Trustwave

Ecosystem of Risk

Understanding the cybersecurity challenges of the modern supply chain

Amidst digital transformation and geopolitical instability, the supply chain is more vulnerable than it's ever been.

Cybercrime cost U.S. businesses more than $6.9 billion in 2021, and only 43% of businesses feel financially prepared to face a cyber-attack in 2022.

The Most Prominent Supply Chain Attacks Since 2020

Colonial Pipeline

Paid over $4M in ransom ($2.3M recovered). U.S. gas prices increased by 20% over the previous week, pushing the national average over $3/gallon[2]

Solarwinds

More than 18,000 customers and 9 U.S. government agencies, with a price tag of about $1B ($12M on average per company)[1]

Log4j

Impacted over 3 billion devises (including mobile) worldwide[4]

Kaseya

Zero-day attack that hit more than 1500 companies in 17 countries with more than 1 million devices and cost millions of dollars in lost revenue[3]

Understanding the Supplier Risk Landscape

650%
In the last **5 years**, software supply chain attacks have increased **650%** [5]

11 seconds
This year, there will be an estimated ransomware attack every **11 seconds** [7]

$812k
An average ransomware payout was **$812k**, a **500%** Y0Y increase from **$170k** [6]

70%
Nearly **70%** of midsize organizations were hit by ransomware in **2021**, double that of **2020** [8]

$4M
The average cost of a data breach rose to over $4M – the highest in 17 years[9]

Taking the Path of Least Resistance

Why are Attackers Increasingly Targeting Suppliers?

- Access to Hundreds of Thousands of Secondary Targets
- Large-scale disruption of critical infrastructure or operations
- Bypassing traditional security controls

A Perfect Storm

How Did We Get Here?

The Rush Towards Digital Transformation: 82% of businesses have experienced a digital transformation related breach[10]

Alert Fatigue: Nearly half of security alerts are false positives[11]

Overwhelming Attack Surfaces: 58% of organizations still lack a third-party cyber risk management program[12]

The Cybersecurity Skills Shortage: 60% of organizations are at-risk due to staffing shortages[13]

What Can You Do?

Understand the Risks

Geopolitical
State-sponsored threat actors, data legislation, stability & sovereignty

Supplier
How secure is your supply chain, and what risk do partners represent?

Technical
Vulnerabilities in systems, tools, and endpoints

Establish a Foundation

- Triage partners to determine risk levels
- Identify who has access to what

Assess Partners For...

- Business criticality
- Security maturity
- Regulatory/framework adherence
- Supply chain risk management
- Willingness to participate in your own security program

Deploy XDR

- Ecosystem-wide monitoring
- Threat intelligence
- Proactive threat hunting
- UEBA for more accurate detection of behavioral anomalies
- Integration with existing solutions/infrastructure

Trustwave

trustwave.com

Sources:

[1] https://orkcat.com
[2] https://www.trustwave.com
[3] https://www.zdnet.com
[4] https://theconversation.com
[5] https://www.sonatype.com
[6] https://www.cybersecuritydive.com
[7] https://www.cybertalk.org
[8] https://www.cybersecuritydive.com
[9] https://www.ibm.com
[10] https://get.cybergrx.com
[11] https://www.riemanlab.org
[12] https://get.cybergrx.com
[13] https://www.isc2.org