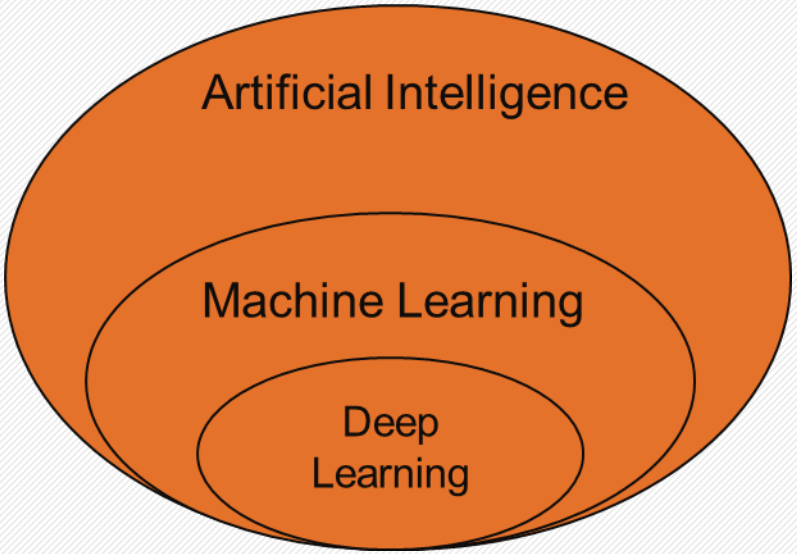
CYBER 503x
Cybersecurity Risk Management

Unit 7: Data Driven Security 2

The Lightning Evolution of AI, ML and DL

- Spam filtering
- Targeted online advertisement & recommendation engine
- Computational perception – face recognition, and speech, text, social, video, etc.
- Machine translations
- Autonomous vehicles (e.g. drones, self-driving cars)
- AI-generated art (e.g. music, poetry, painting)
- AlphaGo AI

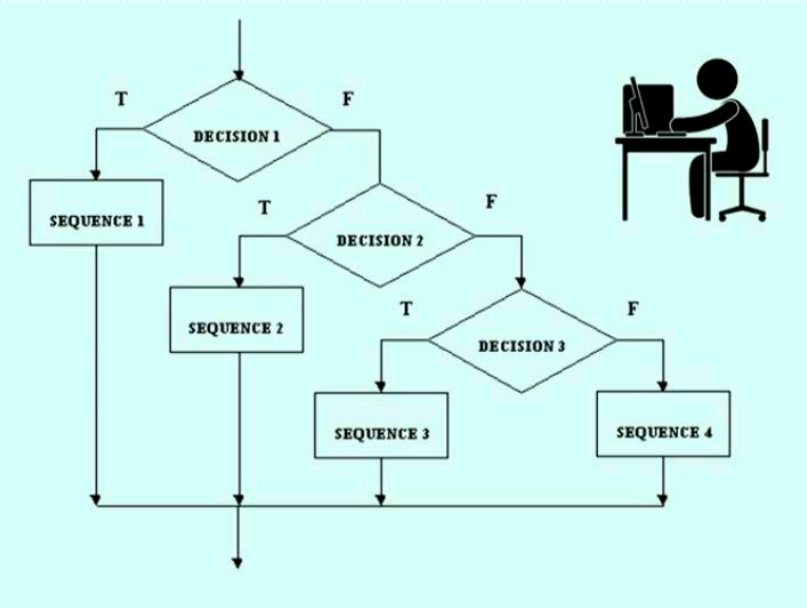
What are AI, ML and DL?



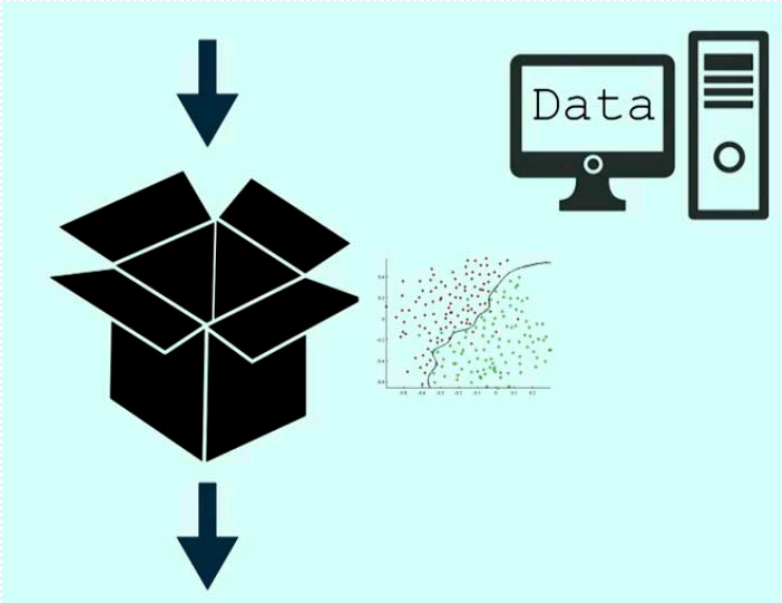
- AI consists of:
  - Perception
  - Search/Planning
  - Reasoning/Knowledge Representation
  - Autonomy
  - Natural Language Processing
  - Machine Learning (ML)

- Machine Learning (ML) is a subfield of AI
- Deep Learning (DL) is a branch of ML that focuses on specific algorithms (i.e. artificial neural networks)

Explicit Programming vs. Machine Learning



vs



Types of Machine Learning Problems

- Supervised Learning
  - Classification (e.g. spam/non-spam or fraud/non-fraud)
  - Regression
- Unsupervised Learning – pattern discovery
  - Clustering
  - Rule extraction

Benefits of ML include automation, being unbiased, and being able to improve over time

Machine Learning vs. Statistical Modeling

	Machine Learning	Statistical Modeling
	An algorithm that can learning from data without specific programming	Relationship between variables in the form of mathematical equations
	A subfield of Computer Science and AI	A subfield of mathematics
Assumptions	Need not specify the distribution of dependent or independent variable	- Linear relation between independent/dependent variables - Independence of observations - Normally distributed error
Types of data	Really well with wide (high number of attributes) and deep (high number of observations) data	Generally applied for smaller data with less attributes or they end up over-fitting

Why ML in Cybersecurity?

Example: Web server activity log file

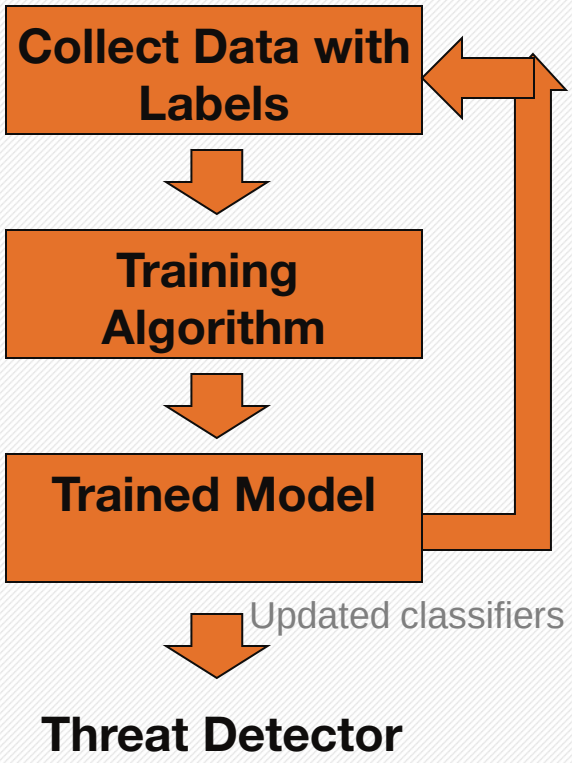
1	s1	ip1664.com	msnbot/1.0 (+http://search.msn.com/msnbot.htm)	/robots.t
2	s1	ip1664.com	msnbot/1.0 (+http://search.msn.com/msnbot.htm)	/gpspubs
3	s2	ip1115.unr	Mozilla/4.0 (compatible; MSIE 5.5; Windows 98; SAFEXPLORER TL)	/news/99
4	s3	ip2283.unr	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	/dmcours
5	s3	ip2283.unr	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	/dmcours
6	s4	ip1389.net	Mozilla/4.0 (compatible; MSIE 6.0; X11; Linux i686; en) Opera 8.5	/gpspubs
7	s4	ip1389.net	Mozilla/4.0 (compatible; MSIE 6.0; X11; Linux i686; en) Opera 8.5	/gpspubs
8	s4	ip1389.net	Mozilla/4.0 (compatible; MSIE 6.0; X11; Linux i686; en) Opera 8.5	/favicon.i
9	s5	ip1946.com	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ys	/news/20
10	s6	ip992.unr	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT; MS Search 4.0 Robot)	/aps/bt4-
11	s7	ip2213.net	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	/
12	s7	ip2213.net	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	/kdr.css
13	s7	ip2213.net	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	/images/k
14	s7	ip2213.net	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	/images/k
15	s7	ip2213.net	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	/aps/aw1
16	s7	ip2213.net	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	/images/r
17	s7	ip2213.net	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	/aps/bt4-
18	s7	ip2213.net	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	/aps/f-sp
19	s7	ip2213.net	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	/aps/t-sa

Security log data:

- **Complex sequential data**
- **Not human-intuitive**
- **Scarce & expensive labels**

How is AI/ML used in cybersecurity today?

- Classic supervised learning
  - Primarily for automated detection
- Heavily rely on data scientists
  - Feature engineering
  - Updates & tweaks model parameters
- Not user-facing



Threat Response Automation – an evolving frontier in cyber security

- Firewall software

- Early IDS solution

- Advanced IDS solution
- Fraud analytics
- Network sniffers
- Web gateway & endpoint protection solutions

Adaptive & Dynamic
Minimal human intervention

AI/ML Adoption in Cyber security

- Drivers
  - Scaling and velocity
  - Automation
  - Sophistication
  - Big data & 360 degree protection
- Benefits
  - Automated protection
  - Faster response
  - Personalization

- Challenges for ML Software
  - Source code + data -> program
  - Data are embedded & opaque
  - Reconstruction is hard or impossible
  - ML data versioning is hard
  - Introduce data and system dependencies

Malware Detection

- Limitation of existing techniques
  - Signature-based approach
    - Fails to detect zero-day attacks
    - Fails to detect threats with evolving capabilities
  - Anomaly-based approaches
    - Producing high false positive rate

Malware Detection with ML-based Approach

- Two Level hierarchical learning:
  - Supervised learning approach to detect malicious flows and further identify specific type
  - Combine unsupervised learning to address new class discovery problem
- Deep Learning approach
  - Uncover the hidden and sophisticated patterns
  - Scan and detect malware never encountered before

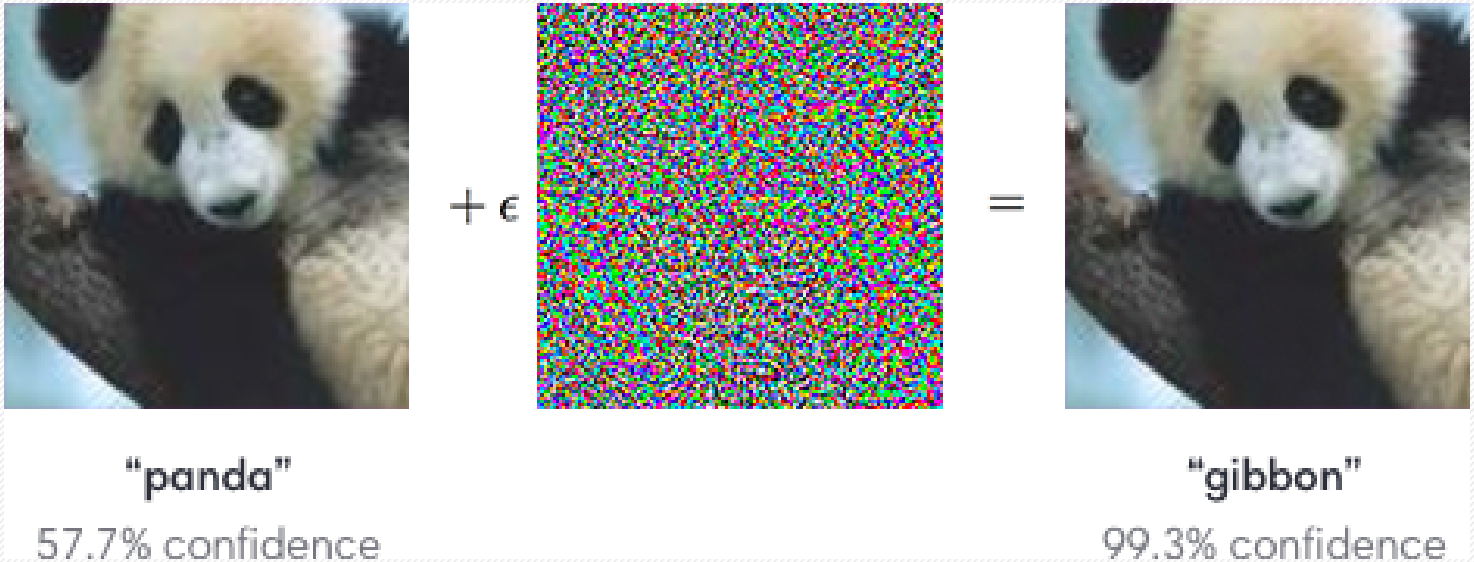
Anomaly Detection & Machine Learning

- Anomaly Detection (AD) – mostly done through rule-based heuristic methods
- It is fundamentally different from other ML problems:
  - Very high cost of errors
  - Lack of training data
  - “Semantic gap”
  - Difficulties in evaluation
  - Adversarial setting

Adversarial Machine Learning

- Model extraction
  - Adversary learns an approximate model using fewest possible queries
- Model Poisoning
  - Adversary biases machine learning model through interaction

Adversarial Examples



An adversarial input, overlaid on a typical image, can cause a classifier to mis-categorize a panda as a gibbon.

I.J. Goodfellow, J. Shlens. C. Szegedy, "Explaining and Harnessing Adversarial Examples". ICLR 2015

How to address “adversarial machine learning”

- Conduct threat modeling of your ML solutions
  - Define the adversary’s goal
  - Assemble the adversary’s knowledge
  - Determine the adversary’s capability
- Taking steps to protect your end-to-end data pipeline, includes securing data uploader & repository
- Test your ML algorithms against common attacks (e.g. AdversarialLib)

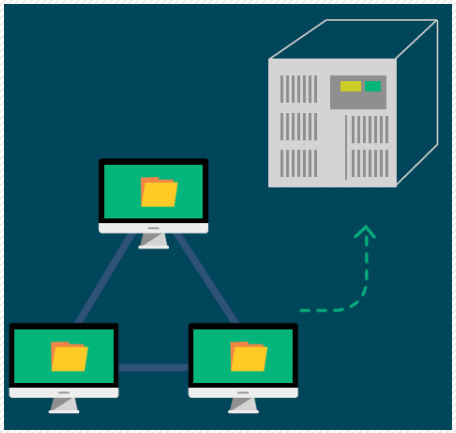
Data Breaches in Retail & Digital Media Industry: How did it happen?

(1) Making Their Way In

In-Store

Online purchases

Central Database with Customer Information



Data Breaches in Retail Industry: How did it happen?

(2) Under attack

- Attack Internet-facing servers
  - hack default or overly simplistic passwords
  - use publicly-known exploits for certain systems – or find their own
  - gain access through a security misconfiguration, i.e. via file upload or SQL injection
- Send a phishing email
- Access through third parties
- Partner with a rogue employee

Data Breaches in Retail Industry: How did it happen?

(3) Stealing the keys to the fortress (5-steps path)

1. Gain access through points of entry
2. Install a bot, Trojan or root kit to maintain access, and/or add another account.
3. Elevate privileges.
4. Move through the network to access higher-level systems and discover more powerful credentials.
5. Access the area targeted with those credentials – a server or a point-of-sale (POS) platform – to acquire credit card information

Questions to ponder

- Who is Attacker? Their Characteristics?
- What is threat/vulnerability?
- What aspect (CIA) of information security is under attack?
- How did the victimized company respond?
- What is the impact?
- Lessons learned?

Security Breaches By the Numbers

- Average cost of a US organization’s data breach $5.85 million
- Rate at which data costs increased from 2015 to 2016 is 29% and continue to rise
- Average cost paid for each lost or stolen record containing sensitive information is $145
- Risk Benefits Assessment Worksheet
- Average cost per hour for a company experiencing downtime is $686,000

Factors that decrease the cost of a data breach

- Having a strong security posture ($14.14 per hacked record)
- Instituting an incident response plan ($12.77 per hacked record)
- Having a Chief Information Security Officer (CISO) ($6.59 per hacked record)
- Institute incident response plan and disaster recovery service to ($16 per hacked record):
  - Reduce your cost and losses by keeping your business running
  - Provide increased security to detect and prevent threats when they emerge
  - Provide greater protection to your customers. Studies have found that customer loyalty decreases after a breach.

The Worst Breach @Yahoo! 2016

The Yahoo! Attack

In case of YAHOO! a 5 Phase Attack

Hackers engaged in a complex attack with 5 phases, multiple dynamic actions per phase

Phase 1: Phishing Email → Back door installed → Stolen Credentials

Phase 2: Conceal unauthorized access → Reconnaissance for 6-12 months

Phase 3a: Locate and infiltrate targets (User DB & Account Management tool)

Phase 3b: Hack emails with compromised authentication information

Phase 4: Copy user DB and Account Management tool → Ex-filtrate over unsecured network

Phase 5: Mine emails for credit card numbers, personal information and more

HORTONWORKS

Behind the Yahoo! Breach
Questions to ponder (1)

- Who is Attacker? Their Characteristics?
  - Russian Agents (state-sponsored attacker)
- What is threat/vulnerability?
  - **Known attacks/exploits:** phishing, email hacking
  - **Known vulnerability:** weak password and account management, especially in detecting and preventing unauthorized access to user accounts
- What aspect (CIA) of information security is under attack?
  - Confidentiality of customer information (e.g. names, email address, phone number, Security questions and answers)

Behind the Yahoo! Breach
Questions to ponder (2)

- How did Yahoo respond?
  - Time is a key factor; but public announcement after 2 years
  - Notifications and recommendations
- What is the impact?
  - Brand damage, customer loyalty decrease due to the number of affected users
  - Verizon hacks $350M from its planned $4.8B acquisition of Yahoo

Behind the Yahoo! Breach
Questions to ponder (3)

- Lessons Learned
  - Security measures could have been taken were not put in place
  - Known vulnerabilities were left unprotected
  - Slow to respond when they first detected a potential breach
  - Effective measures are needed to strengthen the company's security posture, including
    - Implementing technologies such as cloud-based cyber security, big data analytics, advanced authentication
    - Enhancing systems that detect and prevent unauthorized access to critical assets
    - Adopting risk-based cyber security frameworks
    - In addition to external attackers, 3rd party partners and foreign entities are also a mounting concern

HIPAA Privacy & Security Rules for Protected Health Information (PHI)

- HIPAA Privacy Rules: - Patient Information Centric
  - Refers to WHAT is protected – an individual's PHI and the determination of WHO is permitted to use, disclose or access that information.
- HIPAA Security Rules – IT centric
  - Refers to HOW electronic PHI (ePHI) is safeguarded – ensuring privacy by controlling access to information and protecting that information from inappropriate disclosure, destruction or loss.

Protected Health Information (PHI)

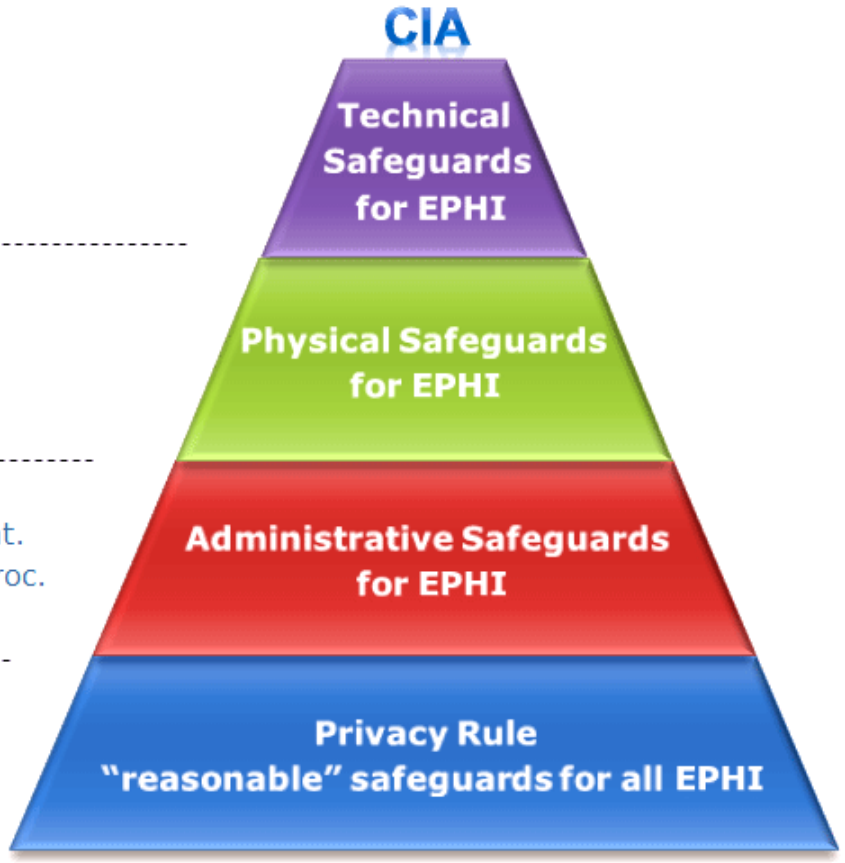
- Individually identified health information
- Concerns physical or mental health, health care or payment
- Created or received by covered entity in its capacity as a healthcare provider
- Maintained in any form or medium, e.g. oral, paper, electronic, images, etc.

HIPAA Security Rule Compliance

- Access Control
- Audit Control
- Integrity
- Person or Entity Authentication
- Transmission Security

- Facility Access Controls
- Workstation Use
- Workstation Security
- Device & Media Controls

- Security Mgmt. Process, Sec. Officer
- Workforce Security, Info. Access Mgmt.
- Security Training, Security Incident Proc.
- Contingency Plan, Evaluation, BACs



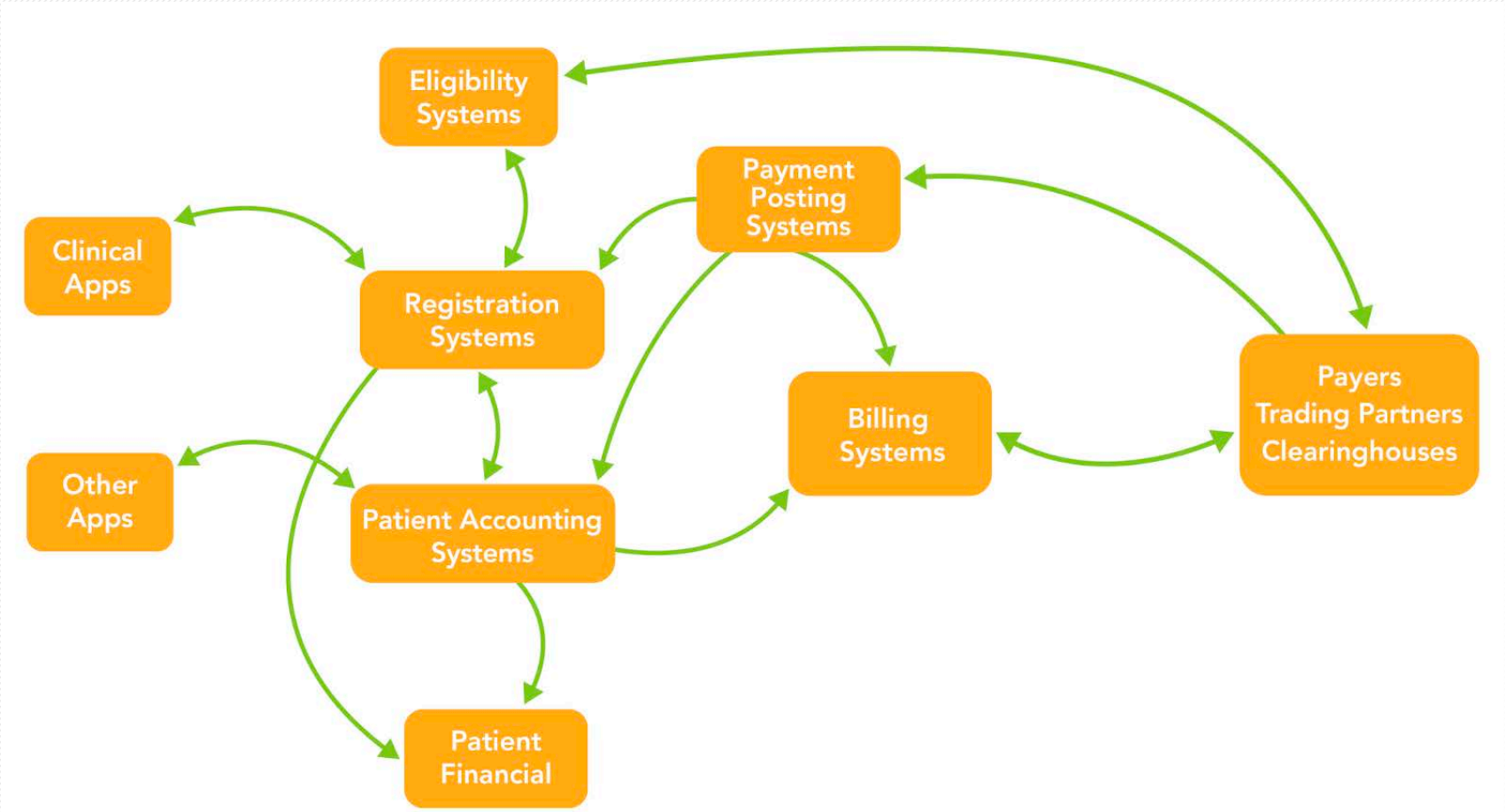
http://www.hipaaacademy.net/managed-compliance/hipaa-consultant-staffing/hipaa-security-rule/

How to conduct HIPAA Risk Management Program

Step 1: Define the scope by defining PHI flow

- Where PHI starts or enters your environment
  - Email, Texts, EHR entries, Faxes, USPS, New patient papers, Databases
- What happens to it in your system
  - Filing cabinets, mobile devices, EHR/EMR systems, Calendar Software, Email, networked medical devices, computers, applications, encryption software
- Where PHI leaves your environment
  - Lifecycle with business associates, recycling companies, trash bins on computers
- Where potential or existing leaks are
  - To find all possible leaks is by creating a PHI flow diagram

PHI Flow Diagram



http://blog.securitymetrics.com/2014/11/diagrams-help-hipaa-audits.html

How to conduct HIPAA Risk Management Program

Step 2: Identify Vulnerabilities, Threats and Risks to Your Patient Data

- What vulnerabilities exist in the system, application, process or people
- What threats, internal, external, environmental and physical, exist for each of those vulnerabilities
- What is the probability of each threat triggering a specific vulnerability? This is the risk.

Step 3: Analyze HIPAA Risk Level and Potential Impact

- Likelihood of occurrence
- Potential impact

Step 4: Identify Top Security Measures Based on Top HIPAA Risks

Step 5: Rinse and repeat (continuing evaluation)