

Understanding the cybersecurity challenges of the modern supply chain

the supply chain is more vulnerable than it's ever been. Cybercrime cost U.S. businesses more than \$6.9 billion in

Amidst digital transformation and geopolitical instability,

2021, and only 43% of businesses feel financially prepared to face a cyber-attack in 2022.

The Most Prominent Supply Chain Attacks Since 2020



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/gallon²



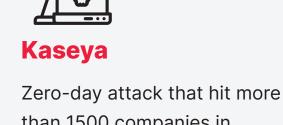
More than 18,000 customers

and 9 U.S. government agencies, with a price tag of about \$1B (\$12M on average per company)1



Impacted over 3 billion devises

(including mobile) worldwide⁴



than 1500 companies in

17 countries with more than 1 million devices and cost millions of dollars in lost revenue³

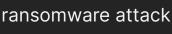
Understanding the Supplier Risk Landscape

In the last **5 years**, software supply

650%

chain attacks have increased 650% 5 11 seconds

This year, there will



be an estimated

every **11 seconds**⁷



the highest in 17 years®

An average ransomware payout was \$812k,

\$812k

a 500% YOY increase from **\$170k** 6 **70%**

Nearly **70%** of midsize

by ransomware in 2021,

organizations were hit

double that of 20208 breach rose to over \$4M -

Why are Attackers Increasingly **Targeting Suppliers?**

Taking the Path of

Least Resistance

Access to Hundreds Large-scale disruption of Thousands of of critical infrastructure



A Perfect Storm How Did We Get Here?

The Rush Towards Digital

Transformation: 82% of

Overwhelming Attack





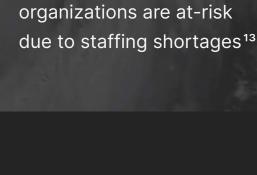
Bypassing traditional

security controls

businesses have experienced a digital transformation related breach 10

still lack a third-party cyber risk management program 12

Surfaces: 58% of organizations



Establish a Foundation

Assess Partners For...

Business criticality

Security maturity

Triage partners to determine risk levels

Identify who has access to what

Shortage: 60% of

Alert Fatigue: Nearly

half of security alerts

The Cybersecurity Skills

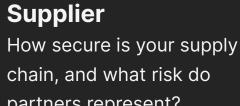
are false positives 11

What Can You Do? Understand the Risks

Geopolitical State-sponsored threat

actors, data legislation,

stability & sovereignty



partners represent?



Technical

Vulnerabilities in systems, tools, and endpoints

Regulatory/framework adherence Supply chain risk management

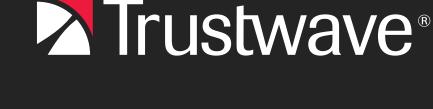
- Willingness to participate in your own security program
- Ecosystem-wide monitoring Threat intelligence

Deploy XDR

UEBA for more accurate detection of behavioral anomalies

Proactive threat hunting

- Integration with existing solutions/infrastructure





9 https://www.ibm.com

13 https://www.isc2.org