# Don't Lose Sight of the Extended Enterprise

Rod Rasmussen

President/CTO – Internet Identity

2011 Annual FIRST Conference

Vienna, Austria


ACTIVELY SECURING THE EXTENDED ENTERPRISE

# Presenter: Rod Rasmussen

- Rod.Rasmussen<at>InternetIdentity.com
- President & CTO Internet Identity (IID)
- Co-Chair APWG Internet Policy Committee
- Member of multiple ICANN working groups
- Active member MAAWG, DNS-OARC, Digital Phish-Net, RISG, OTA
- And of course, IID's FIRST representative

# E-crime Then & Now

Then (and still today) - Threats attack victims and organizations directly

- Hacking – attacking infrastructure directly
- Wide-scale Spam/Phishing
- Viruses/Worms/Malware – sent to you or on your network

# E-crime Then & Now

Now – ADD – Indirect attacks that allow circumventing defenses

- Go after softer targets to gain access to data or controls
  - Attack your partners, vendors, customers
  - Target personnel with access to ancillary systems
- Get on the network first – then traverse
- Get the targeted data from your partners' systems
- Subvert the infrastructure – then redirect

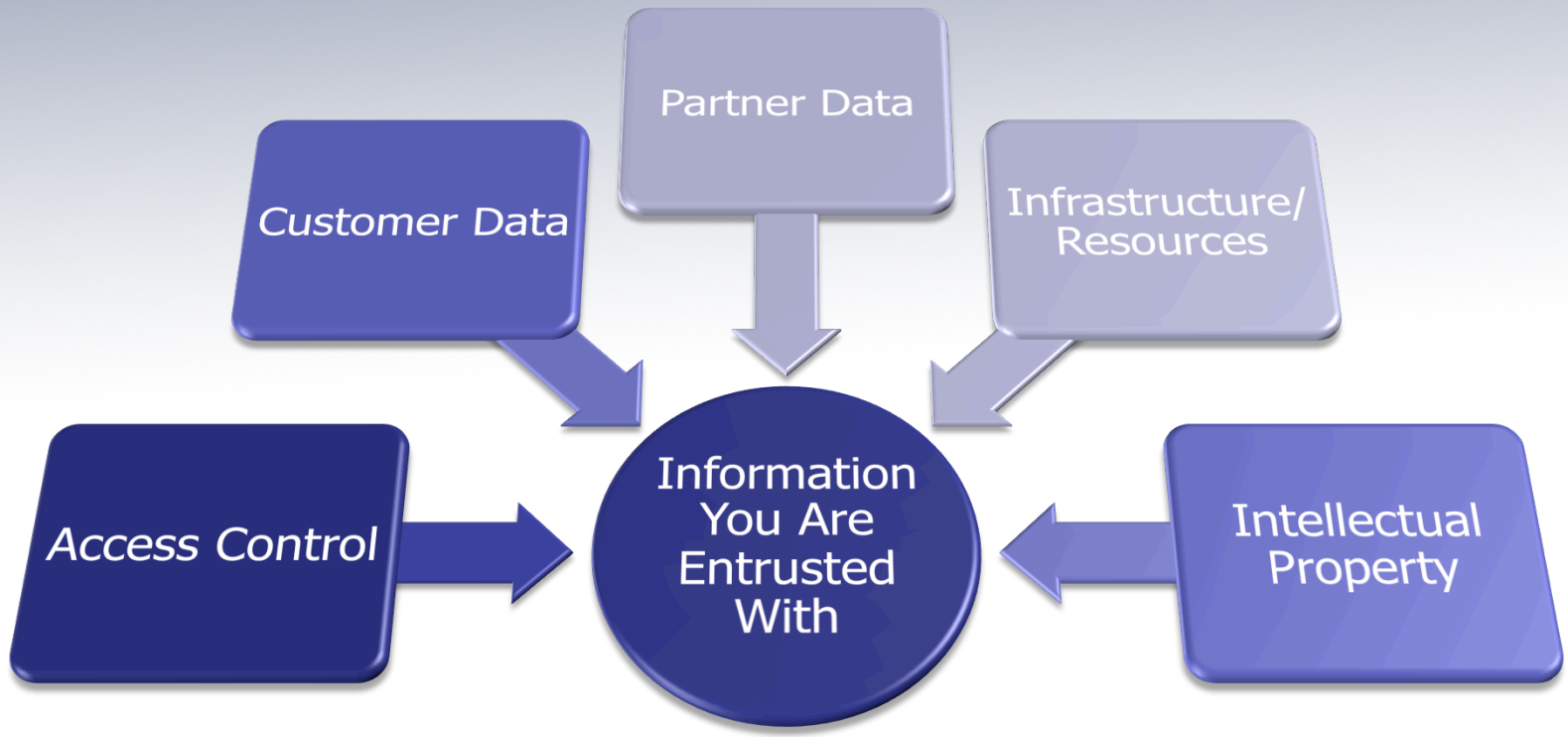
# Get the User, Then the Data

- Techniques du jour
  - Spear phishing
  - Malvertising and exploited websites
  - Social networks and webs of trust

# Today's Biggest Enemies

- Unencrypted data in partners' hands
- Password re-use
- Access to automated systems – subvert yours
- Control of your infrastructure

# Everything is Being Targeted

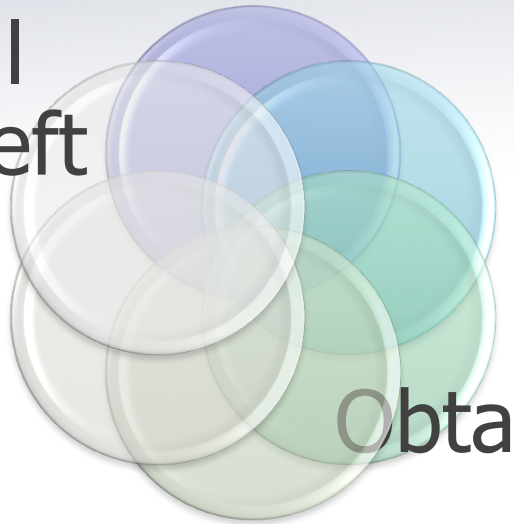


# Motives are Evolving

Direct Theft

$$$$

Intellectual Property Theft



**Chaos**

National Interests

Obtain Infrastructure

Data Resale

# The Extended Enterprise Paradigm

- The "Extended Enterprise" includes relationships with partners, vendors, suppliers and key customers that enable enterprises to succeed
  - To whom do you routinely send PII and other sensitive data about personnel, financials, or customers?
  - Who do you transact with regularly and automatically?
- The Internet has changed commerce, communications, and life forever with instant connections and mash-ups

# The Extended Enterprise

HR/Legal/ Accounting

Suppliers

SaaS/Cloud

Marketing Partners

Financial Partners

Customers

Mobile Workforce

ACTIVELY SECURING THE EXTENDED ENTERPRISE

# EE Infrastructure

- The infrastructure you communicate with all of these partners is outside your control
- With “Cloud Computing” even your physical enterprise assets are extended outside your perimeter of control
- Social networks are now communications channels
- Will regulation push enterprises to patrol their EE?

# Some EE Events: 2011

**Notable Affected Targets**

- Lockheed-Martin
- Sony
- Unveillence
- PBS
- Voice of America
- European (and Australian) Parliaments, EU Commission, Canadian Government
- NASDAQ

**EE Partners**

- InfraGard Atlanta
- RSA
- Epsilon and other ESPs
- Wordpress
- MySQL
- TripAdvisor.com
- HBGary

# The EE Quandary

- The Internet-connected world demands you provide direct web-enabled services to customers and instant data exchanges with partners and vendors
- You have little or no control over the security posture of these external entities
- You have no direct ability to change physical security throughout your EE
- You have limited visibility into events occurring on your EE
- You are STILL responsible for your data – wherever it is

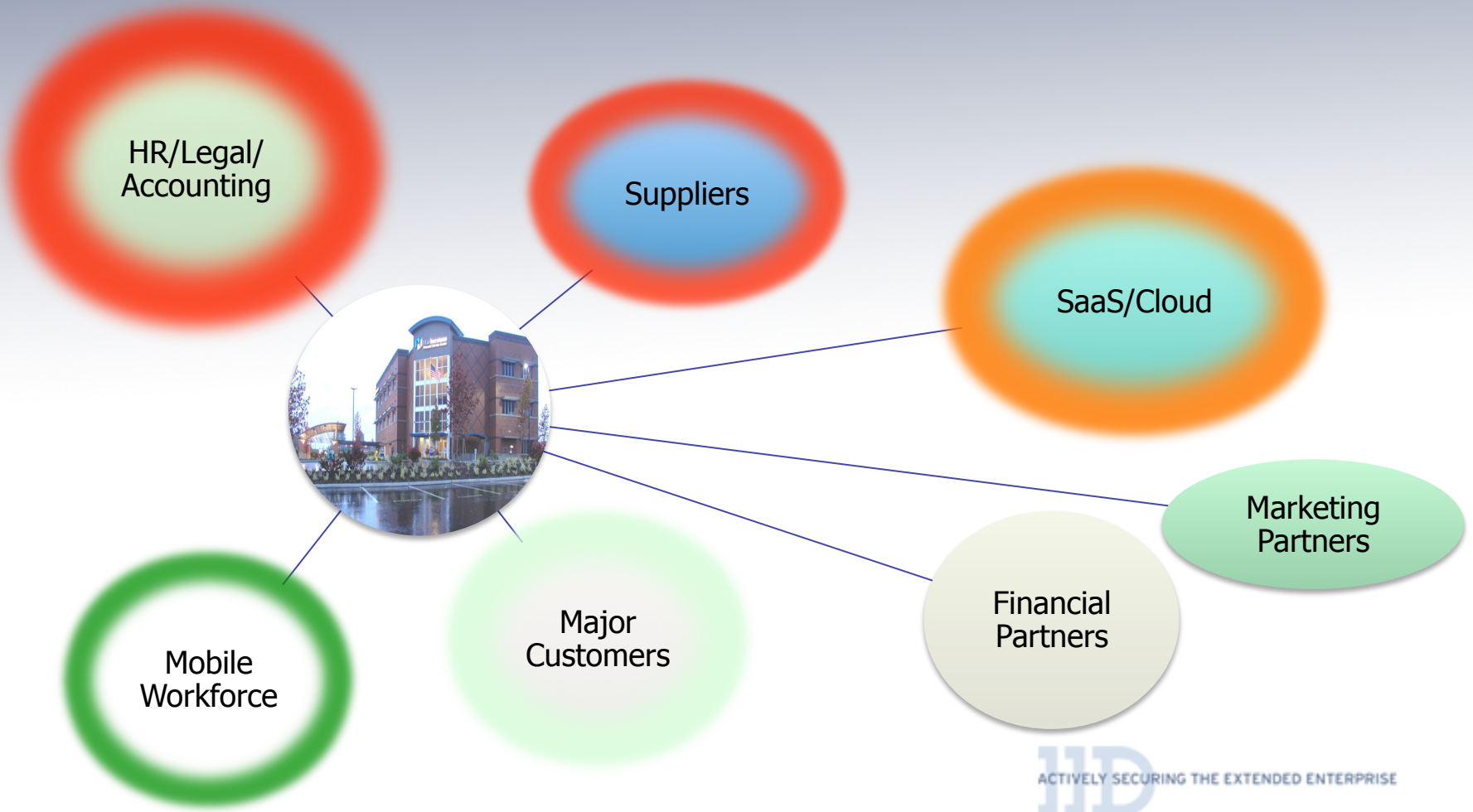
# Some Numbers

- Ponemon/PGP 2010 corporate data breach study:
  - Average was $3.4 million = $142 per customer.
  - 35% involved outsourced data provided to third parties
- There are over X (1, 3, 5, 10, 50, ??) million Conficker infected machines right now
- Zeus lives everywhere, steals everything
- Sony lost $X billion in market cap in wake of breaches – estimates breaches will cost at least $170 million profit hit

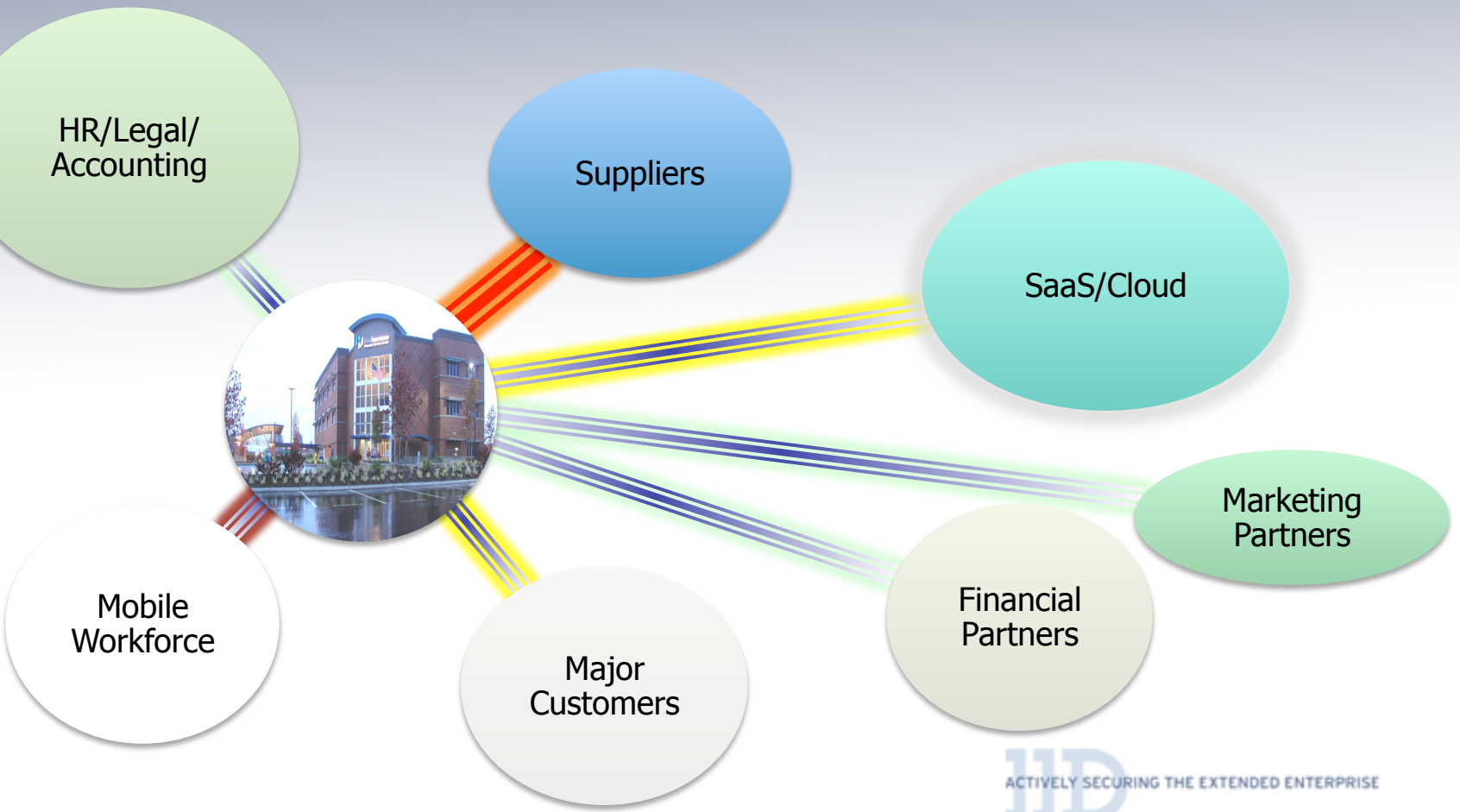
# What Data IS Sensitive?

- Obvious stuff
  - Customer PII, account info, financial history
  - Access credentials
  - Compliance related information
- Your own company plans, financials, legal papers, contracts, personnel information
- Your partners' confidential information

# Data Storage Risks



# Communication and Infrastructure Risks



# EE Members

The Law Offices of Dewey, Cheatem, & Howe

Bank of America

Cook, Books & Hyde Accountants

citibank

Sprint

Network Solutions

Google

Microsoft

CHASE

UNITED STATES FEDERAL RESERVE SYSTEM

twitter

facebook

ACTIVELY SECURING THE EXTENDED ENTERPRISE

# Mapping your EE

- Internal intel
  - Legal contracts
  - Mail server/ firewall/DNS logs
  - Mail/contact databases
  - CRM platform
- External info
  - IP & domain whois data
  - Netflow
  - Open source info

# From Data to a Plan

- Evaluate types and content of data exchanged and business/compliance risks
- Assess data transactions and potential holes back into your systems
- Plan to secure the most important and have contingencies for the rest

# Data Storage in the E.E.

# So Have you Heard of Zeus?

- You may be clean, but what about your EE?
- Hey, it's open source now!
- Not just Zeus – lots of data exfiltration, keyloggers, and "sniffing" malware
- Need to know where it's safe to send/share data
  - Can't block your key partners like you can spam sources or infection points

# Overhyped Security Term

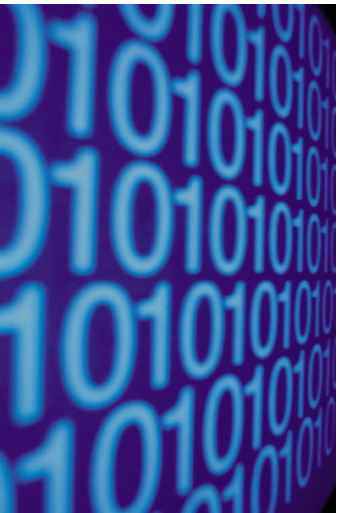
- Attackers are putting “stealthy” malware on networks and trying to surreptitiously exfiltrate date over time
- Not really new, but WOW is this happening a lot now!
- Devastating data losses from well-known, very secure organizations
  - Includes many of your EE partners and providers
  - People who provide your security and DB products
- Likely regulatory ramifications due to high publicity

# EE Member Reputation

- In the real world you get DUNS reports, credit reports or other objective business reputation “scores” to assess risk – why not online?
- Use that EE map to review reputation of your EE
  - IP reputation of netblocks
  - Domain/DNS reputation of data-transfer domains plus main domains
- Open source tools and commercial services
  - Hard to get data on EE though – Arbor, Cymru, etc. don’t “tattle”
- Shut-off processes/data flow when red-flags show up – get them to fix breach asap

# The “Cloud”

- Storage of your data, at some undisclosed location in the world, on an unknown hardware platform, with a third party in control of security…



# Cloud Services

- So beyond the obvious, what do you have to worry about?
  - Your neighbors on the service
  - What are data retention and divulgence policies?
  - What jurisdictions have access?
- Risk management is the key
  - Understand the lay of the land
  - What can you actually place there reasonably?

# Cloud Providers & Security

- Ponemon/CA Study in April 2011 – 127 service providers
  - The majority of cloud providers believe it is their customer's responsibility to secure the cloud and not their responsibility.
  - On average, providers of cloud computing technologies allocate 10 percent or less of their operational resources to security and most do not have confidence that customers' security requirements are being met.
  - The majority of cloud providers in the study admit they do not have dedicated security personnel to oversee the security of cloud applications, infrastructure or platforms.

# Webmail and E-mail Outsourcing


- Google/G-Mail attacks continue
- Phishing targeting webmail providers
- Exposure to XSS and other vulnerabilities
- Bottom line: Are the apparent low-cost and features worth the data exposure risk?

# Outsourced CRM

- Sensitive data on your personnel, customers, and partners
- Big phishing and data extraction target
- Epsilon and other ESP's targets of determined gang
- Bad guys going after your contacts
  - Phishing/malware/spam
  - Use Your name for multi-level attack
- Insist on strong authentication and data encryption

# Content Delivery Systems

- Includes your website, online banking, outsourced web services that are customer facing
- In-house, outsourced, or platform?
- If outside your control – this is your top EE partner!
  - Learn everything about what they do and how
  - Monitor everything you can
  - Not just SLA – but Security SLA!

# Social Networks

- Have become a major communications channel
  - Customer interactions
  - Contact data storage
- NOT designed for security
- Attacks include spoofing, impersonation, account take-over
- Good venue for phishing and malware too

# Dealing with Social Networks

- Set policies for usage
- Monitor for sensitive data leakage
- Block dangerous content
- Work with social network site security teams

# DNS, BGP, and Other Protocols Not a Very Secure Foundation…

All the "security" in the world doesn't matter if your underlying infrastructure foundation is full of holes or can easily be taken out altogether.

Everything based on the Internet has these fundamental problems.

# DNS Infrastructure Vulnerabilities

- Protected at almost all levels with just a user/pass
- Authoritative nameservers can be p0wned
- Successful penetrations at registrars and registries
- Highly vulnerable (Kaminsky bug) at many ISPs
- Malware and p0wned WiFi routers control many endpoints
- DNSSEC only a partial solution (cache poisoning)

# DNS Take-Over Victims

- Registrar Account
  - Microsoft and Coca-Cola in Israel
  - Baidu.com
  - Tata
  - Voice of America
- DNS management account
  - Twitter
- Registry Hacks
  - All of Bangladesh (.bd)

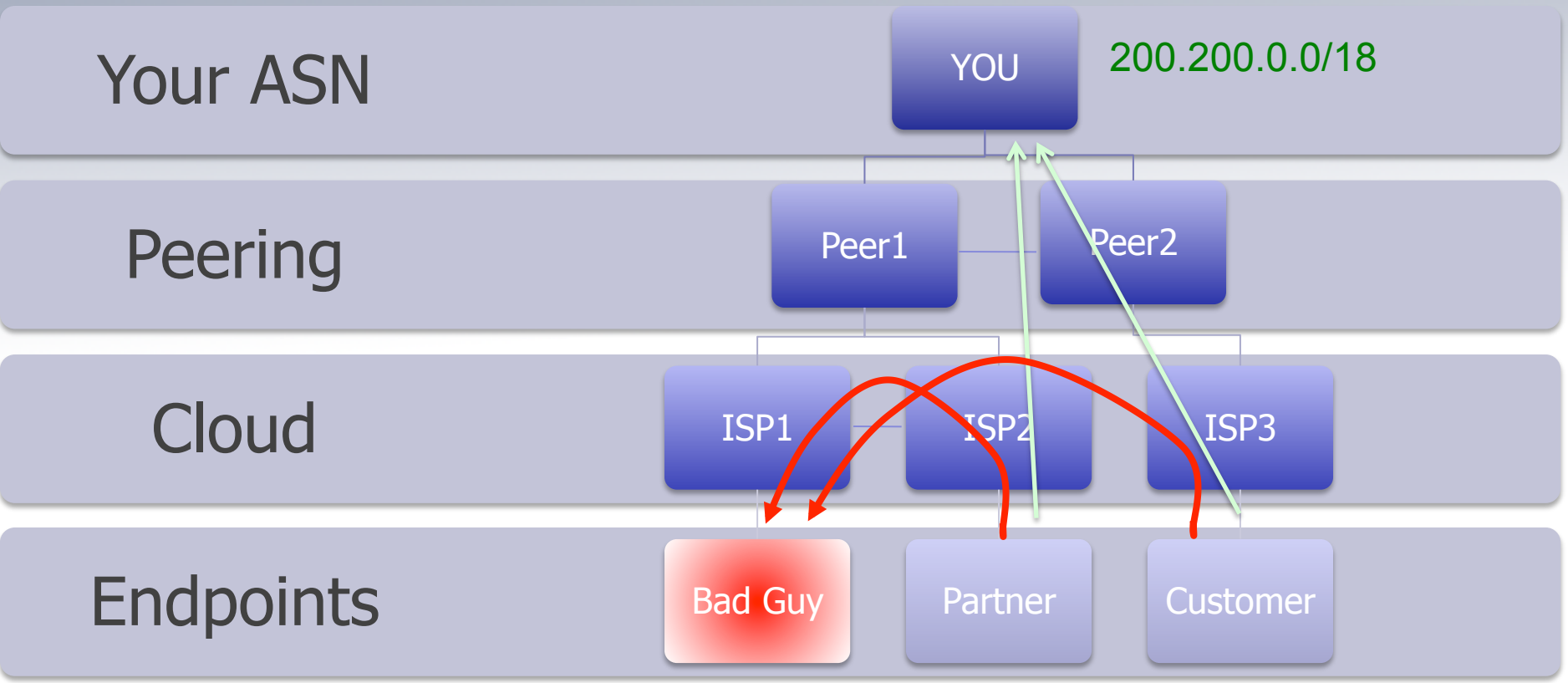
# Hardening DNS

- Implement DNSSEC!
- Lock down your domain registrations
  - ICANN SSAC – SAC 40 & SAC 44
  - Registrar & DNS provider that offer real security
  - Verisign “registry lock” for com/net
- Monitor your DNS and your partners’ DNS too!
- Know when bad guys target your DNS in malware etc.

# BGP and Routing

- The Internet works because a bunch of carriers, ISPs, and webhosts, who often don't actually know each other, decide to route each others' traffic, their customers' traffic and all of their neighbors through them, and so on, and so on…
- ISPs trust their neighbors to get it right
- Trivially easy to advertize space you don't own
- BGP automates the propagation of route info
  - No authentication, encryption, or secure channel
  - Most specific or "least hop" route usually wins

# Example BGP Hijacking




200.200.0.0/18

200.200.0.0/19

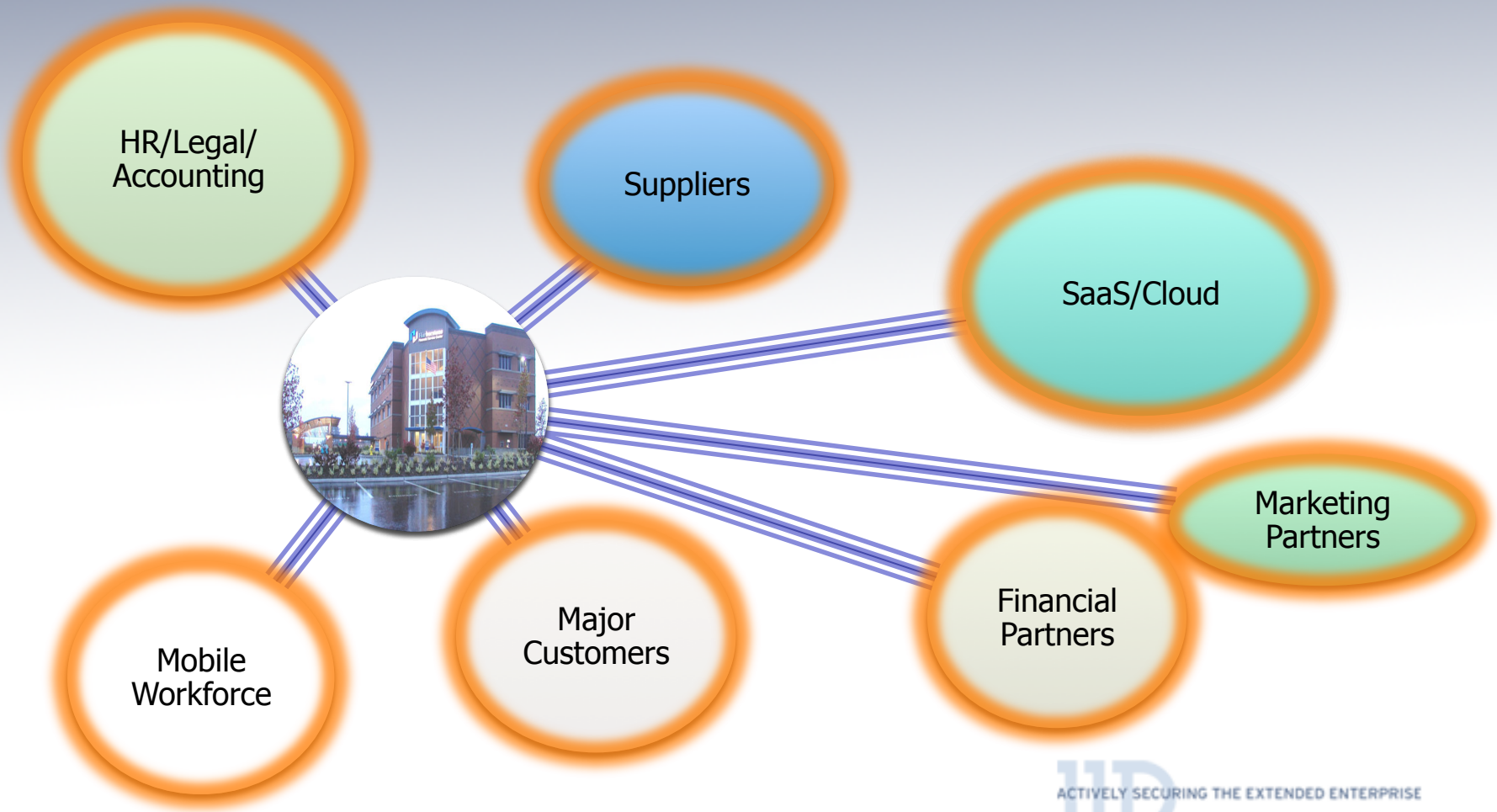
# BGP and Routing Continued

- With BGP spoofing/malvertizing you can take over the IP space of almost any target – at least briefly, but often for quite a while for some portion of the Internet
- It already happens
  - Northrup Grumman (for spamming)
  - Pakistan vs. YouTube, ChinaNet vs. the World
  - Spammers grabbing dormant blocks and announcing other peoples' IP spaces

# Dealing with BGP

- Make sure your ISP knows you well and protects you
- Announce all your routes as narrowly as practical
- Ensure access control and whois are current
- Monitor your and your EE's key BGP routes

# Wrap-up
# The Extended Enterprise = Risk



# Steps to Take

- Determine your key EE members
- Evaluate data flows to them and data stored there
- Risk assessment on vulnerabilities
- Policies and contract clauses for better security
- EE partners must encrypt stored sensitive data – *strongly*
- Monitor and verify where possible
- Problems will happen – plan for them and set yourself up for quick resolution

# Thank You!

**Questions/Discussion**

# Don't Lose Sight of the Extended Enterprise

Rod Rasmussen

President/CTO – Internet Identity

2011 Annual FIRST Conference

Vienna, Austria


ACTIVELY SECURING THE EXTENDED ENTERPRISE