Identifying and Managing Strategic Supplier Risk

Supplier interruption can cause an organization significant operational and strategic risk. Suppliers often hold tremendous amounts of data and intellectual property, relating to the parent organization that they are working with, that can be directly compromised, putting everyone at risk. Adversaries and malicious competitors have even used supplier networks as a launch vector into another organization's network. But not all suppliers are equal in terms of the risk they represent. Some suppliers are difficult to replace, have a tightly integrated relationship, or have critical IP or technical access to the parent organization's network or systems, and therefore are strategic and critical pillars in the supply chain of any organization.

Poor supplier security can have a big impact on all parties involved in the supply chain. For example, look at Larson Studios, a small audio post-production shop that works with big entertainment companies like Netflix. In 2016, hackers were scanning the internet for PCs running older versions of Windows that they could easily break into. When they found an old computer running Windows 7 at Larson Studios, they attacked. Variety interviewed the chief engineer at Larson, who said, "They were basically just trolling around to see if they could find a computer that they could open. It wasn't aimed at us." The attackers infiltrated Larson Studios and ended up dumping 10 unreleased episodes of the series Orange Is the New Black, despite Larson paying the $50,000 demanded as ransom.[1]

Attacks on strategic suppliers are costly because they can impact several organizations at once or can cause an operational or business outage because your operations are so dependent on them. A data breach at the American Medical Collection Agency, a third-party billing company, exposed 7.7 million customer records at LabCorp and 12 million patients at Quest Diagnostics.[2] Attackers compromised the Indian IT outsourcing firm Wipro and used it to launch follow-up attacks targeting over a dozen Wipro customers[3] Some of the best-known data breaches of national concern were also achieved through suppliers. Target's data breach of 40 million credit cards was the result of a compromise at a third-party HVAC company, Fazio Mechanical Services.[4]

Home Depot's loss of 56 million credit card numbers was also caused by a third-party vendor.[5] Attackers use the same strategy when attacking nations, such as the 2018 theft of submarine warfare data from a Navy subcontractor.[6]

A priority for any organization must be to manage strategic supplier risk because of the wide range of scenarios that can surface:

Supplier Disruption

Ransomware attacks or financial fraud that disrupts cash flow can cripple a supplier's operations, preventing them from delivering goods and services, and thereby creating cascading disruptions.

Compromised Data

Many suppliers hold sensitive intellectual property or customer data on their networks that can be compromised. Several recent breaches have involved no compromise on the parent's network, but data was still lost because a supplier had sensitive information that was poorly managed.

Gateway Attack

Suppliers are often treated as trusted partners and may have access to the parent organization's network. Attackers attempt to use the supplier as a gateway to other larger organizations by exploiting the level of trust given to suppliers.

Strategic suppliers make excellent targets because they often have weaker security controls than the organizations they supply. They may have smaller IT budgets due to their size and may not have the same advanced technology available to larger organizations. Many smaller suppliers also believe—because of their size—that they aren't a target. This may have been true years ago, but attackers have since shifted tactics. Instead of targeting specific organizations, adversaries now routinely look for any insecure system, regardless of who owns it. Once an insecure system is found, attackers compromise and attack.

Failures of Supplier Risk Solutions

Organizations have tried a few different strategies for managing supplier risk, but none have worked out well. Many still use a compliance-based approach by using surveys and checklists to approve supplier and partner networks. The limitations of this method are well known. Many surveys are self-validated, aren't backed up by data, are imprecise and ambiguous about safeguards, and are only point-in-time assessments. Their value is extremely limited.

1 variety.com/2017/digital/features/netflix-orange-is-the-new-black-leak-dark-overlord-larson-studios-1202471400/
2 krebsonsecurity.com/2019/06/labcorp-7-7m-consumers-hit-in-collections-firm-breach/
3 krebsonsecurity.com/2019/04/experts-breach-at-it-outsourcing-giant-wipro/
4 krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/
5 www.computerweekly.com/news/2240234281/Home-Depot-traces-credit-card-data-hack-to-supplier-compromise
6 news.usni.org/2018/06/08/china-stolen-vast-amounts-navy-submarine-missile-data-multiple-breaches-contractors-servers

Some have moved on to third-party risk scorers for supplier risk management, but the data and systems that are monitored are based on what the supplier already knows about, so hours are spent investigating internet assets that are known and have already been remediated. Internet assets in the cloud and non-web protocol exposures that are frequent attacker targets are often totally missed—which means that breaches occur via that one system or service that no one knew was a risk.

Improve Security Outcomes

Organizations need an effective way to continually monitor their suppliers based on prioritized policies, and the ability to hold them accountable based on timely, accurate feedback data that indicates how suppliers are responding operationally.

Building a Shared Governance View

Risk scorers and surveys don't improve security. Instead, working with them turns into a compliance exercise. To effect change, your strategic supplier security model should mandate the following:

- **Complete Visibility**

  Organizations must evaluate a supplier's entire public-facing perimeter and assess what their internet assets are doing. Tracking internet assets through the cloud, even when they are ephemeral or multi-tenant, is critical for full situational awareness of the supplier. Monitoring traffic patterns (via NetFlow data) and verifying communication policies (e.g., geoblocking and suspicious communications) can uncover unknown problem areas.

- **Tailored Policies**

  Organizations must be able to evaluate their suppliers against their specific policies and to work with their suppliers to mitigate violations. Organizations need a way to discuss exceptions to policies and to mediate disagreements about systems and services and their associated ownership and business risks.

- **Continuous Alignment**

  Continuous monitoring is needed to verify if risky items are successfully remediated. Waiting weeks or months for a risk score to update is too slow. Instead, organizations can enforce shorter SLAs with suppliers when data is refreshed daily, ensuring that the parent organization and suppliers are continuously aligned.

- **Shared Operational Ownership**

  Organizations must drive actual changes in the operational risks of their suppliers. This should be positioned as shared ownership. The parent organization is protected from potential risk. The supplier benefits from stronger policies and guidance.

A shared view between a parent organization and a strategic supplier is the basis for strong collaboration. Once both parties agree, clear policies can be implemented. SLAs for remediation time, policies on certificate strength, agreement on disallowed devices like database servers, and restrictions on exposed development environments can all be used to posture a network into a more robust state. Even simple requirements like having a designated point of contact for each critical system and service can have a positive impact by reducing costs and improving time to remediate.

Where to Begin

Start with the most critical suppliers first. Rank your suppliers to identify those that have the most influence on your success, such as:

- **Suppliers that have significant access to your network**
- **Suppliers that hold your sensitive data**
- **Suppliers that manufacture specialty components**

Having a shared view with your suppliers gives you an opportunity to mentor suppliers to a higher maturity level. Your economic leverage can be used to improve their security practices.

How to Boost Supply Chain Visibility With Xpanse

The Cortex® Xpanse™ Internet Operations Management Platform provides suppliers and parent organizations with a secure, shared governance model to drive operational outcomes.

Organizations can start by providing Xpanse with as little as the name of the strategic supplier. Xpanse uses its proprietary mapping technology to discover internet assets relating to the supplier across registered ranges, commercial IP space, and dynamic cloud environments. This data is then surfaced in a web portal where the supplier and parent organization can review, triage, and monitor policy violations.

Xpanse brings technical benefits that can break the cycle of poor supplier management, including:

- **Full visibility through intelligent internet inventory:**
  Complete discovery of more internet assets in cloud and other dynamic environments than any other solution.

- **Accurate identification:**
  Highly accurate attribution and full data transparency so that suppliers and parents can quickly determine whether a device is business-critical.

- **Rapid data refreshes:**
  Daily updates to quickly verify remediation.

- **Deep and unique risk analysis:**
  Uniquely able to remotely detect risky and out-of-policy traffic on supplier networks without installing or configuring any local sensors.

Don't Wait to Manage Your Supply Chain

Your organization is only as secure as your least-secure supplier. You must continuously monitor your suppliers' security posture and have a shared governance model for operationalizing policies to remove blind spots on your suppliers' networks that could expose your organization to business disruption or a breach.

Xpanse works with the world's leading organizations to secure their networks and those of strategic partners and suppliers. With complete, current, and accurate data on your suppliers' internet assets and exposures, you can drive operational improvements that reduce risk for both your organization and your suppliers.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

cortex-xpanse-Identitfying-and-Managing-Strategic-Supplier-Risk-wp-050421