The 27th National HIPAA Summit

HIPAA Mandates

Active Cyber Defense

ecfirst | Perfecting the Art of *Active* Cyber Defense

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

Agenda!

The 27th National HIPAA Summit

- Cyber Risk to Business
- Cyber Incident Response Readiness
- Checklist & Standards
- Getting Started: Cybersecurity Program

ecfirst | Perfecting the Art of *Active* Cyber Defense

The 27th National HIPAA Summit

Cyber Risk to Business

ecfirst Perfecting the Art of *Active* Cyber Defense

Cyber Risk to Business Today!

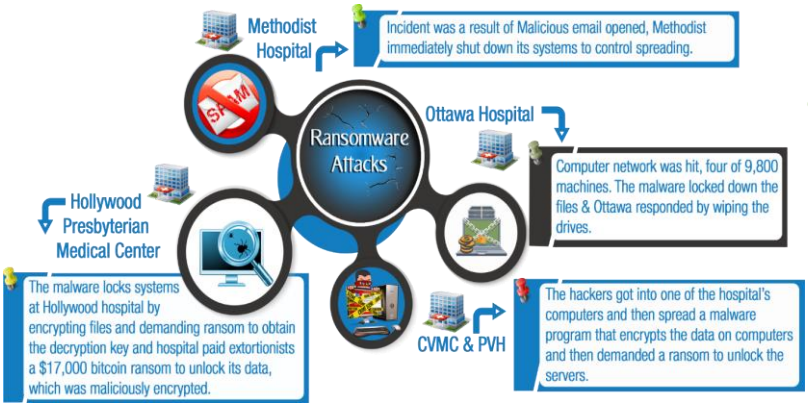
The 27th National HIPAA Summit

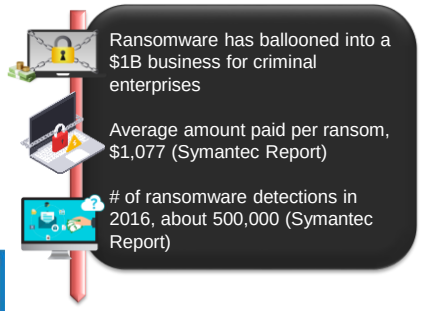
- **34%** of organizations lost revenue due to attacks in past year
- **50%** of organizations use 10 or more security products
- **30%** of organizations lost customers or business opportunities due to attacks
- **30%** of organizations use pen testing or network forensics
- **27%** stated that lack of trained security professionals is a major obstacle to adopting advanced security processes and technology
- **49%** of firms suffered at least one cyber ransom incident
- **82%** of privileged users log in from just one to two IP addresses/month
  - *Activity outside these should be detected and investigated*
- **60%** of privileged users never log out of active sessions

ecfirst Perfecting the Art of *Active* Cyber Defense

Ransomware Cyber-attacks

The 27th National HIPAA Summit





Prepared

ecfirst Perfecting the Art of *Active* Cyber Defense

IoT + DDoS = *Disruption*!

The 27th National HIPAA Summit

- Average of 414,985 DDoS incidents/month
- DDoS attack speeds ~ 1Tbps

84% of large businesses have experienced at least one DDoS attack in past 12 months (WSJ)

DDoS attacks cost firms $2.5 M or more in lost revenue (WSJ)

ecfirst Perfecting the Art of *Active* Cyber Defense

Cyber Attacks: Global & Sophisticated

The 27th National HIPAA Summit

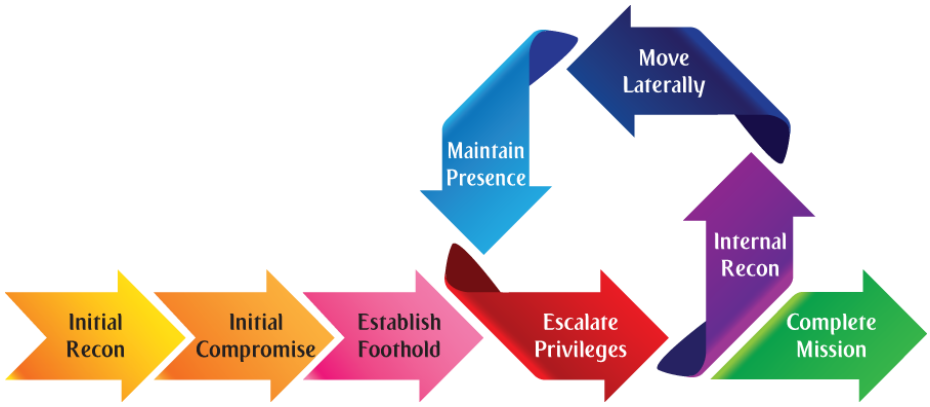
- Use common SQL injection, spear phishing & sophisticated malware to gain initial access
- Next, used privilege escalation exploits to compromise additional systems & move deeper inside the compromised firm

- **How robust is your patch management?**
- **Perform annual comprehensive risk assessments?**
- **Conduct quarterly vulnerability assessments?**
- **Completed a Business Impact Analysis (BIA)?**

ecfirst Perfecting the Art of *Active* Cyber Defense

Bottom Line: Cyber Attack Lifecycle

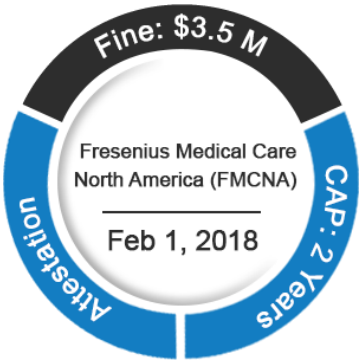
The 27th National HIPAA Summit



ecfirst Perfecting the Art of *Active* Cyber Defense

HIPAA Fines

The 27th National HIPAA Summit



Multiple breaches. Lack of risk analysis.

- ❑ Failed to conduct an accurate and thorough risk analysis to the CIA of ePHI.
- ❑ Impermissibly disclosed the ePHI of patients by providing unauthorized access for a purpose not permitted by the Privacy Rule.
- ❑ Failed to implement policies and procedures to address security incidents & to safeguard their facilities and equipment.
- ❑ Failed to implement encryption.

ecfirst Perfecting the Art of *Active* Cyber Defense

Cost of Breaches: Nine Figure Risk!

The 27th National HIPAA Summit

St. Joseph Health

Over $25 M Settlement

Anthem BlueCross BlueShield

Anthem

$115 M

ecfirst Perfecting the Art of *Active* Cyber Defense

Cybersecurity Challenge

The 27th National HIPAA Summit

CYBERSECURITY IS IN CRITICAL CONDITION

Severe Lack of Security Talent
The majority of health delivery orgs lack full-time, qualified security personnel

Legacy Equipment
Equipment is running an old, unsupported, and vulnerable operating systems

Premature/Over-Connectivity
'Meaningful Use' requirements drove hyper-connectivity without secure design & implementation

Vulnerabilities Impact Patient care
One security compromise shut down patient care at Hollywood Presbyterian and UK Hospitals

Known Vulnerabilities Epidemic
One legacy, medical technology had over 1400 vulnerabilities

ecfirst Perfecting the Art of *Active* Cyber Defense

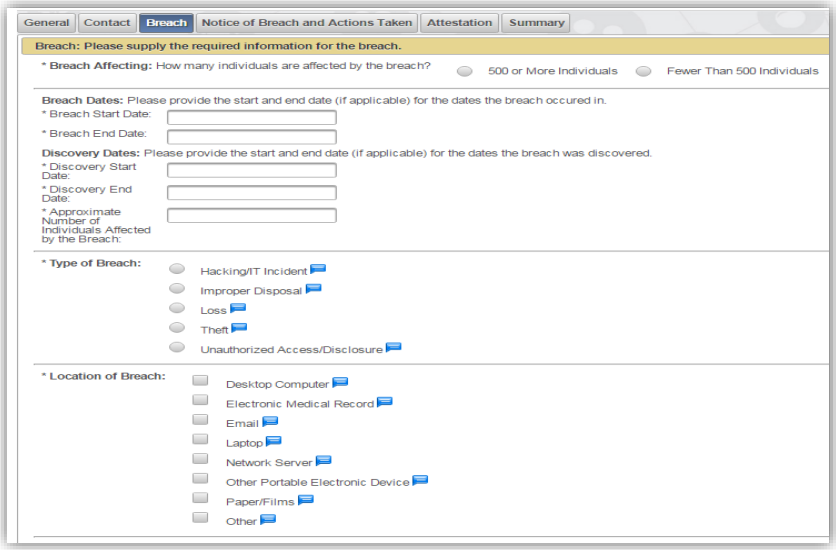
The 27th National HIPAA Summit

Cyber Incident Response Readiness

ecfirst Perfecting the Art of *Active* Cyber Defense

Breach Notification Form

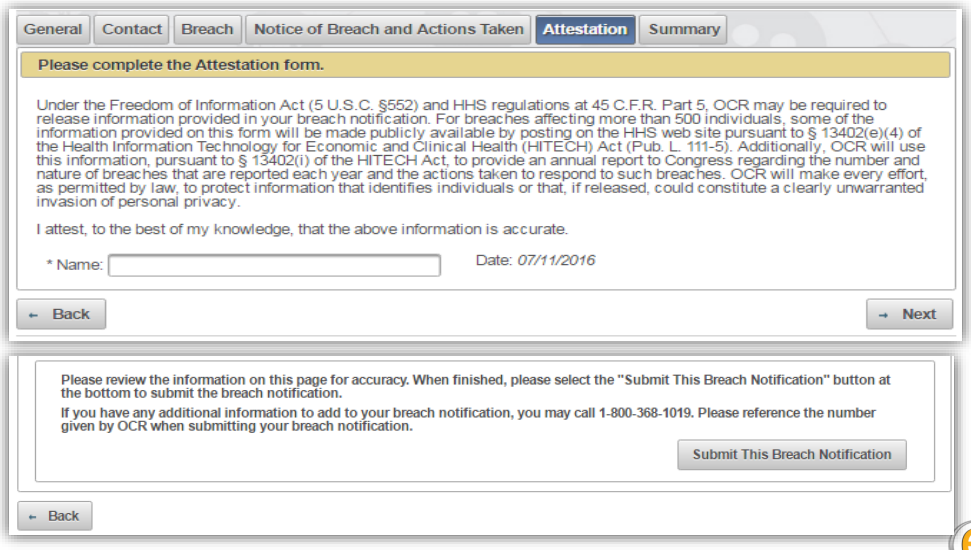
The 27th National HIPAA Summit



ecfirst Perfecting the Art of *Active* Cyber Defense

Breach Notification Form (Cont'd...)

The 27th National HIPAA Summit



ecfirst Perfecting the Art of *Active* Cyber Defense

Breach Readiness Plan

The 27th National HIPAA Summit

Four Key Areas

ecfirst Perfecting the Art of *Active* Cyber Defense

The 27th National HIPAA Summit

ecfirst Perfecting the Art of *Active* Cyber Defense

Checklist for Risk Assessment

The 27th National HIPAA Summit

#	Area	STATUS		Comments
		YES	NO	
1	Document Regulations (Federal, State) & Standards That Business is Mandated to Comply (Privacy, Security) With	☐	☐	
2	Assess Policies (Privacy, Security)	☐	☐	
3	Assess Procedures (IT, Security)	☐	☐	
4	Review Asset Management Process & Documents	☐	☐	
5	Review Vendor (Business Associate) Agreements	☐	☐	
6	Assess Deployed Security Controls	☐	☐	
7	Identify Missing Security Controls	☐	☐	
8	Assess State of Encryption Implementation	☐	☐	
9	Review Cloud Security for Deployed Apps & PII/EPHI	☐	☐	

ecfirst Perfecting the Art of *Active* Cyber Defense

Checklist for Risk Assessment (Cont'd...)

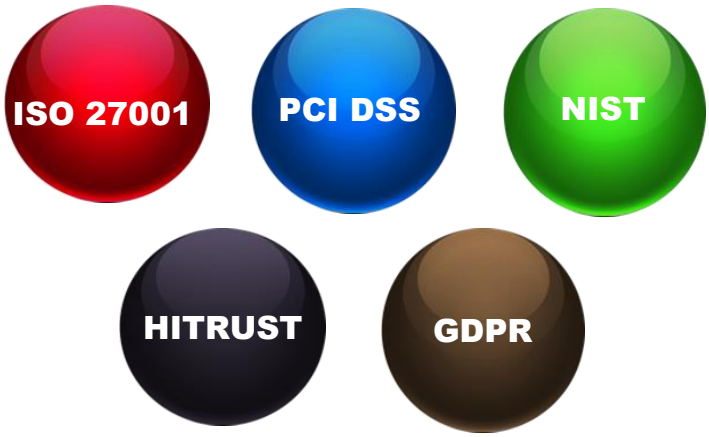
The 27th National HIPAA Summit

#	Area	STATUS		Comments
		YES	NO	
10	Conduct Technical Vulnerability Assessment (External, Internal)	☐	☐	
11	Conduct Wireless Assessment	☐	☐	
12	Review Firewall Architecture & Configuration	☐	☐	
13	Review Mission Critical Applications & Their Security	☐	☐	
14	Assess Requirements for Penetration Testing	☐	☐	
15	Evaluate Risk Management Program	☐	☐	
16	Assess Quality/Depth of Security Awareness Training	☐	☐	
17	Review Information Security Skill Capabilities	☐	☐	
18	Assess Executive Priority/Reporting Structure for Security & Compliance	☐	☐	

ecfirst Perfecting the Art of *Active* Cyber Defense

Compliance Mandates

The 27th National HIPAA Summit



ecfirst Perfecting the Art of *Active* Cyber Defense

ISO 27001: A Global Standard

The 27th National HIPAA Summit

ISO 27002
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 Perfecting the Art of *Active* Cyber Defense

PCI DSS: Important Reference

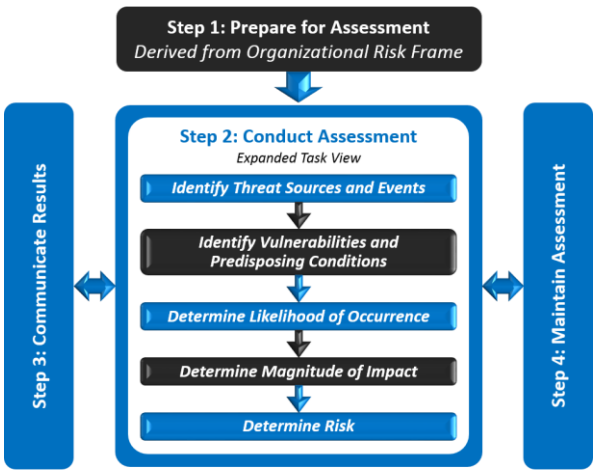
The 27th National HIPAA Summit

PCI DSS Requirements	Testing Procedures
12.1 Establish, publish, maintain, & disseminate a security policy that accomplishes the following:	**12.1** Examine the information security policy & verify that the policy is published & disseminated to all relevant personnel (including vendors & 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, & vulnerabilities, & 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, & results in a formal risk assessment.

ecfirst Perfecting the Art of *Active* Cyber Defense

NIST SP 800-30 Rev 1: Risk Assessment

The 27th National HIPAA Summit



RISK ASSESSMENT PROCESS

ecfirst Perfecting the Art of *Active* Cyber Defense

HITRUST CSF

The 27th National HIPAA Summit

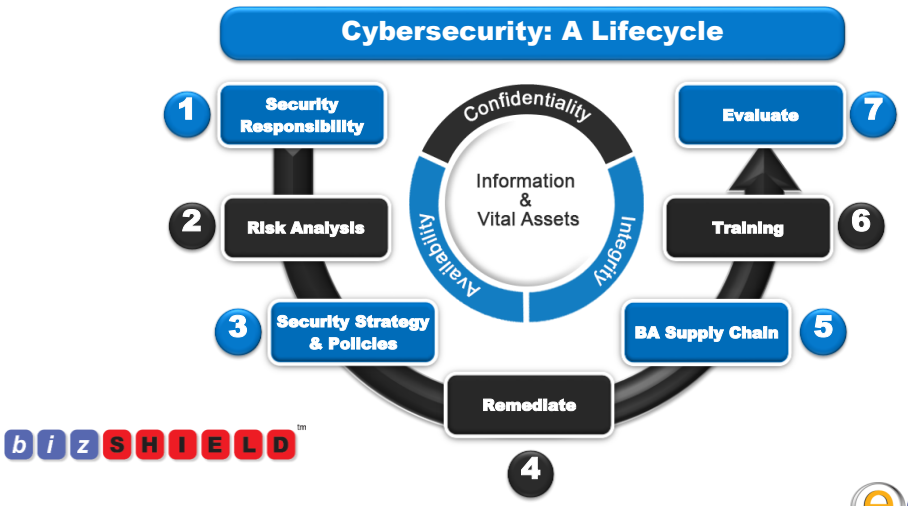
ecfirst Perfecting the Art of *Active* Cyber Defense

The 27th National HIPAA Summit

ecfirst Perfecting the Art of *Active* Cyber Defense

An *Annual* Assessment!

The 27th National HIPAA Summit



ecfirst Perfecting the Art of *Active* Cyber Defense

Credible Vulnerability Assessment?

The 27th National HIPAA Summit

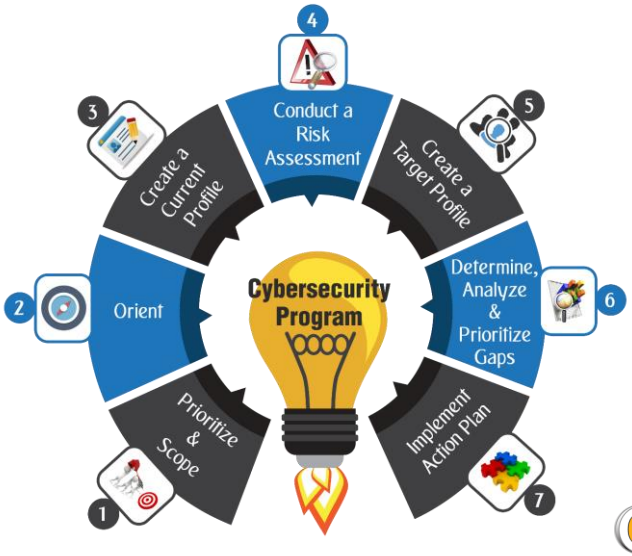
1. Conduct a VA
2. Validate & Remediate Findings
3. Pen Test

ecfirst Perfecting the Art of *Active* Cyber Defense

Cybersecurity Program

The 27th National HIPAA Summit

NIST CsF



ecfirst Perfecting the Art of *Active* Cyber Defense

Cyber Action Required Annually!

The 27th National HIPAA Summit

1. Develop a credible cybersecurity strategy
2. Conduct a comprehensive security risk assessment
3. Ensure a technical vulnerability assessment is performed quarterly, and a pen test annually
4. Perform a Business Impact Analysis (BIA)
5. Develop a detailed Disaster Recovery Plan (DRP)
6. Create a cyber incident response plan
7. Implement a cybersecurity framework (e.g. HITRUST, NIST CSF)

Repeat all areas above, annually!

ecfirst Perfecting the Art of *Active* Cyber Defense

Certification Training

The 27th National HIPAA Summit

CHP Certified HIPAA Professional HIPAA Academy — **Certified HIPAA Professional**	May 22 – 23, 2018 Washington, DC
CSCS Certified Security Compliance Specialist — **Certified Security Compliance Specialist™**	May 24 – 25, 2018 Washington, DC
CCSA Certified Cyber Security Architect — **Certified Cyber Security Architect℠**	
HITRUST Authorized CSF Assessor — **HITRUST Cybersecurity Strategy Workshop**	
PCI Security Standards Council — **PCI DSS Cybersecurity Workshop**	
ISO 27001 & 27799 1-Day Workshop	

ecfirst | Perfecting the Art of *Active* Cyber Defense

HITRUST Strategy Workshop

The 27th National HIPAA Summit

In this fast-paced, fact based HITRUST Cybersecurity workshop you will:

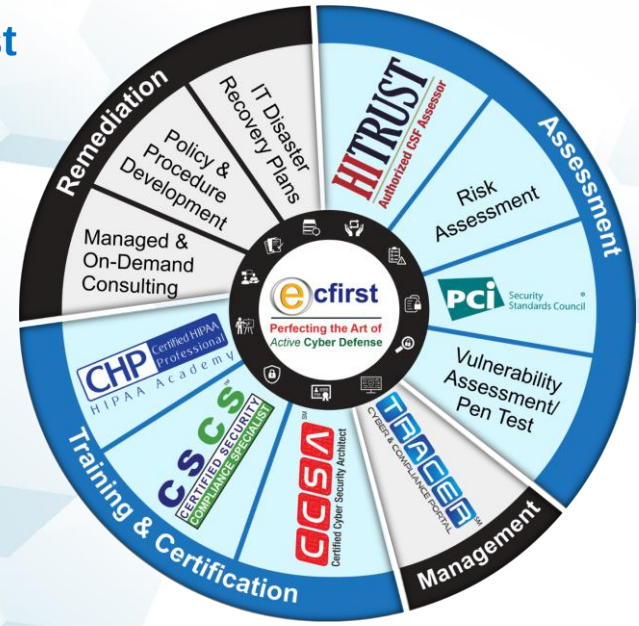
- Learn the process for HITRUST CSF Certification
- Examine about the regulations you can include in one report to save you time, money and resources
- Determine your specific risks as it relates to HITRUST CSF Certification
- Scope sample assessments in-class
- Meet the MY CSF Tool used for HITRUST from Self-Assessment to Certification
- Include your entire team to determine if you are ready for this step or when you should add HITRUST to your project plan
- Includes full set of HITRUST Policy Template (one per company) $1,495 value
- Delivered by ecfirst, Authorized HITRUST CSF Assessor

June 7, 2018
Schaumburg (Chicago), Illinois

Review select HITRUST CSF policies, live, in-class!

ecfirst | Perfecting the Art of *Active* Cyber Defense

About ecfirst



Delivering Everything Compliance. Everything Security.

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

HITRUST Authorized CSF Assessor | PCI Security Standards Council

Control Your Excitement!

The 27th National HIPAA Summit

+1.949.528.5224 | Ali.Pabrai@ecfirst.com

ecfirst | Perfecting the Art of *Active* Cyber Defense