Security Best Practice for Managing Third Parties

Cybercrime is now widely cited as a primary risk to the global economy. Security should extend outside your organisation to the broader ecosystem of vendors, partners, and other third parties.

The below short guide has been drafted to help you review aspects of your outsourced relationships and to assist in identifying risks.

According to a 2016 KPMG survey of professionals who investigated 750 frauds between March 2014 and August 2015, for the majority of organizations, their controls are not strong enough. This survey found that weak internal controls were a contributing factor in no less than 60% of frauds. The threats are constantly changing and organizations need to conduct regular risk assessments, examining whether the controls in place are fit-for-purpose or need to be changed and adapted in the light of the evolving fraud and cybersecurity landscape.

In our opinion the best defensive systems consist of several layers so that a single point of failure does not allow a breach. In addition to a protective layer, further safeguards can be provided by a detection layer that provides on-going monitoring. Organisations should also develop an easily accessible response plan in case the initial defence fails, the response plan should seek to minimise the extent of any attack.

Some basic checks that can reduce your risk exposure are as follows:

- All third parties that provide critical services or that have access to sensitive information should **meet or exceed internal information security and risk requirements.** There have been numerous cases where access to a secure network is facilitated by weak controls on a seemingly unimportant component or system.
- **Comprehensive 'Third Party Information Security Assessment Policy'** and associated compliance verification processes are required. Information security is an important area of focus to ensure that intellectual property and/or sensitive user data is secured by the third party. Intellectual property and/or user data should be secured.
- **Periodic and surprise reviews and/or independent audits** are recommended to confirm standards are being adhered to in relation to information security. The frequency and scope of these reviews/audits should be proportional to risk. Audits should be carried out by an independent trusted party to confirm that agreed processes and levels of security are maintained to a high standard and that gaps are identified and correction actions are documented and actioned.
- **Vulnerability and risk assessments** of third party systems managing critical processes or data should be conducted and reviewed frequently. Depending on the level of risk, external as well as internal assessments should be undertaken. Gaps identified should be tracked through remediation.

- Intellectual property, personally identifiable information, transactional capabilities and other **high risk information/functions should be protected**. Consider the impact to your business, both financial and reputational, if such data was to fall into the wrong hands.
- For third party employees who will be accessing your systems or data, consider implementing strict procedures such as background checks, staff rotations, training, entitlements and access reviews as well as mandatory absences. **Employee due diligence** should be considered an extension of your own high standards.
- **Ensure secure connectivity in communications** with a third party including firewalls, encryption, and other mechanisms to protect data and systems. A minimum standard of security in these communications should be agreed up front and should be validated as part of vulnerability assessments.
- **Segregation of duties** should be implemented for higher risk activities, this should be backed up by audited policies & procedures and password controls.
- Segregation and **restrictions of access to systems** should be considered where "high risk" systems are accessible on the same network segment and comingled with other systems/data.
- **An issue management plan and response process** should be in place and tested in case of any data/system breach or malfeasance. It is important to agree on the components of a response process as well as transparency of any internal reporting.
- **Physical site security should also be reviewed.** Ensure that minimum standards are agreed for both primary and COB premises as required.
- Policies relating to data retention, storage, and privacy should be in place. **Privacy and data retention policies** should be agreed and clearly set out how, where and for how long data will be stored.

Please note that it is important to contact your bank immediately and advise them of any fraudulent activity, doing this as soon as possible may reduce the impact of a fraud.

Treasury and Trade Solutions
transactionservices.citi.com

GRA29064 01/18