Mitigating Insider Threats From Trusted Business Partners

"All lasting businesses are built on friendship and trust."

Let me start by defining what a trusted business partner is? Any external organisation or individual that has contracted to perform services for the organisation.

In most cases, that nature of these services requires the organisation to provide the trusted business partner authorised access to proprietary data, critical files and/or internal infrastructure.

For example, if an organisation contracts with a company to perform payroll services, it would have to provide access to its HR data, thereby establishing trusted business relationships.

It is also interesting to realise, that trusted business partners also include individual consultants, temporary employees, contractors, including any former employee of the organisation who is then hired as a consultant or contractor.

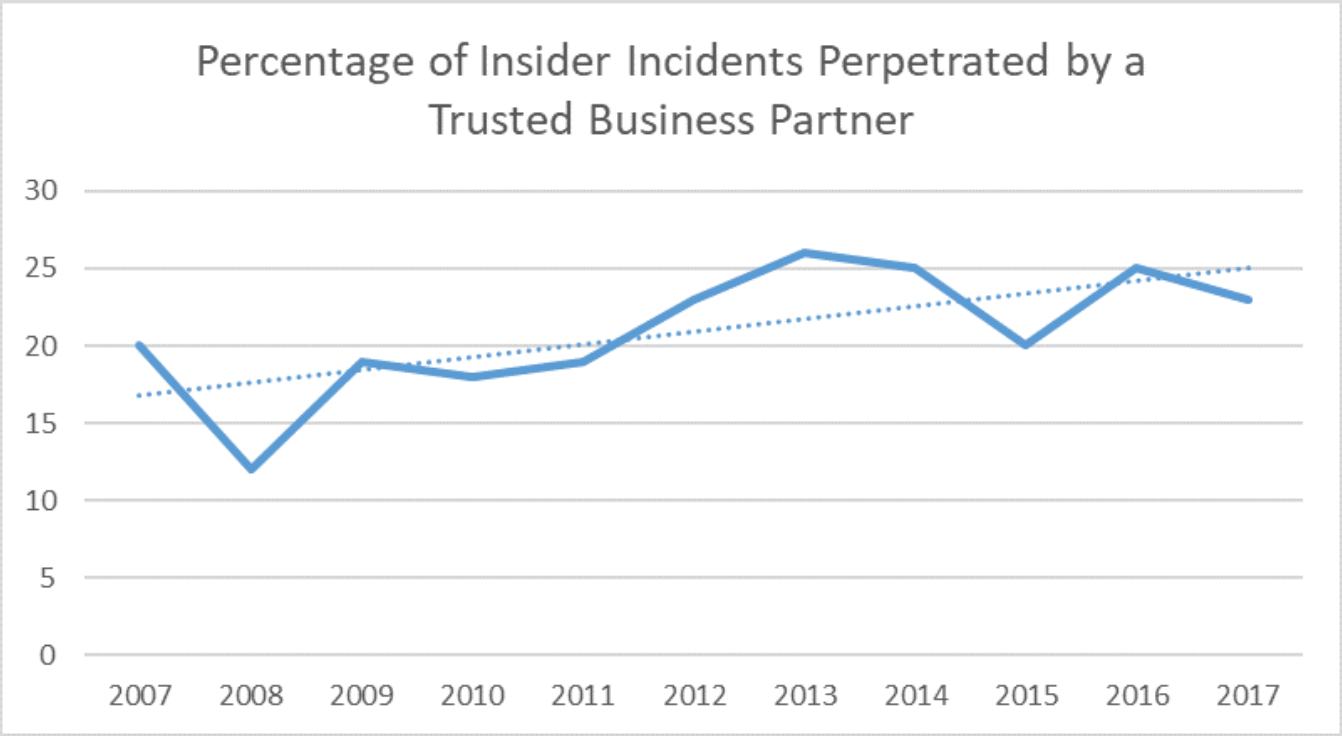
This is why it is essential to realise the potential insider threat risk posed by these contractors. But what could go wrong? Here is an example…

MyPayrollHR, a now-defunct cloud-based payroll processing firm based in upstate New York, abruptly ceased operations in September 2019, after cheating employees at thousands of companies. It is alleged that the CEO involved in wrongdoing and misconduct, resulting in countless people having money drained from their bank accounts and has left nearly $35 million worth of payroll and tax payments in legal limbo.

The use of trusted business partners is common today. Organisations outsource primarily to cut costs. But today, it is not only about cutting cost but also about reaping the benefits of strategic outsourcing such as accessing skilled expertise, reducing overhead, flexible staffing, and increasing efficiency, reducing turnaround time and eventually generating more profit.

All industry sectors have consistently experienced insider incidents committed by trusted business partners - any individuals an organisation has contracted to perform a service. As indicated in the figure below, the percentage of insider incidents perpetrated by trusted business partners has typically **ranged between 15% and 25%**

across all insider incident types and industry sectors according to the insider threat division of CERT.



Breakdown of trusted business partners insider incidents

- Finance and Insurance: 38%
- Federal Government: 31%
- Entertainment: 30%
- Information Technology: 22%
- Health Care: 18%
- State and Local Government: 16%

It is essential to realise that trusted business partners have the same access to your critical assets as employees and, in turn, have misused that access to harm victim organisations in the past.

The following page, breakdown details the different types of insider threats committed by trusted business partners.

Insider Sabotage. This crime is committed by a privileged technical user who seeks revenge for adverse work-related events either with the company that has hired him/her or with the contract organisation.

Example

A contractor was employed as a programmer and Unix engineers by Fannie Mae. The organization notified that insider that his contract would be terminated for a script error that he had made. The insider who was permitted to finish out his day at work and subsequently planted a logic bomb in a script that would have deleted the root passwords for 5,000 of the organization servers. Fortunately, Fannie Mae system admins found the malware days after the contractor left.

Insider Theft. In this case, the trusted business partner has authorised access to organisation assets. The insider uses authorised access to steal these assets from their client.

Example:

In 2016, hackers stole sensitive data - F-35 Joint Strike Fighter and other vehicles and munitions from a small Australian defense company with contracting links to national security projects.

Insider Fraud. Simply, you are at risk from fraud when you hire contractors for positions requiring access to personally identifiable information or financial information.

Example

A claims processor at a company contracted by an insurance company used authorised access to divert million dollars through falsified insurance claims to a personal address.

Recommendation and Mitigation

Who are your trusted business partners?

By now, you probably understand that you need to include trusted business partners as part of your countermeasures for insider threats.

The key question to ask: Who are your trusted business partners? And secondly, is there anyone else that you provide authorised access to your critical assets?

Recommendations

Here are some of the recommended mitigations that you should consider

- Create clear contractual agreements that explicitly state that trusted business partners are also responsible for protecting organisation assets. It should include restrictions on how they handle and share information.
- Understand the policies and procedures of the trusted business partner. The trusted business partner should understand and follow your corporate policies and controls as well as you should ensure that the trusted business partner policies and procedures are at least as effective as your safeguards.
- You should monitor actions performed by trusted business partners. You need assurance that access to and distribution of your data is monitored.
- You should monitor, manage and maintain access rights. Trusted business partners should have the necessary access to their job and not beyond it.
- Deactivate access following termination. You should perform a rigorous termination procedure.
- Enforce separation of duties. Business processes should enforce separation of duties regardless of speed or priority required.
- Manage and anticipate negative workplace issues coming from trusted business partners.

The insider threat landscape is continually evolving. The use of trusted business partners creates a more complex environment to ensure the confidentiality, integrity and availability of your assets.

It is therefore essential for you to to understand that the use of trusted business partners is really an extension of your business. In the same manner, as a tennis racket is an extension of one's arm. The rules that you apply to your business need to be applied to the trusted business partner.

How can we help you?

If you fear that some of your trusted business partners may be taking advantage of your business or maybe placing your organisation at risk by performing unwarranted actions, then we can uncover the risks and security blind spots in how your trusted business partners interact with your organisation through an **insider risk assessment**.

The **insider risk assessment** is your first step in gaining control and certainty about the potential risks from trusted business partners.

Within 30 days, we will be able to provide you with a report on your organisation risks and elevate your highest risk users for inspection.

- Simple deployment collector on endpoints of your choosing
- 30 days we will monitor your endpoints, collect user activity data and analyse
- Threat report – We will review the findings and alerts and compile an executive summary & detailed report that highlights the biggest risks on your organisation

How to get started? Get A Threat Assessment HERE or contact us insider@commsnet.com.au

Contact Us

You can reach us at the following

- Web: www.commsnet.com.au
- Phone: +61 2 6282 5554
- Email: insider@commsnet.com.au
- Twitter: www.twitter.com/commsnetgroup