A Supply Chain Cybersecurity Maturity Model for 2021

Mike Kelly
CEO | ProcessBolt

Dan Gardner
COO | ProcessBolt

The SolarWinds Sunburst hack made it painfully clear that supply chain cybersecurity threats are extremely dangerous. Perhaps the most alarming fact is that SolarWinds' stock price dropped 40% in seven days after the breach became public. The price drop was not so much about SolarWinds being hacked. It reflected the anticipated damage to customer relationships and long-term company value.

The Sunburst megabreach spread in a two-step process. First, the threat actors hacked into a SolarWinds software update system and inserted malicious code into the Orion software update. Second, as SolarWinds customers downloaded and updated their Orion software, they were also infected.

Before the SolarWinds hack, companies often treated supply chain risks as secondary. They focused on protecting internal, company-managed data and systems. Now, the usefulness of distinctions like "internal" and "external" are diminished. Instead, we must think in terms of cyber risk ecosystems: Vast interconnected networks of vulnerable endpoints constantly exposed to extensive arrays of potential attack vectors.

NIST CYBERSECURITY FRAMEWORK

The importance of supply chain cyber risk was upgraded by the National Institute of Standards and Technology (NIST) in 2018 to Version 1.1. The update greatly expanded the role of Supply Chain Risk Management (SCRM) in information security. It augmented its cybersecurity ecosystem concept. And it provided an SCRM maturity model (referred to as Implementation Tiers), which described progressive levels of SCRM.

TIER 1: PARTIAL

The lowest level of SCRM in NIST's Version 1.1 is "Tier 1: Partial." It allows companies to be "generally unaware of the cyber supply chain risks." But in a post-SolarWinds world, can a company be a minimally viable business partner if they are generally unaware of supply chain cyber risks?

In 2021, enterprises must have a minimum level of engagement in SCRM. If a company is not paying attention to SCRM, it may not be a safe business partner. A base maturity level of SCRM for 2021 is:

The organization periodically gathers supplier/vendor security information through risk assessment surveys and on-site inspections. The data is warehoused and scored, and follow-up corrective actions are sometimes initiated when critical cyber threats are identified.

Activities such as conducting and participating in vendor risk surveys are now minimal requirements. They force companies to build a foundational understanding of supply chain risk. Not only does this help the company be a viable vendor, it also helps a company stay abreast of the overall cybersecurity ecosystem and how it is continually evolving. This is the new minimum standard of supply chain cybersecurity.

TIER 2: RISK INFORMED

Today, speed is critical in cybersecurity. As NIST noted in 2018: "The severity of a given vulnerability increases exponentially after it becomes publicly known." NIST and other cyber risk detection groups immediately alert companies about new cyber threats. At Tier 2, SCRM teams build systems that utilize risk detection feeds, scan vendor endpoints for potential threats, and initiate immediate responses.

The organization utilizes one or more real-time cyber threat data feeds. It automatically assesses its vendor asset inventory to identify and flag emerging risk exposures. It builds rapid response capabilities.

The second level of SCRM is real-time scanning and responding. In other words, you cannot be "risk informed" in 2021 without a real-time vendor risk sensing and response program.

TIER 3: REPEATABLE

The next significant SCRM gap to address after Tier 2 involves structure and codification. SCRM spans internal and external organizational boundaries. To make SCRM repeatable and systematic, roles and procedures across the company and its supply chain need to be formalized.

The organization formalizes SCRM roles within ERM and cybersecurity programs. Internal jobs, policies, and processes are aligned with SCRM. Vendor contracts specify cyber compliance standards, information sharing, and processes to be adopted and maintained.

At Tier 3, the company creates the management systems required to fully execute real-time SCRM across business units and functions, within its overall Enterprise Risk Management (ERM) system, and throughout its supply chain.

TIER 4: ADAPTIVE

Threat actors are continually innovating. Their existence depends on creating new and ever more devious tactics.

The major weakness of Tier 3 is the use of fixed rules and protocols to identify, assess, and respond to supply chain risks. At Tier 4, companies deploy AI and machine learning to adapt and respond in near-real-time. Now SCRM targets emerging cyber threats with an emphasis on new and sophisticated attack strategies and tactics.

The organization integrates AI and machine learning into SCRM. It actively scans multitudes of vendor endpoints, attack surfaces, and vulnerabilities. It detects subtle shifts in status and activity. It assesses and responds before or just as threats emerge.

Some ERM programs use AI to detect and respond to cyber threats across company-managed endpoints. At Tier 4, AI and machine learning are deployed to manage cyber risk across the entire cyber risk ecosystem, including all supply chain vendors.

SCRM FOR 2021

An updated SCRM Maturity Model is summarized in Figure 1 below. It builds on the NIST framework but reflects what is required in a post-SolarWinds world where highly sophisticated nation-state actors exploit vendor endpoint vulnerabilities.

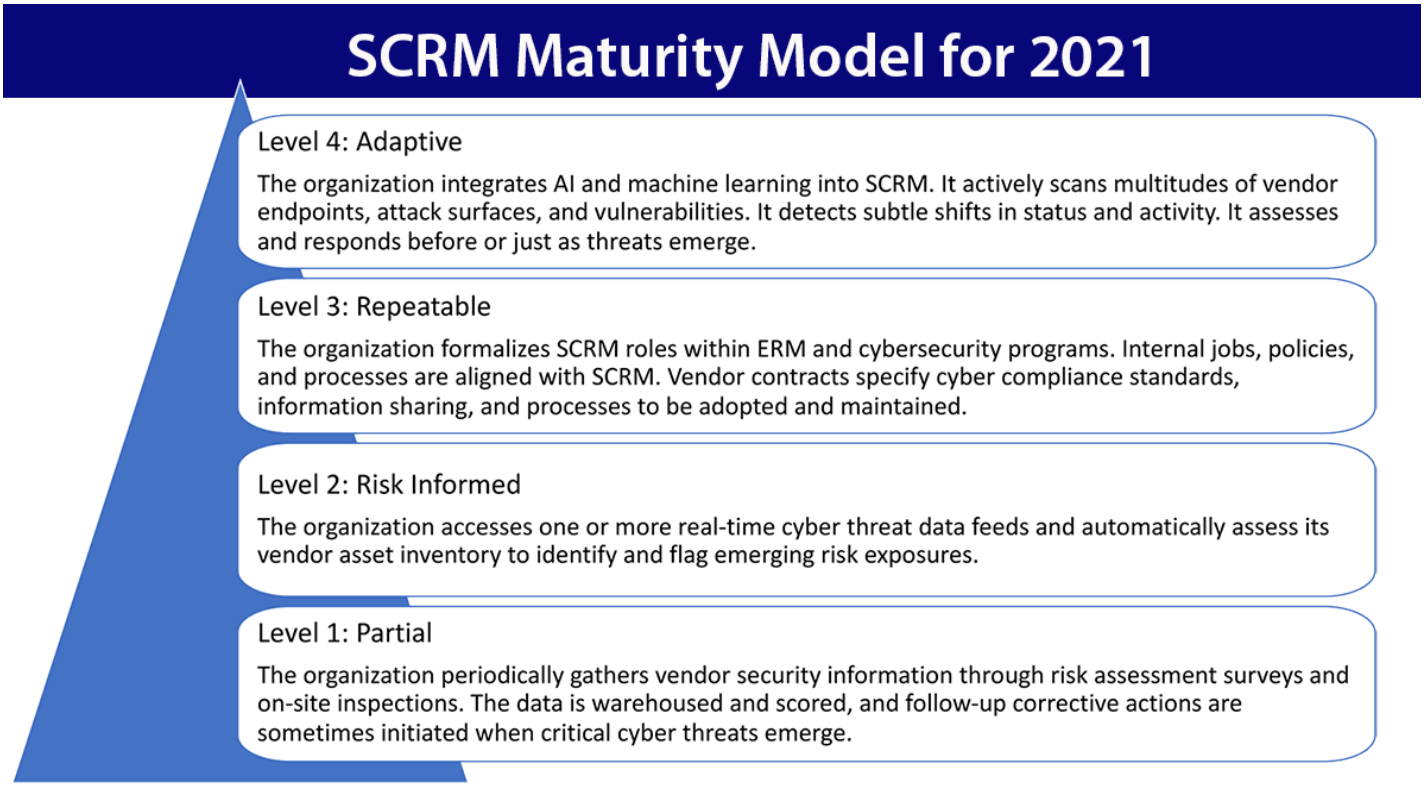

Figure 1: SCRM Maturity Model for 2021 | ProcessBolt

CONCLUSION

Maturity models have long been used in IT departments to assess capabilities and plan for improvements. NIST's Implementation Tiers were an important leap forward in 2018. Now they must be updated to reflect today's reality in a post-SolarWinds world. This will help facilitate technical conversations with business-side stakeholders, which is especially important since SCRM is now a Board and C-suite issue.

A CISO recently said they expect the number of security assessments requested by their customers to increase dramatically in the wake of SolarWinds. These assessments will likely probe how well they manage access to their network and data, whether they have another company's device on their network, and so on.

Every enterprise, large or small, is a potential target of the increasingly aggressive and sophisticated cybercriminals. The commercial risk is too significant to ignore, and the cost to begin to upgrade their SCRM program is not prohibitive.

ABOUT THE AUTHORS

Mike Kelly *is the CEO of ProcessBolt, Inc., a SaaS company that automates regulatory compliance and third-party risk assessments both for companies issuing assessments and those responding to assessments (www.processbolt.com). Prior to joining ProcessBolt, Mike led and ultimately grew and sold several software and analytics businesses in a variety of industries from healthcare to business and legal services.*

Dan Gardner *is the COO and co-founder of ProcessBolt. He has over 25 years of success in software development, IT infrastructure, cloud operations, and startups. Before founding ProcessBolt, Dan was VP of Technology at NetSPI. Prior to that, he was a founder of Renew Data Corp., a company that specialized in high volume electronic data discovery, now part of KLDiscovery (KLDI).*

ProcessBolt