Supply Chain Cybersecurity: 3 Future Advances
How will the cyber protection of the supply chain advance in the future? To answer this question, we surveyed the respondents on the techniques in place today, and audits make up the top approach, as shown in Figure 1.

**Figure 1: Tools and Approaches Used in Supply Chain Cybersecurity Protection**

<table>
<thead>
<tr>
<th>Percentage of Respondents</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Audits That We Do of Our Partners in Supply, Contract Manufacturing or Logistics</td>
<td>65%</td>
</tr>
<tr>
<td>IT Vendor Risk Management Tools</td>
<td>40%</td>
</tr>
<tr>
<td>Supply Chain Risk Management Tools</td>
<td>39%</td>
</tr>
<tr>
<td>Infrastructure Security Vendors</td>
<td>34%</td>
</tr>
<tr>
<td>Cyber Risk Rating Services</td>
<td>30%</td>
</tr>
<tr>
<td>Consultants</td>
<td>21%</td>
</tr>
<tr>
<td>GRC Tools</td>
<td>19%</td>
</tr>
<tr>
<td>Other</td>
<td>3%</td>
</tr>
<tr>
<td>No Tools Used</td>
<td>4%</td>
</tr>
</tbody>
</table>

n = 80 supply chain professionals
Q: What specific tools is your organization using in the protection of your supply chain cybersecurity? Select all that apply.
Source: 2022 Gartner Thriving Amid Heightened Complexities Survey

A typical audit approach involves trying to understand a vendor’s cyber posture against specific cybersecurity controls, either by having the vendor complete a self-assessment, or having a third party evaluate the vendor’s posture or both. But these audits are difficult to scale, and Gartner research uncovered situations where recently audited partners nevertheless succumbed to a breach.

Due to these limitations, as we look to the future, a variety of approaches will be used in conjunction to help provide a holistic, effective defense. These techniques include tools for automation & scale, talent programs, and education & evangelism.
Expanding the Use of Automation and Tools

Because of the scale challenges experienced with audits, companies are trying to automate the process. Solution providers now include governance, risk and compliance tools in their arsenals, as well as supply chain risk management tools. Providers also include among their ranks infrastructure/OT/IoT security vendors, cyber-risk rating services and consultants.

The goal is to automate the manual approach of assessments, audits and validations as much as possible. Supply chain leaders also are trying to use the technology tools shown in Figure 1 for continuous threat monitoring and alerts as part of their overall supply chain ecosystem risk management approach. This is an opportunity for all of these types of vendors, as the data indicates that the supply chain profession has not settled on a preferred approach or vendor segment.

But for now what the profession has settled on is the expectation that spending will increase. The latest Gartner Supply Chain Technology User Wants and Needs Survey shows that supply chain leaders highlighted a concentrated intent to increase spending (see Figure 2).

Figure 2: Year-Over-Year Changes in Supply Chain Cybersecurity Spending

n = 352 supply chain professionals, excluding don’t know
Q: How do you anticipate your organization’s supply chain cybersecurity spending to change year over year?
Source: 2021 Gartner Supply Chain Technology User Wants and Needs (UWaN) Survey
Our Thriving Amid Heightened Complexities Survey data shows that 63% of respondents have budgets for supply chain cybersecurity sitting with IT or information security, and only 23% sitting with some variation of the supply chain team. This is all the more reason for the supply chain to work with IT, which holds the funding, at least for now. We recommend that supply chain pushes to increase their ownership of the budget on cybersecurity spend for supply chain because it’s such a significant risk to their operations.

But companies are also looking for technology to do more than just help them verify and alert. Leaders we spoke to expressed a desire to move from response and recovery after a known threat to continuous and predictive threat monitoring. They also want to take cyber-risk mitigation deeper into their supply chain operations. For example, one consumer products company told us it is piloting an application programming interface between its supply chain risk management solution and its planning solution. This API will enable the company to switch entire planning cycles based on cyberthreats that are detected with its suppliers or contract manufacturing partners.
Searching for Cybersecurity Talent

Competition for talent in cybersecurity is fierce, and made worse when looking at the intersection with supply chain expertise.

In the Gartner 2020 Supply Chain Technology User Wants and Needs Survey, respondents identified the most important technology-related skills and competencies that will be needed in the supply chain organization over the next five years. As shown in Figure 3, the top skill set expected to be needed is “Cybersecurity Experts” (with 71% indicating an importance level of 6 or 7 on a seven-point scale).

Supply chain organizations use a range of strategies for staffing supply-chain-related cybersecurity roles. It typically starts with external consultants and transitions to building an in-house team, commensurate with the underlying level of risk. Cybersecurity talent often comes from outside the business (e.g., former government/military or security specialists). Like other highly technical roles (e.g., data scientists), these employees need grounding in the business and in the supply chain contexts to build proper defenses.

Figure 3: Cybersecurity and AI Experts Considered Most Important Future Roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Bottom 2 Box (1, 2)</th>
<th>Middle 3 Box (3, 4, 5)</th>
<th>Top 2 Box (6, 7)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity Experts (n = 519)</td>
<td>1%</td>
<td>29%</td>
<td>71%</td>
</tr>
<tr>
<td>Artificial Intelligence Experts (n = 519)</td>
<td>2%</td>
<td>31%</td>
<td>67%</td>
</tr>
<tr>
<td>Technology Leaders/Digital Architects (n = 514)</td>
<td>0.2%</td>
<td>35%</td>
<td>65%</td>
</tr>
<tr>
<td>Automation/Robotic/Material Handling Engineers (n = 516)</td>
<td>1%</td>
<td>34%</td>
<td>65%</td>
</tr>
<tr>
<td>Operations Research Specialists (n = 518)</td>
<td>1%</td>
<td>36%</td>
<td>64%</td>
</tr>
<tr>
<td>Modeling and Simulation Experts (n = 516)</td>
<td>1%</td>
<td>37%</td>
<td>62%</td>
</tr>
<tr>
<td>Data Scientists (n = 515)</td>
<td>1%</td>
<td>37%</td>
<td>62%</td>
</tr>
</tbody>
</table>

n = varies for each role, excluding don’t know
Q: How important do you see the following roles and competencies being within your supply chain organizations over the next 5 years?
Source: 2020 Gartner Supply Chain Technology User Wants and Needs (UWaN) Survey
Note: Figures have been rounded to the nearest whole number, may not equal 100%.
Embracing, Evangelizing and Educating About Cybersecurity

Many supply chain leaders we interviewed expressed the challenges involved in doing business with smaller and less established partners — upstream and downstream — that may not have the time, resources or skill sets for proper cyber hygiene. These leaders feel that continued focus on, and evangelism about, the threats will make these smaller partners unable to continue to avoid the issue.

In the Gartner Thriving Amid Heightened Complexities Survey, it was not the head of supply chain or head of supply chain strategy or even head of supply chain risk management who were most commonly involved in the response and recovery efforts after a supply chain cyber attack. We found that 84% of the time it was the function or business unit leader within the supply chain who was involved. Gartner believes that this number is appropriate because many times the attack is impacting a specific functional area, such as sourcing or distribution. However, this is why evangelism is so important, so that these functional leaders can be educated about cyberthreats and mitigation approaches and can work to put protection in place. The CSCO needs to lead the charge — and bring the functional leaders along.

Leaders must change their thinking and stop simply hoping they don’t get hit. Cyber risk cannot ever be completely eliminated. Leaders must accept that “throwing more money” at the issue can help reduce risk, but that no amount of money can eliminate risk altogether.
Actionable, objective insight

Position your supply chain organization for success. Explore these additional complimentary resources and tools for supply chain leaders.

**Webinar**
Supply Chain Cybersecurity Webinar
Combat enterprise and ecosystem threats.

**Tool**
Supply Chain 2035 Roadmap
Explore the path toward supply chain autonomy.

**Tool**
Digital Transformation Playbook
Get the 3-step plan for supply chain digital transformation.

**Report**
Supply Chain AI Report
Explore 3 strategies for AI in supply chain.

Already a client?
Get access to even more resources in your client portal. Log In
Connect With Us

Get actionable, objective insight to deliver on your mission-critical priorities. Our expert guidance and tools enable faster, smarter decisions and stronger performance. Contact us to become a client:

**U.S.:** 1 855 811 7593

**International:** +44 (0) 3330 607 044

Learn more about Gartner for Supply Chain Leaders
gartner.com/en/supply-chain

Stay connected to the latest insights

© 2022 Gartner, Inc. and/or its affiliates. All rights reserved. CM_GBS_1956678