RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: TECH-R03

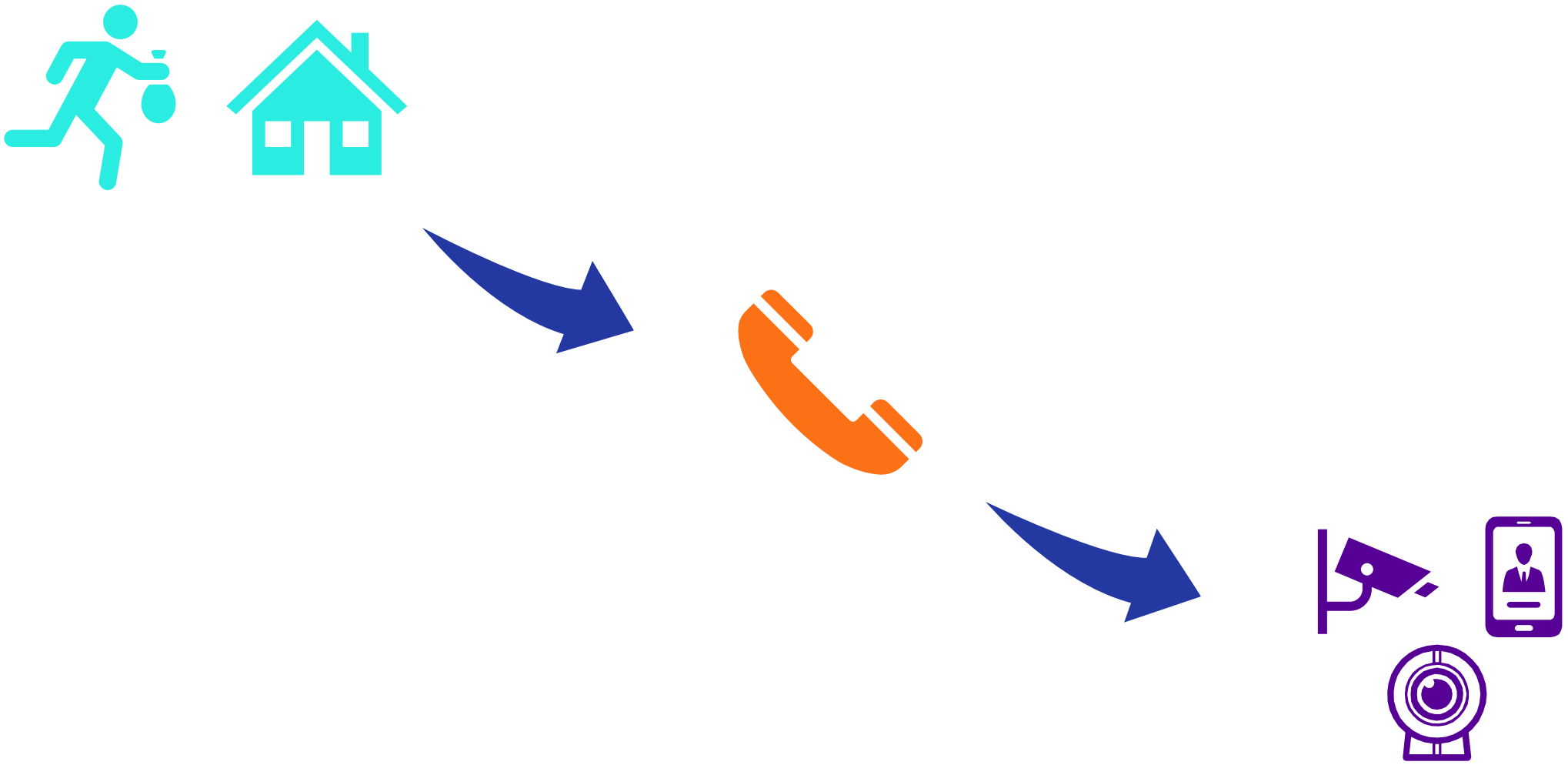
Protecting your Achilles' heel: managing security risk in your legacy product portfolio

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.

First, a personal story about legacy products …



What are the business drivers for better connectivity among products?

Consumer — **Service** — **Industrial**

Purpose

- Maximize revenue
- Improve quality of life

Purpose

- Minimize cost
- Increase asset utilization

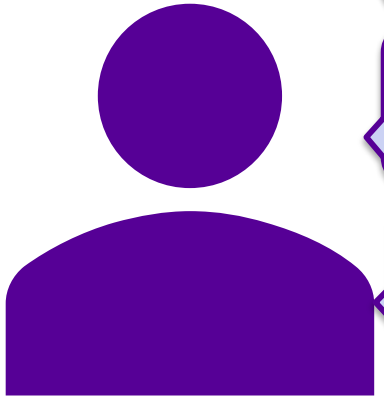
Examples:

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?



Product Manufacturer

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?

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

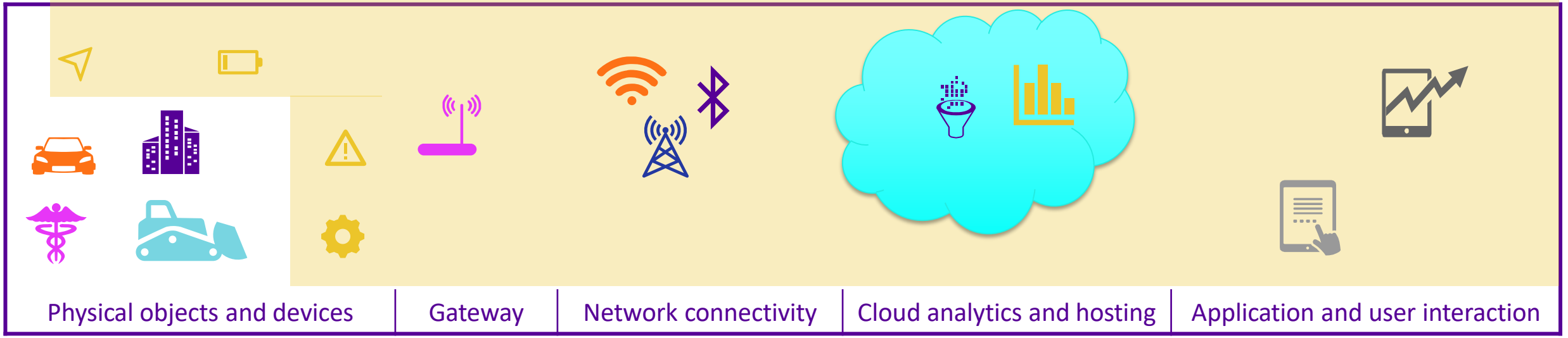
- Developed without current security threats in mind
- Intended to operate in isolation
- Expensive to replace
- Not extensively tested for security
- Difficult to update or upgrade
- Contain rich data, but data is largely inaccessible
- Minimal regulatory requirements
- Lack of security solutions available

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:



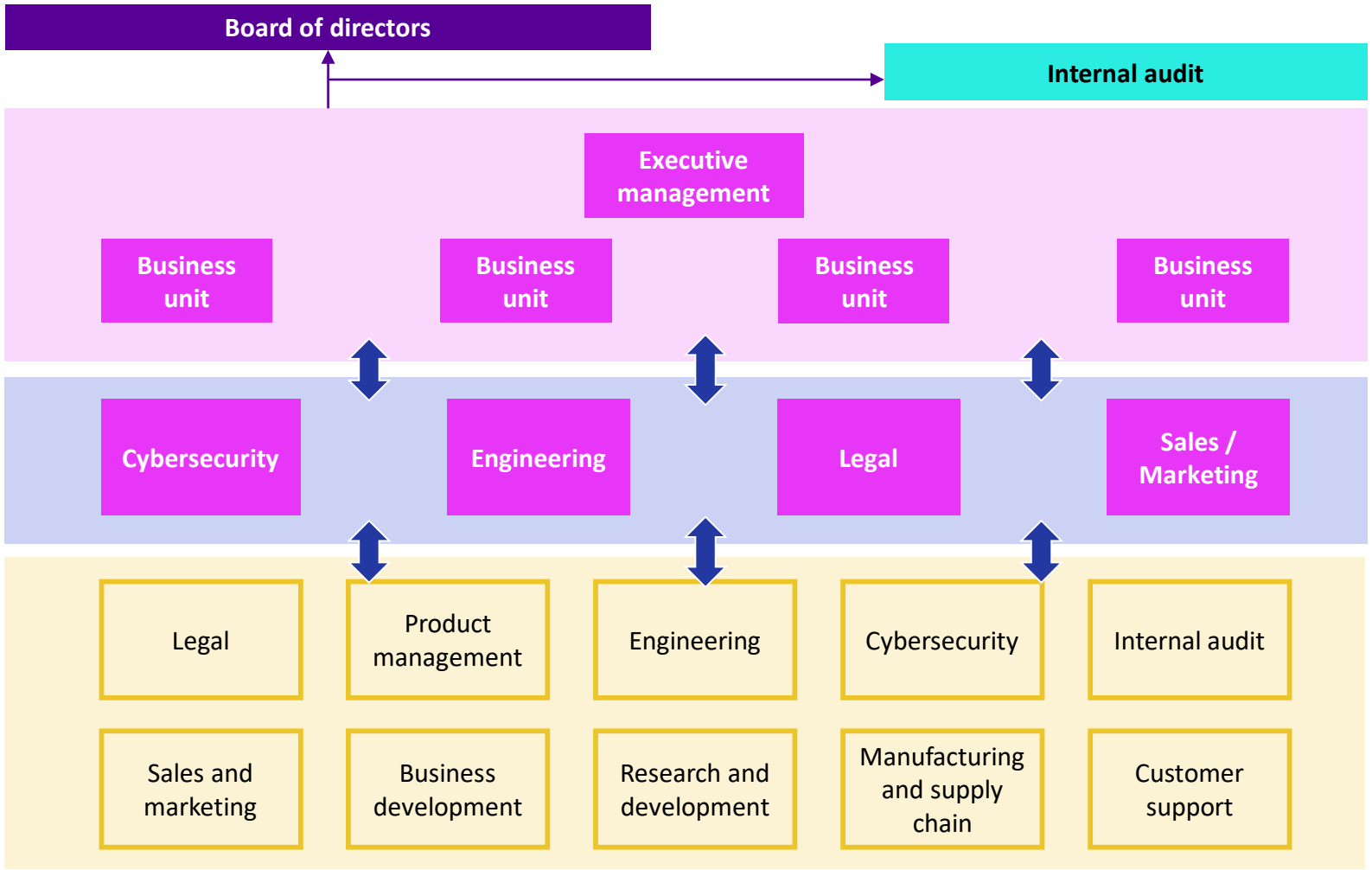
Why is securing legacy products such a complicated problem?

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
3. Establish clear lines of communication with your customers

4. Uncover vulnerabilities through various testing approaches
5. Engage external researchers appropriately
6. Prepare for potential security incidents

1 Involve stakeholders from across the enterprise



Oversight and independent assurance
(Board of directors and internal audit)

Third line of governance — vision
(Corporate operating committee)

Second line of governance — validation
(Steering committee)

First line of governance — evaluation
(Working group)

2 Understand your legacy product portfolio based on risk

STEP 1 Understand the risk of your products

- What is the current or anticipated production volume?
- What is the intended functionality of the product?
- What type of data is stored or processed?
- What connectivity does the product support?
- What security controls have been implemented?

STEP 2 Know where your products are operating

- Which locations are the products operating in?
- Who owns them?
- Who operates them?
- What regulations apply?

STEP 3 Prioritize products based on their risk to the organization

- What is the highest-risk product from a legal or reputational standpoint?
- Which products have the highest potential liability?

STEP 4 Align security activities with the highest-risk products

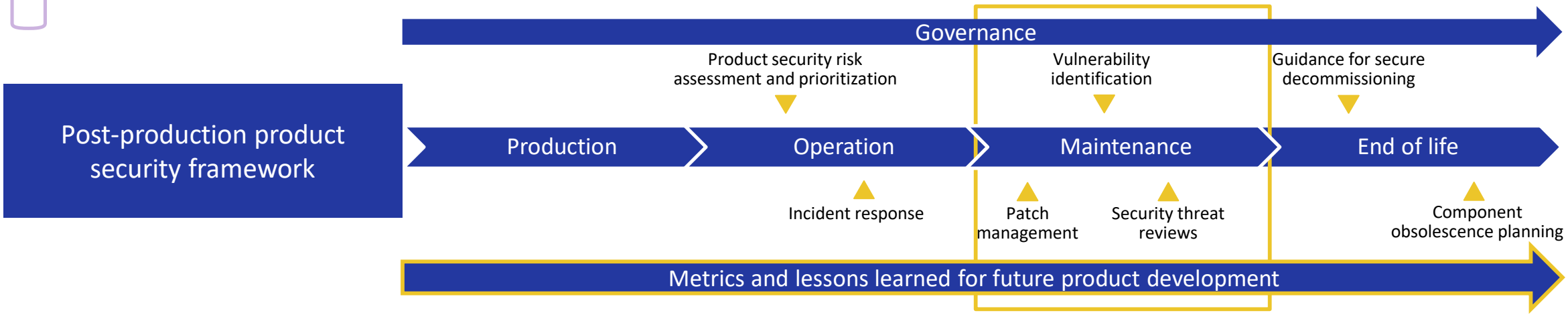
- Are all of the contacts in place and do they understand their responsibilities?
- How do security activities scale based on the risk of the product?
- Have necessary security tests been conducted?

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	Onboarding and deployment	Product support
Program strategy and vision	*Solution security brochure*	*Secure deployment support*
Customer support model	*Solution security controls*	*Solution support and update procedures*
Product security marketing collateral	*Secure deployment guidance*	*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

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	Next 90 days	Next 180 days
• Identify stakeholders • Engage sales team to understand security inquiries	• Identify and prioritize legacy products • Establish a method to submit vulnerabilities • Conduct a tabletop for legacy products	• Develop a testing program

Questions

Kyle Brunell
Connected Product Security Leader
kyle.brunell@ey.com
+1 312 879 2811