

RSA®Conference2019

San Francisco | March 4–8 | Moscone Center



BETTER.

SESSION ID: **TECH-R03**

Protecting your Achilles' heel: managing security risk in your legacy product portfolio

Kyle Brunell

Connected Product Security Leader
Ernst & Young LLP (EY)
@kyle_Brunell

The views expressed by the presenters are not necessarily those of Ernst & Young LLP or other members of the global EY organization.



#RSAC

First, a personal story about legacy products ...

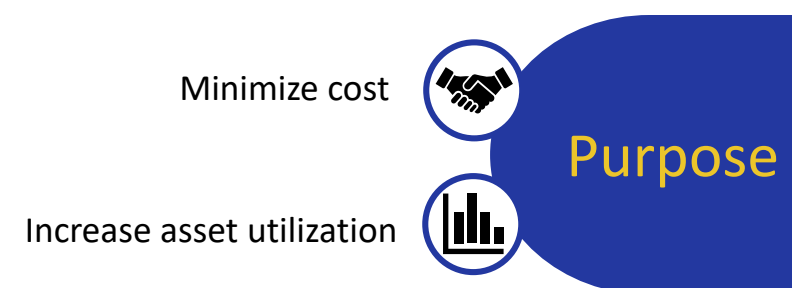
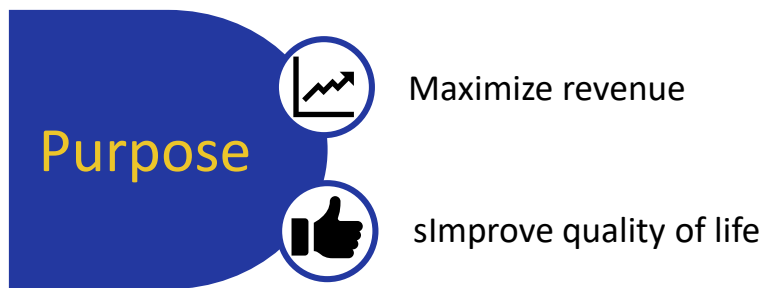


What are the business drivers for better connectivity among products?

Consumer

Service

Industrial



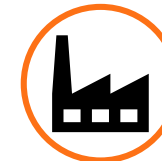
Examples:



Smart homes, connected cars and wearables provide daily life convenience, efficiency and overall improve the customer experience

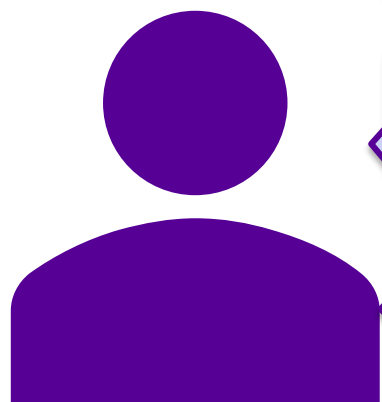


Health care, financial services and utilities provide real-time execution of transactions such as remote payments, prescription filing, health records management and metering



Manufacturing, oil and gas, and agriculture to achieve supply chain optimization, quality control, asset management, remote control and predictive maintenance

Why are we doing this talk?



How can I understand the risk of the legacy products I've developed, manufactured, sold and deployed?

What are some security challenges with legacy products that we have released?

What are some strategic and tactical methods to manage my risk?

Product Manufacturer

What qualifies as a legacy product?

Legacy products were built with different expectations.

These products are still in operation, but the **expectations have changed**

Yesterday's legacy products

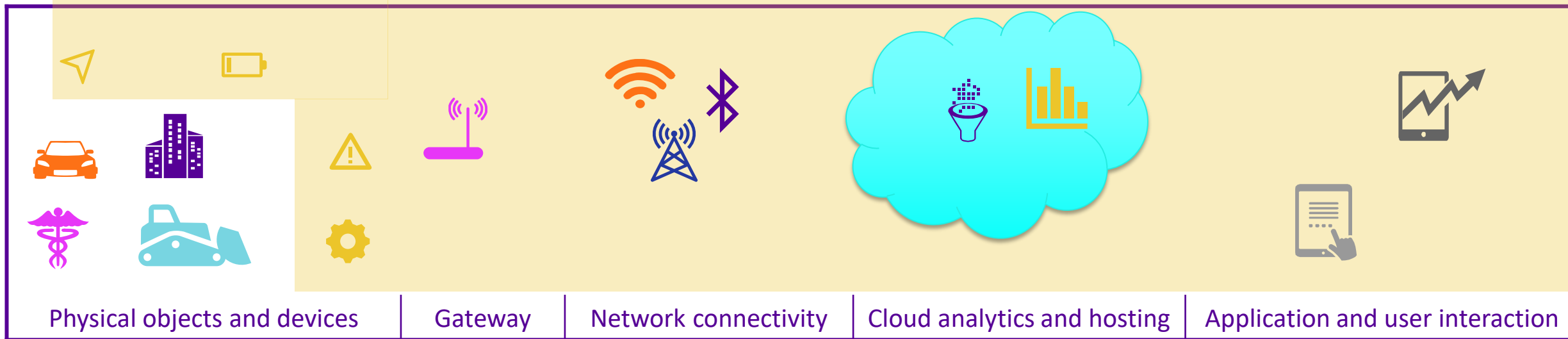
- ▶ Developed without current security threats in mind
- ▶ Intended to operate in isolation
- ▶ Expensive to replace
- ▶ Not extensively tested for security
- ▶ Difficult to update or upgrade
- ▶ Contain rich data, but data is largely inaccessible
- ▶ Minimal regulatory requirements
- ▶ Lack of security solutions available

Today's environment

- ▶ Increased sophistication of threat actors
- ▶ Demand for expanded connectivity
- ▶ Limited capital for improving old products
- ▶ Enhanced security testing tools and techniques
- ▶ Demand for new functionality
- ▶ Greater need for data
- ▶ Increased regulation and standards
- ▶ Heightened customer expectations

Where's the risk?

The expanded attack surface:



Why is securing legacy products such a complicated problem?

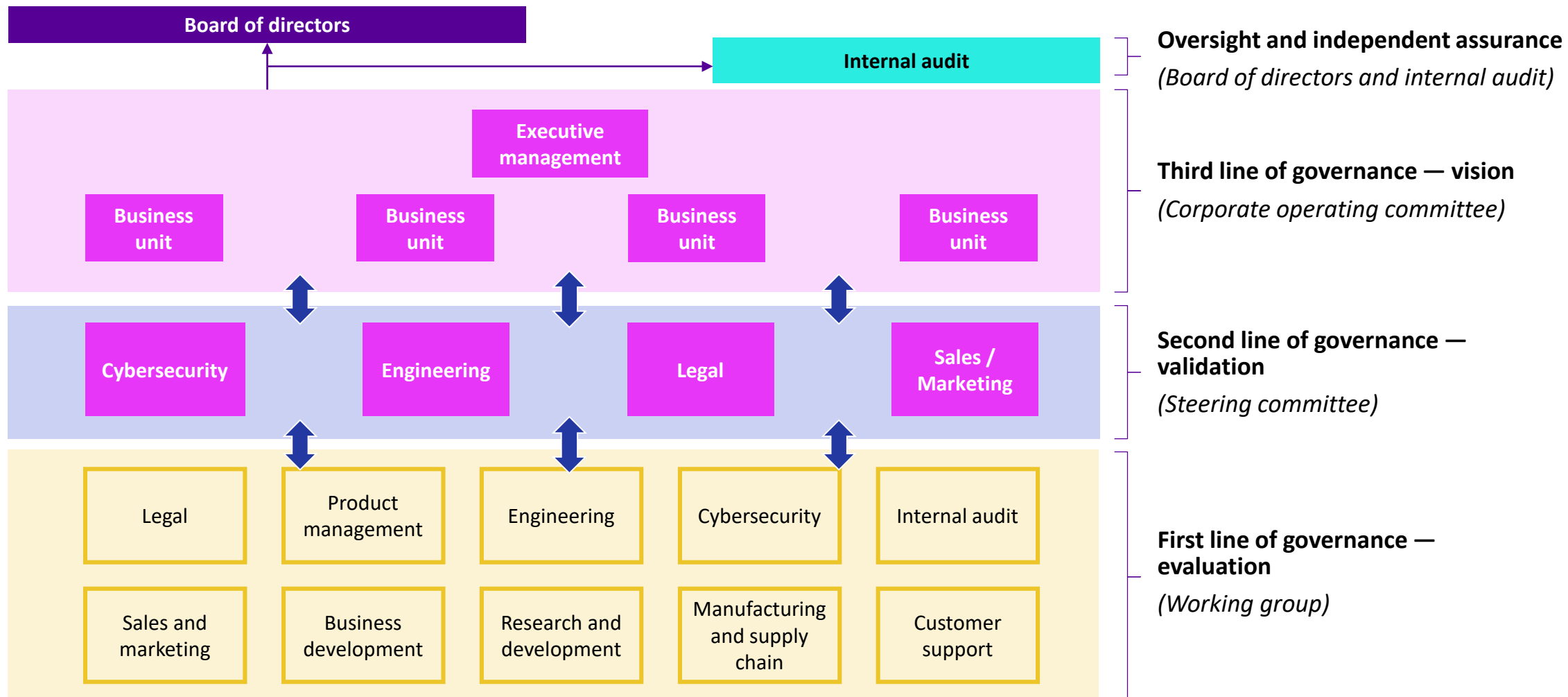


So what can be done to manage the risk of legacy products?



1

Involve stakeholders from across the enterprise

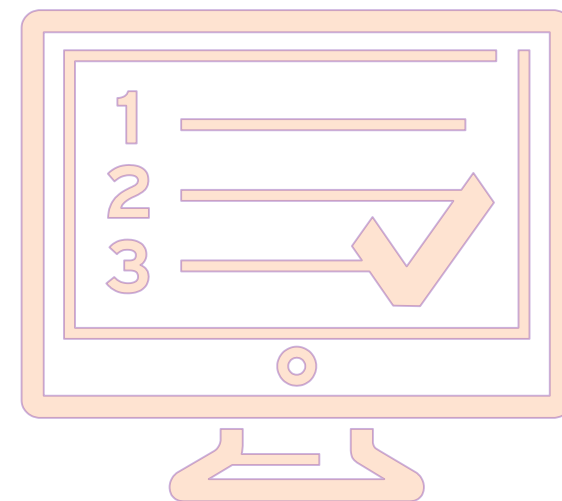


2 Understand your legacy product portfolio based on risk

STEP 2

Understand, identify and prioritize the highest risk products

- What is the highest risk product for the organization?
- What is the risk of the product?
- What is the risk of the product?
- What is the risk of the product?
- What is the risk of the product?
- What is the risk of the product?
- What is the risk of the product?



3 Establish clear lines of communication with your customers

With an increasingly sophisticated and security-aware customer base, the right customer support model is needed to communicate security in a timely and consistent manner

Business development

Program strategy and vision

Customer support model

Product security marketing collateral

Onboarding and deployment

Solution security brochure

Solution security controls

Secure deployment guidance

Product support

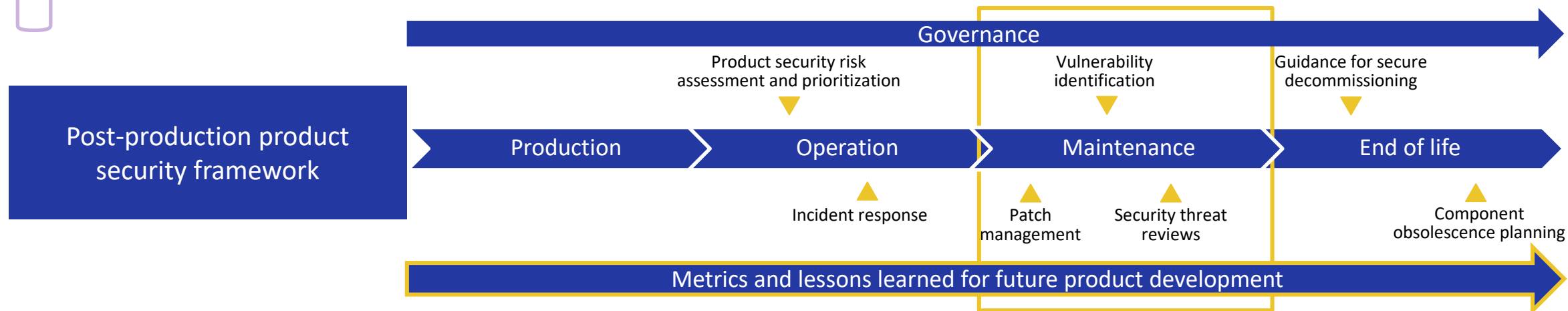
Secure deployment support

Solution support and update procedures

Incident and vulnerability communications

4

Uncover vulnerabilities through various testing approaches



Key challenges

- Difficulty updating products
- Challenges in prioritizing and funding resolution
- Outdated third-party components
- Lack of vendor support
- Deficiency of testing resources

Critical success factors

- Leverage automation to the extent possible
- Integrate into existing reporting and workflow tools
- Scale testing activities based on the risk of the product
- Continued vendor assessments
- Monitor and manage security demand
- Have a plan for different types of issues you may find

5

Engage external researchers appropriately



1

Understand your capacity to consume vulnerability reports from researchers

2

Create easy-to-use avenue for researchers to submit vulnerabilities

3

Actively address submissions and engage with researchers throughout the process

4

Consider monetary and/or non-monetary incentives for researchers

6

Prepare for potential security incidents

Define points of contact between legacy product owners and incident response team (IRT)

Establish channels to receive and escalate security events submitted through customer/dealer intake channels

Maintain criteria to effectively escalate security events to IRT and engage cross-functional teams

Coordinate with legal counsel to evaluate contractual agreements

Establish and maintain appropriate relationships with internal and external stakeholders

Ensure that IRT has appropriate legacy product details

Summary

- Legacy product security requires a collaborative approach with engagement from all parts of the organization.
- Understanding what products you have and their relative risk is a must.
- When used appropriately, external researchers can be essential to improving security.
- Customer communication is paramount, especially in the absence of technical controls.
- Security testing requirements and methods need to be well defined.
- Be prepared for potential incidents.



Next week

- Identify stakeholders
- Engage sales team to understand security inquiries

Next 90 days

- Identify and prioritize legacy products
- Establish a method to submit vulnerabilities
- Conduct a tabletop for legacy products

Next 180 days

- Develop a testing program

Questions



Kyle Brunell

Connected Product Security Leader

kyle.brunell@ey.com

+1 312 879 2811