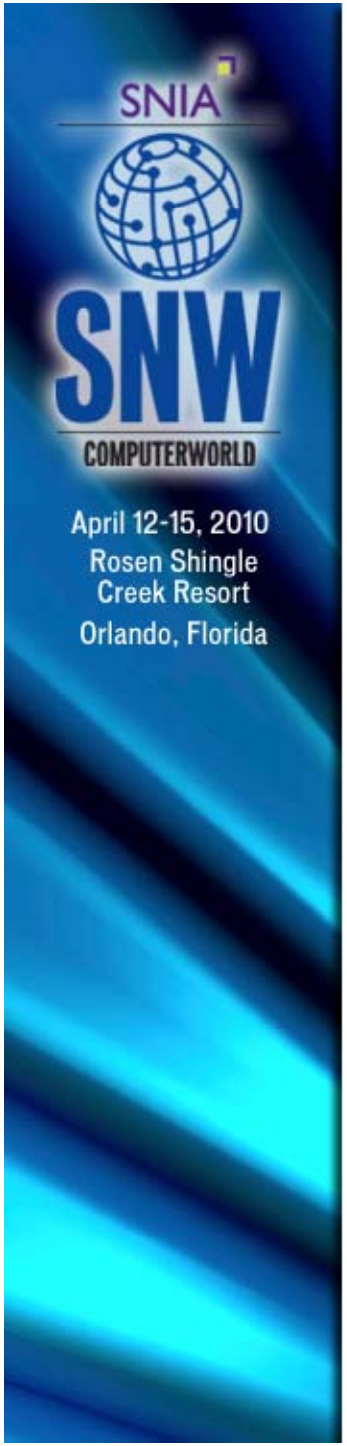
COMPUTERWORLD SNIA

SNW

April 12-15, 2010 | Rosen Shingle Creek Resort | Orlando, Florida

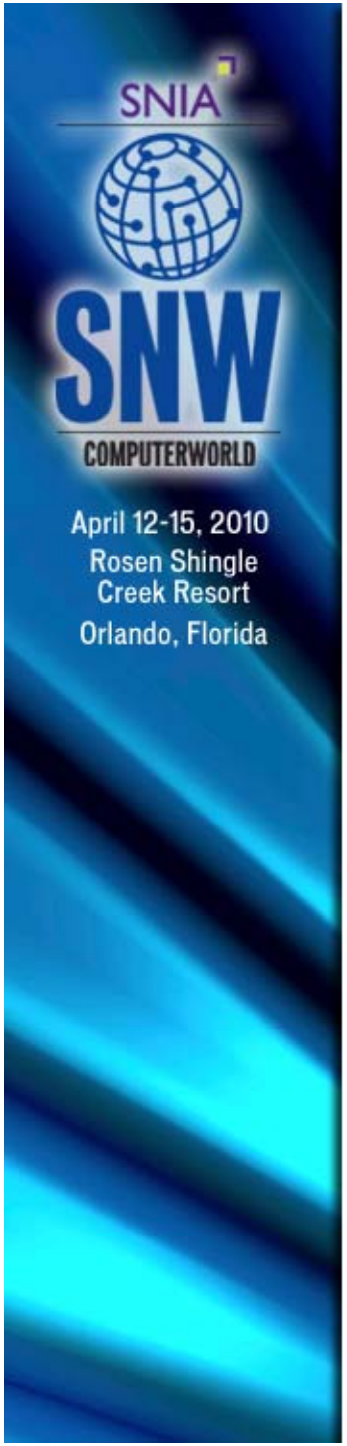


Nanette Lepore: How an International Designer Overhauled its Infrastructure for Security & Mobility

Eric Crutchlow, Sr. Systems Engineer for SonicWALL

Stacy Arruda, Supervisory Special Agent

FBI



AGENDA

- Background
- 2007 Security Breach
- 2008 DDOS Attack
- Lessons Learned & Best Practices

SNIA
SNW
COMPUTERWORLD
April 12-15, 2010
Rosen Shingle Creek Resort
Orlando, Florida

About Nanette Lepore

- Haute couture fashion designer
- 8 Boutiques in the U.S.
  - New York, Los Angeles, Bal Harbour, Chicago, Las Vegas, Boston and Chevy Chase
- 1 Boutique in London and 1 in Tokyo
- Clothes distributed in Bergdorf Goodman, Neiman Marcus, Nordstrom and Saks Fifth Avenue

SNIA
SNW
COMPUTERWORLD
April 12-15, 2010
Rosen Shingle Creek Resort
Orlando, Florida

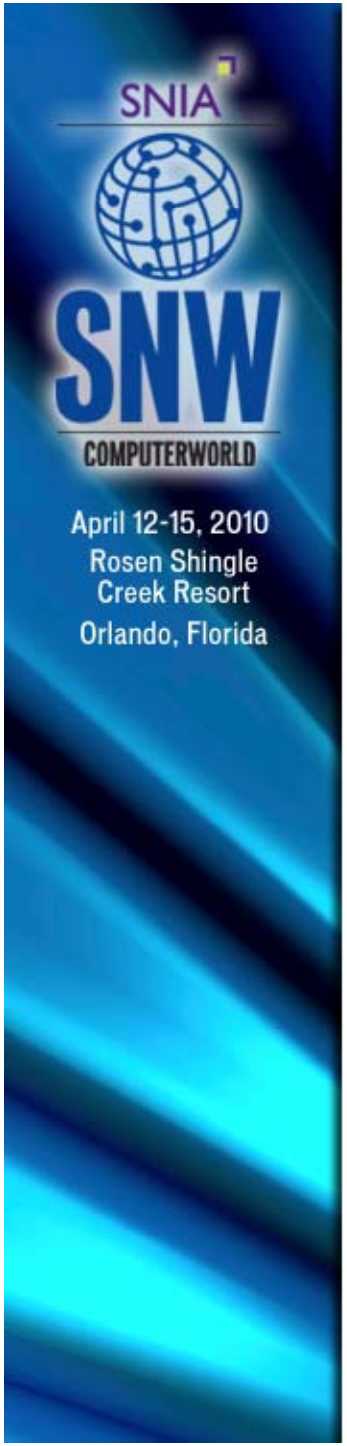
Security Threats Facing The Design Industry

- In 2007, Nanette Lepore was representative of what other designers were doing
  - Networks were wide open
  - Security was an afterthought
- Mostly worried about design theft, fraud and knock-offs
- Business was growing and additional investors were sought
- Needed to revamp network to grow business

2007 PCI Compliance was just starting

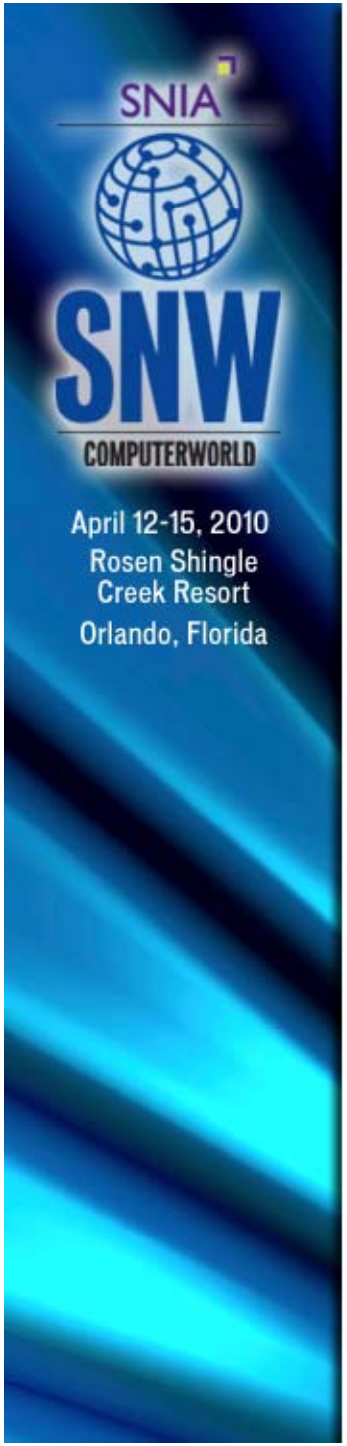
NANETTE LEPORE'S 2007 ATTACK

- Jose Cruz was hired to revamp network
- In 2007, Las Vegas store manager receives information from several customers about credit card charges originating in Italy and Spain
- Store manager contacts Jose, Las Vegas Police contacted
- FBI is contacted and takes all equipment for forensic review
- Las Vegas store closed on a Saturday
- All remote connections (VPN) to HQ closed



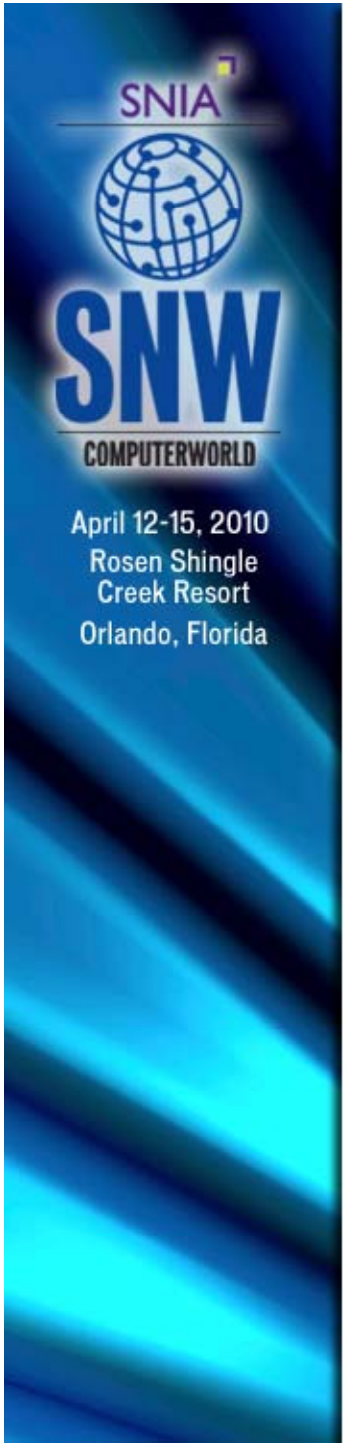
NANETTE LEPORE'S 2007 ATTACK

- Router identified to be controlled by ISP
- Router contained IP routes not part of ISP, but still worked
- Keyboard logger and screen captures made at 2-second intervals
  - FTPed screenshots to Georgia
  - Manufacturing in Italy
  - Sold to card distributor in Spain
  - Cards test at McDonald's in Spain and other minor purchases in Italy



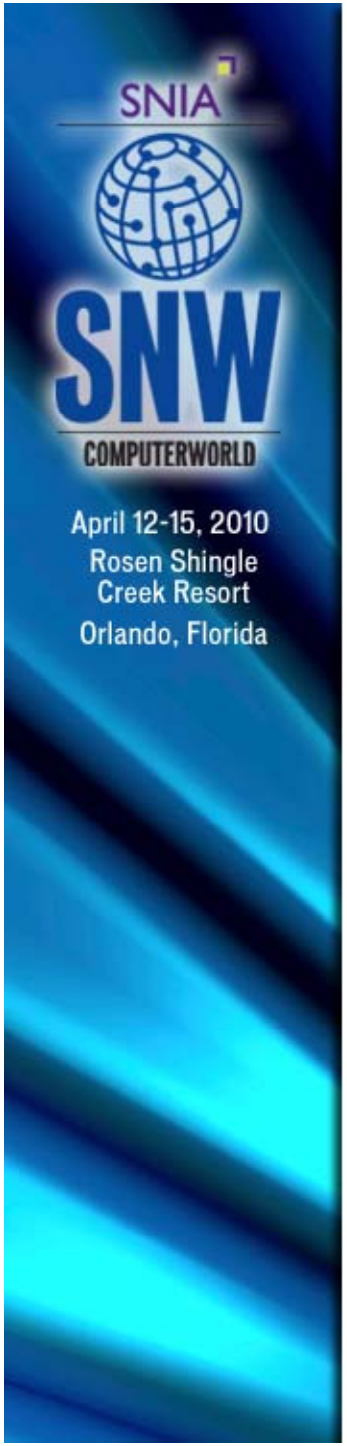
NANETTE LEPORE'S 2007 ATTACK (CONT…)

- Caught security breach early
  - Store manager has close relationship with customers
  - While 300 credit card numbers were stolen, only 2 cards confirmed as compromised
  - Called in L.V.P.D. computer crime lab to investigate, determined breach and FBI got involved
- Loss of $1M to $1.5M due to shutdown in Las Vegas
- Manually collected POS via remote desktop for 1 week for all stores



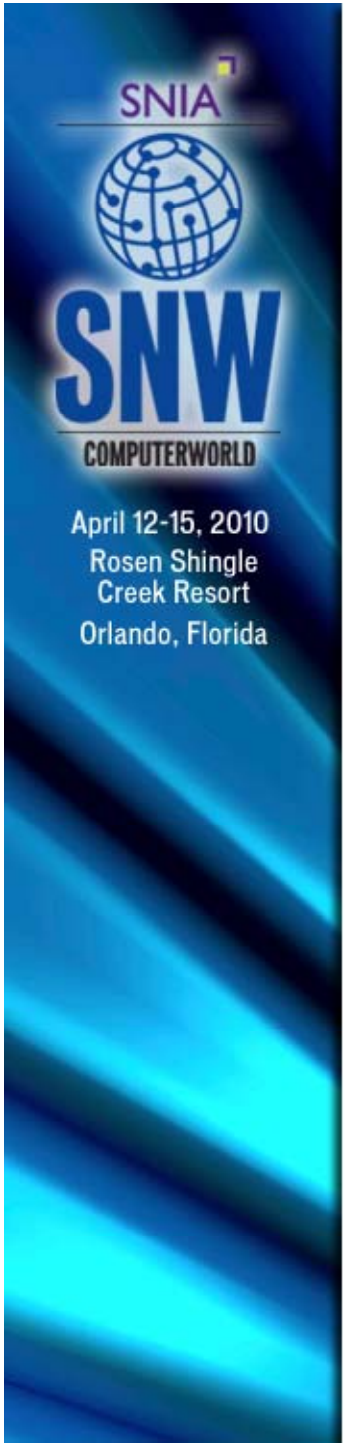
NANETTE LEPORE'S SECURITY INFRASTRUCTURE

- Nanette worked with FBI, PCI, and Webistix to revamp store
- Limited firewall vendors in 2007 doing PCI compliance testing
- Webistix recommends testing Sonicwall TZ180
- Two 3rd party auditing firms hired by PCI review and confirm PCI compliance
- Firewall configuration becomes template for all stores



NANETTE LEPORE'S SECURITY INFRASTRUCTURE

- Install new router, back office server
- POS system could not be replaced, but was cleaned
- Firewall installed
  - PCI requires separate subnet for credit card transaction, and only credit card transactions
  - Second subnet setup for backoffice server, POS, and manager use
  - Firewall must perform DPI, VPN, etc.
- FBI recommendations
  - Motion activated cameras with specific locations
  - Physical layout
- Las Vegas store reopened following Tuesday



NANETTE LEPORE'S SECURITY INFRASTRUCTURE

- Following the 2007 attack, the company recreated its security infrastructure as a distributed security network across the stores and its main warehouse, POS system, inventory management and business applications
- Designed its infrastructure to let employees securely and remotely access the retail database and inventory database from any device
  - Allows Mac, PowerBook, iPhone or Pocket PC on any platform into the system (Mac or PC)
  - All employees have locked-down end-point security
  - Security training explaining what and why

SNIA

SNW

COMPUTERWORLD

April 12-15, 2010
Rosen Shingle Creek Resort
Orlando, Florida

NANETTE LEPORE'S SECURITY INFRASTRUCTURE

- SonicWALL e-mail security gateway - blocks up to 20,000 e-mails/day
- SonicWALL 3060 and SSL VPN Gateway
- SonicWALL CDP for back-up and redundancy (hosted offsite and online for replication)
- Windows 2003 Active Directory
- Mac Open Directory server
- Oracle Systems
- Accounting Systems with Mos 500

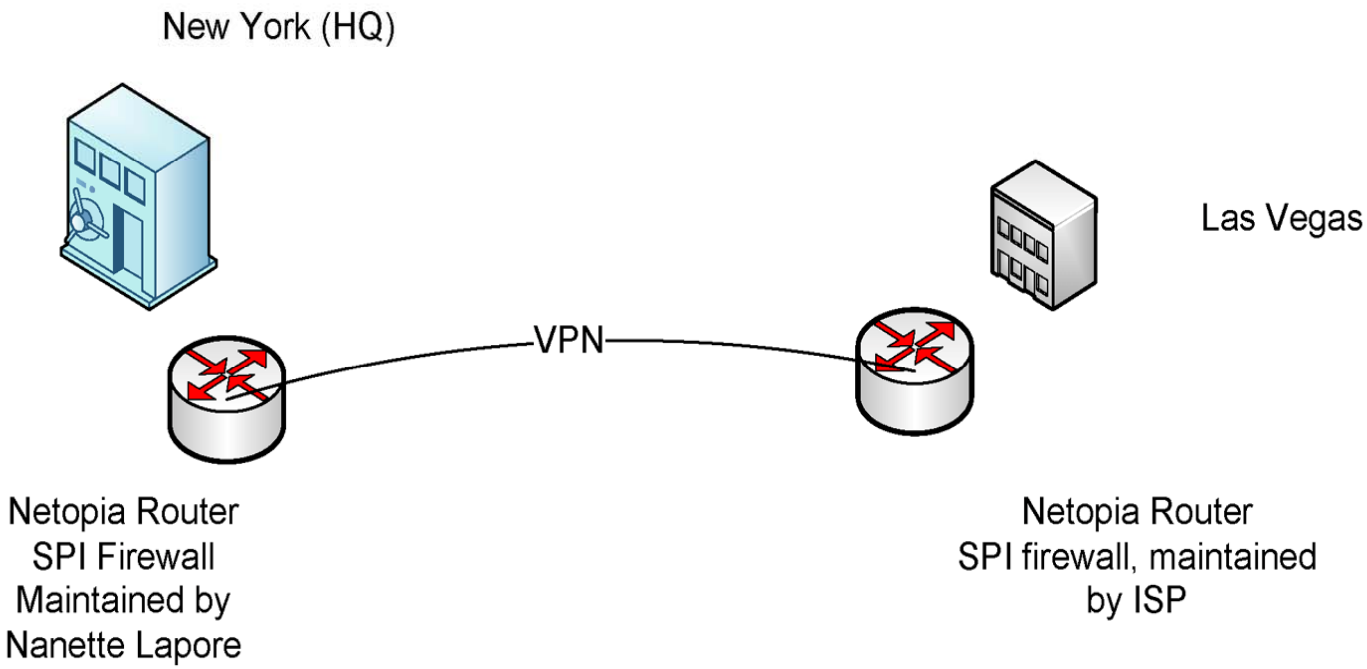
Amount of redundancy and fault tolerance sets industry standard

- TZ 170s for wireless networks
- Other gear includes: Cisco, Net Gear, Powerlink. All are handed off to SonicWALL security infrastructure
- For Bandwidth control, redudancy, fault tolerance and instant disaster recovery: trunked into a 100M wan aggregator, which allows multiple ISP sources (including T1 and Wi-Max) to trunk into 1 piece of equipment to 1 Ethernet to SonicWALL
- For mobile-centric environment: Exchange connectivity for iPhones

Infrastructure for Remote Locations

- For the showrooms
  - Use SonicWALL TZ180s for PCI compliance and security
  - SonicWALL GMS reports provide detail on potential intrusions
  - Keeps track of intrusions before they happen
  - Eyes in the sky
  - Automated monitoring and alerts
  - Employee knowledge first line of defense

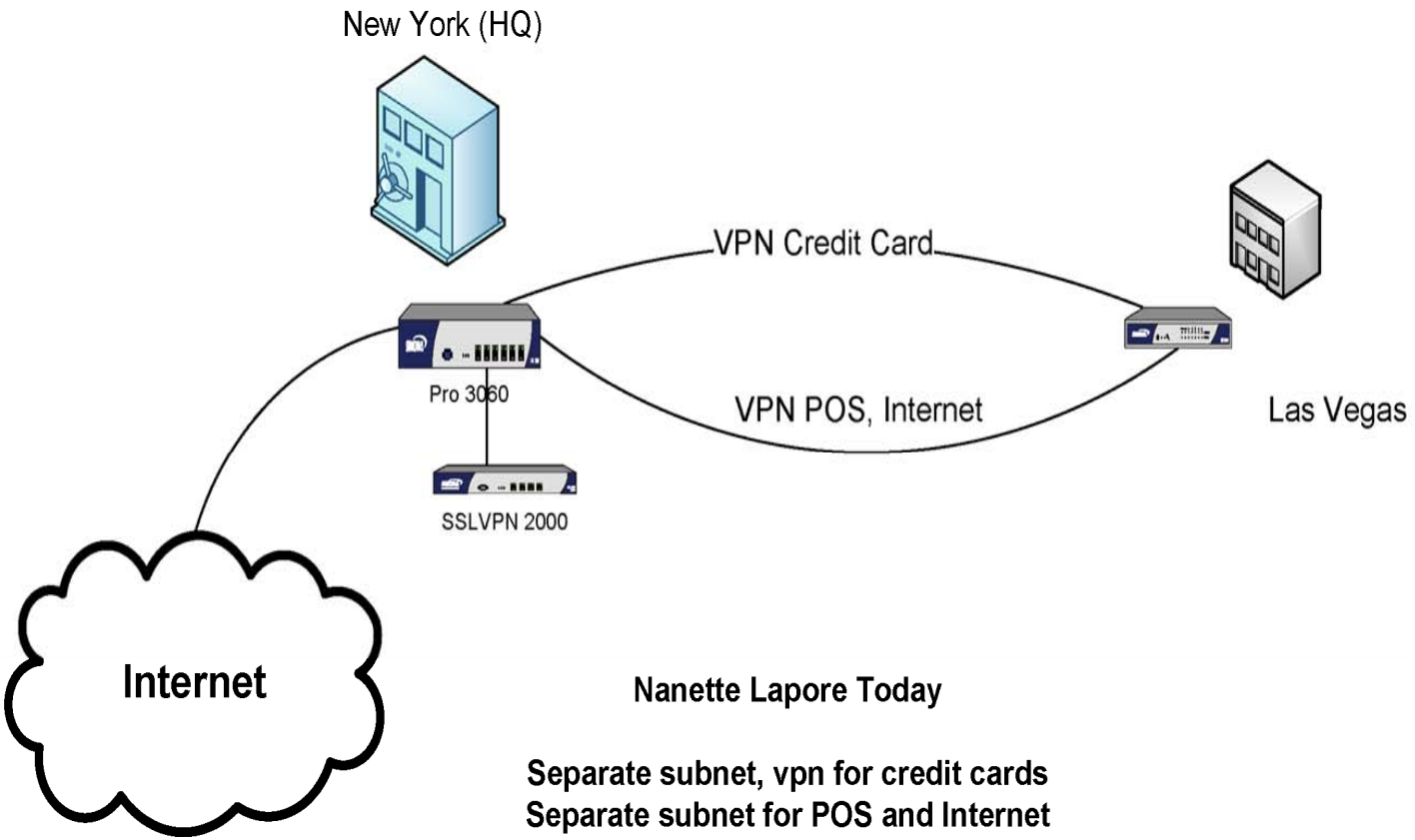
Before Installation: Nanette Lepore's Infrastructure



Nanette Lapore network during attack

All credit card, POS, and other traffic transported over one VPN back to New York HQ

After Installation: Nanette Lepore's infrastructure

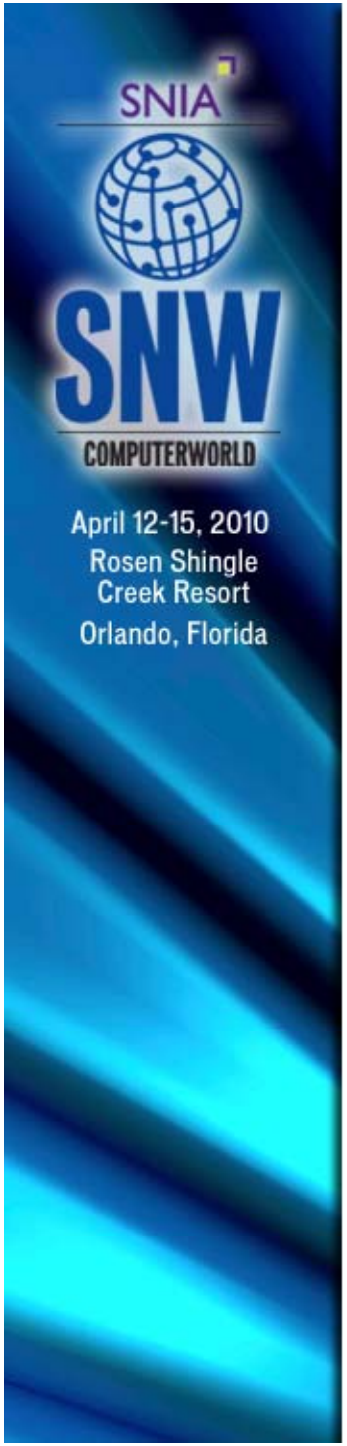


Nanette Lapore Today

Separate subnet, vpn for credit cards
Separate subnet for POS and Internet

2008 DDOS Attack

- In 2008, DDOS attack from China hit Nanette Lepore
  - Company e-mails delayed
  - Admin got kicked off the company's central server
  - Sales machines at the company's 8 boutiques were routinely getting bumped off-line when they tried to connect to the central server



Nanette Lepore Was Prepared

- Had installed redundant servers, with multiple links between stores, the company's central database, and the Internet
- Web hosting was offsite, its security software up to date, Powerlink WAN aggregator did its job and caught the intrusion and SonicWALL renegotiated its handoffs
- Issue with flip/flop
- ISP switched off the link that was being bombarded and established a secondary link for the stores to use
- Returned to normal 3 days later
- Good opportunity to review and enhance system

Lessons Learned

PCI compliance changed the way security infrastructure was managed

- **Employees each have log-ins**
- **Automatically logs out employees after Predetermined amount of time**
- **Gateway intrusions**
- **Password rotation, forced change every 45 days**

Lessons Learned (cont.)

- Deal with IT security needs first
  - Don't just opt for least expensive solution
  - Tried and tested equipment
  - In the cases of security threats, make decisions on how it affects the consumer
  - Catch it and work with the threat early on
- Acknowledge each employee has a role in the company
  - Training of policies
  - Understanding the 'why' behind them

Opting for the least expensive IT security solution can compromise a company's brand

SNIA

SNW

COMPUTERWORLD

April 12-15, 2010
Rosen Shingle Creek Resort
Orlando, Florida

TODAY'S REAL SECURITY THREAT: WEB 2.0 TOOLS

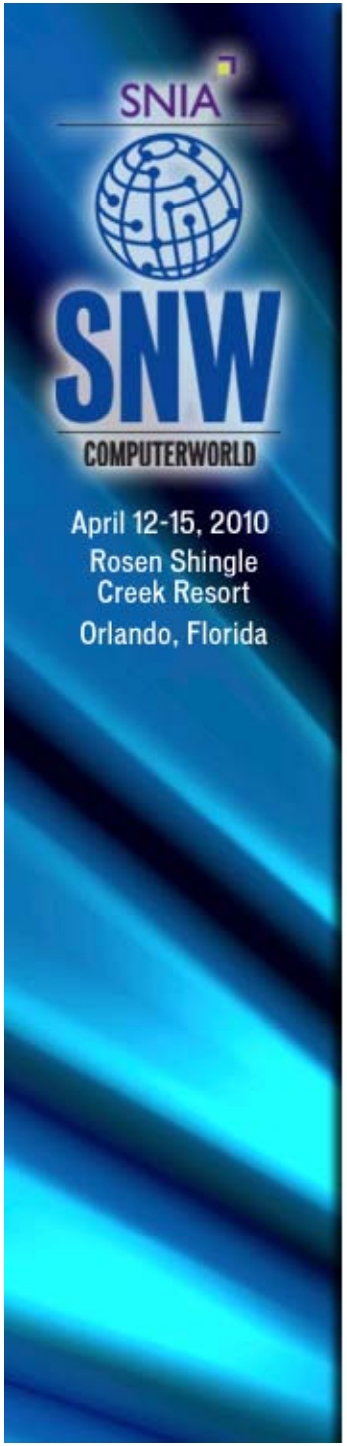
In brand creation, Web 2.0 tools are a necessity at Nanette Lepore

- At first, limited Twitter and social media tools up front
- Realized Nanette needs to be in tune with public, trends in the market
- Facebook, Twitter and MySpace used day to day to interact with fan base
- Use of proxies and isolated networks
- Difference between threats to Mac and PC

There will always be DDOS attacks and security breaches, but real threats come from Web 2.0 tools (Twitter, YouTube, Facebook)

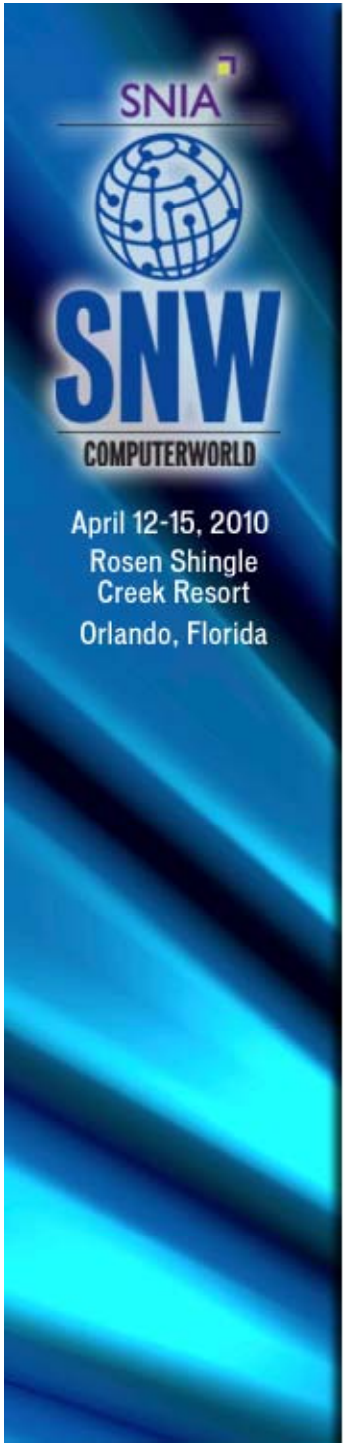
Best Practices for Balancing Network Performance & Web 2.0 Tools

- Authentication is key
  - Standardize desktops and implement mandatory log-ins
  - Integrate into Active Directory and Microsoft Directory
  - Implement policies for remote users
- Keep in mind Mac vs. PC
  - For support 1 admin:60 Macs; 1 admin: 20 Windows
  - Macs primarily handled by gateway
    - Not compromised on the desktop
    - Remote sites are Mac-based
  - Windows are entirely locked down
    - Accounting has access to Web 2.0 tools in their conference room



Best Practices for balancing Network Performance & Web 2.0 Tools (cont.)

- Don't just buy cheapest equipment
- Realize all resource available
  - Employees
  - Law enforcement (FBI, local)
  - Standard organizations (PCI)
  - Resellers
  - Manufactures
  - Non-profit security groups
    - Information Systems Security Association
    - Infragard
    - Information Systems Audit and Control Association
    - List of others at http://csrc.nist.gov/csrc/professional.html


SNIA
SNW
COMPUTERWORLD
April 12-15, 2010
Rosen Shingle
Creek Resort
Orlando, Florida

Questions?