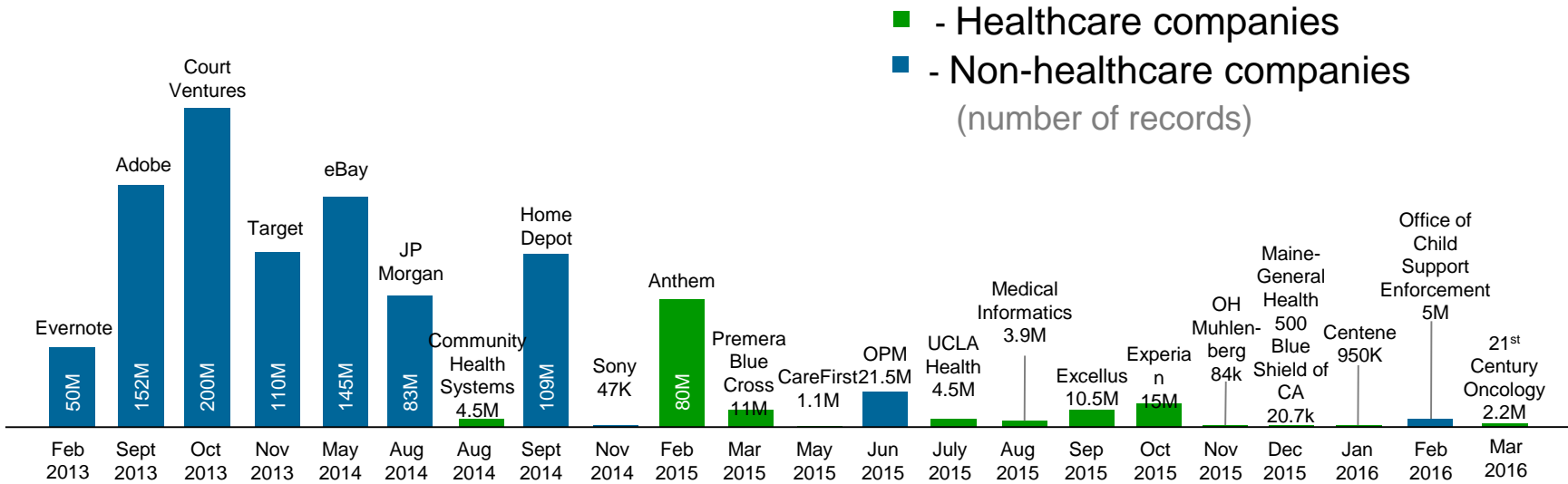


# Healthcare Increasingly Targeted by Cyber Criminals

*Medical insurance information is more valuable than credit card information*



## RECENT HEALTHCARE BREACHES

### Premier Healthcare

- January 4, 2016
- Password-protected but **unencrypted laptop** stolen from billing department
- Stole 205,748 records

### Hollywood Presbyterian

- February 5, 2016
- Attackers infected computer systems with **ransomware** that encrypted patient information
- Paid \$17,000 in ransom

### MedStar Health

- March 28, 2016
- **Malware** affected workstations and caused **network-wide shutdown**
- Closed 10 hospitals and over 250 outpatient facilities for 5 days

# Cybersecurity Threat Actors

	CYBER CRIME AS A SERVICE	ORGANIZED CRIME	STATE-SPONSORED	HACKTIVISTS
Motive	Financially motivated, paid % of profit	Financially motivated	Research, espionage and <b>sensitive proprietary information</b>	Motivated by social justice causes to seek confidential information to <b>defame or damage an enterprise</b>
Characteristics	<b>Allows others to rent infrastructure</b> for attacks: botnets, phishing tools, and vulnerability scanning of targets	Aim to <b>collect ransom, personal data, including medical records, credit cards and social security numbers</b>  Typically have an <b>industry focus</b>  Efficient, <b>profit-focused quick attacks</b> with <b>high return on investment</b>  Increasing sophistication using denial of service <b>ransomware</b>	<b>Highly-skilled and highly-persistent</b> groups with <b>unlimited resources</b>  Employ <b>sophisticated and previously unknown methods</b> (e.g., custom malware)  Pursue and achieve <b>specific objectives</b>  Maintain a <b>low profile</b> to cover their tracks and remain in the network for months, if not years	<b>Unstructured</b> coalitions of individuals that come together based on <b>common cause</b>  Rely on <b>social engineering</b> techniques  Employ <b>less sophisticated</b> attack methods due to resource limitations  Engage <b>armies of infected computers</b> available in the dark web

# Evolving Attack Vectors



## Social Engineering

Exploiting human nature

Email phishing, spear phishing and whaling; telephone and in person fraudulent representations



## Internet Surfing

Malware-laced Internet pages, links & downloads

“Drive-by” and hidden malware



## Credential Theft

Exploiting stolen user IDs & passwords

Elevated access accounts (system and database administrators, report writers) present greatest risk



## Network

Disrupt network traffic, or breach network

Movement to the cloud expands paths attackers can take, and Denial of Service attacks are challenging to prevent



## Software bugs

Software bugs, and/or unpatched systems

Provide breach entry points. Requires ongoing work to keep versions up to date and to apply patches across complex enterprises



## Configuration errors

Systems with configuration errors

Requires constant testing and assessment of applications and infrastructure. Biomedical devices are a special challenge