DEVCONNECT 2021

22 June 2021

Mitigating risk and strengthening security through partnerships

Mira Golsteijn

Information Security Manager,

EMEA & APAC, OCLC

Tina Price

Security Governance Program

Director, OCLC

OCLC

Anna Jones

Community Manager, OCLC

Mira Golsteijn

Information Security Manager
EMEA & APAC, OCLC

Tina Price

Security Governance Program
Director, OCLC

Today’s agenda

The evolution of the internet and its impact

Defining the concept of risk

Assessing and managing supply chain risk

Mitigating risk with contracts and cybersecurity insurance

THE EVOLUTION OF THE INTERNET AND ITS IMPACT

The evolution of the internet

1983 The internet was standardized, permitting worldwide proliferation of interconnected networks

The evolution of the internet

1983 The internet was standardized, permitting worldwide proliferation of interconnected networks

2020 More than 4.5 billion people now use the internet

The evolution of the internet

1983 The internet was standardized, permitting worldwide proliferation of interconnected networks

2020 More than 4.5 billion people now use the internet

2020 Total losses from cybercrime globally now over $1 trillion (Source: McAfee, 2020)

OCLC

The evolution of the internet

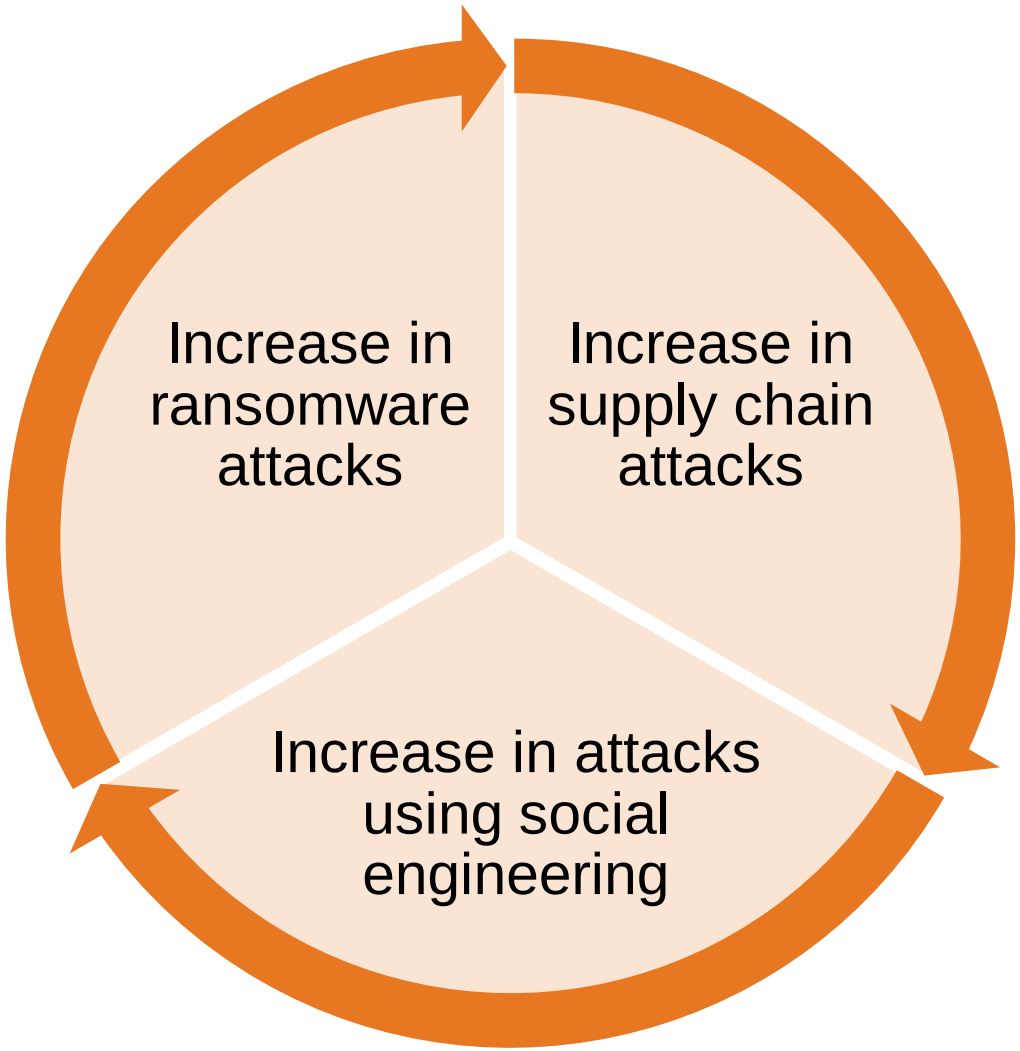
1983 The internet was standardized, permitting worldwide proliferation of interconnected networks

2020 More than 4.5 billion people now use the internet

2020 Total losses from cybercrime globally now over $1 trillion (Source: McAfee, 2020)

2020 Annual increase of losses as a result of cybercrime is greater than 25%

Trends in cybercrime



Recent global headlines

Nedbank's Third-Party Data Breach Impacts 1.7 Million Customers in South Africa

By **CISOMAG** - February 20, 2020

SHARE Facebook Twitter G+

Source: Cisomag, February 2020

PRIVACY & SECURITY

Ontario regional government victim of third-party cyberattack

HOWARD SOLOMON APRIL 9, 2021

Source: Itworldcanada.com, April 2021

Malaysia Airlines hit by 'data security incident' via third-party IT service provider

Incident occured at some point during nine-year period between March 2010 and June 2019

James Henderson (Channel Asia)
02 March, 2021 14:53

FOLLOW US

EVENTS

Channel Asia WIICTA 2021

Nominations Open

Source: Channel Asia, March 2021

04/07/2021

RaceTrac & Shell Impacted by Third-Party Cybersecurity Incident

Unauthorized parties accessed certain data stored in Accellion's File Transfer Appliance.

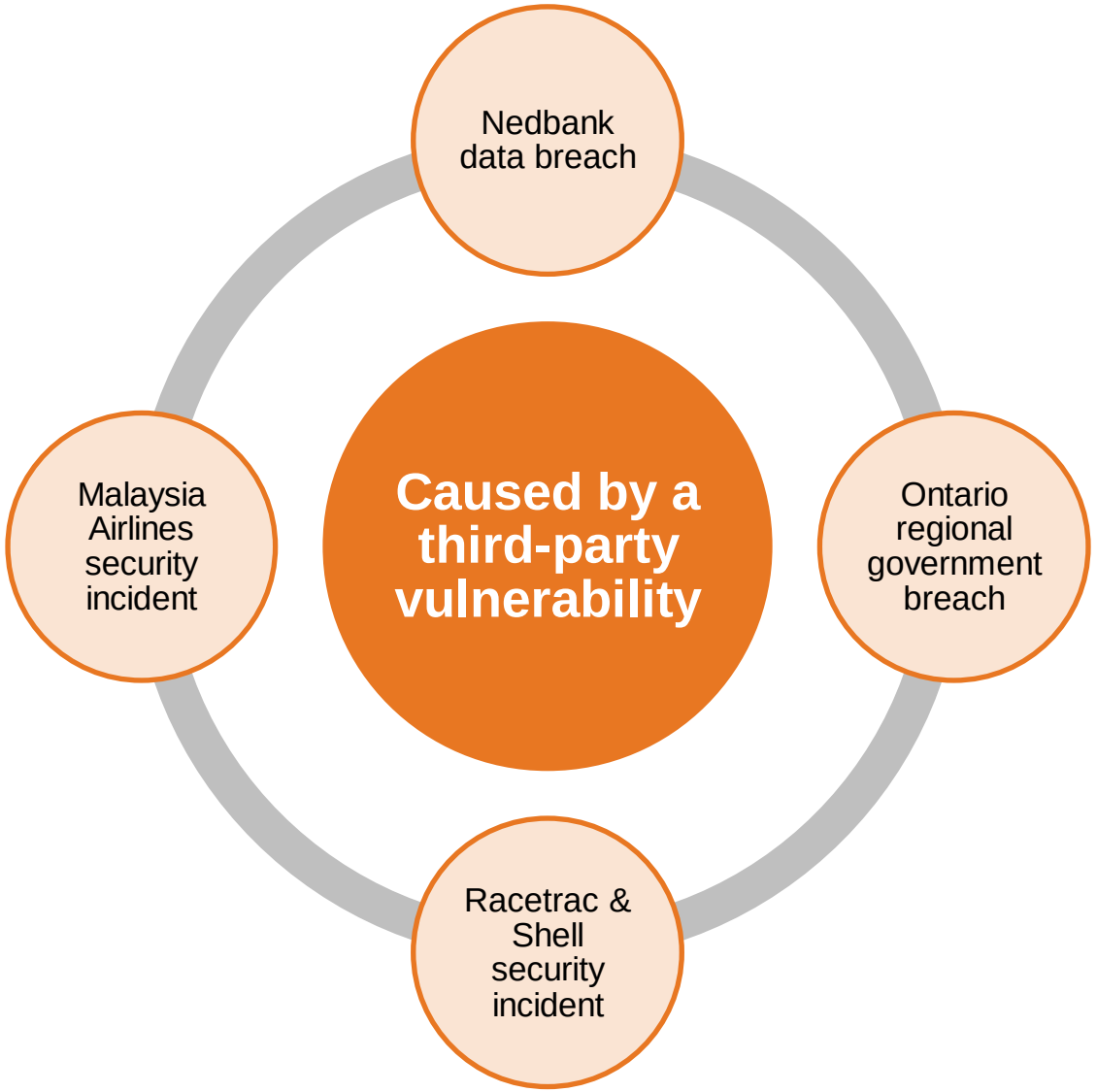
ATLANTA and HOUSTON — RaceTrac Petroleum Inc. and Shell Oil Co. announced they have been impacted by a security incident affecting third-party service provider Accellion Inc., a technology company that specializes in secure file sharing and collaboration.

RaceTrac stated that unauthorized parties were able to access a subset of RaceTrac data stored in the Accellion File Transfer Appliance by exploiting a previously undetected software vulnerability. This includes email addresses and first names of some RaceTrac Rewards loyalty users.

Source: CSNews, March 2021

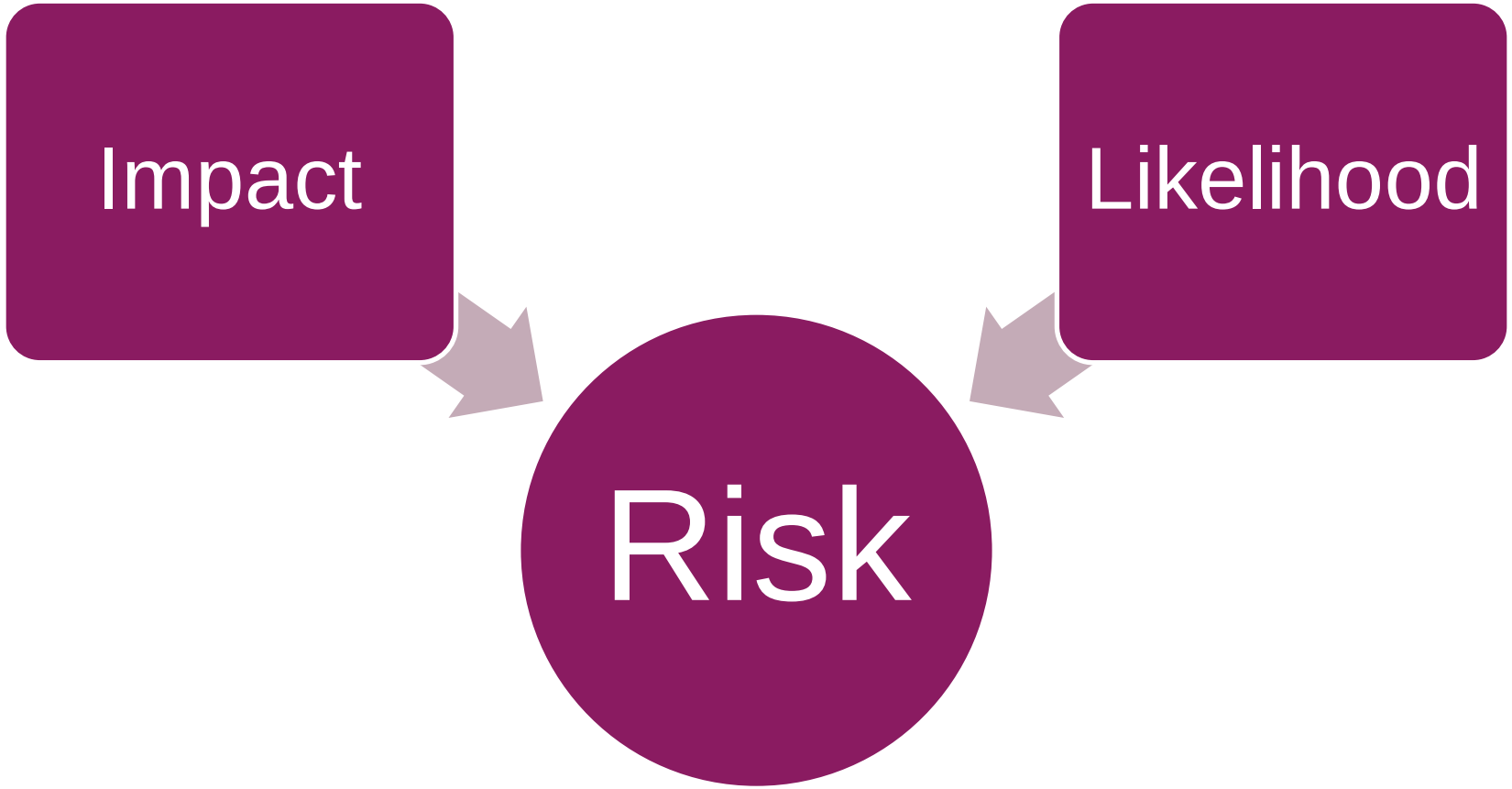
OCLC

The common denominator

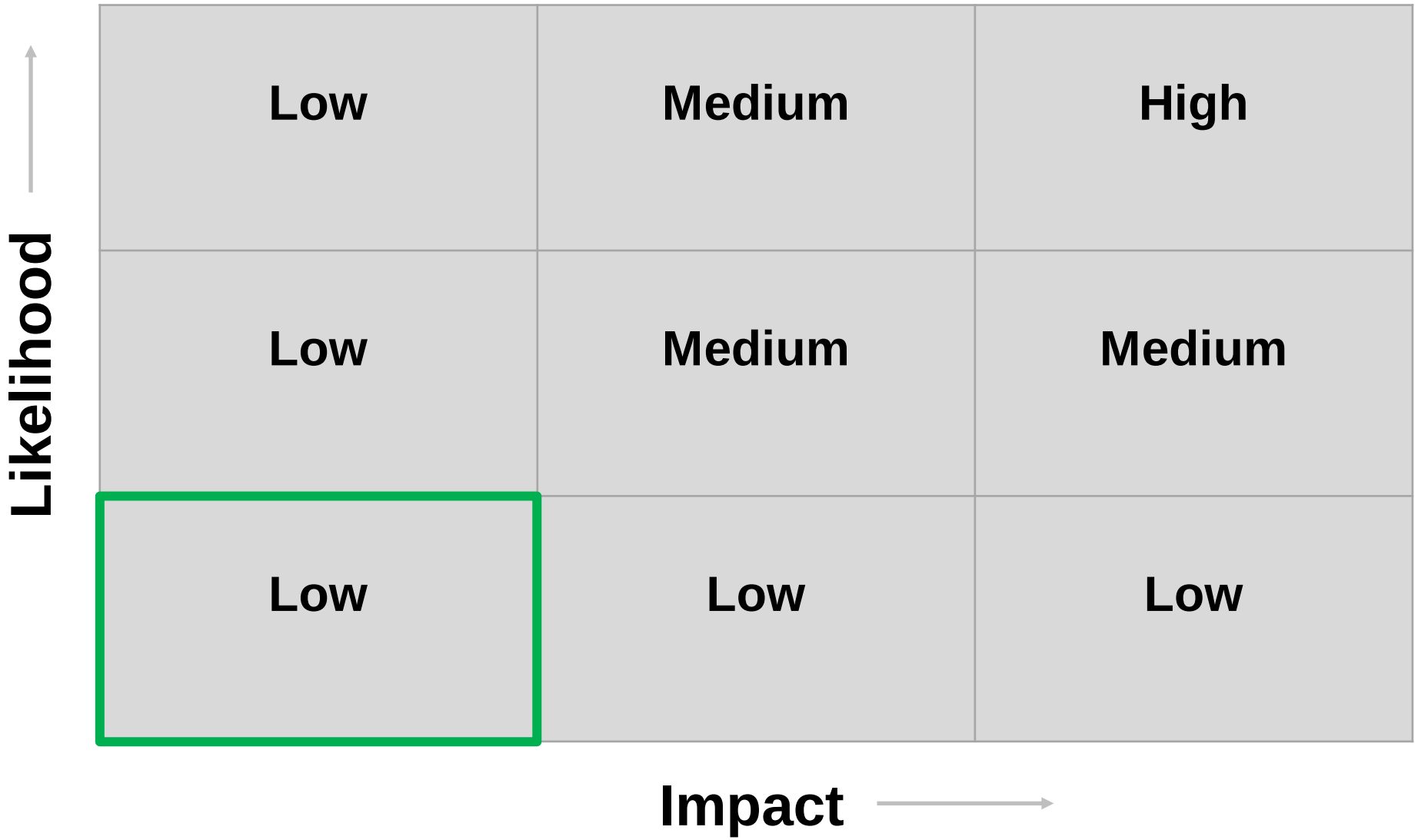


DEFINING THE CONCEPT OF RISK

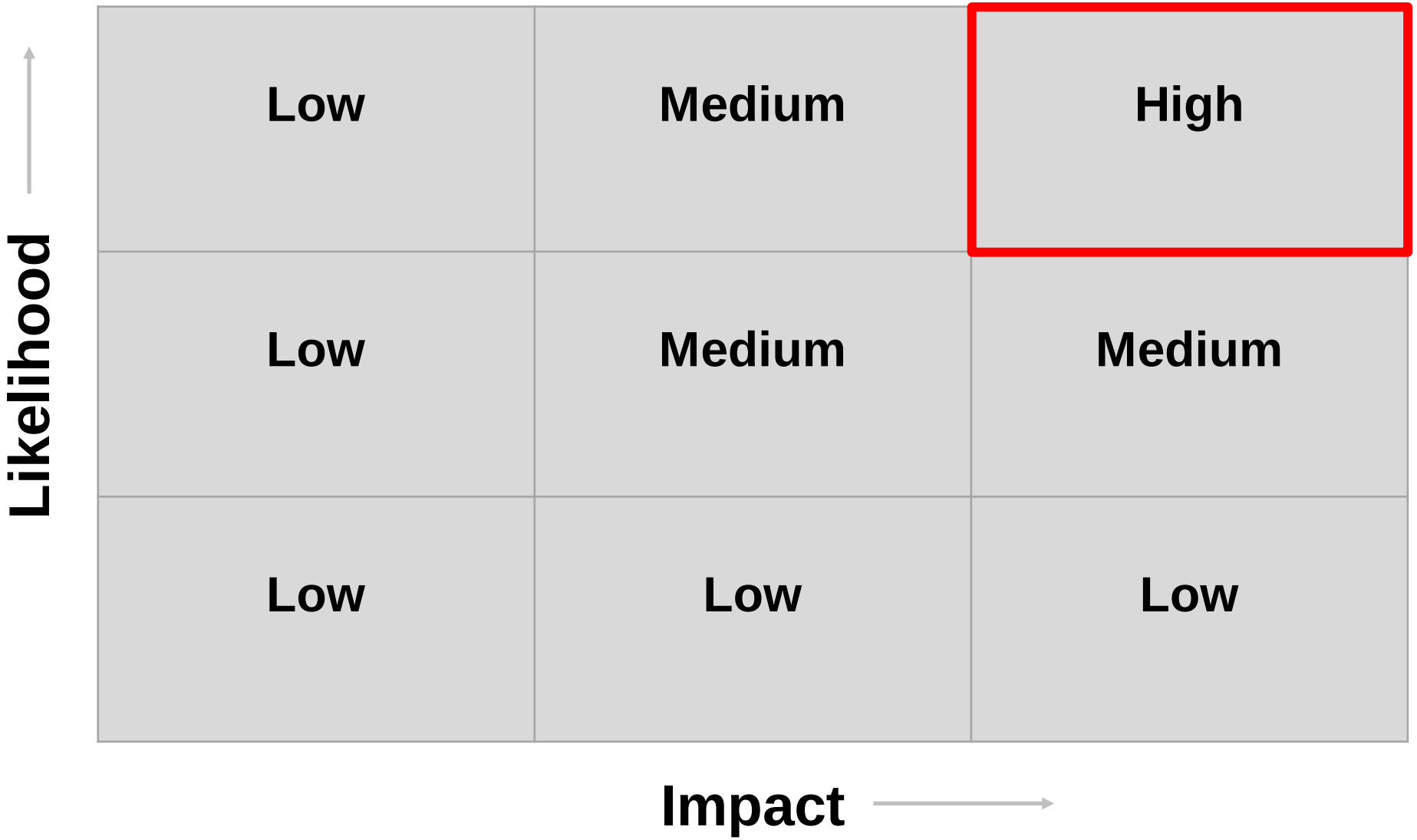
Assessing risk



Assessing a low-risk event



Assessing a high-risk event



Risk is never isolated

Photo by Cytonn Photography on Unsplash

ASSESSING AND MANAGING SUPPLY CHAIN RISK

What is Supply Chain Risk Management (SCRM)?

SCRM is the process of analyzing and minimizing risks associated with outsourcing to third party vendors or service providers because they may have access to intellectual property and sensitive data.

SCRM reduces the risk of doing business

Photo by FLY:D on Unsplash

RISK IS INEVITABLE

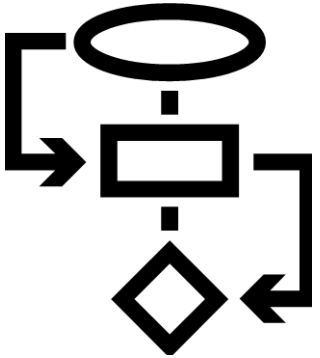
The only way to completely eliminate supply chain risk is to avoid working with external suppliers and how realistic is that?

Key elements of the SCRM process

1. Create a supplier inventory

Create a list of active suppliers (start with accounts payable)

Identify high risk suppliers that have access to your systems and data



Develop a process to review inventory and add / remove suppliers

Key elements of the SCRM process

1. Create a supplier inventory
2. **Develop a risk register (what could go wrong)**

A risk register is a catalog of risks that a supplier can expose your organization to

What if a supplier goes out of business?	**What information would cause disruption if unavailable?**	**What are potential targets or crown jewels?**

Key elements of the SCRM process

1. Create a supplier inventory
2. Develop a risk register (what could go wrong)
3. **Perform a supplier risk assessment**

Once you understand the risk a supplier presents, check that the supplier has the proper controls in place to manage the risk.

Supplier risk assessment methods

- Audit report findings (SOC2, PCI, etc.)
- Financial statements (breach, lawsuit)
- Internet search
- Security questionnaires
- Third party risk management software

Photo by Christian Wiediger on Unsplash

Key elements of the SCRM process

1. Create a supplier inventory
2. Develop a risk register (what could go wrong)
3. Perform a supplier risk assessment
4. **Review supplier risks and make risk treatment decisions:**
    - **Mitigate**
    - **Transfer**
    - **Accept**

Driving supplier behavior with contracts

- Risk mitigation
- Liability
- Breach definition
- Non-disclosure
- SLAs
- Remediation expectations

Photo by Scott Graham on Unsplash

Van Halen supplier contract

"There will be no brown M&Ms in the backstage area, upon pain of forfeiture of the show, with full compensation."

Source: https://www.npr.org/sections/therecord/2012/02/14/146880432/the-truth-about-van-halen-and-those-brown-m-ms

“… they didn’t read the contract.”

“So, when I would walk backstage, if I saw a brown M&M in that bowl….we’ll line check the entire production. Guaranteed you’re going to arrive at a technical error…they didn’t read the contract.”

David Lee Roth of the band Van Halen

MITIGATING RISKS WITH CYBERSECURITY INSURANCE

Cybersecurity insurance

Cyber liability policies have been around since 2020

Mitigate losses from a variety of cyber incidents: Data breaches, business interruption, and network damage

Coverage depends on legislation and insurance policies

thank you

Stay connected

DEVCONNECT 2021

OCLC