Cloud Computing: Finding the Silver Lining

Steve Hanna, Juniper Networks

Agenda

- What is Cloud Computing?
- Security Analysis of Cloud Computing
- Conclusions

Agenda

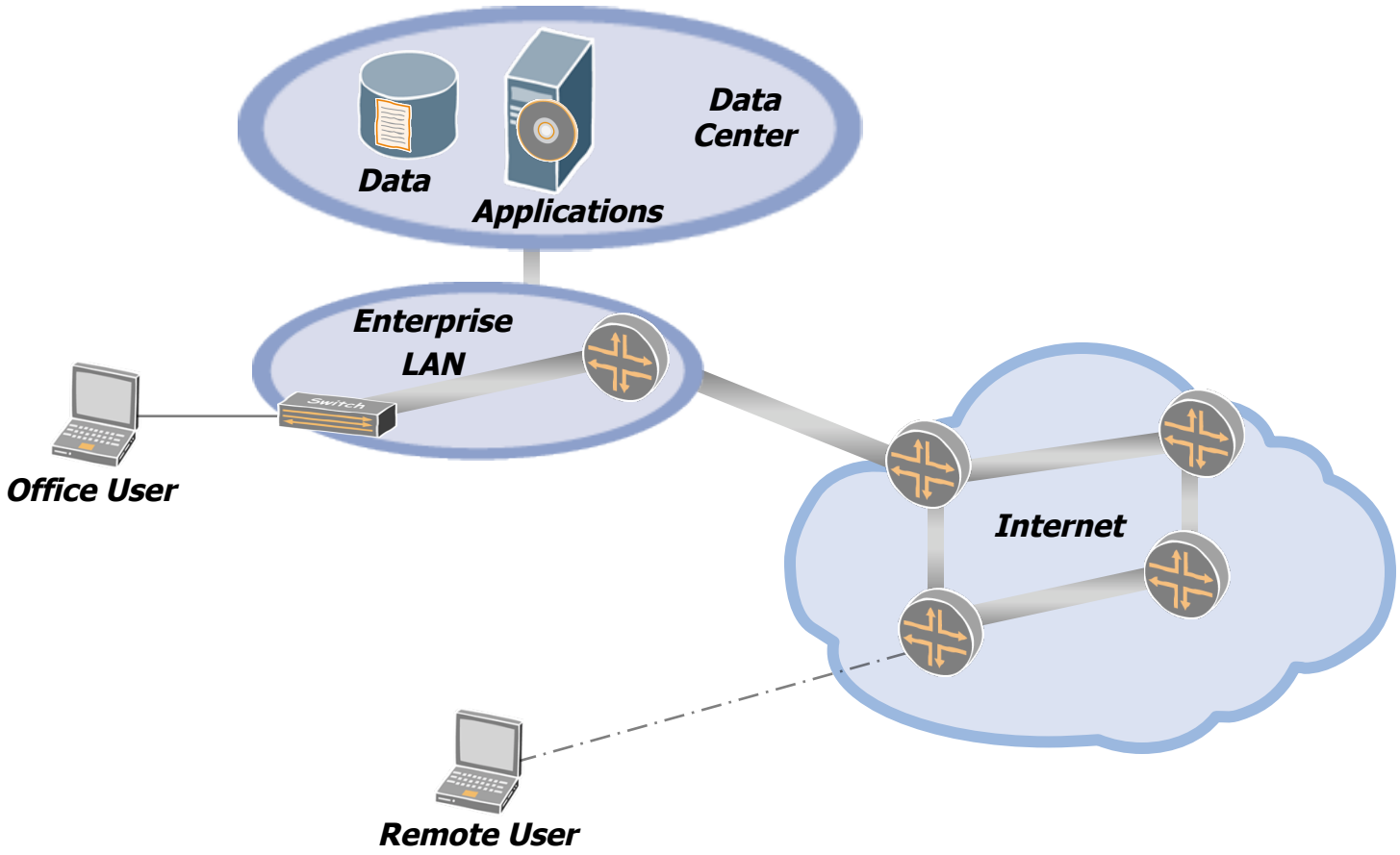
- **What is Cloud Computing?**
- Security Analysis of Cloud Computing
- Conclusions

Cloud Computing Defined

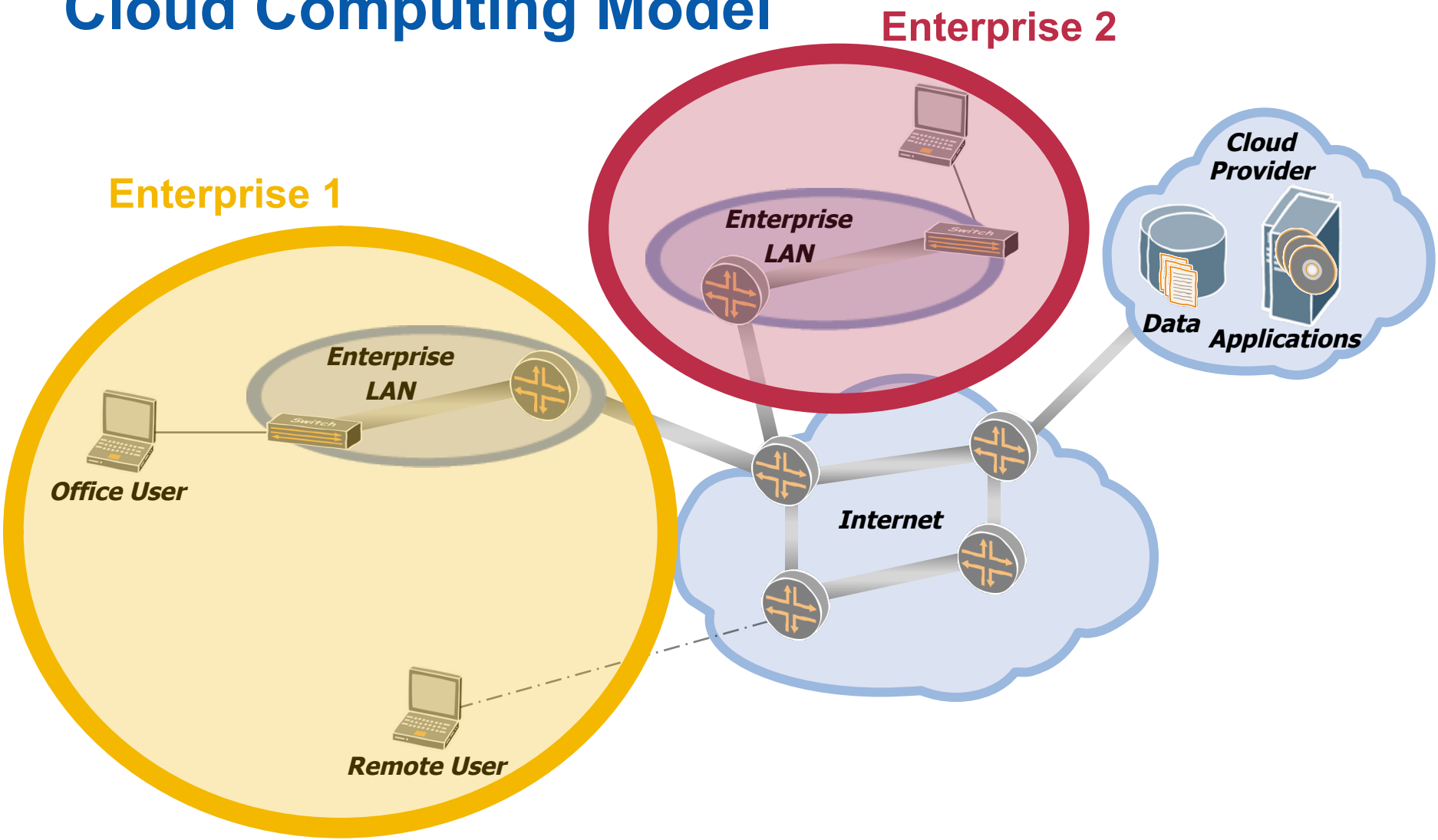
- **Dynamically scalable shared resources accessed over a network**
  - Only pay for what you use
  - Shared internally or with other customers
  - Resources = storage, computing, services, etc.
  - Internal network or Internet

- **Notes**
  - Similar to Timesharing
    - Rent IT resources vs. buy
  - New term – definition still being developed

Conventional Data Center



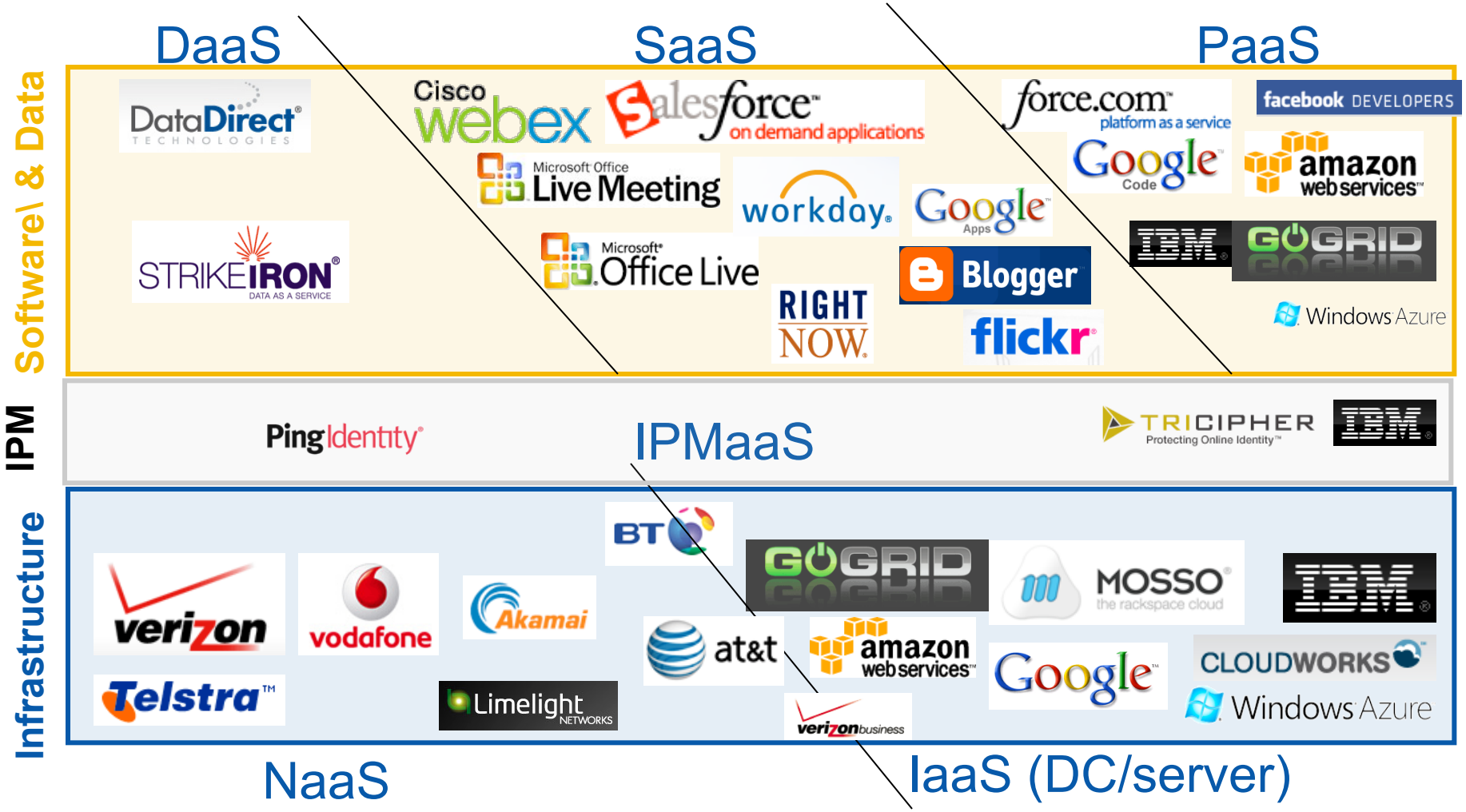
Cloud Computing Model



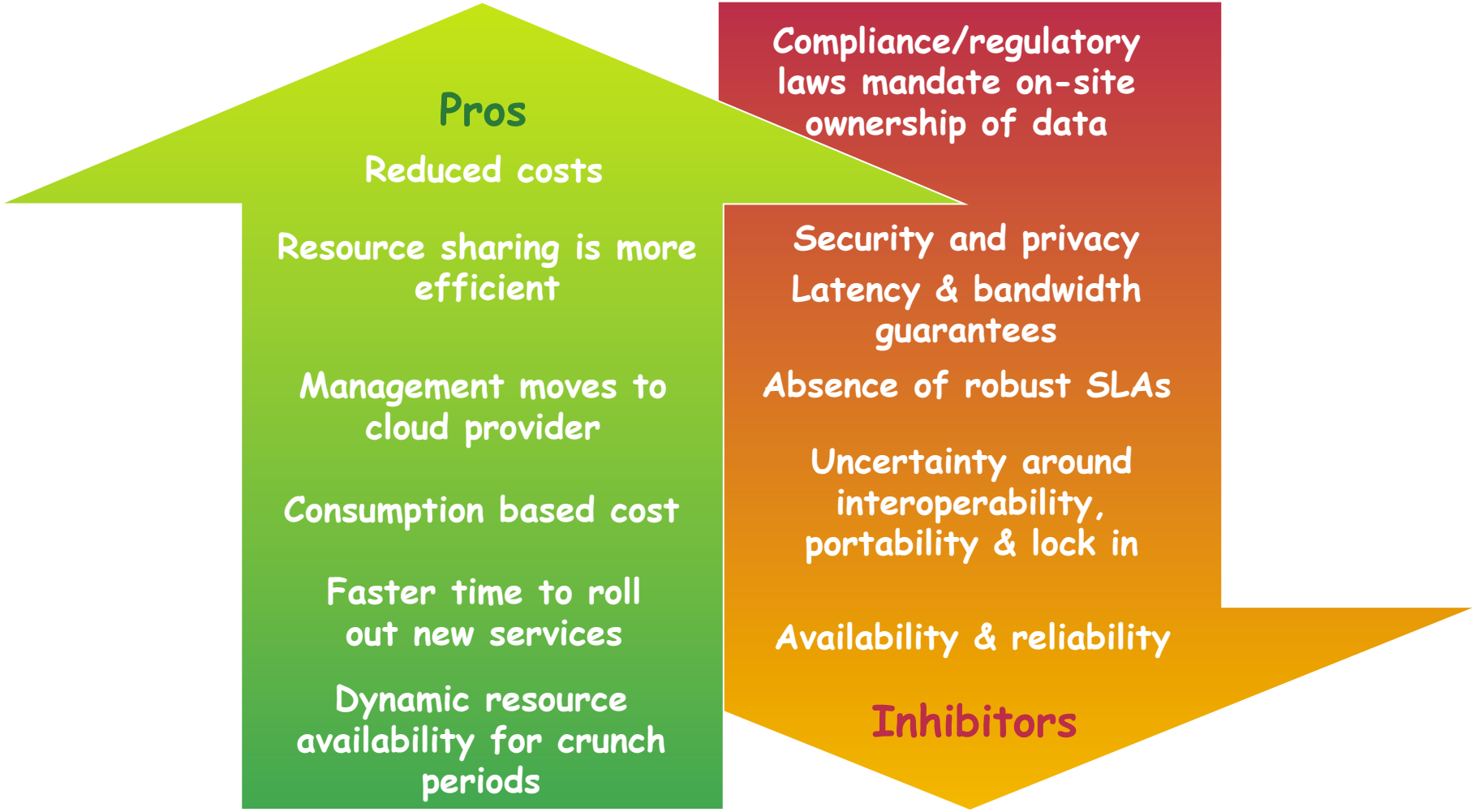
Many Flavors of Cloud Computing

- **SaaS – Software as a Service**
  - Network-hosted application
- **DaaS – Data as a Service**
  - Customer queries against provider's database
- **PaaS– Platform as a Service**
  - Network-hosted software development platform
- **IaaS – Infrastructure as a Service**
  - Provider hosts customer VMs or provides network storage
- **IPMaaS – Identity and Policy Management as a Service**
  - Provider manages identity and/or access control policy for customer
- **NaaS – Network as a Service**
  - Provider offers virtualized networks (e.g. VPNs)

Cloud Computing Providers



Cloud Computing Pros and Cons



Who’s using Clouds today?

Example: Mogulus

- **Mogulus is a live broadcast platform on the internet.** *(cloud customer)*
  - Producers can use the Mogulus browser-based Studio application to create LIVE, scheduled and on-demand internet television to broadcast anywhere on the web through a single player widget.
- **Mogulus is entirely hosted on cloud** *(cloud provider)*
- **On Election night Mogulus ramped to:**
  - 87000 videos @500kbps = 43.5 Gbps
  - http://www.mogulus.com

Example: Animoto

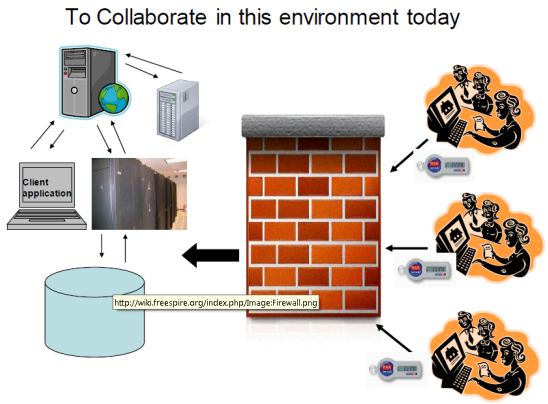
- **Animoto is a video rendering & production house with service available over the Internet**
  (cloud customer)
  - With their patent-pending technology and high-end motion design, each video is a fully customized orchestration of user-selected images and music in several formats, including DVD.
- **Animoto is entirely hosted on cloud**
  (cloud provider)
- **Released Facebook App: users were able to easily render their photos into MTV like videos**
  - Ramped from 25,000 users to 250,000 users in three days
  - Signing up 20,000 new users per hour at peak
  - Went from 50 to 3500 servers in 5 days
  - Two weeks later scaled back to 100 servers
  - http://www.animoto.com

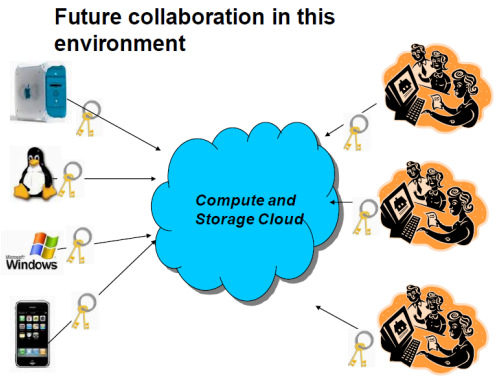
Example: New York Times

- **Timesmachine is a news archive of the NY Times available in pdf over the Internet to newspaper subscribers** *(cloud customer)*
- **Timesmachine is entirely hosted on cloud** *(cloud provider)*
- **Timesmachine needed infrastructure to host several terabits of data**
  - **Internal IT rejected due to cost**
  - **Business owners got the data up on cloud for $50 over one weekend**
  - http://timesmachine.nytimes.com

Example: Eli Lilly

- **Eli Lilly is the 10th largest pharmaceutical company in the world** *(cloud customer)*
- **Moved entire R&D environment to cloud** *(cloud provider)*
- **Results:**
  - Reduced costs
  - Global access to R&D applications
  - Rapid transition due to VM hosting
  - Time to deliver new services greatly reduced:
    - New server: 7.5 weeks down to 3 minutes
    - New collaboration: 8 weeks down to 5 minutes
    - 64 node linux cluster: 12 weeks down to 5 minutes





Who's using Clouds today?

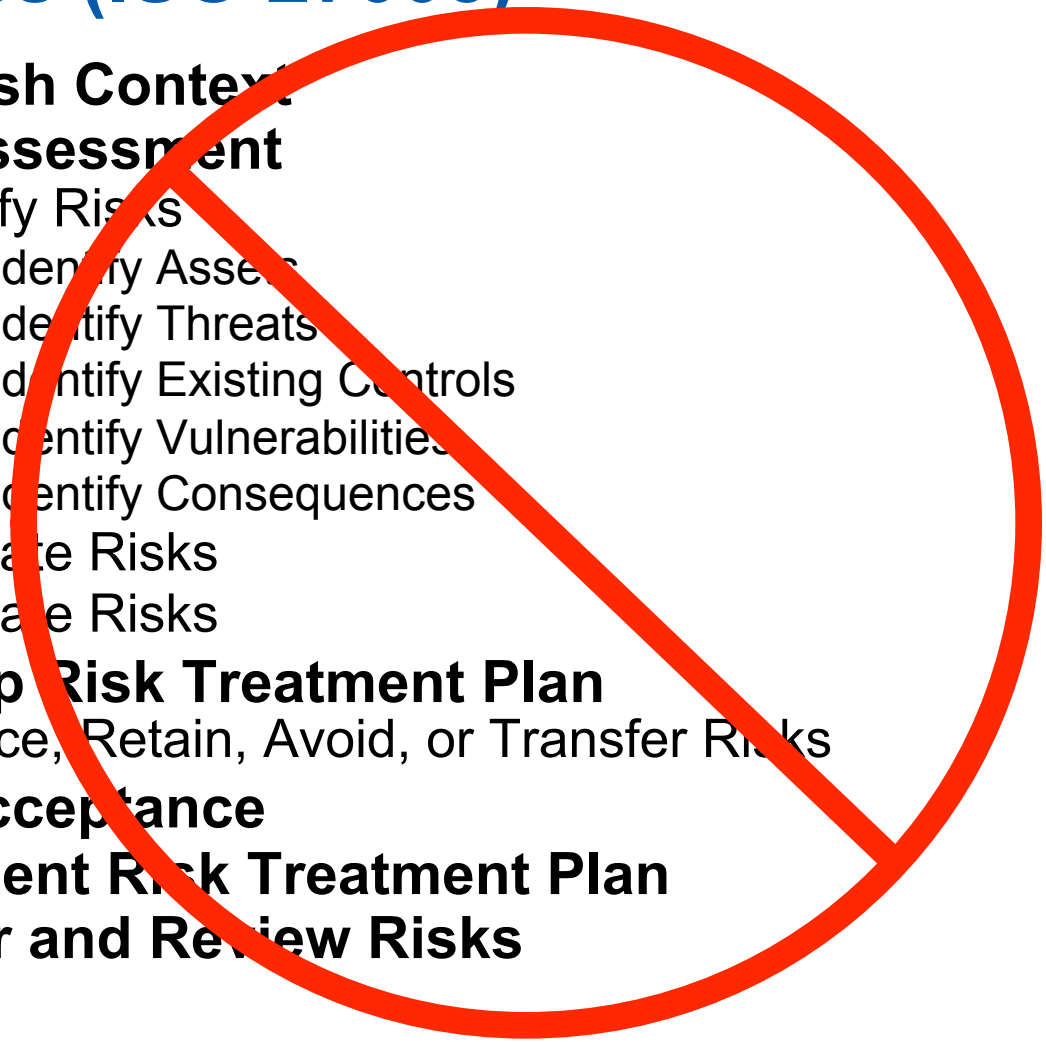
- **Startups & Small businesses**
  - Can use clouds for everything
    - SaaS, IaaS, collaboration services, online presence
- **Mid-Size Enterprises**
  - Can use clouds for many things
    - Compute cycles for R&D projects, online collaboration, partner integration, social networking, new business tools
- **Large Enterprises**
  - More likely to have hybrid models where they keep some things in house
    - On premises data for legal and risk management reasons

Agenda

- What is Cloud Computing?
- **Security Analysis of Cloud Computing**
- Conclusions

Information Security Risk Management Process (ISO 27005)

- **Establish Context**
- **Risk Assessment**
  - Identify Risks
    - Identify Assets
    - Identify Threats
    - Identify Existing Controls
    - Identify Vulnerabilities
    - Identify Consequences
  - Estimate Risks
  - Evaluate Risks
- **Develop Risk Treatment Plan**
  - Reduce, Retain, Avoid, or Transfer Risks
- **Risk Acceptance**
- **Implement Risk Treatment Plan**
- **Monitor and Review Risks**

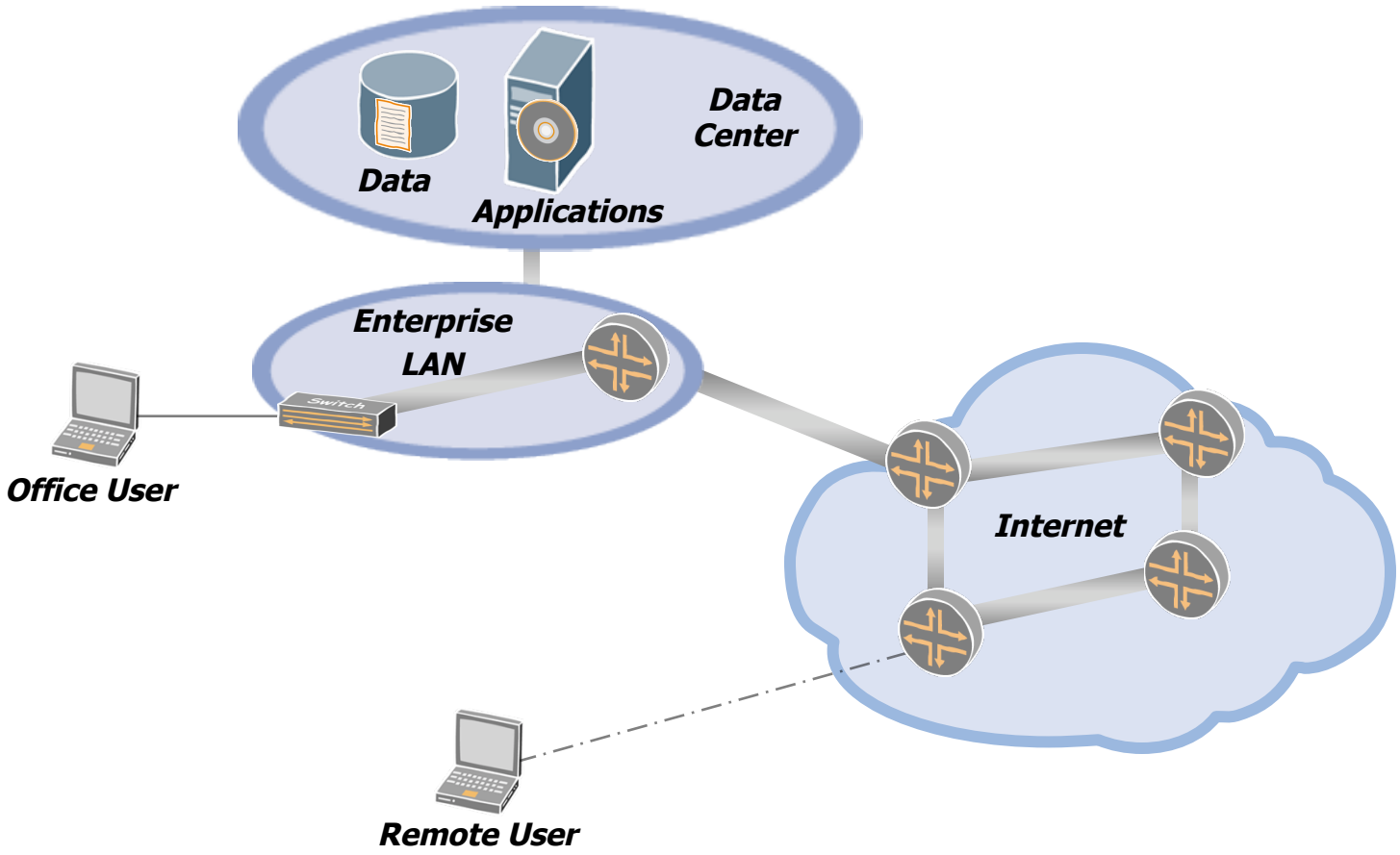


Streamlined Security Analysis Process

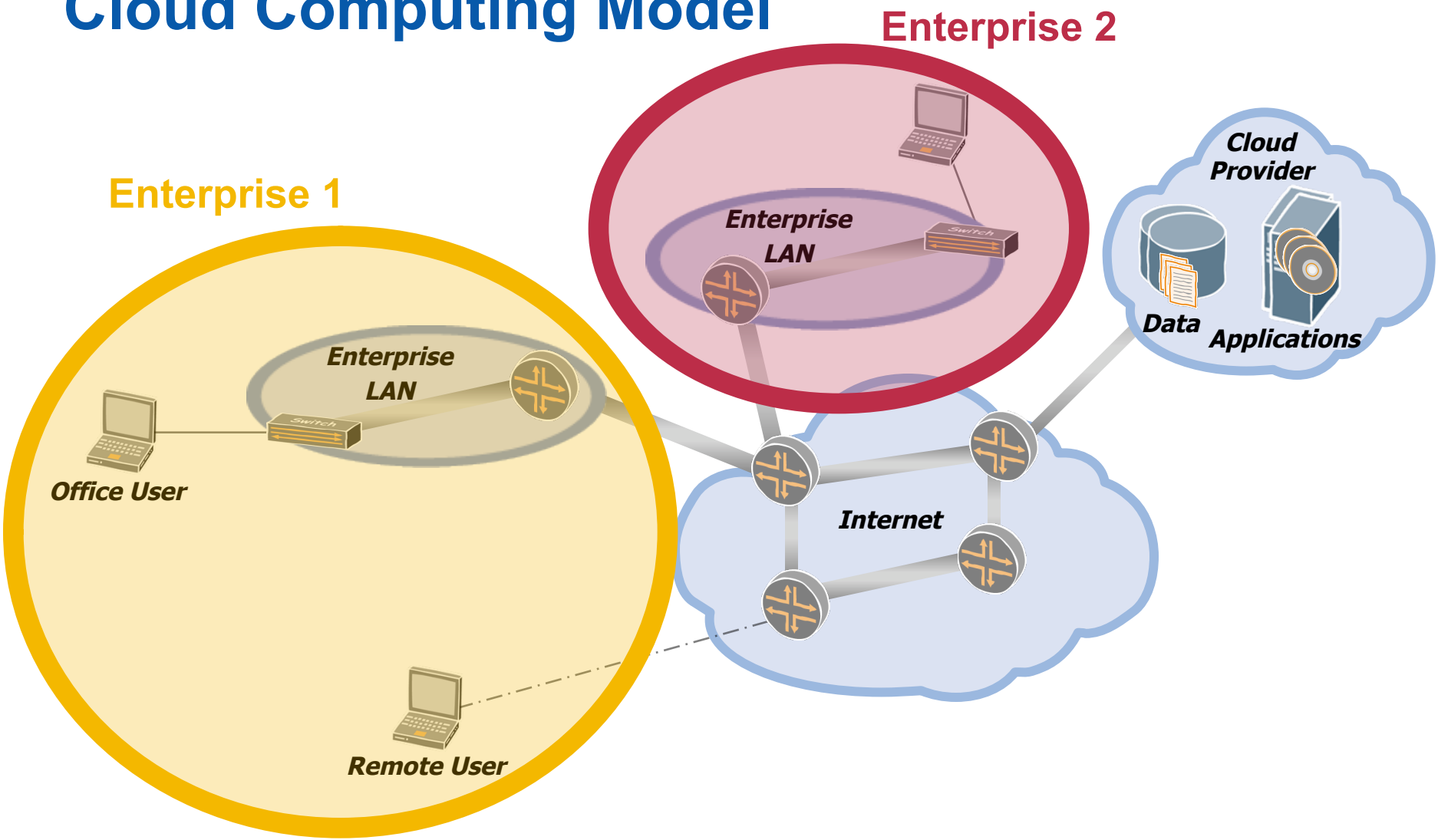
- **Identify Assets**
  - Which assets are we trying to protect?
  - What properties of these assets must be maintained?
- **Identify Threats**
  - What attacks can be mounted?
  - What other threats are there (natural disasters, etc.)?
- **Identify Countermeasures**
  - How can we counter those attacks?
- **Appropriate for Organization-Independent Analysis**
  - We have no organizational context or policies

Identify Assets

Conventional Data Center



Cloud Computing Model



Identify Assets

- Customer Data
- Customer Applications
- Client Computing Devices

Information Security Principles (Triad)

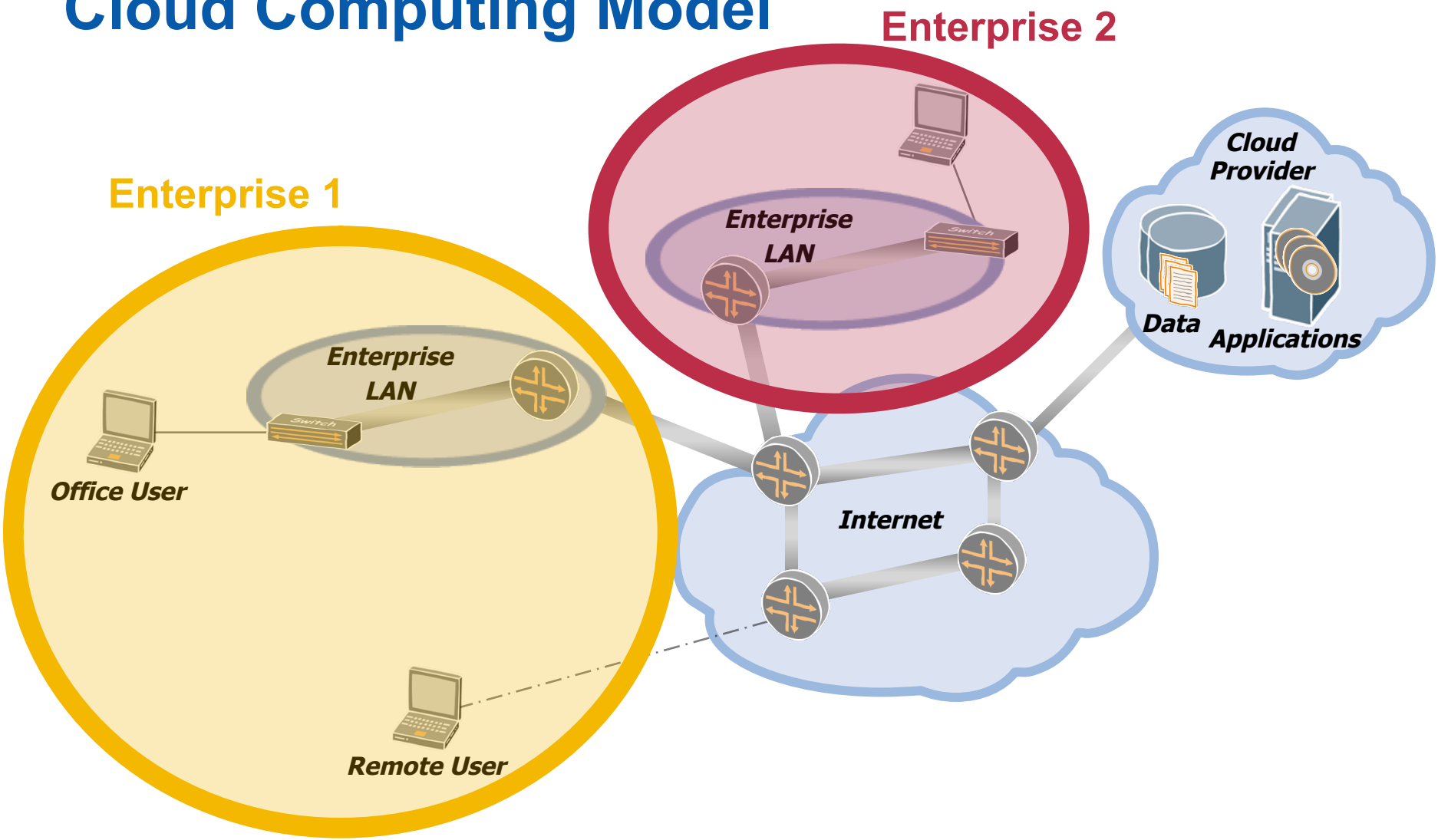
- **C I A**
  - Confidentiality
    - Prevent unauthorized disclosure
  - Integrity
    - Preserve information integrity
  - Availability
    - Ensure information is available when needed

Identify Assets & Principles

- **Customer Data**
  - Confidentiality, integrity, and availability
- **Customer Applications**
  - Confidentiality, integrity, and availability
- **Client Computing Devices**
  - Confidentiality, integrity, and availability

Identify Threats

Cloud Computing Model



Identify Threats

- Failures in Provider Security
- Attacks by Other Customers
- Availability and Reliability Issues
- Legal and Regulatory Issues
- Perimeter Security Model Broken
- Integrating Provider and Customer Security Systems

Failures in Provider Security

- **Explanation**
  - Provider controls servers, network, etc.
  - Customer must trust provider's security
  - Failures may violate CIA principles
- **Countermeasures**
  - Verify and monitor provider's security
- **Notes**
  - Outside verification may suffice
  - For SMB, provider security may exceed customer security

Attacks by Other Customers

- **Threats**
  - Provider resources shared with untrusted parties
    - CPU, storage, network
  - Customer data and applications must be separated
  - Failures will violate CIA principles

- **Countermeasures**
  - Hypervisors for compute separation
  - MPLS, VPNs, VLANs, firewalls for network separation
  - Cryptography (strong)
  - Application-layer separation (less strong)

Availability and Reliability Issues

- **Threats**
  - Clouds may be less available than in-house IT
    - Complexity increases chance of failure
    - Clouds are prominent attack targets
    - Internet reliability is spotty
    - Shared resources may provide attack vectors
    - BUT cloud providers focus on availability

- **Countermeasures**
  - Evaluate provider measures to ensure availability
  - Monitor availability carefully
  - Plan for downtime
  - Use public clouds for less essential applications

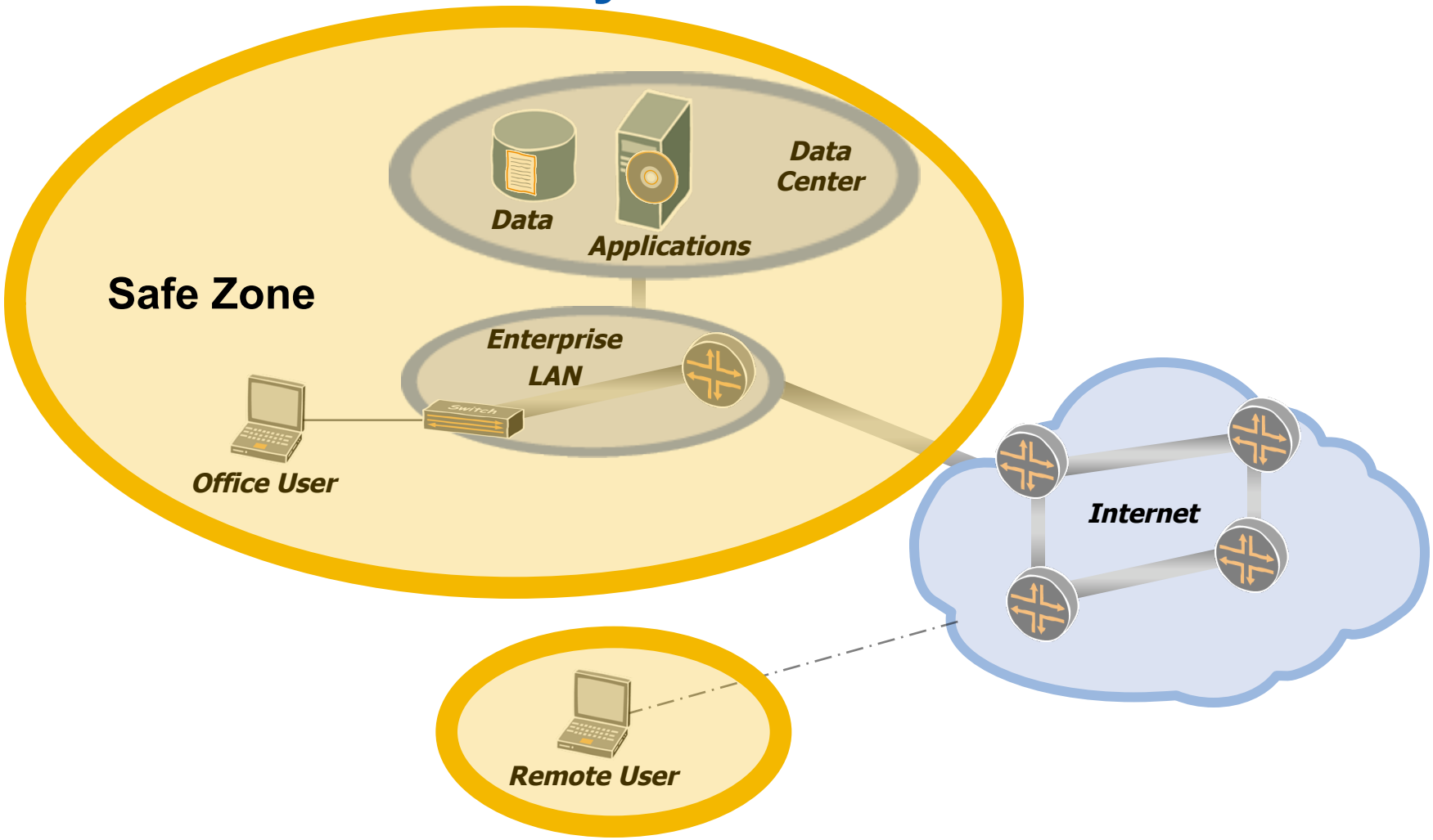
Legal and Regulatory Issues

- **Threats**
  - Laws and regulations may prevent cloud computing
    - Requirements to retain control
    - Certification requirements not met by provider
    - Geographical limitations – EU Data Privacy
  - New locations may trigger new laws and regulations

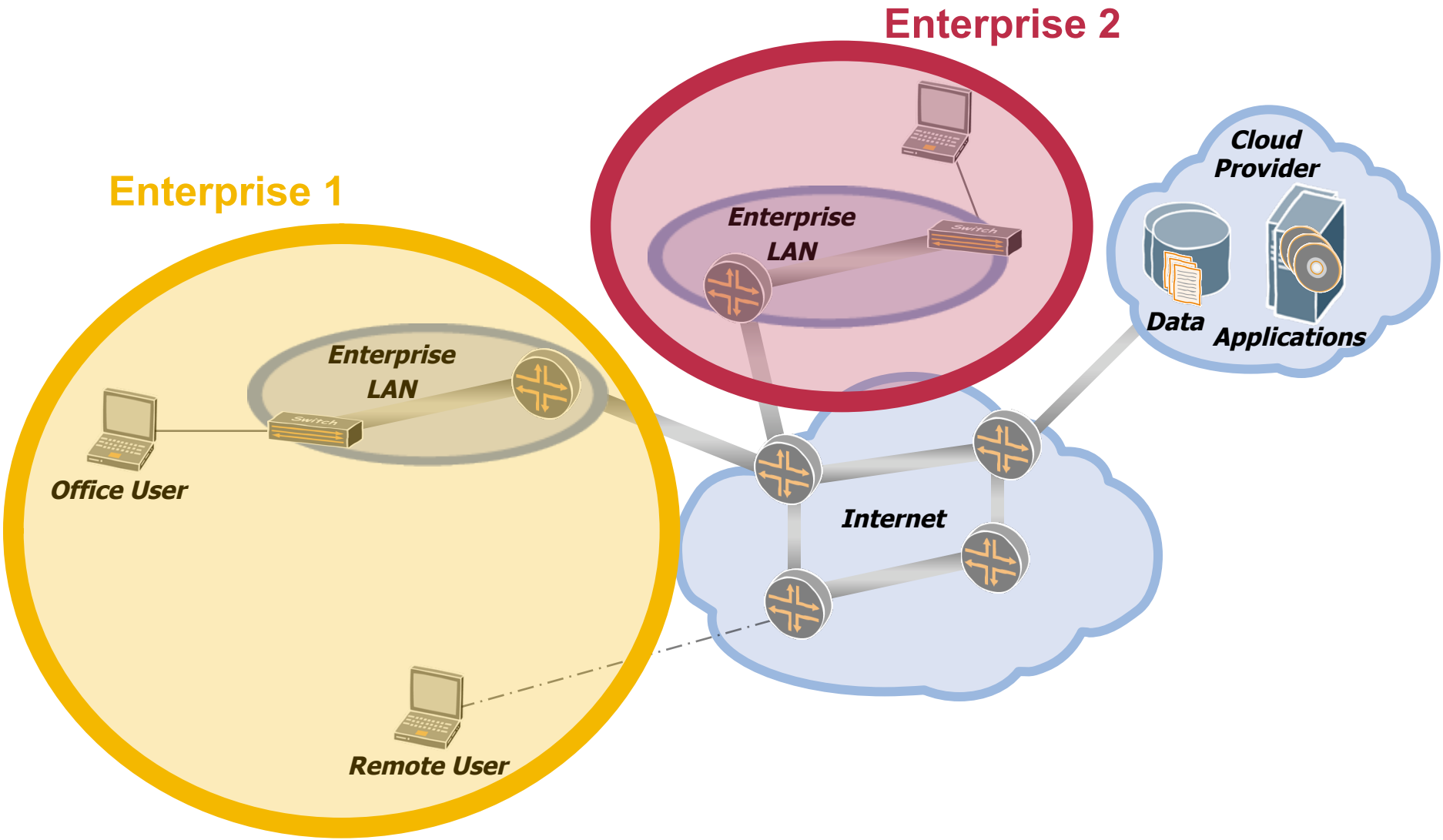
- **Countermeasures**
  - Evaluate legal issues
  - Require provider compliance with laws and regulations
  - Restrict geography as needed

Perimeter Security Model Broken

Perimeter Security Model



Perimeter Security with Cloud Computing?



Perimeter Security Model Broken

- **Threats**
  - Including the cloud in your perimeter
    - Lets attackers inside the perimeter
    - Prevents mobile users from accessing the cloud directly
  - Not including the cloud in your perimeter
    - Essential services aren't trusted
    - No access controls on cloud

- **Countermeasures**
  - Drop the perimeter model!

Integrating Provider and Customer Security

- **Threat**
  - Disconnected provider and customer security systems
    - Fired employee retains access to cloud
    - Misbehavior in cloud not reported to customer
- **Countermeasures**
  - At least, integrate identity management
    - Consistent access controls
  - Better, integrate monitoring and notifications
- **Notes**
  - Can use SAML, LDAP, RADIUS, XACML, IF-MAP, etc.

Agenda

- What is Cloud Computing?
- Security Analysis of Cloud Computing
- **Conclusions**

Bottom Line on Cloud Computing Security

- **Engage in full risk management process for each case**
- **For small and medium organizations**
  - Cloud security may be a big improvement!
  - Cost savings may be large (economies of scale)
- **For large organizations**
  - Already have large, secure data centers
  - Main sweet spots:
    - Elastic services
    - Internet-facing services
- **Employ countermeasures listed above**

Security Analysis Skills Reviewed Today

- **Information Security Risk Management Process**
  - Variations used throughout IT industry
    - ISO 27005, NIST SP 800-30, etc.
  - Requires thorough knowledge of threats and controls
  - Bread and butter of InfoSec – Learn it!
  - Time-consuming but not difficult

- **Streamlined Security Analysis Process**
  - Many variations
    - RFC 3552, etc.
  - Requires thorough knowledge of threats and controls
  - Useful for organization-independent analysis
  - Practice this on any RFC or other standard
  - Become able to do it in 10 minutes

Discussion