the Internet is for everyone

Protecting the Internet's Link & Data Storage Challenges

Shernon Osepa

Manager Regional Affairs Latin America & the Caribbean

ITU Security Workshops

Quito, Ecuador

27 June 2016

Internet Society

InternetSociety.org

Agenda

- How is the Internet Governed?
- The Internet's "Three Operational Layers"
- Addressing Cybersecurity Challenges
- The Internet's Link and its Security
- Data Storage Challenges
  - Costs
  - Security

How is the Internet governed?

- ***Some facts regarding the Internet and its economy***
  - > 3 billion users
  - > 950 million websites
  - Thousands of autonomous networks connected
  - 284 million domain names registered (>120 million .com, >100 million ccTLDs)
  - Last 30 seconds > USD 1.2 million dollars spent on E-commerce
- ***No central control body (chaos?)***
  - Initial focus was not on control but to create something that could grow to a much larger scale
- ***Multi-stakeholder model (openness, collaboration and consensus-oriented decision-making)***
  - Governments, Businesses, Civil Society, Technical Community
  - “Power” is gained by merits not hierarchy
- ***Effectiveness***
  - How it has grown and how stable it is

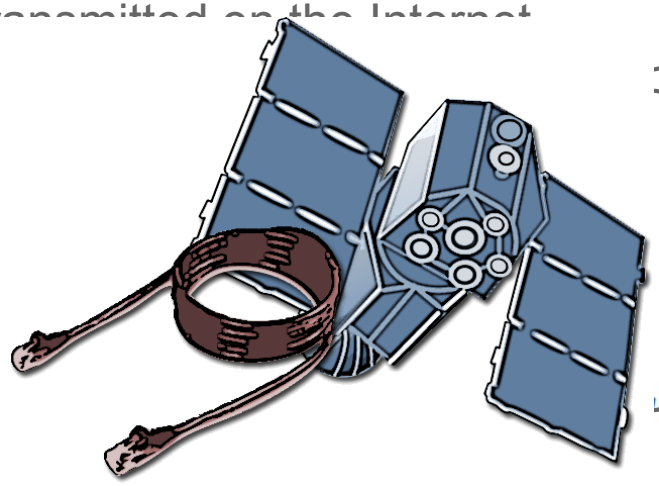
Internet Society
InternetSociety.org

Internet's Three Operating Layers

Content and applications standards (HTML, XML, Java) – Promotes creativity and innovation in applications leading to email, World Wide Web, ebanking, wiki, Skype, Twitter, Facebook, Yahoo, Google, YouTube and much more

Internet protocols and standards (TCP/IP, DNS, SSL) – TCP/IP, controls traffic flow by dividing email and web data into packages before they are tr

Telecommunications infrastructure – Physical network made up of underwater cables, telephone lines, fiber optics, satellites, microwave wi-fi, and so on Facilitates transfer of electronic data over the Internet



4

The Internet's Link and its Security

Definition of cyber security

- *"Cyber security refers to preventative methods to protect information from being stolen, compromised or attacked in some other way";*

- For the purposes of this presentation, cyber security is defined as "*anything that includes* ***security problems*** *specific to the Internet and their technical and non-technical solutions";*

Definition of cyber security

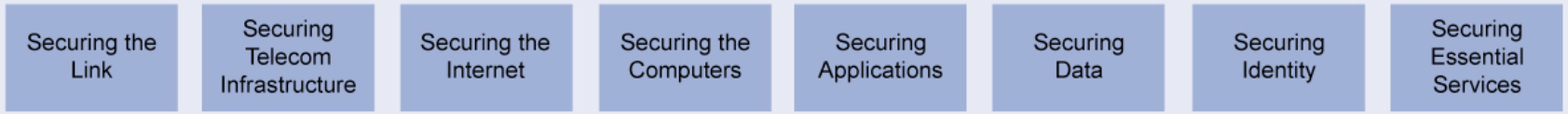
- *"Cyber security refers to preventative methods to protect information from being stolen, compromised or attacked in some other way";*

- For the purposes of this presentation, cyber security is defined as "*anything that includes* ***security problems*** *specific to the Internet and their technical and non-technical solutions";*

- Not every crime that occurs on the Internet is covered by the term cyber security. A **crime is a crime**, and simply moving it to the Internet doesn't make it special!

Cyber Security Themes

- Because the scope of cybersecurity is so broad, it is helpful to break it down into these categories



Cybersecurity Themes

Securing the link

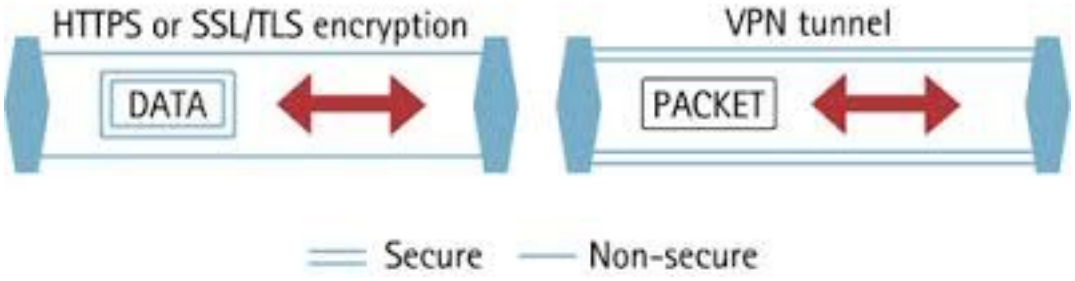
- Internet packets inherently have no security
- To prevent unauthorized “sniffing” or eavesdropping sensitive data must be encrypted
- In 2010 Eric Butler demonstrated with “Firesheep” that unencrypted FB traffic could be eavesdropped in public wifi areas
- A few approaches to encrypting this:
  - At the data link layer(MACSec and Wifi Protected Access);
  - At the IP layer(IPSec);
  - At the application layer(SSL/TLS and SSH etc).

The application/content layer the portal to social and economic development

Successful only if there is trust!

TLS Basics

- Transport Layer Security (TLS) encrypts data sent over the Internet to ensure that eavesdroppers and hackers are unable to see what you transmit:
  - which is particularly useful for private and sensitive information such as passwords, credit card numbers, and personal correspondence.



What is it?

- TLS is a cryptographic protocol that provides end-to-end security of data sent between applications over the Internet
- It is mostly familiar to users through its use in secure web browsing, and in particular the padlock icon that appears in web browsers when a secure session is established
- However, it can and indeed should also be used for other applications such as e-mail, file transfers, video/audioconferencing, instant messaging and voice-over-IP, as well as Internet services such as DNS and NTP

What is it? 2nd

- TLS is a cryptographic protocol that provides end-to-end security of data sent between applications over the Internet
- It is mostly familiar to users through its use in ***secure web browsing***, and in particular the padlock icon that appears in web browsers when a secure session is established
- However, it can and indeed should also be used for other applications such as e-mail, file transfers, video/audioconferencing, instant messaging and voice-over-IP, as well as Internet services such as DNS and NTP.

What is it? 3rd

- TLS evolved from Secure Socket Layers (SSL) which was originally developed by Netscape Communications Corporation in 1994 to secure web sessions
- SSL 1.0 was never publicly released, whilst SSL 2.0 was quickly replaced by SSL 3.0 on which TLS is based
- TLS was first specified in RFC 2246 in 1999 as an applications independent protocol, and whilst was not directly interoperable with SSL 3.0, offered a fallback mode if necessary
- However, SSL 3.0 is now considered insecure and was deprecated by RFC 7568 in June 2015, with the recommendation that TLS 1.2 should be used. TLS 1.3 is also currently (as of December 2015) under development and will drop support for less secure algorithms.

What is it? 4th

- It should be noted that TLS does not secure data on end systems. It simply ensures the secure delivery of data over the Internet, avoiding possible eavesdropping and/or alteration of the content

- TLS is normally implemented on top of TCP in order to encrypt Application Layer protocols such as HTTP, FTP, SMTP and IMAP

- It can also be implemented on UDP, DCCP and SCTP as well (e.g. for VPN and SIP-based application uses). This is known as Datagram Transport Layer Security (DTLS) and is specified in RFCs 6347, 5238, 6083

Why you should care or deploy TLS

- Data has historically been transmitted unencrypted over the Internet

- The IAB therefore released a statement in November 2014 calling on protocol designers, developers, and operators to make encryption the norm for Internet traffic, which essentially means making it confidential by default

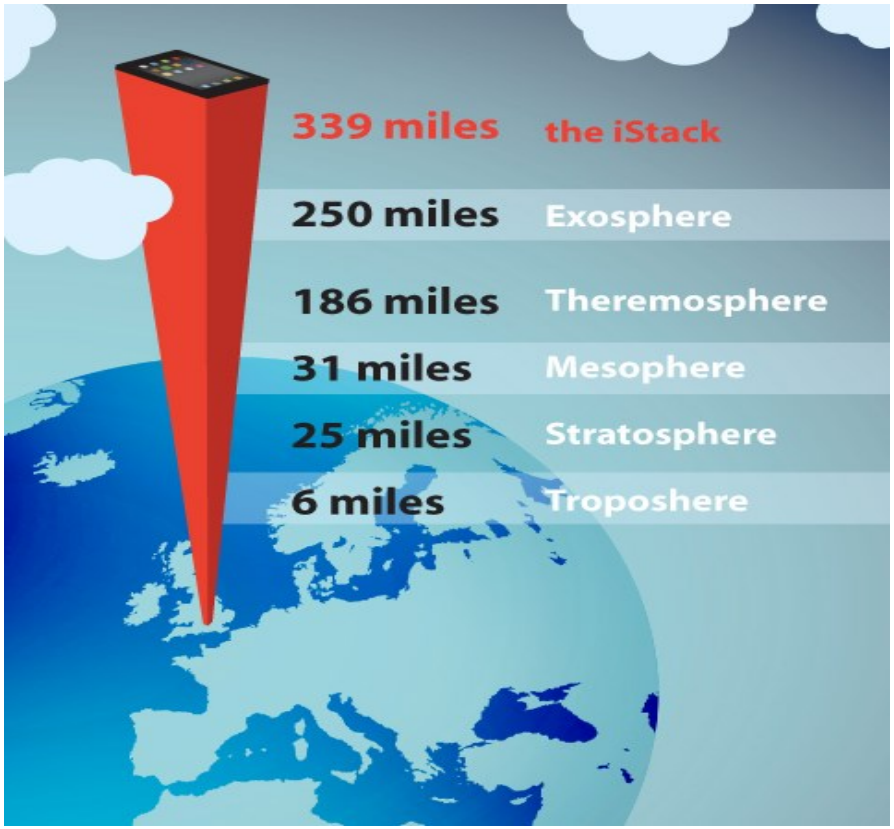
- Without TLS, sensitive information such as logins, credit card details and personal details can easily be gleaned by others, but also browsing habits, e-mail correspondence, online chats and conferencing calls can be monitored

On Data storage challenges

- 1 ***Terabyte*** 62.5 fully loaded IPads (*16 Gigabytes memory*)
- 1 ***Petabyte*** 62,500 fully loaded Ipads
- 1.2 ***Zettabytes*** 75 billion fully loaded IPads

On Data storage challenges

- How big is the Internet?

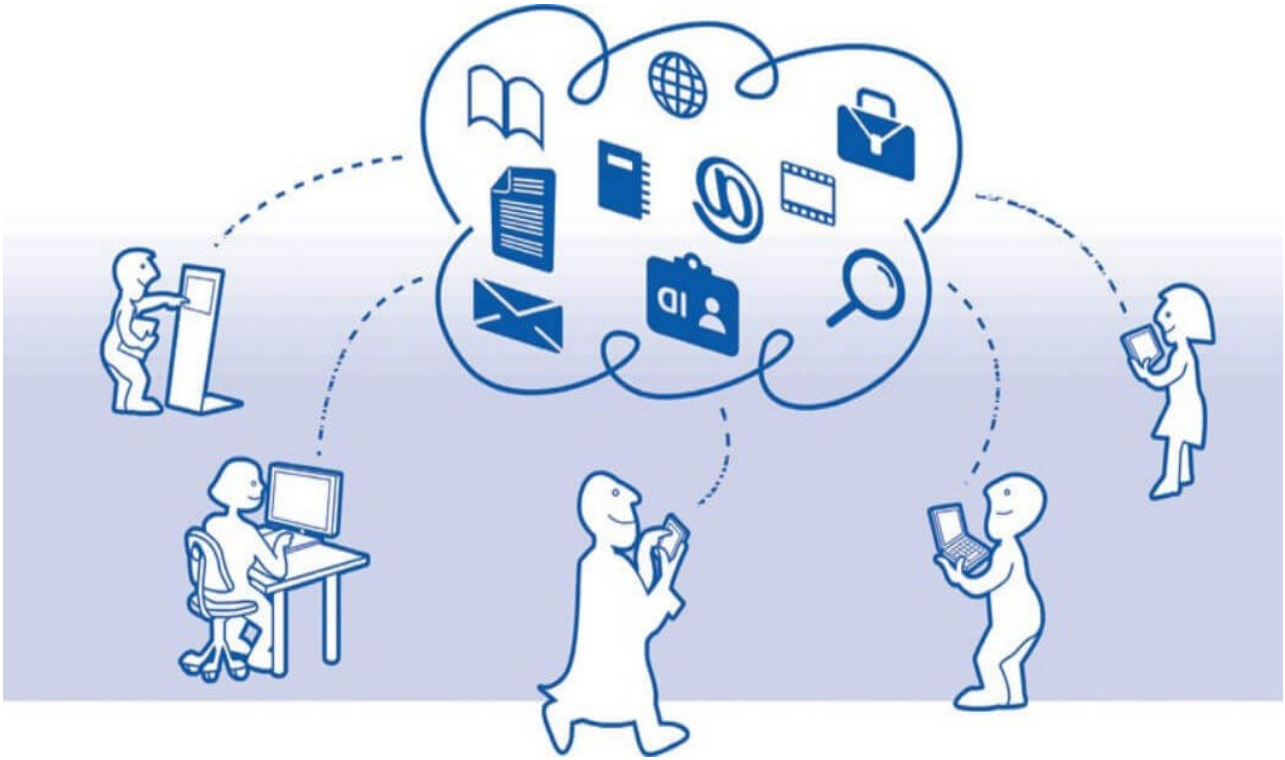


All these data need to be stored somewhere

- Local servers
- Or in the “clouds”
  - in reality clouds don’t exist as these are just private or corporate datacenters

The concept of cloud computing is not new

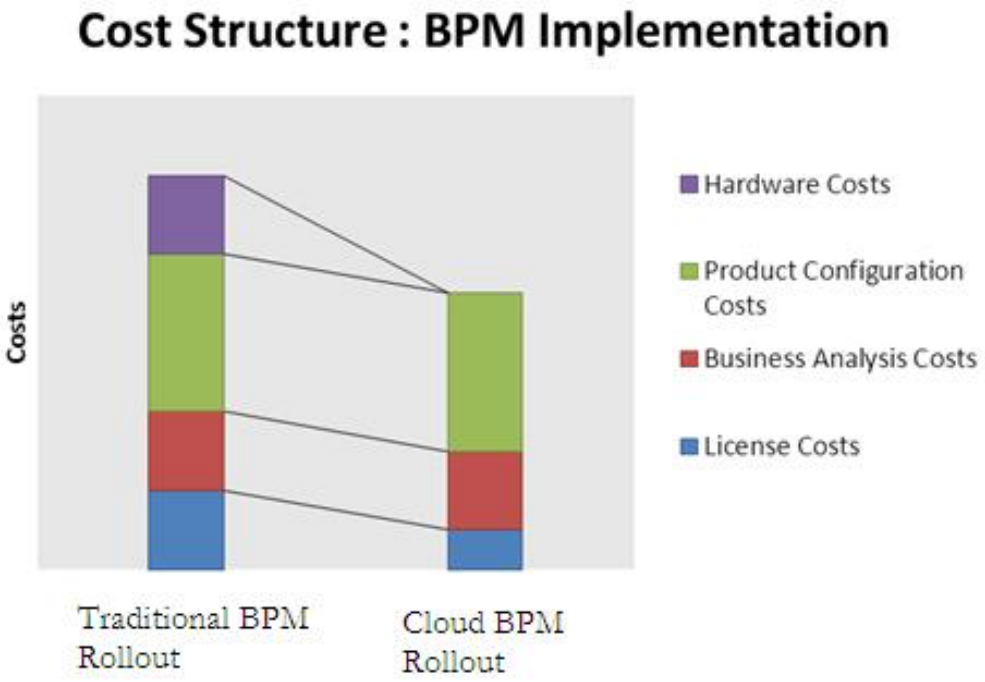
- Yahoo, Hotmail, etc. are all forms of cloud computing



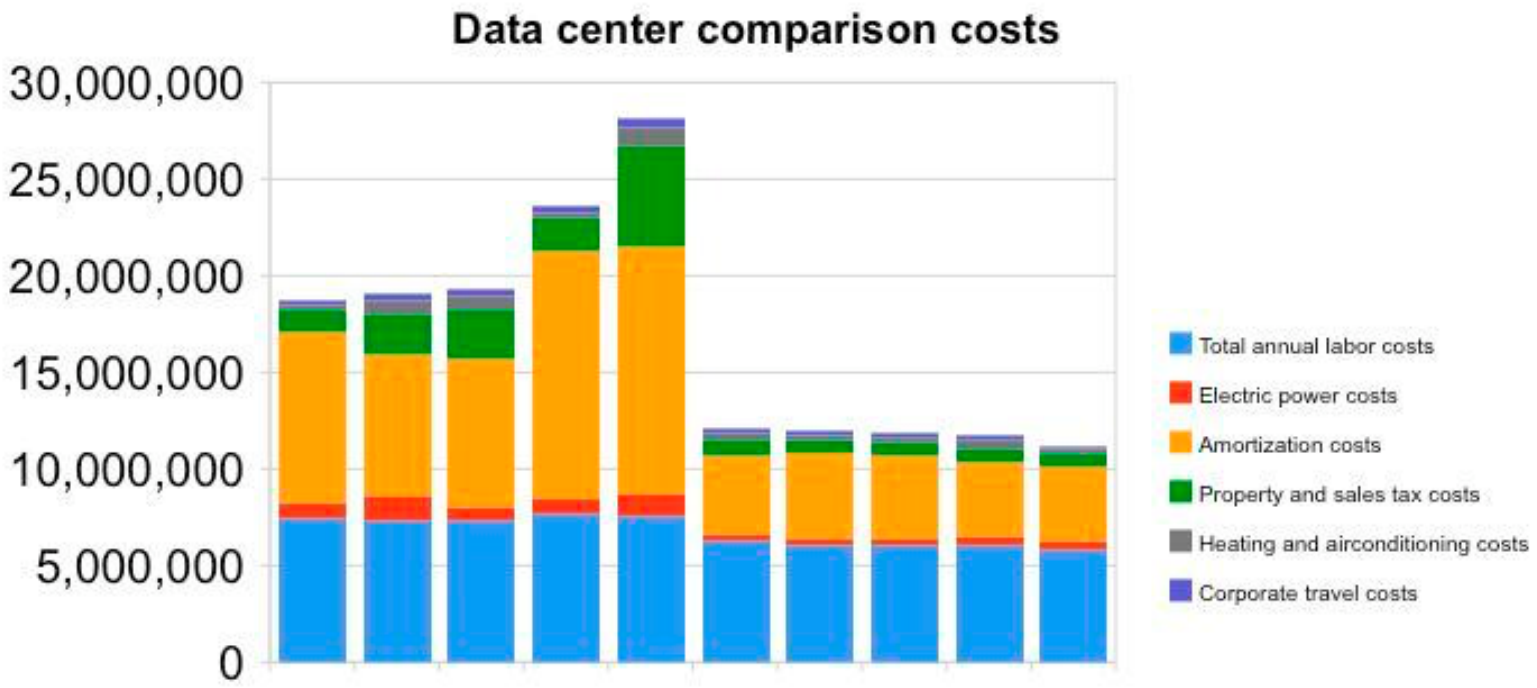
Reasons to storing data in “clouds”

- To focus more on core business
- Avoiding network management complexities
- Costs based

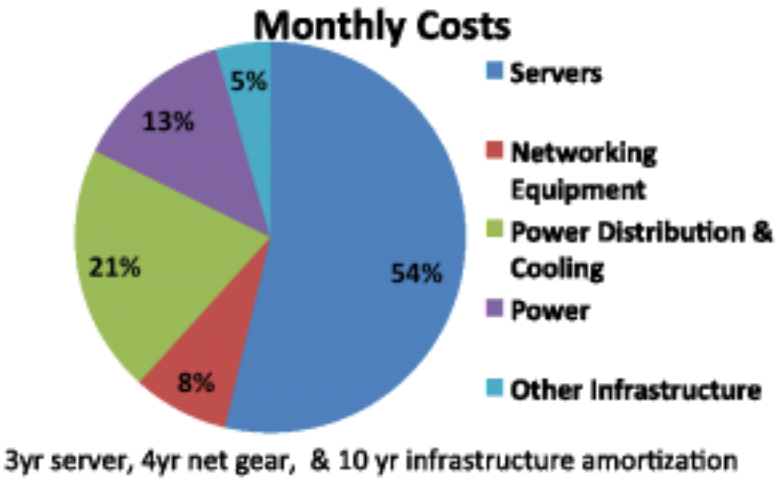
Reasons to storing data in “clouds”/costs



Reasons to storing data in “clouds”/ costs 2

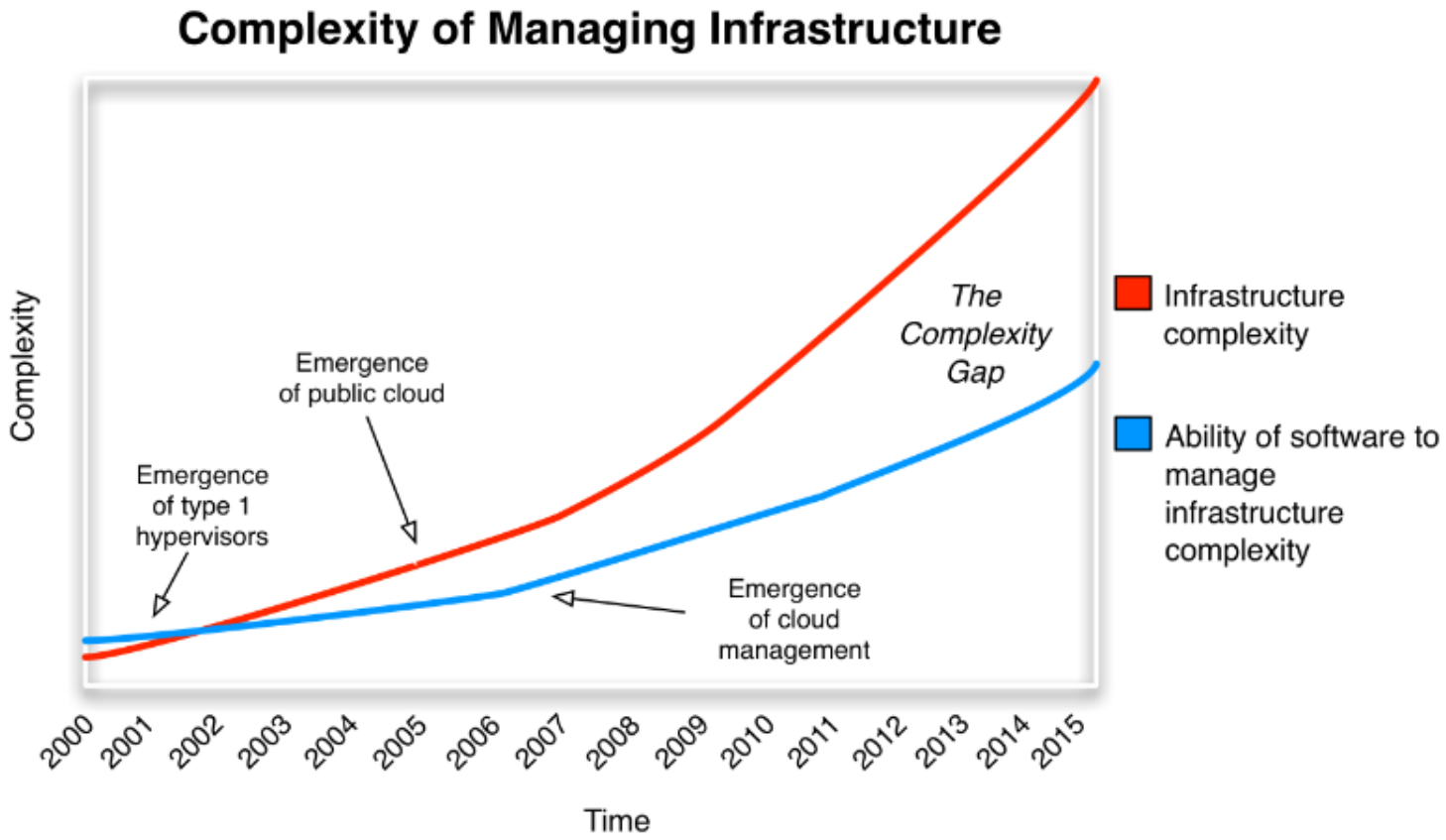


Reasons to storing data in “clouds”/ costs 3



3yr server, 4yr net gear, & 10 yr infrastructure amortization

Reasons to storing data in “clouds”/ infra



Concerns regarding cloud data usage

- **Security**
  - Post Snowden has brought some great concerns globally
- **Privacy**
  - How is being handled with sensitive data
- **Key question: What to put in the clouds!**
  - When considering moving to the clouds an organization might decide for various reasons (security+trust) NOT to put certain services into the clouds……..

Using of cloud based services /data centers?

- Security + trust
  - Essential + sensitive data
- Costs
- Technical aspects/ infrastructure management


the Internet is for
everyone
Thank You
Shernon Osepa
osepa@isoc.org
Internet Society
InternetSociety.org