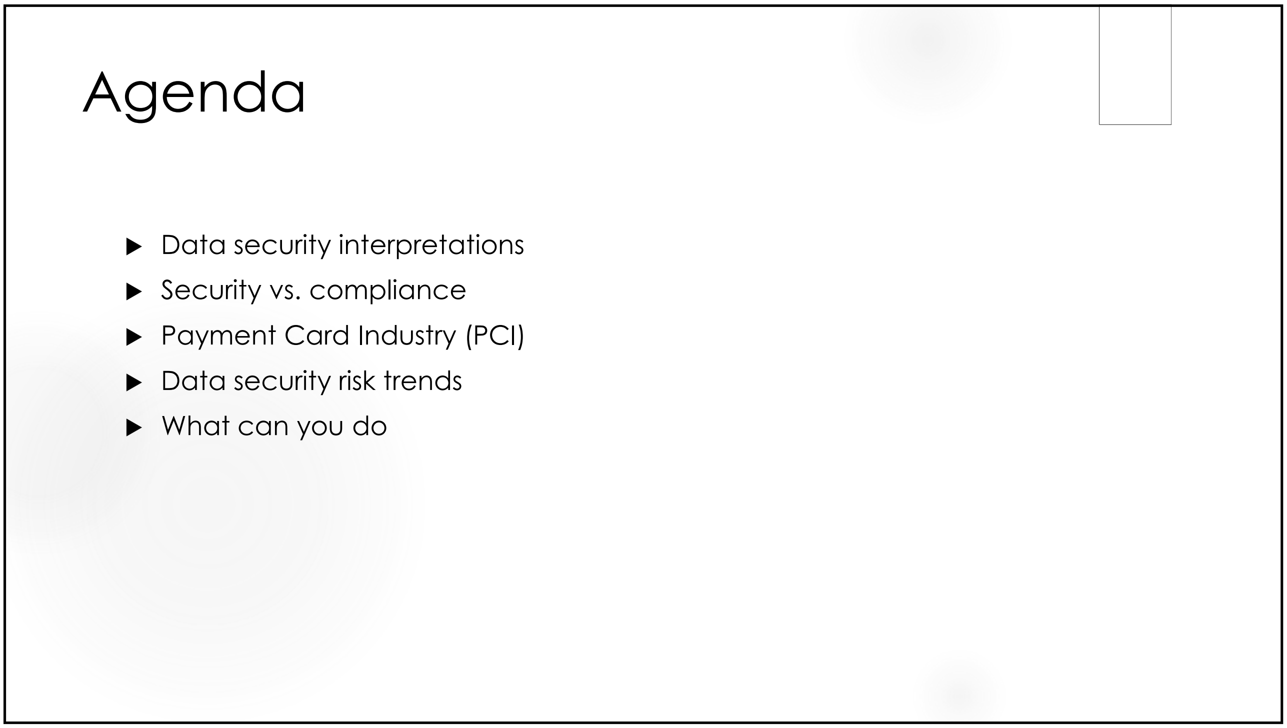
Payment Card Compliance and Challenges

MICHELLE GREELEY

SOCIETY OF CORPORATE COMPLIANCE AND ETHICS MEETING

MARCH 11, 2016



Agenda

- Data security interpretations
- Security vs. compliance
- Payment Card Industry (PCI)
- Data security risk trends
- What can you do

Does data security sound like this to you?

Triple DES Security Insurance ISO Risk Malware

File Transfer Protocol Zero Day Defense in Depth Ease dropping

TLS Data Mining Firewall Switch Botnet Assessment Tunnel Penetration Testing

Ping Access Controls Threat URL Defacement Segment Phishing

Trojan Horse

Investigation Vulnerability Identity Encryption Cyber Honey Pot

Internet Protocol Compliance Disaster Scan

VPN Governance Worm Root Patch

Chain of Custody Biometrics Cache User Log

Spoofing SQL Injection

Password Cracking Policies Malicious Code Network Spam Incident Synchronization

HTTPS Backdoor PPTP Demilitarized Zone

Standards Data Third Parties

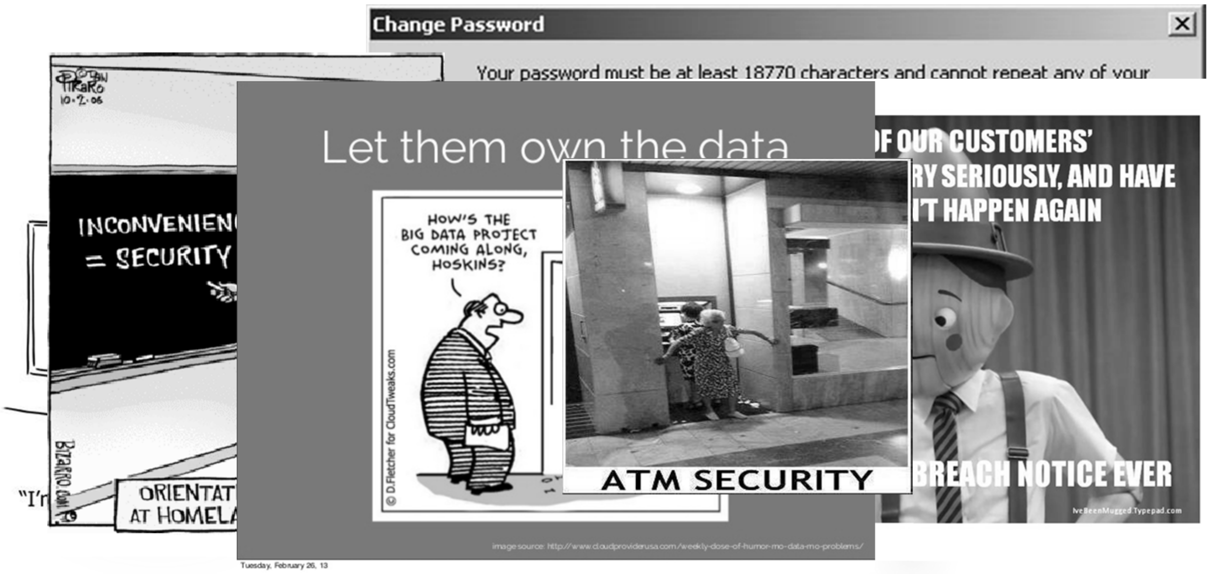
Router Virus Cryptography Brute Force Continuity

Egress Point TCP/IP

Kernel Registry War Dialing SSL Gateway

PKI Secure Socket OSI Layers Data Custodian

Or does data security feel like this?



Change Password

Your password must be at least 18770 characters and cannot repeat any of your

Let them own the data

image source: http://www.cloudproviderusa.com/weekly-dose-of-humor-mo-data-mo-problems/

Tuesday, February 26, 13

How about like this?*

Worlds biggest data breaches

*informationisbeautiful.net

Finally, does data security sound like this to you?

HITRUST

CSA STAR

Certified Penetration Testing Consultant

Certified Ethical Hacker

Internal Security Assessor

Certified Expert Penetration Tester

Sarbanes Oxley

Safe Harbor

National Institute of Standards and Technology (NIST)

Gramm-Leach Bliley

Standards for Attestation Engagements (SSAE 16) Service Organization Controls (SOC)

Certified Security Testing Associate

Payment Card Industry (PCI)

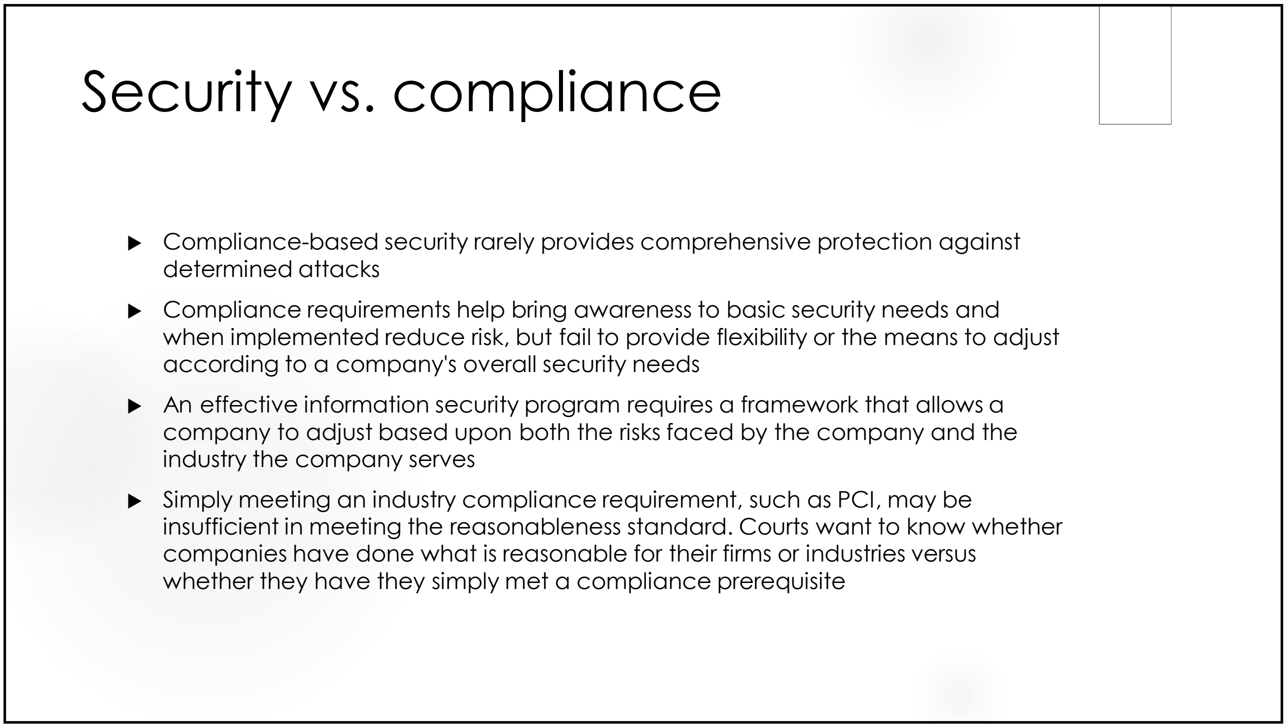
HIPAA

Qualified Security Assessor

Certified Penetration Testing Engineer

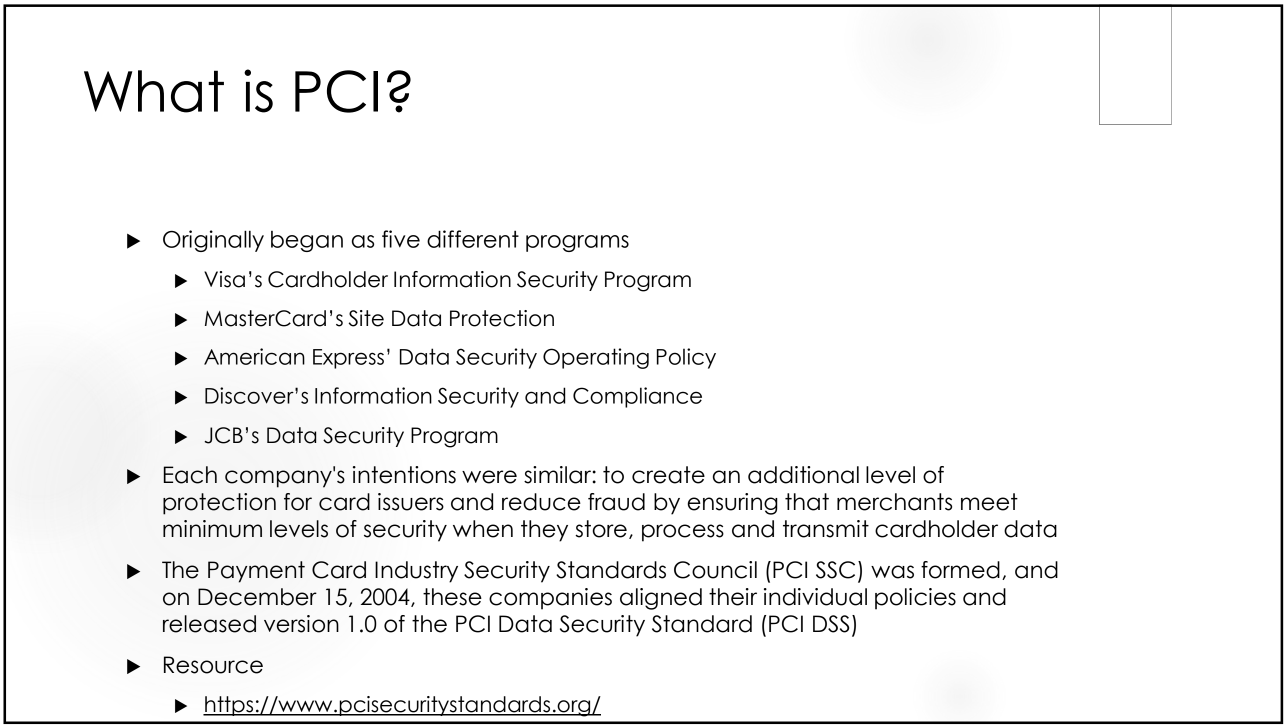
EC-Council Certified Security Analyst

International Organization for Standardization (ISO)



Security vs. compliance

- Compliance-based security rarely provides comprehensive protection against determined attacks
- Compliance requirements help bring awareness to basic security needs and when implemented reduce risk, but fail to provide flexibility or the means to adjust according to a company's overall security needs
- An effective information security program requires a framework that allows a company to adjust based upon both the risks faced by the company and the industry the company serves
- Simply meeting an industry compliance requirement, such as PCI, may be insufficient in meeting the reasonableness standard. Courts want to know whether companies have done what is reasonable for their firms or industries versus whether they have they simply met a compliance prerequisite

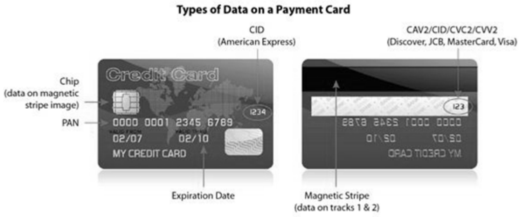


What is PCI?

- Originally began as five different programs
  - Visa's Cardholder Information Security Program
  - MasterCard's Site Data Protection
  - American Express' Data Security Operating Policy
  - Discover's Information Security and Compliance
  - JCB's Data Security Program
- Each company's intentions were similar: to create an additional level of protection for card issuers and reduce fraud by ensuring that merchants meet minimum levels of security when they store, process and transmit cardholder data
- The Payment Card Industry Security Standards Council (PCI SSC) was formed, and on December 15, 2004, these companies aligned their individual policies and released version 1.0 of the PCI Data Security Standard (PCI DSS)
- Resource
  - https://www.pcisecuritystandards.org/

PCI standards and cardholder data

- Six standards
  - PCI DSS – Data Security Standard
  - PCI PA-DSS – Payment Application Data Security Standard
  - PCI P2PE - Point-to-Point Encryption
  - PCI PTS - PIN Transaction Security
  - PCI Card Production
  - PCI TSP – Token Service Providers
- Cardholder data includes
  - Primary Account Number (PAN)
  - Cardholder Name
  - Security Code (CID/CAV2/CVC2/CVV2)
  - Expiration Date



PCI DSS

- PCI DSS is a collection of 12 security requirements with over 240 sub-requirements applicable to entities who store, process and/or transmit cardholder data
  - Regardless of business size or quantity of payment cards accepted
  - Business processes, IT processes, facilities, service providers and systems

Control Objective	PCI DSS Requirement
Build and maintain a secure network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	3. Protect stored data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement strong access control measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an information security policy	12. Maintain a policy that addresses information security for all personnel

PCI DSS compliance challenges

- Executive commitment - PCI compliance is a business objective, not just a security objective
- Investment in certified Internal Security Assessors (ISA) and external Qualified Security Assessors (QSA)
- Knowing and routinely documenting your scope – data flows, assets, physical locations, system interfaces, service providers and processes
- Creating and maintaining a knowledge base for critical decisions
- Maintaining compliance after achieving compliance – it’s a lifestyle, not just a project or a point in time
- Obtaining BAU budget for ongoing compliance costs – remediation and testing
- Technology limitations and resource capacity
- Staying current with PCI DSS versions and interpretation changes from the PCI SSC

Current data security risk trends*

Cybercrime

Organizations must be prepared for the unpredictable so they have the resilience to withstand unforeseen, high impact events

Privacy and Regulation

Organizations need to treat privacy as both a compliance and business risk issue, in order to reduce regulatory sanctions and business costs such as reputational damage and loss of customers due to privacy breaches. The patchwork nature of regulation around the world is likely to become an increasing burden on organizations in 2015

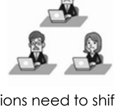
Threats From Third-Party Providers

Third-party providers will continue to come under pressure from targeted attacks and are unlikely to be able to provide assurance of data confidentiality, integrity and/or availability. Organizations need to think about the consequences of a supplier providing accidental, but harmful, access to their intellectual property, customer or employee information, commercial plans or negotiations

BYOx Trends in the Workplace

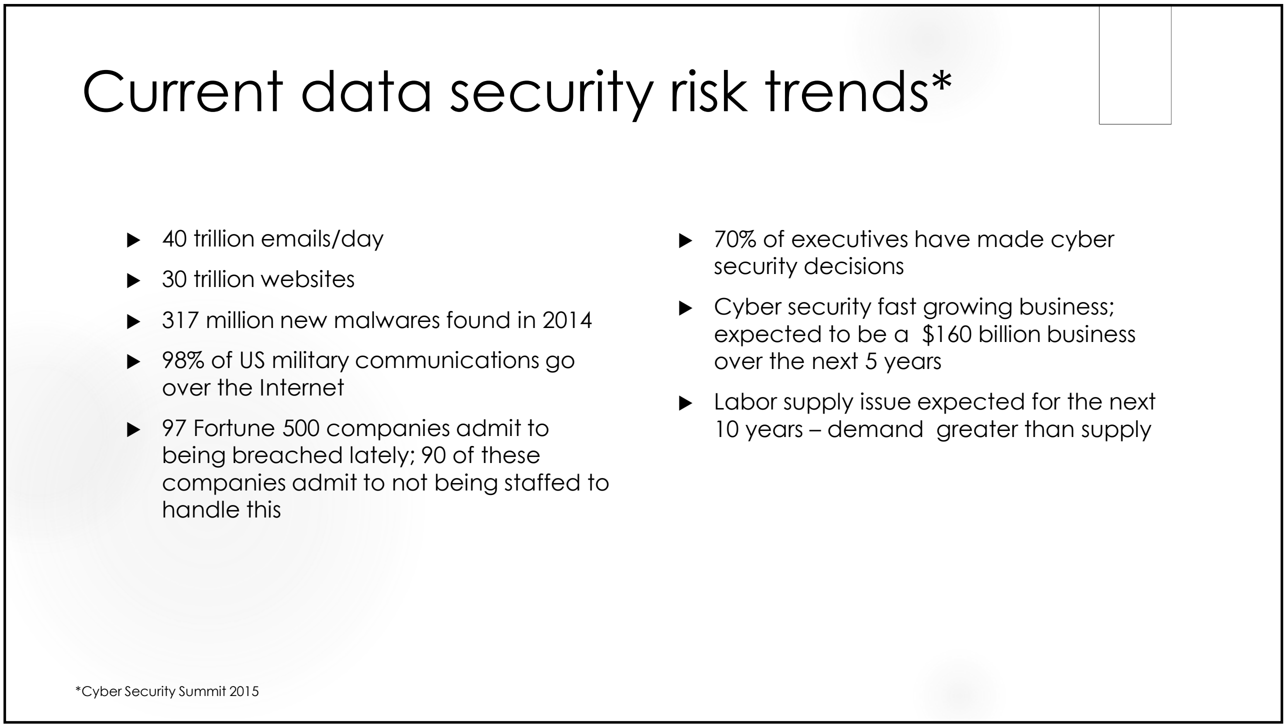
As the trend of employees bringing mobile devices, applications and cloud-based storage and access in the workplace continues to grow, businesses are seeing information security risks being exploited at a greater rate than ever before. These risks stem from both internal and external threats including mismanagement of the device itself, external manipulation of software vulnerabilities and the deployment of poorly tested, unreliable business applications

Engagement With Your People



Organizations need to shift from promoting awareness of the problem to creating solutions and embedding information security behaviors that affect risk positively. Many organizations recognize people as their biggest asset, yet many still fail to recognize the need to secure 'the human element' of information security. In essence, people should be an organization's strongest control. Embed positive information security behaviors that will result in 'stop and think' behavior becoming a habit and part of an organization's information security culture

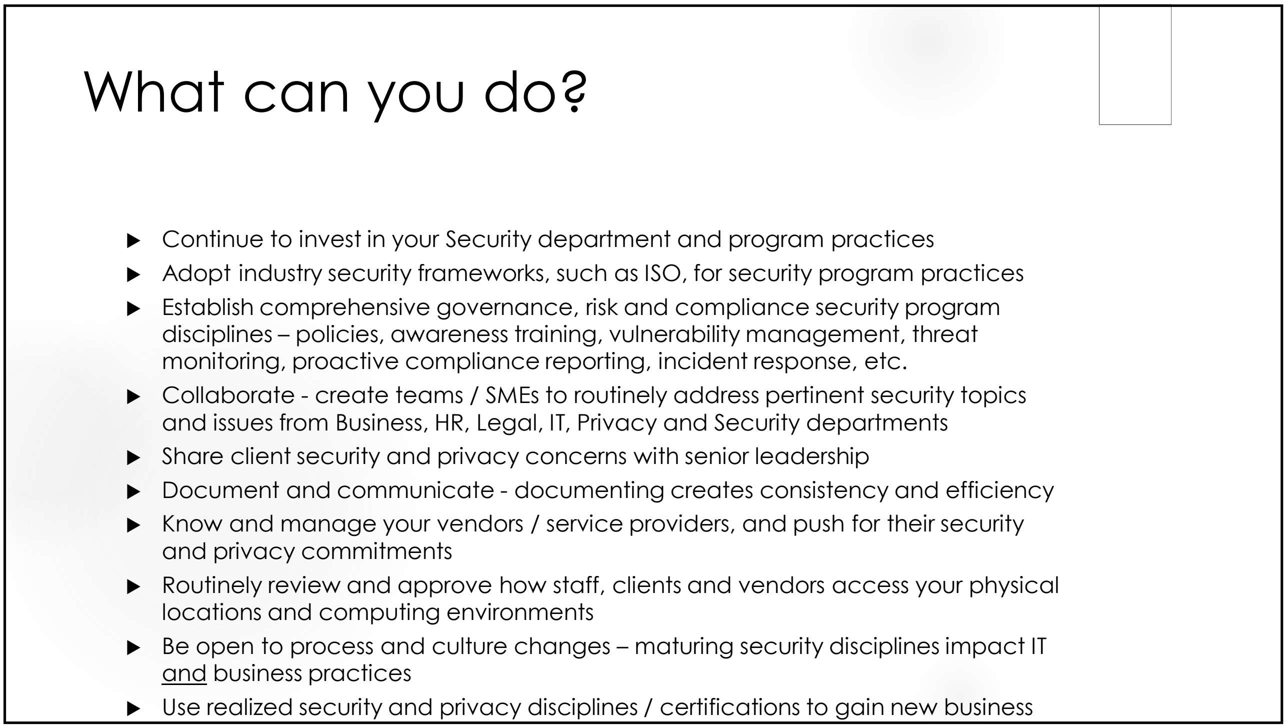
*CIO.com



Current data security risk trends*

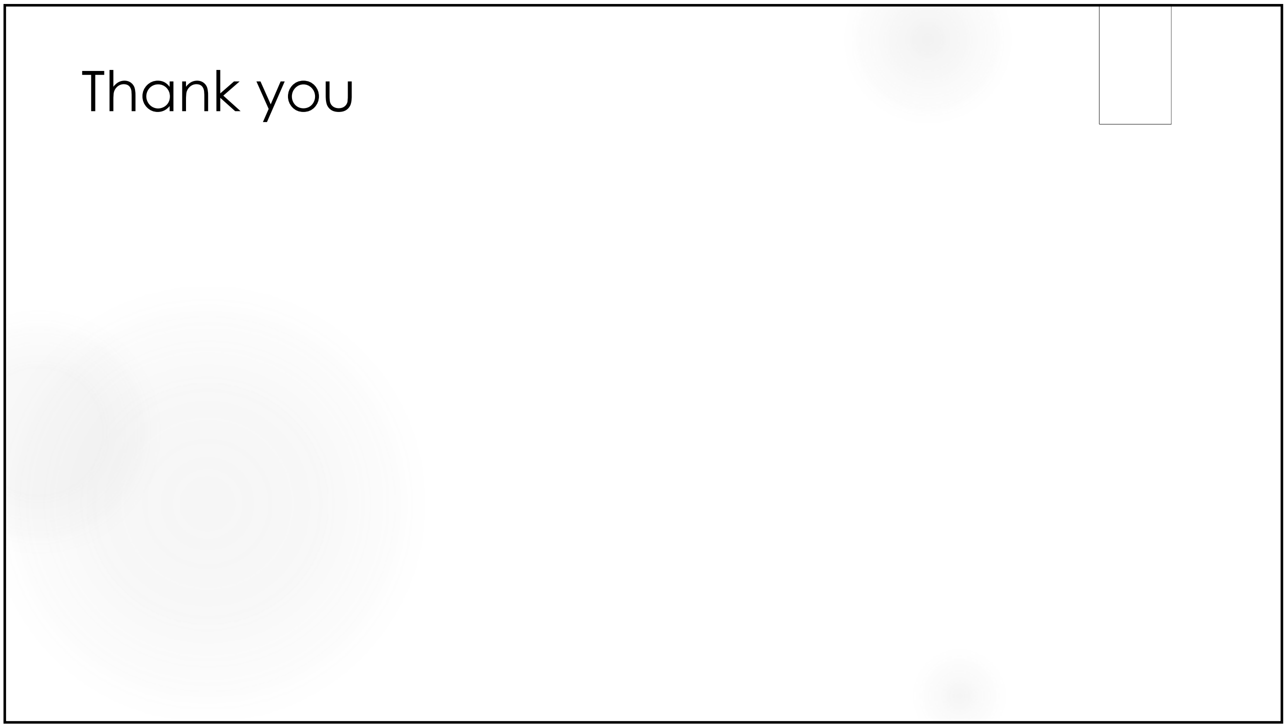
- 40 trillion emails/day
- 30 trillion websites
- 317 million new malwares found in 2014
- 98% of US military communications go over the Internet
- 97 Fortune 500 companies admit to being breached lately; 90 of these companies admit to not being staffed to handle this
- 70% of executives have made cyber security decisions
- Cyber security fast growing business; expected to be a $160 billion business over the next 5 years
- Labor supply issue expected for the next 10 years – demand greater than supply

*Cyber Security Summit 2015



What can you do?

- Continue to invest in your Security department and program practices
- Adopt industry security frameworks, such as ISO, for security program practices
- Establish comprehensive governance, risk and compliance security program disciplines – policies, awareness training, vulnerability management, threat monitoring, proactive compliance reporting, incident response, etc.
- Collaborate - create teams / SMEs to routinely address pertinent security topics and issues from Business, HR, Legal, IT, Privacy and Security departments
- Share client security and privacy concerns with senior leadership
- Document and communicate - documenting creates consistency and efficiency
- Know and manage your vendors / service providers, and push for their security and privacy commitments
- Routinely review and approve how staff, clients and vendors access your physical locations and computing environments
- Be open to process and culture changes – maturing security disciplines impact IT and business practices
- Use realized security and privacy disciplines / certifications to gain new business



Thank you