BLACKDUCK

OPEN SOURCE SECURITY
RISKS, REWARDS AND REGULATION

Black Duck Webinar

© 2014 Black Duck Software, Inc. Proprietary & Confidential All Rights Reserved.

AGENDA

- Introductions
- Open Source Deployment in Enterprise IT
- Cybersecurity Threat Landscape
- **Software Security and Regulation**
- **Practical Measures**
- Conclusion
- Audience Q&A

© 2015 Black Duck Software, Inc. All Rights Reserved.

ABOUT THOMAS EGGAR LLP

A *refreshing* approach to client relationships

Creative solutions for legal and business issues

By thinking differently, we deliver *inspiring* results

Thomas Eggar

Industry specific expertise

Retail

TMT

Financial services

Manufacturing & logistics

Sport & Leisure

Private client

© 2015 Black Duck Software, Inc. All Rights Reserved.

BLACKDUCK

DANIEL HEDLEY, ASSOCIATE

Thomas Eggar

Before becoming a lawyer Dan worked in the IT industry for a number of years as a systems administrator. He advises businesses ranging in size from single person start-ups to billion pound multinationals on software licensing, IT service and cloud contracts, data privacy issues and open source compliance.

© 2014 Black Duck Software, Inc. Proprietary & Confidential All Rights Reserved.

BLACKDUCK

Control Risks

Control Risks provides a unique joint cyber security offering to answer the key questions

- Threat Intelligence
  - Who is targeting us, why and how?
  - How is these threats evolving?
- Cyber Protect
  - What are our key assets and how are they threatened?
  - How well defended are we, and how can we improve?
- Cyber Respond
  - How can we manage, investigate and remediate a breach?

© 2014 Black Duck Software, Inc. Proprietary & Confidential All Rights Reserved.
BLACKDUCK

OLIVER FAIRBANK, INTELLIGENCE ANALYST

Control Risks

As an Analyst on Control Risks cyber Threat Intelligence team, Oliver is responsible for conducting a range of primary research into emerging cyber threats and the evolving threat landscape, and managing and producing a number of Control Risks' cyber security products, including the CTI subscription service, bespoke threat assessments and Control Risks' work with the Bank of England's CBEST scheme.

© 2014 Black Duck Software, Inc. Proprietary & Confidential All Rights Reserved.

BLACKDUCK

BLACK DUCK CREATED AN INDUSTRY

24
Countries

185+
Employees

1,600
Customers

27 of the Fortune 100

7 of the top 10 Software companies, and 44% of the top 100

6 of the top 8 Mobile handset vendors

6 of the top 10 Investment Banks

Four Years in the "Software 500" Largest Software Companies

Six Years in a row for Innovation

Gartner Group "Cool Vendor"

Award for Innovation

"Top Place to Work," The Boston Globe

© 2015 Black Duck Software, Inc. All Rights Reserved.

BILL WEINBERG, SR. DIRECTOR OSS STRATEGY

Bill helps Global 1000 companies enable, build, secure and deploy software for IoT, enterprise data centers, and cloud infrastructure.

Bill's worked with FOSS since 1997, and for thirty years total in embedded and open systems, telecoms, and enterprise software. He was a founding team-member at MontaVista Software, and Senior Analyst at OSDL (today, the Linux Foundation)

Learn more at Linuxpundit.com

© 2015 Black Duck Software, Inc. All Rights Reserved.

OPEN SOURCE DEPLOYMENT IN ENTERPRISE IT

An unstoppable force

© 2014 Black Duck Software, Inc. Proprietary & Confidential All Rights Reserved.


CORPORATE USE
@FUTUREOFOSS
#FUTUREOSS
78% OF COMPANIES
RUN ON OPEN SOURCE
LESS THAN 3%
DON'T USE OSS IN ANY WAY

CORPORATE USE

@FUTUREOFOSS
#FUTUREOSS

USE OF OPEN SOURCE TO RUN BUSINESS IT ENVIRONMENTS HAS GONE UP

2x

SINCE 2010

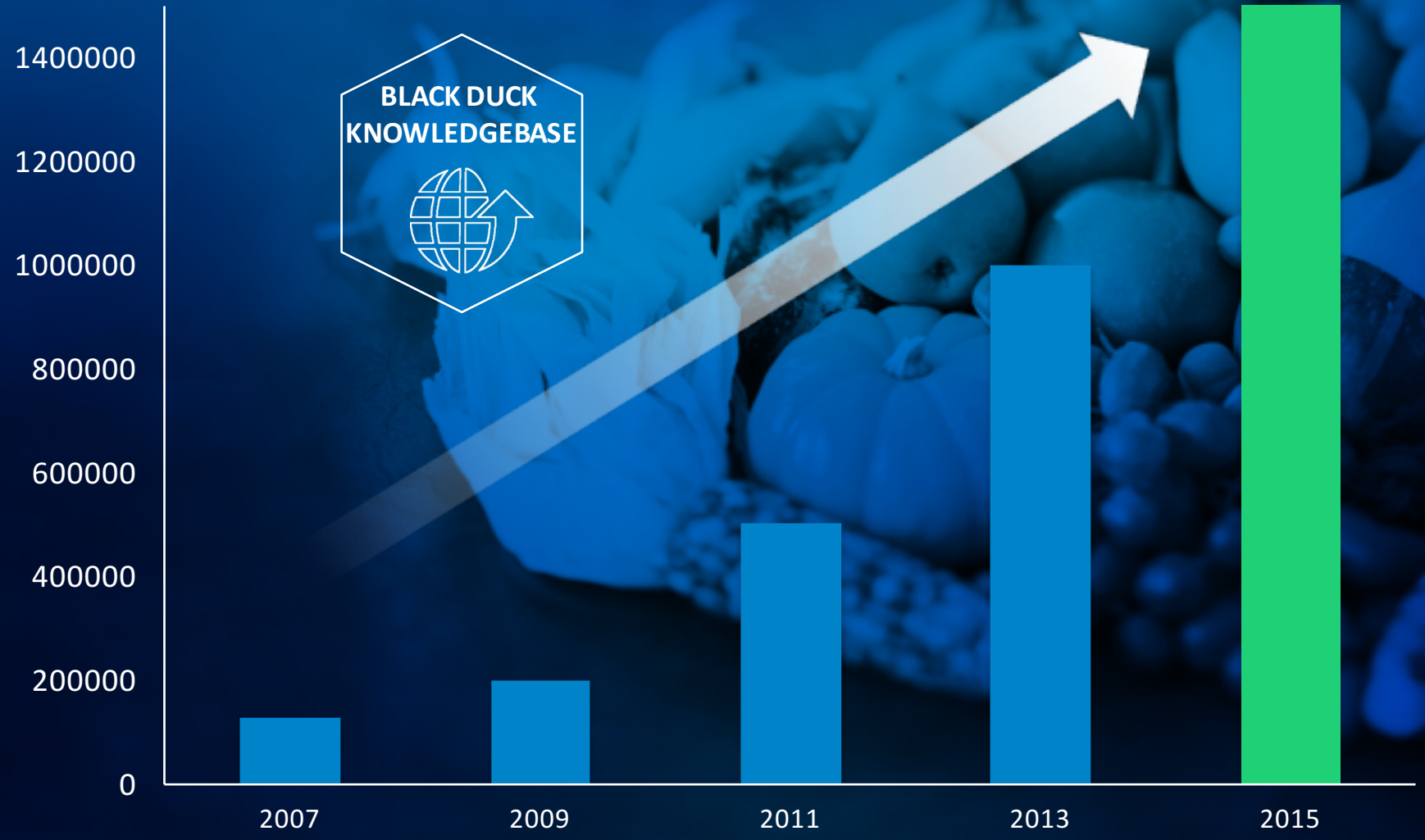
CORPORATE USE

@FUTUREOFOSS
#FUTUREOSS

INCREASING **ABUNDANCE**

Open Source Projects

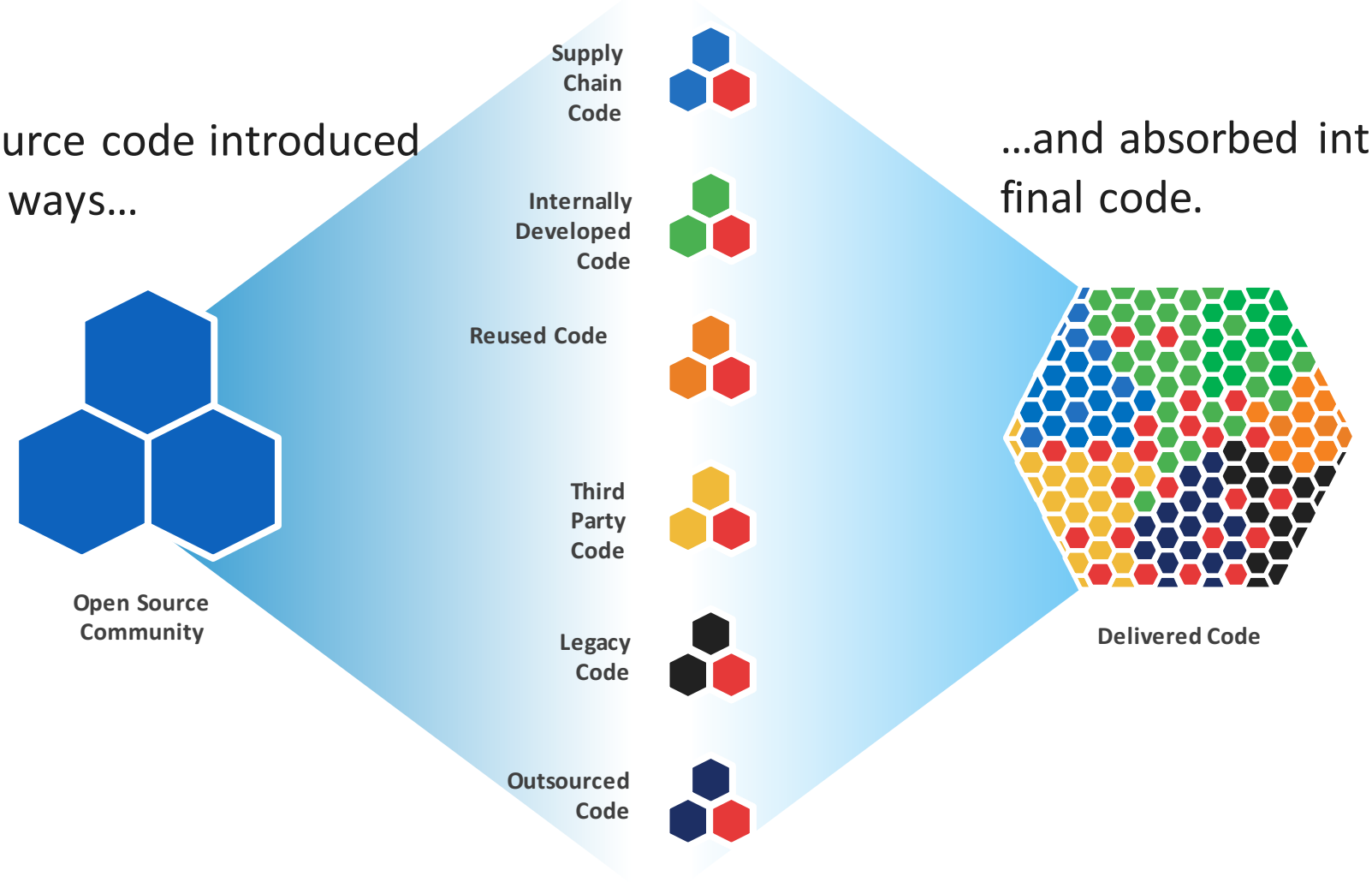
BLACK DUCK KNOWLEDGEBASE



Source: Black Duck Software

HOW OPEN SOURCE ENTERS THE ENTERPRISE CODEBASE

Open source code introduced in many ways…



…and absorbed into final code.

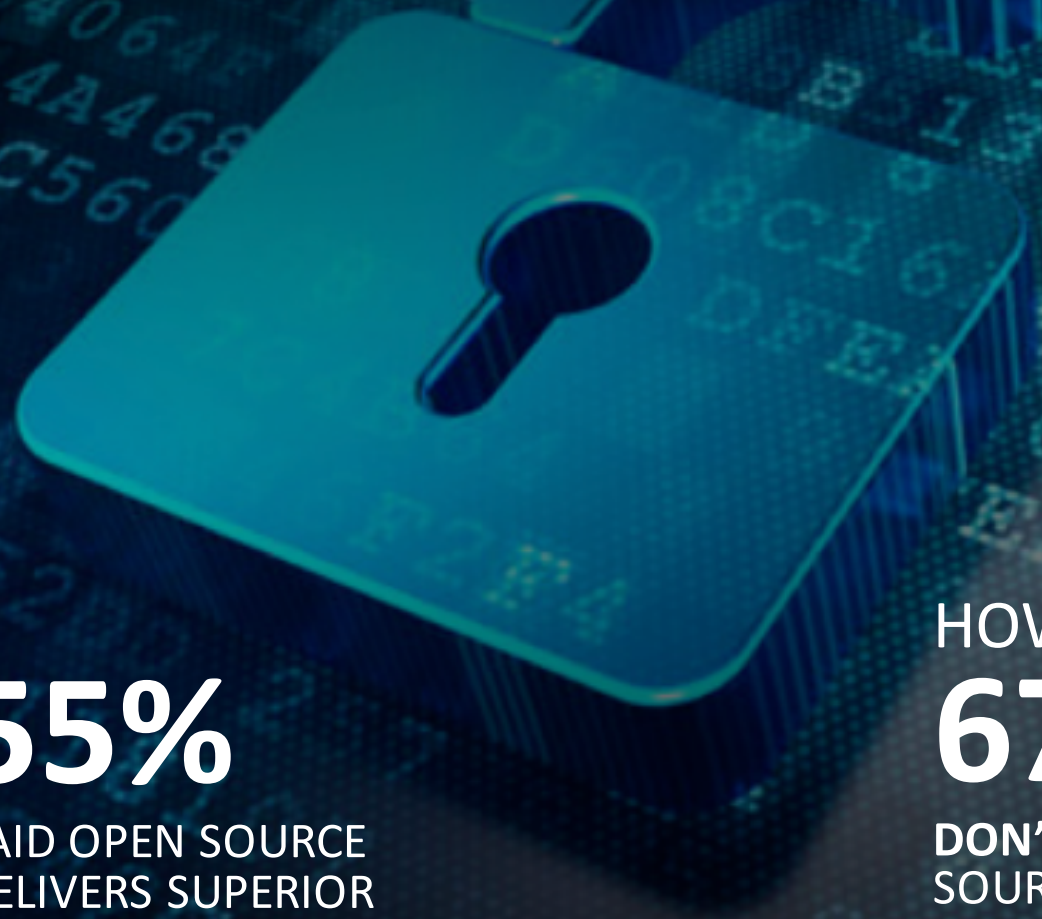
© 2015 Black Duck Software, Inc. All Rights Reserved.

BLACKDUCK

SECURITY

@FUTUREOFOSS
#FUTUREOSS

THE SECURITY OF OPEN SOURCE



46%

GIVE OSS FIRST CONSIDERATION AMONG SECURITY TECHNOLOGIES

55%

SAID OPEN SOURCE DELIVERS SUPERIOR SECURITY

HOWEVER,

67%

DON'T MONITOR OPEN SOURCE CODE FOR SECURITY VULNERABILITIES.

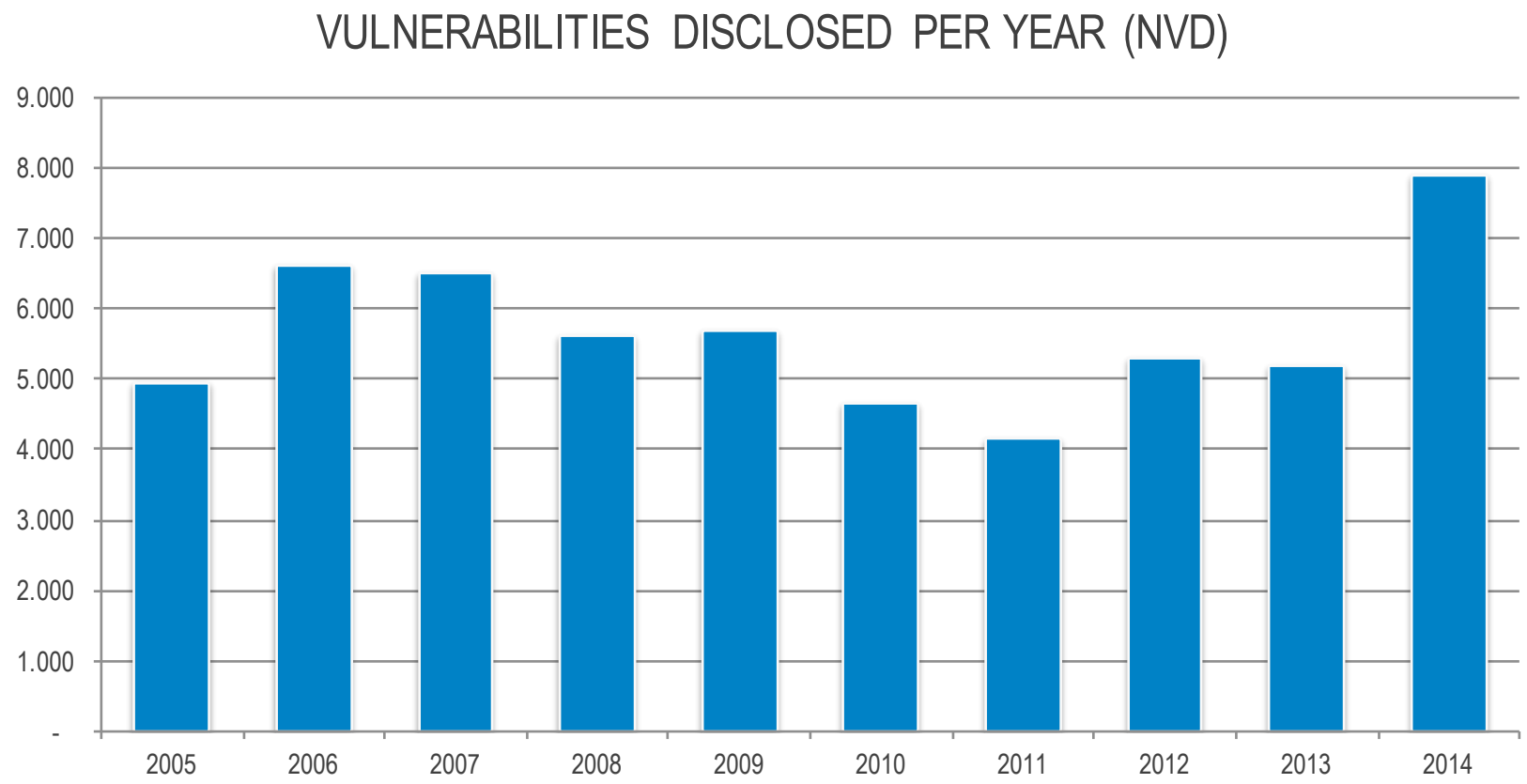
RISKS OF OPEN SOURCE DEPLOYMENT

Cybersecurity Threat Landscape

© 2014 Black Duck Software, Inc. Proprietary & Confidential All Rights Reserved.

BLACKDUCK

INCREASING VULNERABILITIES



In 2014:

- Over 7,900 new vulnerabilities disclosed & catalogued
- ~4,300 in Open Source, ~3,600 in commercial software

Reference: Black Duck Software knowledgebase, NVD

© 2015 Black Duck Software, Inc. All Rights Reserved.

WHAT DO THESE VULNERABILITIES HAVE IN COMMON?

	Heartbleed	Shellshock	Freak	Ghost	Venom
Since:	2011	1989	1990's	2000	2004
Discovered:	2014	2014	2015	2015	2015
Discovered by:	Riku, Antti, Matti, Mehta	Chazelas	Beurdouche	Qualys researchers	Geffner
Component:	OpenSSL	Bash	OpenSSL	GNU C library	QEMU

© 2015 Black Duck Software, Inc. All Rights Reserved.

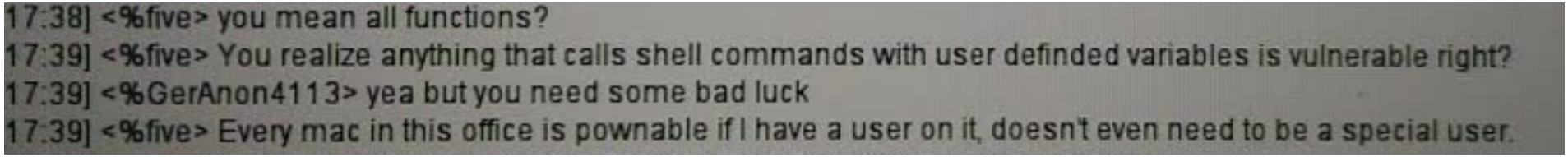
BLACKDUCK

- Have vulnerabilities in open source software contributed to actual exploits and breaches to date?
- Have nation state/cybercriminal/cyber activist attacks targeted OSS in particular?
- Given the ubiquity of open source, is going proprietary even an option?

© 2015 Black Duck Software, Inc. All Rights Reserved.

REAL WORLD EXAMPLES OF VULN EXPLOITATION

Discussion on a cybercriminal forum of techniques for exploiting the Shellshock vulnerability



Cyber activists discuss exploiting Shellshock on an Internet Relay Chat (IRC) Channel

© 2015 Black Duck Software, Inc. All Rights Reserved.
BLACKDUCK

SOFTWARE SECURITY AND REGULATION

© 2014 Black Duck Software, Inc. Proprietary & Confidential All Rights Reserved.

BREACHES

Many breaches are enabled or worsened by lax security practices (e.g., Sony, multiple retail sites, et al.)

Governments are reacting by attempting to regulate corporate security practices

(e.g., the Royce Bill in the U.S.)

BLACKDUCK

REGULATION

- How are governments in Europe and elsewhere working to regulate cybersecurity?
- How does open source fit into legislative vision for security?
- How effective will attempts be to reduce cyber attacks through regulation?

© 2014 Black Duck Software, Inc. Proprietary & Confidential All Rights Reserved.

BLACKDUCK

OPEN SOURCE GOVERNANCE – WHAT IS IT?

- Open source governance comprises the policies, processes, procedures and also tradition and culture that surround the creation, development, integration, deployment and maintenance of open source software (OSS).
- It can apply to community projects, to individual, and to organizations who consume, contribute to, (re)distribute, and use open source software
- Governance is important for communities and commercial and governmental organizations, and also comprises tools that facilitate governance activities.

© 2015 Black Duck Software, Inc. All Rights Reserved.

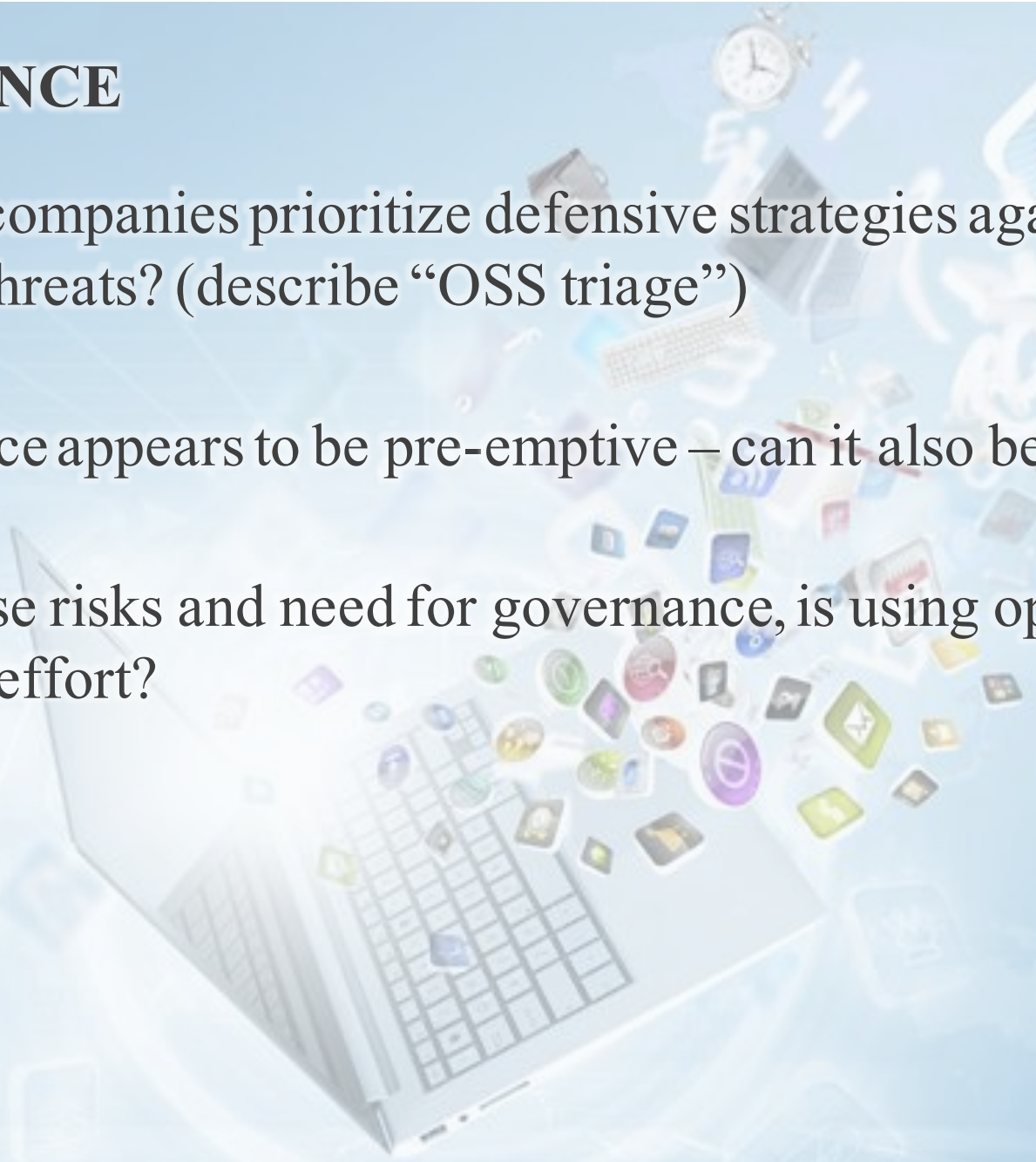
GOVERNANCE

- Do businesses need to treat open source software differently? How?
- What risks arise from poor open source governance?
- How does OSS security form part of good overall OSS governance, and how does good governance enhance security?
- How can engineering and legal teams collaborate for better governance?

© 2014 Black Duck Software, Inc. Proprietary & Confidential All Rights Reserved.

GOVERNANCE

- How can companies prioritize defensive strategies against evolving threats? (describe “OSS triage”)
- Governance appears to be pre-emptive – can it also be remedial?
- Given these risks and need for governance, is using open source worth the effort?



© 2014 Black Duck Software, Inc. Proprietary & Confidential All Rights Reserved.

CONCLUSIONS AND Q&A