CZ4064
Security Management
Project 5 Group 2

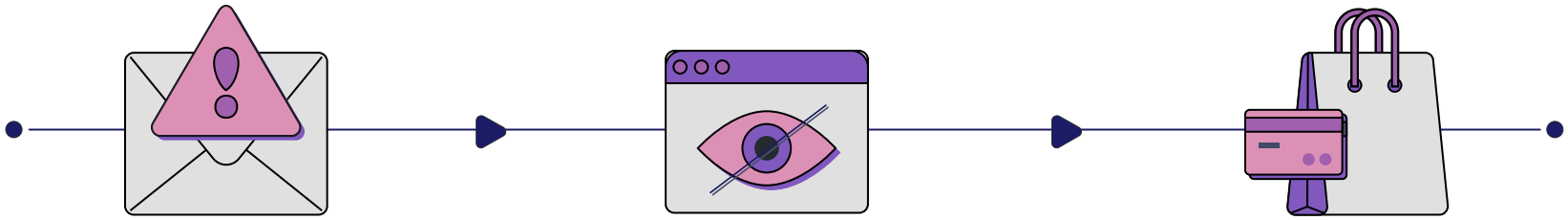
Addressing Cyber Supply Chain Security Risks

Noel
Yan Shiun
Sanskar
Kshitij
Cheng Yin
Bryan

1

Introduction

Introduction



Security of Cyber Supply Chain

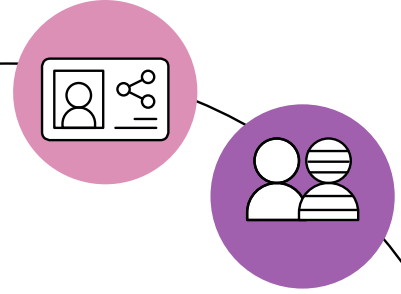
- Dependency on interconnected digital systems
- Concerns on integrity and security

Software Supply Chain Attacks

- Compromise integrity of software
- Exploit processes involved in creating, distributing or updating software

Overview of Study

- Case studies conducted
- Analysis on threats, vulnerabilities and risk

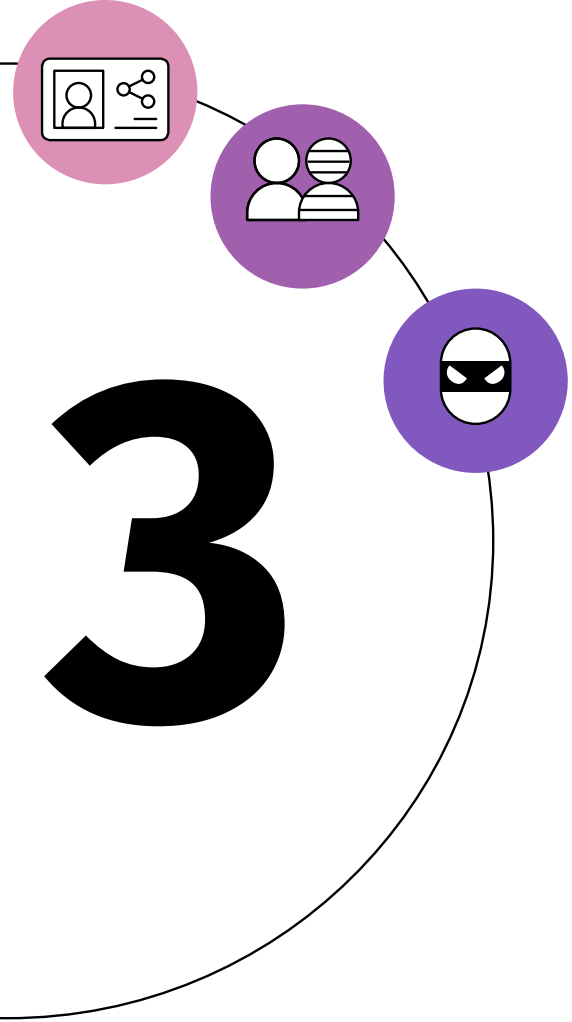


2

Purpose

Purpose

- Find out the security risk involved in software supply chain attacks
- Compare the aforementioned security risk with conventional security risk
- Essentials factors organizations should consider when managing such risk
- Study and suggest security strategies and effective measures that organizations should consider implementing
- Suggest a metric to measure success of strategies

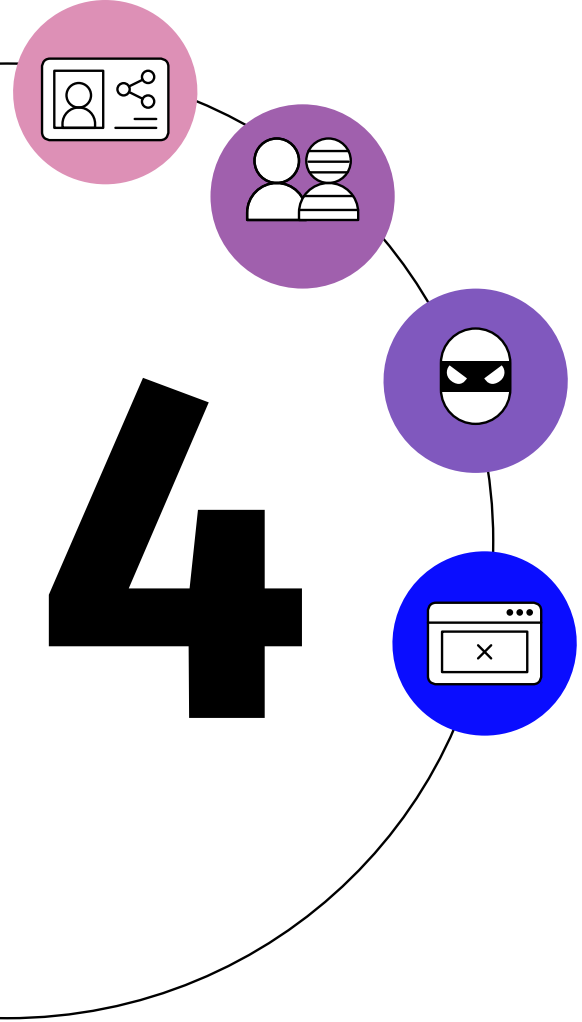


3

Scope

Scope

- To provide information to organizations and the relevant personnels
- At organizational level: any organizations that utilizes third-party software services
- Inclusive Audience: individuals who have engaged in the design, development, integration, deployment, and maintenance of software within the organization.

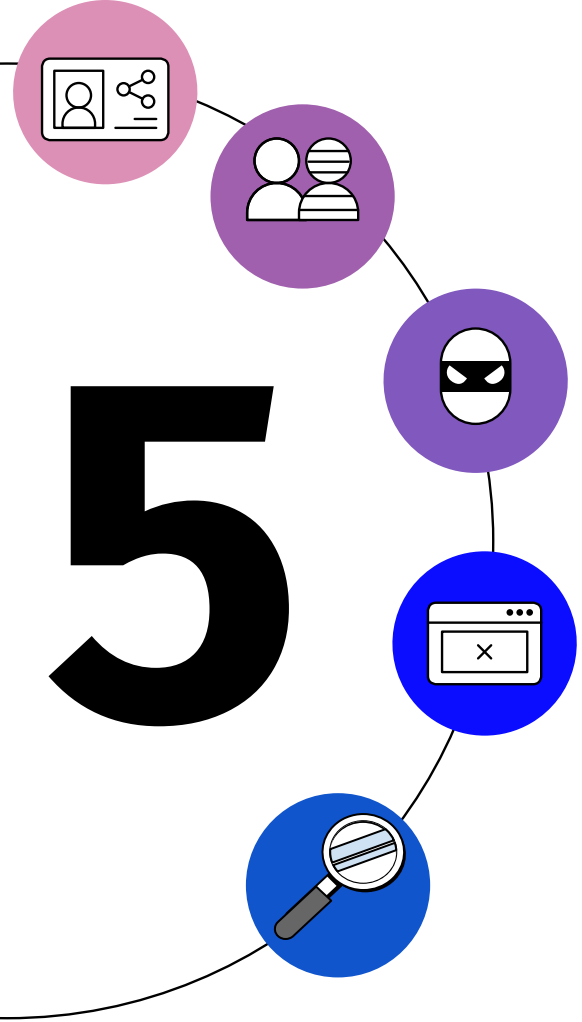


4 Methodology

Methodology

Our research was guided by:

- Existing recommendations and best practices with cybersecurity standards like NIST
- Literature Review
- Studying real world cases like Operation Shadow Hammer , SolarWinds and Kaseya

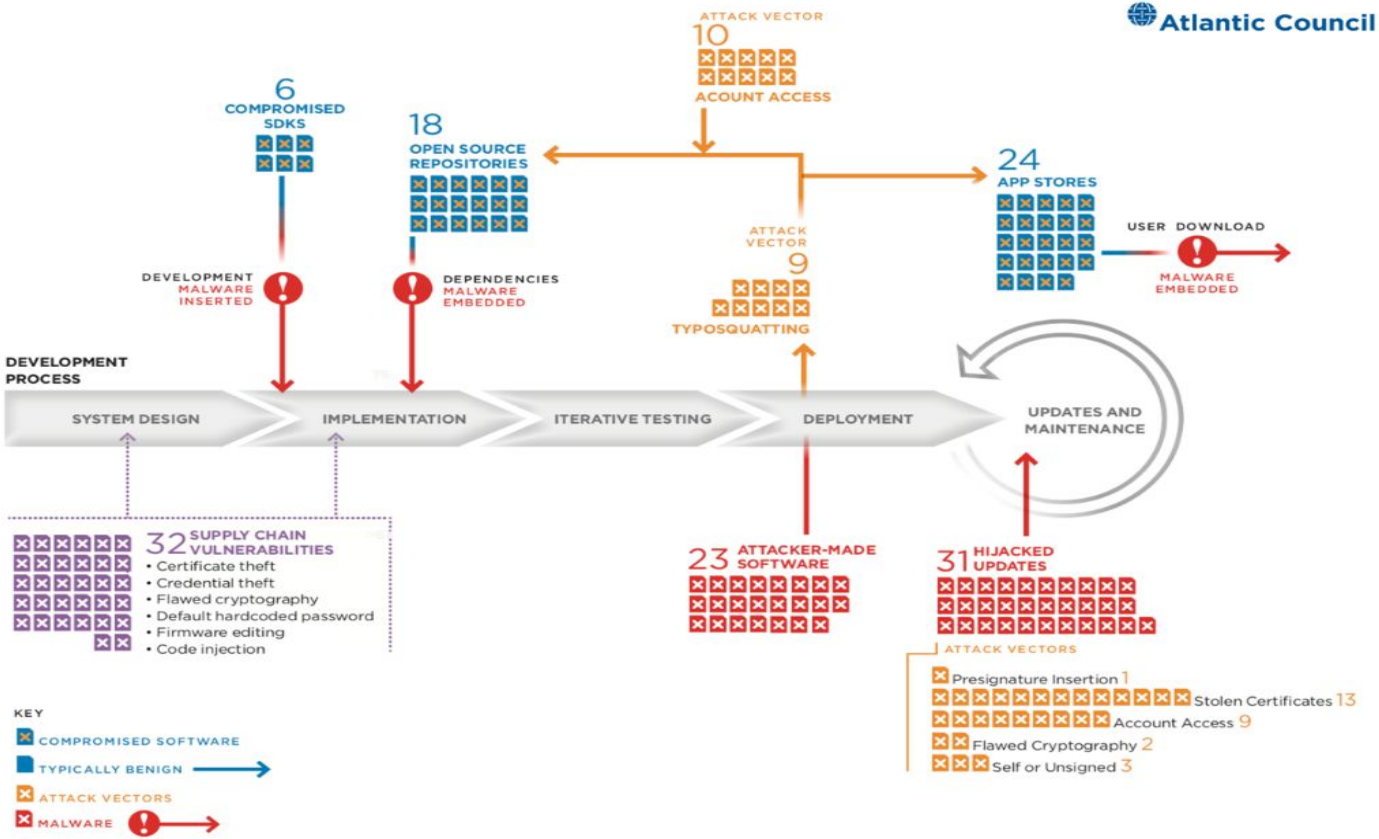


5 Findings and Analysis

Vulnerabilities Identified from Case Studies

	Dependency Confusion	Zero-Day Exploits	Compromised Updates	Backdoors	Web application vulnerability
Where & When	NPM and PyPI (2021)	Kaseya (2021)	SolarWinds (2020)	Operation ShadowHammer (2018)	Equifax (2017)
Attack vector	Overriding privately used software packages (dependencies) – with malicious, public packages of the same name.	Multiple zero-day vulnerabilities were exploited, including an authentication bypass flaw and an arbitrary command execution vulnerability.	Malicious code was inserted into the SolarWinds Orion software update.	Injected malicious backdoors into legitimate software updates	A vulnerability in the Apache Struts software allowed attackers to exfiltrate PII of around 150 million individuals.

Software Supply Chain Life Cycle



Common attack techniques

Undermining Code signing

Compromising integrity of code and identity of its author

Open source compromise

Malicious packages

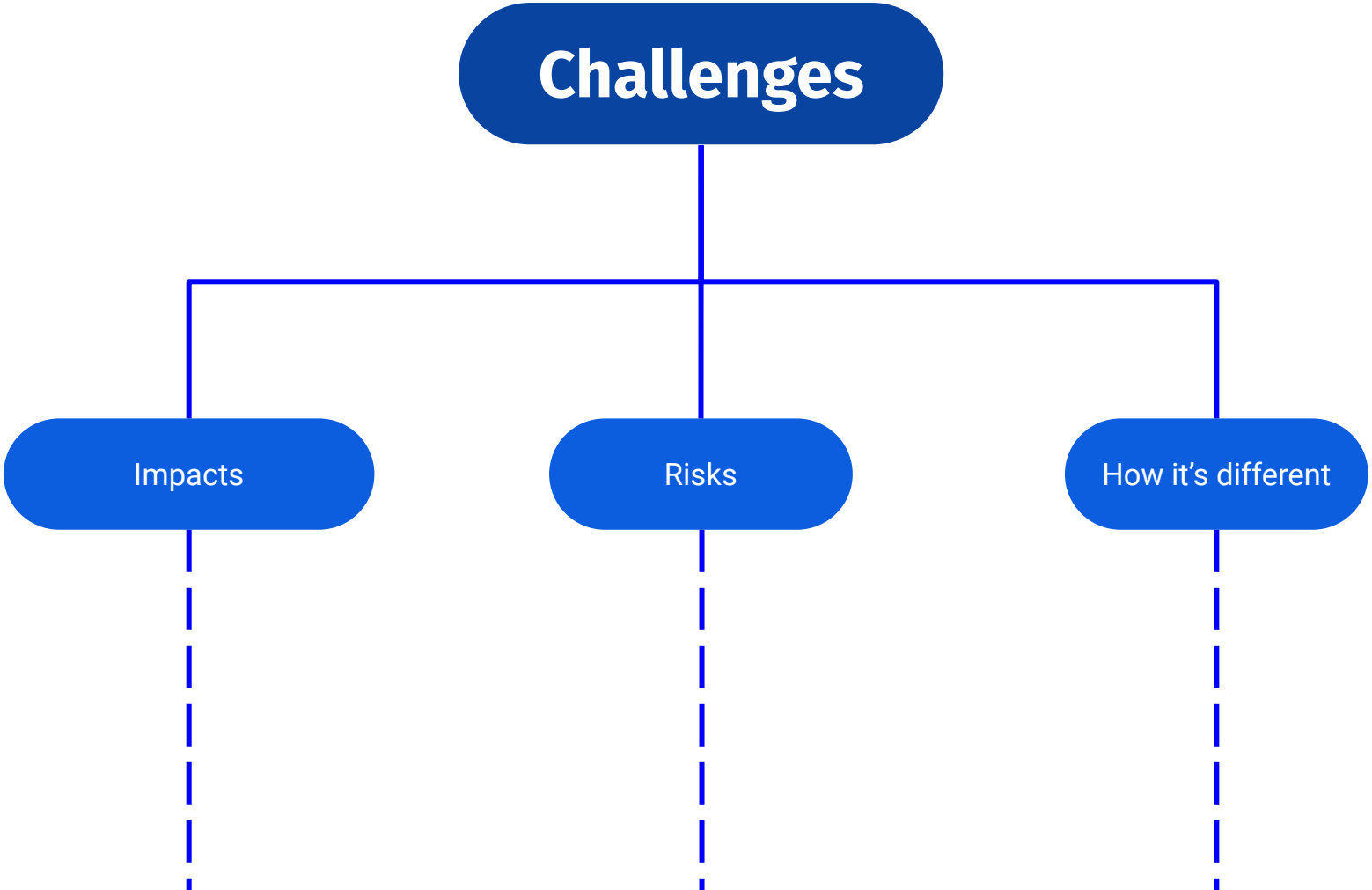
Hijacking updates

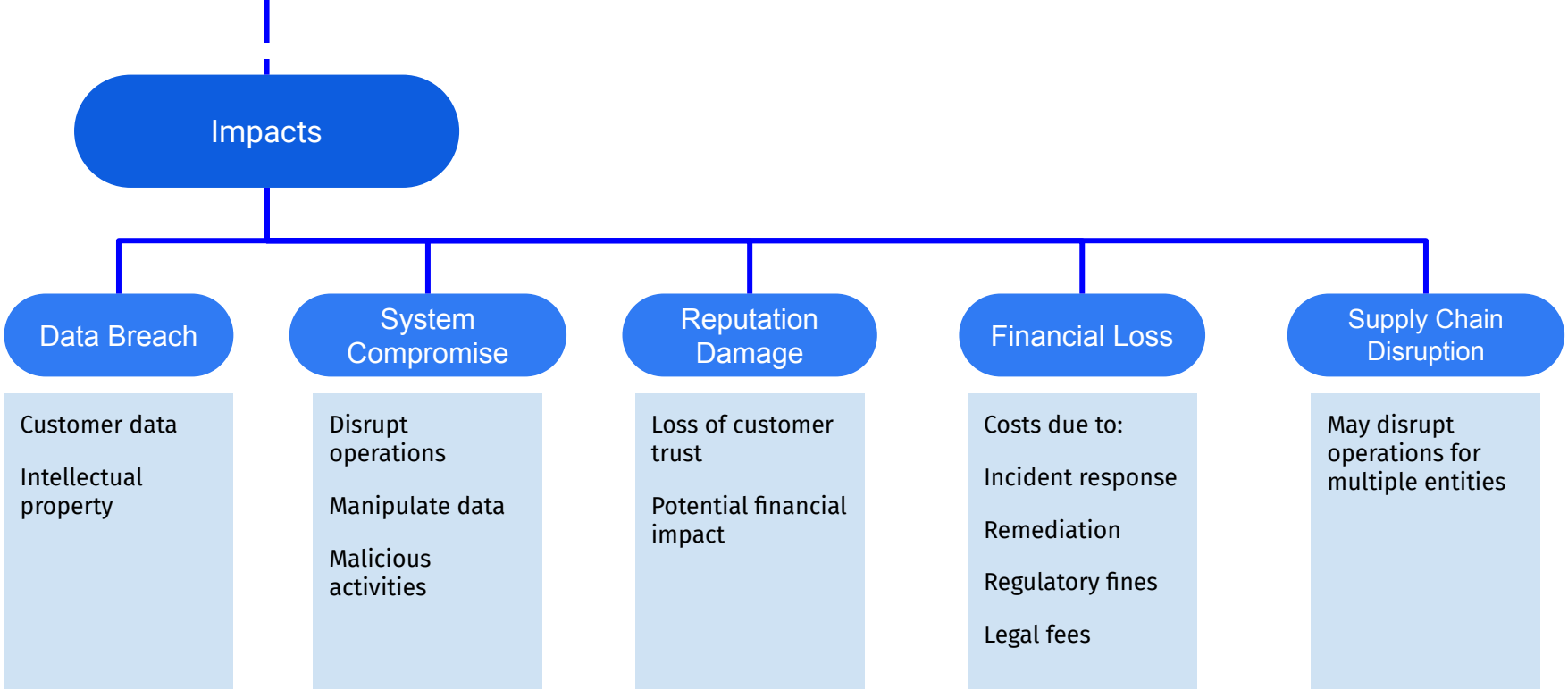
Carry malware to targets

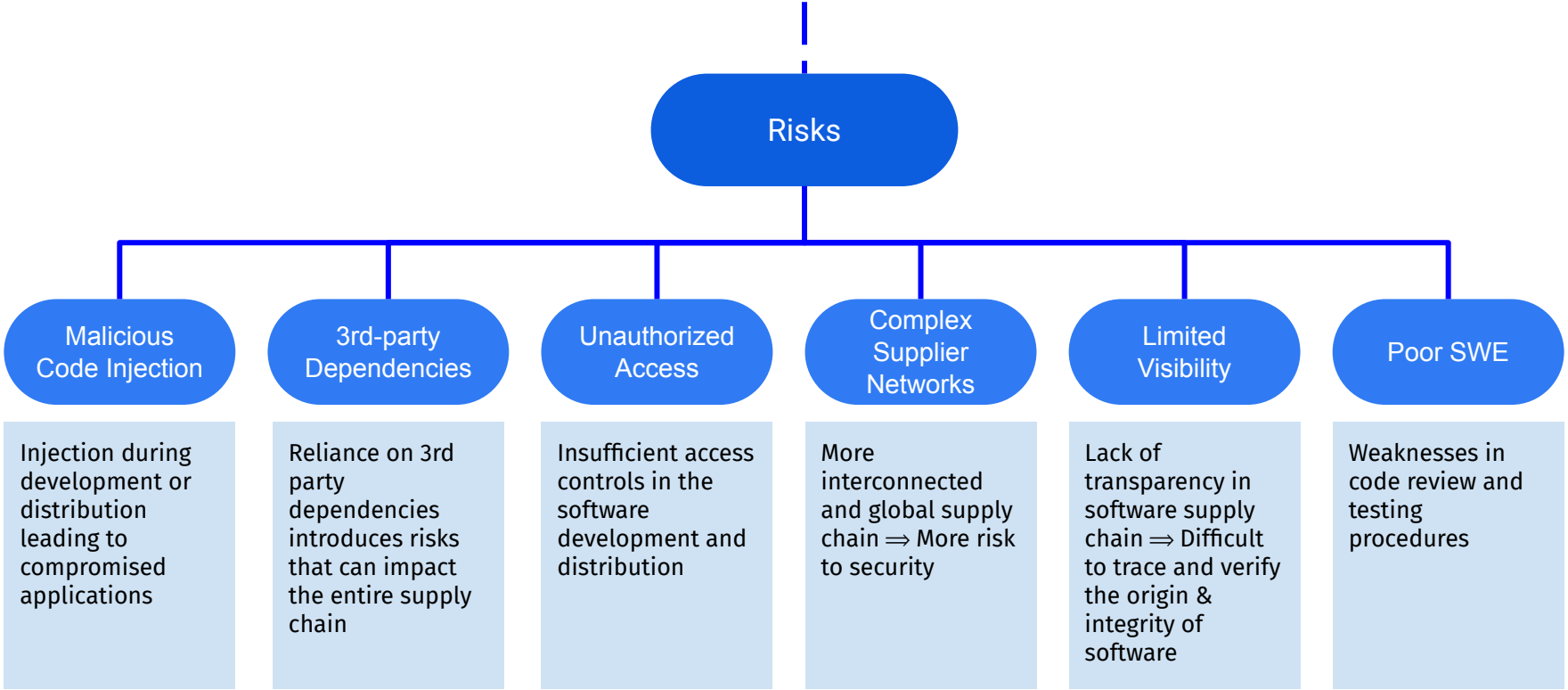
App store attacks

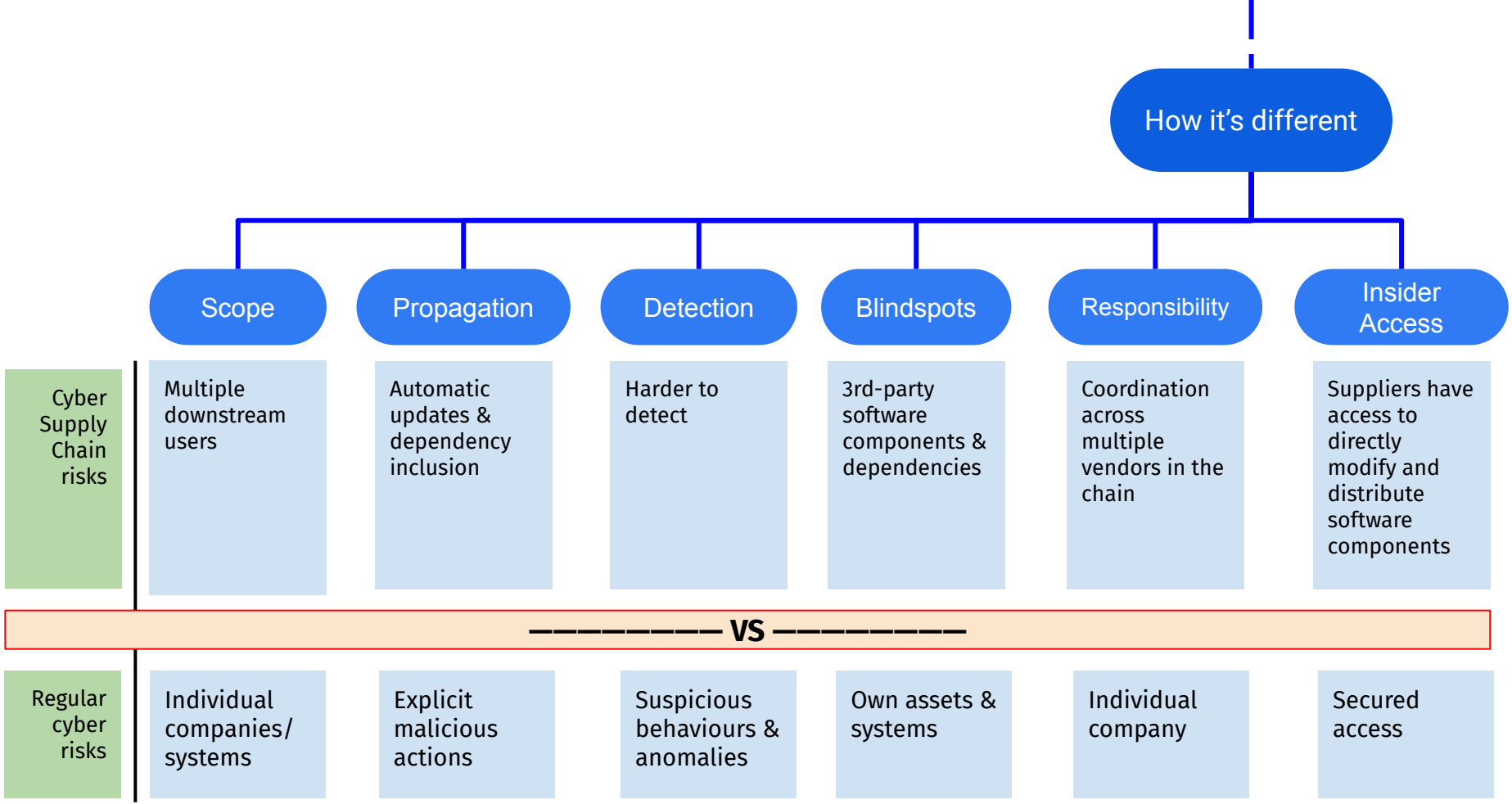
Spread malware through mobile apps

Speaker: Malavade Sanskar Deepak

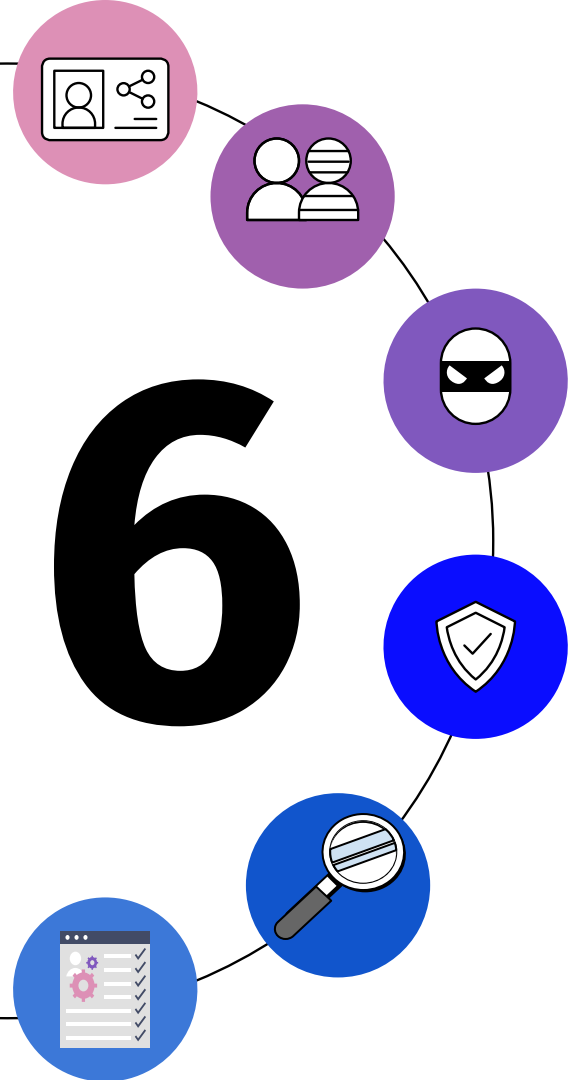








Parashar Kshitij



Recommendation

Recommendation

Detection

- Comprehensive Supply Chain Risk Management (C-SCRM)
- Signature Based Threat Detection
- Behavior Based Threat Detection
- ML Based Threat Detection

Mitigation

- Software Updates
- Access Control
- Backup and Recovery
- And much more ...

Proposal Strategy

ML Based Threat Detections

Training Effectiveness

Comprehensive Supply Chain Risk Management (C-SCRM)

Measurement of Success (Metrics/Output)

Incident Response Metrics
MTTD & MTTR,
No of Incidents

Vendor Risk Metrics
Risky Vendor,
Percentage of vendor

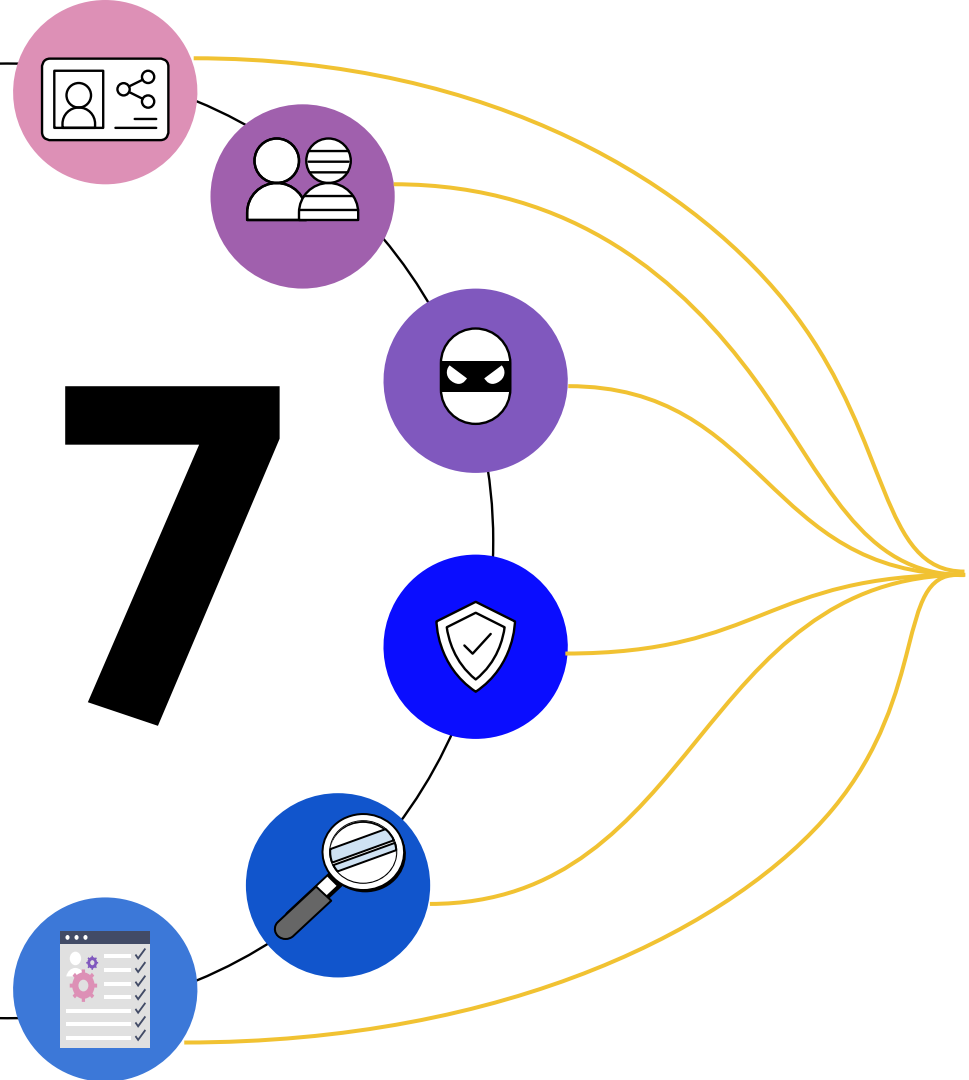
Monitoring Metrics
Number of attack,
False positive rate

Training Effectiveness
Employees knowledge

Supply Chain Resilience
Critical Supplier,
Time to recover

Compliance Metrics
Cybersecurity Standard,
Vulnerabilities addressed

Bryan



7 Conclusion

Key Takeaways

- Identification of vulnerabilities
- Evolving threat landscape
- Unique Characteristic

Bryan

Important Considerations

- Potential blind spots
- Ongoing Changes
- Emerging technologies
- Budget Considerations
- Supply chains complexities
- Human element

Bryan

Questions?