

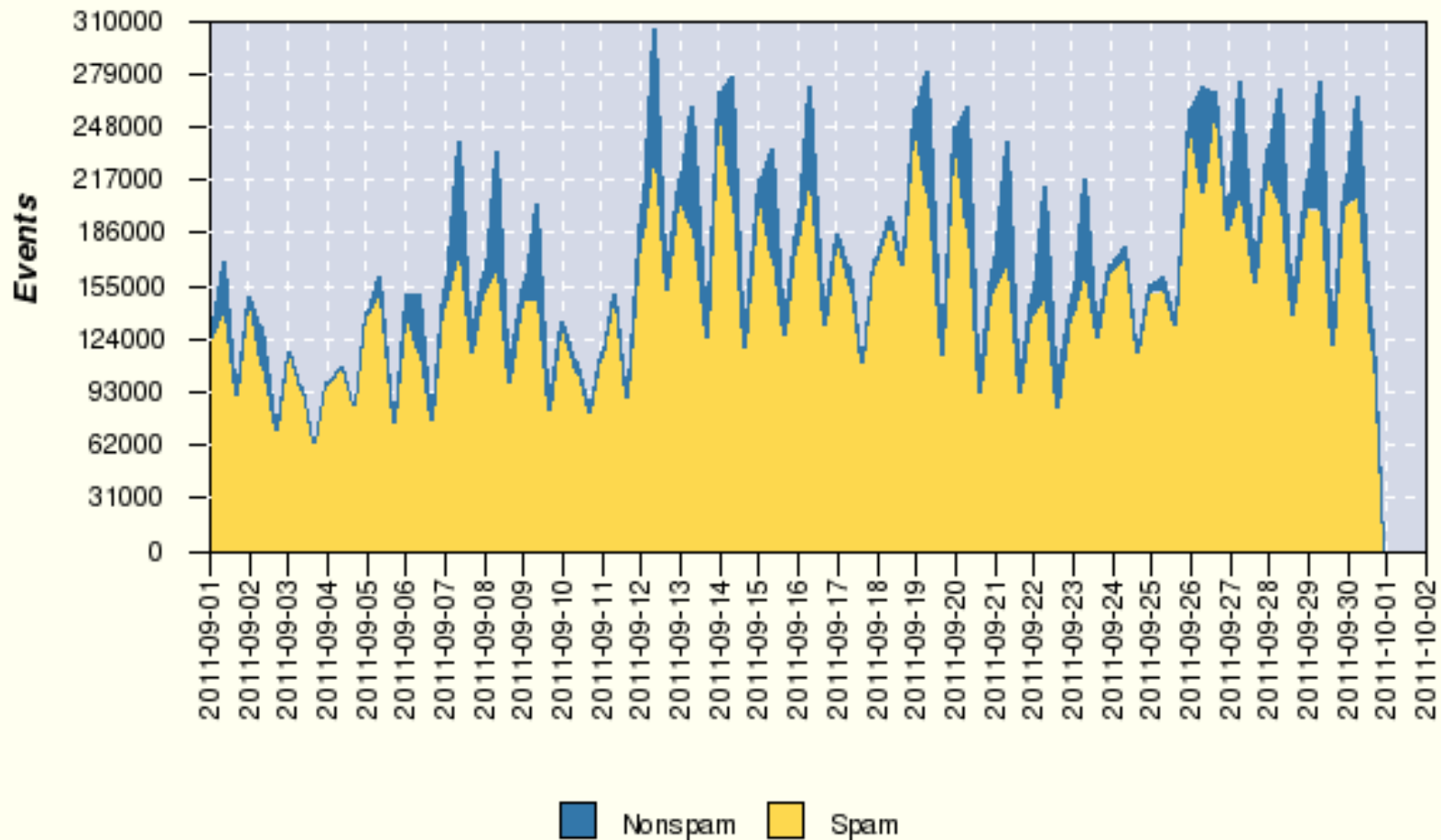


# Cyber Threat Briefing

Jeff Franklin, M.S., CISSP, CISM  
Chief Information Security Officer  
State of Iowa  
Dec. 15, 2011

# Cyber Threat: SPAM

*Total Spam and Non-Spam*



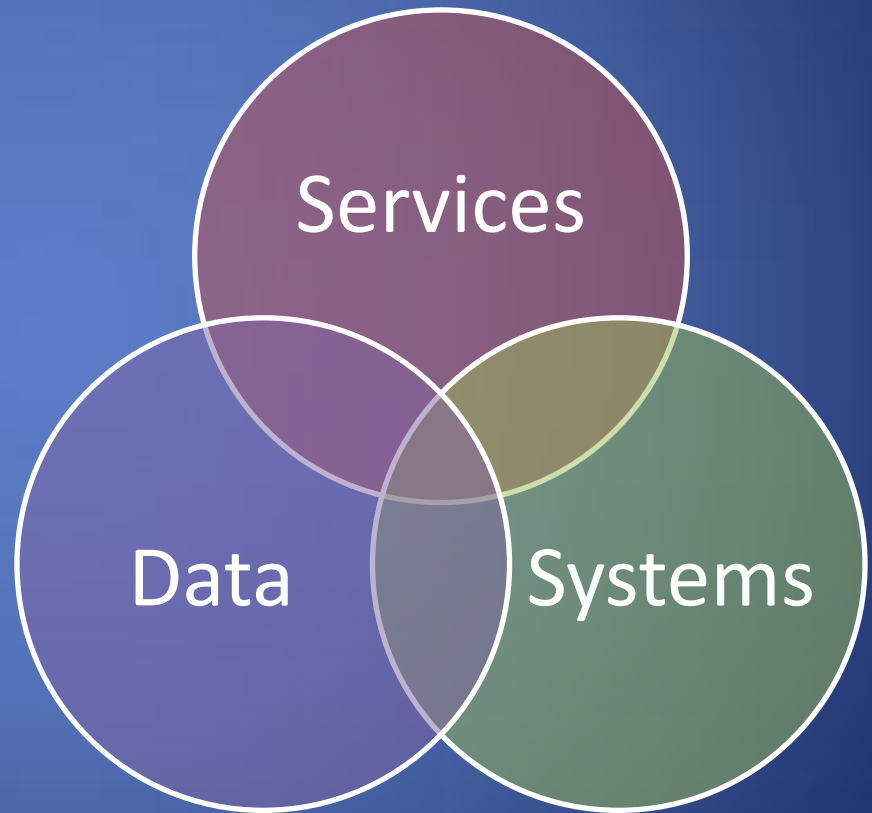
# State of Iowa – E-mail (Sept. 2011)



- 12,000 e-mail accounts
- 15,000,000 e-mails
  - 500,000 per day
  - 21,000 per hour
- 13,000,000 blocked
- 52,000 had malware
- 2<sup>nd</sup> Filter
  - 200,000 blocked
  - 3374 had malware

# What is a Cyber Threat?

- Anything that threatens the confidentiality, integrity and availability of your Data, and/or IT Systems. Disruption to these, disrupt business Services.



# Do Cyber Threats Matter?

- Operations – What IT systems do you rely on?
- Integrity – Does your data need to be accurate?
- Privacy – Are you collecting confidential data?
- Website – Does your public image matter?

# Which Critical Sectors depend on IT?



Agriculture and Food



Banking and Finance



Chemical



Commercial Facilities



Communications



Critical Manufacturing



Dams



Defense Industrial Base



Emergency Services



Energy



Government Facilities



Healthcare and Public Health



Information Technology



National Monuments and Icons



Nuclear Reactors, Materials and Waste



Postal and Shipping



Transportation Systems



Water

# Where is the threat coming from?

- Nation States
- Organized Crime
- Terrorist
- Professionals
- Amateurs



# Motives behind a cyber attack?

- Money
- Intellectual Property
- Intelligence gathering / Espionage
- Political Statements
- Thrills

# Cyber Threats: Attacks

- Persistent
- Targeted
- Stealthy



# Cyber Threat: Malicious Websites

- More than 1 million Web sites were believed to be infected with malware in the fourth quarter of last year, nearly double from the previous year,
- "The probability that an average Internet user will hit an infected page after three months of Web browsing is 95 percent,"

– Cnet March 8, 2011

# Identity Theft

- **Data breaches affect 2m in Mass**
  - “Personal information from nearly one out of three Massachusetts residents, has been compromised through data theft or loss since the beginning of 2010, of Attorney General Martha Coakley.”
    - September 21, 2011
- **4 times more likely to have your identity stolen if your data has been compromised**
  - 2009 Javelin Research & Strategy

# Data Breaches

- 2011 – 275 Data Breaches, 22.4 million records “reported”
- Since 2005 – 2707 Data Breaches, 540 Million records “reported”
- Unintended Disclosure, Hacking or Malware, Payment Card Fraud, Insider Threat, Portable Device, Stationary device

# Other Cyber Threats

- Applications – Custom and Commercial
- Out of date Browsers
- Unencrypted Smart Phones
- Social Engineering
- Weak / Shared/ Non-expiring passwords
- Poor patching practices
- Physical Security
- Many, many more

# What you should not do!

- Buying one “device” will not fix it
- Utilize the head in the sand model
- Believe that “we are too small for them to pay attention to us”
- Give up

# You do not have to be perfect !!

- Be more difficult to attack than the next guy !!
  - Criminals will typically take the path of least resistance and automation.
  - Do the fundamentals well
    - Most breaches are preventable with basic security practices and good processes
- You will most likely not stop APT so focus your time and money on the basics first and complex security solutions last

# How to fix it.

- \$0 expenditures (primarily personnel time)
  - Policy, procedures and enforcement
  - Complex passwords
  - Implement principle of least privilege
  - Consistent patching for systems and applications
  - Security awareness training
  - Up to date Anti Virus and other end point protections
  - Network segregation by vLan
  - Prioritize what to assets to protect
  - Focus efforts on what's most critical for your organization
  - Utilize risk assessment frameworks to get a holistic view

# How to fix it.

0 – \$1,000

- All the \$0 stuff +
  - Introduce open source solutions
  - Spam filtering
  - Web filtering
  - Encrypt mobile devices
  - Traffic monitoring
  - Proxy web services

# How to fix it.

\$1,000 – \$5,000

All the \$0 stuff +

- Web application firewall
- Continuous scanning solution
- Log file management

# How to fix it.

\$5,000 – \$25,000

All the \$0 stuff +

- Introduce commercial solutions
- Intrusion detection system
- Vulnerability assessment

# How to fix it.

\$25,000 – \$100,000

- All the \$0 stuff +
  - Introduce security consultants and vendors
  - Security personnel
  - Independent penetration test
  - Network architecture
  - Security policy review

# How to fix it.

\$100,000 – \$1,000,000

- All the 0 \$ stuff +
  - Possibly outsource some specialized security functions
  - Commercial Security Information Event Management system (SIEM)
  - Commercial Data Leakage Prevention (DLP)

# Partnerships & Information Sharing



**MULTI-STATE**

Information Sharing & Analysis Center



**Iowa Infragard**



**Homeland  
Security**

Questions ???

# Resources

Iowa Information Security

[secureonline.iowa.gov](https://secureonline.iowa.gov)

Security Awareness List

[join-security-news@lists.ia.gov](mailto:join-security-news@lists.ia.gov)

Security Alert list

[securityalert@iowa.gov](mailto:securityalert@iowa.gov)

Iowa Infragard

[iowainfragard.org](https://iowainfragard.org)

NIST (800 series)

[nist.gov](https://nist.gov)

US Cert

[us-cert.gov](https://us-cert.gov)

MS-ISAC

[msisac.org](https://msisac.org)

# Thank you

Jeff Franklin

[jeff.franklin@iowa.gov](mailto:jeff.franklin@iowa.gov)

515-281-4820

State of Iowa Information  
Security Office

[secureonline.iowa.gov](http://secureonline.iowa.gov)

