Mitigating risk and strengthening security through partnerships

Mira Golsteijn
Information Security Manager, EMEA & APAC, OCLC

Tina Price
Security Governance Program Director, 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)
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

- Increase in supply chain attacks
- Increase in ransomware attacks
- Increase in attacks using social engineering
Recent global headlines

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

Source: Cisomag, February 2020

Ontario regional government victim of third-party cyberattack

Source: Itworldcanada.com, April 2021

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

Source: Channel Asia, March 2021

RaceTrac & Shell Impacted by Third-Party Cybersecurity Incident

Unauthorized parties accessed certain data stored in Accelion’s File Transfer Appliance.

Source: CSNews, March 2021
The common denominator

Caused by a third-party vulnerability

- Nedbank data breach
- Malaysia Airlines security incident
- Ontario regional government breach
- Racetrac & Shell security incident
DEFINING THE CONCEPT OF RISK
Assessing risk

Impact

Risk

Likelihood
Assessing a low-risk event

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medium</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medium</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medium</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medium</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Low likelihood and low impact result in a low-risk event.
Assessing a high-risk event

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
</tbody>
</table>
Risk is never isolated
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

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
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
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
“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