond on all matters relating to information security
- Security incident and data breach notification
- Right of inspection (audit) by your organisation
- Security policies and risk governance
- Employee security awareness training
- Access controls
- Change management
- Physical security of premises
- Systems development practices (where applicable)
- Escrow (where applicable)
- A range of technical security controls such as anti-malware, system patching, system hardening, firewalls, encryption, security event monitoring are in place (precise range and implementation priority will depend upon the type of agreement)
- Third party's own security assessment and testing practices
- Data protection, transfer, handling and acceptable use, retention, and destruction
- Resilience measures and backup regimes
- Confidentiality and non-disclosure
- Sub-contracting
- Defect or conflict resolution
- Mechanism for providing regular reviews and reporting on effectiveness (e.g. service level agreements)
- Termination and exit.

Security Reviews

This links back to the "right of inspection" clause included in the contract. As a minimum, you should carry out, on an annual basis, a formal check of how compliant the supplier is with your SLA's and Contract terms. The way this is conducted will vary depending upon the business relationship, type of service being offered, and the criticality of the services.
This can range from a self-completed checklist exercise; a questionnaire that you request the third-party to complete; through to a site visit to inspect facilities, interview key personnel, and verify at first-hand, how effectively are procedures being implemented.

Needless to say, the latter is the most effective method of carrying out a security review, but realistically this can be constrained by your own people resources (or budget, in case you want to use an auditing managed service).
This means that you will need a way of risk-assessing which third-party suppliers are the most critical and therefore will be the subject of more focus and attention.

In conclusion, it is critically important that information security requirements are included at all stages of supplier relationship management. For this to work effectively, the business needs to foster a spirit of collaboration between potentially siloed departments and separate agendas; and ensure that Procurement teams, Vendor Management, Legal Counsel, and Information Security practitioners are all working together through an integrated process, with security firmly included as a key component.

> "Standard procurement practices dictate that an invitation to tender (ITT) or a request for proposal (RFP) exercise is carried out to acquire responses from candidate service providers."