# Open Source Alignment & Policies for Management

***Thomas Costello – UpStreme, Inc.***
***Francis X. Taney, Jr. – Buchanan Ingersoll & Rooney, PC***
***Frank Curran – Black Duck Software, Inc.***
***Phil Laplante – Penn State University***
***Anthony Gold – Unisys***

# Welcome and Introductions

- Presenters
  - UpStreme, Inc.
  - Buchanan Ingersoll & Rooney, PC
  - Black Duck Software, Inc.
  - Penn State University
  - Unisys

# Goal of This Presentation

- Provide overview of Open Source
- Discuss real-life OS Risk examples
- Discuss OS Licensing
- Provide overview of OS Policy triggers
- Discuss components of a solid OS Policy
- Open discussion

# Does OS Impact Your World?

## Are you doing “any” of the following?

- Offshore Development?
- Vendor Provided Software?
- Embedded Systems?
  - Internal Tools?
  - Products / Devices?
- Merger & Acquisition (Buying or Selling)?
- OEM?
- Outsourcing?

# Open Source Use

## Where Do You Find Open Source in an Organization?

- It is the blanket that lays over all of IT:
  - OS and NOS
  - Security
  - Business Applications
  - Desktop Applications
  - Core of SaaS (Google, SugarCRM, etc)
  - Development Methodologies and Tools
- And More...
  - Cultural, Governance, and Organization Shift

# Ways Open Source Can Enter Your Environment

- Products
  - Code embedded in products and/or devices you use and/or distribute/sell.
- Code
  - Internal team development
  - Embedded in purchased packages
  - Contracted development
    - Partners and Subcontractors – onshore and offshore

# There Aren't New Risks

## Why Is The Risk Greater Now?

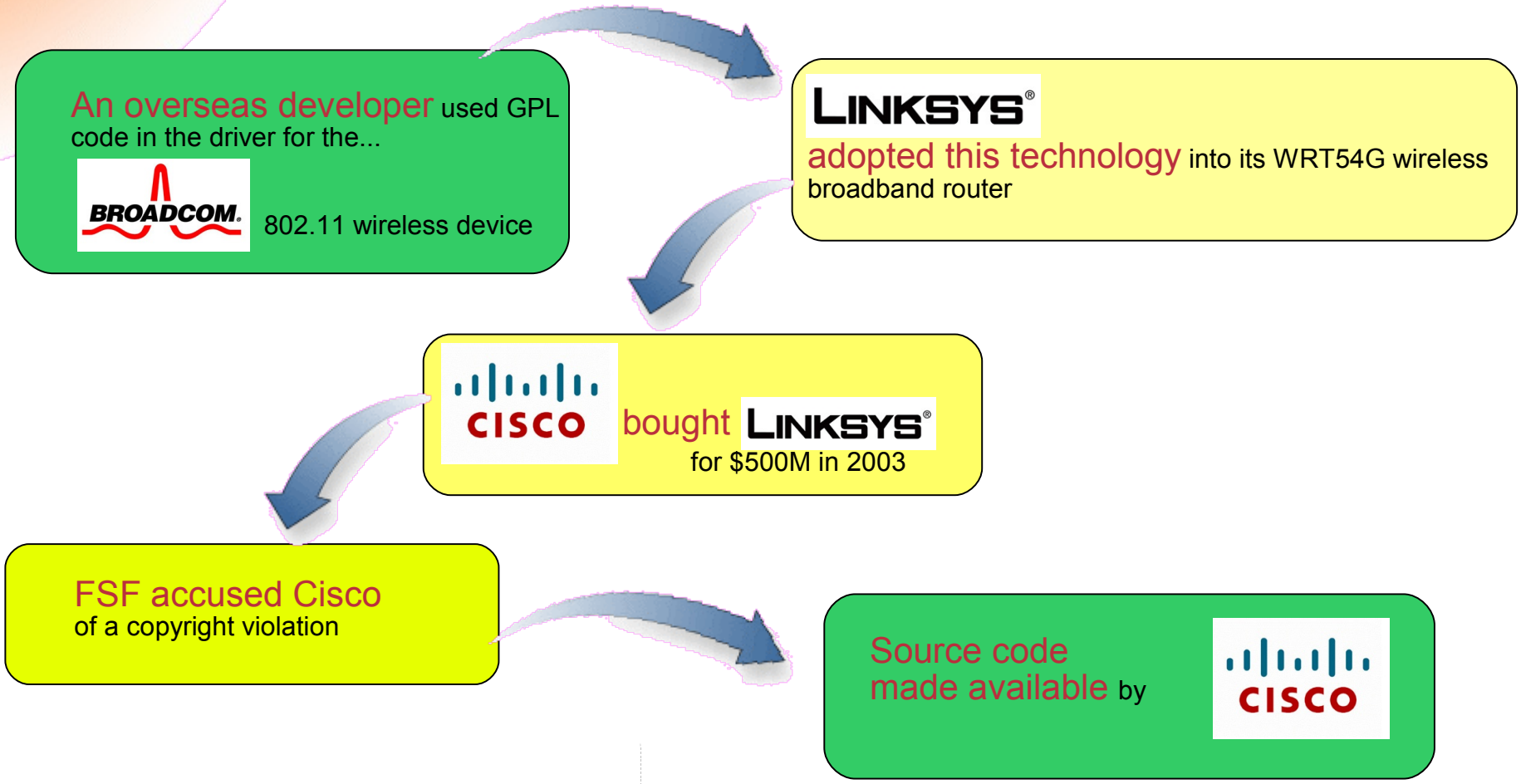
- Pressure to increase speed of delivery
- Availability of tools, code, and packages
- Weaker software development practices
- Increased reliance on subcontracted software development
- Increased use of component based development

# Examples of Component Based Risks

- Tank

Others...

# Cisco - Linksys - Broadcom




The story ends...

Developers modified firmware turning a low-end ($60) device into a high-function router

# What Are My Real Risks?

- Increased risk and cost of litigation from IP infringement claims
  - Copyrights
  - Patents
- Decreased value of your IP (and products)
- Decreased value of company

# Just a Legal Issue?

- It is predominately a legal risk, but the solution requires
  - A Balance of legal and operational activities to manage the risk.
  - An Internal and External view of the risks.
  - A Policy
  - A Process
  - Ongoing Monitoring and Tuning

# How do you tackle this?

- How is the market reacting?
- What kind of solutions are working?
- What approaches are not?

# What is the goal of an Open Source Policy?

# What is the Goal of an OS Policy?

- Governing Principles
  - Ensure alignment with corporate goals
  - Ensure efficient and effective procedures are created
  - Ensure staff and vendors are educated
  - Ensure Compliance with procedures
  - Ensure Process is revisited and tuned.

# Key Parts of Open Source Policy

- Components
  - Clearly state corporate goals
  - Define a formal process for the use, creation, and release of code
  - Define and create and education program for both internal and external use (and don't forget ongoing new-hires)
  - Create a formal process for monitoring
  - Create a formal process for continuous improvement.

# What Does an Open Source Policy Look Like?

- An Open Source Policy is more than just a paragraph from an executive to developers.
- A solid Open Source Policy will require:
  - Executive, legal, staff, and vendor involvement
  - Aligned policies
  - Living documents
  - Automated tools with “human” verification
  - Education and communication programs
  - Ongoing commitment

# Key Stages of Building an Open Source Policy

Formulate

Assess

Develop

Monitor

# What Does an Open Source Policy Look Like?

**Formulate**

Assess

Develop

Monitor

- Determine corporate goals
- Open Source Baseline for Management Team
- Vision on Open Source Use
- Create OS Review Board
- Define Assessment Process
- Review “Findings” following the Audit phase and revisit.

# What Does an Open Source Policy Look Like?

Formulate

**Assess**

Develop

Monitor

- Interview Staff.
- Interview Key Vendors.
- Perform Code Reviews.
- Produce Findings
- Produce Risk Profile
- Produce Remediation Plan
- Review with OS Review Board

# What Does an Open Source Policy Look Like?

Formulate

Assess

**Develop**

Monitor

- Document initial Policy Statement (version 1)
- Rollout to all stakeholders
- Integrate into employee programs
- Integrate into vendor contracting processes
- Remediation
  - As approved by OS Review Board and Sr. Management

# What Does an Open Source Policy Look Like?

Formulate

Assess

Develop

**Monitor**

- Create process for continuous monitoring of processes.
- Watch for new monitoring tools or techniques in the future.
- Perform regularly scheduled reviews for Continuous Improvement

# What is the Cost/Benefit of an Open Source Policy?

- Top Line Revenue Creation
  - For only a few business models (e.g. Google)
- Bottom Line Savings?
  - Internal Cost Reduction
  - Reduced Risk of Litigation
    - Compliant with licensing
    - Awareness of patent risk

# What Will an OS Policy Accomplish?

- Align Open Source use with corporate goals.
- Balance goals and process with productivity.
- Identify and manage risks.
- Education (Internal & External)
- Create a repeatable, consistent, and living processes as Open Source use evolves and expands in your organization.
- Manage use of components, devices and code
- Take advantage of Open Source benefit

# Recap – Accomplish Goals

- ETE Event:
  - Provide overview of Open Source
  - Discuss real-life OS Risk examples
  - Discuss OS Licensing
  - Provide overview of OS Policy triggers
  - Discuss components of a solid OS Policy
  - Open discussion

# Q & A?

# Thank You!!


**Thomas Costello**
**UpStreme, Inc.**
7 Great Valley Pkwy
Suite 210
Malvern, PA 19355
w: 610.430.3270
tcostello@upstreme.com

**Francis X. Taney, Jr.**
**Buchanan Ingersoll & Rooney, PC**
1835 Market St
14th Floor
Philadelphia, PA 19103-2985
w: 215.665.3846
francis.taney@bipc.com

**Frank Curran**
**Black Duck Software**
265 Winter Street, North Entrance
Waltham, MA 02451
w: 781.810-2073
fcurran@blackducksoftware.com

Dr. Phil Laplante
**Penn State University – Great Valley**
30 East Swedesford Rd
Malvern, PA 19355
w: 610.725.5314
plaplante@psu.edu

Anthony Gold
**Unisys**
S1108
Unisys Way
Blue Bell, PA 19424
w: 215.986.4354
anthony.gold@unisys.com