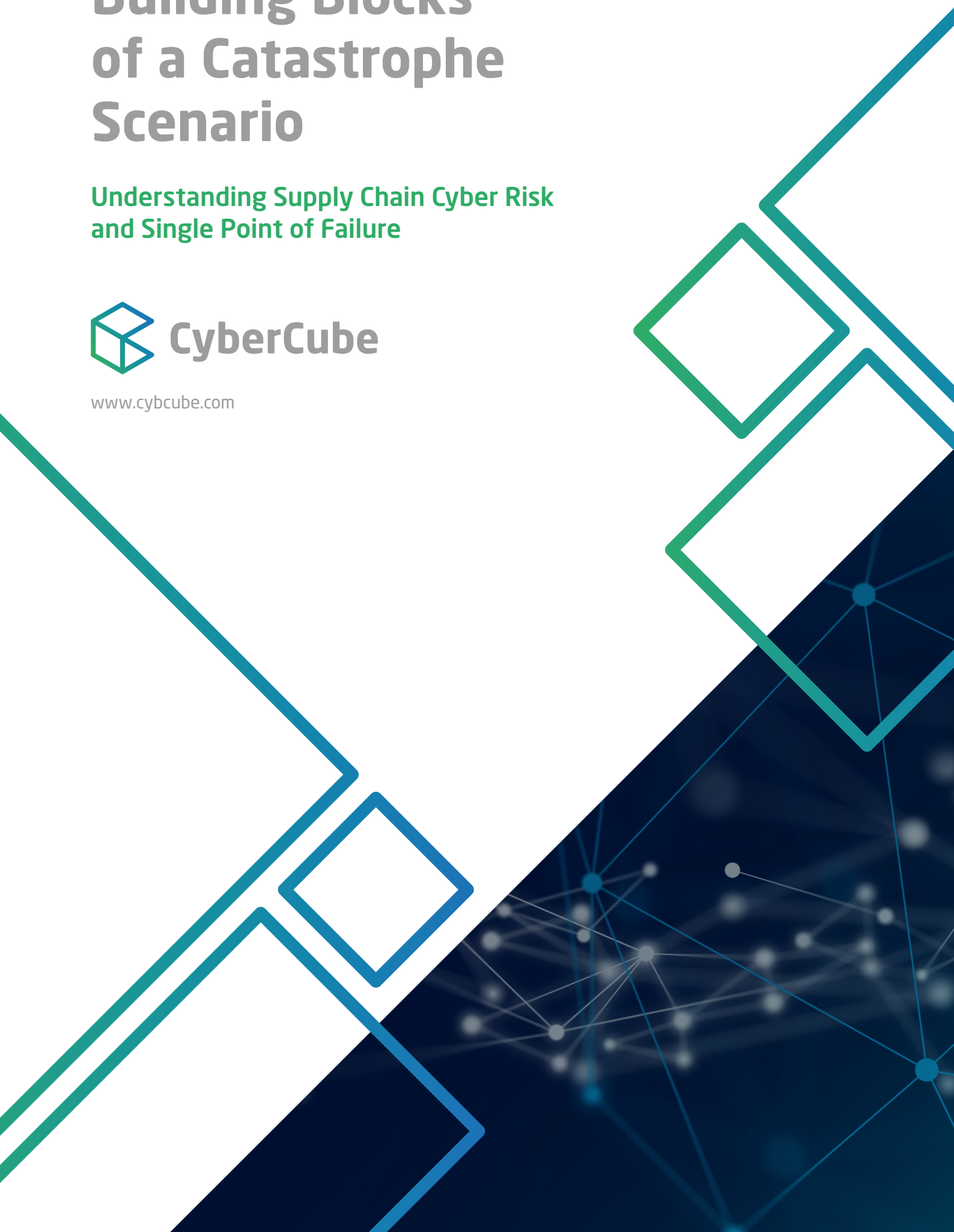
Building Blocks of a Catastrophe Scenario

Understanding Supply Chain Cyber Risk and Single Point of Failure

CyberCube

www.cybcube.com



With major attacks such as Microsoft Exchange, Blackbaud and SolarWinds making headlines over the past year, supply chain cyber risk has shifted from an identified risk area to become a key topic of interest in the security and insurance industries.

The SolarWinds software supply chain attack reported in December 2020 was a catastrophic-scale data breach that impacted 18,000 entities including major governmental bodies such as the U.S. Department of Defense and large private sector companies including FireEye and Microsoft. The Microsoft Exchange attacks in March 2021 impacted more than 30,000 companies and resulted in follow-on ransomware infections causing data breach and business interruption. Additional supply chain attacks over the past year have included the Accellion File Transfer Application (FTA) breach exposing data of more than 100 companies, the SITA breach impacting millions of airline passengers, Silver Sparrow malware infecting Macs in 153 countries, the Codecov software development attack impacting more than 250 organizations, and the PHP Git repository hack which, if successful, could have impacted the majority of global websites.

In this connected landscape, each individual company is under increasing pressure to play its part in terms of shoring up cyber defense, but not only for its own sake. Businesses face the potential of cyber incidents rippling outward, causing impact to a company's partners, customers, and the greater industry. Furthermore, understanding supply chain cyber risk can be complicated; focusing on a company's own individual risk seems like enough of a problem to handle.

CyberCube's *Portfolio Manager* product focuses on modeling supply chain cyber risk - the risk that a company faces due to the exposures and actions of interconnected entities such as vendors, suppliers, service providers, partners, contractors, and consultants.

Supply chain cyber attacks are attractive to criminals in a cost-benefit analysis as they provide:

- A high volume of potential targets reached via an existing infrastructure channel
- Smoother pathways to advanced, privileged access via abuse of a trusted company-supplier relationship
- An increased attack surface with points of entry at multiple companies rather than at a single company
- The ability to target specific company types or profiles at scale
- High-profile precedents that confirm feasibility and enable attackers to build upon existing tools and attack patterns

Definitions

Supply Chain Risk is a type of third-party risk based on the exposure of the products and services purchased by a company, and its relationship with vendors and suppliers.

SPoF (Single Point of Failure) is the targeted entity for a given attack scenario that has multiple dependent and interconnected entities. (Note: The SPoF may or may not itself be in an insurer's portfolio.)

A number of factors are driving an increased exposure to supply chain cyber risk for many businesses. Supply chain cyber risks are a function of the attack surface, and will grow with the integration of new Internet of Things (IoT) devices, mobile endpoints, and operational technologies (OT). Additionally, the blending of personal/public/workplace networks and devices and a movement away from the traditional corporate IT network perimeter model will increase the opportunity for supply chain cyber risk. Increased vendor counts and outsourcing in the "as-a-service" economy, deep reliance on cloud and open-source software, and the proliferation of complex global supply chains with exposure in the physical and digital realms, will provide further opportunities for disruption.

In this report, we will discuss the six major types of supply chain cyber threats and what organizations and insurers can do to understand and quantify risk in these areas.

These threats are: 1) data exposure, 2) supplier outage, 3) vulnerable products, 4) business email compromise, 5) access abuse, and 6) product tampering. This research highlights the "scenario count" (the number of times this incident appears in the 29 scenarios captured in our *Portfolio Manager* tool designed to quantify losses from cyber risk aggregation events), "risk factors" (the key exposures that magnify risk of a particular threat) and the "loss potential" (the major cost components associated with a given threat type).

Single Point of Failure

To effectively model systemic cyber risk, it is vital to understand the physical and digital relationships between connected entities, particularly dependencies on those Single Point of Failure (SPoF) entities which provide core products and services with a wide footprint of users. Infiltrations or failures at SPoFs can result in cascading impacts to many interconnected entities.

For example, in recent months, there have been a number of instances of the world's largest commercial cloud computing providers being vulnerable to downtime. In November 2020, Amazon Web Services, the world's largest cloud provider, experienced a major outage in its US-EAST-1 data center. Weeks later, Google's primary authentication system for its entire Cloud Platform went down, with many companies impacted by both cloud outages. In March 2021, Microsoft Azure experienced a 14-hour service outage due to an error in an authentication mechanism.

These events demonstrate how cloud providers can act as SPoFs in the event of an incident that causes an outage impacting many related services utilized by a large user base. CyberCube has focused on SPoFs, creating a database that can help (re)insurers develop an edge in cyber portfolio management by obtaining insights on SPoFs and their connectivity with risks in a portfolio. SPoF intelligence can help underwriters create new insurance products with terms and conditions tied to specific points such as data centers and cloud providers. It can help inform underwriting strategies by optimizing exposure to SPoFs based on risk appetite, and provide an understanding of potential exposure and claims arising from recent or ongoing catastrophic SPoF incidents.

Understanding supply chain cyber risk

Top Supply Chain Threats

Data Exposure

Supplier Outage

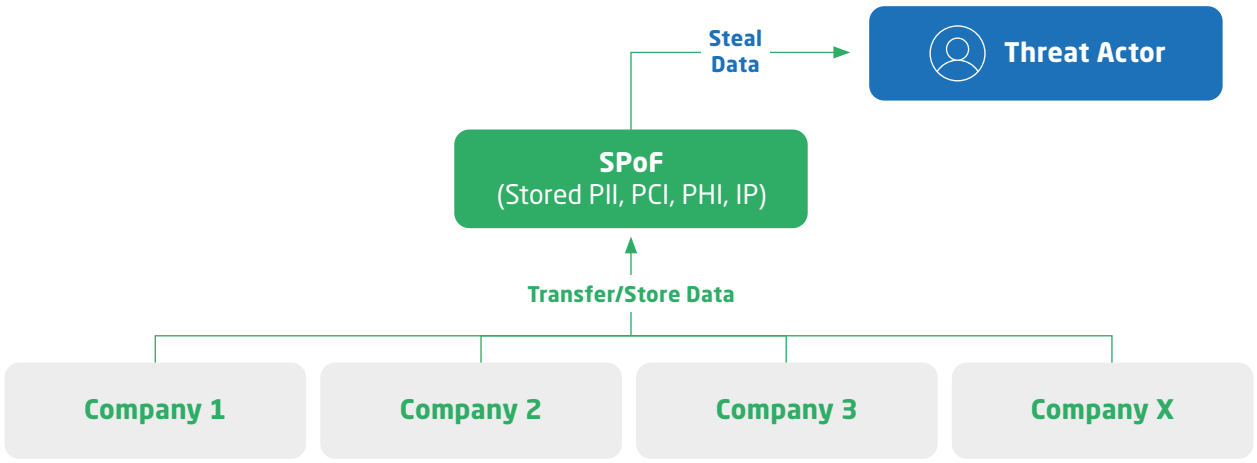
Vulnerable Products

Business Email Compromise

Access Abuse

Product Tampering

Threat 1: Data Exposure



Description:

Supplier who stores or manages a company's sensitive data and/or financial assets, gets breached.

CyberCube Scenario Count: 7

CyberCube Scenario Example:

Large-scale data theft of a leading outsourced payroll provider.

Real-World Examples:

- **Blackbaud** - PII and financial data was exposed for hundreds of institutions such as the Boy Scouts of America and Oxford University when a leading software-as-a-service (SaaS) provider to the education and non-profit sector was hit by ransomware in May 2020.
- **SEI Investments** - A ransomware attack against a vendor of fund administrator SEI Investments exposed PII of 100 of its clients in May 2020.

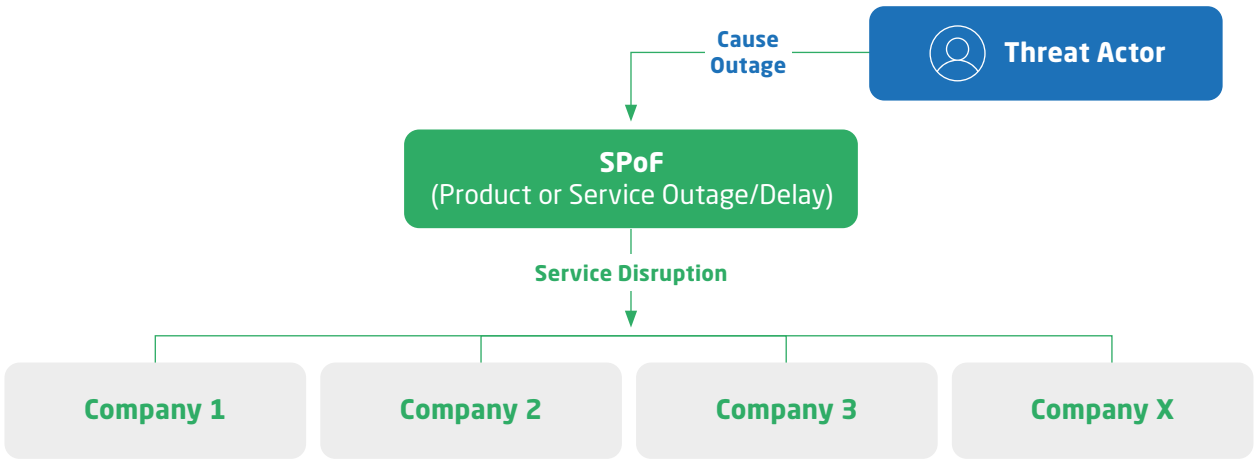
Risk Factors:

1. High volume of sensitive data stored by supplier
2. Lack of vendor vetting to assess compliance, security maturity, and incident history
3. Lack of SLAs/contracts with effective third-party security requirements

Loss Potential:

1. Investigation and response costs including customer notification and credit monitoring
2. Legal liabilities
3. Misdirected payments via exposed financial assets

Threat 2: Supplier Outage



Description:
Supplier experiences extended outages or delays due to a cyber incident.

CyberCube Scenario Count: 9

CyberCube Scenario Example:
Long-lasting outage of a leading cloud services provider.

Examples:

- **Garmin** - Leading GPS technology company Garmin experienced a multi-day outage in July 2020 due to WastedLocker ransomware that impacted applications used by pilots and vessels for navigation, causing flight and shipping delays.
- **PrismHR** - Major payroll provider PrismHR experienced a ransomware attack in March 2021 that knocked systems offline for three days impacting hundreds of professional employment organizations (PEOs).

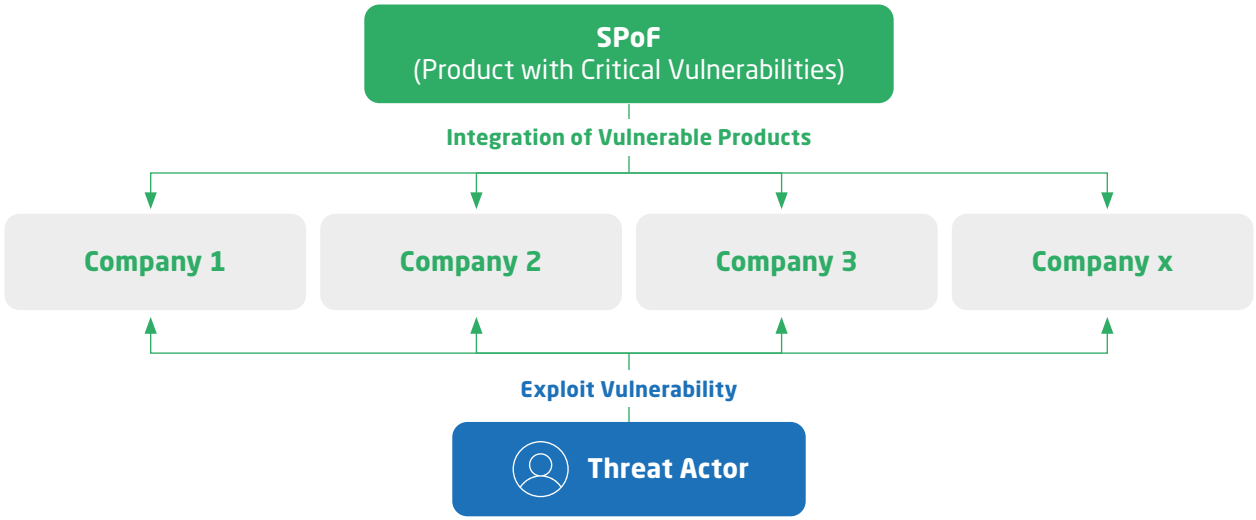
Risk Factors:

1. Poor data and service resiliency and redundancy (e.g. lack of data backups, secondary providers, failover options)
2. Lack of comprehensive and current business disaster recovery plan
3. Specialized product dependency on a single supplier

Loss Potential:

1. Business interruption costs including lost revenue and additional operating expenses
2. Investigation and response costs including detection/escalation expenses and customer notifications
3. Legal liabilities due to SLA violations and negligence

Threat 3: Vulnerable Products



Description:

Supplier produces products with critical vulnerabilities.

CyberCube Scenario Count: 4

CyberCube Scenario Example:

Vessel weaponization due to leading Maritime Very Small Aperture Terminal (VSAT) vulnerability.

Examples:

- **Microsoft Exchange** - Four zero-day vulnerabilities in Microsoft's Exchange Server product were targeted by nation state attackers in March 2021 in an espionage/ exfiltration scheme impacting hundreds of thousands of global customers.
- **Urgent 11/Ripple20** - In July 2019 and June 2020, critical vulnerabilities were discovered affecting the TCP/IP communication stack and the networking software used in hundreds of millions of IoT devices embedded across multiple industries.

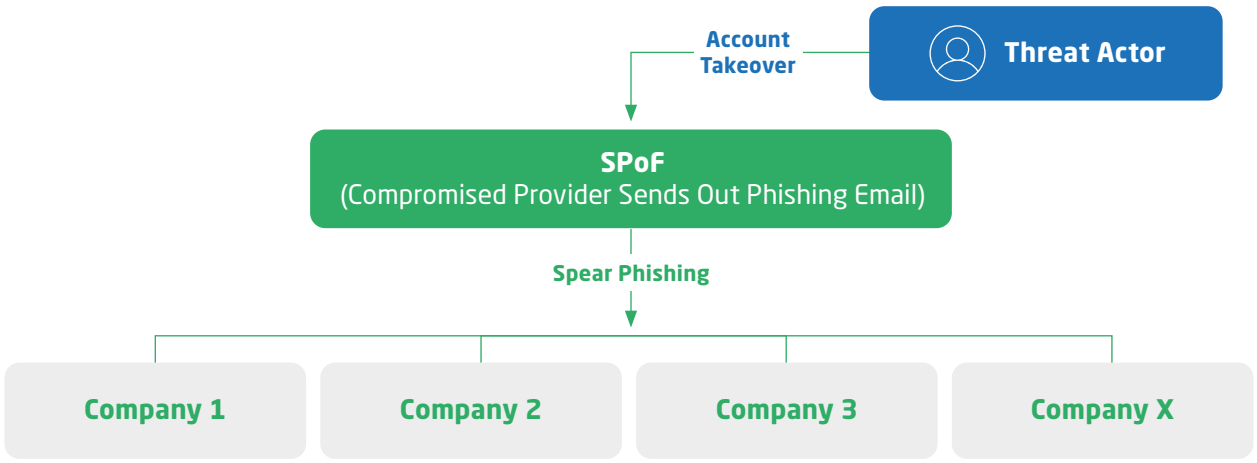
Risk Factors:

1. Poor vulnerability management leading to incomplete coverage and long patching cycles
2. Poor asset management leading to out-of-date, poorly monitored and weakly configured products
3. Lack of proper network segmentation to prevent lateral movement

Loss Potential:

1. Business interruption costs including lost revenue and additional operating expenses
2. Data and asset recovery costs
3. Investigation and response costs including customer notifications

Threat 4: Business Email Compromise



Description:

Supplier domains are compromised or mimicked for targeted phishing/BEC attacks, which have a higher success rate due to higher trust relationship between company and supplier.

CyberCube Scenario Count: 2

CyberCube Scenario Example:

Large-scale data theft via spear phishing from vendor email compromise of leading online banking services provider.

Examples:

- **Nikkei** - Media company Nikkei lost $29 million in 2019 when attackers used a vendor email account to successfully conduct a business email compromise attack.
- **Silent Starling** - Threat actor group Silent Starling conducted a major campaign in 2019 to compromise the email accounts of more than 700 employees working in the finance departments of hundreds of globally distributed companies, then sent out carefully crafted phishing emails to targets resulting in large scale BEC losses.

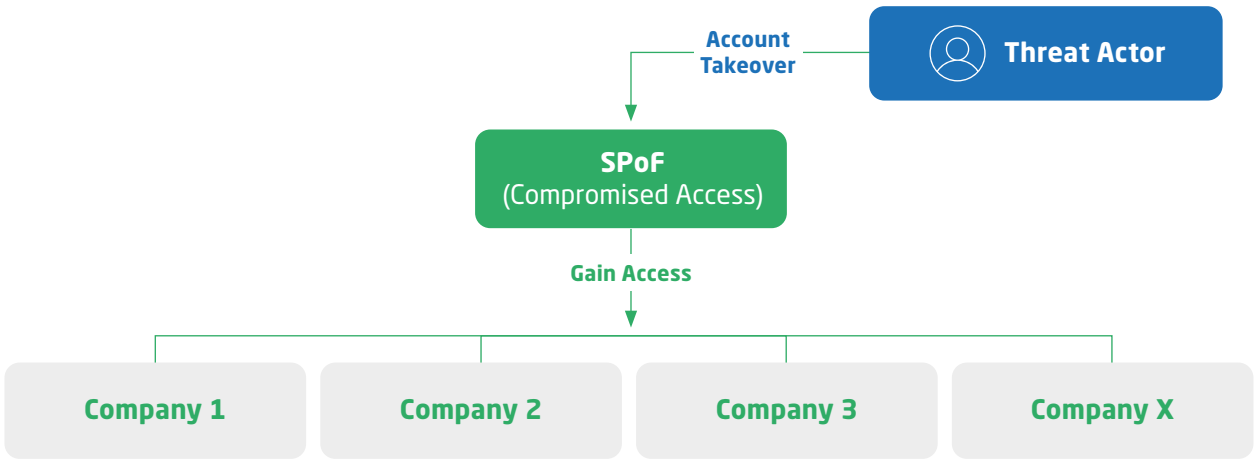
Risk Factors:

1. High volume of vendors and suppliers
2. Weak email security defenses including DNS-based authentication configurations and filtering tools
3. Lack of effective, consistent employee security training

Loss Potential:

1. Misdirected payments including financial fraud
2. Investigation and response costs including customer notifications and detection/escalation expenses
3. Legal liabilities

Threat 5: Access Abuse



Description:

Attackers infiltrate one or more supplier network(s) with the deliberate intention of pivoting to a target network ("island hopping") to conduct an attack.

CyberCube Scenario Count: 1

CyberCube Scenario Example:

Large-scale cash theft at a leading financial transaction provider via a compromised affiliate account.

Examples:

- **Airbus** - Nation state-sponsored actors targeted Airbus suppliers Rolls Royce and Expleo in 2019 and used compromised VPN access to expose confidential product specification documents.
- **DDS Safe** - Ransomware actors targeted two providers behind medical records software DDS Safe in August 2019, abusing access to deploy ransomware at hundreds of dental offices around the US.

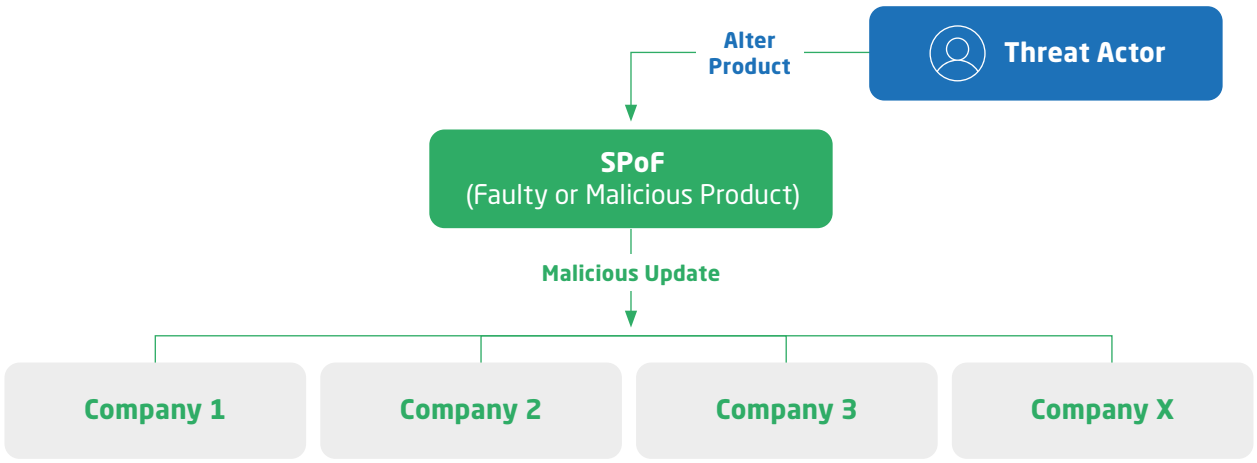
Risk Factors:

1. Lack of monitoring and oversight of supply chain access points, especially VPN or sensitive/air-gapped systems
2. Failure to remove ("sunset") supplier access to company network upon contract termination
3. Poor identity access management (IAM) practices and/or lack of Zero Trust

Loss Potential:

1. Investigation and response costs including detection/escalation expenses and customer notifications
2. Misdirected payments including financial fraud

Threat 6: Product Tampering



Description:

The product is altered to be faulty, to have malicious code, or to cause other types of damage.

CyberCube Scenario Count: 6

CyberCube Scenario Example:

Targeted data theft via malicious update of leading mobile point of service (PoS) software.

Examples:

- **SolarWinds** - Nation state hackers hacked into IT company SolarWinds' Orion network management software and inserted malware into a software update enabling the adversaries to infiltrate hundreds of public and private sector entities, including security company FireEye, the Department of Homeland Security, and the Pentagon.
- **Avast** - State-sponsored actors targeted cybersecurity company Avast's CCleaner Windows registry cleaner software product twice, successfully in 2017 and unsuccessfully in 2019, provisioning malicious updates to infect more than two million users.

Risk Factors:

1. Ineffective security logging and monitoring to detect attacks at early stages
2. Lack of quality checks before deploying software, hardware, and firmware updates
3. Lack of visibility into suppliers' security and privacy maturity, including compliance, auditing, security processes and attack history

Loss Potential:

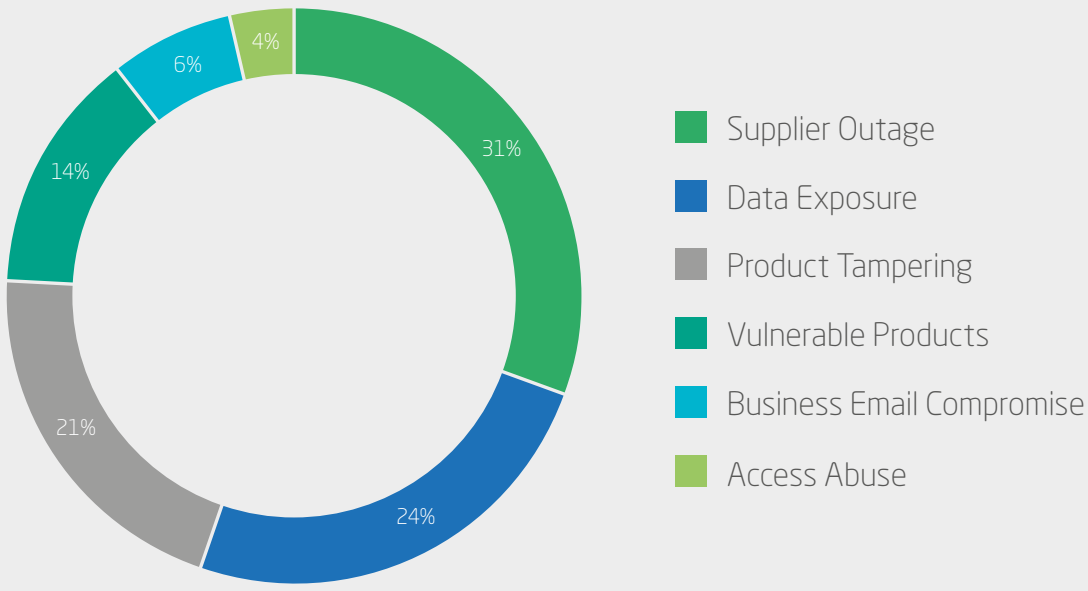
1. Investigation and response costs including credit monitoring
2. Business interruption costs including lost revenue and additional operating expenses
3. Legal liabilities
4. Misdirected payments including financial fraud

Portfolio Manager scenarios fall into six supply chain threat categories

CyberCube's 29 *Portfolio Manager* Scenarios fall into six supply chain categories, with the greatest risk to overall insurable loss concentrated around the threats of Supplier Outage (with the potential for significant business interruption and legal liabilities), Data Exposure (leading to data loss with legal and regulatory liabilities), and Product Tampering (resulting in potential data or cash theft as well as lost revenue). Within each of these threat types, modeled scenarios have varying designations of threat actor classes and motivations, kill chain sequences, SPoF categories, industry and regional footprints, and overall loss frequencies and severities.

An overall view of catastrophic cyber risk thus encompasses a wide variety of industries, geographies, technologies, and revenue streams that can be impacted by these supply chain threats.

Porfolio Manager Scenario Composition



CyberCube's Portfolio Manager Version 3.0 product includes updates to key scenarios

As cyber is a dynamic peril, it is vital that CyberCube's models reflect the current threat landscape. With this in mind, we recently (May 2021) updated our *Portfolio Manager* product, releasing Version 3.0 to explicitly address new/revised assumptions and events that have recently occurred. Updates include:

Expanded Footprint

SPoF list and market share updates capturing the major market players and the increased attack surface as well as the new and evolving connections and up-to-date digital dependencies.

Multi-Threat Actor

Includes new analyses for various threat actor motivations and capabilities underlying scenario assumptions to account for the evolving threat landscape.

Severity Improvements

Updates to modeling for various loss components such as business interruption as well as notification costs, investigation and response, and legal liability arising from data exposure events.

Scenario Updates

CyberCube models 29 core scenarios in *Portfolio Manager* looking at a variety of potential catastrophic events causing widespread insurable and systemic loss.

Conclusion

CyberCube expects the importance of analysing supply chain cyber risk and identifying SPoFs to continue to be paramount as digital dependencies increase, Internet infrastructure remains centralized, and attackers continue to target supply chains for initial access and distribution of threats to maximize gains from a single cyber attack.

CyberCube's *Portfolio Manager* product models scenarios that fall into six major types of supply chain threats. In CyberCube's view, the top threat types for catastrophic cyber risk causing insurable impacts in today's landscape are Supplier Outage, Data Exposure, and Product Tampering. These threats are increased by exposure to risk factors such as lack of data and service redundancy and resiliency, specialized dependency on a single supplier, a high volume of sensitive data stored by a supplier, lack of quality checks before deploying updates, and poor logging and monitoring capabilities for detecting early-stage attacks. Overall the areas of greatest loss potential stemming from these threats are business interruption, response and recovery costs, and legal liabilities.

Five key areas that insurers can focus on when assessing a portfolio for catastrophic cyber risk potential are (1) resiliency in the form of redundant systems and defined recovery plans, (2) extent of dependency on a single or small subset of suppliers, (3) maturity of vulnerability and patching management practices, (4) comprehensive identity access management particularly around vendors and third parties, and (5) overall security posture of a company's vendors, contractors and suppliers.

Some underwriters name specific cloud and service providers on their policies by "scheduling" or endorsing them into policy language. In the future, we may see insurance carriers scheduling specific cloud providers on their policies in greater abundance.

With the Technology Dependencies module in CyberCube's SPoF intelligence providing key insights into companies' digital supply chains as well as updates to the suite of *Portfolio Manager* cyber catastrophe scenarios in the Version 3.0 release, (re)insurers can better understand the risk at a single risk level (in terms of a single company's supply chain exposure) as well as at the portfolio level (in terms of the cascaded impact a supply chain attack can have on a high volume of companies in a given portfolio).

For more information on CyberCube's scenarios go to **www.cybcube.com**

Author

Charlotte Anderson, Senior Cyber Risk Analyst

Contributors

Morgan Hervé-Mignucci, Director, Cyber Risk Modeling
Josh Pyle, Senior Director, Product & Analytics

Editorial Management

Yvette Essen, Head of Content & Communications

United States

CyberCube Analytics
58 Maiden Lane
3rd Floor
San Francisco CA94108
Email: info@cybcube.com

United Kingdom

CyberCube Analytics
51 Eastcheap
1st floor
London EC3M 1JP

Estonia

CyberCube Analytics
Metro Plaza
Viru Väljak 2
3rd floor
10111 Tallinn

CyberCube

www.cybcube.com