SPECIAL SUPPLY CHAIN REPORT

Cyberattacks in the Supply Chain

Created by Resilinc Risk Analysis Team
Updated: November 8, 2022

resilinc

Executive Summary

This report covers cyberattacks and the impact to the supply chain, specifically the vendor-client relationship. Cybercrime is a top threat for digital firms worldwide; as organizations expand dependency on technology the threat of cyberattacks grows. Read on to see the types of cyberattacks, vulnerabilities in the supply chain, the trend of cyberattacks, and best practices to mitigate and protect your supply chain against attacks.

Key Takeaways:

- The move to work-from-home has increased cyberattacks
- 93% of organizations have suffered at least one indirect data breach since 2020
- Risk in weak third-party services
- Hackers look to extract and sell data

resilinc

Table of Contents

resilinc

Background on Cyberattacks

Last Updated: 11/8/22

resilinc

Background on Cyberattacks

- Cybercrime has increased since the beginning of the pandemic, and is expected to become more prevalent as hackers replicate and learn from one another – fraudsters are exploiting supply chain weaknesses
- Cybercrime can occur as a result of opportunistic threats or focused strikes. There are specific cyberattacks designed to enter a supply chain and create damages and disruptions to several interconnected businesses
  - Focused strikes can cause more harm in the supply chain
- Intruders can breach the supply chain network of a business in nearly any sector
  - Neither the banking sector, the oil industry, nor the government are free from the potential of supply chain assault
  - Impacts from shipping and logistics to consumer sales, and more
- Attacks on the supply chain impact more than just the business attacked. They may even enter the supply chain and infect highly secured customer networks' systems
- **Since 2020, 93% of worldwide businesses have suffered at least one indirect data breach**, due to weaknesses in supply networks (BlueVoyant)
  - **Supply chain data breaches have increased by 37% in the last 12 months** (BlueVoyant)
  - There has been an increase in the number of organizations who claim they have no method of identifying a data breach in their supplier chain (Yahoo!Business)

resilinc

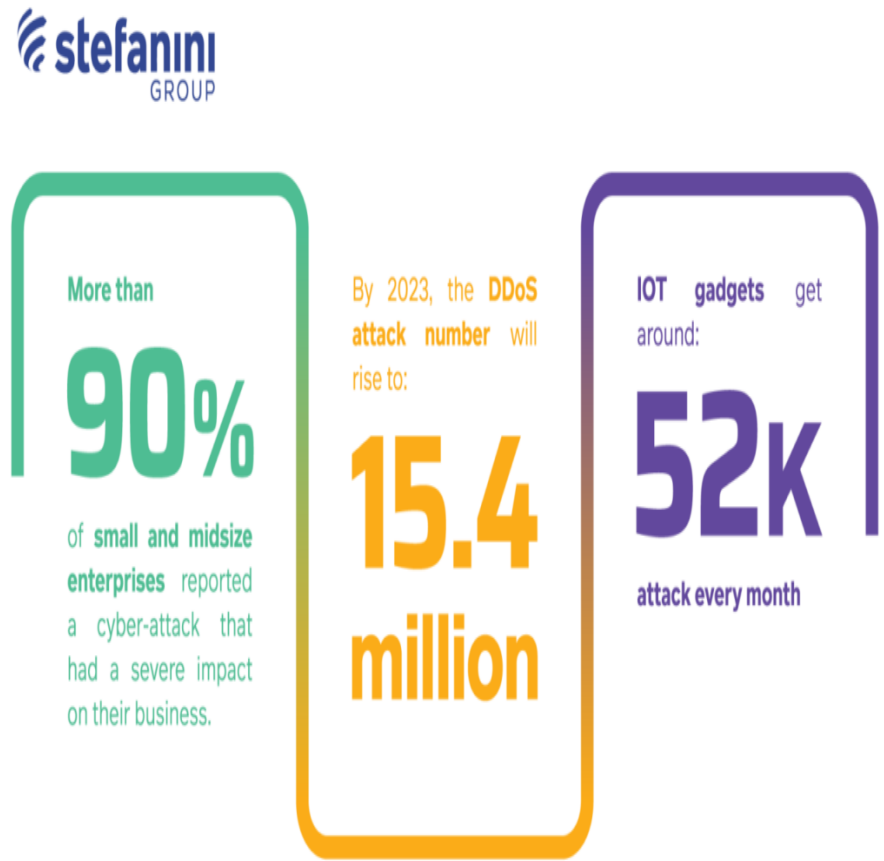
Cyberattacks in the Supply Chain

- As technology develops, supply networks become more complicated making them more susceptible to cyberattacks
  - One company's security flaws could expose its partners or suppliers
- **Up to 40% of cyber dangers now arise indirectly via the supply chain (AAG)**
  - 60% of 900 organizations in a survey by Kaspersky report supply chain assaults as their most probable cyberattacks (AAG)
  - Other cyberattacks Kaspersky shows organizations worry about include cyber espionage (59%), APT (57%), and ransomware and data theft (66%)
- Cybersecurity executives are worn out and 'always on' due to growing digital connections – cybercriminals exploit user tiredness
  - 23% of security executives monitor partners and suppliers for cyber security concerns in real time (AAG)
- Third-party risk is rising. 60% of organizations will utilize cyber security risk as a key factor to determine third-party transactions and engagements by 2025
  - Some companies restrict third-party coverage to only suppliers and vendors, excluding consumers, partners, investors, etc.
- **Nearly 2,000 enterprises rely on vulnerable organizations for cyber security** (AAG)

resilinc

Third-Party Cyber Protection Risk

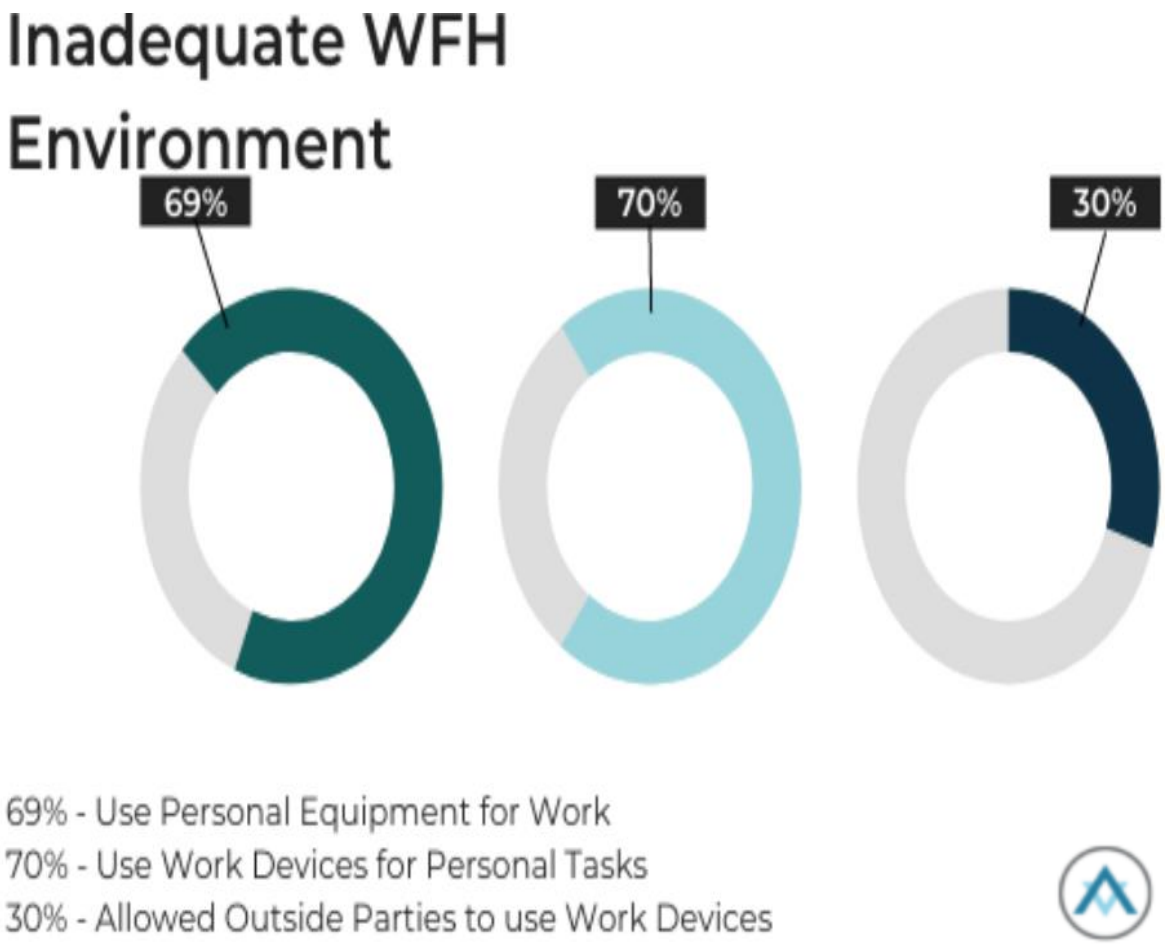
- **Businesses that elect to choose third-party providers for their cybersecurity can unknowingly put themselves at risk**
  - Companies may outsource their IT and security administration to managed service providers (MSPs) in order to save money and bring more efficiency
- Many third-party security providers are new or startup companies that may not have the best protection
  - Third-party security providers can be more appealing as they offer more purchasing power, wider carrier networks, and cost savings
  - While third-party services save businesses time and money, they may also pose cybersecurity threats
- **Hackers tend to identify and attack weak third-party services to extract and sell data**
- **Third-party suppliers have been increasingly targeted by cybercriminals** wanting to broaden their scope of assaults according to the NTT Security Holdings' 2022 Global Threat Intelligence Report
  - Increased attacks in hopes of utilizing third-parties as a steppingstone to target thousands of downstream customers in the supply chain



resilinc

Increased Risk in Work From Home

- Cyber risk has increased as the proliferation of software-as-a-service (SaaS) offerings and widespread use of cloud hosting has enabled people to work efficiently from anywhere
  - The transfer of data between business and personal devices is often inevitable due to the increase of remote work
  - Keeping sensitive data on personal devices significantly increases vulnerability to attacks
- Remote work has increased the cost of data breaches by $137,000 for the average company since the beginning of the pandemic (Alliance Virtual Offices)
- The expansion of global supply chains has enabled businesses to source materials and support functions at competitive prices from a global supply
- 44% of remote workers get cybersecurity trainings once a year or less (Alliance Virtual Offices)
- **74% of the most globally remote jobs include IT and technology, digitization and analytics, and consulting**



Source: Working from Home Increases Cyberattack Frequency by 238% | Alliance Virtual Offices

Types of Cyberattacks

Malware

Refers to harmful software such as spyware, ransomware, viruses, and worms. Malware infiltrates a network through a weakness, generally when a user clicks on a malicious link or email attachment, which then installs harmful software

- Access to critical components is denied (ransomware)
- Installs malware or other potentially dangerous applications
- Collects information covertly by sending data from the hard drive (spyware)
- Certain components are disrupted, rendering the system unworkable

Phishing

The technique of delivering fake messages that seem to originate from a trusted source, often by email. Phishing is a rising cyberthreat

- Steal sensitive information such as credit card and login information
- Install malware on the victim's PC

resilinc

Sources for Supply Chain Attacks

1. Stolen certificates

If a hacker takes a certificate meant to vouch for the legality or safety of a company's product, they may distribute harmful code under the certificate's name

Even before the development process is employed to construct an application, hackers use the tools for creating software applications to introduce security vulnerabilities

2. Compromised software development tools

3. Preinstalled malware on gadgets

When a victim connects a compromised phone, USB drive, camera, or other mobile device to their system or network, the virus is activated

Firmware controls digital hardware, facilitating its operation and interaction with people and other systems. To obtain access to a device or network, hackers may embed malicious malware in firmware

4. Included in the firmware of components is program code

resilinc

Examples of Supply Chain Attacks

Event-stream 2018
Data Breach

- Hackers inserted a backdoor into an open-source code library that was utilized by Fortune 500 corporations and startups
- Malicious code was injected in two phases into event-stream, a code library with 2M downloads
- **Tried to steal Bitcoin wallets and transfer their funds** to a server in Kuala Lumpur
- Backdoor was discovered in 2018 within five days by a Github user

ASUS 2018
Hijacking and Phishing

- Compromise in an ASUS update system, **allowing malicious updates to be sent to up to 500,000 machines**
- Malware was spread through its automatic software update mechanism – infected updates included a backdoor software that tried to connect to an attacker-controlled domain. **The upgrades were validated using genuine ASUS digital certificates**
- The supply chain assault began in June 2018 and lasted until late October 2018
- **At least 13,000 PCs got the Trojanized upgrades – 80% of victims were customers, 20% were organizations**
- Malicious update used to sell customer data

SolarWinds 2020
Malware

- Target of a large cyberattack that expanded to its customers, including Microsoft and other major corporations
- Software updates with malware installed was sent out to 33,000 customers
- **Up to 18,000 clients installed the hacked upgrades**, including Fortune 500 organizations
- Hackers got into US government and commercial firms, some for months. Parts of the Pentagon, State Department, DOE, and NNSA were targeted, acquiring unclassified material at the Treasury Department
- Over 80% of the victims were nongovernmental groups
- **Allowed hackers to spy on companies and organizations**

resilinc

Resilinc Data

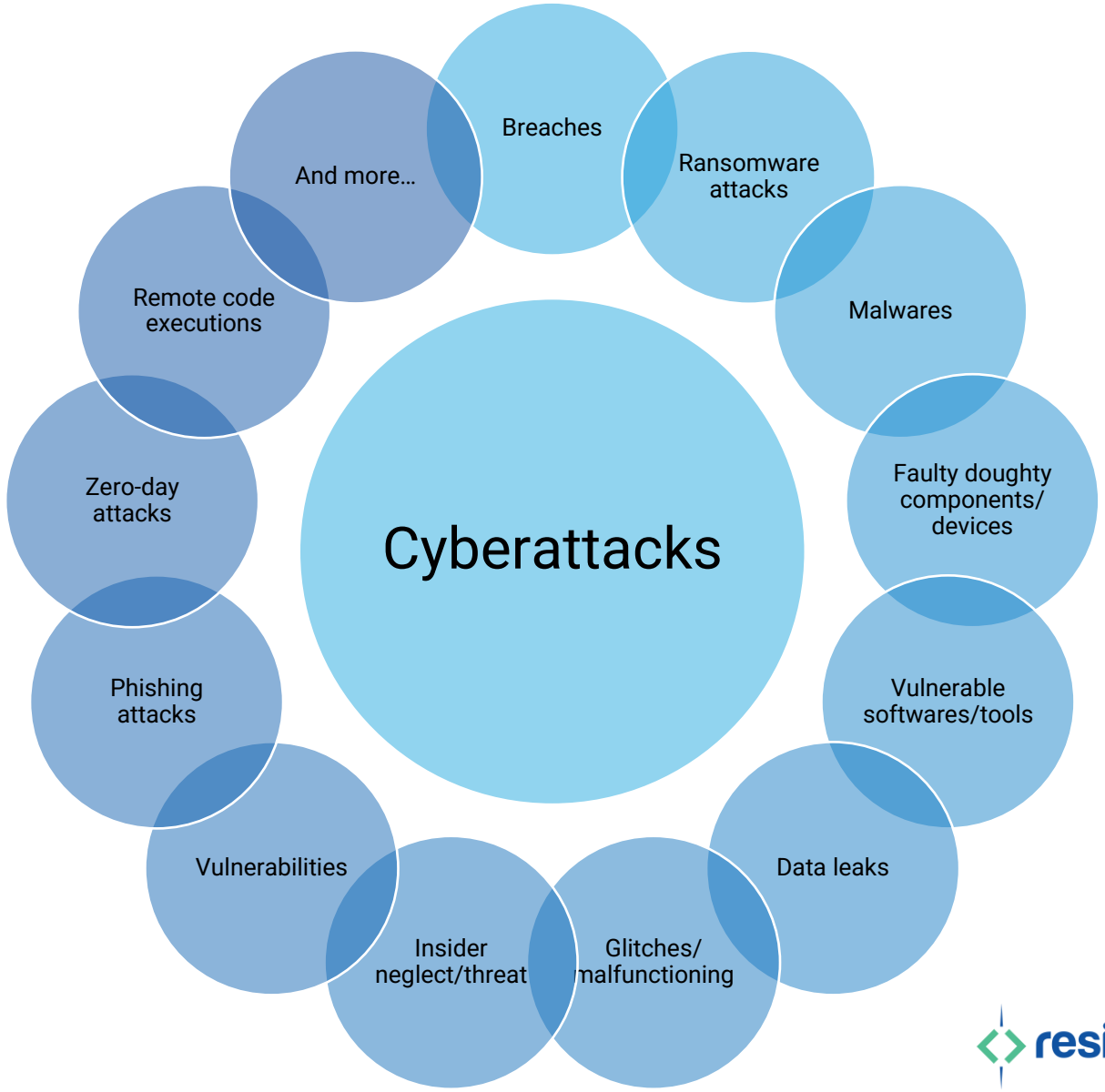
Last Updated: 11/8/22

resilinc

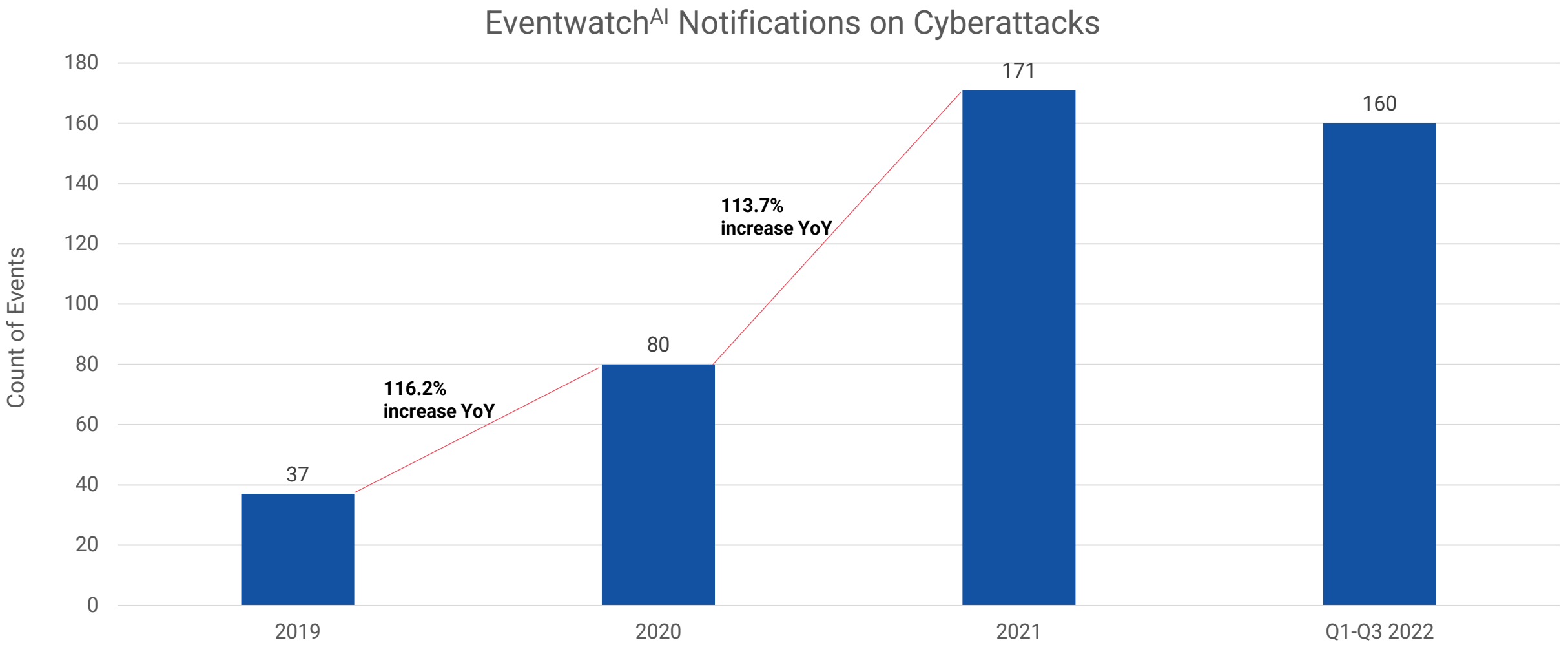
How Resilinc Tracks Cyberattacks

Reporting Criteria

- Data breaches/attacks reported at a:
  - Service provider, manufacturer, utility service, data center, financial institution, communication service, cargo/freight service, etc.
- All kinds of hacks, breaches, ransomwares, attacks, etc.
- Glitches in software or hardware that are vulnerable to cyberattacks
- Service interruptions
- When companies confirm impact in the public domain
- And more…

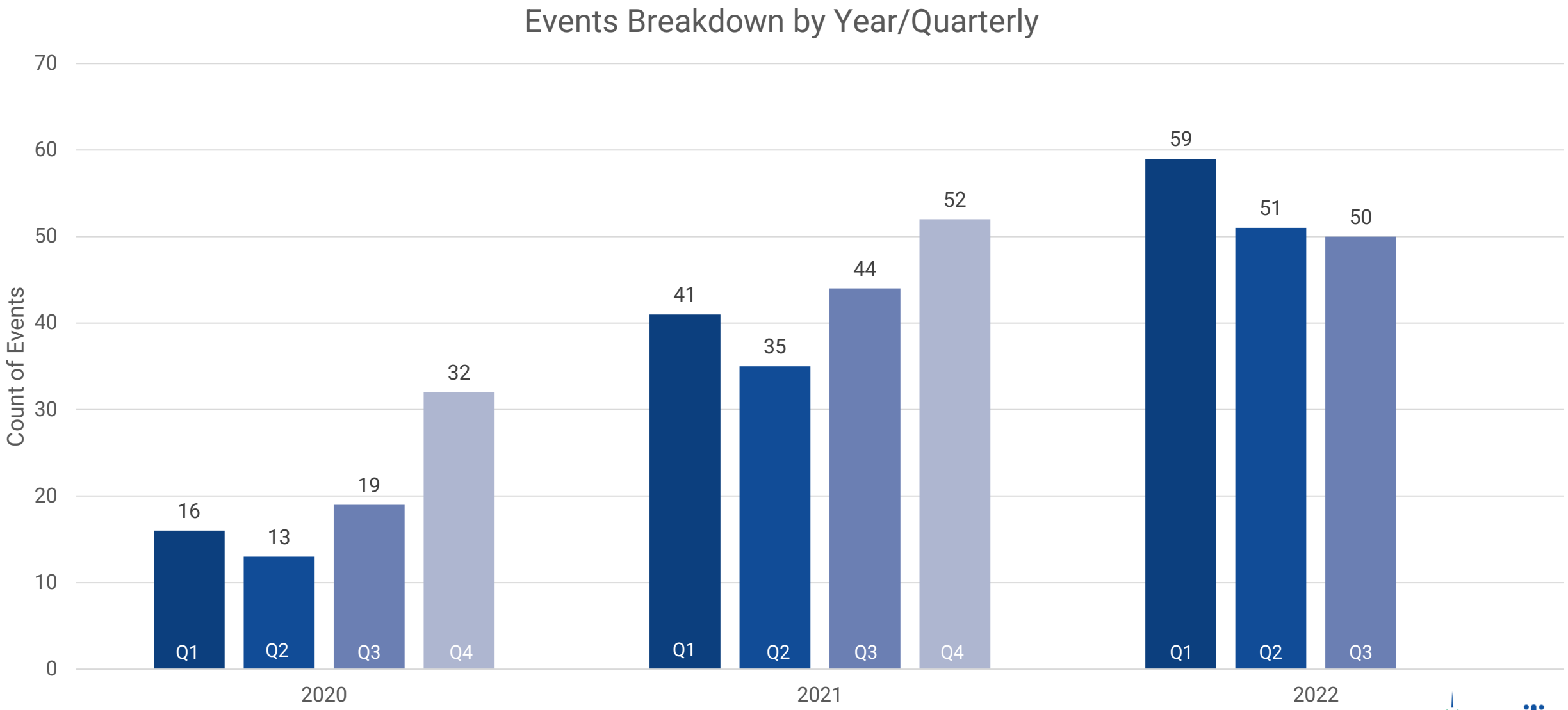


Increase in Cyberattacks



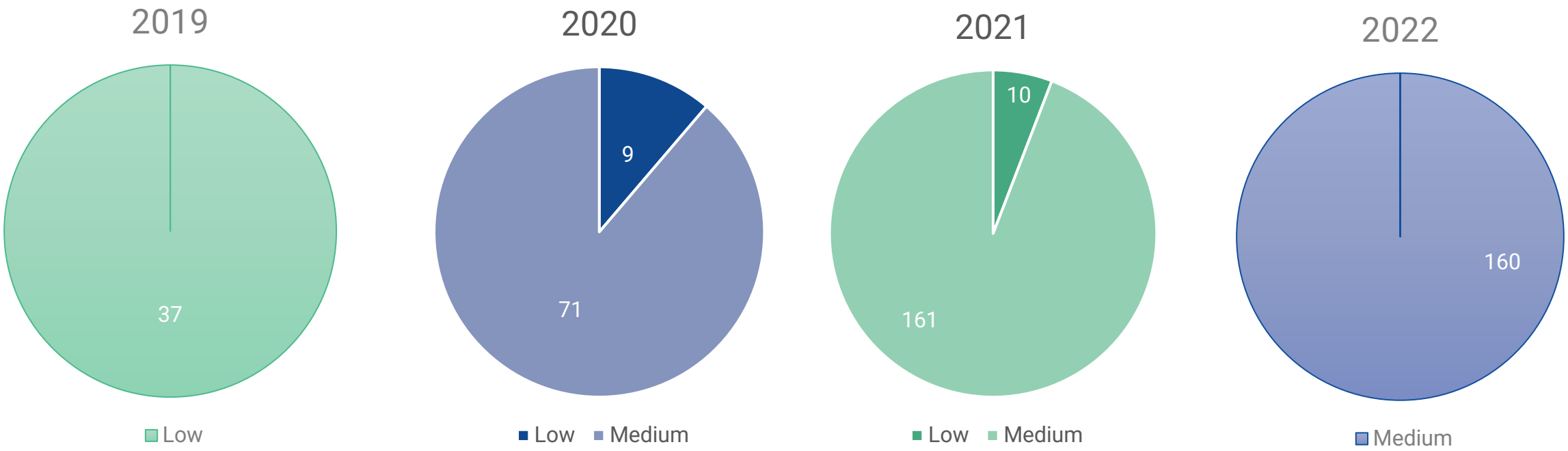
resilinc

Increase in Cyberattacks



resilinc

Severity of Cyberattacks



resilinc

Best Practices & Resilinc Solutions

Last Updated: 11/7/22

resilinc

Cyberattack Prevention

Prioritize third-party risk management

- Ensure the third-party is sufficient to protect against cyber risk
- Create a team that is staffed, trained, and prioritized to address supply chain concerns

Determine supply chain weaknesses

- Risk management teams should prioritize protecting ALL important supply chains, including information and physical supply channels

Engage key chain providers

- Examine and audit suppliers' security policies regularly
- Look down to the nth tier – anyone that makes, alters, or distributes supply chain components and engages with suppliers

Create a lab to identify issues in hardware and software

- Organizations who can afford to establish a full-time test lab should do so
- Cyberattacks can impact motherboards

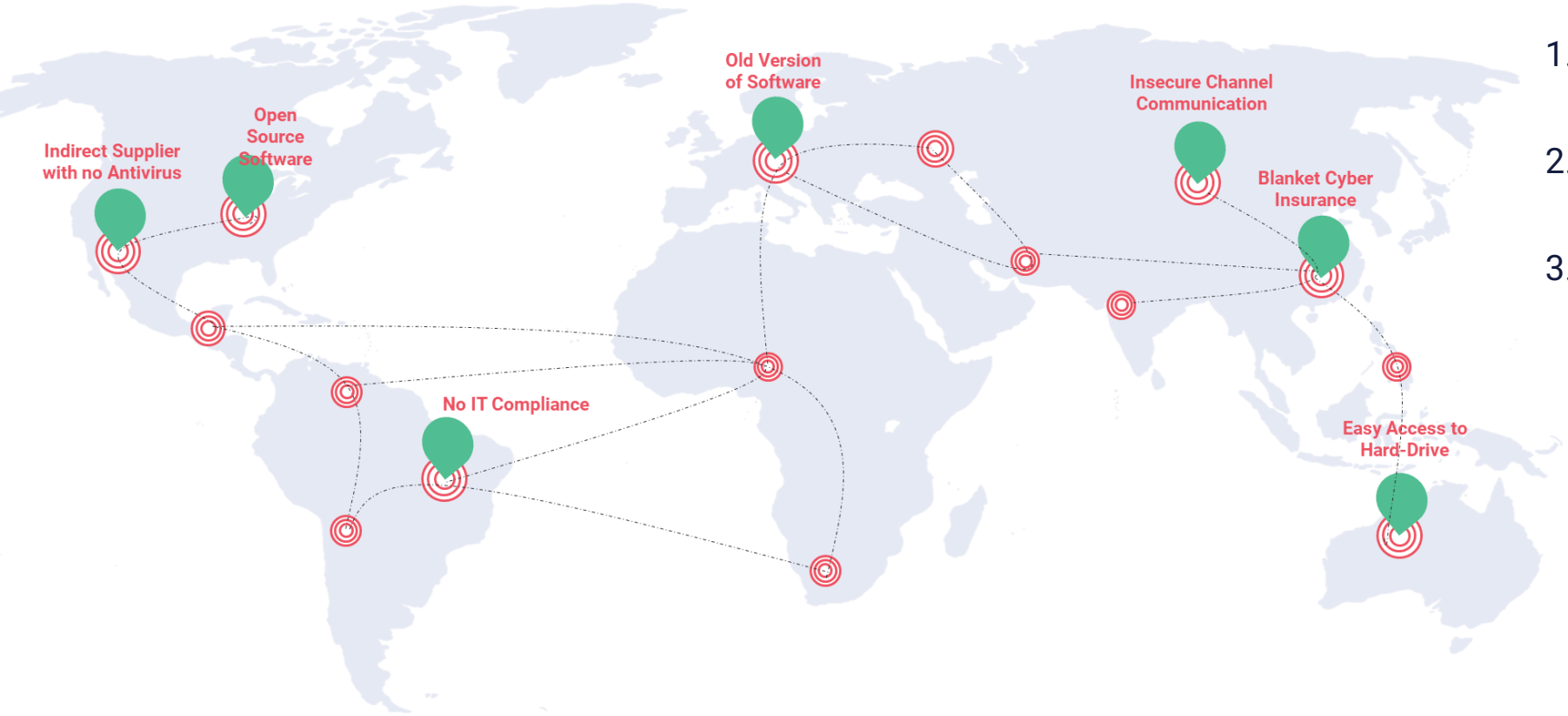
Validate supply chains from concealed attacks

- Can validate using end-to-end Blockchain or Hyperledger
- Important to have a source and time-stamped system that verifies every update

Source: https://www.techtarget.com/searchsecurity/tip/5-steps-to-help-prevent-supply-chain-cybersecurity-threats

resilinc

Unknowns can Cause Unprecedented Potential Impact to Business Continuity



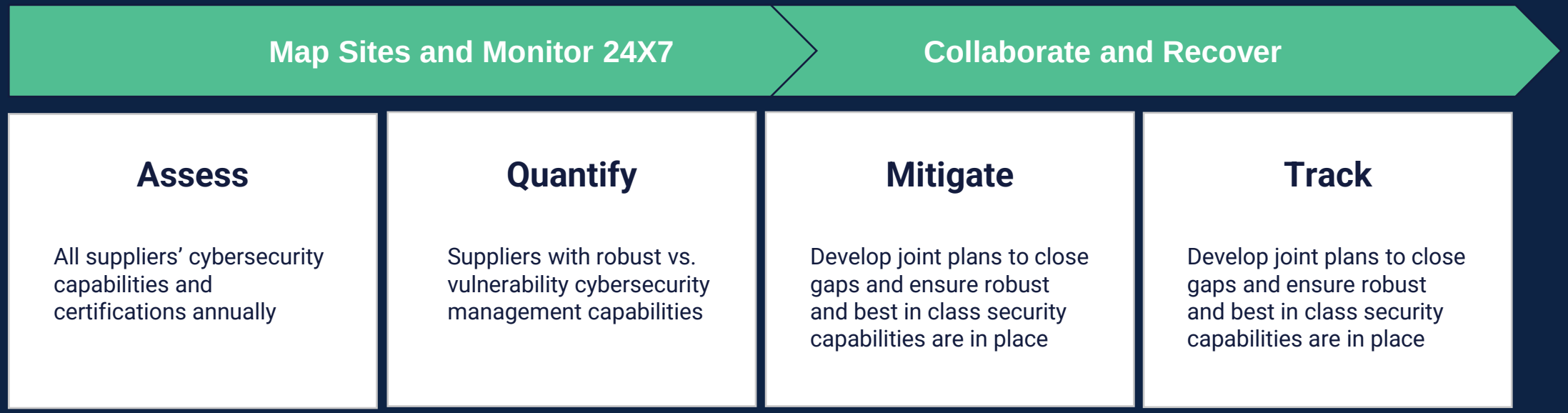
Resilinc's Governing Principles for Data Security and Privacy

1. Trust is everything. We only get one chance and we lose it forever
2. Be **more** paranoid than our most paranoid customer
3. Data remains property of sharer. They decide who to share it with

- Global Exchange of Data
- Interconnected Systems & Business
- IoT & Industrial Control Systems
- Intellectual Property
- Multi-tier Supply Network
- Brand Value
- Shareholders Confidence
- Financial & Revenue Impact

resilinc

Suppliers’ Information Systems Have Many Vulnerabilities



resilinc

Resilinc Supplier Assessment Library: all in one system

Your experts don't need to waste time getting supplier data out of multiple systems

Use from our Library of Assessments, or Create your Own

VISIBILITY
Sub-Tier Supply Chain Mapping
Part-Site Mapping
Material Flow Mapping

REPUTATION
Supplier ESG & Sustainability
Supplier Code of Conduct
Supplier Screening

COMPLIANCE
REACH, RoHS, WEEE, FCPA
Brexit Readiness Assessment
UK Modern Slavery Act
California Supply Chain
Transparency Act

READINESS
Hurricane Readiness
Factory Fire Readiness
Pandemic Readiness

SECURITY
Cyber Security & GDPR
Supplier C-TPAT Assessment
COPE* for Insurance

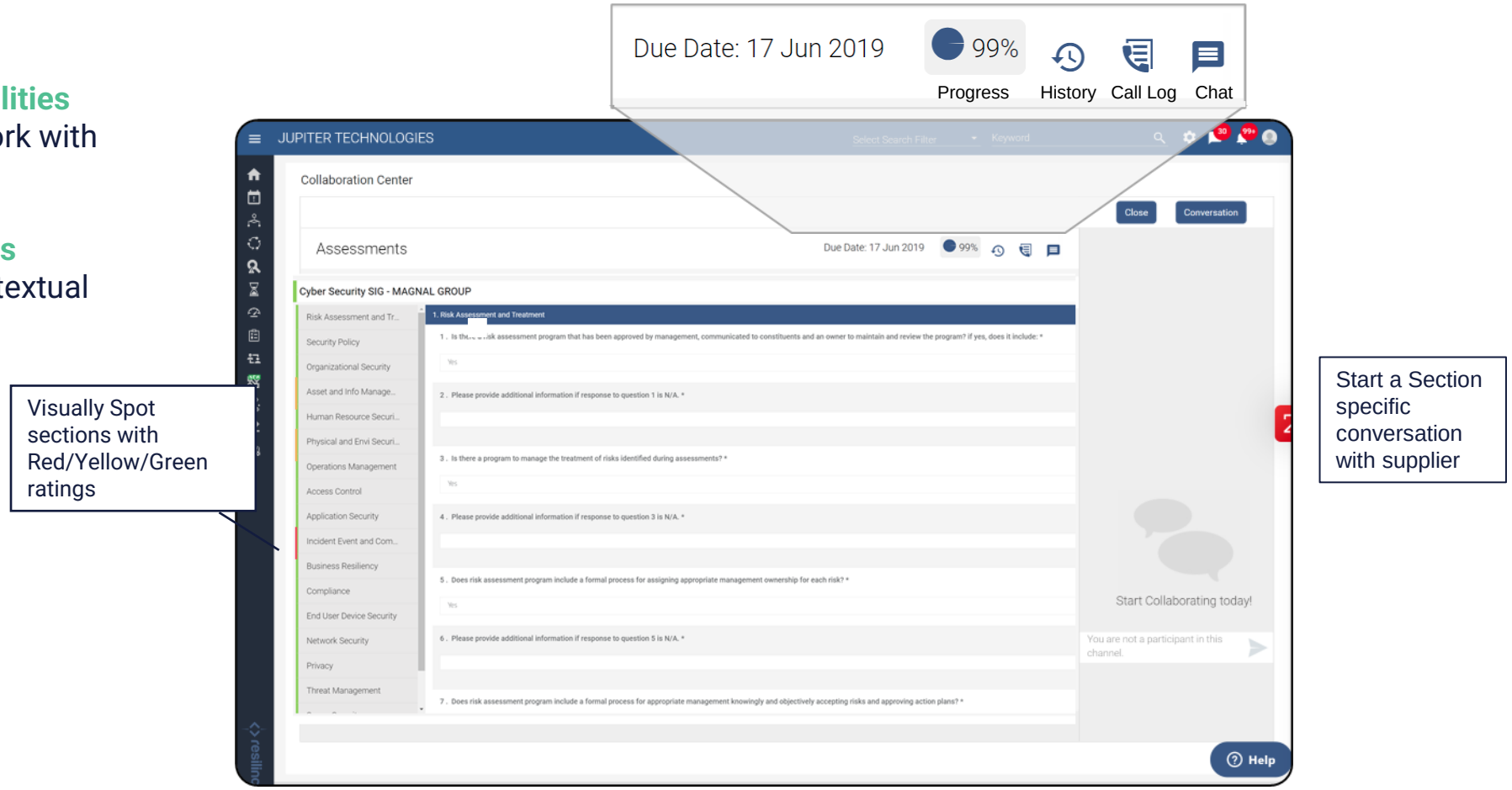
CONTINUITY
Corporate Business Continuity Program
Supplier Site BCP Assessment
Backup site and Recovery Time

resilinc

Collaborate, Audit, Track Progress Over Time

Uncover hidden vulnerabilities with assessments and work with supplier to fix them.

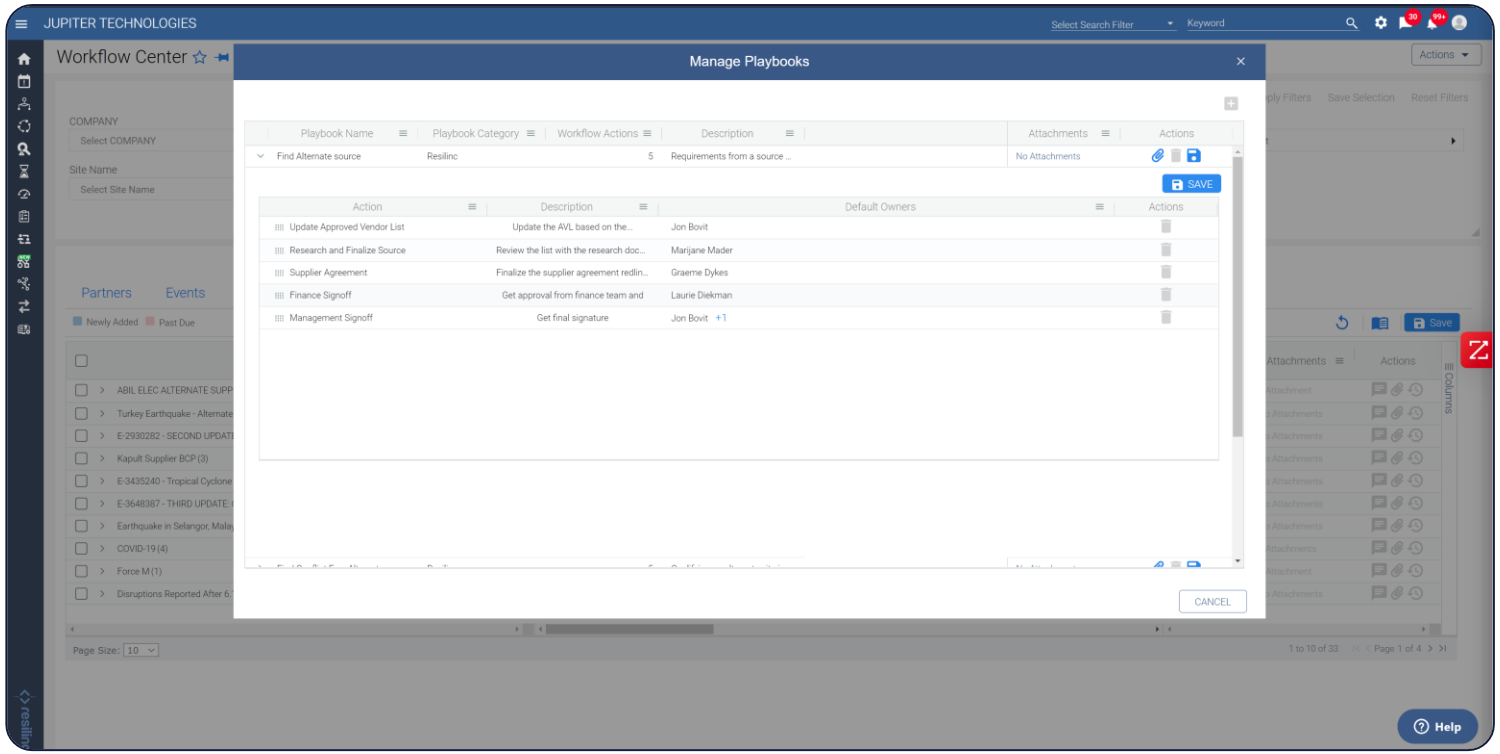
Audit history and progress recorded over time – contextual rather than over email.



resilinc

Model your Cyber Processes with Workflows functionality

- **Automatically assign actions** and start mitigating Cybersecurity risks
- **Eliminate ambiguity** in areas of responsibility when mitigating Cybersecurity incidents
- **Centrally monitor all activities** related to Cybersecurity incident management
- **Provide timely and relevant updates** to your customers, executives, and other key stakeholders



resilinc

Thank You!

Got feedback? We want to hear it at specialreports@resilinc.com

resilinc