WHY YOU SHOULD NOT GET A CISSP™©®

Timmay, with a dose of Jericho

Overview

- Introduction
- About the (ISC)2 and the CISSP
- (ISC)2 on Benefits of a CISSP
- What I Look For in a Certification
- How “Required” Is It?
- (ISC)2 Code of Ethics
- Conclusion

Introduction

- Background
- What this talk is not
- Why the CISSP?

About the (ISC)2 and the CISSP

- Headquartered in Palm Harbor, Florida
- Formed by individuals from different groups in 1988
- Re-formed (ISC)2 as a non-profit in 1989
- Common Body of Knowledge (CBK) finalized in 1992
- First CISSPs certified in 1994, with 300 “grandfathered” in
- ISO/IEC 17024 accreditation awarded in 2006

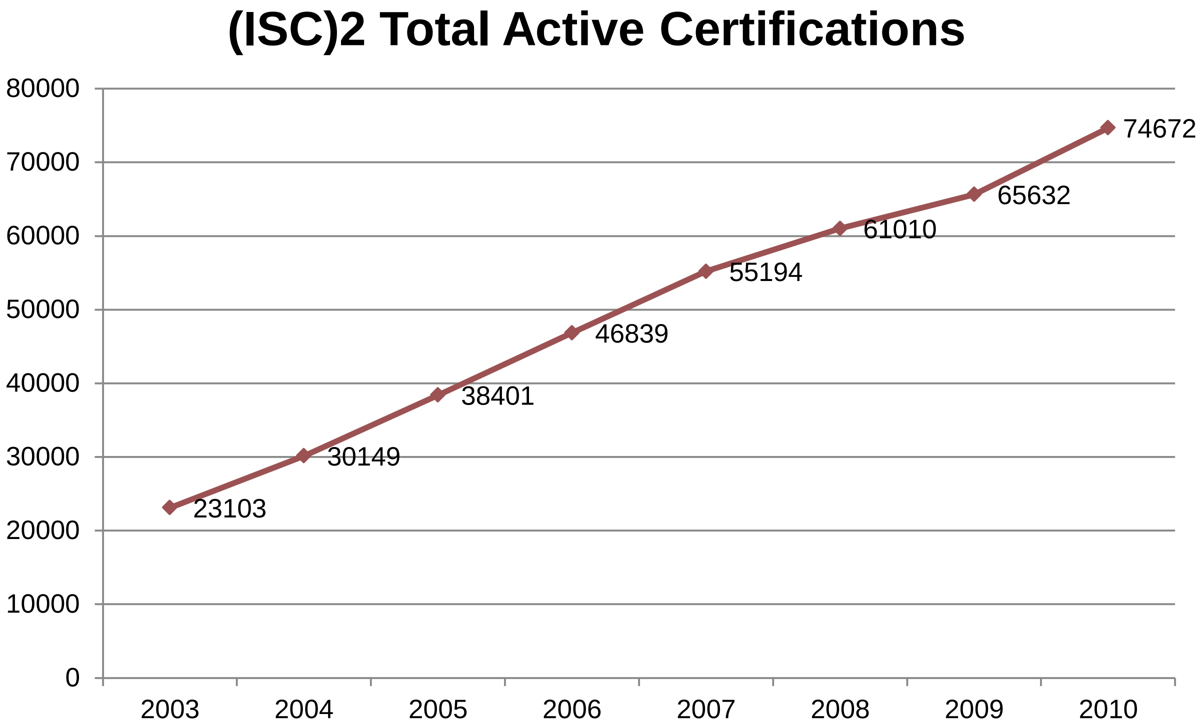
About the (ISC)2 and the CISSP

- Requirements:
  - A resume claiming 5 yrs in InfoSec, or 4 yrs with a combination of education/certifications
  - Endorsement from another CISSP
  - Claim to be committed to the (ISC)2 “Code of Ethics”
  - Claim to have a clean background
  - Submit continuing professional education (CPE) credits (stuff you claim to do) after certification
- Anyone see problems yet?

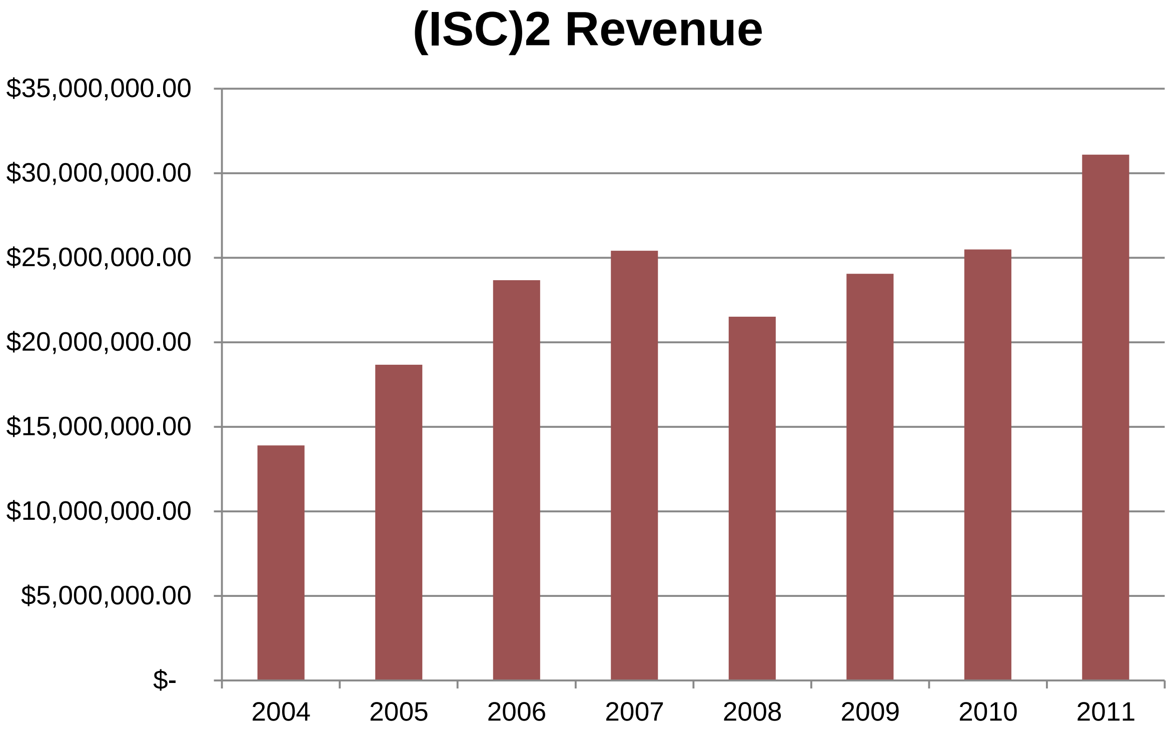
About the (ISC)2 and the CISSP

- The Test:
  - 250 multiple-choice question test
  - Six-hour time limit
  - 25 sample questions not graded
  - Passing score 700 out of 1000

People Are Passing



And (ISC)2 is Cleaning Up



(ISC)2 on Benefits of CISSP

- Career differentiator, with “enhanced credibility and marketability”
- Many business now “require” it
- “Earn 25% more than non-certified counterparts”
- Join an “elite network” of professionals
- “Access to discounted publications”

(ISC)2 on Benefits of CISSP

- Career differentiator, with “enhanced credibility and marketability”
  - Not easily proved or disproved
  - Marketability depends ½ on what is being marketed and ½ the market itself
  - Whether the market for CISSP-certified employees is so strong will be discussed later
  - There is a reason CISSP jokes abound in the Information Security industry

(ISC)2 on Benefits of CISSP

- Many business now “require” it
  - … we’ll talk more on this in a minute

(ISC)2 on Benefits of CISSP

- “Earn 25% more than non-certified counterparts”
  - Derived from a single document: the (ISC)2’s *Global Information Security Workforce Study*
  - $14K disparity between certified vs. non-certified respondents’ salaries in the US, amounting to 15%, 25% was a *global* average, including Asia.
  - Conducted by Frost & Sullivan on ten thousand people who both claimed to be InfoSec practitioners and also answered their spam

(ISC)2 on Benefits of CISSP

- Join an “elite network” of professionals
  - “Elite” professionals who managed a C on a cram-easy test?
  - “Elite” BS notwithstanding, I have never gained anything from this alleged network but spam and flame wars about what “DMZ” means
  - I don’t know anyone that has benefited from it, either
  - YMMV

(ISC)2 on Benefits of CISSP

- Access to discounted publications
  - Like their *Global Information Security Workforce Study.*
  - Yay

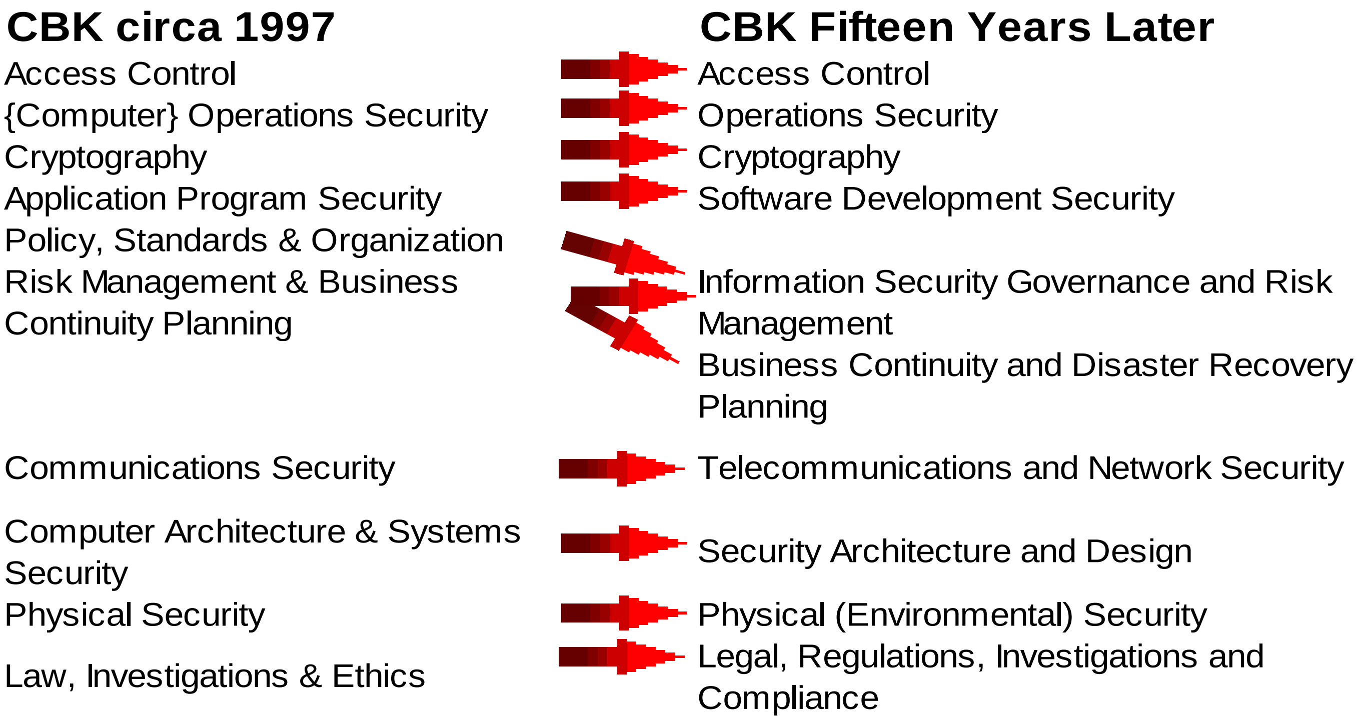
(ISC)2 on Benefits of CISSP for Employers

- Validates commitment and years of experience gained in the industry
  - Except that you only have to claim experience on a resume
- Requires Continuing Professional Education (CPE) credits to ensure that personnel keep their skills current
  - So the CISSP benefits the employer because it makes the employee submit CPE’s for the work that they do for the employer?

What I Look for in a Certification …

- Currency
- Relevance to the industry
- Applicability to the discipline
- Confidence-inspiring rigor?

Relevance: Dissecting the Aging CBK



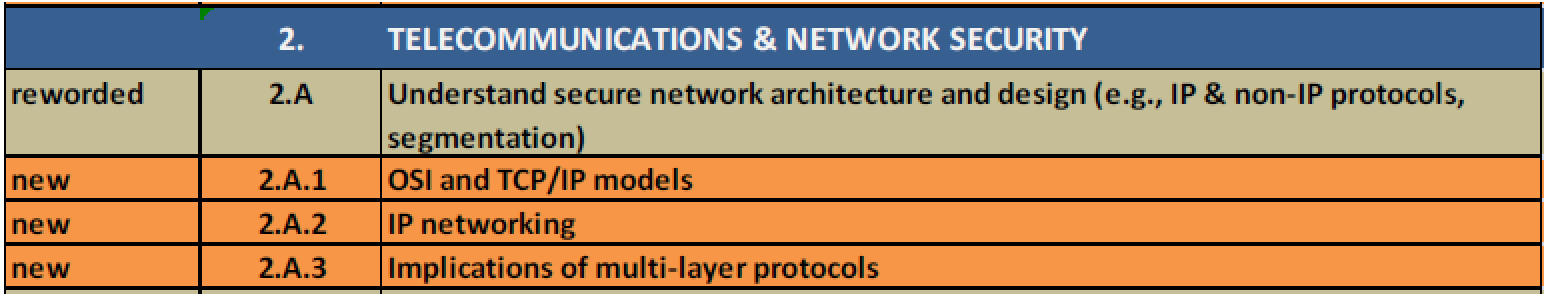
CBK circa 1997	CBK Fifteen Years Later
Access Control	Access Control
{Computer} Operations Security	Operations Security
Cryptography	Cryptography
Application Program Security	Software Development Security
Policy, Standards & Organization	Information Security Governance and Risk Management
Risk Management & Business Continuity Planning	Information Security Governance and Risk Management Business Continuity and Disaster Recovery Planning
Communications Security	Telecommunications and Network Security
Computer Architecture & Systems Security	Security Architecture and Design
Physical Security	Physical (Environmental) Security
Law, Investigations & Ethics	Legal, Regulations, Investigations and Compliance

Source: Wayback Machine

Relevance: Dissecting the Aging CBK

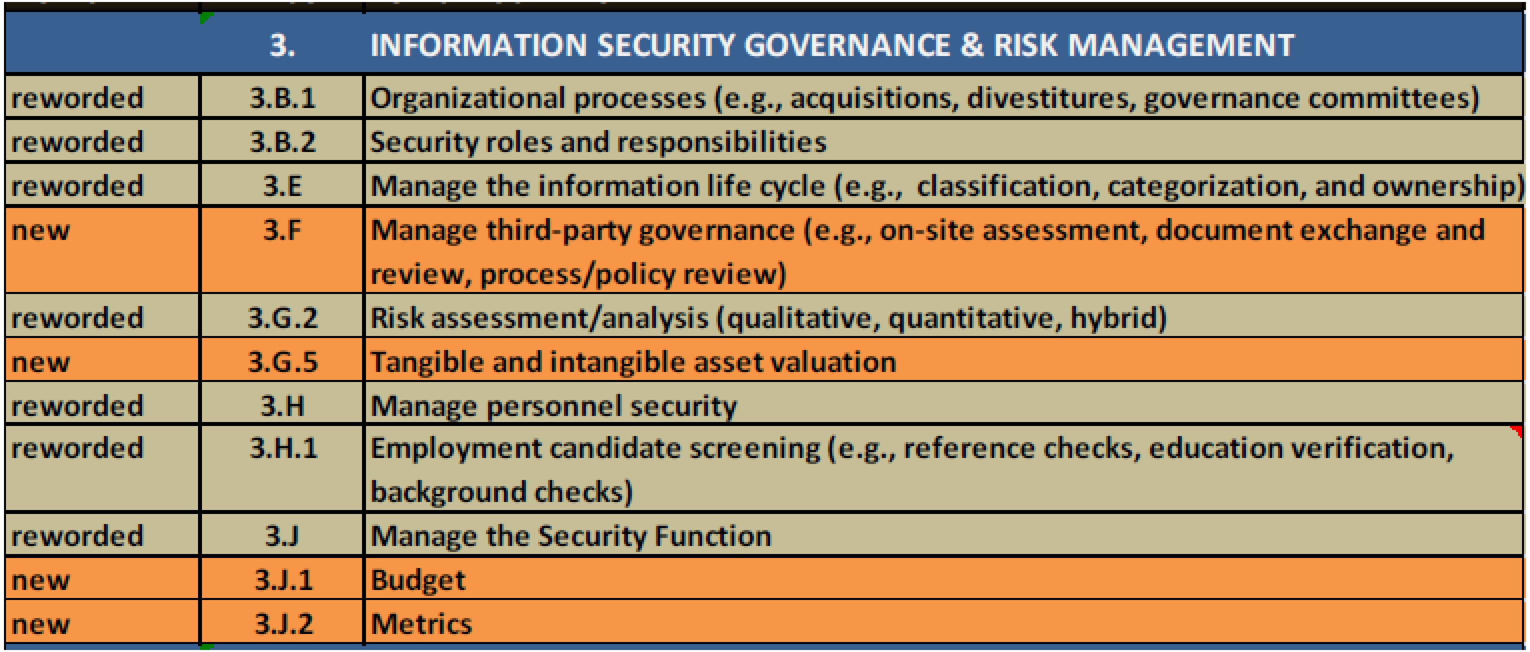
- CBK Committee
- Meets annually
- Determines material to be added, reworded, or removed
- Communicates results in the Candidate Information Bulletin (CIB)
- Let’s look at the most recent one …

Relevance: Dissecting the Aging CBK



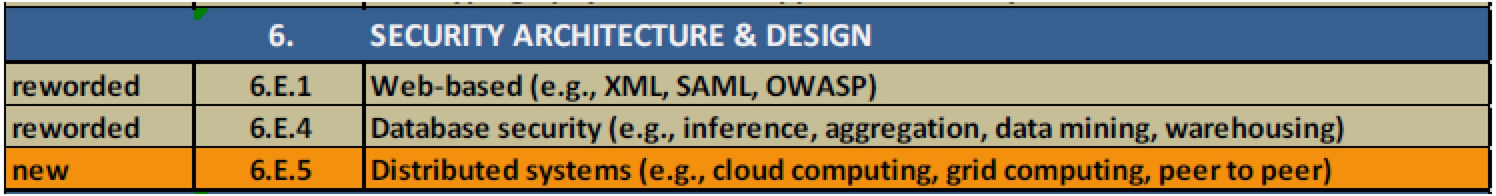
	2.	TELECOMMUNICATIONS & NETWORK SECURITY
reworded	2.A	Understand secure network architecture and design (e.g., IP & non-IP protocols, segmentation)
new	2.A.1	OSI and TCP/IP models
new	2.A.2	IP networking
new	2.A.3	Implications of multi-layer protocols

Relevance: Dissecting the Aging CBK



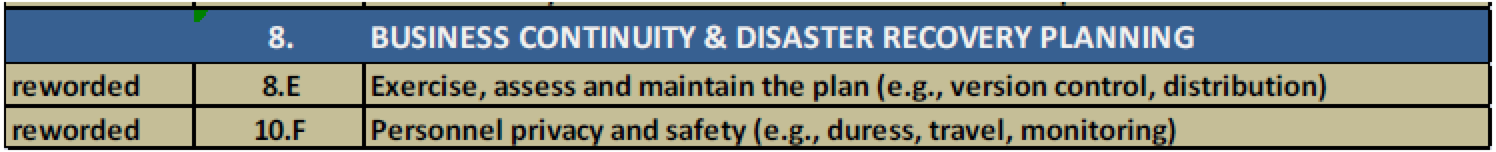
	3.	INFORMATION SECURITY GOVERNANCE & RISK MANAGEMENT
reworded	3.B.1	Organizational processes (e.g., acquisitions, divestitures, governance committees)
reworded	3.B.2	Security roles and responsibilities
reworded	3.E	Manage the information life cycle (e.g., classification, categorization, and ownership)
new	3.F	Manage third-party governance (e.g., on-site assessment, document exchange and review, process/policy review)
reworded	3.G.2	Risk assessment/analysis (qualitative, quantitative, hybrid)
new	3.G.5	Tangible and intangible asset valuation
reworded	3.H	Manage personnel security
reworded	3.H.1	Employment candidate screening (e.g., reference checks, education verification, background checks)
reworded	3.J	Manage the Security Function
new	3.J.1	Budget
new	3.J.2	Metrics

Relevance: Dissecting the Aging CBK



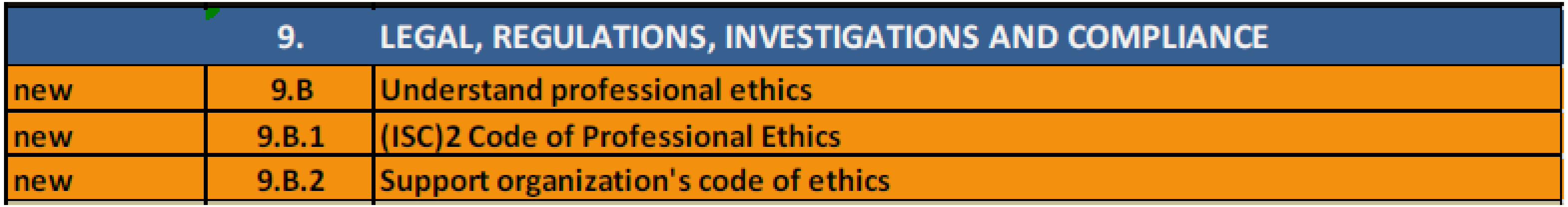
	6.	SECURITY ARCHITECTURE & DESIGN
reworded	6.E.1	Web-based (e.g., XML, SAML, OWASP)
reworded	6.E.4	Database security (e.g., inference, aggregation, data mining, warehousing)
new	6.E.5	Distributed systems (e.g., cloud computing, grid computing, peer to peer)

Relevance: Dissecting the Aging CBK



	8.	BUSINESS CONTINUITY & DISASTER RECOVERY PLANNING
reworded	8.E	Exercise, assess and maintain the plan (e.g., version control, distribution)
reworded	10.F	Personnel privacy and safety (e.g., duress, travel, monitoring)

Relevance: Dissecting the Aging CBK



	9.	LEGAL, REGULATIONS, INVESTIGATIONS AND COMPLIANCE
new	9.B	Understand professional ethics
new	9.B.1	(ISC)2 Code of Professional Ethics
new	9.B.2	Support organization's code of ethics

Relevance: Dissecting the Aging CBK

“The CISSP CBK looks barely acceptable on the surface, but in practice it fails miserably to reflect issues security professionals actually handle.”

- Richard Bejtlich, Mandiant (and Tao Security)

Rigor: Wanna Pass the CISSP Fast?

- Don’t worry!
  - There are literally thousands of 7-day “CISSP Boot Camp” services!
  - Google that string for 134,000 hits!
  - 93% pass rate!
  - No prerequisites!
  - This is the source of an insane amount of spam!
  - Why else would I know who Shon Harris is?!

Rigor: Wanna Pass the CISSP Fast?

- What they know that hiring managers don’t
    - The CBK is too broad for the questions to go into depth
    - This makes it predictable
    - This means that it can’t get hard enough to keep idiots from cramming and passing
    - This means any idiot can pass

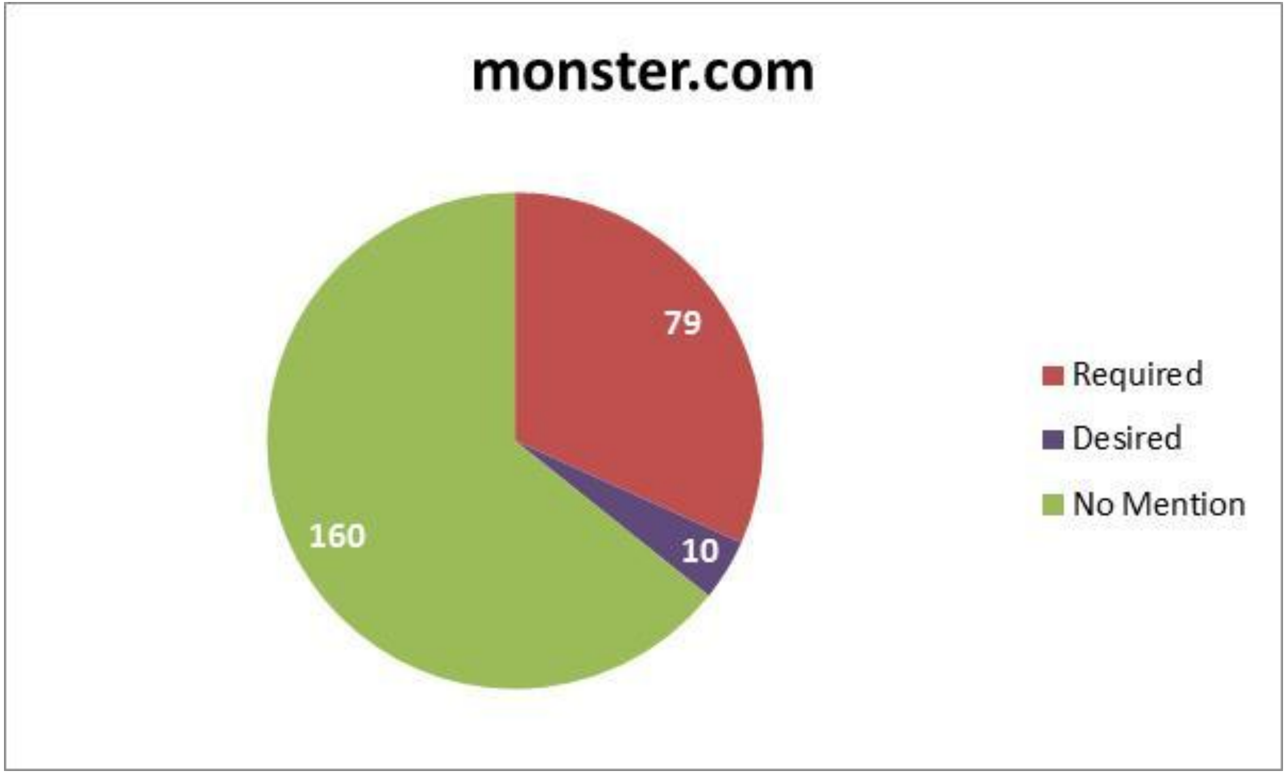
Demand for CISSPs

- “You can’t get a job in InfoSec without a CISSP”
- “It’s required to get you past the HR screening”

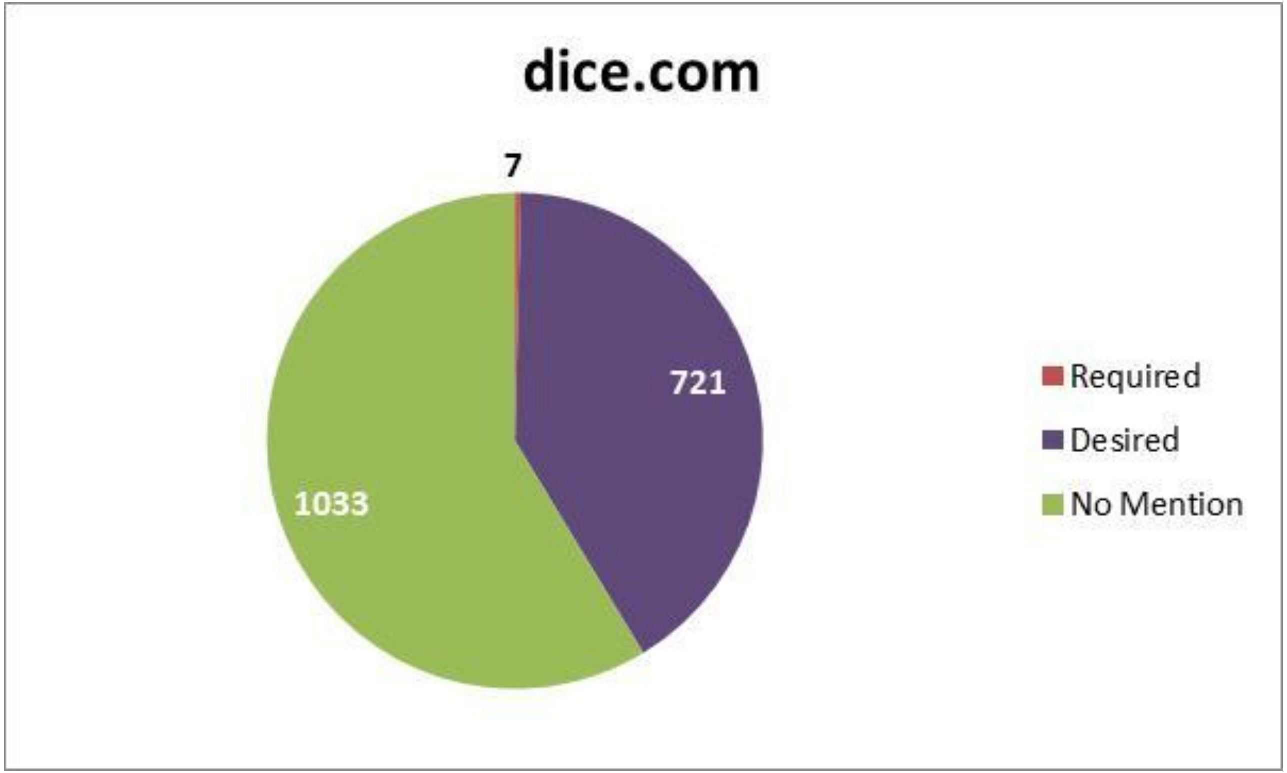
How “Required” Is It?

- Let’s look at job postings!
  - No geographic restrictions
  - A: Search on string “information security”
  - B: Filter on string “CISSP”
  - C: Add further filter language for CISSP as a mandatory requirement
  - Subtract B from A to get InfoSec postings that don’t mention it at all
  - Subtract C from B to get mentions of CISSP that don’t require it
  - C indicates that the certificate is required
- Not perfect, but it’s good for a snapshot in time …

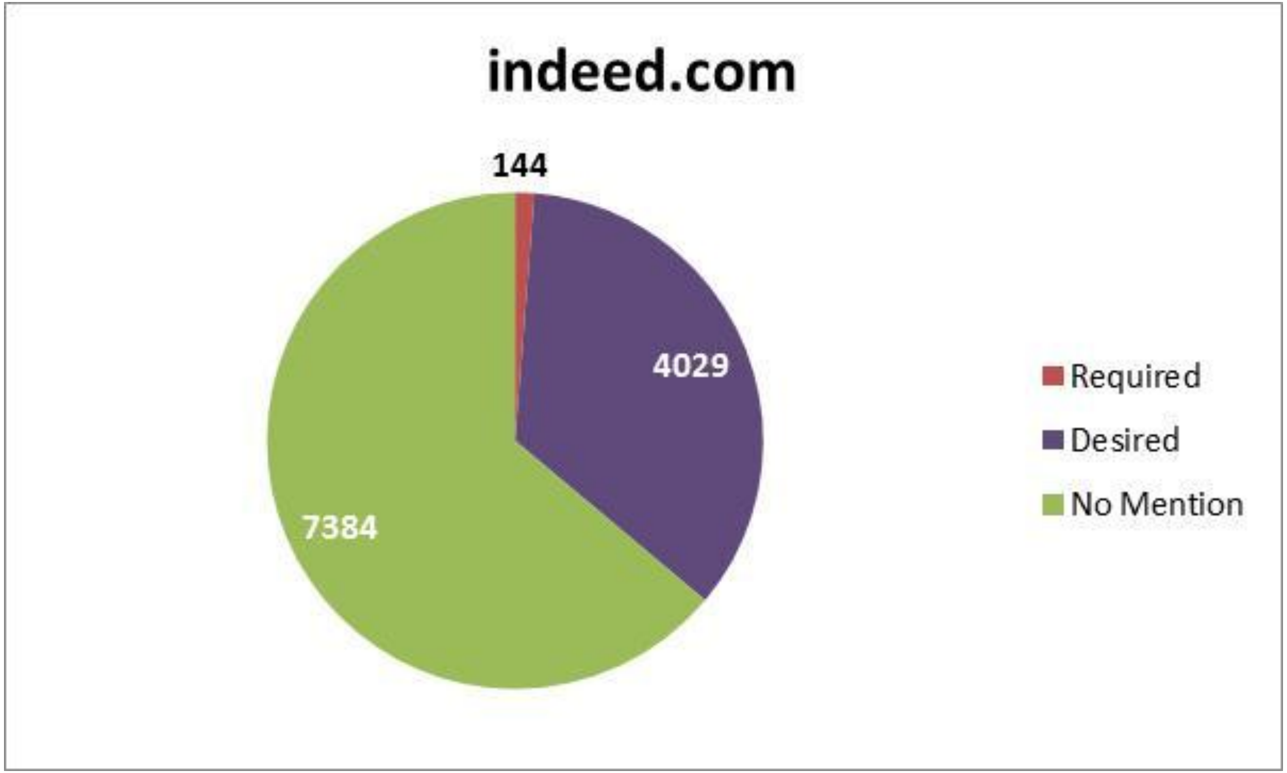
How “Required” Is It?



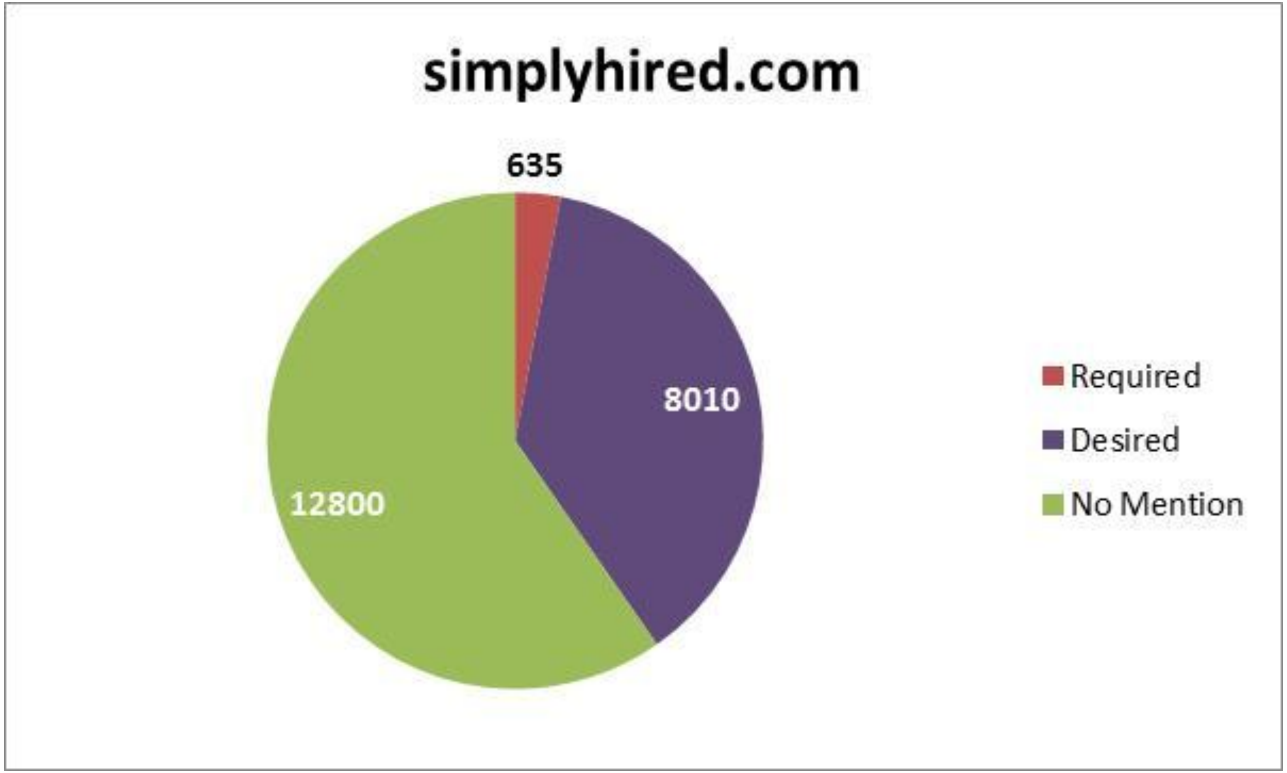
How “Required” Is It?



How “Required” Is It?



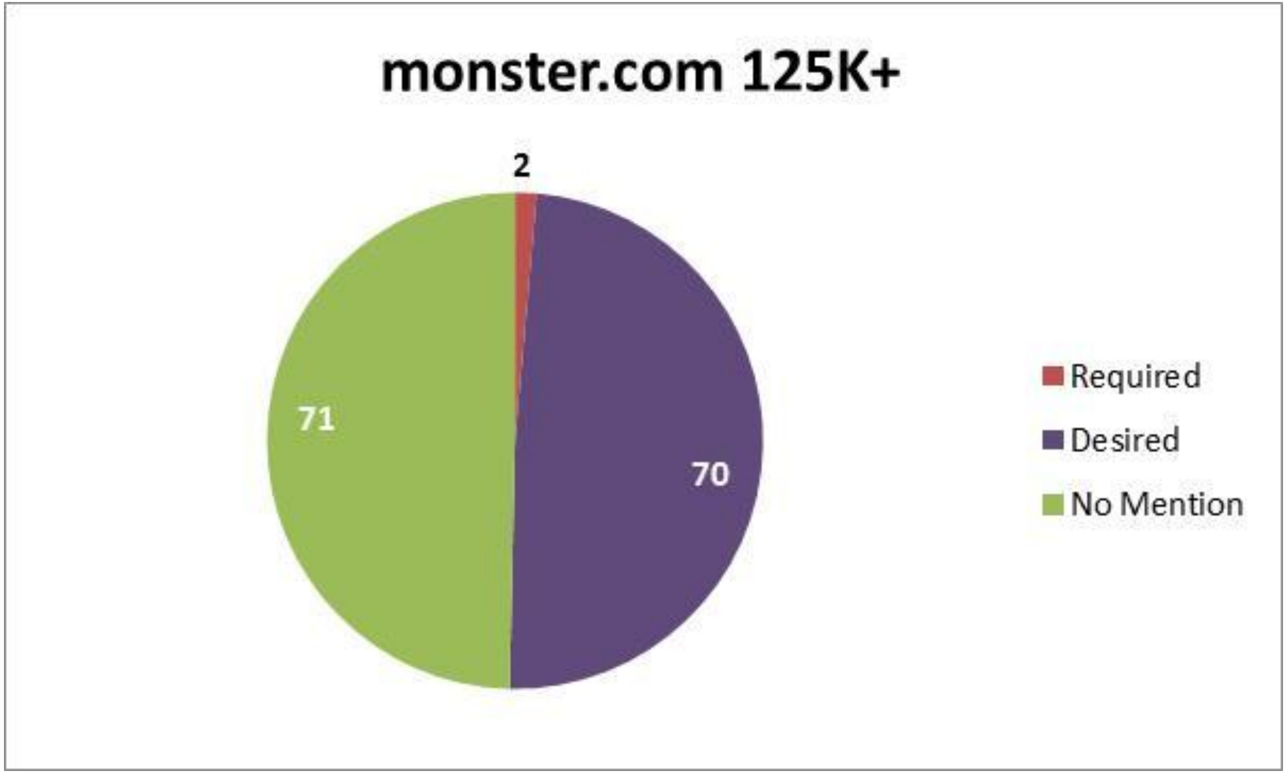
How “Required” Is It?



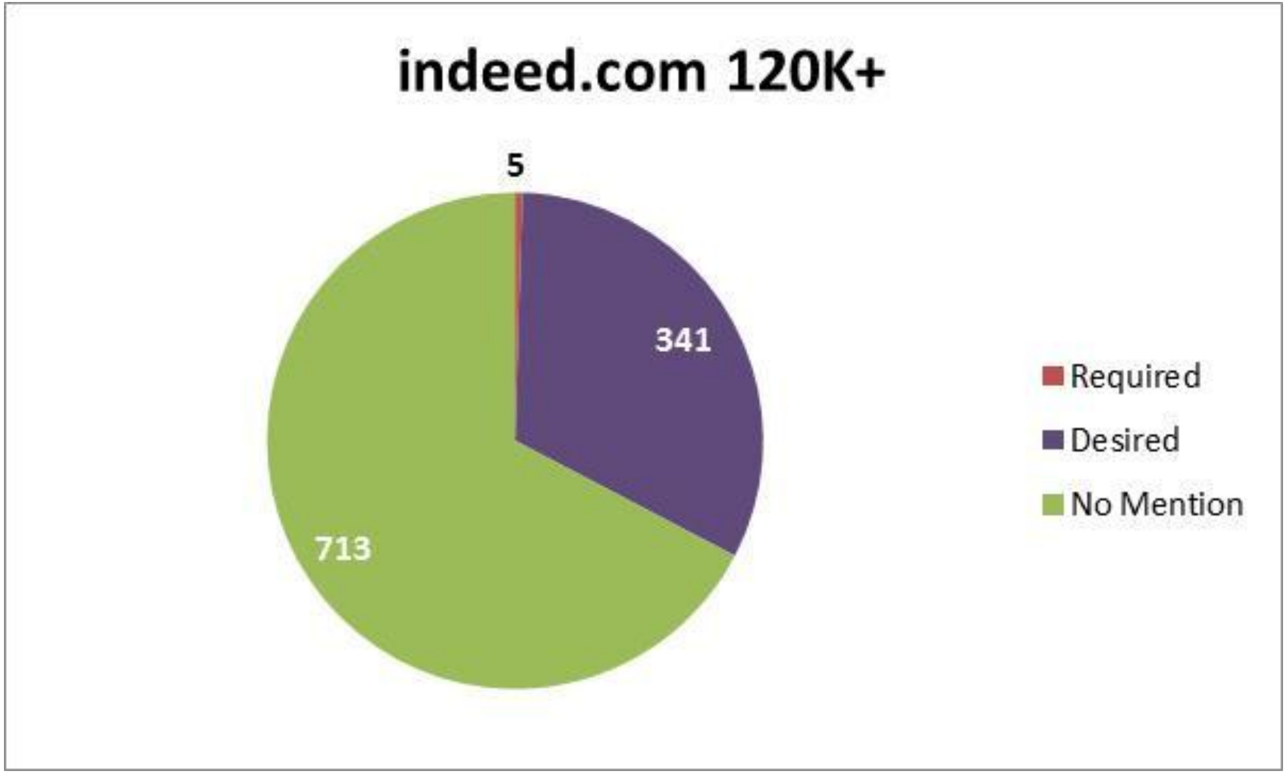
So it’s Just Required for Mad $?

- “I doubled my income with a CISSP. It’s the *high dollar* jobs that require it. Cuz it’s so hard.”
- Some of the job boards let you filter on salary …

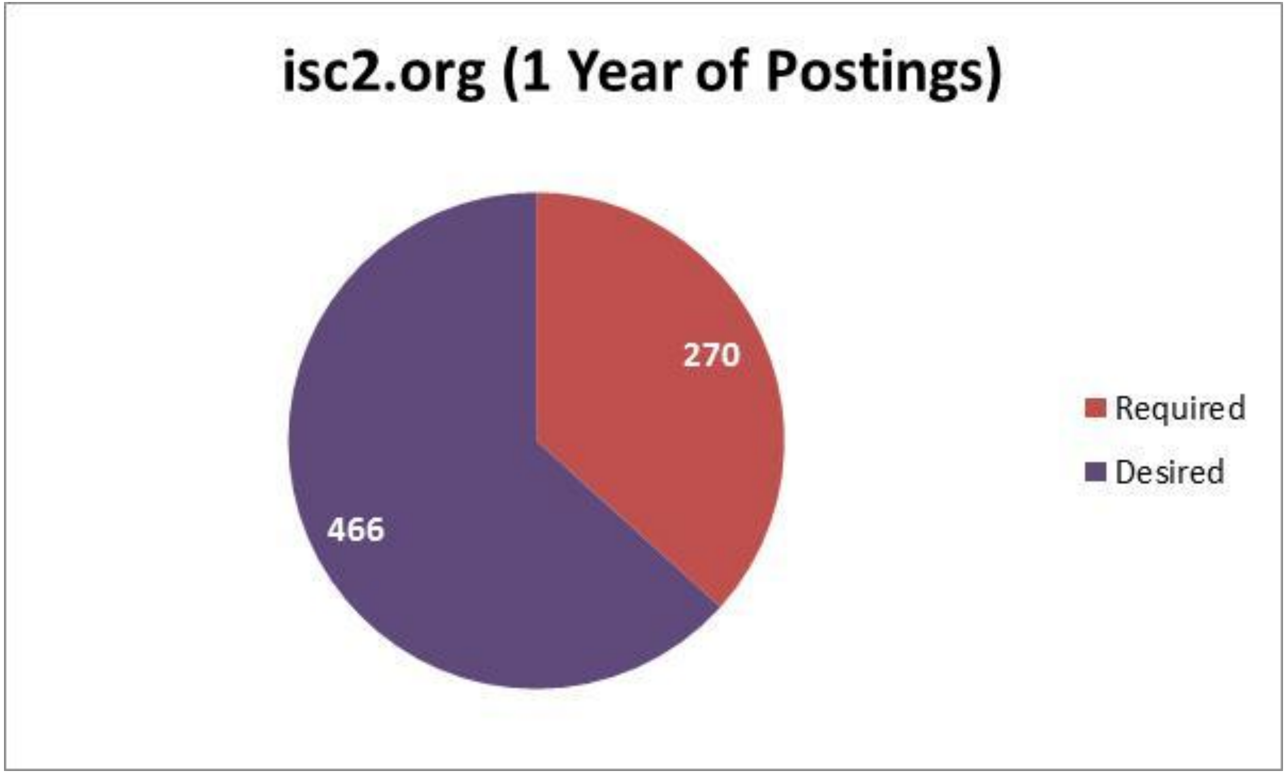
So it’s Just Required for Mad $?



So it’s Just Required for Mad $?



And My Favorite …



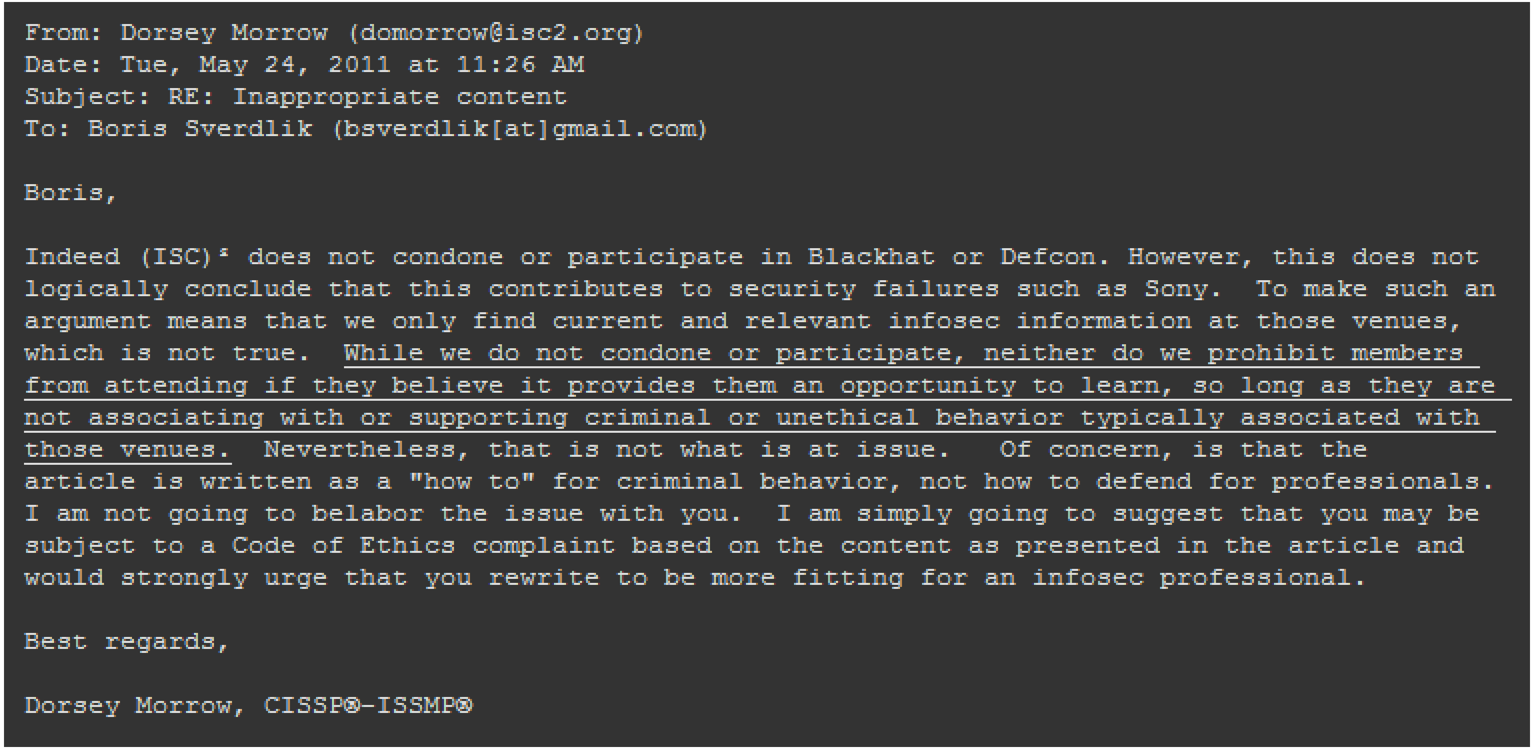
(ISC)2 Code of Ethics

- Protect society, the commonwealth, and the infrastructure
- Act honorably, honestly, justly, responsibly, and legally
- Provide diligent and competent service to principals
- Advance and protect the profession

(ISC)2 Code of Ethics

- Hypocritical ethics
  - “Competence” used frequently (we all have stories …)
  - Protecting the org trumps the code of ethics
  - Learn about bad guys but don’t go near them?

(ISC)2 Code of Ethics



From: Dorsey Morrow (domorrow@isc2.org)
Date: Tue, May 24, 2011 at 11:26 AM
Subject: RE: Inappropriate content
To: Boris Sverdlik (bsverdlik[at]gmail.com)

Boris,

Indeed (ISC)^2 does not condone or participate in Blackhat or Defcon. However, this does not logically conclude that this contributes to security failures such as Sony. To make such an argument means that we only find current and relevant infosec information at those venues, which is not true. While we do not condone or participate, neither do we prohibit members from attending if they believe it provides them an opportunity to learn, so long as they are not associating with or supporting criminal or unethical behavior typically associated with those venues. Nevertheless, that is not what is at issue. Of concern, is that the article is written as a "how to" for criminal behavior, not how to defend for professionals. I am not going to belabor the issue with you. I am simply going to suggest that you may be subject to a Code of Ethics complaint based on the content as presented in the article and would strongly urge that you rewrite to be more fitting for an infosec professional.

Best regards,

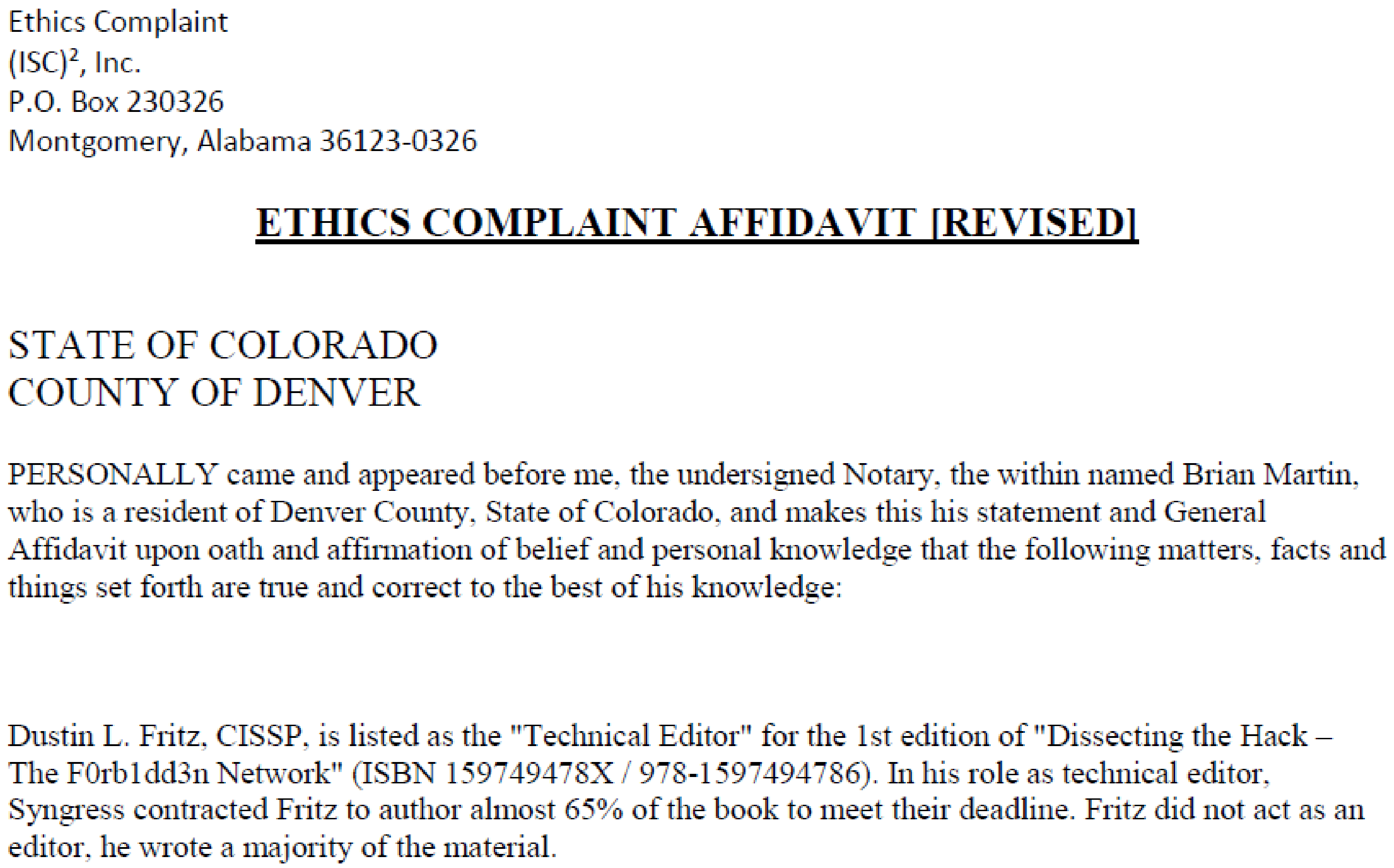
Dorsey Morrow, CISSP®-ISSMP®

(ISC)2 Code of Ethics

- Complaint procedure
  - Must be notarized
  - Must be snail-mailed
  - Entire process likely to take 90+ days
  - Your name likely to be disclosed to offender
  - Must show “standing” which is arbitrary and murky
  - Entire burden of proof on complainant

(ISC)2 Code of Ethics

- Example of complaint procedure
  - Filed plagiarism complaint against Dustin Fritz (tech editor who also wrote material for a book)
  - Included URLs as evidence
  - One URL had him admitting to the plagiarism
  - (ISC)2 responded insufficient evidence
  - Re-filed with affidavit from book author attesting to plagiarism
  - (ISC)2 denied ethics complaint
  - Moral of the story: plagiarizing and admitting to it is ethical



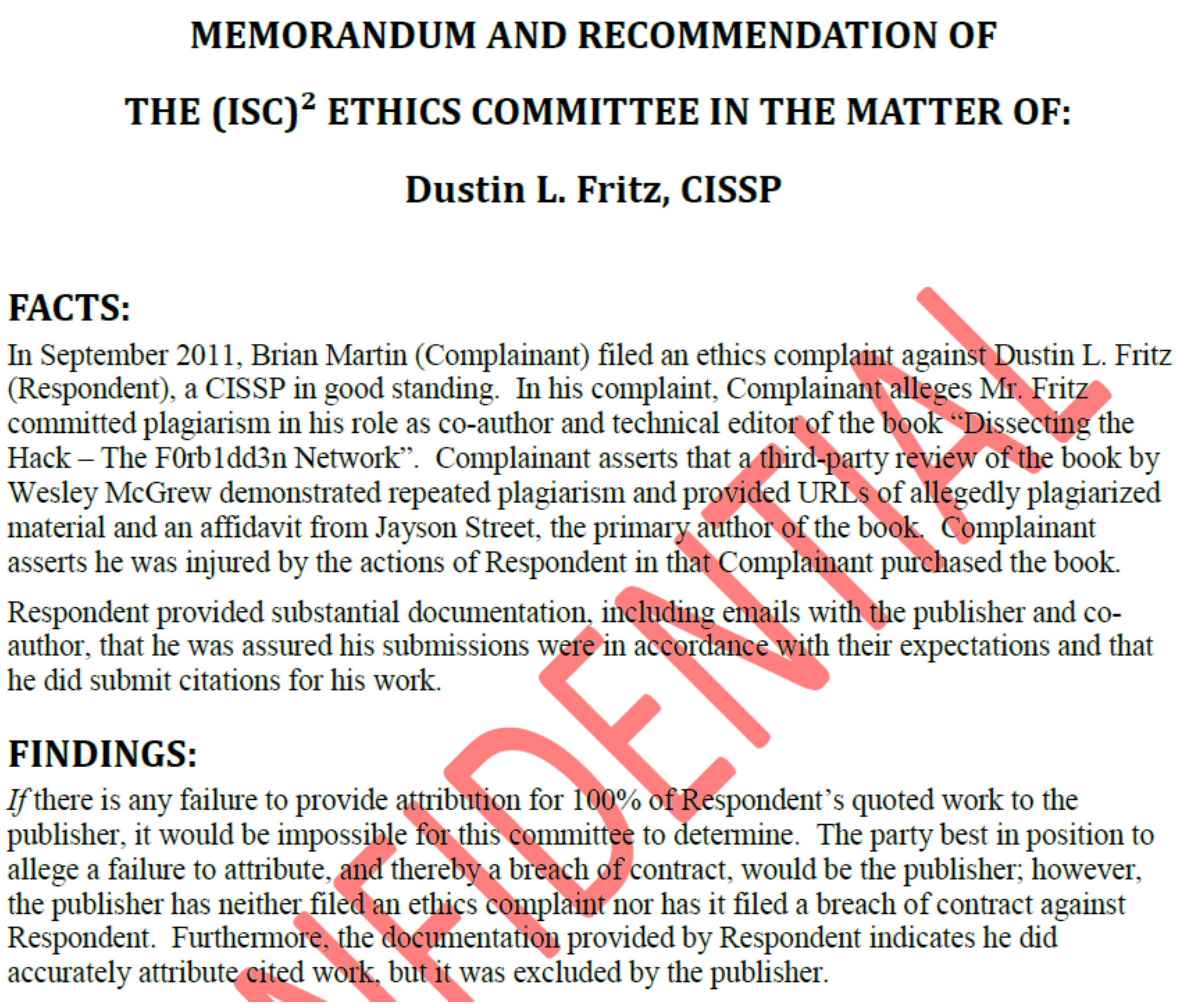
Ethics Complaint
(ISC)^2, Inc.
P.O. Box 230326
Montgomery, Alabama 36123-0326

ETHICS COMPLAINT AFFIDAVIT [REVISED]

STATE OF COLORADO
COUNTY OF DENVER

PERSONALLY came and appeared before me, the undersigned Notary, the within named Brian Martin, who is a resident of Denver County, State of Colorado, and makes this his statement and General Affidavit upon oath and affirmation of belief and personal knowledge that the following matters, facts and things set forth are true and correct to the best of his knowledge:

Dustin L. Fritz, CISSP, is listed as the "Technical Editor" for the 1st edition of "Dissecting the Hack – The F0rb1dd3n Network" (ISBN 159749478X / 978-1597494786). In his role as technical editor, Syngress contracted Fritz to author almost 65% of the book to meet their deadline. Fritz did not act as an editor, he wrote a majority of the material.



MEMORANDUM AND RECOMMENDATION OF

THE (ISC)^2 ETHICS COMMITTEE IN THE MATTER OF:

Dustin L. Fritz, CISSP

FACTS:

In September 2011, Brian Martin (Complainant) filed an ethics complaint against Dustin L. Fritz (Respondent), a CISSP in good standing. In his complaint, Complainant alleges Mr. Fritz committed plagiarism in his role as co-author and technical editor of the book "Dissecting the Hack – The F0rb1dd3n Network". Complainant asserts that a third-party review of the book by Wesley McGrew demonstrated repeated plagiarism and provided URLs of allegedly plagiarized material and an affidavit from Jayson Street, the primary author of the book. Complainant asserts he was injured by the actions of Respondent in that Complainant purchased the book.

Respondent provided substantial documentation, including emails with the publisher and co-author, that he was assured his submissions were in accordance with their expectations and that he did submit citations for his work.

FINDINGS:

If there is any failure to provide attribution for 100% of Respondent's quoted work to the publisher, it would be impossible for this committee to determine. The party best in position to allege a failure to attribute, and thereby a breach of contract, would be the publisher; however, the publisher has neither filed an ethics complaint nor has it filed a breach of contract against Respondent. Furthermore, the documentation provided by Respondent indicates he did accurately attribute cited work, but it was excluded by the publisher.

The Timmay Code of Ethics

- Refuse to need anyone else’s code of ethics forced on you
- You’re part of a community: act like it
- Don’t let anyone convince you that being taught skills and being influenced ethically are the same thing
- Take your *real* credentials seriously
- Be offended when someone pees in the pool

Conclusion

- The CISSP doesn’t deliver on its claimed benefits
- The CISSP doesn’t live up to sensible standards for a certification
- Management confidence in the relevance of the CBK and rigor of the CISSP exam is misplaced and unwarranted
- Avoiding this certification can’t hurt your career as bad as contributing to this dilutory exercise hurts the entire community
- How many Shon Harris books can you buy for thirty pieces of silver?