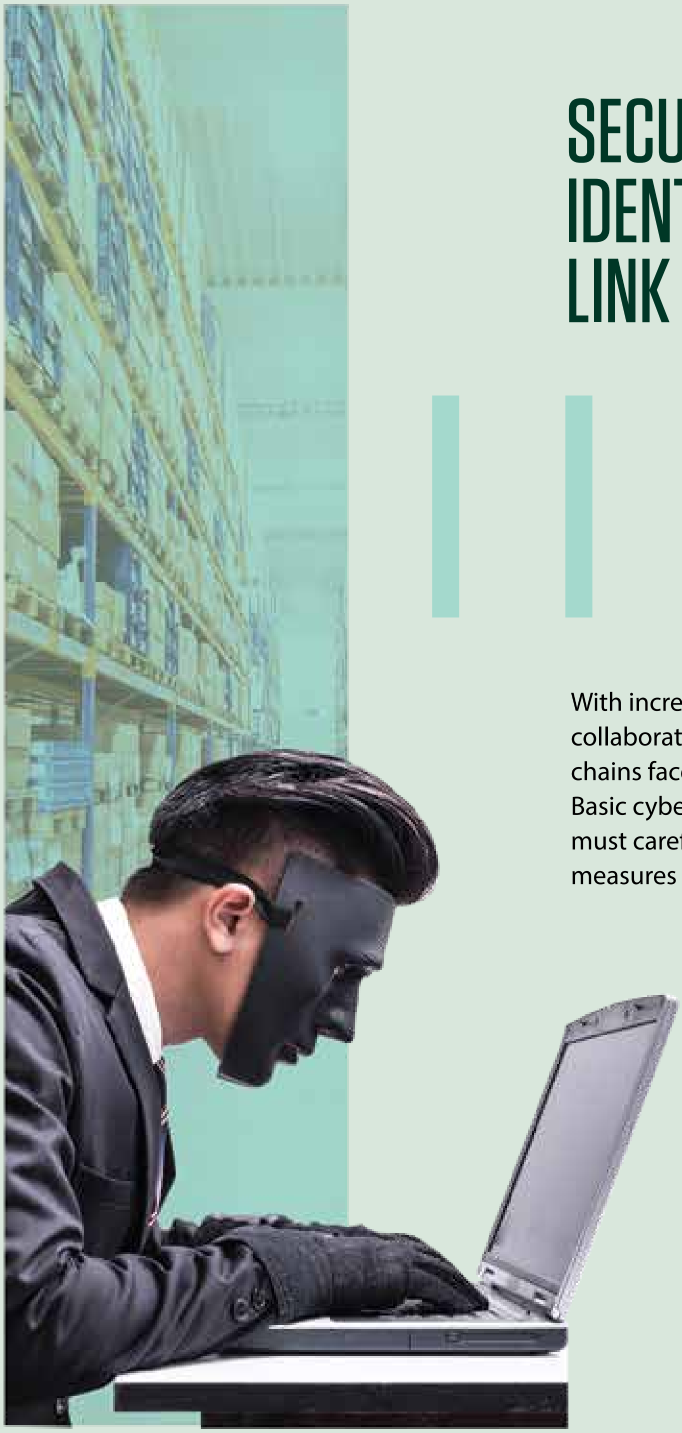
Infosys®
Navigate your next

VIEWPOINT



SECURING THE ECOSYSTEM: IDENTIFYING THE WEAKEST LINK IN YOUR SUPPLY CHAIN

With increased cloud adoption, connectivity and collaboration within business ecosystems, supply chains face a mounting threat from cybercriminals. Basic cybersecurity hygiene is no longer enough. Firms must carefully assess their partner ecosystems and take measures to ensure security and business resilience.

Infosys® | Knowledge Institute

The risk of cyberattacks has never been higher due to increased digital connectivity driven by wide-spread adoption of cloud. And attackers now have more resources and tools at their disposal. Consumer packaged goods (CPG), retail, and logistics companies are particularly attractive targets for cybercriminals. These firms hold a wealth of exploitable data, including personal information, shipping details, and consumer demographics.

An attack on any one company can have cascading effects across the ecosystem. For example, a cyberattack on Lion, an Australia-based beverage company, halted production, and other activities for almost three weeks.[1] This in turn impacted the customers and partners for many weeks.

Apart from financial and operational ramifications, cyberattacks also damage firms' reputations and the trust placed in them. Gaining back that trust could take years. This can be particularly devastating for consumer facing industries that rely on loyalty and brand.

Identify the weakest links

Eighty percent of organizations have experienced a breach due to vendor negligence or weakness, according to a 2020 survey conducted by Opinion Matters. Despite this, 77% of respondents have limited visibility into their vendors.[2]

Companies are increasingly aware that they must look beyond themselves to ensure their supply chain networks are secure. They must regularly assess the entire ecosystem to identify high-risk, vulnerable partners and take action to safeguard them.

But this isn't an easy task since CPG, retail, and logistics firms navigate hundreds of direct and indirect partners and vendors, from production to distribution. Strict rules and coordination can help them build a stronger ecosystem.

Data sharing and high connectedness among partners provides easier paths for hackers. They can invade larger organizations through unsuspecting businesses that might not have the right awareness or resources to shield themselves from cyberattacks. New-age attacks include post-exploitation actions such as impersonating normal update traffic, additional payload transfers, or credential harvesting that are hard to detect. The attacks could also potentially move to cloud-hosted infrastructure systems having a wide impact on the organization. "In the supply chain network, larger partners are relatively more secure. It is the smaller ones that are more vulnerable and need to be supported," said the chief information security officer (CISO) of a large beverage manufacturer.

> While there can be multiple cyberattack entry points, a practical approach is to prioritize the security of the most vulnerable companies

Firms must regularly assess their own security posture and that of their supply chain partners. Some CISOs suggest three or four audits every year to ensure that organizations stay ahead of constantly evolving cyberthreats. And with more factories, devices, and sensors connected to the internet, operational security needs to be as important as information technology security.

Once organizations assess and identify their risks, they must develop effective strategies to close those vulnerabilities. That's often a daunting effort. CPG companies have thousands of vendors and partners spread around the globe, including ingredients suppliers, subcontracted manufacturers, packaging material suppliers, and distributors. It can be time-consuming and expensive to secure all of them at once.

A more practical approach, according to one CISO of a leading FMCG company, is to prioritize security of the most vulnerable of these companies in the network. "You cannot boil the ocean. You need to identify the high-risk links and secure them first," the CISO said.

Establish checks and balances to manage risk across the ecosystem

To effectively protect an ecosystem, companies need to establish rules to evaluate the security control measures and practices of supply chain partners and vendors before onboarding. Security requirements can be made a part of contracts with third-party providers for software, hardware and services to explicitly demand that the providers have a commitment to securing their own environments. Vendors must be mandated to practice third-party static code analysis, regular security scanning of local and cloud-based environments, DevSecOps and integrity check of codes. Further security risks are also posed by the vendor's additional tier of suppliers, which are often invisible to others in the network.

Organizations can use a tiering system to classify these partners into different risk categories based on their profiles. This helps companies decide the level of engagement they can have with the vendors and partners without a risk of security breaches.

Many firms use questionnaires and surveys to get a sense of partner and vendor preparedness. But on their own, these are not enough. Even firms with high assessment scores on paper can be noncompliant in practice. Firms must regularly inspect vendors to ensure the right security protocols are followed and address the gaps.

Doing this is surely a demanding exercise. Most organizations still use spreadsheets to monitor their cybersecurity metrics, making this process tedious and unreliable.[3] The problem compounds when there are a large number of vendors and each has its own approach to monitoring security. Ultimately, there is no clarity on an organization's overall risk position. A platform that provides a holistic view of the security landscape and manages security metrics across the supply chain can help identify and prioritize key areas that need immediate attention.[4]

Security does not stop at protecting the digital systems. Many times, vulnerabilities like unauthorized access can threaten the security of the firms. So, businesses must do a comprehensive evaluation of security posture.

> A cloud-based platform offers a holistic security view while managing security metrics across the supply chain to help identify and prioritize areas requiring immediate attention

To deliver the fastest results, some firms are tempted to adopt cheaper, less secure software. However, this can put the entire community at risk. Companies should consider a cloud-based supply chain software to achieve scalability and elasticity. Subscription-based model makes it affordable for smaller companies. With automation, it brings speed in decision-making and enhances efficiency. At times, human errors — even as simple as sharing passwords — can expose the firms to cyberattacks and potentially stall operations. Such issues can be mitigated by creating awareness and training people on security.

Participants of the supply chain must build transparent and responsive cultures where firms speak out when they're vulnerable. Instead of fearing a loss of reputation, firms with this mindset can foster trust and build resilience. This threat sharing and collaboration can help mitigate the impact of any transgressions.

United, the supply chain is stronger

Closely knit global supply chains are both valuable and vulnerable. Cyberattacks will likely increase as more companies move to the cloud; collect and share more data; and connect more devices to digital networks.

Every firm has its own way of handling cybersecurity. But measures taken in silos are not a foolproof way to defend from threats. All the stakeholders in a supply chain must work together, share information, and oversee and guide each other in order to secure the ecosystem.

Of course, breaches are inevitable even with the best defenses. But coordinated efforts from all stakeholders in the supply chain can help identify, mitigate, and recover from an attack much faster.

References

1. Lion attack puts spotlight on cybersecurity, Jul 02 2020, BrewNews,com
2. Maria Korolov, "Supply chain attacks show why you should be wary of third-party providers", Feb 04, 2021, CSO
3. "Cybersecurity – safeguarding your digital journey", 2020, Infosys
4. "Cyber Gaze – A tool by a CISO for a CISO", Infosys

Authors

Harish Bangalore

Regional Director, Cyber Security Services – East Americas, Infosys
bangalore_harish@infosys.com

Rachana Hasyagar

Infosys Knowledge Institute
rachana.hasyagar@infosys.com

About Infosys Knowledge Institute

The Infosys Knowledge Institute helps industry leaders develop a deeper understanding of business and technology trends through compelling thought leadership. Our researchers and subject matter experts provide a fact base that aids decision making on critical business and technology issues.
To view our research, visit Infosys Knowledge Institute at infosys.com/IKI

For more information, contact askus@infosys.com

Infosys®
Navigate your next