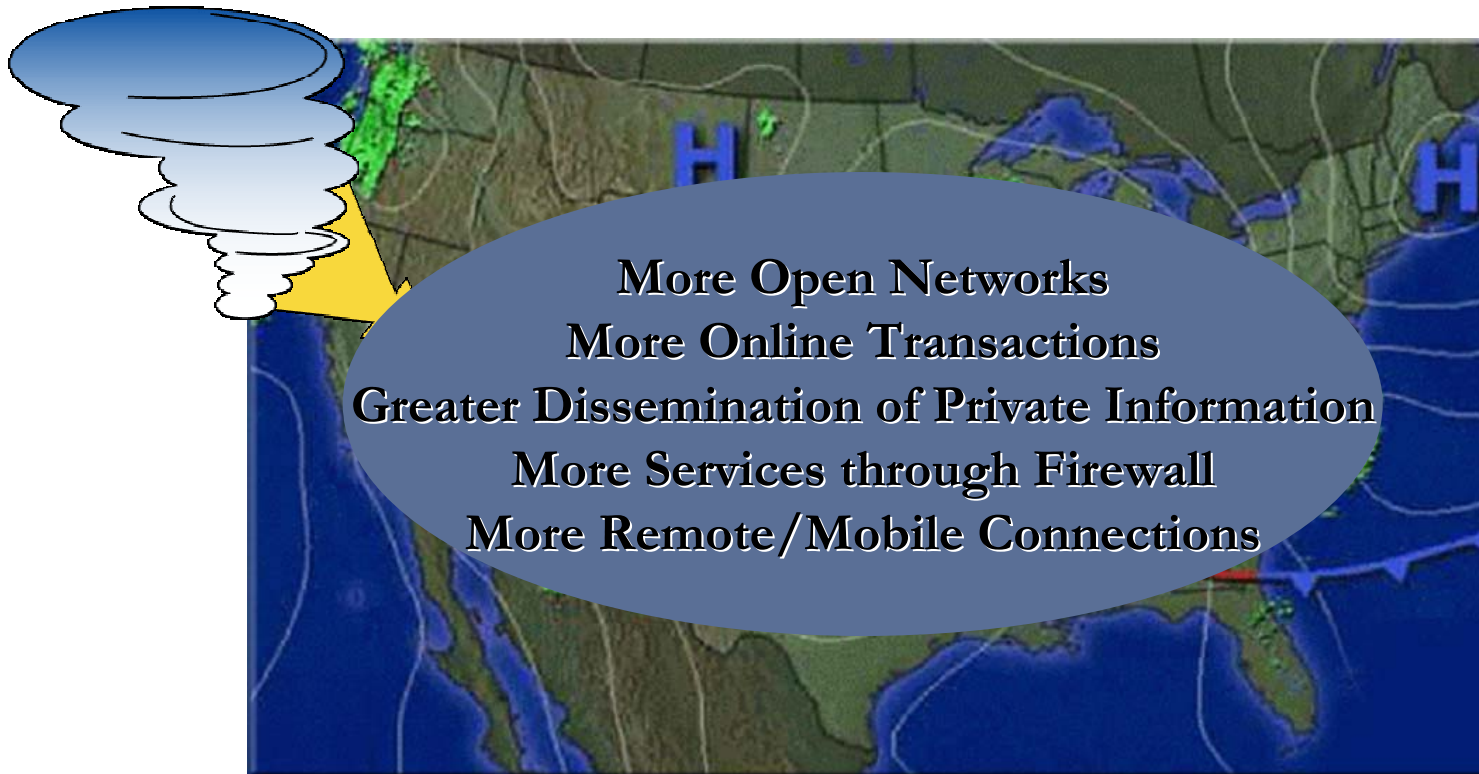




Implementing a Flexible and Secure Network Architecture

Ken Silva
Vice President and CSO
VeriSign

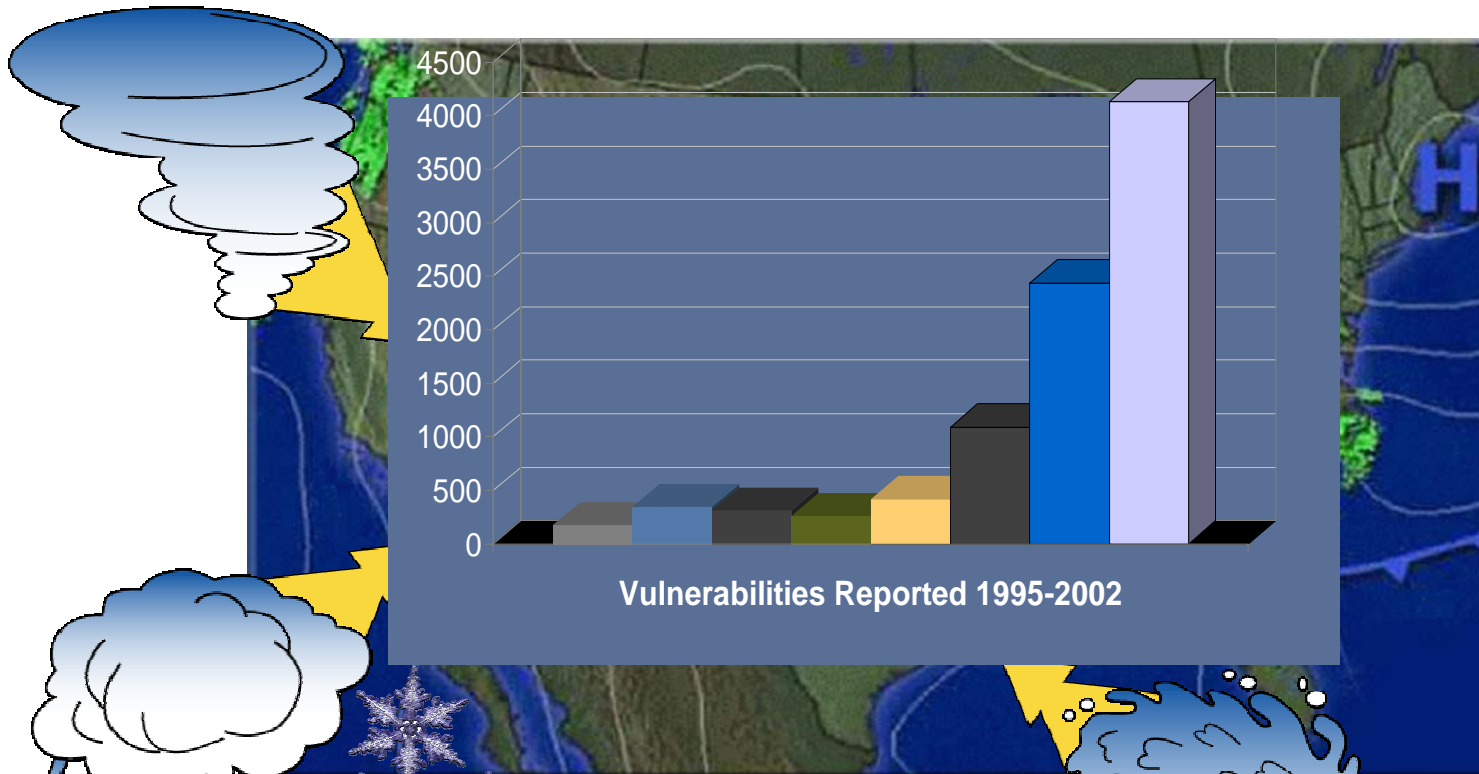
The Perfect Storm



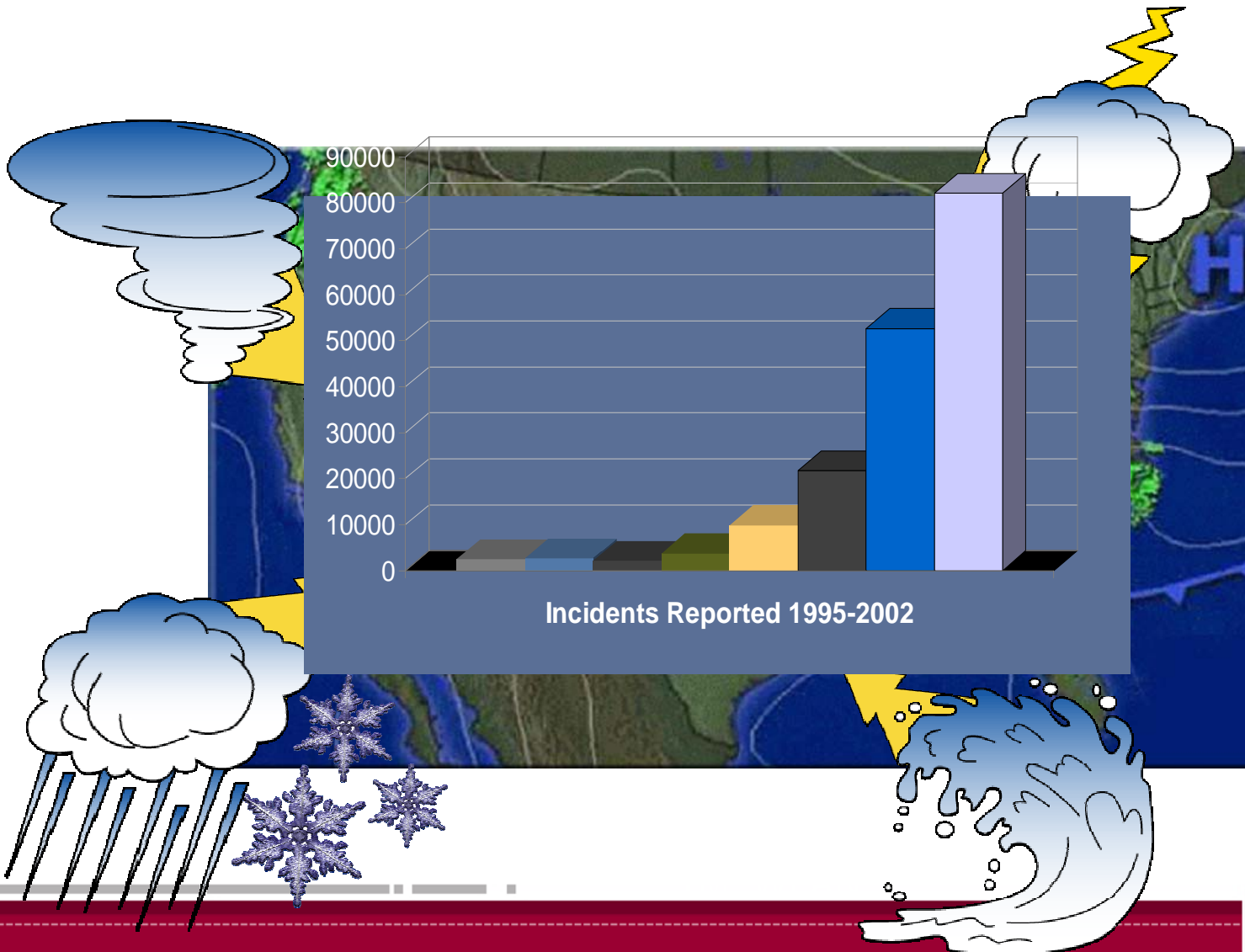
The Perfect Storm



The Perfect Storm



The Perfect Storm



The Perfect Storm



Things that Impact Security Decisions



- + Cost
- + Complexity
- + Time
- + Agility
- + Someone else has a better idea
- + Business model
- + Integrations

Brutal Facts

- + Security is not the most well-liked team in any organization
- + Security is usually a slow down to any deployment
- + Whatever rules you have will get overturned
- + Your rules will have to change frequently with your business
- + There was always tidbit that was left out in your decision process
- + Executives will always overrule your process

General Rules

- * **+ Maintain separate environments for each business unit**
 - + Allows for separate policies if needed
 - + Prevents the need for ever changing policies
- + Keep it crunchy to the core**
 - + Internal network policies are just as important as the external policies
 - + Keeps consistent methodology throughout
- + Different businesses have different needs**
 - + Cope with it
 - + If you fight it, you will lose
- + Start with security**
 - + Performance is easier manage
- + Firewalls are only as secure as the process behind them**

The Pieces



Routers with ACL



Packet Shapers



Firewalls



Switches



Load Balancers



Servers

Architecture

- * + Router ACLs are essential
 - + Don't rely on the lower performing Firewalls to do all of the filtering
 - + Routers generally perform better than firewalls
 - + Stop it before it ever gets in
- + Use QoS to manage the loads to various products
 - + Don't let one product damage another
- + Use firewalls for more fine grain packet inspection
 - + Firewalls manage state
 - + Better logging
- + Load balance and use the filters in the LB to further offer protection
 - + Performance of load balancers is very good today

Standards

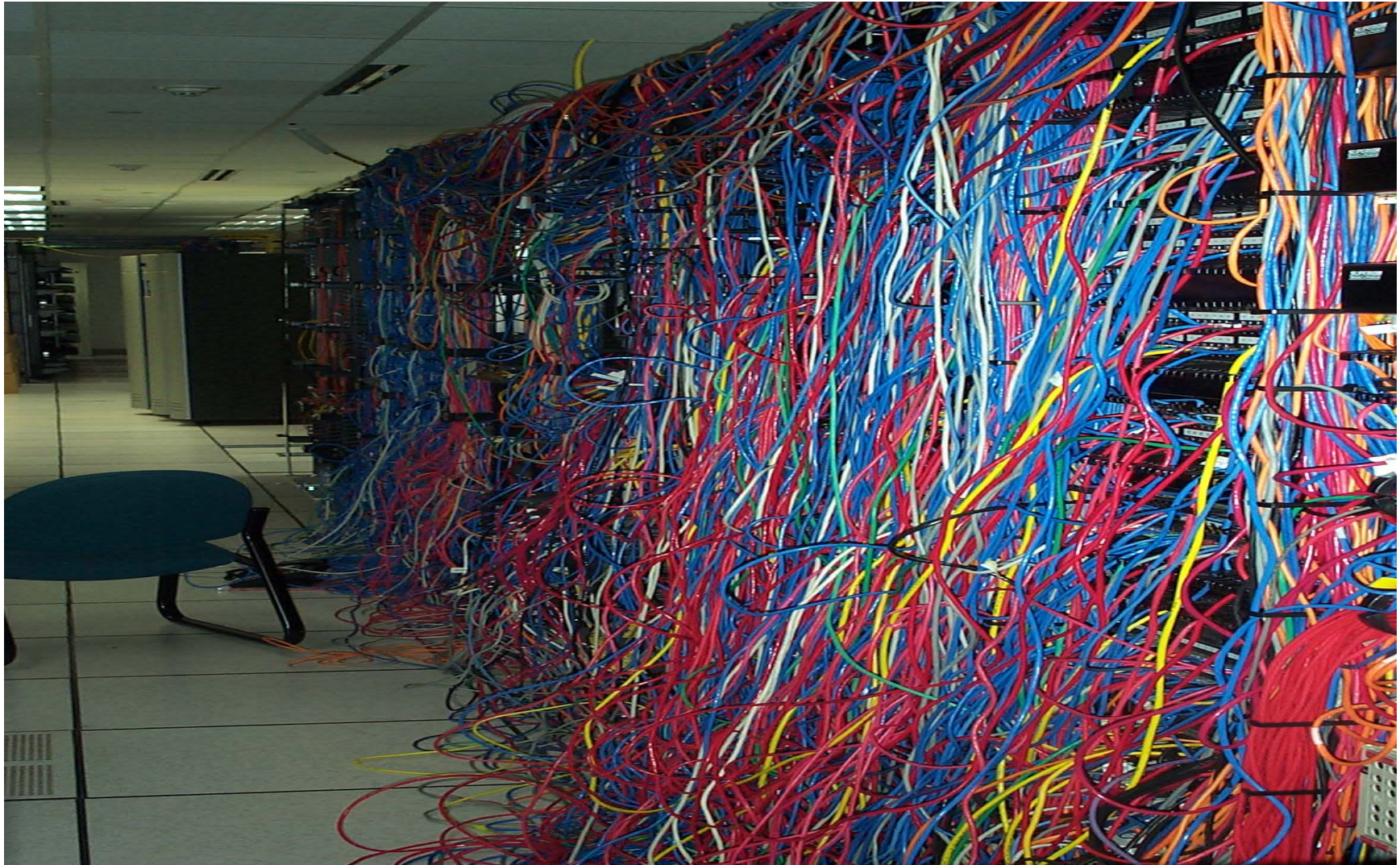


- + Having standards saves an enormous amount of work
- + Build all servers from a master build
 - + Put your security effort into that build
- + Have a couple of standards
 - + DMZ servers and backend servers for example
- + Do not let people build from CD/DVD
 - + Humans will make errors
 - + Not scalable
- + Continuously scan for changes or alterations from the standards
- + Standardize everything
 - + Routers, switches, firewalls, servers, firmware
 - + It's the only way to know what state you are in when vulnerabilities arise

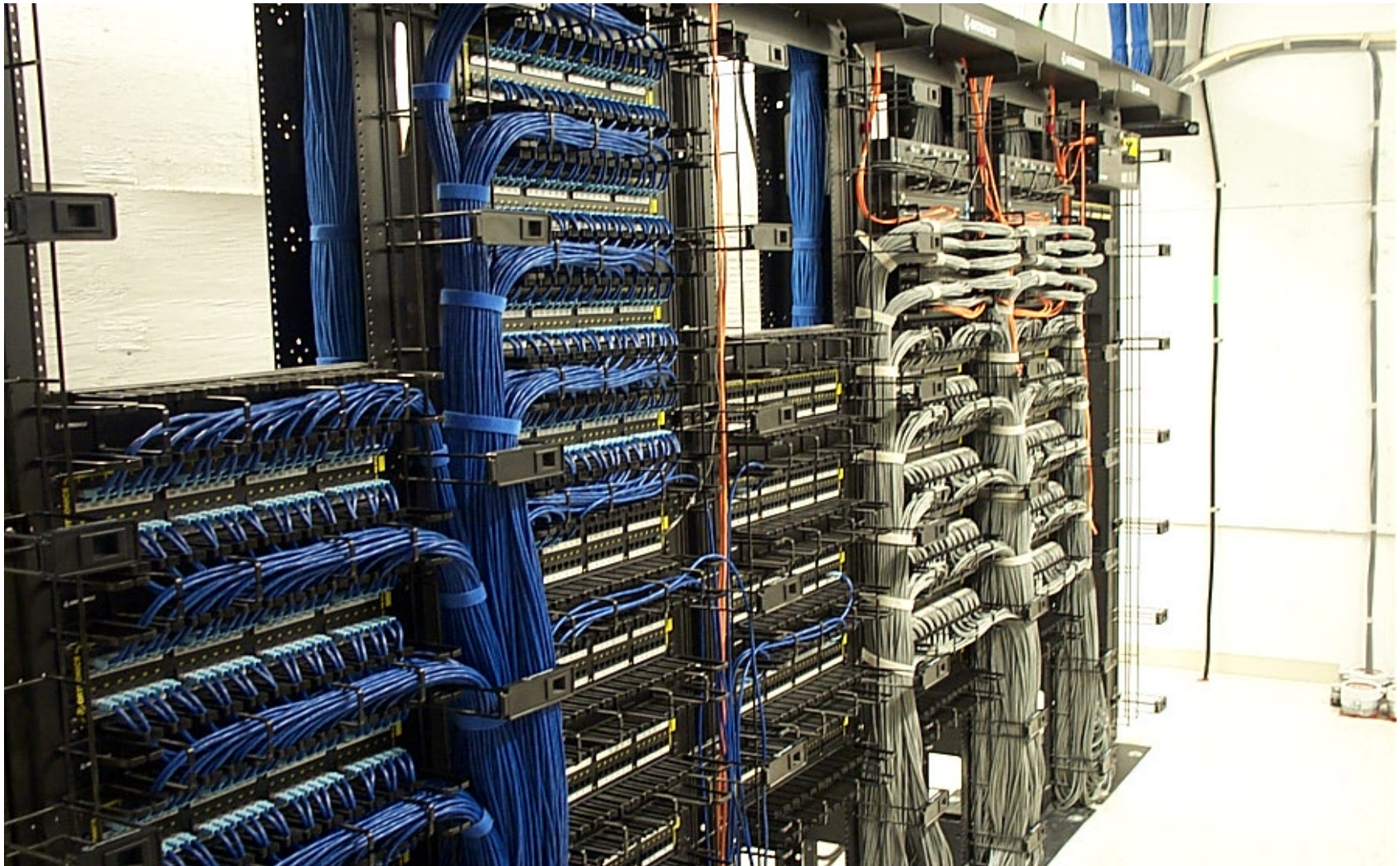
Extreme Standardization



Unmanageable



Manageable



Automated Standards

- * + **Have machines build new servers**
 - + People make mistakes
 - + Servers are already locked down for better security
 - + Security is involved at all phases
 - + Protect the build server

Overdo it

- * + Standards and change control just about can't be overdone (although it may seem that way)
- + Color coding patch cords can be a huge help
- + Don't let anything on the network that doesn't belong there
- + Protect your network from an inside threat just as much as an external threat

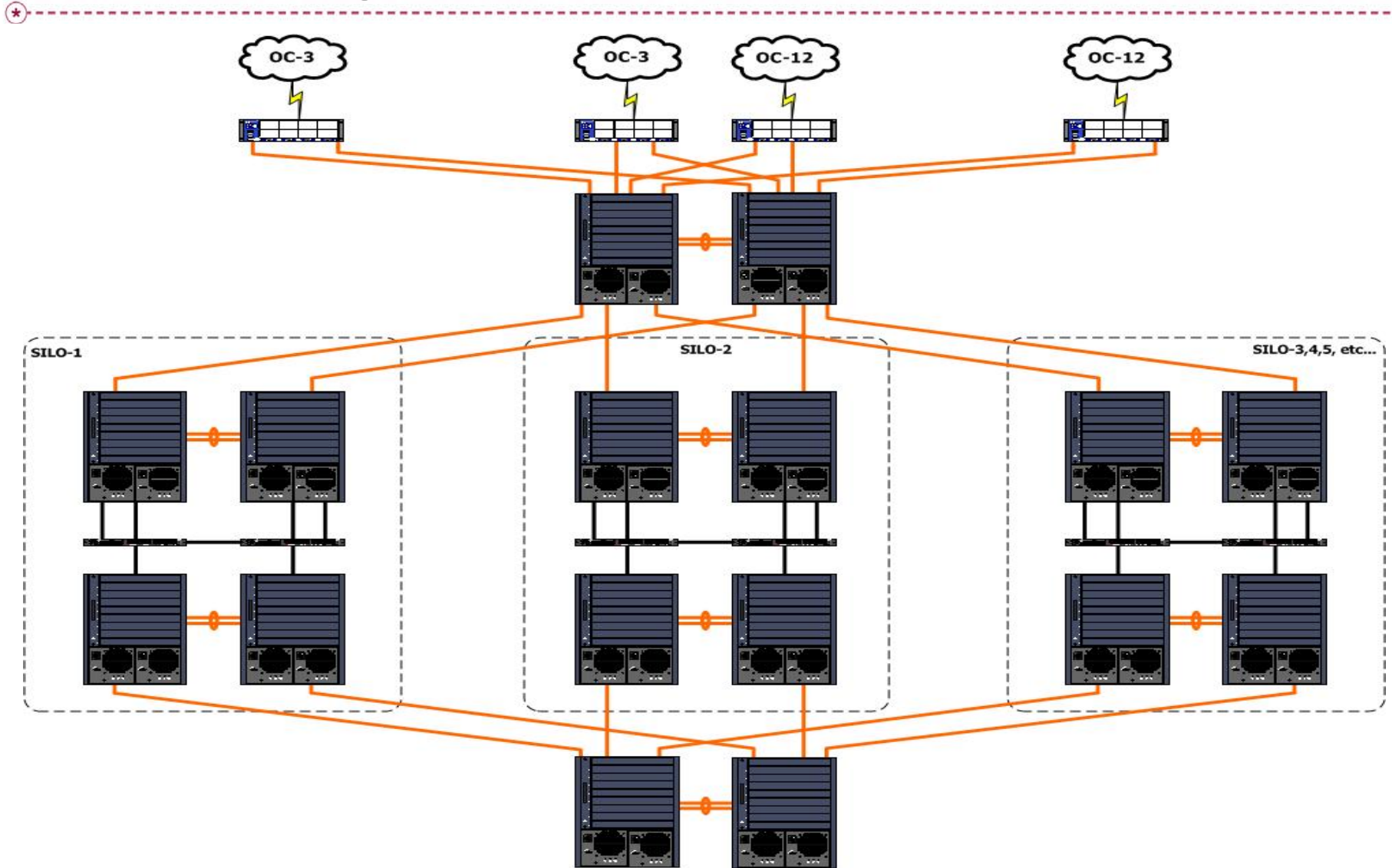
Know your Business

- + **Every business unit has differing needs**
 - + Some are open and some are very closed
 - + Some need more relaxed security
 - + Some need much tighter security
- + **Understand how the product works**
 - + Also how it will work in the future
- + **Develop strategically**
- + **Get in on the ground floor**
- + **Allow only the services that are required for that product**

Manage your Network Space

- + Standard VLANS for all networks
- + Use VLAN Management Policy Service (VMPS)
- + Aggressively seek out anyone adding machines to the network
- + Document every machine on the network (ALL OF THEM)
- + Use 802.1x authentication wherever possible
- + Keep stovepipes separate

The Building Blocks



Manage Compromise

- * + Businesses have to provide new services
- + Sometimes these involve scenarios you didn't anticipate.
- + Always push back on variance to standards, but be prepared to compromise
- + Understand where your REAL risks are

Getting to the Right Place

- * + Always start with what you really want
 - + Perhaps a little more
- + Always have a fallback position
- + Always know what you can live with
- + Explain the real risks
 - + Not something far fetched
- + Wherever possible, prove it
- + Build it with flexibility and you will thank yourself later

Help is on the way



- + Deep packet inspection
- + Intelligent IPS
- + Application aware Firewalls
- + ISP-based IPS systems
- + Intelligent traffic shaping
- + Network Access Controls

Questions



+ Questions?