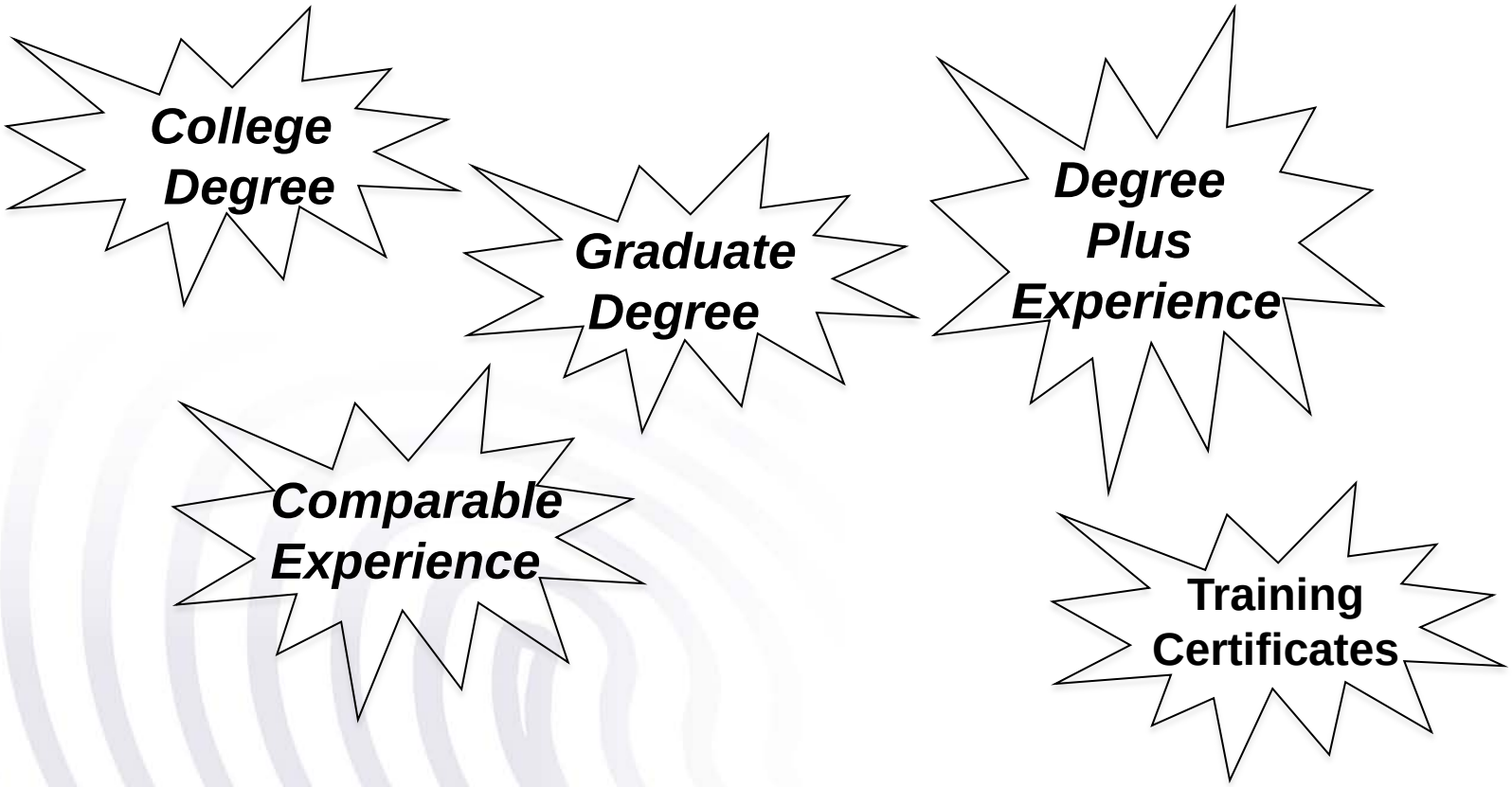
emēsec
INFORMATION ASSURANCE

Adapting and Establishing New Education Strategies to the Continuously Evolving Cyber Terrain

Grayson L. Koogle
Vice President – Operations
EmeSec Incorporated

I Remember When ____Was Enough



And Now . . .

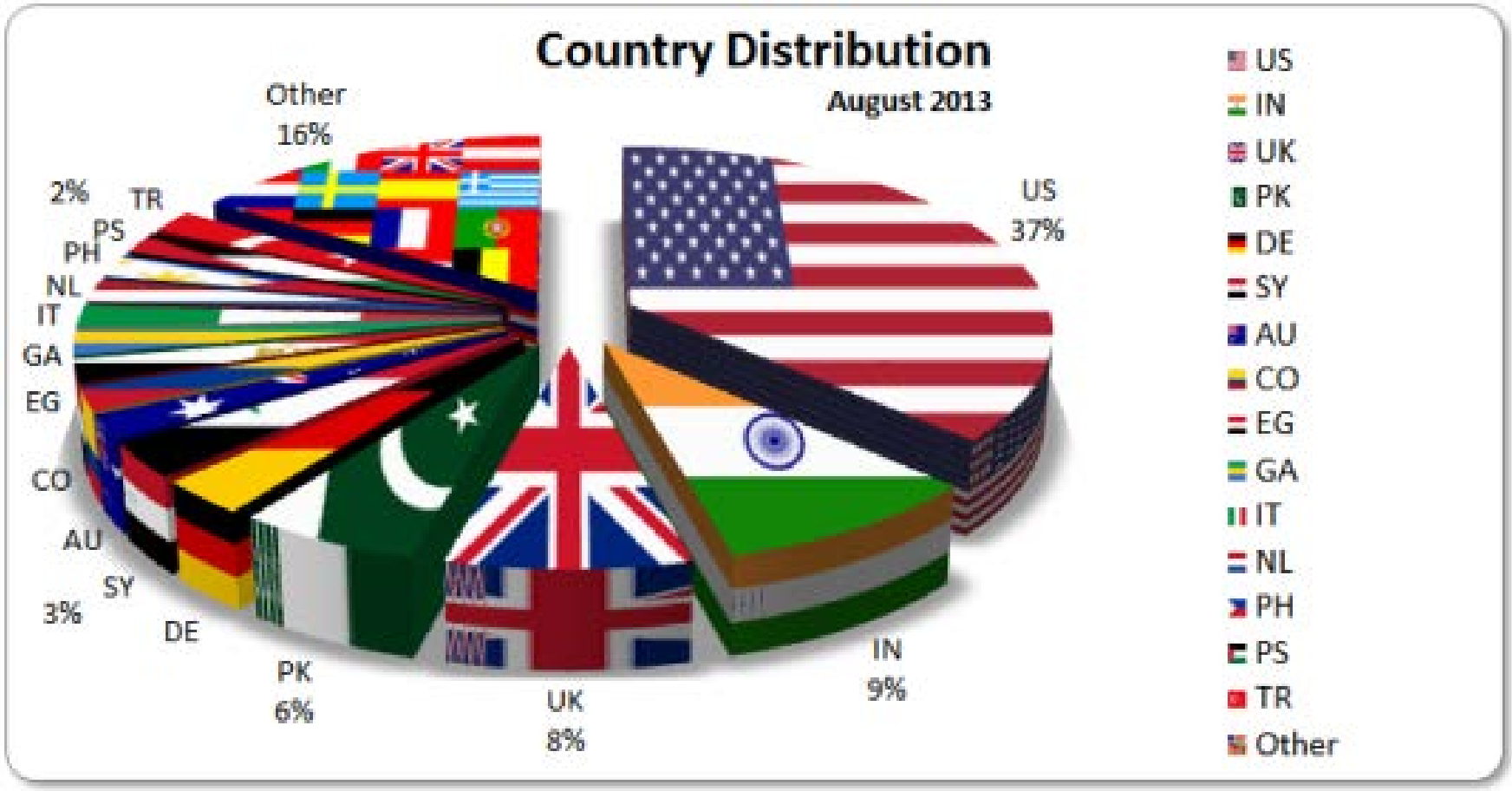

WHAT DO YOU MEAN THERE'S NO MORE BUDGET FOR TRAINING?!? HOW DO I GET MY PDUs?
PM

Setting the Stage

"With an increased level of cyber crime and even internet espionage and terrorism from other countries, the demand for cyber security experts is likely to increase. This high paying field is demanding **and requires security experts to constantly keep up with growing computer, attacks and changing technology.** "

(eHow.com – "How to Get a Cyber Security Job")

CYBER ATTACKS/SECURITY BREACHES BY COUNTRY



Examples - Cyber Attacks/Security Breaches
February – March 2014

- 1 February - Bell Canada (40,000 users affected)
- 5 February - St. Joseph Health System (400,000 users affected)
- 14 February - Forbes (1 million records leaked)
- 7 March - Navy Marine Corps Intranet (800,000 users)

Four Years Ago

"The current generation of cybersecurity professionals tends to be zealots; people who are passionate about computers, coding and hacking, who started out as teenagers spending hours in the basement playing with gadgets, educating themselves to the point that where they are co-opted by organizations where they find themselves bored."

"The next generation will be young professionals who choose cybersecurity as a career path and enter the field with a different set of expectations."

"We'll lose something along with the passion, but they'll be able to pay the mortgage and we'll have the minds and hands we need to keep watch on our cyber defenses."

(GCN-William Jackson, 2010)

The Value of Certifications

- From the Cyber Security Company Perspective
  - Attaining/maintaining a professional workforce with applicable current certifications is a business imperative in order to stay competitive (and profitable) in the market place.
  - Documents their experience and expertise in the understanding of and countering of current and projected cyber threats.
  - Proactive training environment /program is required to keep up with continuously increasing cyber threat technologies.

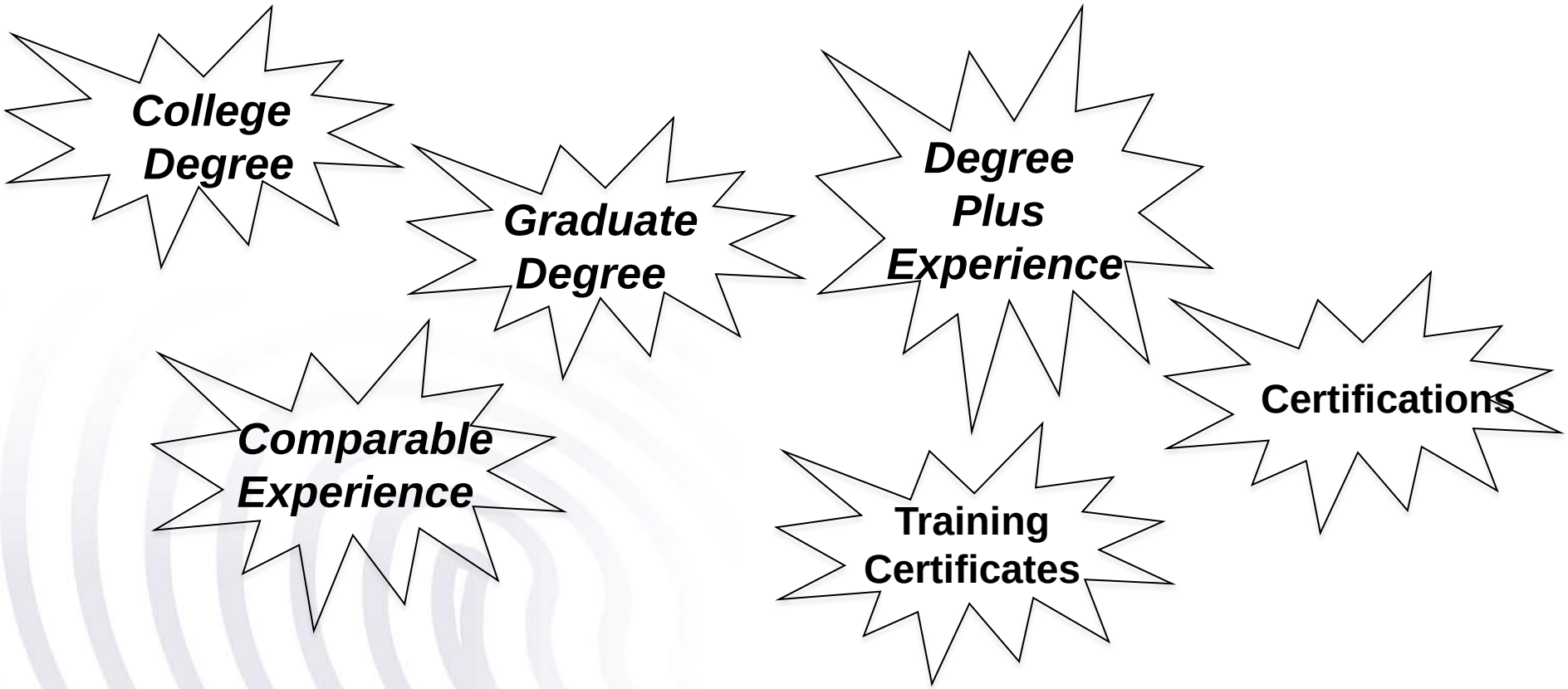
- From the Individual Perspective
  - Certifications demonstrate that the individual has the requisite training and understands the issues.
  - That said . .. certifications qulckly become outdated as threat technologies continue to evolve and change....requiring additional/continuous education to maintain the applicable certification(s) AND related experience.
  - Perception that the more certifications and related experience, the more marketable he/she is . . .and the resultant tendency to go where the money is. . . .

The Current Business Reality

- In Commercial work, value (salary/rates) driven by need for IA services, competition and available resources.

- In DoD/Government work, value (salary/rates) limited by fiscal/contractual environment.

I Remember When ____Was Enough



CERTIFICATIONS ARE NOT ENOUGH

Certifications

+

Continuing Education

+

RELATED WORK EXPERIENCE

DoD 8570 – IA Workforce Improvement Program

- "Develop a DoD IA workforce with a common understanding of the concepts, principles, and applications of IA ...to enhance protection and availability of DoD information, information systems, and networks."
- "Implement a formal IA workforce skill development and sustainment process, comprised of resident courses, distributive training, blended training, supervised on the job training (OJT), exercises, and certification/recertification."
- "Augment and expand on a continuous basis the knowledge and skills obtained through experience or formal education."

Standard Classroom Training ?
vs
Online Training ?

Training During Work Week ?
vs
Training During Off Hours ?

"In House" Developed Training?
vs
"Outside" Contracted Training ?

"COOPERATIVE" CYBER SECURITY TRAINING ENVIRONMENTS

- TWO EXAMPLES -

Lesson Learned
Remaining Current with Cyber Technology

"Due to the nature of the Information Technology Industry, the Government requires the skill level of the staff to remain current with technology. The contractor will be responsible, at no additional cost to the government, for ensuring that their personnel remain up to date for current, next generation and any future releases of COTS technologies used by _____."

Lesson Learned
Training Integrated into the Working Environment

Government 24/7 cyber security operations facility with integrated government/contractor watch teams.

Online web based training related to specific cyber security certifications (ex. CEH related training) and other security courses related to the 24/7 facility operations.

Training approved on a case by case basis for all qualified watch personnel including contractors during off watch hours or during watch assignment with the approval of the watch supervisor.

CLOSING THOUGHTS

- Cloud and mobile technologies continue to evolve.
- “Cyber hackers” continue to advance in their capabilities to breach our infrastructures.
- Proactive and new approaches to cyber security training are required.

CYBER SECURITY TRAINING
- A CONTINUOUS UPHILL BATTLE-