# 11 May 201 de512

# 11 May 2017 MassMITREPartners Cyber Resilience Workshop

# 11 May 2017 MassMITREPartners Cyber Resilience Workshop

# 11 May 2017 Mass/MITRE/Partners Cyber Resilience Workshop

▾ Remarks by CISO from Partners, Jigar Kadakia

- Health care incidents expose more SSN's than any other industry
- Health care hit hardest by both employee error and hacking_skimming_phishing
- cybercrime damage to hit $6m annual by 2021
- Up to 200 billion devices need securing by 2020
- human attack surface to hit 4 billion by 4 billion

▾ What makes health care different?

- could have more than 200k endpoints in a hospital
- Risk of patient harm

▾ value of information

- Patients treat their health data much more sensitively (desire for privacy) than other types of data
- Number/diversity of applications
- need to interconnect diverse systems
- Number of different users/environments
- smaller low-resource organizations are part of critical infra responsible for patient safety

▾ what is at risk?

- PCI, PII, HIPAA, HITECH
- CPOE and mobile EHR
- Medical devices

▾ threat actors threat model in increasing order of risk

- accidental
- Hospital employee/accidental misuse
- lone hacker/hobbyist
- Business associate
- script kiddy
- Disgruntled ex-IT / employee
- competitor
- Disgruntled patient
- APT
- Organized crim
- Hacker collectives
- cyber terrorism
- hacktivism

▾ New and now — cyber security landscape

▾ IoT

- DOS on Dyn — knock out connections to critical systems like EHR, web-based services
- Mirai — IoT

▾ ransomware

- Targeting hospital EMRs
- Cyber attacks targeting medical devices

▾ Idea of cyber resilience

- About managing security w/ a multi-layered approach — people, process, technology

▾ why?

- Avoid catastrophic failure
- ensures conversation goes beyond IT or InfoSec

▾ cycle

- Prepare/identify
- protect
- detect

- respond
- recover

▸ What can be done?

▾ Addressing regional cyber resilience

- governance
- planning and prioritization
- funding and investment
- operationalization
- Technology and infrastructure

▾ Remarks by Secretary of Executive Office of Public Safety (MA), Daniel Bennett

- MA is developing a 5th division within Public Safety, focused on cybersecurity/ intelligence. Will be announced in the next 2 weeks

▾ Remarks by CISO from Children's, Paul Scheib

- DDoS event post-mortem

▾ Regional cyber resilience maturity model

▾ governance

- Less mature — no regional organization or ad-hoc at best
- more mature - standing mechanisms to collaboratively address resilience are in place, exercised, and effective

▾ planning and prioritization

- Less mature
- more mature - regional entities establish shared goals and objectives and assess performance against plans

▾ funding and investment

- Less mature
- more mature - funding synchronized to address shared priorities

▾ operationalization

- Less mature
- more mature - stakeholders consistently collaborate and take collective action

▾ Technology and infrastructure

- Less mature
- more mature — tools, tech, infra support critical function resilience, O&M, regular updates are supported

#learning/conferences