

RSAC®Conference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN
ELEMENT

SESSION ID: PS-T10

The emerging role of the CPSO



Stephanie Domas

CPSO and Executive Vice President
MedSec

#RSAC

Outline

- What is a CPSO
- Differences from a CSO
- The need for a CPSO
- An ace in the hole: the CPSO
- Conclusion

RSA®Conference2020

CISOs & CSOs are invaluable



Healthcare

FDA announces first-ever recall of a medical device due to cyber risk

<https://blogs.cisco.com/healthcare/fda-announces-first-ever-recall-of-a-medical-device-due-to-cyber-risk>

The need for product security

- Product sales represent the income base for companies
- Loss of trust in their products can ruin a company overnight
- Cybersecurity product liability is an emerging field in litigation
 - The risk of a company's product being the source of a customer's breach, or harming a person, creates a huge financial risk
- Customers are adding product security specific clauses to purchase contracts
 - Notifications, indemnification, patching

The need for product security

- Cybersecurity breaches represent one of the single largest reputational and monetary risks for companies
 - **USD 3.92 million** Average total cost of a data breach ¹
 - **United States** Most expensive country: USD 8.19 million ¹
 - **Healthcare** Most expensive industry: USD 6.45 million ¹
- Companies focus a tremendous amount on their internal infrastructure security but not on their product security

1: <https://www.ibm.com/security/data-breach>

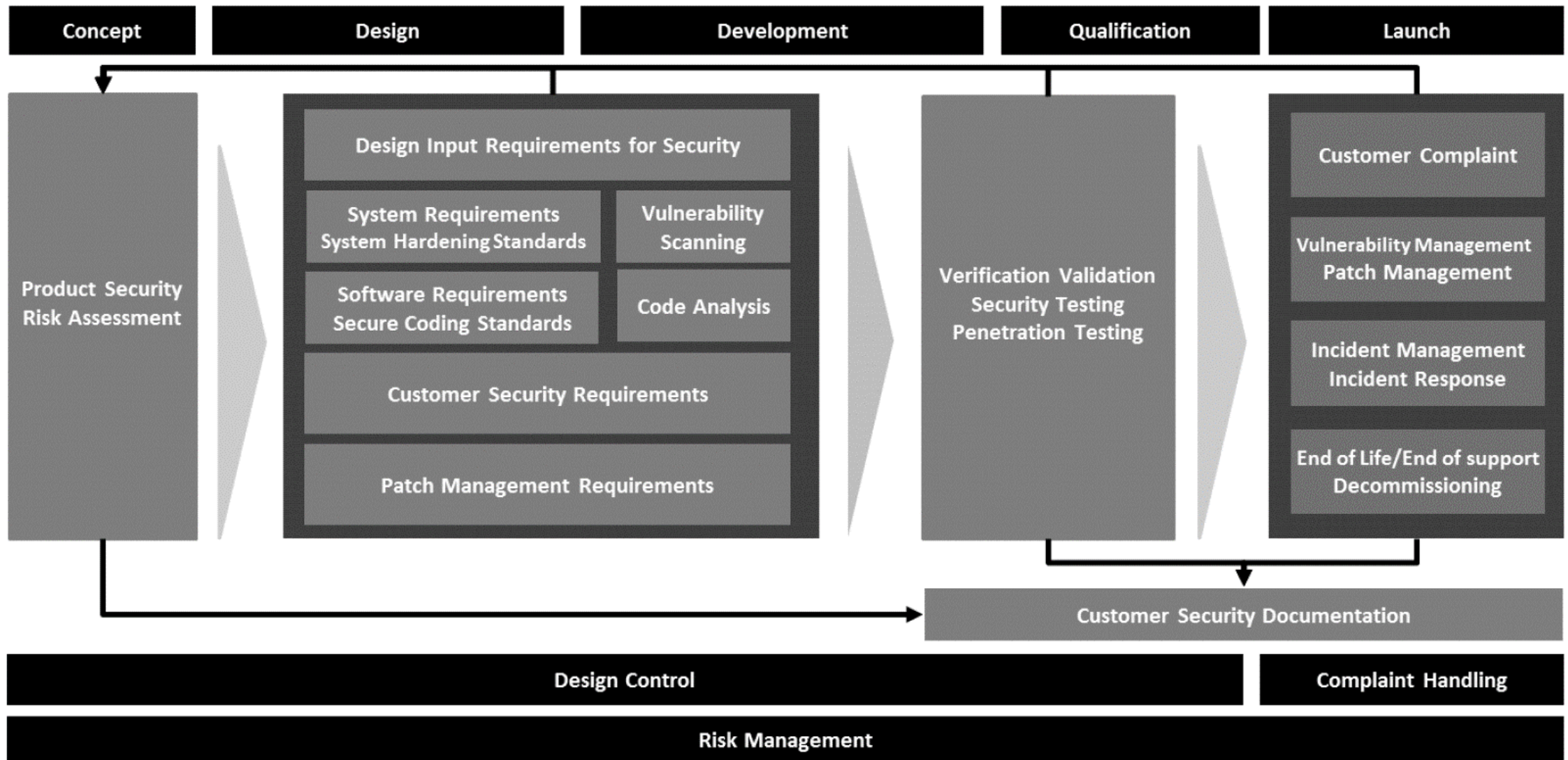
What is a CPSO

- Chief Product Security Officer (CPSO)
- Oversee cybersecurity of a company's products
 - Digital products (software, firmware, or product with code)
- Implement and oversee a product security program
 - Addresses cybersecurity in all stages of a product's lifecycle

Responsibilities of a CPSO

- Secure Product Design
- Cybersecurity Risk Management
- Vulnerability Management
- Incident Response
- Policies & Procedures
- Standards

CPSO – Product Security Program



Differences from a CSO and CISO

- At a high level some responsibilities are similar
- Execution of responsibilities is vastly different
- Product Security is a separate domain of knowledge than enterprise environment security

Example – Incident Response

- Incident reported through customer disclosure
- R&D Team tries to recreate the issue
- If recreated
 - Legal
 - Verify contractual customer patch timelines
 - Verify contractual customer notification timelines
 - Write new code
 - Build a new release
 - Test the release
 - Release the patch
 - Legal team investigates any liability

Example: The need for CSPO



Home » Hacking News » Hackers attack Casino's fish tank thermometer to obtain sensitive data

Hackers attack Casino's fish tank thermometer to obtain sensitive data

<https://www.hackread.com/hackers-casinos-fish-tank-smart-thermometer-hack/>

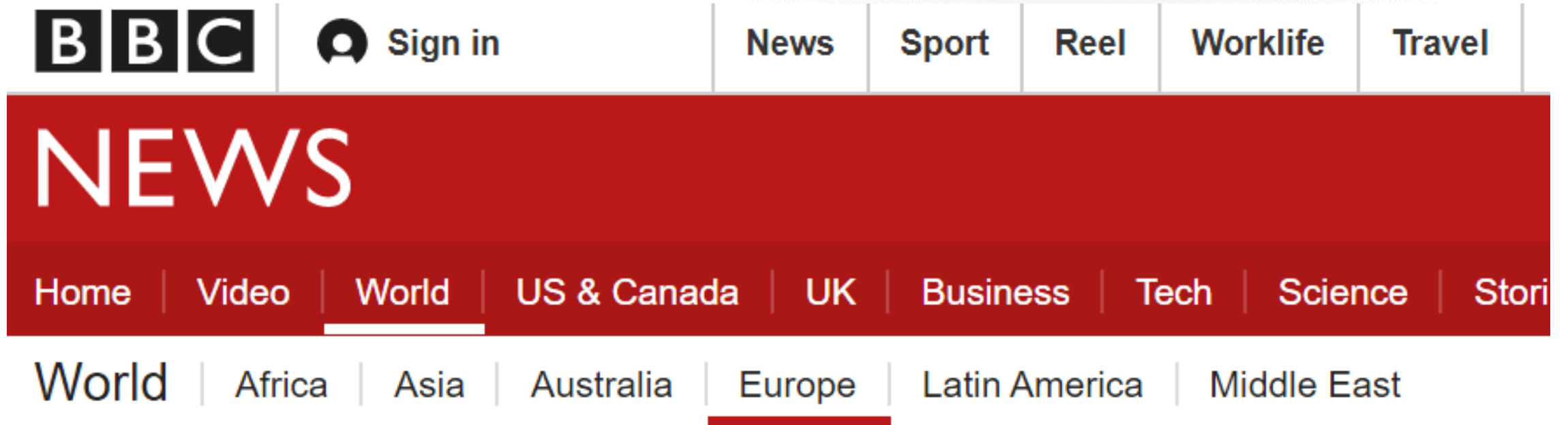
Example: The need for CSPO



HVAC Company, Fazio Mechanical Services, Was The Gateway For The Target Data Breach

<http://techfaster.com/target-fazio-mechanical-services/>

Example: The need for CSPO



The image is a screenshot of the BBC News website. At the top, the BBC logo is on the left, followed by a 'Sign in' button. To the right are navigation links for 'News', 'Sport', 'Reel', 'Worklife', and 'Travel'. Below this is a large red banner with the word 'NEWS' in white. Underneath the banner is a horizontal menu with links for 'Home', 'Video', 'World', 'US & Canada', 'UK', 'Business', 'Tech', 'Science', and 'Stori'. The 'World' link is underlined. Below this menu is another row of links for 'World', 'Africa', 'Asia', 'Australia', 'Europe', 'Latin America', and 'Middle East'. The 'Europe' link is underlined. The main headline reads 'German parents told to destroy Cayla dolls over hacking fears'. To the right of the headline is a URL: <https://www.bbc.com/news/world-europe-39002142>.

German parents told to destroy Cayla dolls over hacking fears

<https://www.bbc.com/news/world-europe-39002142>

An ace in the hole: the CPSO

- The tech skillset
 - Engineering (Computer, Electrical, Systems)
 - Product Cybersecurity
 - Threat Modeling
 - Secure Coding
 - Security Risk Management
- The background
 - Research and Development
 - Product Lifecycle

An ace in the hole: the CPSO

- The evangelism
 - Cybersecurity always has a usability tradeoff
 - Spreading awareness and education is key to a successful program
 - Changing the status quo
- The culture changer
 - Cybersecurity is HARD
 - It adds to development timelines, proper tools cost money
 - Support for cybersecurity efforts is paramount

An ace in the hole: the CPSO

- At the C-Suite level, not buried in R&D
 - Briefing the board on product security as frequently as enterprise security
 - CPSOs need authority to successfully drive product security
 - CPSO should report to the CEO or CSO

Summary

- CPSO is a unique need at any company that sells products containing software
- CPSO is different from a CSO/CISO
 - CSO/CISO focuses on enterprise
 - CPSO focuses on products
- CPSOs control business cybersecurity risk created by your products

Apply What You Have Learned Today

- Immediately following this presentation you should:
 - Reflect on your company's products, their cybersecurity needs, and their potential impact to your company
- In the first three months following this presentation you should:
 - Evaluate your company's products and risk tolerance for product cybersecurity
 - Review organizational structure to determine effective location for a CPSO
 - Leverage CPSO to control business risk of product cybersecurity