Operational Technology Security

Capabilities enabled by
Azure Defender for IoT

pwc | Microsoft

What is Operational Technology (OT) and where is it found?

Operational Technology (OT) systems are combinations of hardware and software that **detect or cause a change to a physical device or process.** OT is **pervasive, and expanding** as firms continue to digitally transform and depend on automation the information generated by these systems. Below are examples of OT across a variety of industries:

Energy, Utilities, & Resources

- **Oil & Gas** – Boilers, Pressure Sensors, Drilling/Drilling Telemetry, Rig Stabilization, Leak Detection
- **Power & Utilities** – Wind turbines, Water Dams, Solar Farms, Nuclear, Natural Gas, Coal
- **Chemicals** – Furnaces, Pressure Sensors, Gas/Meteorological Sensors, Pipelines
- **Mining** – Autonomous Vehicles, Drills, Collapse Sensors/Alarms, Air/Water Quality Sensors, Lighting

Manufacturing

- **Food & Beverage** – Ovens, Fryers, Boilers, Actuators, Bottlers/Canners, Conveyor Belts, Palletizers
- **Automotive/Industrial** – Robotic Assembly, Painters, Conveyors, Material Handling Robots
- **Electronics** – Clean Room BMS, HMI's and Controllers

Healthcare

- **Medical Devices** – Pacemakers, Insulin Pumps, Patient Monitors
- **Pharmaceuticals** – Robotic Arms, Refrigerators, Packagers
- **Building Management Systems** – HVAC/Air Filtration, Lighting, Fire Suppression, Physical Access Control
- **Laboratory/Surgical Equipment** – Robotic Surgical Instruments, Imaging Scanners, Pharmaceutical Dispensers

Transportation & Logistics

- **Locomotive** – Train Track Switching, Defect Detectors, Height/Width Sensors, Weight Distribution Sensors, Locomotive Control System, Braking
- **Aerospace/Maritime** – Autopilot, Safety Control, Steering Control, Propulsion, Buoyancy Control, Port Management
- **Retail/Warehouse** – Conveyors, Palletizers, Material Handlers, Pickers, Refrigerators, Building Management Systems

How has digitization increased OT risk to organizations?

Historical Context

Operational technology predates the information systems era and initially consisted of isolated systems running proprietary control functions on specialized hardware/software and communication protocols. These have been replaced with the same products, systems and services already in use in the information technology domain: Windows operating systems running on Intel-based hardware and connected via TCP/IP networks.

~How to Organize Security and Risk Management in a Converged IT/OT Environment (Gartner)

Digital transformation, coupled with enterprise **need for data, specifically around resource planning**, led to a need to connect systems and transfer data more effectively. For OT systems, connecting legacy systems that had not previously been exposed to the enterprise network exposes new risk.

OT Data Generated From Supporting Critical Processes

- Production Data
- Production Quality Assurance
- Inventory
- Supply Chain
- Maintenance Planning

OT Site Data

Enterprise Resource Planning (ERP) Data

- Sales
- CRM
- Purchasing
- Financials
- Human Resources

ERP

=

Save Money Increase Efficiency

Client Impact: This connectivity and move to commodity hardware and software, viewed more urgently after several OT related incidents around the world, has **acted as a driver for increased security in the OT space**. Many organizations are viewing this challenge as an opportunity to align Operations, IT, and Information Security in order to increase the security posture of the OT environment and reduce risk to the organization.

Solutions overview

- Technical & Maturity Assessments
- Program Strategy
- SOC Integration
- Remediation & Maturity Advancement
- Incident Response
- Assets Management

The use cases are real…and the implications are significant

Global industry has continued to be affected by cyber attacks impacting operational environments. As the frequency and severity of attacks increase, the **cost to firms in lost revenue and remediation will continue to escalate.**

Stuxnet | 2010

- Sophisticated malware designed for use against specific PLCs that controlled electromechanical processes of nuclear centrifuges at a uranium enrichment facility in Iran.
- Leveraged multiple 0day exploits as well as stolen digital certificates to replicate and achieve it's destructive objectives.
- Widely considered the first of its kind OT specific malware.

Duqu/Flame/Gauss | 2011

- Three (3) related pieces of malware designed to gather information pertaining to control systems, likely for reconnaissance purposes.
- Flame leveraged microphones, web cameras, keystroke logging, and image geolocation to steal information.

HAVEX | 2013

- Modular malware that focused on information gathering, but could have been remotely expanded to perform other functions
- Represents the evolving geopolitical influence in cyberspace, specifically with regards to critical infrastructure.

BlackEnergy/CRASHOVERRIDE | 2015 & 2016

- First publicly confirmed cyber attack to impact a power grid (2015), left approximately a quarter-million people without power in Ukraine.
- Second attack carried out to similar effect the following year.
- Sophisticated attacks against control systems were paired with attacks against telephone call centers to delay reporting of issues and coordination of response.

NotPetya | 2017

- Designed to appear similar to the recent Petya ransomware, but purely destructive as it had no way to decrypt the data.
- **Multinational pharmaceutical company** was affected by a global malware attack from the malware NotPetya that encrypted many of their computer systems causing a loss of production and revenue as well as a worldwide disruption to operations **(Est $1B+ in Damages).**
- **Major shipping company's** operations shut down globally **(Est $250M in Damages).**
- **Global consumer goods company** fell victim to the NotPetya malware that inhibited its ability to send and ship invoices causing a 3% decline in revenue for that quarter. **(Est $100M+ in Damages).**
- **Other Companies** were also impacted in this extensive attack **(Est $10B+ in Damages).**

Trisis/TRITON | 2017

- Specifically designed to target safety systems, allowing the attacker to cause unsafe potentially life threatening or physically destructive outcomes.
- First known malware of its kind to target safety systems.

LockerGoga | 2019

- LockerGoga Ransomware caused a shutdown of operations at **a renewable energy company** resulting in a financial impact of ~$35M in the first week.
- Overall costs to the renewable energy company are estimated at approximately $75M.

Ekans | 2020

- Halted operations at several **major auto manufacturers facilities**.
- Impacted operations at a **healthcare company's** pharmaceutical sites.
- **Natural gas disibutor** confirms isolating it's IT network from operational networks.

Our Offering - Operational Technology (OT) Security Services

Overview

PwC is a leading advisor to organisations in sectors like oil and gas, transportation, retail, mining industries - and we work with key business stakeholders to provide solutions that are tailored to meet your needs.

OT knowledge and production systems experience was a critical factor in our team selection. We are committed to harvesting and combining our diverse business, technical, analytical, regulatory, investigative and law enforcement knowledge and know-how to deliver practical and sustainable solutions

We have worked on hundreds of cybersecurity engagements developing OT strategies,frameworks, policies, and standards.

Key services

OT maturity assessment

We can provide you with a detailed current state analysis to help you understand your current OT maturity and provide recommendations to help reduce the gaps and improve your OT maturity posture. The assessment can also review your IoT security architecture and provide the necessary recommendations to improve and enhance.

OT penetration testing

Our team understands the challenges and the sensitivity of ICS systems when it comes to penetration testing. Our proven methodology helps us identify critical and high vulnerabilities without disrupting your OT operations and provides you with a detailed remediation plan.

OT cybersecurity risk assessment

We have extensive experience conducting cybersecurity risk assessment exercises by identifying our clients asset inventory and analyzing security threats by leveraging our partnerships with leading ICS vendors in the market such as Nozomi Networks.

OT Governance and Strategy

We are a strong and experienced OT team that has engaged with major industrial clients within the region. We can help decision makers develop and govern a practical strategy that can increase their cybersecurity maturity (people, process and technology) while optimising budget spending within the OT infrastructure, leveraging partnership with key vendors such as Nozomi Networks.

Developing IT/OT target operating model

Our team can work closely with you to develop an effective operating model by defining the key functions, roles and responsibilities, interaction and communication model and key performance indicators (KPIs) to ensure your OT security objectives are delivered in alignment with industry best practices.

We can help…OT security service offerings

Organizations must adopt a proactive security posture in order to programmatically manage cybersecurity risk to operational systems. PwC Cybersecurity and Privacy offers a variety of services to enable integrated IT and OT security programs and reduce risk to organizations.

Incident Response

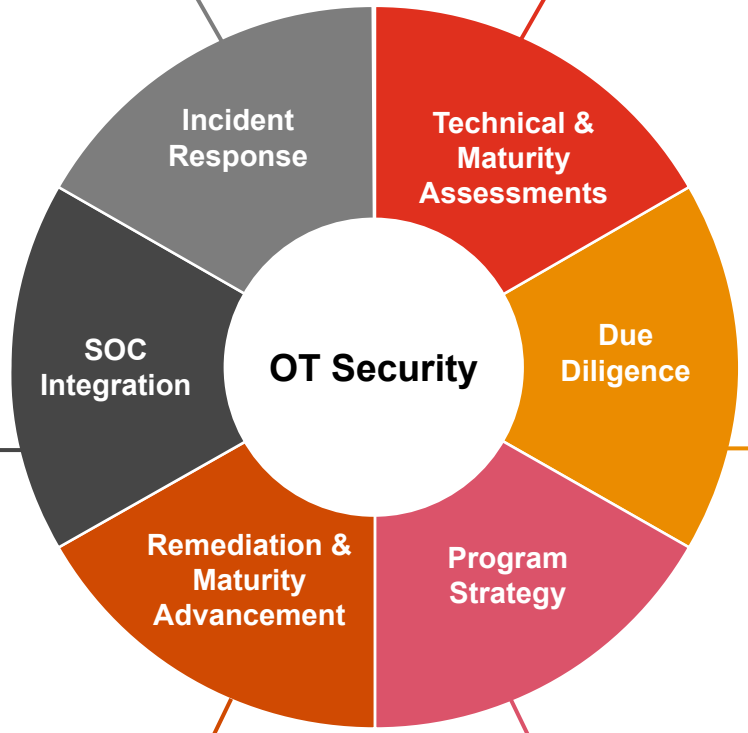
Properly investigate and assist in the isolation and response to anomalous cyber activities impacting operations originating from both internal and corporate sources

SOC Integration

Deploy and integrate detection and monitoring tools designed with industrial operations in mind based on modern practices

Remediation & Maturity Advancement

Work side-by-side with your engineers to develop acceptable compensating controls and provide in depth rationale and updated asset views to address concerns.



Technical & Maturity Assessments

Discover, document, and risk assess the current environment; notifying you of changes that can be validated

Assets Management

Provide rapid insight as to the details and risks of the assets and data being added and subtracted from the environment

Program Strategy

An asset based, risk focused protection program with clarity for roles, responsibilities, and accountability

PwC and Microsoft – Operational Technology (OT) Security: Defender for IoT

Solution overview

The fourth industrial revolution has brought substantial gains in productivity and efficiency, as well as an increased cyber threat landscape for asset owners. As organisations work to quantify and mitigate the increased cyber risk stemming from their interconnected control systems, they continue to struggle with the foundational need of understanding what is on their network, what is communicating, and what is the impact if assets are compromised.

PwC works with Microsoft to deliver services that rapidly deploy, operationalise, and integrate Microsoft Defender for IoT into your Operational Technology (OT) and cybersecurity programs. Whether you are looking to improve existing capabilities or building from the ground up, PwC and Microsoft can help you

PwC Service Offerings for Azure IoT Defender

We have built our service offerings around 3 key service offerings. These service offerings can be performed independently, but the most value is achieved when our clients step through them sequentially.

1 Deployment optimisation

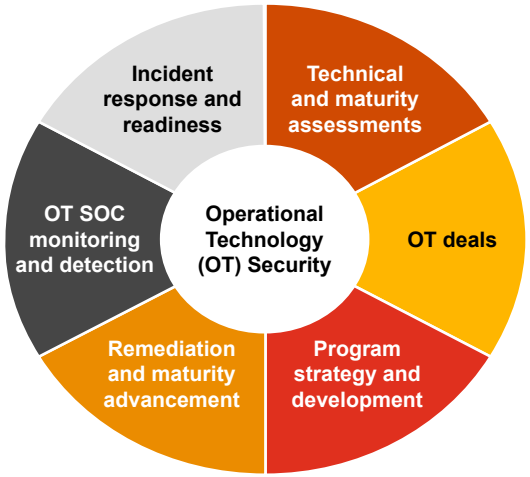
Leverage PwC accelerators to finalise Azure IoT defender deployment approach, deploy Azure IoT defender across your OT environment, and assist clients in managing organisational change to help drive rapid adoption through training and empowering client teams.

2 Rapid pilot and expand model

Pilot Azure IoT defender capabilities using PwC's rapid deployment approach, including the option to pilot remotely from our OT lab. Support clients in expanding and optimising the rollout of the tool and operationalise with incident response planning playbook development.

3 Cyber portfolio integration

Utilise our team of OT security experts to integrate the offering with other Microsoft tools, such as Sentinel, as well as other best of breed products for Asset Management, SIEM, Perimeter Security, and Workflow management.



Key benefits for our clients

Asset management	Anomaly detection	Risk assessment
• Identify devices communicating on your network. • Categorise assets by criticality. • Integrate with leading Asset Management tools.	• Baseline network activity. • Identify anomalous communications. • Dissect OT protocols and alert on OT specific actions such PLC configuration change. • Integrate with leading SIEMs e.g., Microsoft Sentinel.	• Perform rapid risk assessments to understand how changes in your environment impact your security posture. • Measure progress of remediation efforts through reporting and metrics.

Who to Engage

IoT/OT – PwC OT experience, advisory and delivery. Microsoft solutions

Defender for IoT

PLCs & DCUs

HMIs

Engineering Workstations

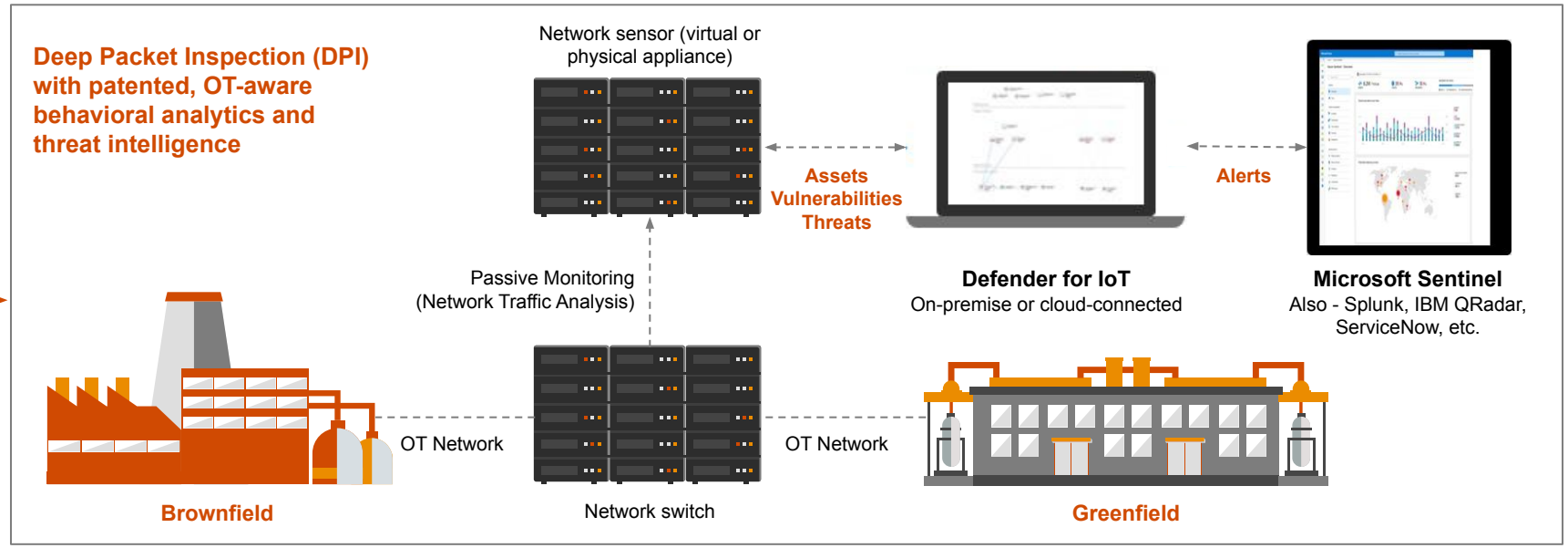
Historians

Enterprise IoT

Building automation

Secures both legacy and greenfield devices

https://www.youtube.com/watch?v=RTOSmWOMChs



Learn more

Contact us to learn more about how you can transform your cybersecurity operations

Haitham Al-Jowhari
Partner
Haitham.Al-Jowhari@pwc.com
+971 56676 1146

James Toulman
Director, Cloud Services
James.Toulman@pwc.com
+971 56227 1811

Appendix

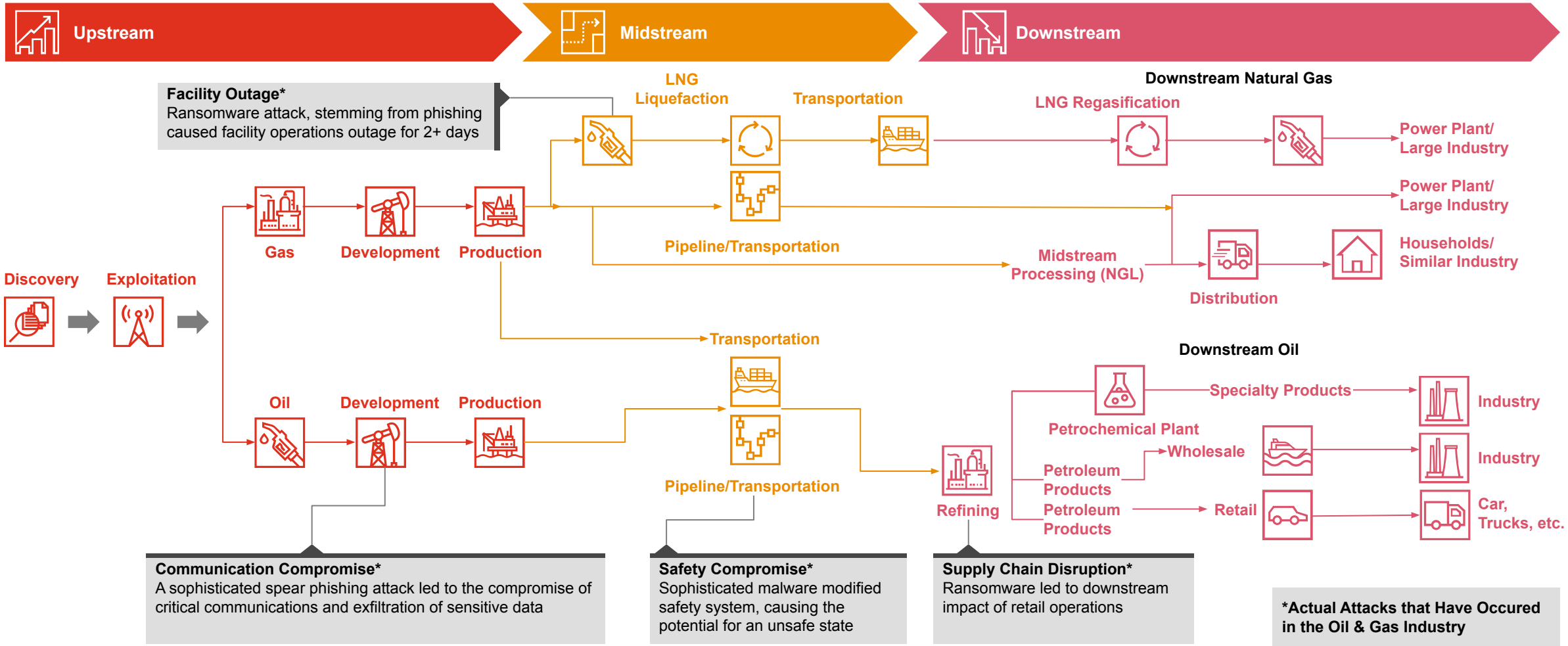
What are the trends in OT?

As companies continue their digital transformations and further blur the lines between their IT and OT systems they need to be prepared to defend their networks against emerging threats.

Attacks Impacting Both IT & OT	Most cyber attacks impacting OT environments also impact IT environments, resulting in incidents that require both groups to collaborate and respond, however 61%* of companies report they have no cross training between the two.
IT/OT Convergence	As OT transitions from highly specialized hardware & software to more traditional IT technology stacks there are opportunities for cost savings, increased visibility, and improving security, yet 24%* of companies say their IT & OT departments have little to no interaction.
Increased Intensity of Attacks	Cyber attacks targeting OT assets have increased in both volume and sophistication. While past attacks focused on data gathering, modern attacks are capable of not only operational disruption, but can even cause physical damage.
Evolving Defenses	The growing need to protect OT assets has led to investment from the private and public sectors to build new defenses in the form of new trainings, methodologies, and tools.
Focus on Risk Management	Regulated & unregulated industries alike are putting a renewed effort into improving cyber risk management to help drive change & prioritize limited resources. Additionally, new approaches are taking a more holistic approach to consequence reduction to help reduce risk.

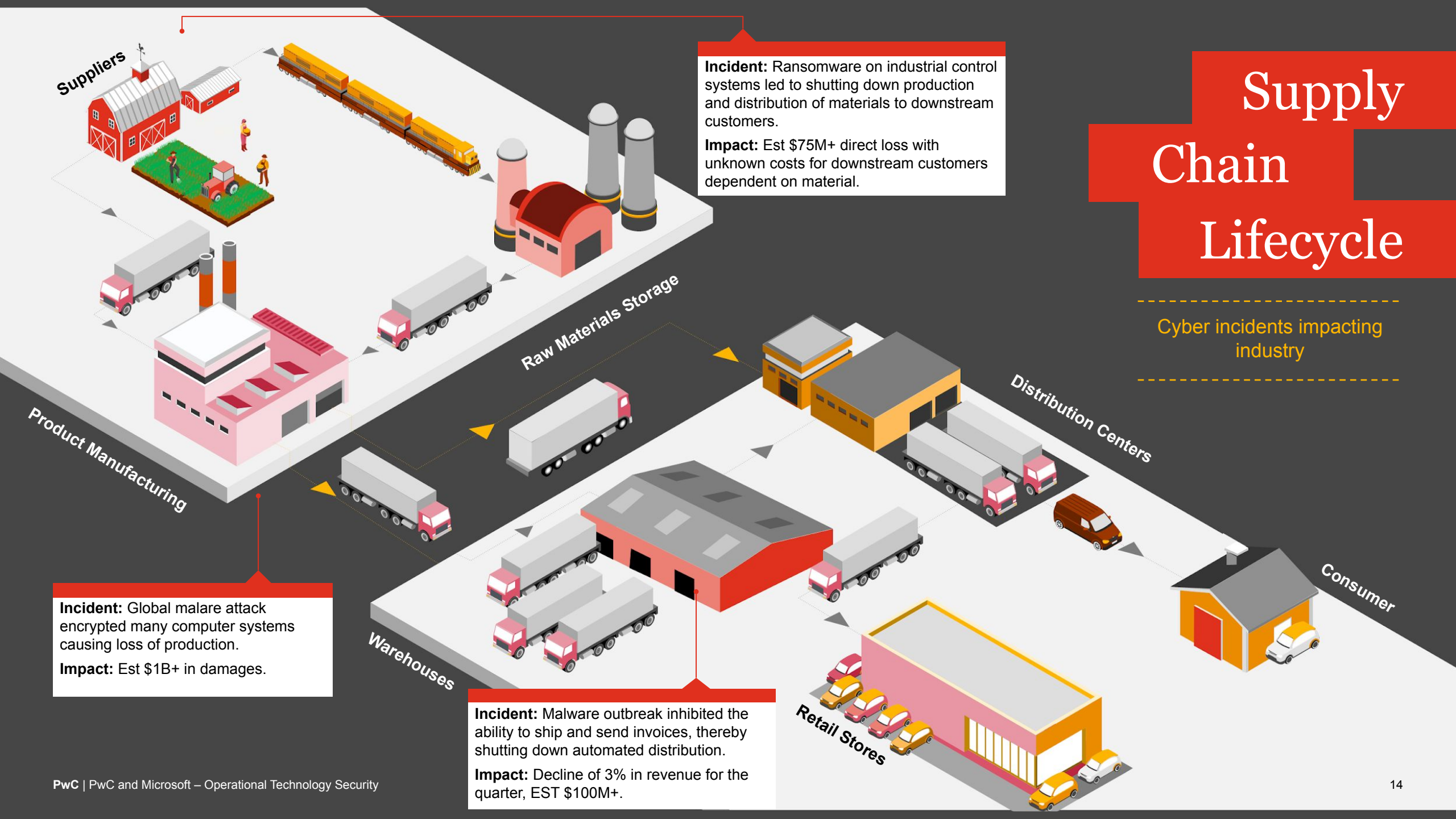
*Source: Automation World survey, 2017

Example value chain – Oil & Gas – What's at risk?



Supply Chain Lifecycle

Cyber incidents impacting industry



Incident: Ransomware on industrial control systems led to shutting down production and distribution of materials to downstream customers.

Impact: Est $75M+ direct loss with unknown costs for downstream customers dependent on material.

Incident: Global malare attack encrypted many computer systems causing loss of production.

Impact: Est $1B+ in damages.

Incident: Malware outbreak inhibited the ability to ship and send invoices, thereby shutting down automated distribution.

Impact: Decline of 3% in revenue for the quarter, EST $100M+.

Thank you

pwc.com