Strengthen the Chain: Integrative supply chain Cybersecurity risk insights

Collaborate with Confidence

KPMG in Qatar
January 2024

Navigating Cybersecurity Supply Chain Risks in Fast-changing World

Understanding What's at Stake

In a fast-paced world and extensive emerging technology adoption, organizations across various sectors (i.e. Technology, Finance, Telco, O&G, Government, etc.), are increasingly reliant on an ecosystem of suppliers to provide products and services such as software, hardware, legal, advisory and more to fulfill their missions in a cost-effective, timely and efficient manner.

This intricate inter-dependence does not only exist within organizations, but extends to the suppliers themselves as operating entities. Managing cybersecurity supply chain risks has become an imperative to empower secure, resilient and trusted operation for organizations.

Cybersecurity supply chain risk materializes when one of the suppliers used by an organization experiences a security incident that consequently result in a breach to the data they are retaining, or processing on your-behalf, or renders the services they provide unavailable or insecure. Such a compromise could be attributed to third-party supplier access to your systems or data within your organization, use of their applications or software components. Therefore, such a breach might not be necessarily confined to data breach but could also lead to operational, health and safety, brand, financial or regulatory compliance impacts on your organization mission.

In the past 2 years, a startling 53% of organizations experienced one or more cyber breaches attributed to 3rd party suppliers costing an average of $7.5M to remediate. Also, In 2022, 63 attacks on vendors caused third party breaches: from those 63 attacks, 298 data breaches occurred across impacted companies[1].

Cybersecurity supply chain breaches to products (including software, hardware), services continue to impact many organizations as a single point of failure (i.e. due to dependence on single core suppliers) as witnessed over the past few years with key cybersecurity supply chain breaches (i.e. MOVEit, 3CX, Log4J, etc).

The Solarwinds breach was a rude awakening in 2020 and impacted government, Big Tech, Services, and other sectors bringing more focus on supply chain risk.

Since then, threat actors relentlessly continued to intensify their attacks against supply chain organizations (third-party suppliers) due to its lucrative ROI for cyber-criminal syndicates and state-sponsored threat actors.

More recently, in January 2024 Microsoft security team detected a Russian nation-state attack on corporate systems. This attack has led to unauthorized access to emails accounts including senior members and leadership teams and employees. The same threat-actor is expected to be behind the subsequent breach with HPE announced later in January 2024. This is a true reflection of the on-going intensity of cybersecurity attacks associated with supply chain.

[1] BlackKite 2023 – Third Party Breach Report.

Understanding What's at Stake

The cost of such cyber supply chain breaches is predicted to reach a startling $138 billion by 2031[2]. This projected loss is only attributed to software-related breaches within supply chain.

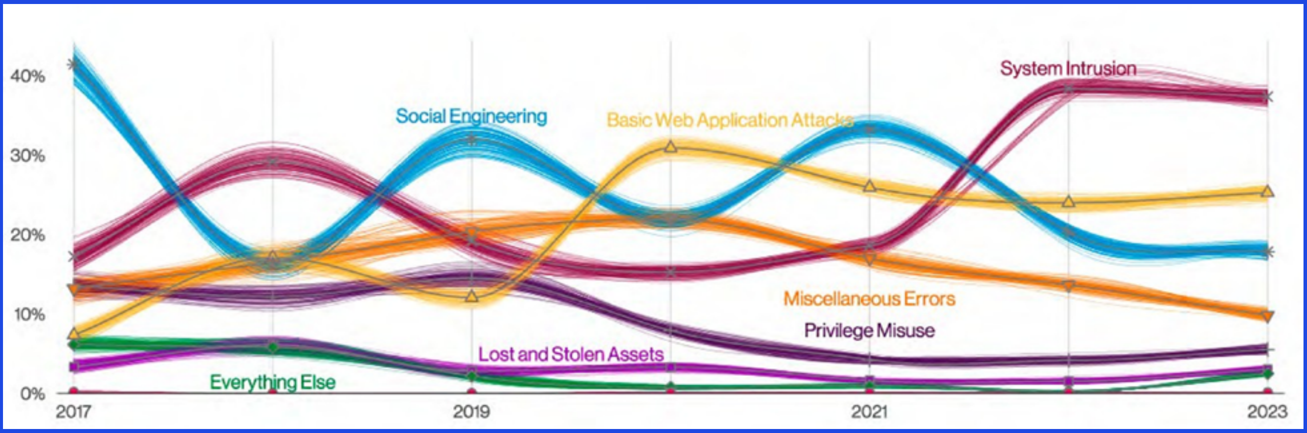
Whilst boards and senior leadership teams rely on existing enterprise risk management frameworks and practices to gain assurance over their supply chain risk exposure, cyber- attacks have gained significant momentum and made headlines over the past few years. Which brought the question to the boards as to whether organizations are doing enough to manage their cybersecurity supply chain risk, including the extended landscape due to increased cloud adoption.

[2] Cybersecurity Ventures 2023 Software Supply Chain Attack Report

Understanding What's at Stake

Common Patterns Revealed

Basic Web Application Attacks	These attacks are against a Web application, and after the initial compromise, they do not have a large number of additional Actions. It is the "get in, get the data and get out" pattern.
Denial of Service	These attacks are intended to compromise the availability of networks and systems. This includes both network and application layer attacks.
Lost and Stolen Assets	Incidents where an information asset went missing, whether through misplacement or malice, are grouped into this pattern.
Miscellaneous Errors	Incidents where unintentional actions directly compromised a security attribute of an information asset fall into this pattern. This does not include lost devices, which are grouped with theft instead.
Privilege Misuse	These incidents are predominantly driven by unapproved or malicious use of legitimate privileges.
Social Engineering	This attack involves the psychological compromise of a person that alters their behavior into taking an action or breaching confidentiality.
System Intrusion	These are complex attacks that leverage malware and/or hacking to achieve their objectives, including deploying Ransomware.
Everything Else	This "pattern" isn't really a pattern at all. Instead, it covers all incidents that don't fit within the orderly confines of the other patterns. Like that container where you keep all the cables for electronics you don't own anymore: Just in case.



Patterns over time in breaches[3]

[3] Verizon 2023 Data Breach Investigations Report

Bridging the chasm in Cybersecurity Supply Chain Risk Management

Dealing with cybersecurity supply chain risk management is a team sport that requires a shift-left (Secure-By-Design) paradigm where all cross-functional stakeholders (CEO, CIO, CISO, CFO, CPO, Procurement, SMEs, etc.) appropriately contribute and are accountable to the organization, mission/ business Process and operational risk levels.

Building appropriate practices involves unwavering leadership commitment to support investment in governance, people, and technology to streamline and integrate within the overall integrated enterprise risk management framework.

Furthermore, managing cybersecurity supply chain risks cannot be reactive response to findings or remain at a risk monitoring level. Active visibility of key metrics, risk tolerances and effective controls where the organization systematically takes charge of its cybersecurity supply chain risks to bring them within its acceptable risk appetite. Whilst some organizations have mature risk culture, trying to establish cybersecurity supply chain risk management in a low-maturity risk culture poses significant challenges and requires solid leadership support and change programs across the enterprise.

Did Somebody Say AI?

With the ever-increasing adoption of Artificial Intelligence and Generative AI, businesses have flocked with a bigger risk appetite than ever to leverage AI to achieve competitive business advantages such as cost-cutting, faster innovation, reduce go-to-market time and lower product development costs. AI plug-ins, usage scenarios and integrations whether leveraging AI cloud-based or on-premise providers pose a number of cyber security supply chain risks that might be left unaddressed, with control implementations lagging due to a slower implementation pace.

In early 2023 OpenAI's ChatGPT, which exposed the payment-related and other sensitive information of 1.2% of its ChatGPT Plus subscribers due to a bug in an open-source library it used[4].

Cyber criminals are keen on exploiting AI prompt-engineering and other vulnerabilities to exploit organizations (i.e. Biometric scraping, steal trade secrets, leak sensitive information, etc.) which continue to be some of the emerging challenges, where cybersecurity risk management needs to exhibit agility.

It might sound like mission-impossible, but more mature organizations with strong risk culture continue to leverage emerging technologies and innovate with cybersecurity guard-rails within their engineering and product development practices whilst leverage agile governance models to their advantage. Clear articulation AI policy, decision-rights and mixture of centralized and de-centralized risk governance are some of the key enablers for sound cybersecurity supply chain risk management organizational enablers.

One Size Doesn't Fit All!

Managing supply chain cybersecurity risks at-scale for multinational and multi-disciplinary organizations needs to take into account jurisdiction-specific considerations (i.e. privacy laws, Federal/State- specific considerations, concentration risks, embargos, etc.)

Having a full end-to-end visibility of supply chain from a cyber risk perspective starts with legal, privacy and procurement teams collaborating with the CRO, CIO and CISO to establish well-defined requirements, including cyber security clauses within contracts (i.e. expected controls, incident reporting, etc.), surveys, supplier categorization, and working with cyber security certified suppliers (i.e.ISO27001, SOC2, HIPAA, etc.)

This is not a one-off thing, it requires a continuous cyber assurance program that favors early detection and monitors the cyber posture of critical suppliers and considers the impacts of M&A, Divestments, etc within suppliers. It needs to both build internal and external (i.e. disseminate/gather industry-based) insights and report clearly to senior leadership and boards on the state of cyber security supply chain risk posture and compliance through effective metrics and KRIs.

[4] https://www.cmswire.com/digital-experience/chatgpt-suffers-first-data-breach-exposes-personal-information/

Bridging the chasm in Cybersecurity Supply Chain Risk Management

Where to go from here?

Organizations need to know their current state and where they stand today within their risk transformation journey, articulate clear risk appetite statement, risk tolerances, and ensure that they manage cybersecurity risk as an operational risk in an integrated manner. Long gone the days where cybersecurity is an IT or security department problem, it is a business problem and ownership must be with senior leaders and boards as with any other operational business risk.

Structuring and enabling an integrated risk-prioritized cybersecurity supply chain management program is essential. Governance must be supported with appropriate change management program to empower key transformations across, people, process and technology.

Lastly, placing the cybersecurity terms in agreements with suppliers and inclusion of incident response clauses are integral part of any cybersecurity supply chain risk. Data lifecycle visibility is crucial along with proper the application of data security controls (i.e. DevSecOps, Data Discovery and Classification, Data Minimization/Retention, MFA, Encryption, Static/ Dynamic Data Masking, DLP, etc.) to reduce organizational cybersecurity supply chain exposure footprint.

Contact us

KPMG in Qatar
25, C Ring Rd, Doha
Qatar

Nizar Hneini
Partner, Head of Digital & Innovation

T: +974-44576444
E: nhneini@kpmg.com

Sofiane El Abdi
Partner, Advisory

T: +974-44576444
E: selabdi@kpmg.com

Marwan Zalloum
Director, Advisory

T: +974-44576444
E: mzalloum@kpmg.com

kpmg.com/qa

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.