The Future of Cybersecurity Education

Being Better than “Best Practices”

Mark Heckman, Ph.D., CISSP, CISA
Center for Cyber Security Engineering and Technology
University of San Diego
Severe Cybersecurity Workforce Shortage!

Cybersecurity job market to suffer severe workforce shortage

Cybersecurity's hiring crisis: A troubling trajectory

Cybersecurity talent: Worse than a skills shortage, it’s a critical gap

Shortage of Cybersecurity Professionals Poses Risk to National Security

Cybersecurity Skills Shortage Panic in 2015?
Early Aviation Attempts
Wright Brothers
Wright Brothers’ Experiments
Model of Aerodynamic Forces

Orville’s diagram from experiments:

http://airandspace.si.edu/explore-and-learn/multimedia/detail.cfm?id=5804
Success!
Experiments to Verify Model

1930 test at NASA Langley (NACA) https://www.youtube.com/watch?v=3_WgkVQWtno
Continuing Improvements to Models
## Aviation Safety

<table>
<thead>
<tr>
<th>Type</th>
<th>per bn km</th>
</tr>
</thead>
<tbody>
<tr>
<td>Air</td>
<td>0.05</td>
</tr>
<tr>
<td>Bus</td>
<td>0.4</td>
</tr>
<tr>
<td>Car</td>
<td>3.1</td>
</tr>
<tr>
<td>Foot</td>
<td>54.2</td>
</tr>
<tr>
<td>Motorcycle</td>
<td>108.9</td>
</tr>
<tr>
<td>Pedal cycle</td>
<td>44.6</td>
</tr>
<tr>
<td>Rail</td>
<td>0.6</td>
</tr>
<tr>
<td>Van</td>
<td>1.2</td>
</tr>
<tr>
<td>Water</td>
<td>2.6</td>
</tr>
</tbody>
</table>

[https://en.wikipedia.org/wiki/Aviation_safety#Accidents_and_incidents](https://en.wikipedia.org/wiki/Aviation_safety#Accidents_and_incidents)
Aviation Safety Trend

Number of fatalities from airliner hull-loss accidents per year

https://en.wikipedia.org/wiki/Aviation_safety#Accidents_and_incidents
A record of improvement in predictive range and accuracy

http://opinionator.blogs.nytimes.com/2013/08/24/what-is-economics-good-for/?_r=0
Aviation and Cybersecurity

How do they Compare?
## Side-by-side Comparison

<table>
<thead>
<tr>
<th>Feature</th>
<th>Aviation</th>
<th>Cybersecurity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Experimental data</td>
<td>Wind tunnels, computer sims</td>
<td>?</td>
</tr>
<tr>
<td>Model</td>
<td>Aerodynamics</td>
<td>?</td>
</tr>
<tr>
<td>Record of Improvement</td>
<td>Unmatched safety record</td>
<td>😞</td>
</tr>
</tbody>
</table>
Cybersecurity Incident Trend

Security incidents grow 66% CAGR
The total number of security incidents detected showed an increase of 48% over 2013.
Cyber Attack Trend, Year Over Year

- Increasing number of attacks
- Increasing severity
- Increasing impact
- Prevention and detection techniques largely ineffective
- Attackers increasingly aggressive and proficient

Is it that organizations don’t know what to do, or that they don’t have sufficient resources?
What are We Doing?

Industry “best practices”

Standards and compliance

But the trend is getting worse

Are we doing them wrong?
If we can do them better, will we be secure?
Consider the Source

Where do industry “best practices” come from?

Experiments?
Scientific models?

Intuition – “This should work”
  • Maybe it has worked in some circumstances
Popularity – “The 50 largest companies do it”
System Security Engineering - Capability Maturity Model (SSE-CMM, ISO/IEC 21827)

- “ISO/IEC 21827:2008 does not prescribe a particular process or sequence, but captures practices generally observed in industry.”

Building Security In Maturity Model (BSIMM)

- “We built the BSIMM entirely from observations we made by studying sixty-seven real software security initiatives. The BSIMM does not tell you what you should do; instead, it tells you what everyone else is actually doing.”
Cargo Cult

Replacement of content by style or magical thinking
Cargo Cult Cybersecurity

Copying security practices or techniques, or applying security design principles, without understanding how they work or the context in which they work.
From the point of view of those who depend on them

http://www.nedmartin.org/v3/amused/how-planes-fly
Not Unexpected Result

Major companies hacked in 2014:

That was easy.
Compliance vs. Security
Security is (usually) not the mission
Security may interfere with the mission
Security is a cost sink and often an afterthought
To Be Fair to Ourselves

What happens when you build a house on a foundation of sand?
We have to protect systems and networks often developed without security in mind
• And we usually can’t change them
• And we don’t get enough resources
Compliance is all we are allowed to do
• It’s how “security” is measured

But that implies that there is a “right way”
What is the “Right Way”? 

How can we know what that “right way” is?

How can we be better than “best practices”? 
Cybersecurity education should teach how to differentiate between cargo cult security and real security

Cybersecurity education should teach cybersecurity engineering
What is Cybersecurity?

Cybersecurity definition:

**Trustworthy control of authorized access by people to information in computer systems**

(or by programs working on behalf of people)
What is Cybersecurity Engineering?

Cybersecurity engineering: A field of practice that combines techniques of systems engineering, operational security, software engineering, and acquisition in order to develop processes, tools, and measures that help protect digital information.
Why Cybersecurity Engineering?

The only way to stay ahead of the curve

Depending on understanding the latest malware means you are always playing catch up with adversaries

Compliance always lags behind reality

Training in fundamentals prepares for whatever turns up and is never obsolete
Some Foundations of Cybersecurity Engineering

Difference between and importance of:
- Policy
- Mechanism
- Assurance

Reference monitor concept
Severe Cybersecurity Workforce Shortage!

Cybersecurity job market to suffer severe workforce shortage

Cybersecurity's hiring crisis: A troubling trajectory

Cybersecurity talent: Worse than a skills shortage, it’s a critical gap

Shortage of Cybersecurity Professionals Poses Risk to National Security

Cybersecurity Skills Shortage Panic in 2015?
CIOs and CISOs today know that that being attacked is a matter of if, but when. With the frequency of attacks growing exponentially, businesses need to be confident that candidates have the right skills and knowledge to address cybersecurity incidents from their first day on the job. At the same time, cybersecurity professionals need hands-on training to keep their skills sharp as adversaries develop new technical and creative tactics for attack. The time is now to reshape cybersecurity.

"James Gosler," eWeek continued, "a cyber-security specialist who worked at the Central Intelligence Agency, has argued that the United States needs some 30,000 technical cybersecurity workers, essentially hackers."

Hoff told ZDNet that vendors are experiencing difficulty finding suitable candidates "in a highly competitive job market that have the required experience in a number of emerging disciplines such as advanced malware detection/mitigation, reverse engineering, forensics."
Why Would That Help?

What proof do we have that simply hiring more people with “hacker” skills would solve this urgent problem?

- Are there any successful, fully staffed examples?
- If people are not doing the right thing, will more people doing the same thing be better?

Malware detection and reverse engineering, forensics, incident handling are all reactive

- Implying that we are doing as well as possible with securing our systems up front?
Where are we going to find 30,000 Hackers?

How do we train so many people in these very specific skills?

DHS has “National Initiative for Cybersecurity Careers and Studies”

NIST has “National Initiative for Cybersecurity Education”
Some NSA/DHS “centers of academic excellence” IA programs
  • List of required courses

Many highly specialized cert prep courses
  • E.g., SANS

Collections of cert prep courses
  • Some (many? most?) MS and certificate programs
  • At the end of the program, you have an “MS” and a handful of certs
Technicians and Engineers

Engineers

- Apply science and mathematics to solve problems
- Design processes, measures, and tools
- Capable of adapting processes to new situations
- Must understand why as well as how

Technicians

- Focused primarily on how
- Follow processes created by engineers
- Generally don’t deviate from accepted processes
The current concern over cybersecurity could easily abate, driven by new technology and more secure architectures. Pushing too many people into the profession now could leave an overabundance of highly trained and narrowly skilled individuals.

Why That is a Problem
Why That is a Problem
Cargo Cult Cybersecurity Education

Teaching specific security practices and techniques without adequately explaining the context in which they work, but with the expectation that students will somehow understand “security” when they are done.
Continued growth in near term of “cert prep”, technical training programs
• And lots of new certs

Gradual realization that hiring more pure technicians doesn’t appreciably improve security

Growing emphasis on teaching cybersecurity as a field of engineering
• Growing emphasis developing secure systems
The Future of Cybersecurity Education

Being Better than “Best Practices”

Mark Heckman, Ph.D., CISSP, CISA
Center for Cyber Security Engineering and Technology
University of San Diego