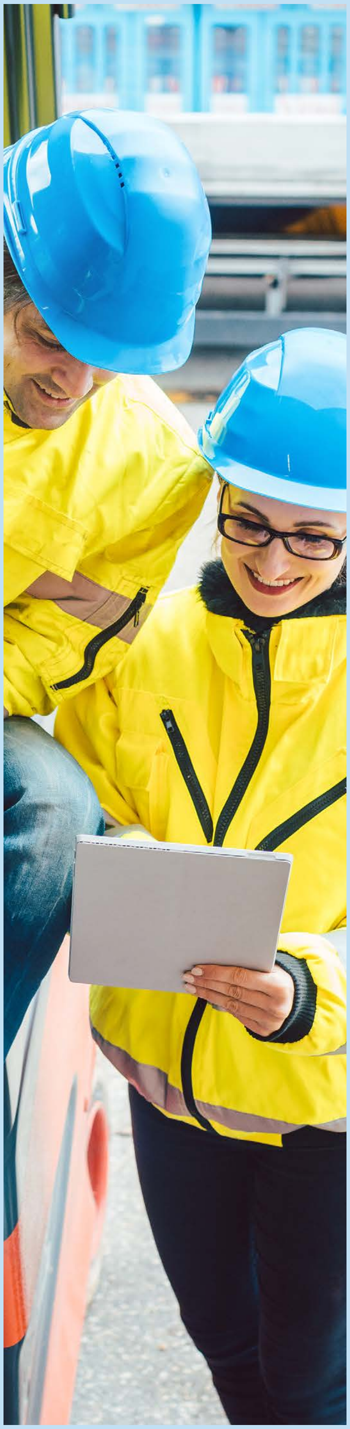
VIEW POINT



SECURE PROCUREMENT: THE KEY TO ENSURING ORGANISATIONAL STABILITY AND GROWTH

Abstract

Procurement and supply chain processes can be quite dynamic and complex, increasingly so with digitalisation. The rising interconnectedness with third-party providers leads to a corresponding deepening vulnerability to cyber-attacks across the procurement function. Cybercrimes can occur through software, hardware, service providers, system access, and authentication weaknesses. Organisations must take robust and ongoing measures to prevent, detect, and remediate breaches within their infrastructure and third-party supplier systems. Regular audits, personnel training, and a comprehensive cyber-security protocol for the parent organisation and all third-party suppliers are imperative. Using AI tools to prevent potential breaches, detect intrusions at the earliest, and speed up recovery, helps organisations minimise attacks and the fallout of any attacks that could not be stopped.

Infosys®
Navigate your next

Introduction

Most organisations have a range of suppliers for products, systems, and services. Consequently, the procurement workflows can be complex, involving multiple data interfaces and exchanges. Procurement function data is highly sensitive, with payment information like credit cards and bank account details, contact data, and confidential data like bids, contracts, and agreements. Additionally, the digitalisation of the supply chain with IoT, automation, and AI-based advanced analytics has led to a surge in data that enables the supply chain to be streamlined and delivers real-time visibility across the procurement network. This optimisation is achieved only through integrating disparate systems, which involves third-party technology partnerships across the cloud, data management, hardware, and software.

This rising interconnectedness creates a complex web of digital dependencies, leading to an increase in the vulnerability of the procurement system to cyber-attacks. Weaknesses can be inherent or introduced at many possible points in the supply chain, leaving it open to exploitation, damage, and disruption. The fallouts of a supply chain attack are far-reaching and grave: disruption of operations, critical data leaks, erosion of customer and stakeholder trust, and loss of customer base.

Some examples of potential areas for supply chain attacks are third-party software providers, website builders, third-party data stores, and watering hole attacks. Cyber-espionage groups attack software providers and introduce malware into legitimate supply chain software. Unsuspecting customers download the compromised application, which then disrupts operations or steals data from their systems. Software tampered with at source is next to impossible to detect, and reliance on the supplier is absolute. Inspecting every hardware piece or download thoroughly enough to prevent such a scenario is not feasible. Website builders used by digital and creative agencies to develop customer websites can be targeted using redirect scripts to send users to malicious domains. These malicious domains can then install malware into the user systems. This type of attack allows maximum reach with minimal effort.

Third-party data stores run by data aggregators, if attacked using bots or by other means, could put at risk valuable information regarding business structure, financial health, strategy, and risk exposure. IoT sensor networks are now essential parts of procurement infrastructures. Spoofing, denial of service, elevation of privileges, physical access, and unauthorised code executions are some common threats supply chain IoT systems face. In watering hole attacks, a frequently visited website like a procurement conference or industry standard body will be infected using malicious code. Users' systems will then be infected with malware and remotely accessed. Other general cyber-attacks like phishing, SQL injection, zero-day exploits, and business email compromise can prove extremely damaging for the procurement function due to the sensitivity of data and the implications for the business.

A plan to identify, respond to, and recover from a breach is vital. Recognising the critical business risk factors within third-party contracts, ensuring adherence to a comprehensive cyber-security protocol, and training of all personnel is a must.

Analysis of Possible Threats: A comprehensive threat analysis strategy to build a broader picture of the threats can help enrich the internal security data. A thorough understanding of critical systems and data and marking the gaps in visibility over the supply chain is essential. This profiling will help spot potential threats and vulnerabilities. Simulation exercises using the intelligence derived from threat analyses and system profiling can fortify defences and response plans.

Security Assessment: Organisations should conduct detailed third-party risk assessments covering technical security controls, governance, risk, and compliance processes. Each supplier's maturity levels and gaps should be assessed as an ongoing audit process. Such a detailed appraisal is essential to implement the checks and procedures required for quick and effective responses to supply chain security breaches. The procurement function and IT security should hold responsibility.

System Access by Supply Chain Partners: System access and authentication controls are prime targets for cyber-attacks. Suppliers' level of access to an organisation's environment should be constantly monitored, and access provision should follow the principle of least privilege. Managed service provider (MSP) accounts should have only the necessary rights and follow organisational directives in password creation, and these accounts should be monitored and disabled when not needed. If the MSPs providing critical IT operations also provide cyber-security breach responses, then there is bound to be a conflict of interest. A level of separation is necessary to prevent cover-ups and uphold security.

Log, Review, and Analyse Supplier Activity: A baseline of normal activities should be created for all suppliers, facilitating tracking and detection of any divergent activity. Logging, regular review, and analysis of supplier activity will help in quick detection. Managed detection and response services elevate threat detection capabilities by integrating contextualised threat intelligence, behavioural analytics, proactive threat hunting, and remote response.

Response Plan: The incident management protocol should address readiness, response, and recovery at an organisational level and be regularly reviewed and updated. A supply chain cyber-attack requires swift assessment, containment, and straightforward communication with regulators and stakeholders. The response plan should include a business response process and communication plan and ensure all cyber-insurance requirements are fulfilled. Additionally, it should ensure regulatory compliance, systems, business, and data recovery.

AI and analytics can play an important role in the above steps to secure the supply chain. AI-enabled analyses of phishing risk, sourcing risk, and files and documents can reduce the prospect of cyber-attacks. AI-enabled Security Information and Event Management (SIEM) systems use algorithms to collect and correlate data from multiple sources, including network logs, firewall logs, and intrusion detection systems, to analyse and categorise security incidents in real-time. The derived insights help ML-powered SIEM systems to spot patterns and anomalies representative of cyber threats, allowing a quick and effective response. If a SIEM system detects a pattern resembling a distributed denial-of-service attack, it can set off an automated counter measure to block the malicious traffic, preventing service breakdowns. AI can launch preset actions as part of the remediation process based on incident classification and severity, speeding up the recovery process and reducing manual intervention. An AI-based endpoint protection solution can detect an infected workstation and automatically isolate the impacted device from the network, preventing further spread by confining the damage.

Cyber-attacks on supply chains are a grim reality in today's digital business world. Ensuring that the right people, processes, and technologies are deployed to identify, prevent, manage, and remediate is critical.

* For organizations on the digital transformation journey, agility is key in responding to a rapidly changing technology and business landscape. Now more than ever, it is crucial to deliver and exceed on organizational expectations with a robust digital mindset backed by innovation. Enabling businesses to sense, learn, respond, and evolve like a living organism, will be imperative for business excellence going forward. A comprehensive, yet modular suite of services is doing exactly that. Equipping organizations with intuitive decision-making automatically at scale, actionable insights based on real-time solutions, anytime/anywhere experience, and in-depth data visibility across functions leading to hyper-productivity, Live Enterprise is building connected organizations that are innovating collaboratively for the future.

For more information, contact infosysbpm@infosys.com

Infosys®
Navigate your next

Infosysbpm.com

Stay Connected