



Security 2012: A Handbook for Cyber Security

Amichai Shulman, CTO

**Robert Rachwald, Director of
Security Strategy**

IMPERVA

Session ID: SECT-204

Session Classification: General Interest

RSACONFERENCE2012

Agenda

- Trend selection process
- Score card for 2011
- Brief overview of 2012 trends
- In-depth discussion and mitigation techniques:
 - SSL Gets Hit in the Crossfire
 - Internal Collaboration Meets Its Evil Twin
 - NoSQL = No Security?
 - The Kimono Comes off of Consumerized IT
- Mitigation strategies for the other trends



Trend Selection Process

- Collect Information
 - Media reports
 - Analysts
 - Incident reports
 - Customer feedback
 - Vulnerabilities, hacker forums
- Analyze
 - Extract the chaff from the wheat
- Trends are not necessarily technical
 - Information security is influenced by human nature at least as it is by technology
 - Business environment and legislative trends have huge impact



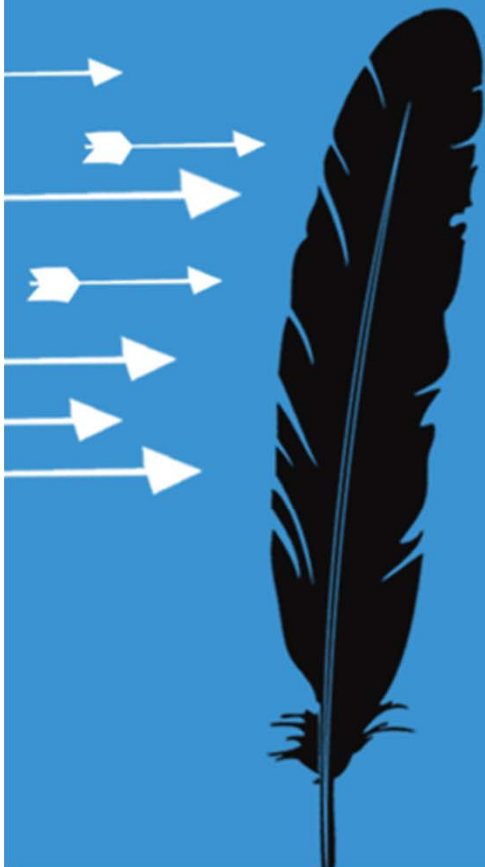
Top Security Trends for 2012: Brief Overview

- SSL Gets Caught in the Crossfire
- HTML5 Goes Live
- DDoS Moves Up the Stack
- Internal Collaboration Meets Its Evil Twin
- NoSQL = NoSecurity?
- The Kimono Comes Off of Consumerized IT
- Anti-Social Media
- The Rise of the Middle Man
- Security (Finally) Trumps Compliance

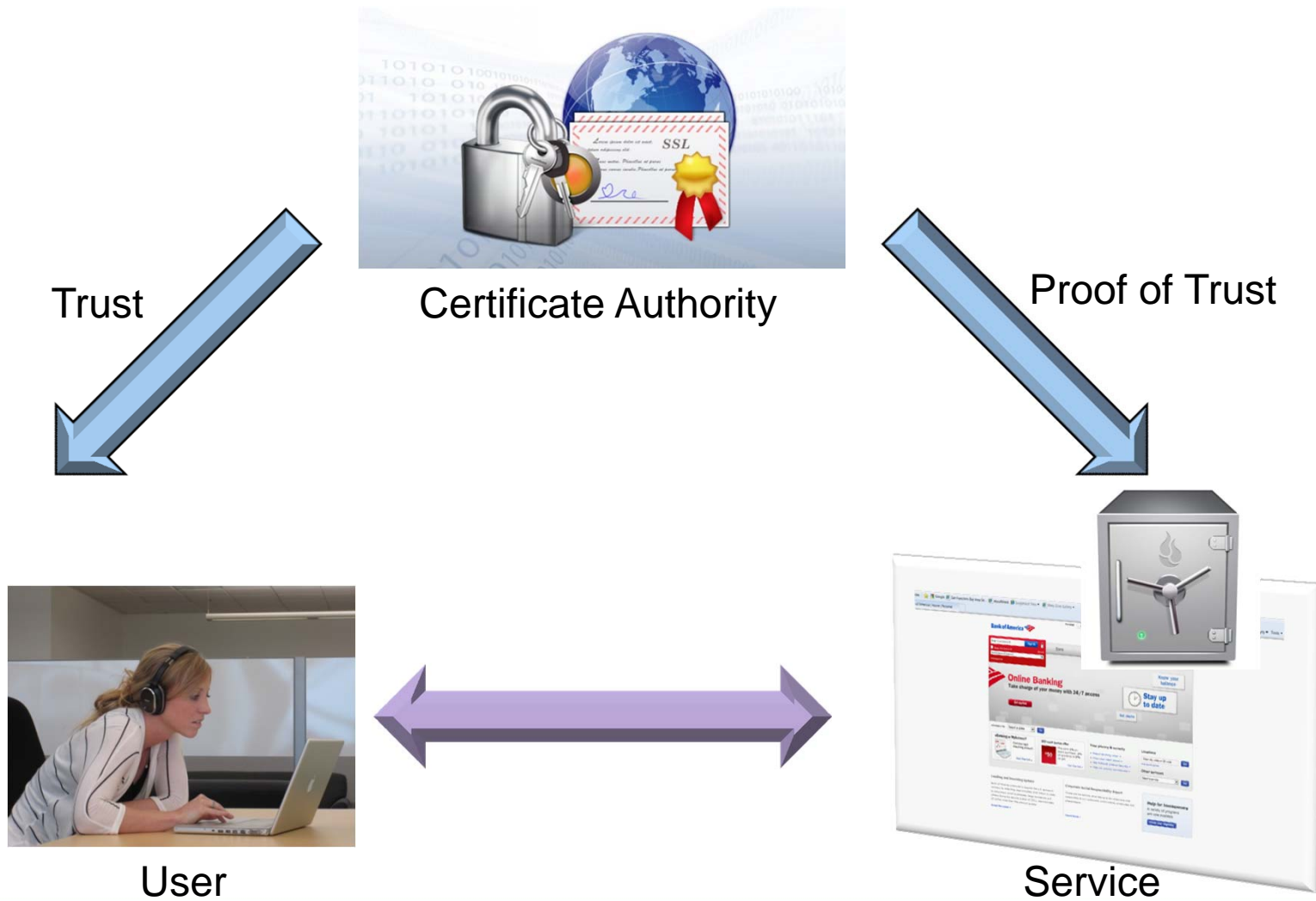


SSL Gets Caught in the Crossfire

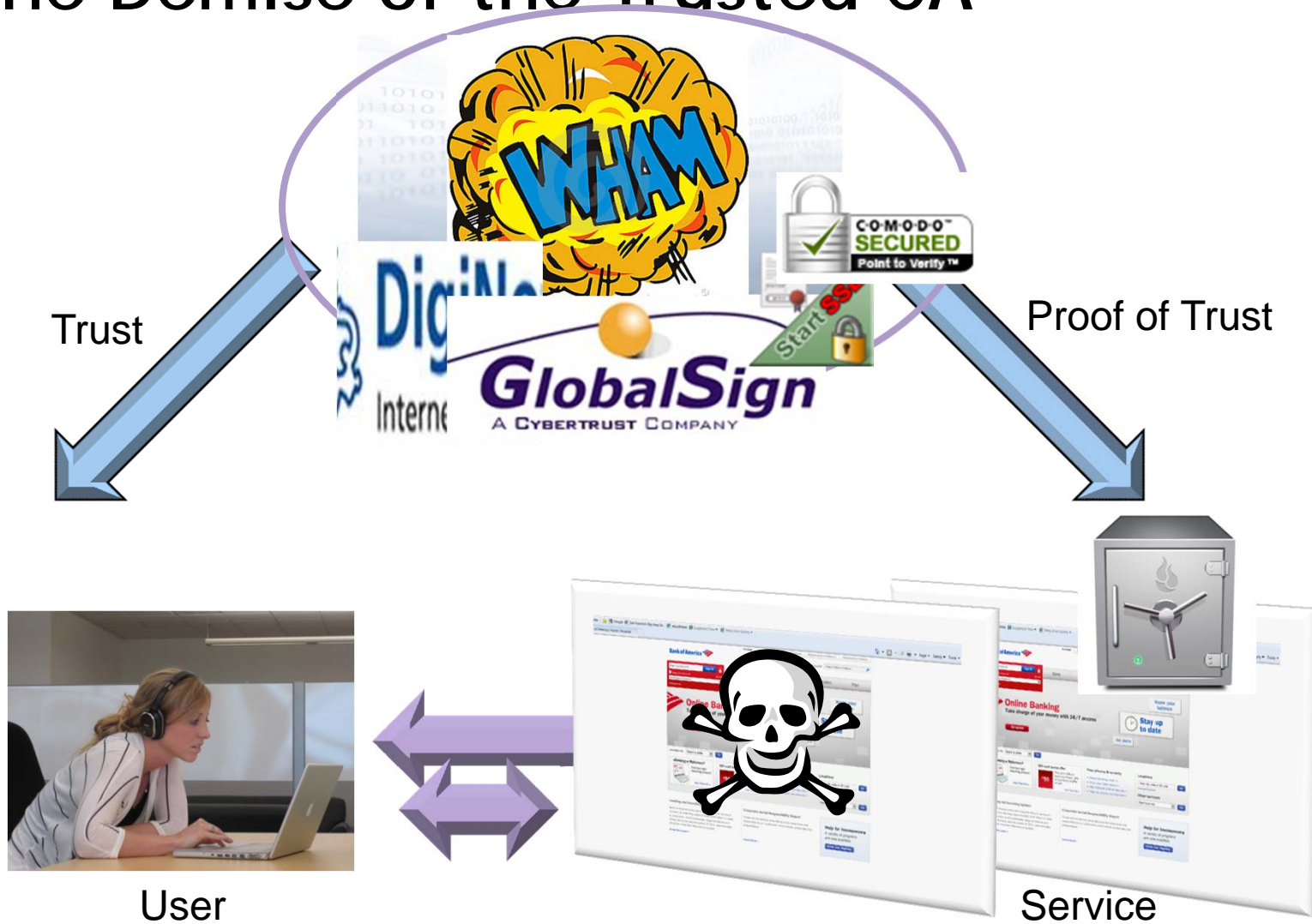
The distributed trust model based on SSL and PKI as currently implemented is going bankrupt



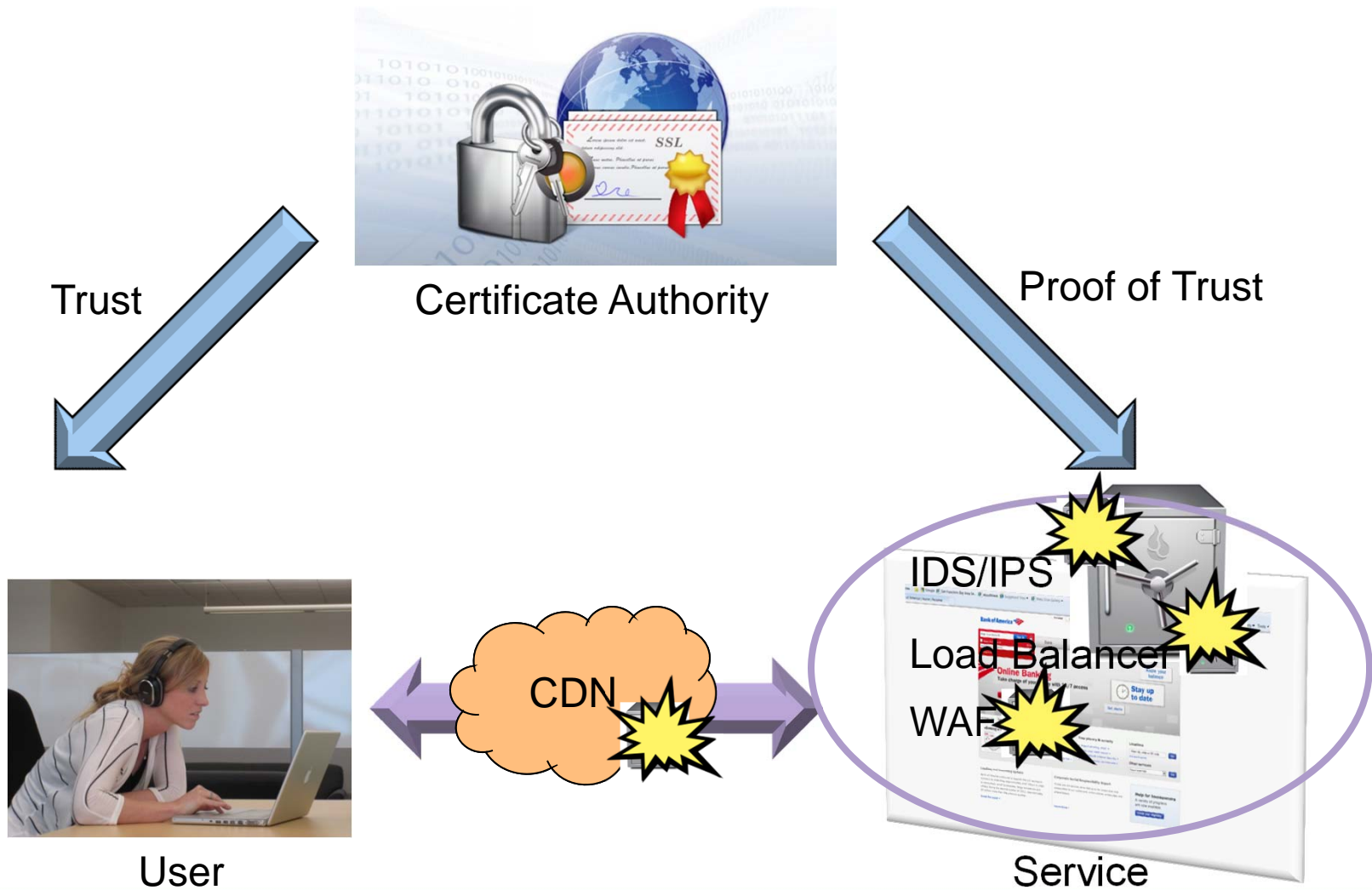
Brief Overview of SSL



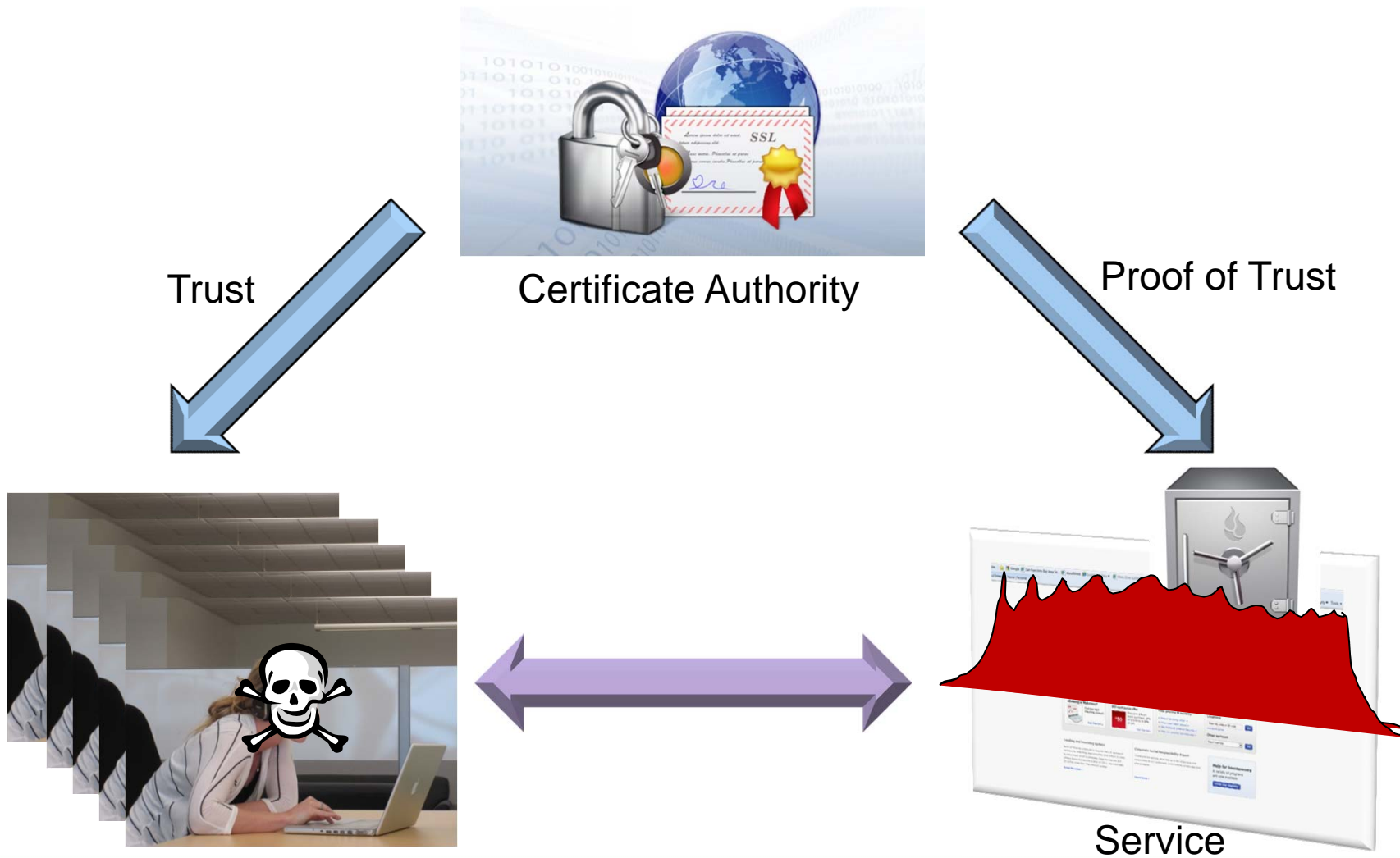
The Demise of the Trusted CA



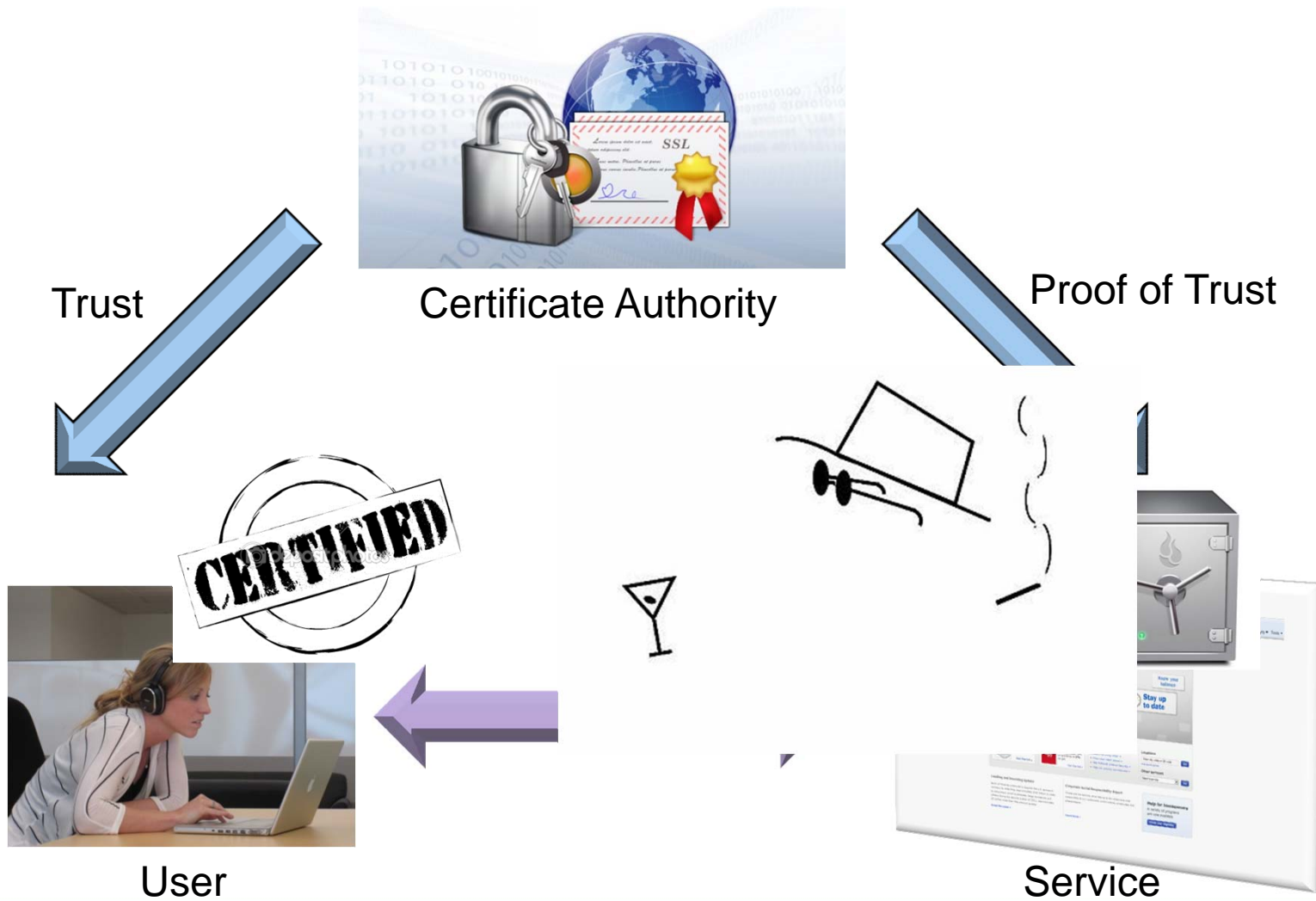
Targeting Corporate Certificates



Denial of Service Attacks



There's More ☺



SSL Caught in the Crossfire: Mitigation Strategies

- Invoke a serious discussion about real alternatives for secure Web communications
 - Moxie Marlinspike took off the glove in Blackhat 2011
 - Requires both industry and academic research
- Strengthen anti-Dos and anti-DDoS protection



SSL Caught in the Crossfire: Summary

- Attackers are increasingly focusing their attacks against the various components of SSL
- Attacks against PKI
 - Attackers have repeatedly compromised various CA organizations
 - Any CA can issue a digital certificate for any application
 - A hacker, who gains control on any CA, can issue forged certificates and impersonate any website
- The theft of issued certificates
 - Application certificates are no longer limited to being stored by the application
 - Proxies, load balancers, content delivery networks, DLP and WAF solutions need to access the certificate's private key
- Denial of service attacks
 - Heavy computational burden by the SSL-handshake process



SSL Caught in the Crossfire: Summary (cont.)

- Hackers will leverage SSL to carry out their attacks with increased confidentiality
 - Intermediate proxies cannot add headers to indicate original sender IP address
 - Loss of information when following a link from an SSL page to a non-SSL page
 - Security devices lose visibility due to encryption
- Same PKI infrastructure is used for code signing
 - OS security
 - Mobile app market security

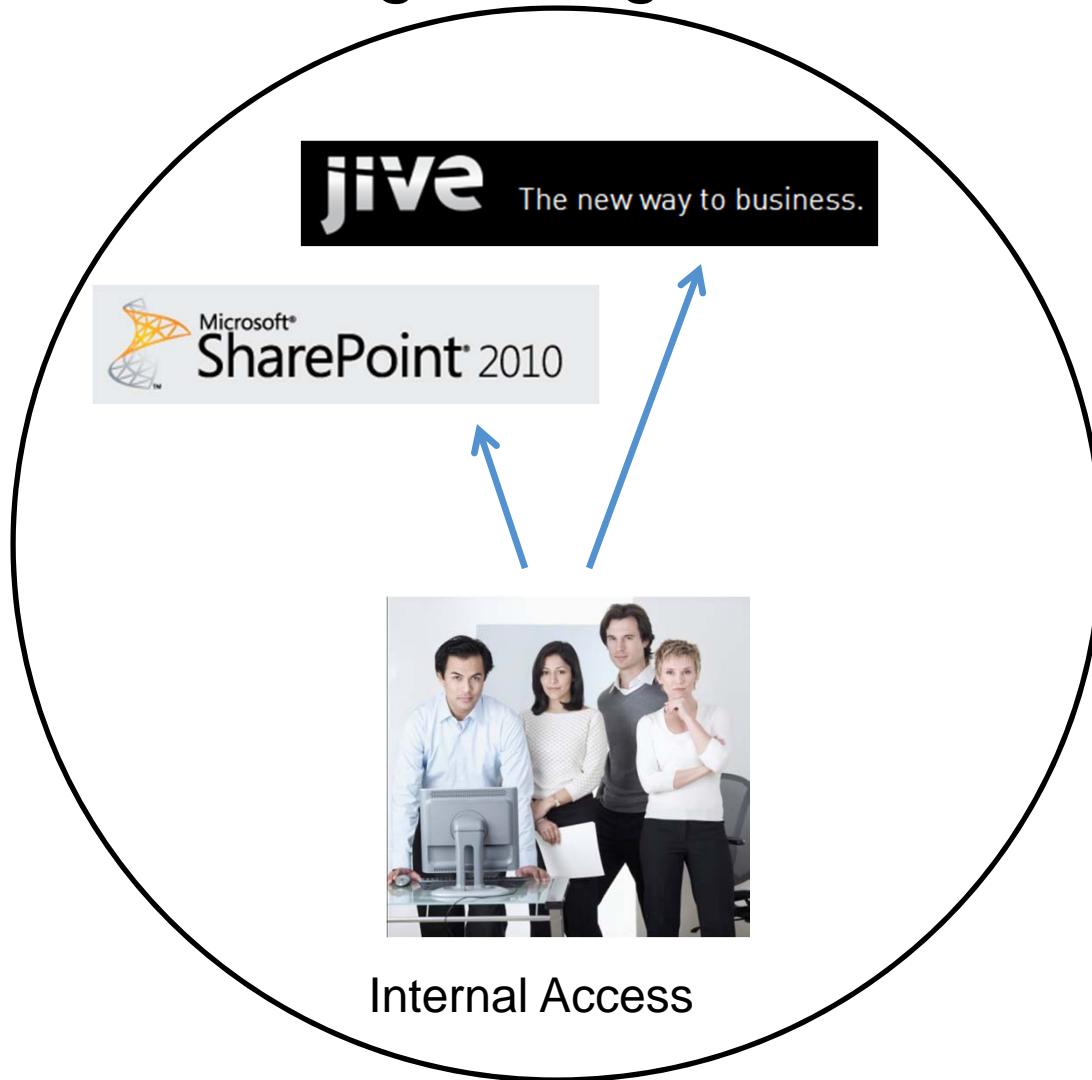




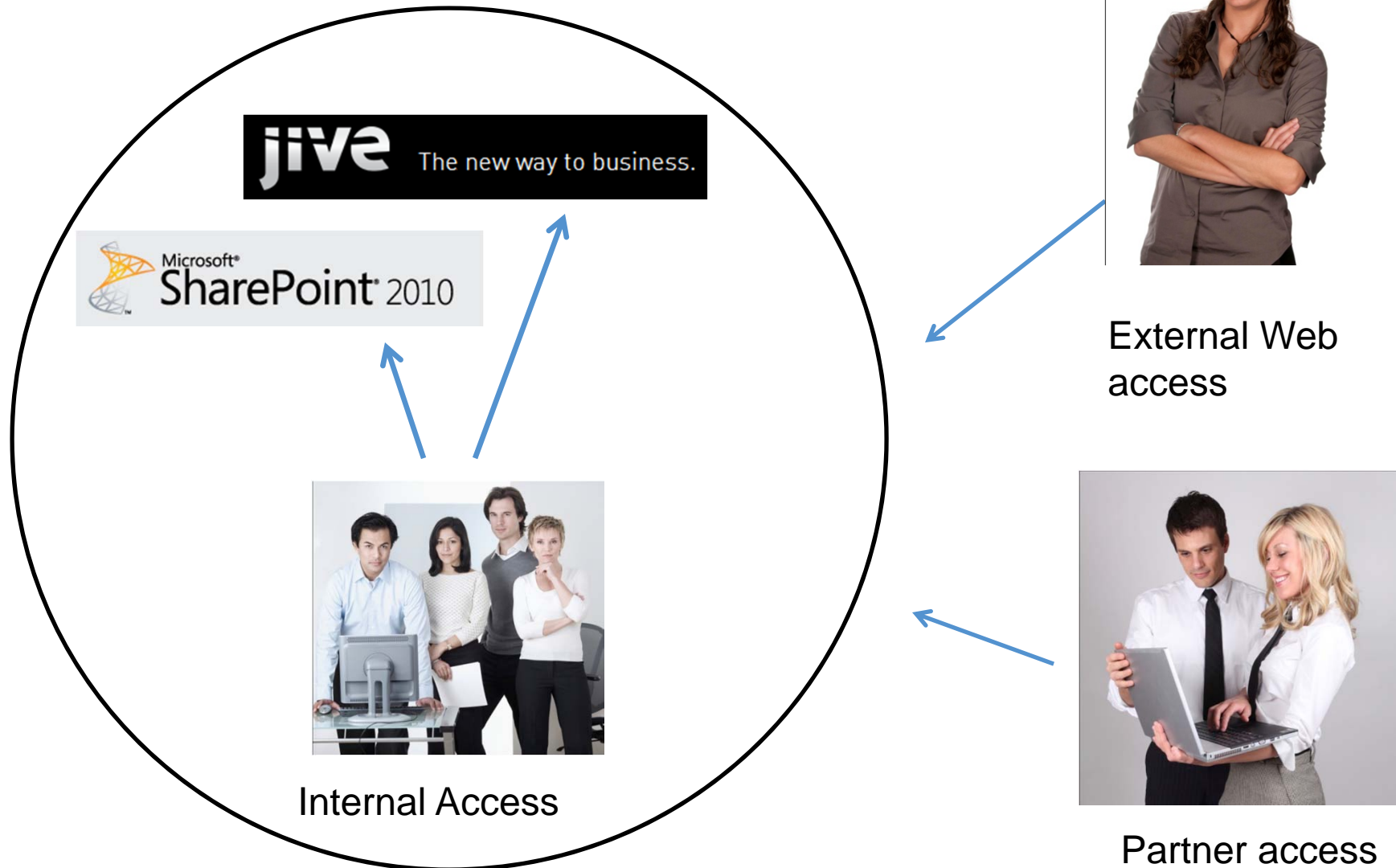
Internal Collaboration Meets its Evil Twin

We expect to see a growing number of data breaches from internal collaboration platforms used externally.

In the Beginning...



Food Brings Appetite



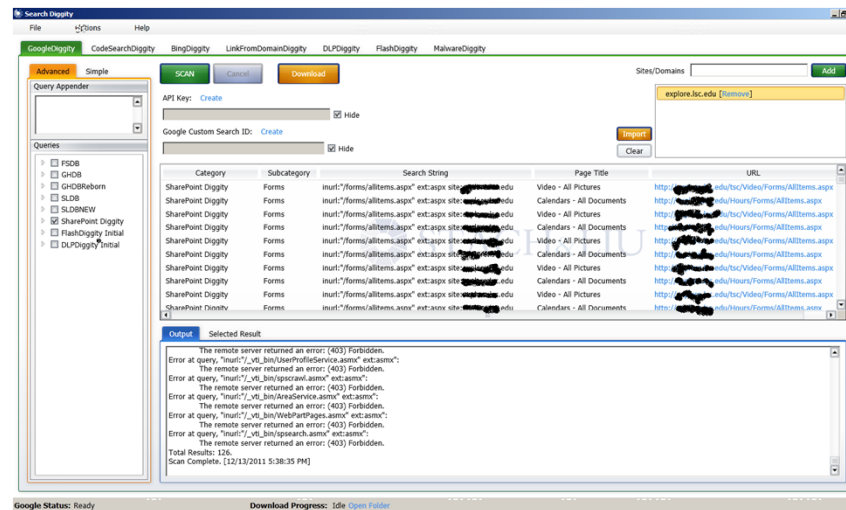
Risks

- Confidential Data Control
 - A platform hosting confidential information is exposed externally
 - Access control and governance mechanisms are not necessarily scalable to large crowds
 - Lack of security and governance expertise around existing capabilities



Risks

- Exposure to Search Engines
 - Search engines constantly crawl and update their indexing policies so that any breaches or mis-configured entry points are quickly apparent to all.
 - Google hacking tools. E.g. SharePoint GoogleDiggity, Sharepoint URLBrute



Risks (cont.)

- Increased Threat Profile - Hackers
 - Advanced technical skills
 - Global access and population size
 - Additional motivation



Internal Collaboration Meets its Evil Twin: Mitigation Strategies

- Add attack protection solutions around collaboration suites
- Use strict monitoring and look for increased data governance solutions
- Introduce scalable user rights management solutions
- Look for data leakage by integrating classic DLP and Google Hacking services tools



Internal Collaboration Meets its Evil Twin: Summary

- We predict a growing number of data breaches due to internal collaboration platforms which are used externally.
 - Platforms such as Microsoft SharePoint and Jive are used by many organizations to share information and manage content.
 - Some organizations have also extended the use to partners and even to the public via Websites.
- Risks of extending an internal platform to external use:
 - Data segregation.
 - Ensuring that stored sensitive data does not become accessible through the less restricted interfaces of the platform is not an easy task.
 - For the entire lifetime of the systems, controls should be put in place to allow collaboration and sharing of sensitive information within the organization while keeping it out of the reach of the general public.



Slide 21

a2

I feel that the next two slides are redundant

amichai, 12/13/2011

Internal Collaboration Meets its Evil Twin: Summary (cont.)

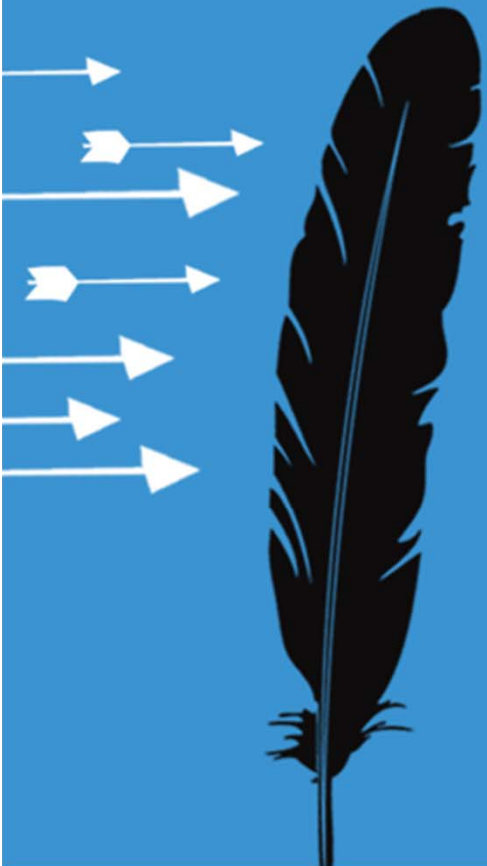
- Risks of extending an internal platform to external use -cont:
 - Threat profile - the difference between the internal and external threat.
 - The size of potential attacker population increases instantaneously.
 - Search engines constantly crawl and update their indexing policies so that any breaches or mis-configured entry points are quickly apparent to all.
 - Google hacking tools. E.g. SharePoint GoogleDiggity, Sharepoint URLBrute



Slide 22

a3

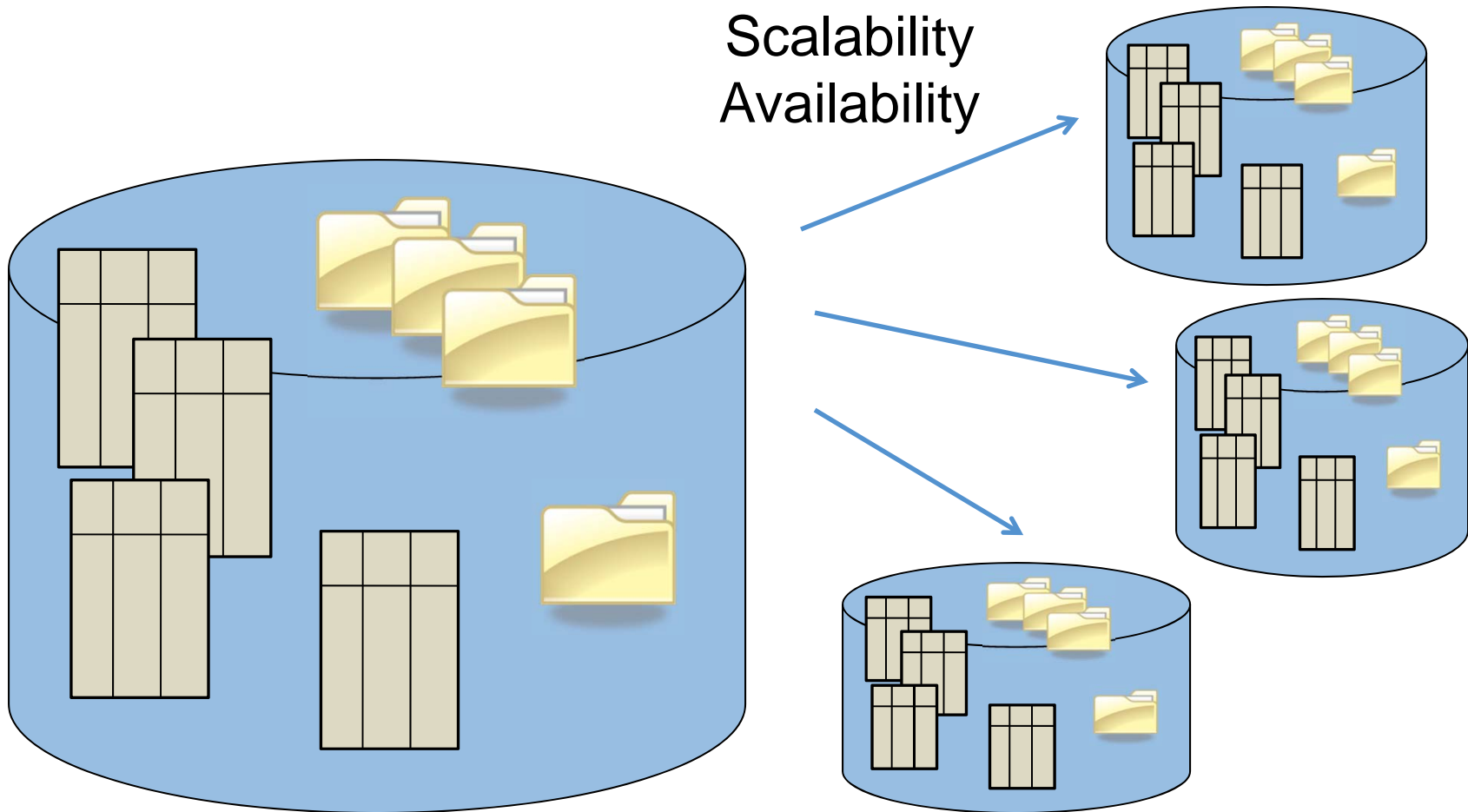
See previous comment
amichai, 12/13/2011



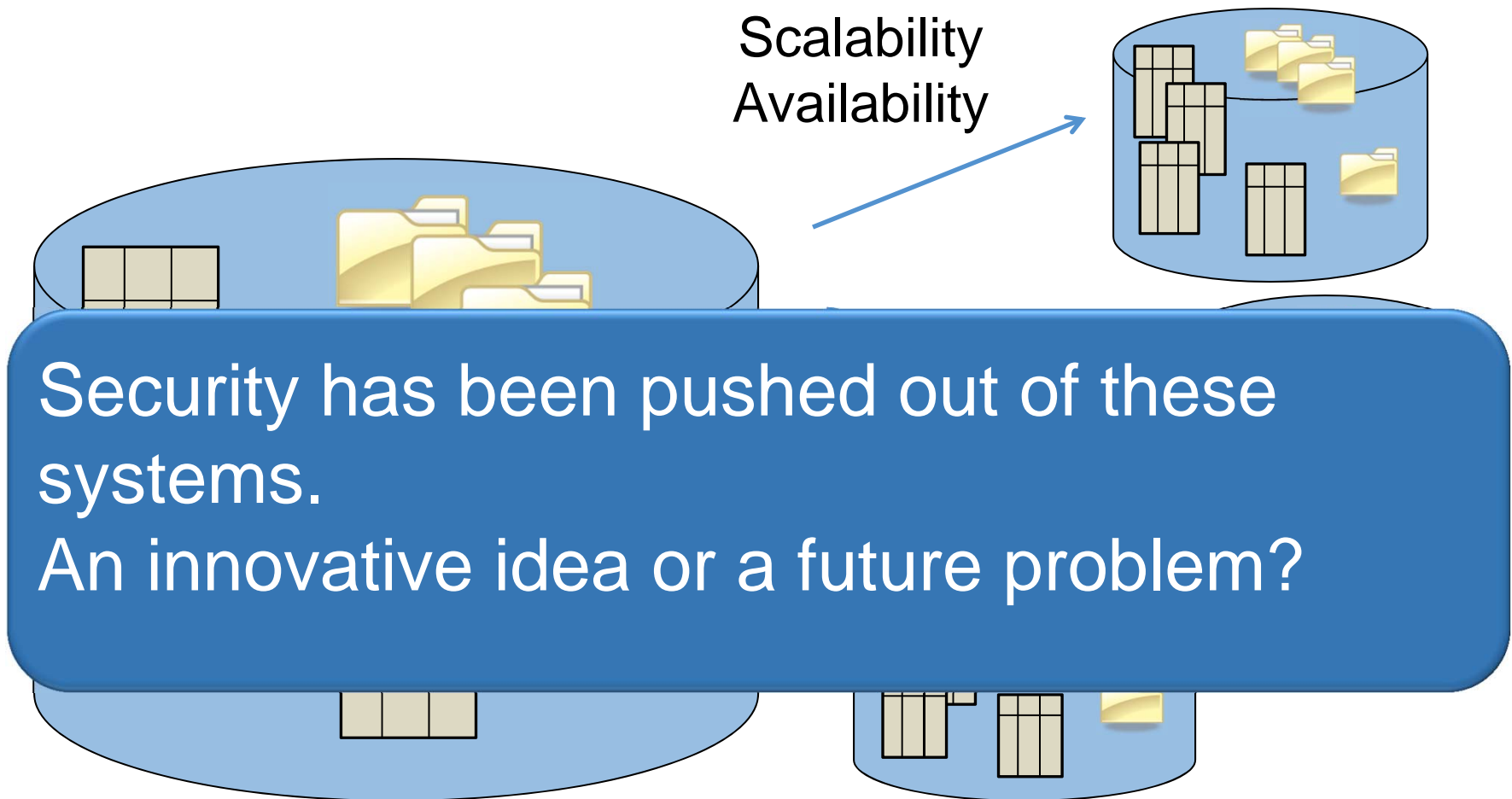
NoSQL = No Security?

We expect NoSQL data security to become a concern for enterprises next year, possibly following some actual breaches.

BIG Overview of Big Data



BIG Overview of Big Data Security



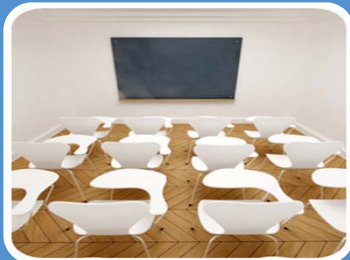
RISKS



Model Maturity



Software Maturity



Staff Maturity



Risks (cont.)



Client Software – Re-inventing the Wheel



Data Redundancy and Dispersion



Privacy



NoSQL = No Security?: Mitigation Strategy

- General solutions are not expected before 2013
- Carefully choose dev team to include industry veterans
- Heavy use of code reviews
- Reduce direct exposure to end-users through intensive input validation and network



NoSQL = No Security?: Summary

- Model Maturity
 - Not enough security built into existing offering
 - Desired security model is unclear
 - No guarantee that there is a match between existing capabilities and desired model
- Software Maturity
 - Server software is prone to vulnerabilities
 - Expect 5 years of vulnerability turmoil (based on past experience with SQL technologies)
- Staff Maturity
 - Everyone is new to NoSQL
 - Make it work first, if you're still standing try to configure security
 - Staff bound to make configuration mistakes



NoSQL = No Security?: Summary (cont.)

- Client software is rebuilding security
 - Since security does not exist on server side it is rebuilt into every application
 - Adds complexity, lack of security expertise
 - Always left for last
- Data redundancy and dispersion
 - Inherent distribution and replication
 - Model is non-normalized
 - Harder to locate sensitive data
- Privacy concerns
 - Use cases jeopardize our ability to avoid being tracked by service providers

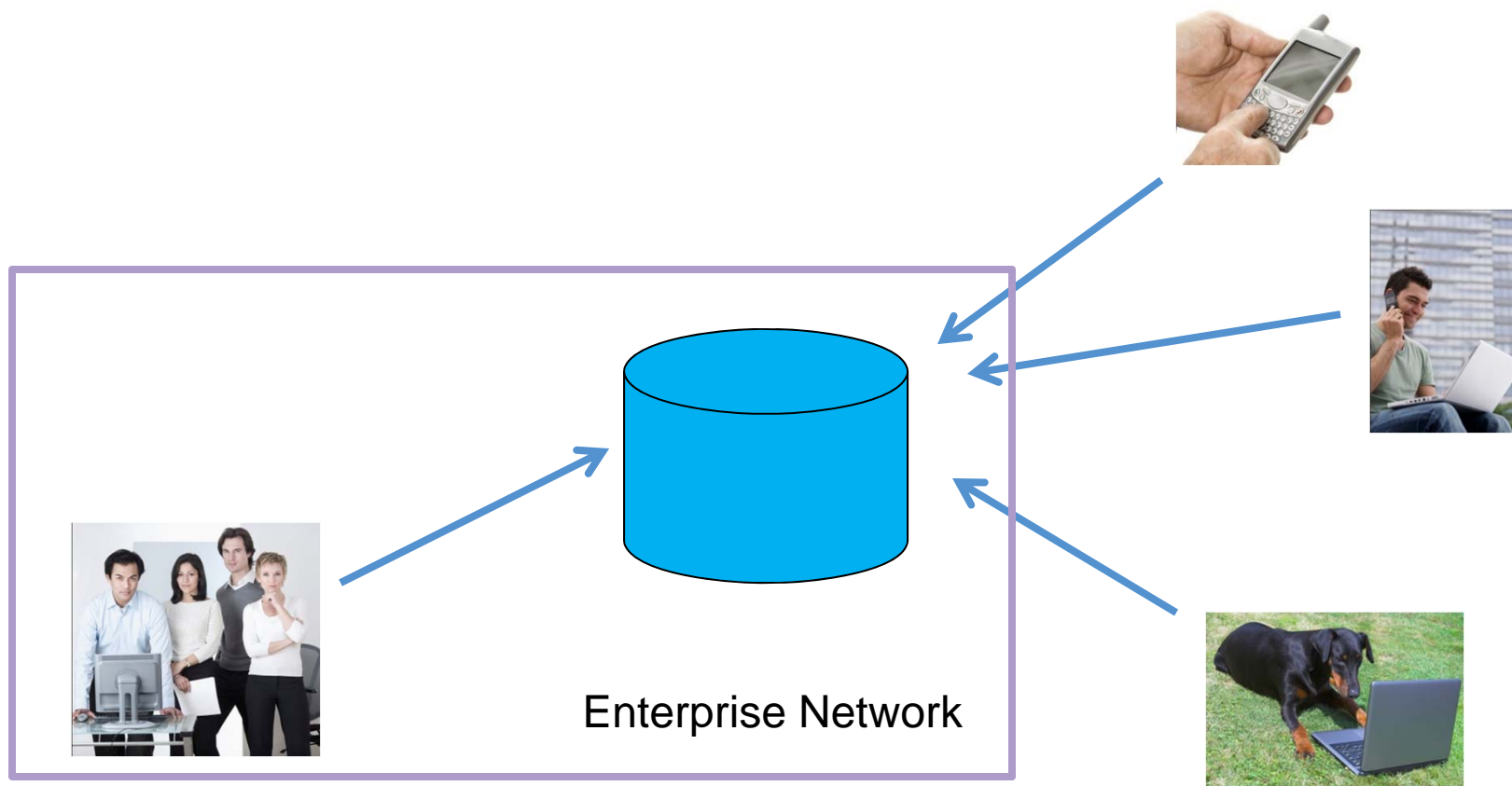




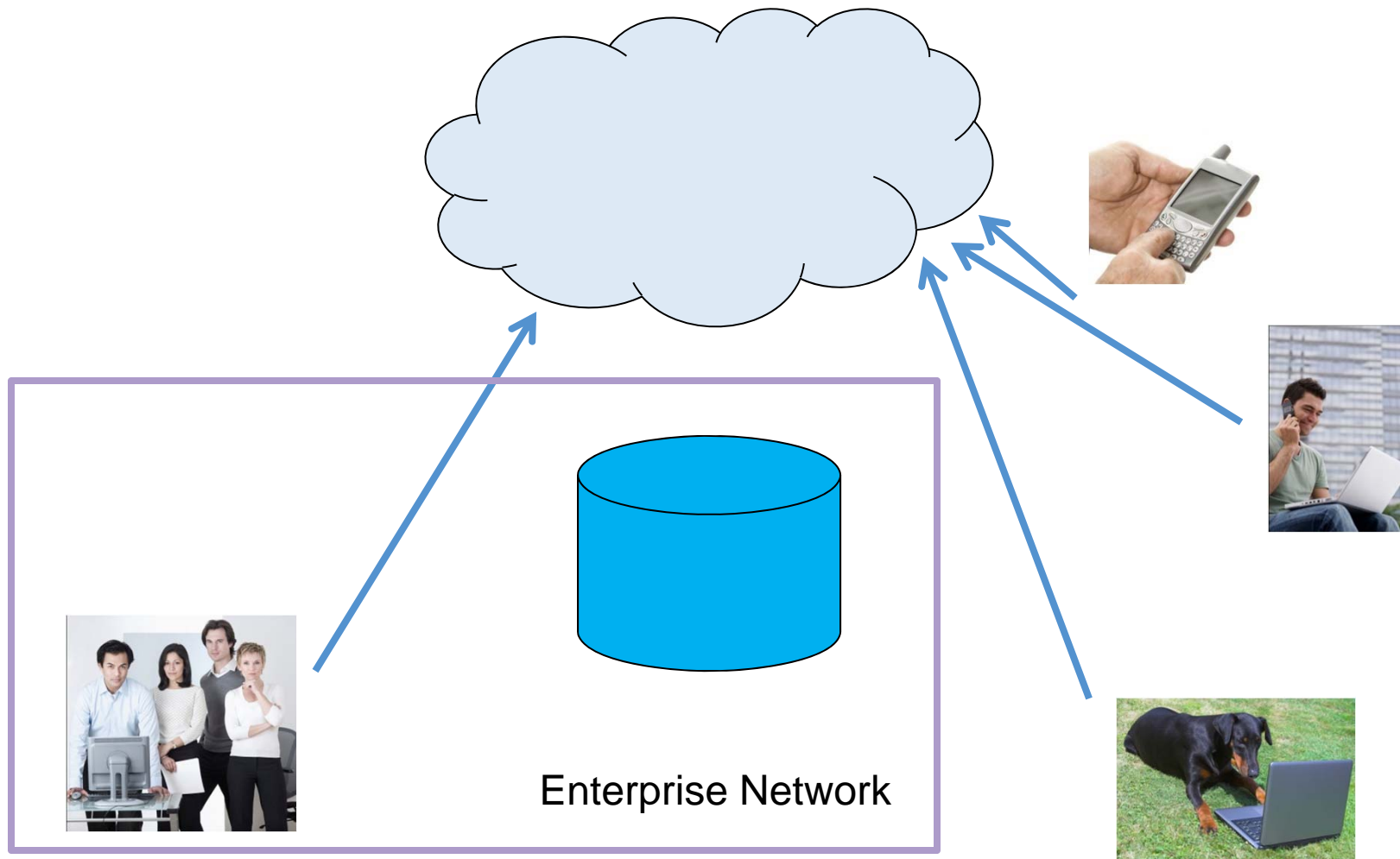
The Kimono Comes Off of Consumerized IT

We expect organizations to spend a lot of time, money and effort on these techniques and technologies next year, with very poor results.

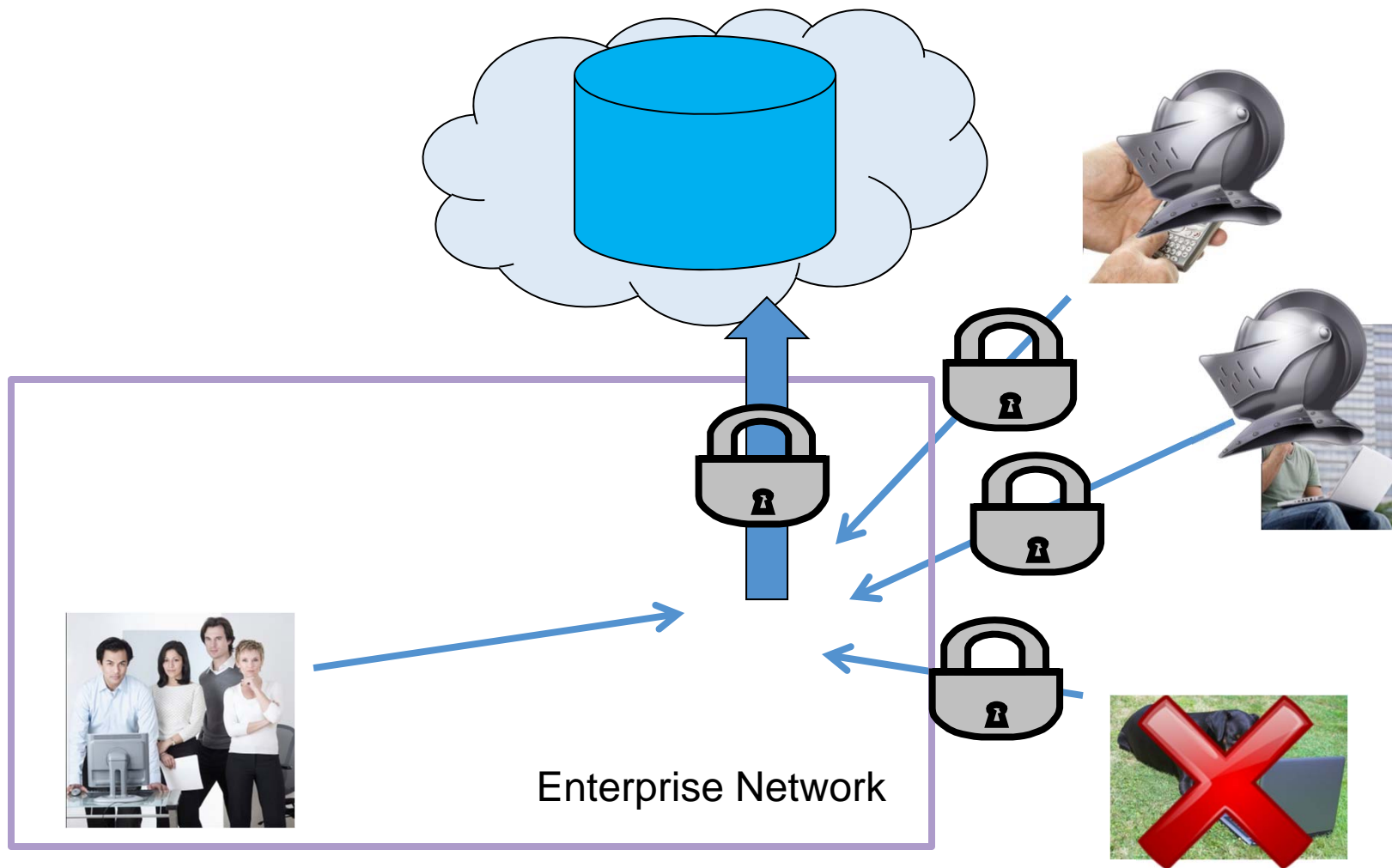
IT Consumerization



IT Consumerization + Cloud



Taking Control Back?



Taking Control Back?



Enterprise Network



The Kimono Comes Off of Consumerized IT: Mitigation Strategies

- Put more control around data store rather than end-point
- Consider structured and unstructured data alike
- Increase efforts towards detecting abuse of privileges



The Kimono Comes Off of Consumerized IT: Summary

- Companies are trying to get control back the wrong way – Restricting their users
- It never worked in the past
 - Allow no Javascript
 - Don't access social network from work
- Enterprise IT cannot scale to manage and control the amount of devices and its diversity
 - Track record of enterprise IT in avoiding infections and leakage from internal, enterprise owned machines is not that great



The Kimono Comes Off of Consumerized IT: Summary (cont.)

- Enterprise infrastructure is required to provide the same level of world-wide availability and robustness of all cloud services together and defeats the purpose of using cloud solutions
- Enterprise will need to address concerns regarding personal information controlled by corporate on end-user devices





Mitigation Strategies for the Other Trends

RSA CONFERENCE 2012

Dealing with the Other Trends: Mitigation Strategies

- HTML5 Goes Live
 - Assume user devices are compromised
 - Learn to interact with infected clients (challenge users, reduce functionality on the fly)
- DDoS Moves Up the Stack
 - Look for application layer protection
 - Visibility into SSL connections
 - Understand application messages
 - Differentiate application data from network Gibberish



Dealing with the Other Trends: Mitigation Strategies

- Anti-Social Media

- Solutions must be incorporated into existing platforms by enterprises themselves.
 - Solutions will have to rely on 3rd parties that offer trust and data control services over the social media platform.
 - No current market solution ready to handle these problems.

- Security (Finally) Trumps Compliance

- Perform wise security decisions based on actual risk management
- Implement security and then assess whether they have done enough in the context of each regulation





Questions??