Combating The Insider Threat Supply Chain Trust

In today's business landscape, organisations often rely on suppliers such as technology vendors, businesses partner resources, suppliers of raw materials, shared public infrastructure, and other public services. These “outside” entities are all examples of the supply chain, which is a type of trusted business partner (TBP). However, these outside entities can pose significant security risks.

Example - Target

The infamous Target hack back in November 2013 was traced back to network credentials that were stolen from a third-party vendor. The vendor in question was a refrigeration, heating and air conditioning subcontractor that has worked at several locations at Target and other top retailers.

It wasn’t clear why Target would have given an HVAC company external network access, or why that access would not be cordoned off from Target’s payment system network.

The result was the data leakage of personally identifiable information of over 100 million individuals.

So, what is a supply chain attack?

A supply chain attack also called a "value-chain" or "third-party attack" occurs when someone infiltrates an organisation system through an outside partner or provider with access to the victim systems and data.

The risks associated with a supply chain attack have never been higher, due to increased cooperation and partnership between organisations.

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.

Meanwhile, attackers have more resources and tools at their disposal than ever before, targeting the smaller, less abled security-abled organisation that leads access to the bigger prize.

As the saying goes: "*why try to break the front door when you can come around the back*"

According to a survey conducted in late 2018 by the Ponemon Institute, found that 56% of organisations have had a breach that was caused by one of their trusted business partners.

The Ponemon Institute went on to say that misuse or unauthorised sharing of confidential data by third parties was the second-biggest security worry for 2019 among IT professionals.

Here are two questions for you:

1. How many of you consider the risks when the supplier relationship is terminated? And
2. Do you include adequate details for managing the tricky process of vendor termination?

Other risks to consider

- **Risks in hardware and software supply chain** - Almost every company uses outside software and hardware. Each purchased device, each downloaded application needs to be vetted and monitored for potential security risks, and all patches have to be up to date.
- **Risks in using cloud providers –** Your business applications and data are housed in a trusted cloud provider site that you have no control, let alone know who has access to it.
- **Risks from professional services –** Just because services are provided by trusted business partners, it doesn't mean they are not immune to the same problems that you may be experiencing. They too could be impacted by an insider incident.

Highly recommended practices to adopt

The list below outlines several best practices that are available to assist you with mitigating insider threat risk within the supply chain.

- **Acknowledge that supply chain trust risks exist**. Identify each supplier's scope of activities and where they fit into your organisation's supply chain.
- **Define and document the rules of engagement.** Define the terms and conditions, ensuring that these rules are integrated into the contract between the supplier and your business.
- **Deploy a monitoring strategy.** Never assume that the trusted business partners are doing the right thing by you. Trust and verify. Monitor their actions and identify anomalies and deviations.
- **Form effective partnerships** by having clear communications that are supported at all levels of your organisation.
- **Background screening**. Don't rely on the trusted business partner to screen their people. Do your own investigation to mitigate insider threat risks adequately.

- **Develop a formal onboarding process** to help your business set up a coherent, trustworthy and communicative relationship. That includes inducting the TBP into the organisation policies and procedures.
- **Develop an intellectual property (IP) ownership policy**. Define your organisation ownership rights over IP created.
- **Ensure an acceptable use policy** that informs the TBP the use of organisations assets
- **Reporting of a policy violation by the TBP.** Any violation by the TBP must be reported through a defined process.

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 organization 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

For more information, you can also send them an email at: info@commsnet.com.au Or give us a call at: +61 26282-5554.