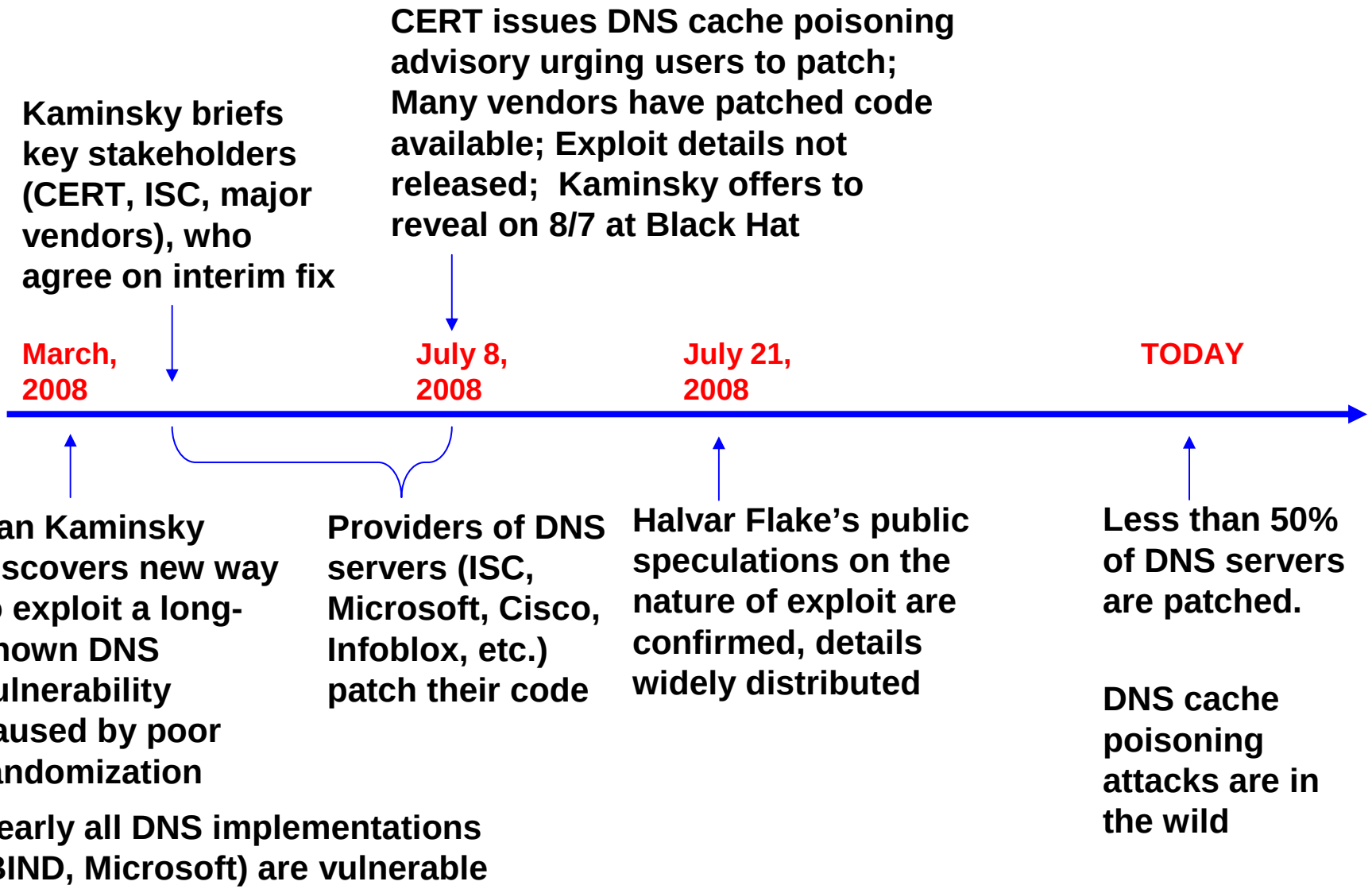
Infoblox

DNS Security: New Threats, Immediate Responses, Long Term Outlook

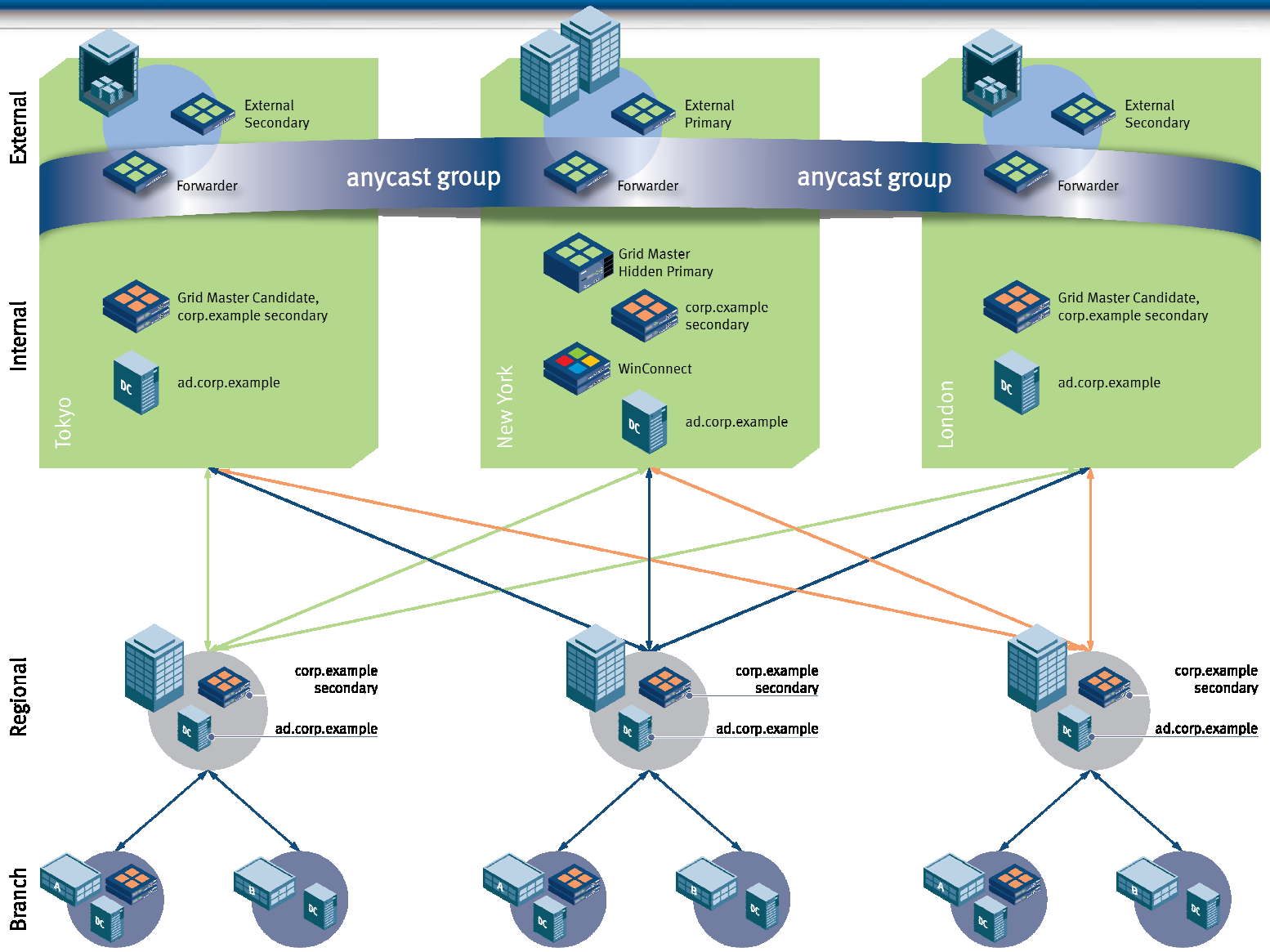
A Brief History of the Recent DNS Vulnerability



What Do I Do?

1. **Upgrade to the latest (patched) version of your name server**
   - That is, the newest version that includes a patch for the new vulnerability
     - ISC has a new version of BIND
     - Microsoft has a new version of the Microsoft DNS Server
     - Infoblox has a new version of NIOS
     - And so on
   - The patch actually addresses some other known vulnerabilities, too
   - Concerned about patching (labor, DNS outages, errors, etc.)?
     - Understandable, but do it anyway!
     - It's important, and it works
       - >600 Infoblox customers have downloaded patched code since July 8, most have upgraded and are in production today
2. **Restrict or disable recursion wherever possible**
   1. Note: There can be issues with recursive DNS servers behind NAT/PAT firewalls
3. **Monitor and act quickly when attacks are ongoing**
4. **Start working on a plan for DNSSEC**

DNS Best Practices Architecture is the Start: Redundancy, Resiliency, Serviceability



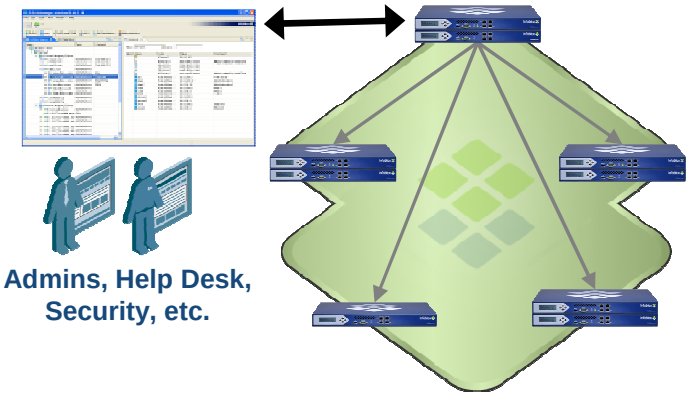
Modern Approaches Make it Easier to Implement and Manage Best Practices DNS Architectures

Infoblox

DNS Appliances

- Hardened, secure platforms
- Integrated core network services: DNS, DHCP, IPAM, RADIUS, FTP/TFTP/HTTP, FTP, more…
- Built-in high availability

Appliance Grid



- Centralized management, visibility & control
- One-touch disaster recovery
- One-touch patching & upgrades with no downtime

Serviceability and Security go Hand in Hand

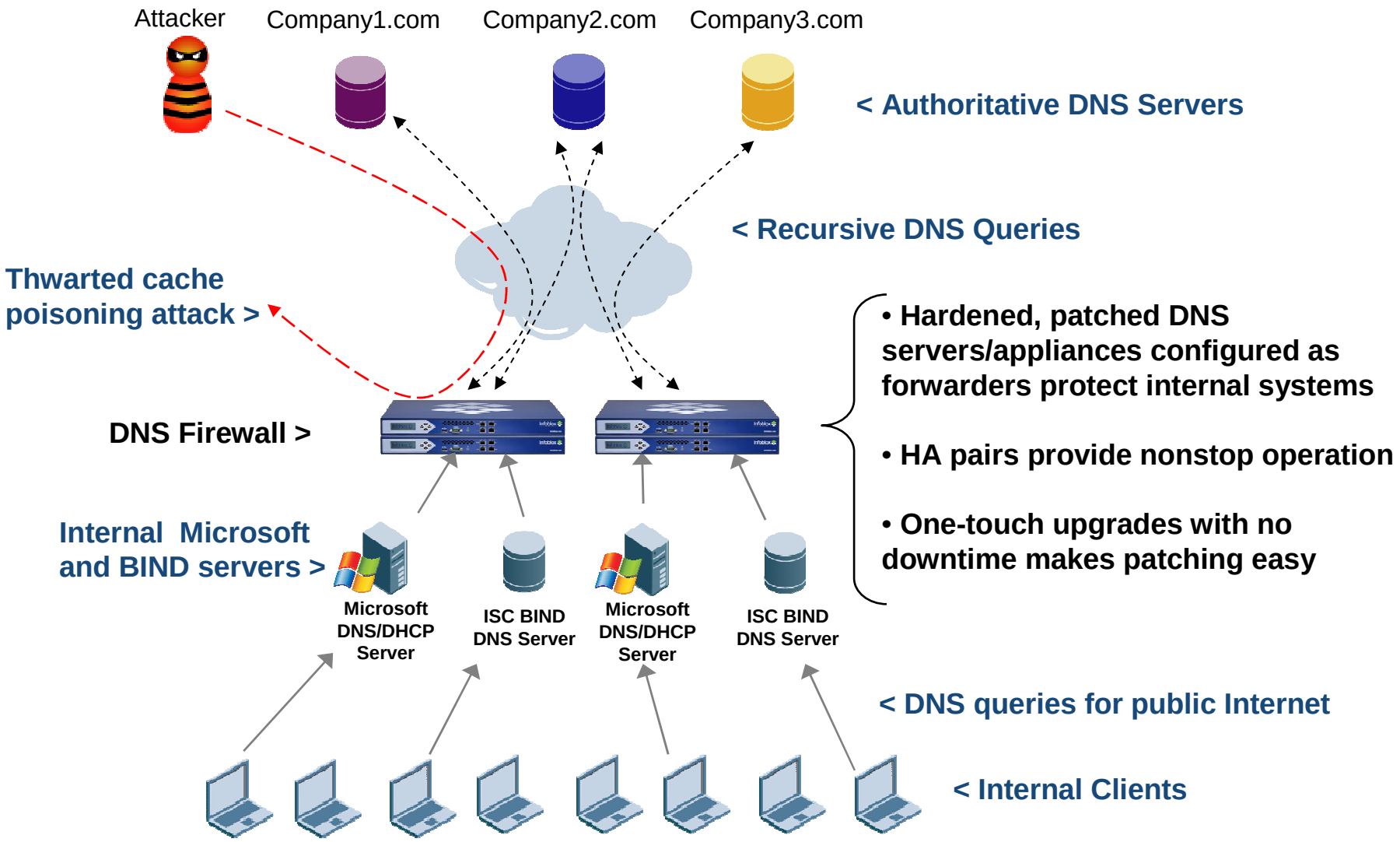
- "Serviceability needs to start becoming a more important purchasing metric.
- Serviceability is, ultimately, the measure of software flaw survivability"
  - **Dan Kaminsky**

✓ **Infoblox Grid Technology makes upgrading groups of DNS servers easy, fast and reliable**

– The Ultimate in serviceability

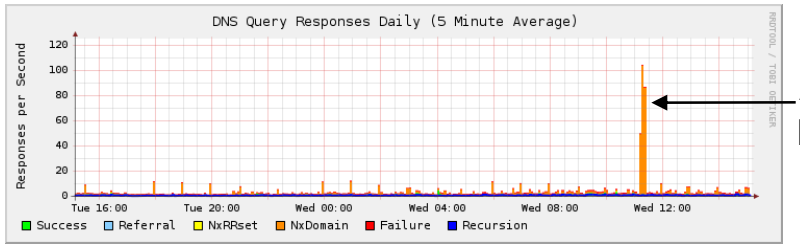
> ***"Ok, that was too easy.***
>
> ***Much better than upgrading***
>
> ***BIND. Thanks!!!!"***
>
> *- Michael L Hershberger, Armstrong*

Implementing a Hardened Forwarding Tier Provides a "DNS Firewall", Protecting Internal Servers



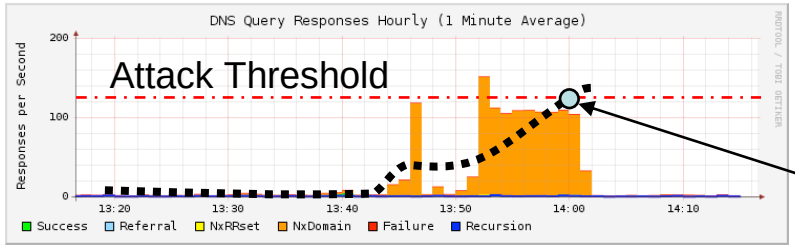
Infoblox DNS Security Features Provide Visibility & Response

- **DNS Protocol Monitoring**
  - Real-time reporting



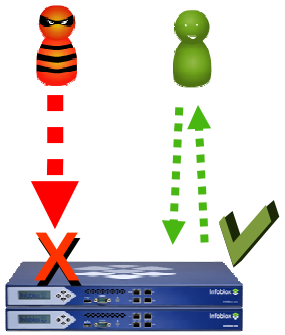
Attack in Progress

- **Attack alerts**
  - Email/trap when attack profile thresholds exceeded



Alert Trigger

- **Attack mitigation**
  - Limit DNS query rate by source address and other parameters



Free Tools are Available to Support DNS System Testing and Assessment

- **DNS Vulnerability Test**
  - http://www.doxpara.com
- **DNS Advisor (External) & DNS Advisor Pro (Internal)**
  - http://www.infoblox.com/services/dns_advisor.cfm
- **DNS Audit Guidelines**
  - http://www.infoblox.com/library/dns-security-center.cfm

Looking Forward: The Path to roll-out DNSSEC

- **2004-2005: Infoblox trials DNSSEC with US Government agencies**
  - Project put on hold because of lack of Interest
- **2007-2008: Infoblox re-connects with DNSSEC pioneers**
  - Steve Crocker *www.dnssec-deployment.org*
  - Olaf Kolkman *www.NLnetlabs.nl*
  - Staffan Hagnell www.iis.se
  - Cricket Liu, www.infoblox.com , Author of O'Reilly's "DNS and BIND"
  - Some end-users (primarily finance sector)
- **Today: Infoblox works on a phased approach for practical DNSSEC rollout**
  - DNSSEC in the Internet resolver (cacher/forwarder)
  - Infoblox Grid as the front end DNSSEC authoritative server (secondary)
  - Infoblox key management
    - Most challenging area in DNSSEC, together with last-mile and NSEC3 problem
    - Key distribution difficult (will be better when root and TLD's sign their zones)
    - Current tools store the key online and lack monitoring/logging and scalability
      - DISI, ZKT and DNSSEC-tools

Why is deployment rate of DNSSEC <1%

- **“DNSSEC is to complex to deploy”**
  - The weapon with which to shoot oneself in the foot is not a pop-gun but a military grade full automatic
- **“The root will never get signed”**
- **“There is no economy to push deployment”**
- **“Cache poisoning can be mitigated by correctly implementing random query ports and proper query ID”**
- **“The specification is still a moving target”**
- **“New technology; chicken and egg”**
- **“Zone walking possibility”**
- **“Automation for key rollover and distribution is not fully available”**
- **“Yes, .se TLD is signed, but what about my .com zone than?”**

Implementing DNSSEC Requires a Complete Set of Standards, Tools and Processes

- RRsets signing algorithm? (RSA/SHA1 or DSA or …)
- TTL for all records in a RRset?
- How to store your private key?
- Signature (RRSIG) expiration time? (determines frequency of re-signing)
- Key Management tools? (DISI, DNSSEC-tools or ZKT - none scale well)
- Process for key certification by parent zone (DS) records?
- Certification of .com zone?
- Chain of trust?
- DNSSEC-capable resolvers configured to ask for signed responses first?
- Handling of queries that don't request signed responses?
- Application checks for DNSSEC signed responses (AD bit set)?
- Will resolvers configured to only accept signed responses?
- How to roll back to unsigned zones?
- ….????

The role of DNS solution manufacturers

- **Don’t just howl with wolfs**
- **Be smart, do research and develop a practical solution and process together with early adopters!**
- **Define a technology roadmap that could deliver key elements of a practical DNSSEC solution and process. These elements include:**
  - Implementation of a DNS protocol engine that completely complies to all DNSSEC standards. RFC 4033, 4034, 4035 (eg. BIND 9.3.2, NIOS 4.2)
  - Improved management tools to performing the administrative tasks related to DNSSEC
  - Development of high-powered, high-capacity hardware platforms that handles the cryptographic DNSSEC computations.

Summary

- **New threats can arise for vulnerabilities once believed "impractical" to exploit**
- **News of a new exploit (and fix) can happen at any time – serviceability (fast updates) is crucial to close vulnerability windows**
- **Best practices architecture can reduce risk**
- **Automated systems speed patching and eliminate downtime**
- **Everyone should do the following:**
  - Limit/disable recursion
  - Don't let internal devices directly query the Internet
  - Ensure sufficient DNS capacity
  - Update your software whenever a known vulnerability is found and patched
- **Organizations like ISACA and ISSA can take a leading role in developing, promoting and verifying DNS best practices**

References

- **CERT Advisory VU800113**
  http://www.kb.cert.org/vuls/id/800113ISC
- **ISC**
  www.isc.org
- **DNS Cache Poisoning Test**
  www.doxpara.com
- **DNS Best Practices White Paper**
  http://www.infoblox.com/library/whitepapers.cfm
- **DNS Advisor, Advisor LE, and Advisor Pro**
  http://www.infoblox.com/services/DNS_advisor.cfm
- **DNS Audit Guidelines**
  http://www.infoblox.com/library/DNS-security-center.cfm