Securing the supply chain with risk-based assessments

Whether it’s caused by poor quality control or a malicious actor, third-party software, solutions, and manufacturers can introduce risk to corporate, employee, and customer data. Microsoft is committed to building and implementing best-in-class security programs and processes, and is constantly working to reduce exposure to cybersecurity risks. Microsoft Core Services Engine (CSE, formerly Microsoft IT) helps support the overall security mission at Microsoft by offering key security services that help protect corporate data and users. We are also securing the supply chain that we use to procure third-party software, goods, and services that are used at Microsoft.

An unsecured supply chain can introduce great risk to an organization. If vendor staff aren’t properly vetted, or if we purchase hardware that does not meet our security standards, we can lose data. The factories that build Microsoft products must have a secure infrastructure to ensure that manufacturing data and facilities are secure. As you may have seen in the media, several companies have had data breaches that allowed hundreds of millions of customer records to be compromised. On average, it takes 229 days after a breach for it to be detected. Often, these breaches were caused by a vulnerability in third-party software or services being exploited, costing those companies tens of millions of dollars and damaging customers’ confidence.

A company is only as strong as its weakest link. We needed a way to help ensure that we hold our suppliers to the same security standards that we apply to ourselves. Our supply chain assurance program helps us evaluate and prioritize the risk level and security of third-party suppliers across Microsoft. Some of the benefits we have seen from introducing a security framework as part of the procurement process include:

- **Reduced risk.** Supply chain security services help us proactively address compliance or security issues and reduce financial and legal exposure.
- **Operational efficiencies.** Standardized governance and lifecycle management processes have helped streamline our fulfillment processes.
- **Cost savings.** Our strategic alignment with competitive technology objectives helps us avoid unnecessary software purchases.
- **Risk-informed decision making.** We assess procurement requests and make recommendations to business groups and leadership teams that help them make more risk-informed decisions.

It is important to note that each organization is different; this program and strategy was designed to align with Microsoft business processes. It represents only a few key areas of our assurance program and is not a roadmap for implementation.

Developing a framework for assessing risk

The supply chain assurance program helps inform the procurement process, which includes the business group and leadership approval chain. We use a combination of supplier risk profiling and focused control-based assessments that include:

- Risk indicators.
- Scoring.
- Risk profile.
- Recommended courses of action.

The first thing we had to do was create a comprehensive inventory of all the third-party suppliers, software, and services at Microsoft. Once we had this inventory, we could focus on controls and determine where to use profiles and
scoring to optimize our resources. But assessing each purchase request for software, services, or hardware is resource intensive and not scalable.

**Policies, standards, and control procedures**

We created policies, standards, and control procedures for software, goods, and services from third-party suppliers. These policies map to industry regulations and authoritative sources that help us meet both our external and internal security obligations.

Control procedures give us detailed steps to follow for specific technologies or processes. Our security technical control procedures (TCPs) are created by a board of security experts and are regularly updated to address the latest technology, industry security standards, and best practices.

**Creating a supplier risk profiling model**

We gather information from each supplier and build a risk profile for them. The supplier’s profile is scored for risk based on our experience with past purchases. This score helps us determine how much more assessment we need to give us confidence in their product or service.

We use a dashboard for at-a-glance information about each supplier and the health of the products or services that they offer. The dashboard, shown in Figure 1, pulls from multiple data sources, including the supplier’s profile score and any documented findings from the supplier risk profiling model.

<table>
<thead>
<tr>
<th>Supplier Risk</th>
<th>Business Criticality</th>
<th>Privacy Impact</th>
<th>Regulatory &amp; Compliance</th>
<th>Global Cybersecurity Index Score</th>
<th>External Score</th>
<th>Assessment Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Yes</td>
<td>Yes</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Advanced</td>
</tr>
<tr>
<td>Medium</td>
<td>Yes</td>
<td>Yes</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>Advanced</td>
</tr>
<tr>
<td>High</td>
<td>Yes</td>
<td>Yes</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Advanced</td>
</tr>
</tbody>
</table>

**Service Health**

<table>
<thead>
<tr>
<th>Service</th>
<th>SERVICES</th>
<th>SOLUTIONS</th>
<th>FACTORIES / OFs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>2 Services Provided</td>
<td>3 Solutions Provided</td>
<td>2 Factories Provided</td>
</tr>
<tr>
<td>Health</td>
<td>G</td>
<td>8/10</td>
<td>0</td>
</tr>
</tbody>
</table>

**Figure 1. Supplier risk profile dashboard**

microsoft.com/itshowcase December 2017
Integrating assurance into the procurement lifecycle

The supply chain assurance program is a collaborative effort between security, procurement, and governance. The program integrates security escalations to ensure that we choose secure third-party software, goods, and services from trusted suppliers.

Figure 2 illustrates the three supplier services that are currently governed by the supply chain assurance program.

Figure 2. Supplier services that are governed by the supply chain assurance program.

Software

Third-party software is any software that is not developed by Microsoft and is not Microsoft intellectual property. It can be cloud-based software as a service (SaaS), on-premises server-based, or installed on client devices. Any third-party software that processes or accesses corporate data is subject to software governance.

Procurement obtains third-party software and services for use at Microsoft and negotiates contracts and service subscriptions. Once procured, the end-to-end governance process is accountable for the effective management of software licenses, subscriptions, inventory, and maintenance through the entire product life cycle.

When procurement acquires third-party software, they assess the supplier, look at their risk profile, and present their findings to management. That information helps leadership make risk-informed purchasing decisions, and helps us negotiate remediation during contract negotiation. Continuous monitoring helps ensure that security controls that are in effect at the time of purchase remain so during their life cycle.

Solution integrators

Solution integrators are suppliers that provide staff augmentation and consulting services. Helping to ensure security around people and services requires different controls than assessing software suppliers. We use supplier risk profiles and assessments to continuously monitor the risk score of the suppliers. Then we partner with them on remediation activities to improve supplier and solution security, which is then reflected in their updated risk score.
Factories
Factories all around the world build components and products for Microsoft. We have worked with most manufacturers since before we rolled out our supply chain assurance program, so we have been assessing them, creating supplier remediation plans, and helping them to improve their profile score. For new manufacturers, we would assess and score them up front so that our findings can be part of contract negotiations.

As Figure 3 shows, supply chain assurance begins during the selection phase of the procurement life cycle.

Pre-selection
We work with the centralized contracting team and give them access to the supplier risk dashboard to help them consider onboarding a new supplier. For suppliers that already have a profile, the contracting office has the information on hand to make more informed decisions and gives them the ability to refine the security language within a statement of work (SOW).

Selection
During procurement, we assess security at the selection phase, before contract negotiation. In the past, we did not usually review security until after software was purchased. Now we assess first, which gives us the ability to seek remediation before onboarding. This helps us avoid known risks with new suppliers or allows us to make change requests part of the contract negotiation.
As illustrated in the table below, for each security category we require attestation—security reviews. We accept some industry-standard compliance attestations in lieu of some of the more detailed security questionnaires. Security questions are based on Microsoft security standards, requirements, and technical controls that apply to our internal applications, as well.

**Table 1. Assessment requirements from the supplier**

<table>
<thead>
<tr>
<th>Category</th>
<th>Required</th>
<th>Alternative</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical location</td>
<td>ISO 27001</td>
<td>None. Supplier will receive findings. Supplier’s risk profile is affected.</td>
</tr>
<tr>
<td>Hosting platform security</td>
<td>ISO 27001 and/or SOC2</td>
<td>None. Supplier will receive findings. Supplier’s risk profile is affected.</td>
</tr>
<tr>
<td>Supplier’s security controls</td>
<td>ISO 27001 and/or SOC2</td>
<td>A questionnaire with 50 detailed security questions* Supplier will receive findings. Supplier’s risk profile is affected.</td>
</tr>
<tr>
<td>Software vulnerability assessment</td>
<td>Third-party PEN test report</td>
<td>Security team performs black-box (PEN) test (only offered to high-risk suppliers based on resource availability).</td>
</tr>
<tr>
<td>Additional security questionnaire*</td>
<td>Supply chain assurance program questionnaire**</td>
<td>None Supplier will receive findings. Supplier’s risk profile is affected.</td>
</tr>
<tr>
<td>Other technical tests</td>
<td>Security team performs the test/scan</td>
<td>None Supplier will receive findings. Supplier’s risk profile is affected.</td>
</tr>
<tr>
<td>Ongoing</td>
<td>Based on supplier/solution risk profile, combination of: Monitoring tools run by security team. Certificate and evidence requests. Full security reengagement.</td>
<td>None</td>
</tr>
</tbody>
</table>

**Contracting**

Because reviews and assessments are done during the selection phase, we can make change requests part of the contract negotiation. We look at contracts and legal as our first line of control. We can require suppliers to make fixes before onboarding and ensure that all provisions are included in the contract.

**Ongoing monitoring**

We have moved beyond one-time assessments and incorporated ongoing monitoring to help ensure that a supplier stays in compliance. The ongoing monitoring is based on data elements in our risk profile, which are updated continually from internal and external sources. When new versions of products or services are released, or when a purchase order is set to renew, we reassess based on the risk profile score and determine if it still passes our assurance needs or if new, control-based activities are required.
Measuring customer satisfaction and program health

We use key performance indicators (KPIs) to measure our own success and refine how we offer services within the program. We are still working to determine which KPIs best communicate the health and overall progress of our program. Defining KPIs is an ongoing—and not always easy—task. We have been incrementally adding features to the program, and with each new feature comes new metrics that we analyze to measure adoption, performance, and customer satisfaction.

Addressing security in the future

The rapid pace of change in technology requires continued investment in cybersecurity to protect our resources from the evolving threat landscape. By programmatically addressing security during procurement of software, goods, and services, we are reducing our risks and preparing for a cloud-only future. A future iteration of our supply chain assurance program will provide governance for the third-party intelligent cloud solutions and intelligent edge devices that interact with our vital business assets.

In the immediate future we plan to include more service categories. We are also looking at ways to include more automation and use cloud intelligence and analytics to boost security programs and processes.

For more information

Microsoft IT Showcase

microsoft.com/ITShowcase

Top 10 ways SQL Server R Services helps to optimize supply chain operations

Bringing digital transformation to the supply chain with Azure IoT Suite

Creating an integrated plug-and-play supply chain with serverless computing

Securing the enterprise

© 2017 Microsoft Corporation. This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.