The 25th National HIPAA Summit

Special Fall Edition

Sep. 14 - 16, 2016 • Washington, DC

A Hybrid Conference and Internet Event

GHC HEALTH CARE
Global Health Care, LLC

Establishing a Credible Cybersecurity Program

September 2016

Ali Pabrai, MSEE, CISSP (ISSAP, ISSMP)
Member FBI InfraGard

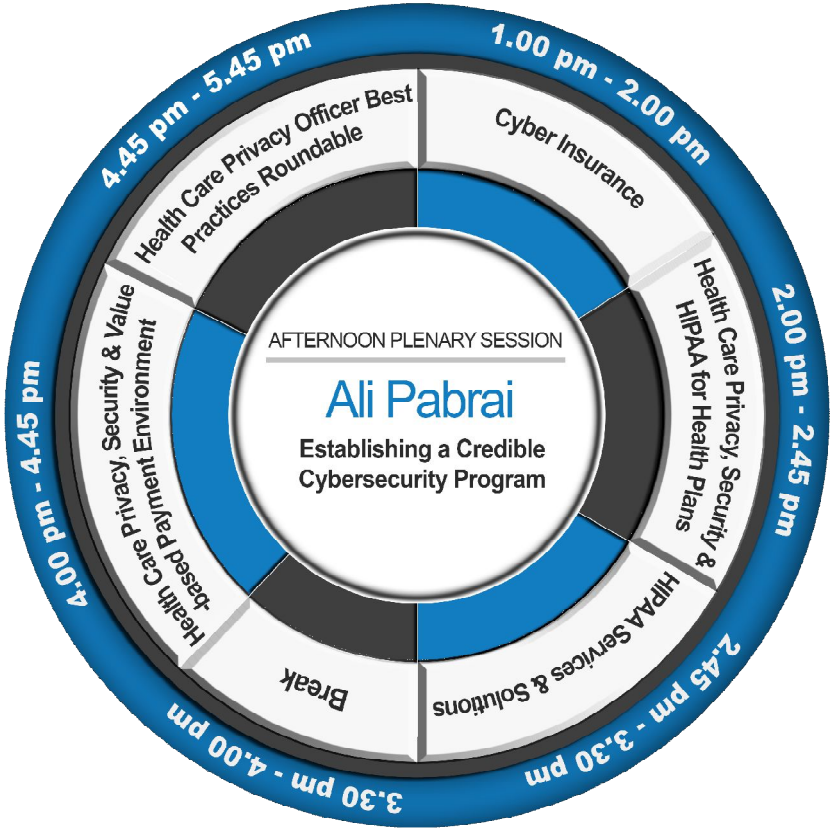
ecfirst

AFTERNOON PLENARY SESSION

The 25th National HIPAA Summit
Special Fall Edition
Sep. 14 - 16, 2016 • Washington, DC

A Hybrid Conference and Internet Event

GHC HEALTH CARE
Global Health Care, LLC



ecfirst

AGENDA

- **Cyber Risk = *Disruptive* Business Risk**
  - Breaches: banks, retailers, healthcare
  - Cyber attack lifecycle
- **Risk Assessment**
- **Standards**
- **Preparation**
- *Assessing* **Controls**
  - Firewalls to Encryption
  - Vulnerability Assessments & Pen Tests
- *Establishing* an **Enterprise Cyber Security Plan**
- **December 31, 2016**

The Risk!

kely Sources of Cyber Attack

#	Required Activities	STATUS		Your Response?
		Yes	No	
1.	Criminal syndicates, 59%.	☐	☐	
2.	Employee, 56%	☐	☐	
3.	Hactivists, 54%	☐	☐	
4.	Lone-wolf hacker, 43%	☐	☐	
5.	External contractor, 36%	☐	☐	
6.	State-sponsored attacker, 35%	☐	☐	

gh Security Priority in 2016!

#	Required Activities	STATUS		Your Response?
		Yes	No	
1.	Data leakage/Data loss prevention, 56%	☐	☐	
2.	Business continuity/Disaster recovery, 55%	☐	☐	
3.	Identity & access management, 47%	☐	☐	
4.	Security awareness & training, 44%	☐	☐	
5.	Incident response capabilities, 44%	☐	☐	
6.	Security operations (e.g. encryption, patching), 41%	☐	☐	

Challenges to Information Security Operations

#	Required Activities	STATUS		Your Response?
		Yes	No	
1.	Budget constraints, 62%	☐	☐	
2.	Lack of skilled resources, 57%	☐	☐	
3.	Lack of executive awareness or support, 32%	☐	☐	
4.	Lack of quality tools for managing information security, 28%	☐	☐	
5.	Management & governance issues, 28%	☐	☐	
6.	Compliance/regulation issues, 23%	☐	☐	

CYBER ATTACKS: GLOBAL & SOPHISTICATED

Iran Cyber Attacks

- Used common SQL injection, spear phishing & other attacks to gain initial access
- Next, used privilege escalation exploits to compromise additional systems & move deeper inside the compromised firm

Sony

- Used highly sophisticated malware to carry out the attack

Chase

- Hackers compromised flaw in bank web-site
- Hackers reached deep into enterprise infrastructure
- Gigabytes of customer account & other data siphoned slowly
- Attack routed through several countries, including Brazil, & then re-directed to Russia

How robust is your patch management?

RESULTS OF A RECENT CYBER ASSESSMENT!

THREAT	IMPACT
Remote Code Execution	Complete Control of the System
Unsecured PII	Breach
System configuration issues	Loss of Data
Buffer Overflow Vulnerability	Denial of Service Attack or Complete Control of the System

RANSOMWARE CYBER ATTACKS

The 25th National HIPAA Summit
Special Fall Edition
Sep. 14 - 16, 2016 • Washington, DC
A Hybrid Conference and Internet Event

GHC HEALTH CARE
Global Health Care, LLC

Methodist Hospital

Incident was a result of Malicious email opened, Methodist immediately shut down its systems to control spreading.

Ottawa Hospital

Computer network was hit, four of 9,800 machines. The malware locked down the files & Ottawa responded by wiping the drives.

Hollywood Presbyterian Medical Center

The malware locks systems at Hollywood hospital by encrypting files and demanding ransom to obtain the decryption key and hospital paid extortionists a $17,000 bitcoin ransom to unlock its data, which was maliciously encrypted.

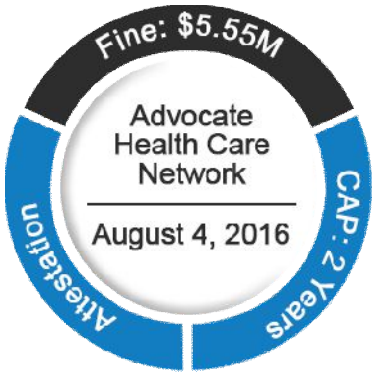
CVMC & PVH

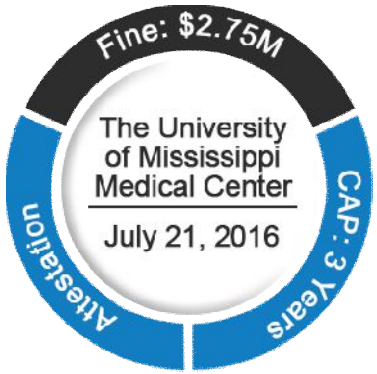
The hackers got into one of the hospital's computers and then spread a malware program that encrypts the data on computers and then demanded a ransom to unlock the servers.

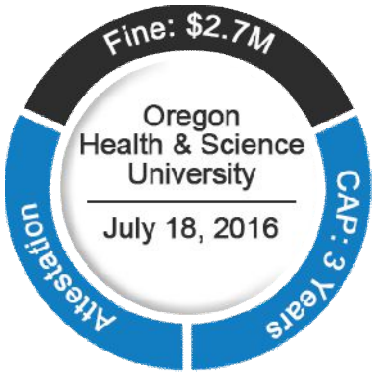
Prepare

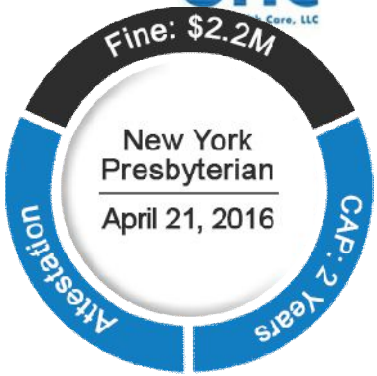
ecfirst

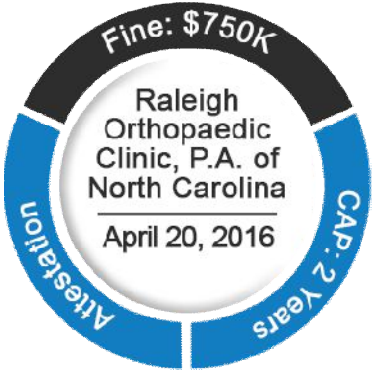
HIPAA FINES 2016

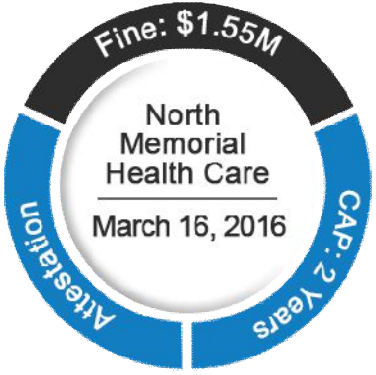












COST OF BREACHES:
EIGHT FIGURE RISK!

St. Joseph Health

Over $25M Settlement

TARGET

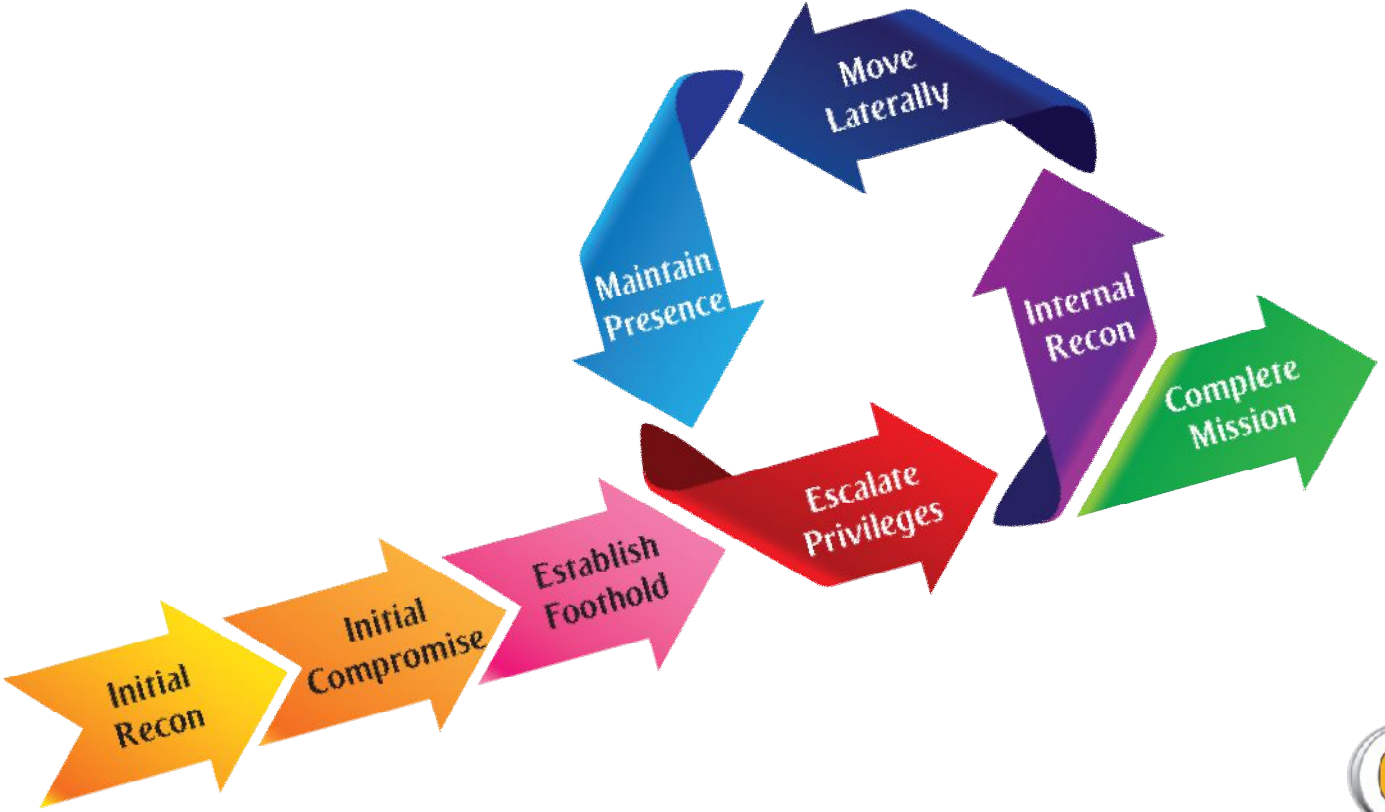
Over $130M Settlement

---

at&t

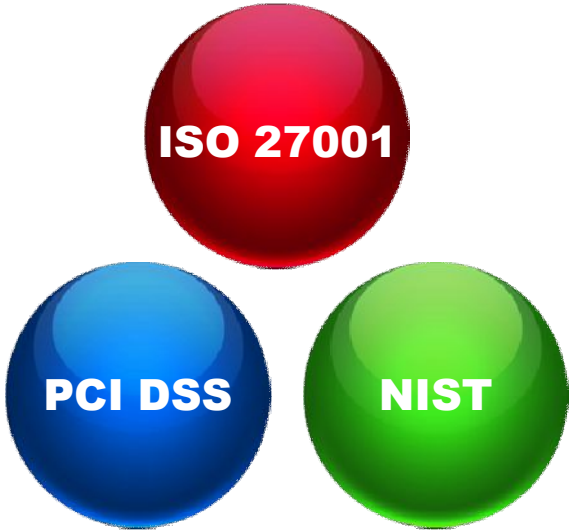
$25M Settlement

CYBER ATTACK LIFECYCLE



Standards

COMPLIANCE MANDATES



HITRUST
Authorized CSF Assessor

ecfirst

ISO 27001:
A GLOBAL STANDARD

GHC HEALTH CARE
Global Health Care, LLC

ISO 27002: 2013
Information Security Policies
Organization of Information Security
Human Resource Security
Asset Management
Access Control
Cryptography
Physical & Environmental Security
Operations Security
Communications Security
System Acquisition, Development & Maintenance
Supplier Relationships
Information Security Incident Management
Information Security Aspects of Business Continuity Management
Compliance

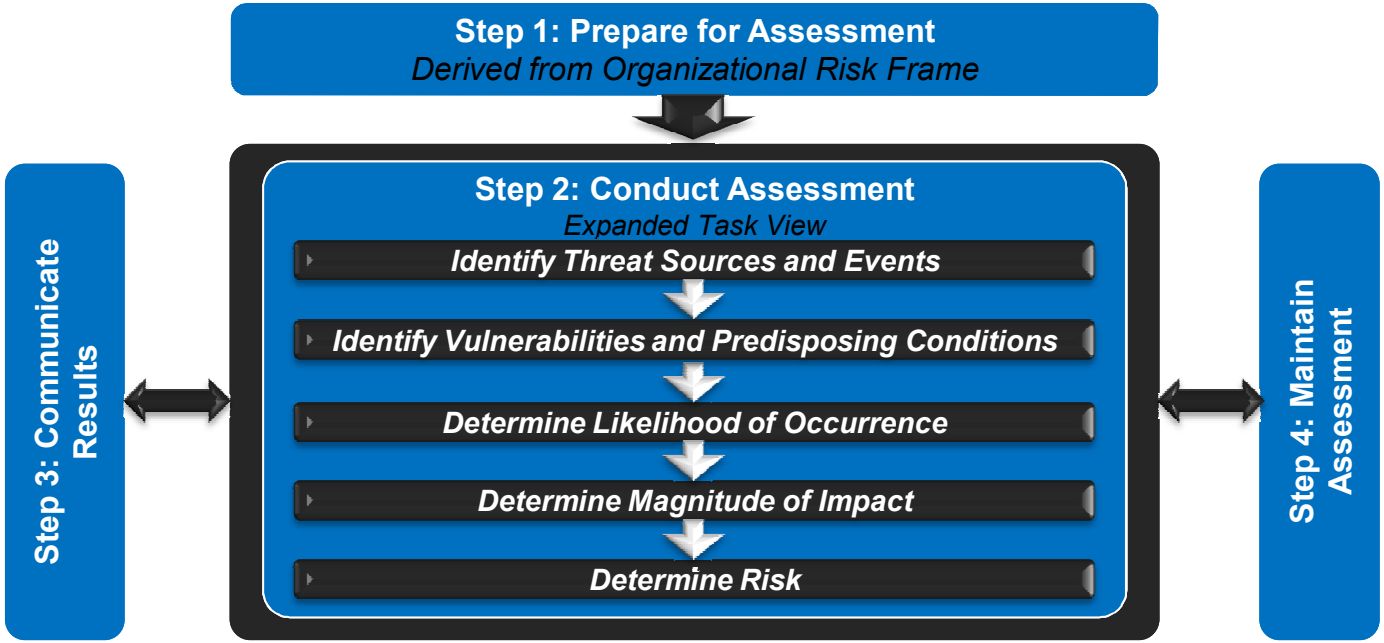
ecfirst

PCI DSS: IMPORTANT REFERENCE

PCI DSS Requirements	Testing Procedures
12.1 Establish, publish, maintain, and disseminate a security policy that accomplishes the following:	**12.1** Examine the information security policy and verify that the policy is published and disseminated to all relevant personnel (including vendors and business partners).
12.1.1 Addresses all PCI DSS requirements.	**12.1.1** Verify that the policy addresses all PCI DSS requirements.
12.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment. (Examples of risk assessment methodologies include but are not limited to OCTAVE, ISO 27005 & NIST SP 800-30).	**12.2.a** Verify that an annual risk assessment process is documented that identifies threats, vulnerabilities, and results in a formal risk assessment.

NIST & RISK ASSESSMENT

NIST SP 800-30 REV 1: RISK ASSESSMENT



RISK ASSESSMENT PROCESS

Closing Thoughts

ASSESSING ENCRYPTION!

AREA	STATUS		Comments
	YES	NO	
Database Servers	☐	☐	
PII/PHI on Cloud Systems	☐	☐	
Backup Media	☐	☐	
Desktops	☐	☐	
Laptops	☐	☐	
Tablets	☐	☐	
Smart Phones	☐	☐	
USB Devices	☐	☐	
Email	☐	☐	
Text Messages	☐	☐	
Remote Access	☐	☐	
Wireless	☐	☐	
Transmission	☐	☐	

CREDIBLE
RISK ASSESSMENT?

The 25th National HIPAA Summit
Special Fall Edition
Sep. 14 - 16, 2016 • Washington, DC
A Hybrid Conference and Internet Event

GHC HEALTH CARE
Global Health Care, LLC

1. Conduct a VA
2. Validate & Remediate Findings
3. Pen Test

ecfirst

SECURITY CONTROLS & COMPLIANCE

The 25th National HIPAA Summit
Special Fall Edition
Sep. 14 - 16, 2016 • Washington, DC
A Hybrid Conference and Internet Event

GHC HEALTH CARE
Global Health Care, LLC

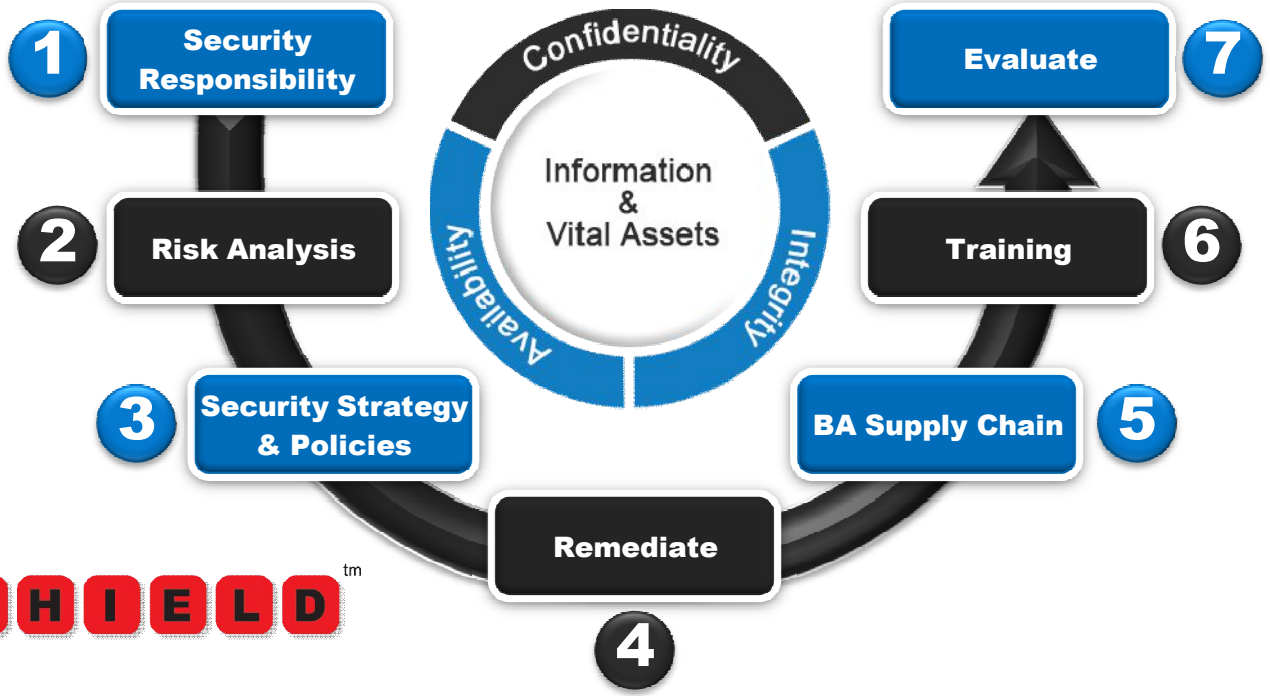
Key Security Controls	
Implemented	**Missing**
Firewall *(Sonic Firewall TZ210)*	Two-factor authentication
IDS *(Dell SecureWorks)*	DLP
Antivirus protection *(Webroot)*	Secure text messaging
Data transfer *(SFTP, HTTPS)*	USB & portable device encryption
Remote access *(VPN, Citrix)*	MDM
Asset management *(Dell KACE)*	
Laptop encryption *(TrueCrypt at the Bios Level; Windows OS & File Vault on Mac OS)*	
Email encryption *(Voltage)*	

ecfirst

AN ANNUAL CHECKLIST

The 25th National HIPAA Summit
Special Fall Edition
Sep. 14 - 16, 2016 • Washington, DC
A Hybrid Conference and Internet Event
GHC HEALTH CARE
Global Health Care, LLC

The Seven Steps to Enterprise Security™



bizSHIELD™

ecfirst

ENTERPRISE CYBER SECURITY PLAN

The 25th National HIPAA Summit
Special Fall Edition
Sep. 14 - 16, 2016 • Washington, DC
A Hybrid Conference and Internet Event

GHC HEALTH CARE
Global Health Care, LLC

Sample Topics

Key Facts
- Compliance Mandates to Meet Priorities
- Security Priorities in 2016
- Compliance Priorities in 2016
- Current Security Controls
- Security Control Deficiencies
- Security Control Priorities in 2016

Risk Analysis – Scope & Timeline
- Vulnerability Assessment – Scope & Timeline
- Penetration Testing

Documentation
- Security Policies – Summary
- Privacy Policies – Summary
- Security Procedures – Summary

Contingency Plan
- Business Impact Analysis (BIA) in 2016
- Disaster Recovery Plan (DRP)

Incident Response Plan
- Breach Discovery & Reporting Tools

Audit Controls
- Log Automation & Consolidation Tools

ecfirst

December 31,

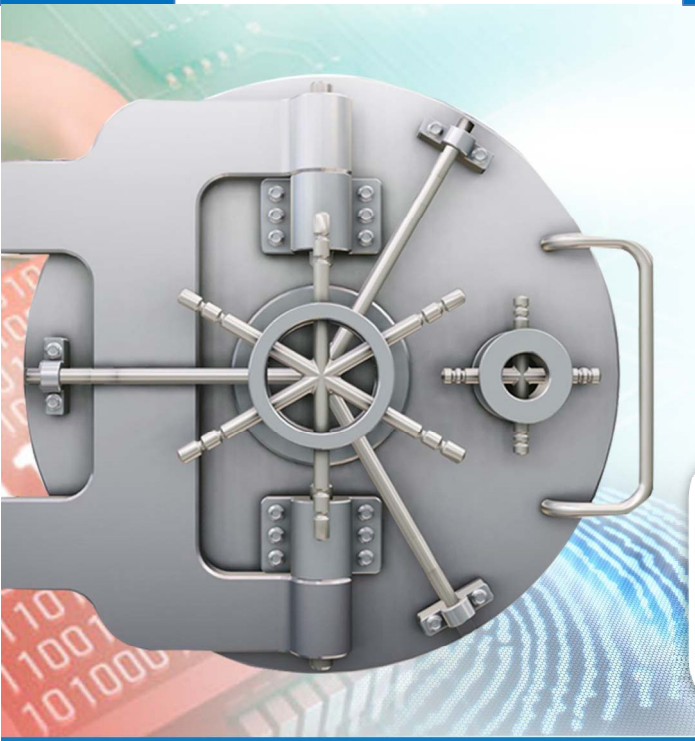
What is the state of your enterprise security & compliance?

Establish a *credible* cybersecurity program!

ecfirst

ecfirst

Compliance & Cyber Secu



TRAINING
Certification

Training & Certification
CHA • CHP • CSCS • CCSA

Managed Compliance
Managed Security

Security Risk Assessment
HIPAA • PCI DSS • ISO 27000 • NIST

On-Demand Consulting
Flexible • Flat Rate • Fixed Cost

HITRUST
Authorized CSF Assessor

PCI Security Standards Council
QUALIFIED SECURITY ASSESSOR

Delivering Everything Compliance. Everything Security.

1000s of Clients | Clients in all 50 States | Clients on 5 Continents

CSCS™ CERTIFIED SECURITY COMPLIANCE SPECIALIST

Certified Security Compliance Specialist™

From this compliance & security training program you will:

- Examine HITECH & the HIPAA Security Rule, including Final Rule updates
- Learn about FISMA, NERC CSS, & GLBA
- Step through the core requirements of PCI DSS
- Analyse ISO 27001, ISO 27002, ISO 27799
- Examine California's SB 1386, SB 541, AB 1950, AB 1298, AB 211 & other U.S. State information security related regulations
- Walk thru NIST security standards

San Diego, CA | Sep 22-23

Las Vegas, NV | Dec 8-9

Program Delivered as a Private Class Anywhere, Worldwide!

The 25th National HIPAA Summit
Special Fall Edition
Sep. 14 - 16, 2016 • Washington, DC
A Hybrid Conference and Internet Event

CCSA℠ Certified Cyber Security Architect

Certified Cyber Security Architect℠

An Executive Cyber Security Program

- First executive training program designed to enable development of a cyber security program in the class.
- The CCSA℠ training validates knowledge and skill sets in cyber security with particular focus and emphasis on the development of an applicable cyber security incident response and an enterprise cyber security program.

Las Vegas | Dec. 10, 2016

Orlando, FL | Feb. 24, 2017

Program Delivered as a Private Class Anywhere, Worldwide!

About Your Presenter

The 25th National HIPAA Summit
Special Fall Edition
Sep. 14 - 16, 2016 • Washington, DC
A Hybrid Conference and Internet Event

GHC HEALTH CARE
Global Health Care, LLC

Ali Pabrai, MSEE, CISSP (ISSAP, ISSMP)

Information Security & Compliance Expert

- Consults extensively with technology firms, government agencies and business associates
- Created *biz*SHIELD^{tm} – a Signature Methodology - to address compliance & information security priorities
- Featured speaker at InfoSec conferences worldwide
- Presented at Microsoft, Kaiser, Intuit, E&Y, Federal & State Government agencies & many others
- Established the HIPAA Academy & CSCS Programs – gold standard for cyber security & compliance solutions
- Interim CISO for large health system with 35+ locations across the USA
- Member InfraGard (FBI)
- www.facebook.com/ecfirst & www.facebook.com/Pabrai.

+1.949.528.5224 |

ecfirst