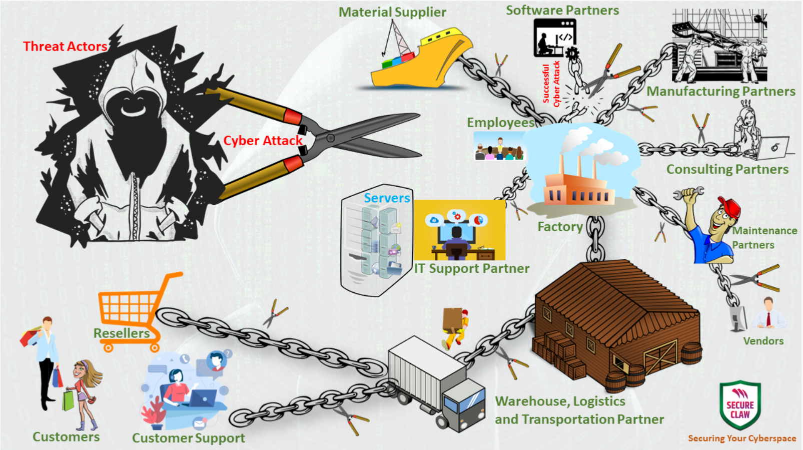
EINPRESSWIRE

The BDSLCCI Cybersecurity Framework prevents Supply Chain Attacks securing Small and Medium Businesses (SMBs / SMEs)

Business Domain Specific Least Cybersecurity Controls Implementation (BDSLCCI) provides a better security posture, protecting the company's important assets.

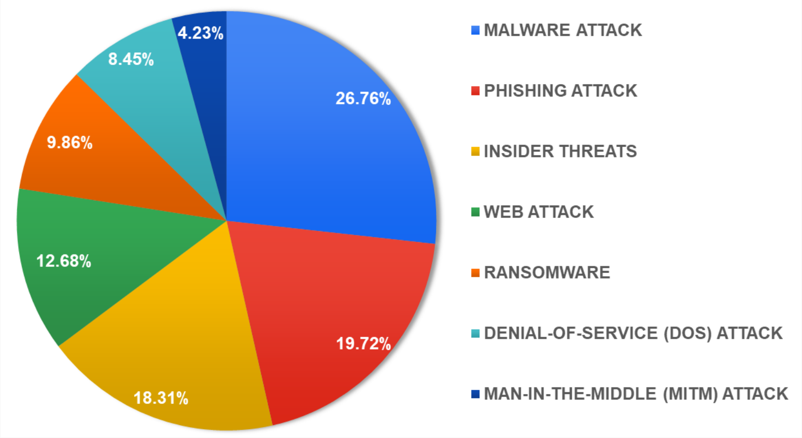


Typical Supply Chain Cyber Attack Illustration

DOVER, DELAWARE, UNITED STATES, October 30, 2023 /EINPresswire.com/ -- In the last few years, many businesses globally have been facing various sophisticated cyber threats. While most companies have invested in cybersecurity for months and years, cybercriminals still have plenty of avenues to exploit, such as supply chain attacks. A supply chain attack occurs when an intruder gains access to organization’s systems and data and utilizes them to compromise organization’s digital infrastructure. The attacker just needs to breach the defenses of the third party or program a vulnerability into a vendor-provided solution in order to gain access to organization’s system because the outside party has been given permission to use and manipulate specific portions of organization’s network, various applications, or sensitive data. Open-source supply chains, foreign products, and commercial software are some of the most common sources of supply chain attacks. A cyberattack against a company's software or service providers within its digital supply chain is widely known as a "software supply chain attack". These threats' primary goal is to penetrate inside the target organization by taking advantage of weaknesses in the suppliers' or vendors' systems. This gives cybercriminals the ability to access resources and sensitive data without authorization, interfere with business processes, or damage the organization's reputation.

> “
> BDSLCCI cybersecurity framework is playing an important role in securing supply chains made by small and medium companies (SMBs/SMEs) and helping to gain more trust in the market, hence more business.”
>
> *Dr. Shekhar Pawar, CEO, SecureClaw Inc., Inventor of BDSLCCI*

A branch of supply chain management known as supply chain security deals with the risks provided by outside vendors, suppliers, resellers, logistics companies, and transportation. As authored by Dr. Shekhar Pawar in a recent white paper published by the EC-Council, United States, with the title [“Cloud Security: A Comprehensive Survey of Challenges and Trends”](), even gaps in configurations or access controls can pose big threats to organizations that have several vendors in their supply chain.



Various Cyber Threats Faced by SMB or SME companies. Refer research paper - LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs)

Business Domain Specific Least Cybersecurity Controls Implementation (BDSLCCI) Logo

Attacks against several clients resulted from the supply chain breach of 3CX, a vendor of VoIP phone systems that is extensively used, in March 2023. Originally a provider of PBX software, 3CX is nowadays offering collaboration, video, and voice solutions. The same hackers who breached 3CX also stolen an application from Trading Technologies, a financial software company, and used that to gain access to a PC belonging to a 3CX employee. It is commonly assumed that the hacker organization, also going by the names Kimsuky, Emerald Sleet, or Velvet Chollima, is operating on behalf of the North Korean regime.

Another popular ransomware attack affecting Apple supplier Quanta Computer is an eye-catching, high-profile supply chain attack. Following the theft of an enormous number of engineering and production schematics for both existing and upcoming products from Quanta, a Taiwan-based company that produces MacBooks and other products for Apple, Apple has become the subject of a $50 million ransomware attack.

Since 2020, an additional, incredibly complex cyberattack was operating using a commercial version of SolarWinds software. The supply chain of SolarWinds was found to have been breached by advanced persistent threat (APT) attackers who had added a backdoor to the program. At least nine federal agencies and over 100 corporations were compromised in the December 2020 SolarWinds supply chain attack, which gave hackers access to up to 18,000 government organizations and Fortune 500 companies.

Apart from these supply chain attacks, now researchers discover that threat actors can use "AI package hallucinations" to generate malicious code packages that ChatGPT recommends. Developers may download these packages unintentionally while utilizing the chatbot, incorporating them into software that is subsequently widely used. This poses a serious risk to the software supply chain. As cybercriminals employ supply chain assaults and data exfiltration to increase their advantage, ransomware instances are on the rise once more.

As an organization that will be outsourcing or using the services of any SMB, has it been checked whether that SMB as a sub-contractor is cyber-secured?

If SMB is willing to get more business from other organizations, is it time to check if it is cyber-secured?

Any SMB can check how the BDSLCCI cybersecurity framework can serve it with a less resource-consuming and business-domain-specific tailored cybersecurity control implementation.

Dr. Shekhar Pawar's research study revealed several key problems preventing SMBs from setting up a strong cybersecurity posture. SMBs need to adhere to the very minimum as well as comprehensive cybersecurity requirements in order to prevent being attacked. A few schools of practical thought could help SMBs rapidly fix their current problems. Any SMB can prioritize the adoption of controls based on the areas indicated in this research, as compared to deploying cybersecurity measures randomly or none altogether. The primary topics are listed below to conclude the offerings.

(1) Calculate the mission critical asset (MCA) for the SMB's domain;
(2) Put the SMB's domain-specific security needs into practice while taking into account all relevant criteria mentioned;
(3) The entire SMB should use must-have minimum baseline controls;
(4) Determine the level of BDSLCCI; and
(5) Continue raising organization’s level of BDSLCCI.

BDSLCCI Level 1 offers SMBs efficient cyber-threat protection, mitigating ransomware attacks, phishing scams, ransomware, online attacks, and insider threats to some degree. Moreover, BDSLCCI Level 2 offers stronger cybersecurity protection than Level 1. SMBs would be best served by implementing Level 3 of the BDSLCCI as the minimum cybersecurity control. SMBs can choose an additional MCA that is essential to their goal and keep establishing controls for each one. Since more than a year, BDSLCCI implementation has improved the cybersecurity posture of various SMB or SME companies worldwide. BDSLCCI is now available as an AI-ML-based web portal, where SMB companies can get a view of the cybersecurity controls they need to implement. Also, without any cost, today BDSLCCI provides various essential cybersecurity policies protecting various layers of the organization, vulnerability gap analysis and monitoring tools, a daily cyber threat alert email notification service, cybersecurity awareness posters, etc.

If SMB implements BDSLCCI recommended controls and further undergoes its audit or assessment online or offline, as the final deliverable, it receives a BDSLCCI certificate displaying the level achieved, a BDSLCCI transcript, and a BDSLCCI implemented control’s effectiveness and coverage web analytics report.

BDSLCCI implementation certificates and reports help SMBs gain more confidence as a cyber-protected service provider in the market, resulting in more business opportunities.

Dr. Shekhar Pawar
SecureClaw Inc.
+1 218-718-2121
customercare@secureclaw.com
Visit us on social media:
Facebook
Twitter
LinkedIn
Instagram
YouTube
Other

This press release can be viewed online at: https://www.einpresswire.com/article/664916108