General Information

1) Yes I am involved as the CTO of a Cyber Security training company - Security Innovation. We provide software developers the training they need to understand and mitigate application security related threats.

Growing and Sustaining the Nation's Cybersecurity Workforce

1) The metrics we see used most often are:

- Training course completion
- Training exam score

and then when more mature we see some organizations measuring and correlating the training program data against:

- Number and severity of security defects in the code, trending over time
- Time to fix security defects once discovered, trending over time

Most organizations have a very difficult time measuring the effectiveness of training programs on the end-goal of reducing cyber-security risk. There is a real need for standardization of metrics and technology for gathering, analyzing and correlating these metrics for improved decision making.

2) In the area of application security there is some confusion around the need for a central security organization vs. the need for distributed security workers within each development team. There are pros and cons to each approach and a blended model is generally accepted as the best. The problem is how much security training each member of the development team needs, since training is expensive both in terms of money and time and there is a reluctance to over-train workers who are not designated security champions or auditors.

3) Yes

4) Most organizations want to train their developers to an existing standards. Its not clear what the best standard is for training - PCI, NIST, ISO, OWASP, etc. It would be worthwhile to determine which existing standard is the best fit for each role and vertical as well as determining if there is a need for a new standard specifically focused on developer education.

5) The most effective programs include the following components:

- Tied to business-driven security policy goals
- Deployed as an enabling factor to achieve these policy goals
- Broken into short, engaging, easy to consume chunks
- Entertaining, game-ified and hands on to promote long term knowledge retention

6) No comment

7) Internet of things sets us back at least a decade due to lack of homogeneity and lack of security tools support. AI will become increasingly relevant as an attacker tool and threat which will require similar AI investment in defense and operator education. There will be a large need to invest in developer training to ensure lessons of the past are not lost as we move to new platforms and to ensure we keep our developer work force at the forefront of new threats and mitigations.

8) Here are the critical steps:

- Standardization of cybersecurity roles in application development including titles and responsibilities both for security focused roles (e.g. data security specialist or security engineer) as well as standard engineering roles (e.g. development manager, architect)

- Development of a standard that represents what each engineering role in a development organization should be trained on, and know, in order to reduce the number of vulnerabilities being introduced into software

- Development of metrics that can be used to judge the training level of a development organization and measure progress over time, specifically tied to real impact on the goal of reducing application security risk

- Data repository with required reporting from cyber-security insurance companies that can be used to determine the steps an organization can take that will reduce their risk - as measured in the real world.