Understanding Cyber Threats & Cyber Security

NCPERS 2016 Healthcare Symposium
Washington, D.C.

Jan. 24, 2016

Doug Porter
Senior Vice President, Operations and CIO
Agenda

• Introduction

• How did we get here?

• Who are we dealing with?

• What can we do about it?
Unmatched Scale and Market Share

BCBS spans every ZIP code in the U.S.

104+ million members

96% of all U.S. hospitals

92% of all U.S. physicians

84 of Fortune 100 companies served

Unparalleled Depth and Breadth of National Healthcare Data

Reflecting

• $380 billion in annual claims
• $145 billion in annual claims tied to value-based payment arrangements

Including

• 36 million provider records
• 1.7 million active unique providers
• 700,000+ validated BCBS patient reviews on 90,000+ providers

Treatment cost estimates from

• 2.3 billion covered procedures performed annually
• $82 billion in claims paid
• 20,000+ healthcare facilities
• 540,000+ professional providers
BCBS Axis℠ Powers Market-Leading Solutions

**Industry Leadership**
Health of America reports; Community Health Hub; Plan Innovations

**Empowering Members to Make Smarter Decisions**
Data on doctors, hospitals, and procedures is made available to members so they can locate the right doctor at the right cost, and make better informed and personalized healthcare decisions

**Designing High-Value Benefit Strategies**
Data is shared with employers to identify cost drivers, benchmark their performance, and to design custom network and benefit strategies to drive improved healthcare quality and affordability

**Facilitating High-Performance Healthcare**
Data is analyzed and shared with doctors and hospitals to facilitate stronger care coordination and enhance care delivery decisions that result in better patient outcomes and lower cost

**High-Value Benefit Strategies**
- Make Decisions
- Get Care
- Live Healthy
- Transparency
- Care Management
- Health & Wellness

**High-Performance Healthcare**
- BlueDistinction
  - Specialty Care
  - Total Care

**Network Strength**
- BlueCross BlueShield | Axis
Our Shared Interests

Protect brand, mission, strategy, and viability amid an emerging chaos of bad actors.

Professionally, ethically, and objectively work for the benefit of our constituents.
How Did We Get Here?

Culture of immediacy

The age of impatience

[Diagram with categories: BIG DATA, SOCIAL MEDIA, SOCIETAL EXPECTATIONS, CLOUD COMPUTING, INTERNET OF THINGS, MOBILE TECHNOLOGY]
Third Wave of Computing

How Did We Get Here?

- **MAINFRAME**: SNA, TERMINAL
- **SERVER**: LAN/WAN, CLIENT
- **CLOUD**: LTE, PRODUCTS
- **THOUSANDS**
- **MILLIONS**
- **50 BILLION CONNECTED “THINGS”**
Threat Actor Motivation

**Organized Crime**
Illicit gains related to theft, fraud, abuse, human trafficking, pornography, prostitution, ransomware and other underworld operations.

**Nation State Actors**
International entities targeting Americans of interest, guests to White House, Security clearances, Federal Employees, Corporate Intellectual Property, etc.

**Hacktivists**
Disruption in support of social agendas by groups such as Anonymous.

**ISIS Cyber Army (ICA)**
Organized to destroy entities as a war-time strategy.
Organized Crime

- $400B industry\(^1\)
- Extracts 15-20% of the $2-$3 trillion dollars (300-600B) generated by the Internet economy\(^2\)
- High level of sophistication coupled with an ecosystem of various “service providers” that interact in a rich underground economy
- Specialized skill sets and professionalized business practices (e.g., SOPs)
- Form private, trusted, and organized groups to conduct cyber crime
- Continuously recruiting experienced actors

\(^1\)McAfee
\(^2\)Center for Strategic and International Studies
\(^3\)IBM (2015)
Organized Crime

- Possible to find any kind of illegal product or service (drugs, weapons, stolen merchandise, medical records, credit cards, bank account passwords, fake identities, hacking services, or hit men).
- Access with anonymity (e.g., via Tor which is virtually untraceable).
- **Silk Road**: $1B of goods sold before shut down.

**Who Are We Dealing With?**

- **Surface Web**: 4% Content that can be found using search engines.
- **Deep Web**: 96% The Invisible Web – not easily accessed and hard to keep track of. Estimated to be 500 times the size of the Surface Web.

- **Evolution Market**: follow-up to Silk Road. Launched in January 2014; one of the two largest drug markets. It was shut down on March 18, 2015 in an apparent "exit scam" in which the site's administrators shut down the market and walked away with $12 million in bitcoin (in user's escrow).
- **Enigma**: a bid-and-ask forum akin to eBay. Bids looking for names of people who could serve as insiders at corporations (i.e., lists of people who might be susceptible to being recruited or extorted).
- Other recent examples of hacking services found in the black market: The Hell Hacking Forum (Gmail account takeover for $300 or .68Bitcoin), TheRealDeal Market (24-hour DDoS service), Nucleus (custom FaceBook hack, $250 or .57Bitcoin).
- Transactions in the cyber black markets are often conducted by means of digital currencies. Bitcoin, Pecunix, AlertPay, PPcoin, Litecoin, Feathercoin, etc.
Nation-State

Persistent, stealthy, patient, well resourced, work-around-the clock, documented procedures.

Goals vary from espionage and intelligence gathering to sabotage (i.e., Sony).

Why Nation state and Healthcare?

- Feed sustainable growth:
  - In support of China’s twelfth five-year plan which launched in 2011
  - Cover a range of topics to improve and stabilize China’s future
  - One important element of this plan is “inclusive sustainable growth” w/ specific considerations for welfare of the populace
  - Commitment to growth in social security, pensions, and medical insurance
  - Improvement in medical technology advances, foreign investment in developing the healthcare sector
- Intel for future operations
  - Build out profiles on individuals
Hacktivists

• Ideologically motivated.
• Wide range of skills & abilities
• Responsible for more data breaches than cybercriminals (Verizon DBIR).
• Some have links to foreign governments.
ISIS Cyber Army

- At war with Anonymous. Last month, ICA released personal information of numerous high-ranking French and U.S. military officials as a response to Anonymous-led "ISIS day of trolling."

- This month, Caliphate Cyber Army (CCA) announced a partnership with AnonGhost.

- CCA was led by Junaid Hussain until his recent death via a US air strike. He was the second-most prominent British member of the Islamic State, after “Jihadi John.”
0. Reconnaissance
1. Weaponized Word doc sent to target.
2. Word macro calls out to C2 and downloads text file.
3. Script calls out to C2 server and downloads, unpacks and installs Upatre (a Trojan horse).
4. Upatre downloads and executes Dyre virus.
5. Dyre pulls down configuration file.
6. Target reaches out to banking site but is proxied.
Who Are We Dealing With?

Attacker Sophistication: Hactivist DDoS

Amplification attack

Attacker with 1 Mbps

1 Mbps connection

10 compromised trigger machines with 1 Gbps

1 Gbps connection x10

400 ‘amplifier’ machines

Amplification factor of 50x

500 Gbps hits target machine from amplifiers
Trends: Digital Economy

Generation Y and Millennials will comprise half of the nation’s workforce by 2020.

- Most educated, diverse and tech-savvy generation ever.
- Internet and connective technology is “the way it’s always been.”
FOUNDATION KNOWLEDGE AND DEFENSES
• Know your critical assets and attractiveness to adversary
• Who are the adversaries interested in this data and what are their TTPs
• Mature IR capability – tier1, tier 2 (respond), tier 3 (hunt, CI, close to adversary)

STAFF VIGILANCE
• Established Intelligence Sources
• Internal (employees, Sim, big data, crowd sourcing
• Government sponsored sources (FBI, Secret Service)
• Industry sources (ISACs)
• OSINT (consolidate malicious IPs, domains, spammers)
• Commercial sources (e.g., Crowdstrike, FireEye, Mandiant, iSight, Dell, RSA)

DRIVE INTELLIGENCE
• Operational Intel (inputs imported into IDS; monitor-to-block)
• Search for IOCs (querying endpoints and network.
• Map kill chain indicators back to defender courses of action (increase the difficulty for the adversary; get to know them).
• Produce strategic intelligence products to inform decision makers (historical data including threat trends and predictive analysis).