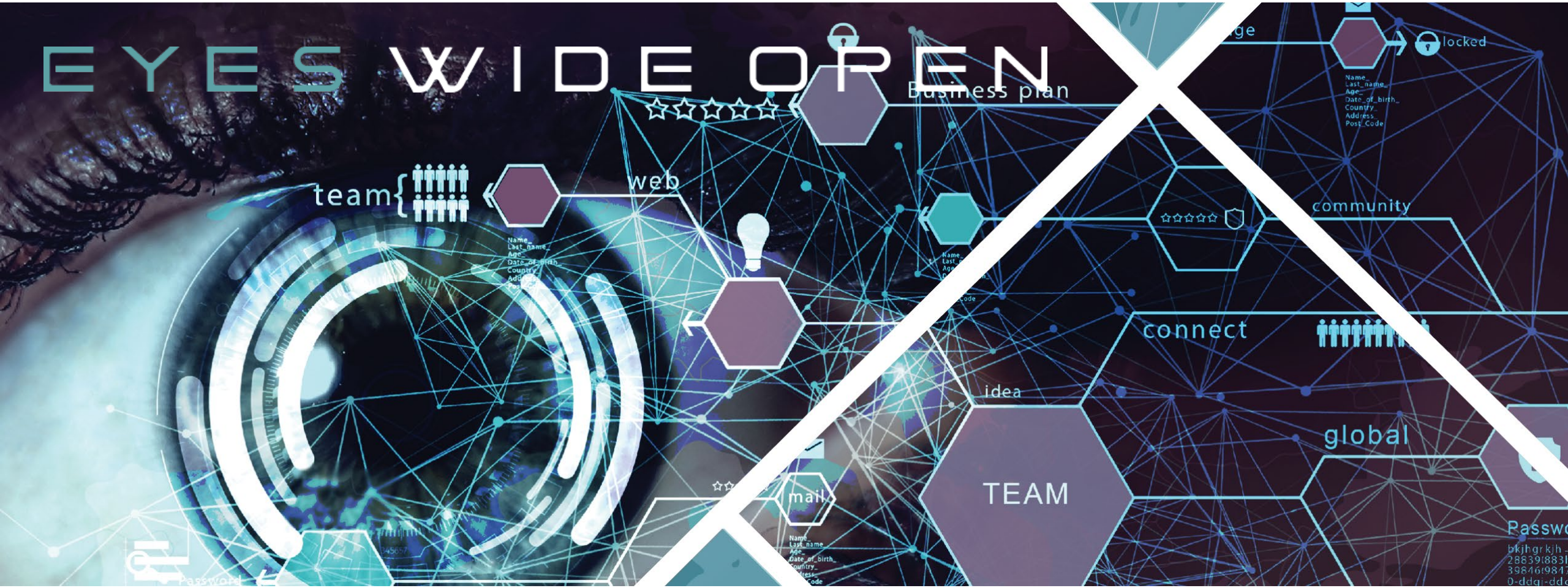
12TH ANNUAL LEADERSHIP EVENT

CYBER SECURITY SUMMIT

Security solutions through collaboration.™

TITLE SPONSOR

Island



Third-Party Risk

October 2022

Gretchen Block

CISO of UnitedHealthcare & SVP of Enterprise Information Security

Optum

Third-Party Risk

- Third-Party Risk Management
- Ransomware Control Considerations
- Third-Party Resiliency Considerations
- Q&A and Closing Remarks

Gretchen Block

Sr. Vice President of the Optum Global Technology Enterprise Risk Governance Program and the Chief Information Security Officer (CISO) for UnitedHealth Care.

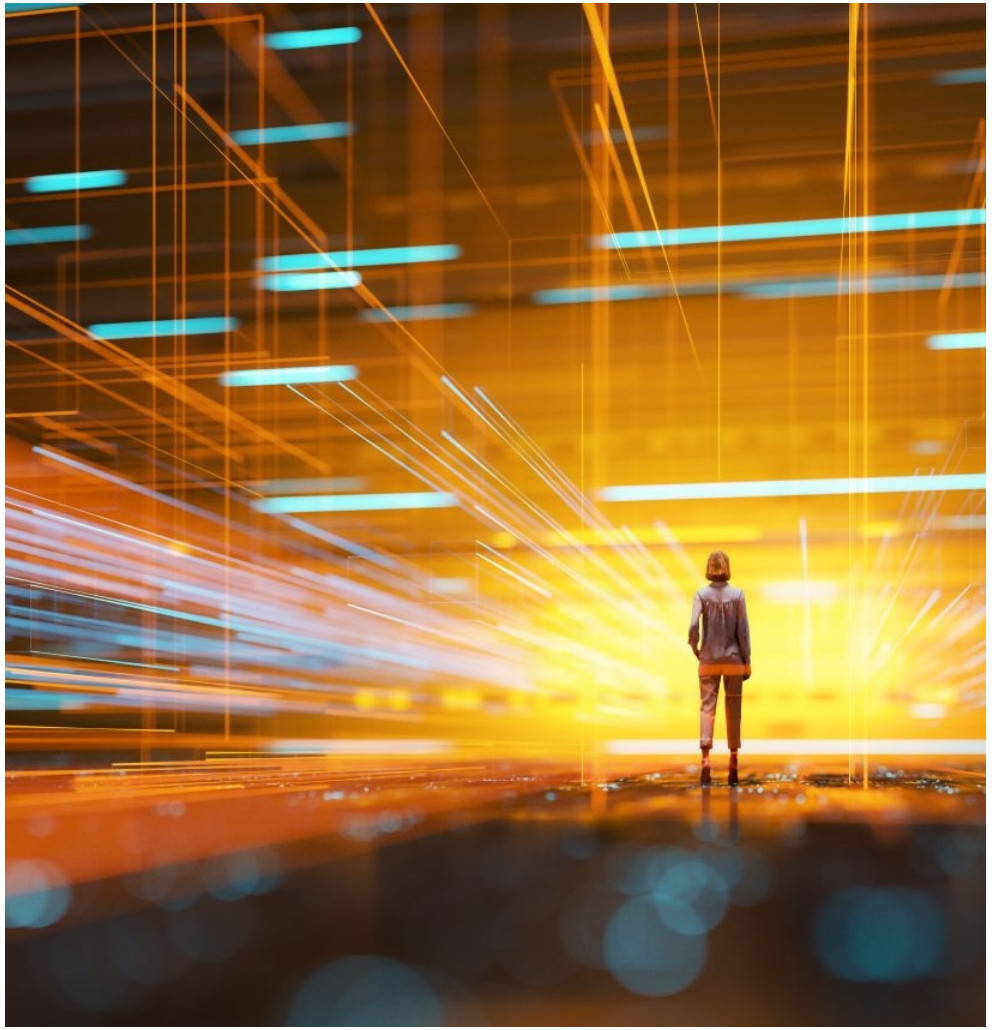
Third-Party Risk

Definition:

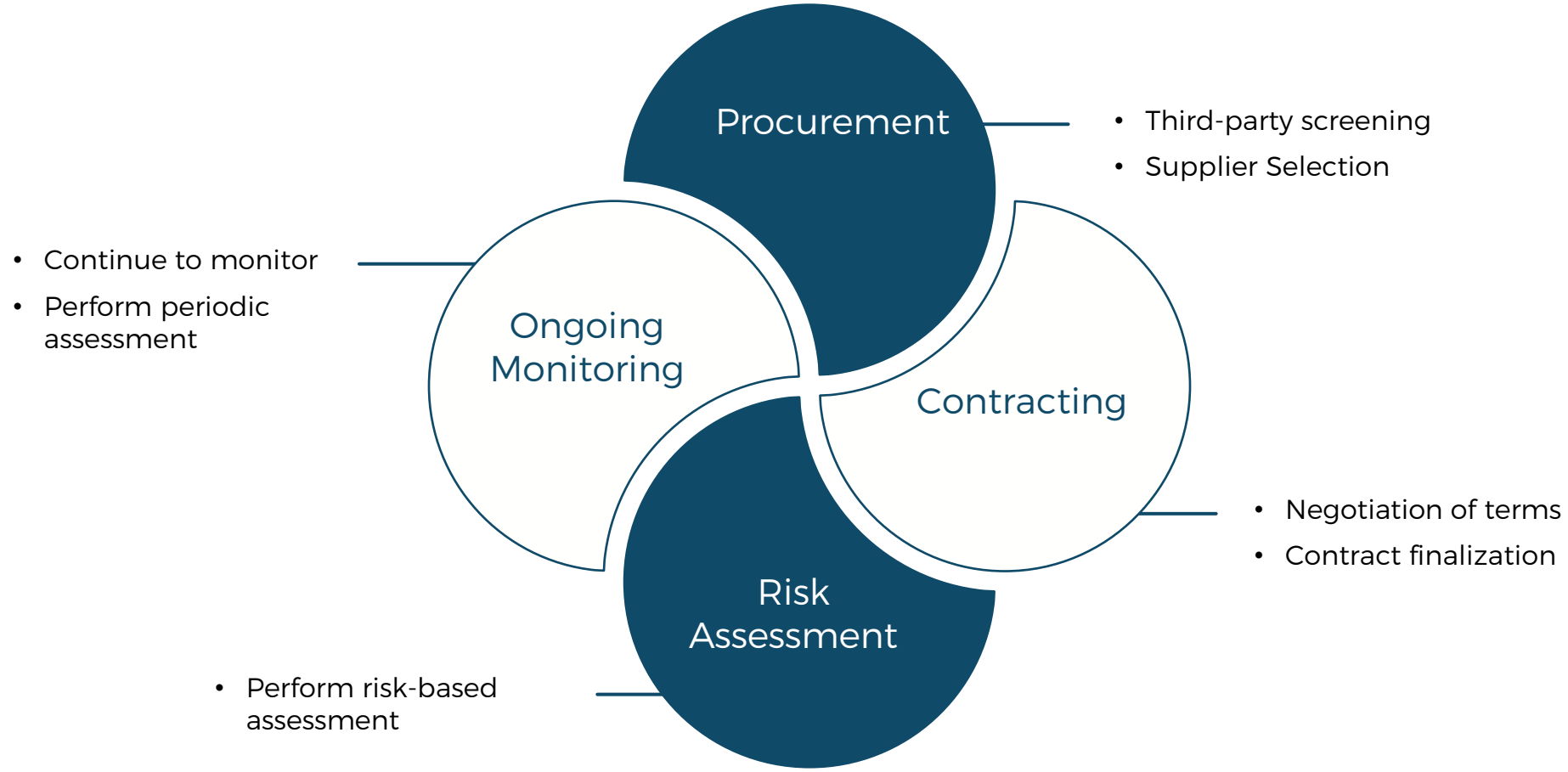
The risk that is brought into your organization's environment by an external party. Third-parties can be suppliers or contractors that act as a service provider and could have access to critical processes, customer data, or privileged information. An outage from a third-party could cause substantial impacts including revenue or data loss.

Increased Risk:

The Hackers are targeting larger enterprises through their smaller, less-sophisticated partners and subcontractors as attack vectors into their larger clients' networks.



Third-Party Risk management Ecosystem



Ransomware Control Considerations

With supplier ransomware and other cybersecurity incidents having an increased impact on organizations today, it is pivotal to focus on business-critical suppliers.

Information Protection Program	Endpoint Protection	Vulnerability Management	Network Protection	Incident Management
▪ Conduct background screening before authorizing access to information resources.	▪ Centrally-managed, up-to-date anti-spam protection is implemented. ▪ A formal policy or control is in place for mobile code protection and to ensure protective measures are in place and regularly updated	▪ An inventory of software inventories, and services are maintained	▪ The organization has a blacklist or whitelist model for restricting access to high-risk sites. The organization also forces outbound traffic to the Internet through an authenticated proxy server or equipment control on the enterprise perimeter. ▪ Network environment hosting data is isolated from corporation network environment	▪ The organization test and/or exercises its incident response capability Annually.

Third-party Resiliency Considerations

- **Identify the most critical suppliers** across your business that would cause the greatest impact to your business if they were completely unavailable.
- **Improve assessments methodology and reporting** on critical suppliers for resiliency including cybersecurity, business continuity, and disaster recovery
- **Ensuring business accountability** when engaging high risk suppliers
- **Develop deeper/robust Business Continuity strategies** across business areas dependent on critical suppliers (including downstream dependent applications or processes)
- **Develop enterprise level supplier response plans** that are connected to both the Enterprise Event Management response and the individual business continuity plans across the business
- **Improve Event Management** processes and support for command centers to better coordinate responses to supplier outages causing large scale impact

Q&A