



To Catch A Thief: Preventing the Next Fortune 500 Data Breach

Rob Eggebrecht

President and CEO, BEW Global

John Ochman

Manager, Security Operations, BD



Who is BEW Global?

- Internationally recognized leader in critical asset protection
 - Founded in 2002
- DLP Expertise
 - Symantec Master Specialization DLP Partner
 - 1st Managed DLP services provider (2008)
 - Manage DLP solutions in 22 countries
 - Daily management of 1,000,000+ users
 - Global support in more than 130 countries
 - Completed 500+ assessments
 - Deployed 400+ DLP projects

Who is Becton, Dickinson and Company?

- Global medical technology company
 - Founded in 1897
 - Focus on improving drug delivery and advancing drug discovery
 - Enhancing the quality and speed of diagnosing infectious diseases and cancers
- Three worldwide business segments: BD Medical, BD Diagnostics, BD Biosciences
- ~30,000 employees in over 50 countries
- FY13 revenues in excess of \$8 billion
- Global Research Segment – Research Triangle Park, NC

Session Agenda

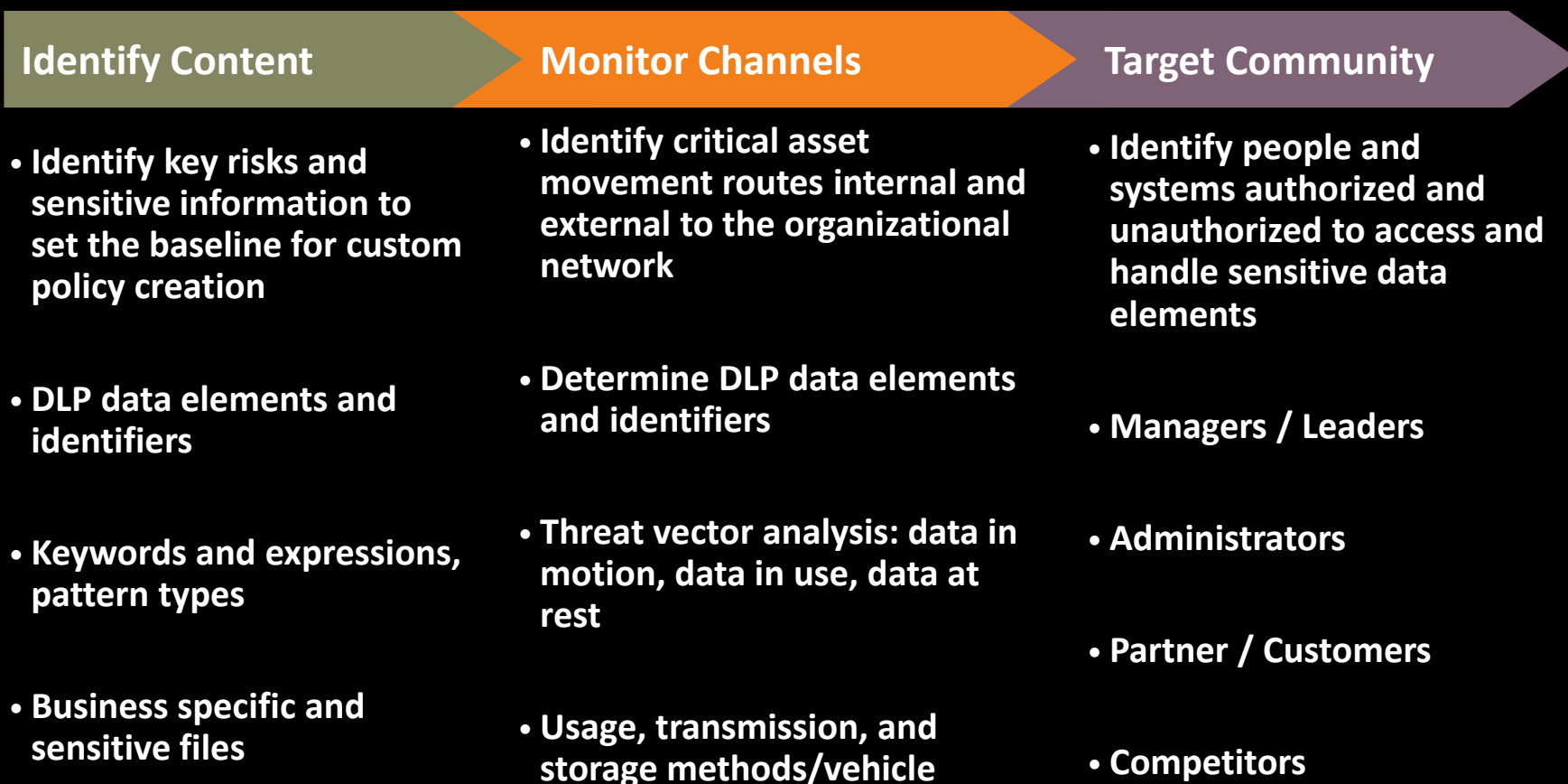
- 1 BD and Critical Asset Protection
- 2 Designing and Operating BD's DLP Program
- 3 Attempted Intellectual Property Theft

Data Protection Concerns and Programmatic Needs

- Top priority: protection of intellectual property
- Existing tools: SIEM
 - Worked well for certain bits and bytes, not content and context
- Gap identified: inability to describe IP to existing systems
- Evaluate potential options with a consulting engagement

Develop Policy Governance

Establish information content and context criteria to accurately detect, monitor and protect critical assets



Designing the Critical Asset Protection Program Leveraging Symantec DLP

- First, reached out to HR, Legal, various business units
 - Goal: identify and target specific areas of highly-valued intellectual property
- Second, reached out to different business regions
 - Goal: make sure DLP system compliant with different regions' regulations
- Forged relationships with key business unit executives to gain buy-in for program development

** Consider pitfalls companies encounter when designing DLP programs*

Narrowing the Scope

- Identified greatest risk areas based on revenue, income, reputational impact
- Narrowed down scope after research
- Sought volunteer for program
- Business unit volunteered after John described DLP solution

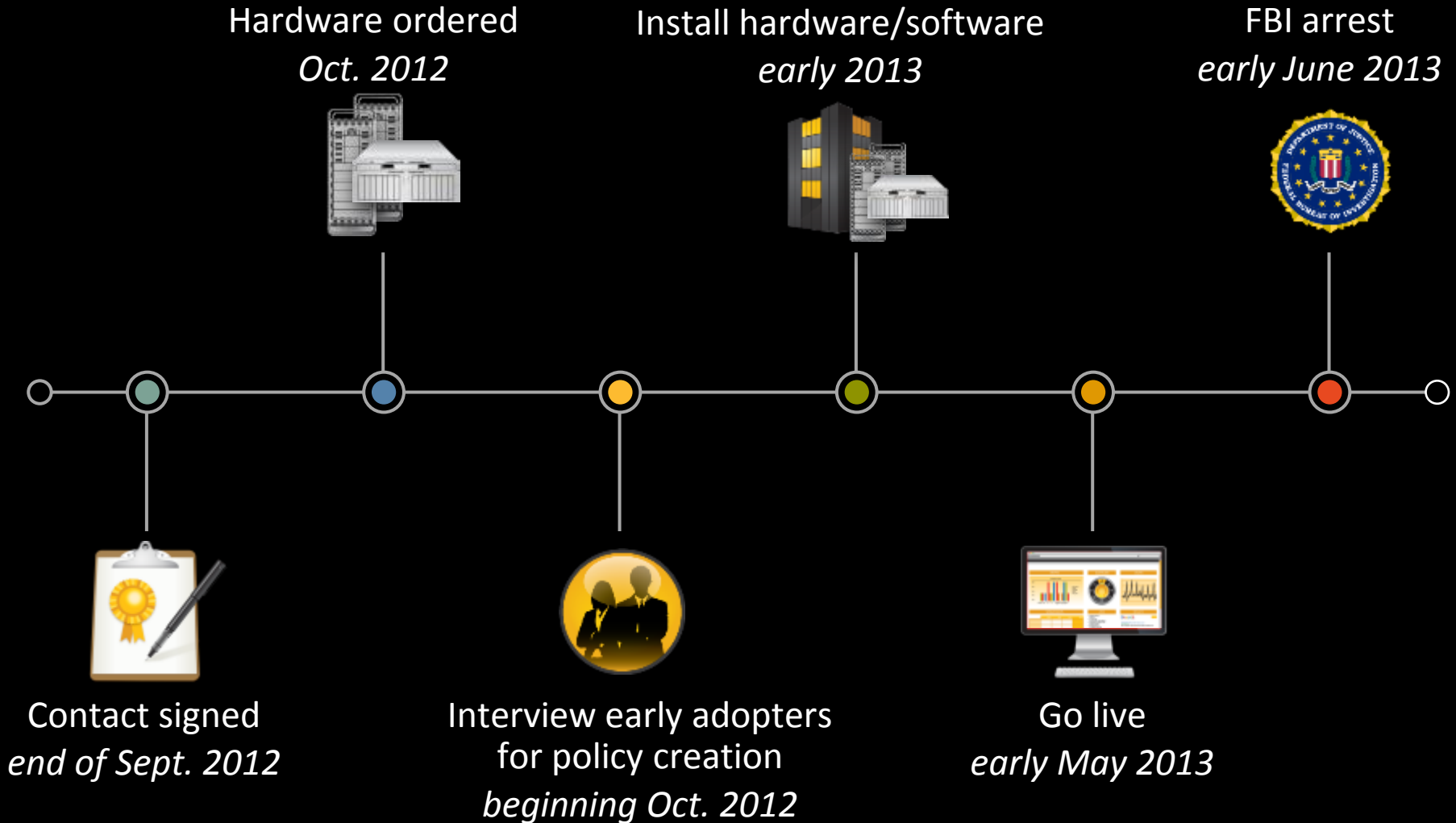
A close-up photograph of a hand holding a black pen, writing on a document. The document has several checkboxes, and the pen is currently positioned over one of them. The background is blurred, showing what appears to be a desk or office environment.

Deploying and Operating BD's DLP Program

Deploying the DLP Technology Globally

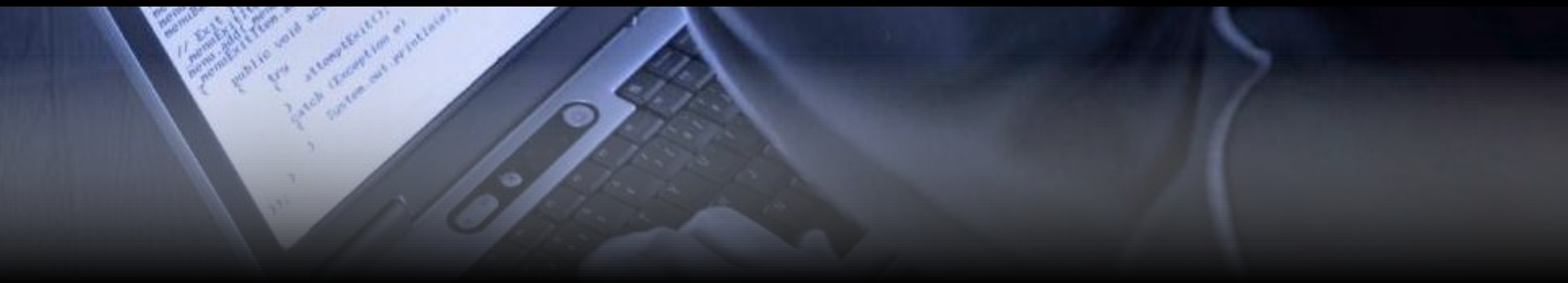
- Full global rollout of Symantec DLP
 - 22,000 endpoints
- Deployed DLP in motion, in use, at rest
 - Data at rest targets were defined at end of rollout
- Expected rollout 12 to 18 months
 - In reality, 9 months start to finish
 - Deployed technology while John's team collected policy information
- Began with early adopters, then expanded

Deployment Timeline





The Attempted Intellectual Property Theft



Identification of Suspicious Activity

- Single user with numerous endpoint infractions
- Downloading of sensitive documents and storage on USB device
- High network activity by the same user
- Notification to Becton Dickinson for follow up



Incident Response Process

- Internal investigation
- Worked with business unit management, HR, and internal legal council
- Notified local authorities who contacted federal officials
- FBI arrest



Key Takeaways

- Streamlined business processes
- Greater insight into information flow
- Prevented theft
- Strong buy-in from the business

Tell us what you thought!

Session Survey

Please take a few minutes to fill out the short session survey available on the mobile app—the survey will be available shortly after the session ends. Watch for and complete the more extensive post-event survey that will arrive via email a few days after the conference.

To download the app, go to <https://vision2014.quickmobile.com> or search for Vision 2014 in the iTunes or Android stores.

To Learn More About DLP

Wednesday, May 7th

- 9:00 AM – Hands-on Tour of DLP Lab
- 4:30 PM – The Balancing Act Between Security and the Business

Thursday, May 8th

- 9:00 AM – Solving the Mystery of Data Ownership Lab
- 10:15 AM – The Future of DLP: Vision & Roadmap
- 11:30 AM – Hands-on Tour of DLP Lab





Discoveries from the DLP Program

Discoveries

- Addressing Business Requirements
 - Consultant downloading sensitive design documents to USB
 - DNA sequencing
 - Macintosh
- Windows Desktop/Laptop Management Issue
 - 2000 machine gap
- Office 365
- Change security standard policy
 - Change from 'may monitor' to 'does monitor'
- Active Directory Groups
 - HR versus Security Policy and Reporting needs
- Span Ports – multiple security tools require same traffic
 - Lesson learned: Buy with future needs in mind

Avoiding Common Pitfalls – A New Way of Thinking

- Old vs. New
 - Technology professionals well-versed in IS, using bits and bytes technology
 - New challenges require different paradigm
- Content and context thinking
- DLP requires different business units to be involved to help describe IP
- DLP is visible to end users, unlike firewalls or IDS/IPS



Thank you!

Rob Eggebrecht
robert@bewglobal.com

John Ochman
john_ochman@bd.com

Copyright © 2014 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.