The Future Of Information Security

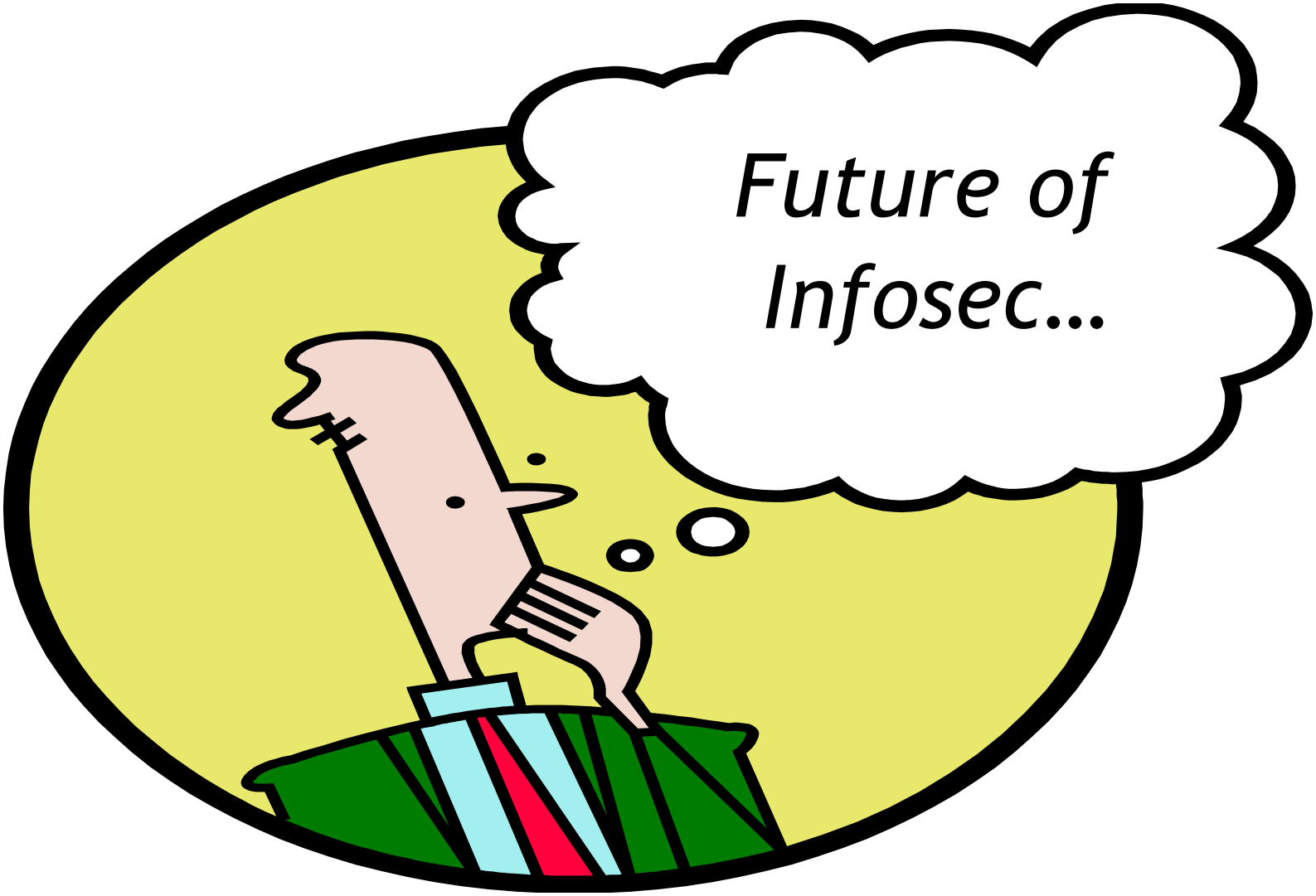
Ron Woerner, CISSP, CEH, CHFI

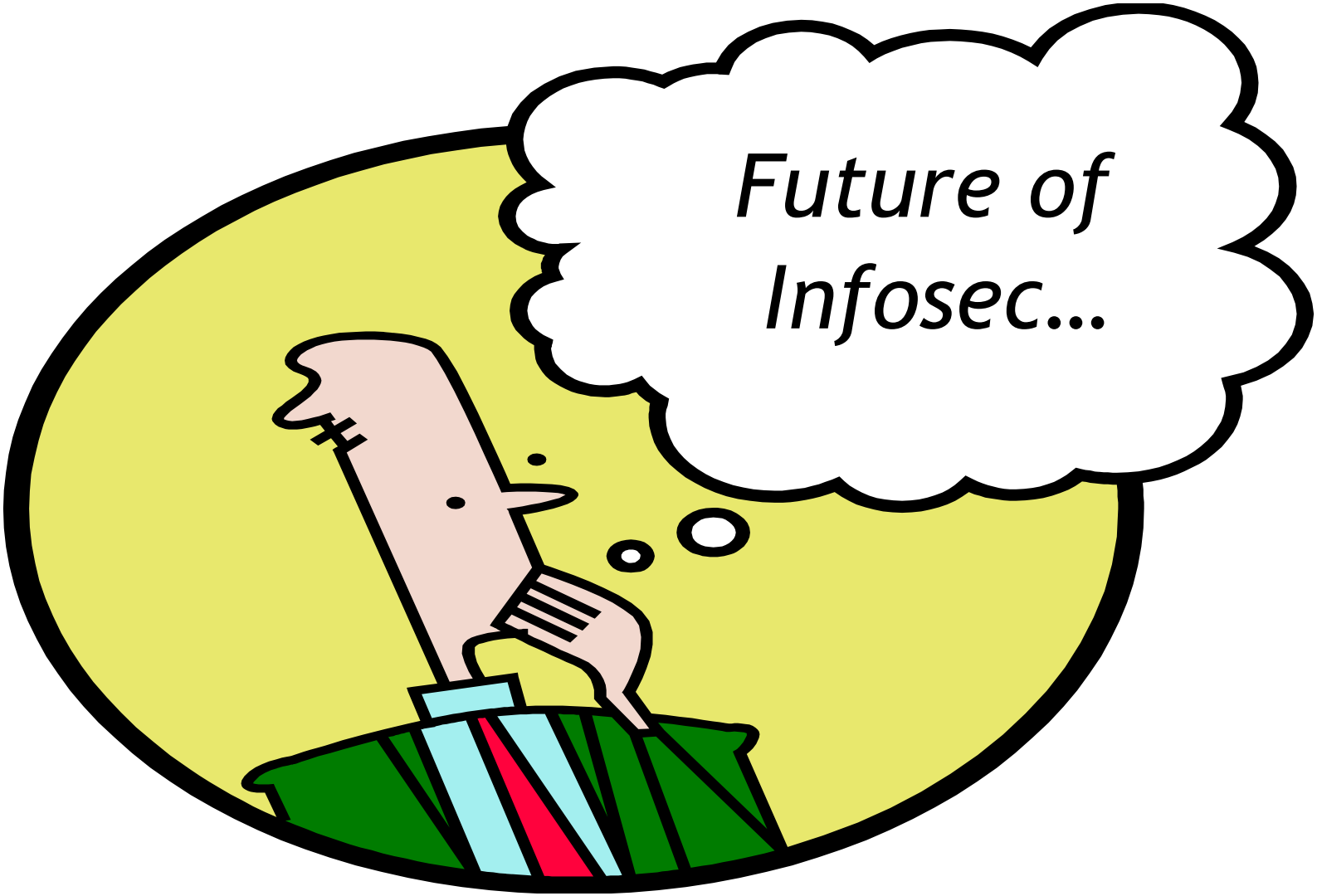
Who is this guy?

BELLEVUE UNIVERSITY
CIT
College of Information Technology

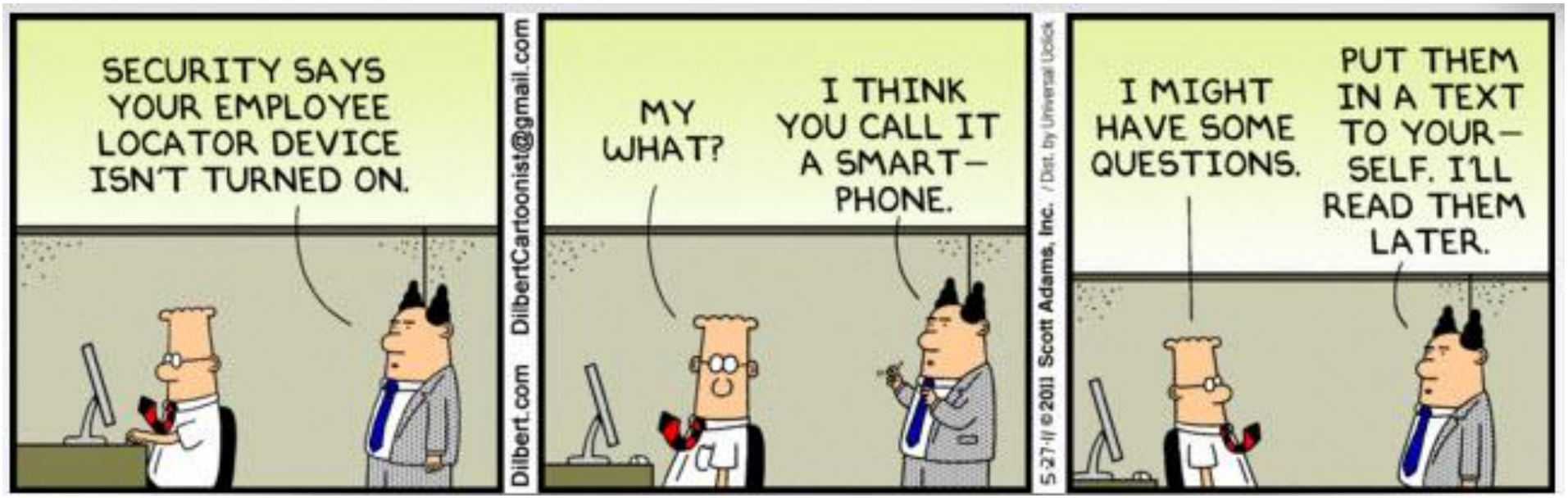
http://academic2.bellevue.edu/~rwoerner/

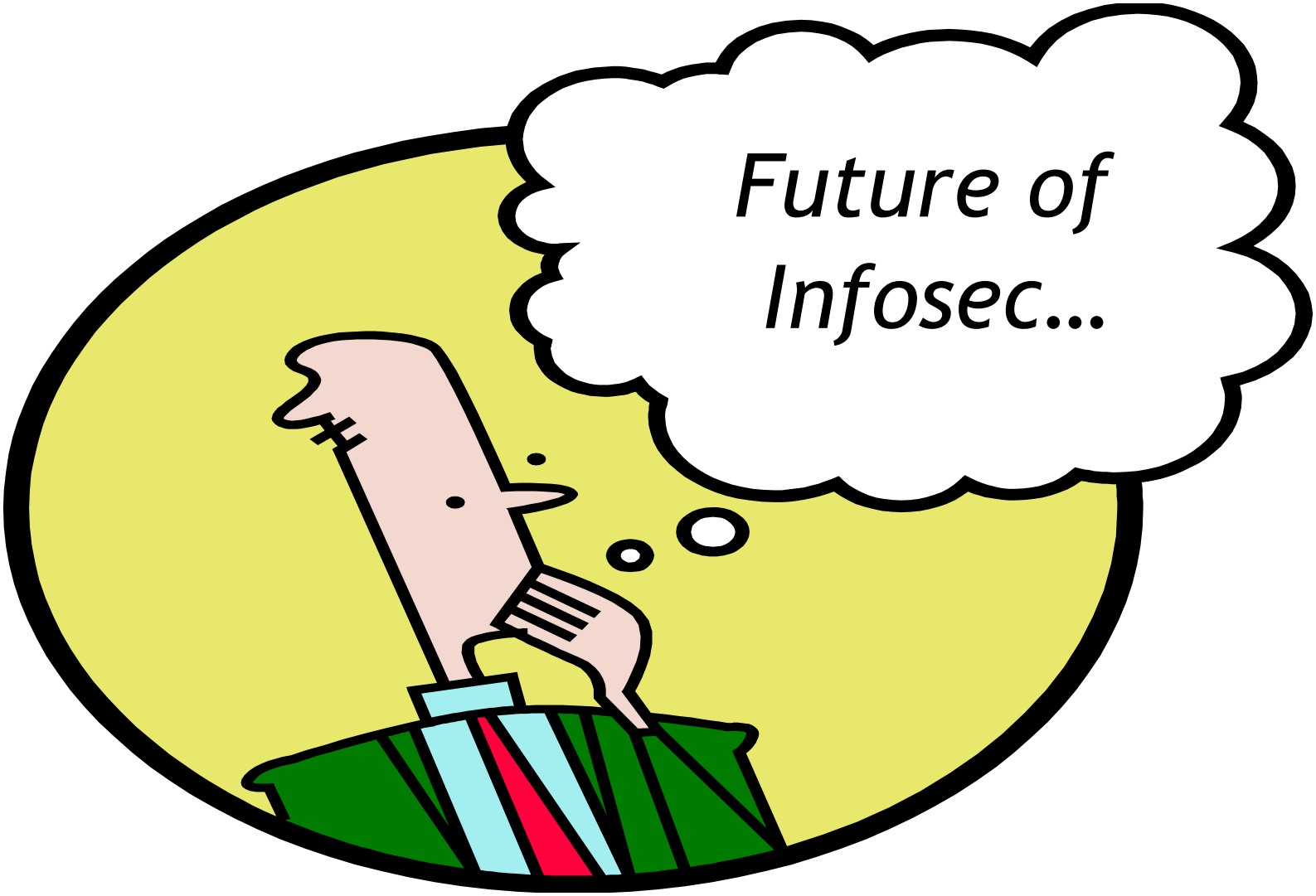

These are my thoughts.
Use at your own risk.


Future of
Infosec…


Future of
Infosec…

Dilbert


SECURITY SAYS YOUR EMPLOYEE LOCATOR DEVICE ISN'T TURNED ON.
MY WHAT?
I THINK YOU CALL IT A SMART-PHONE.
I MIGHT HAVE SOME QUESTIONS.
PUT THEM IN A TEXT TO YOURSELF. I'LL READ THEM LATER.
Dilbert.com DilbertCartoonist@gmail.com
5-27-11 © 2011 Scott Adams, Inc. / Dist. by Universal Uclick


Future of
Infosec…

FUD

ALERT!

2011 Worst Year Ever for Security Breaches!

SONY

EPSILON
Systems Solutions, Inc.

citi®

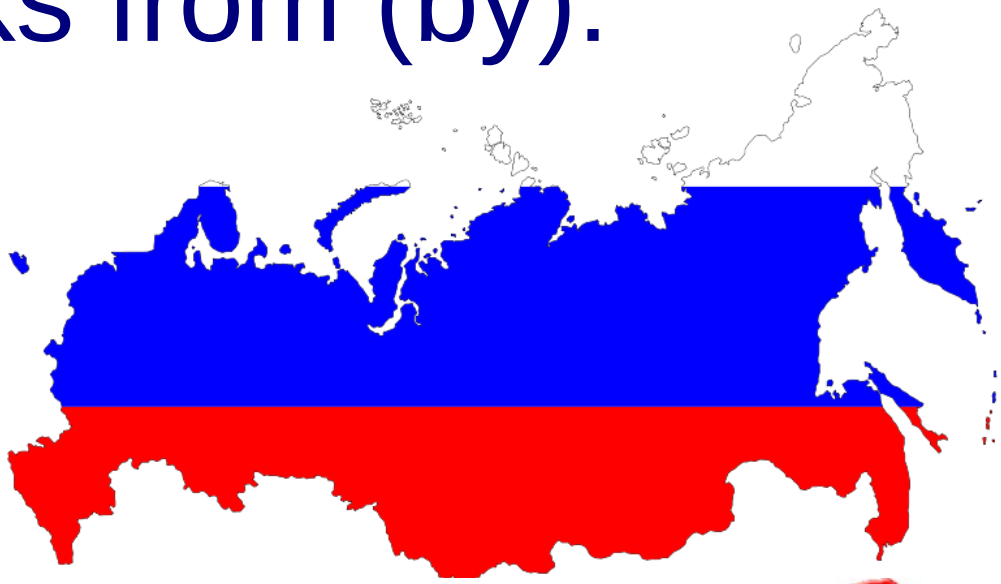
RSA®
The Security Division of EMC

NASA

PBS


[HACKED]
Google™

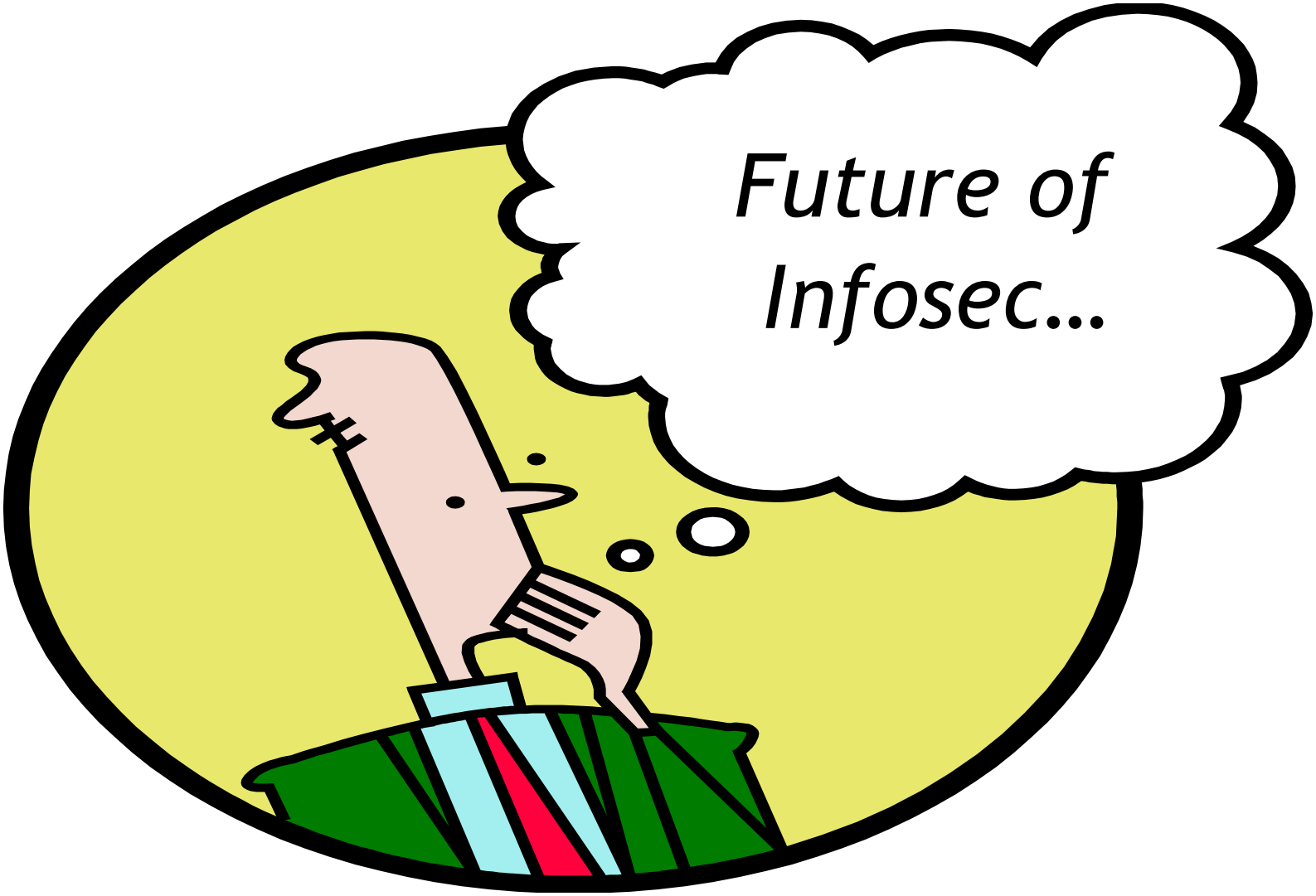
Attacks from (by):



Russia

China

Basically:


Future of
Infosec…

Dr. Carl Sagan

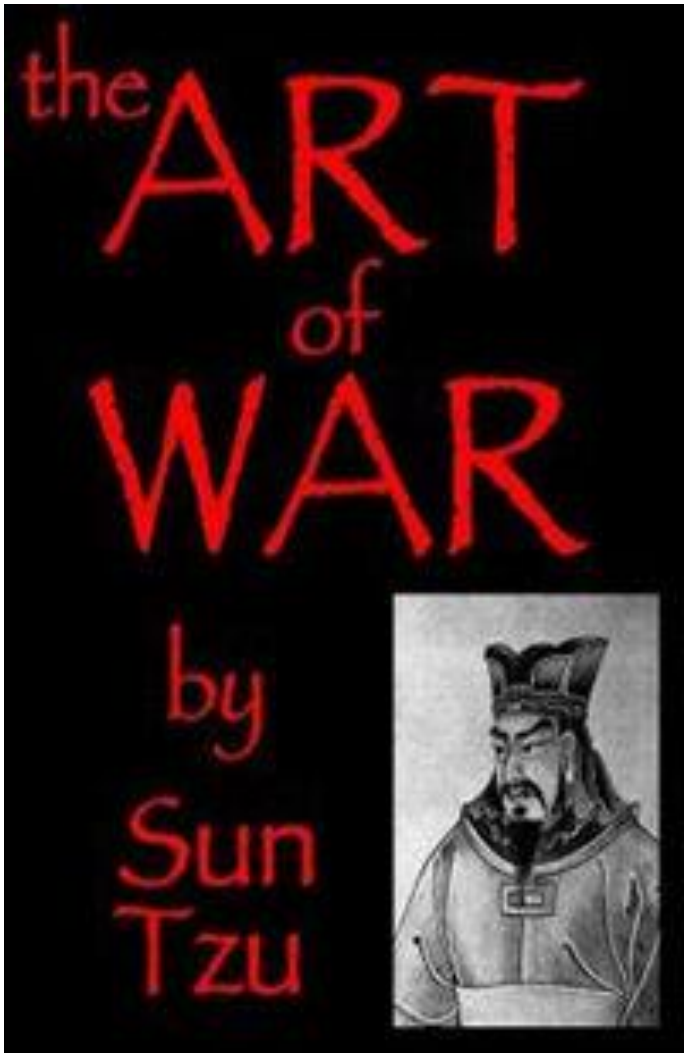
“You have to know the past to understand the present (and the future).”

Sun Tsu – The Art of War

"It is said that if you know your enemies and know yourself, you will not be imperiled in a hundred battles;

if you do not know your enemies but do know yourself, you will win one and lose one;

if you do not know your enemies nor yourself, you will be imperiled in every single battle."



Remember your history

- The Protection of Information in Computer Systems by Saltzer & Schroder
- The Cuckoo's Egg by Clifford Stoll
  - http://pdf.textfiles.com/academics/wilyhacker.pdf
- Practical Unix & Internet Security by Garfinkel & Spafford.
- How to Win Friends & Influence People by Dale Carnegie


EVIDENCE
First known victim
Suspects implicated in security breach
2011
Data Breach
Investigations Report
A study conducted by the Verizon RISK Team with cooperation from the U.S. Secret Service and the Dutch High Tech Crime Unit.
POLITIE
Korps landelijke politiediensten
verizon

Data Breach Investigations Report (DBIR) series

An ongoing study into the world of cybercrime that analyzes forensic evidence to uncover how sensitive data is stolen from organizations, who's doing it, why they're doing it, and, of course, what might be done to prevent it.

Available at: http://verizonbusiness.com/databreach
Updates/Commentary: http://securityblog.verizonbusiness.com

Overview – What's New?

- Over **750 new breaches** studied since the last report

  Total for all years = 1700+

- Just under **4 million records** confirmed compromised

  ~100x less than 2008 alone

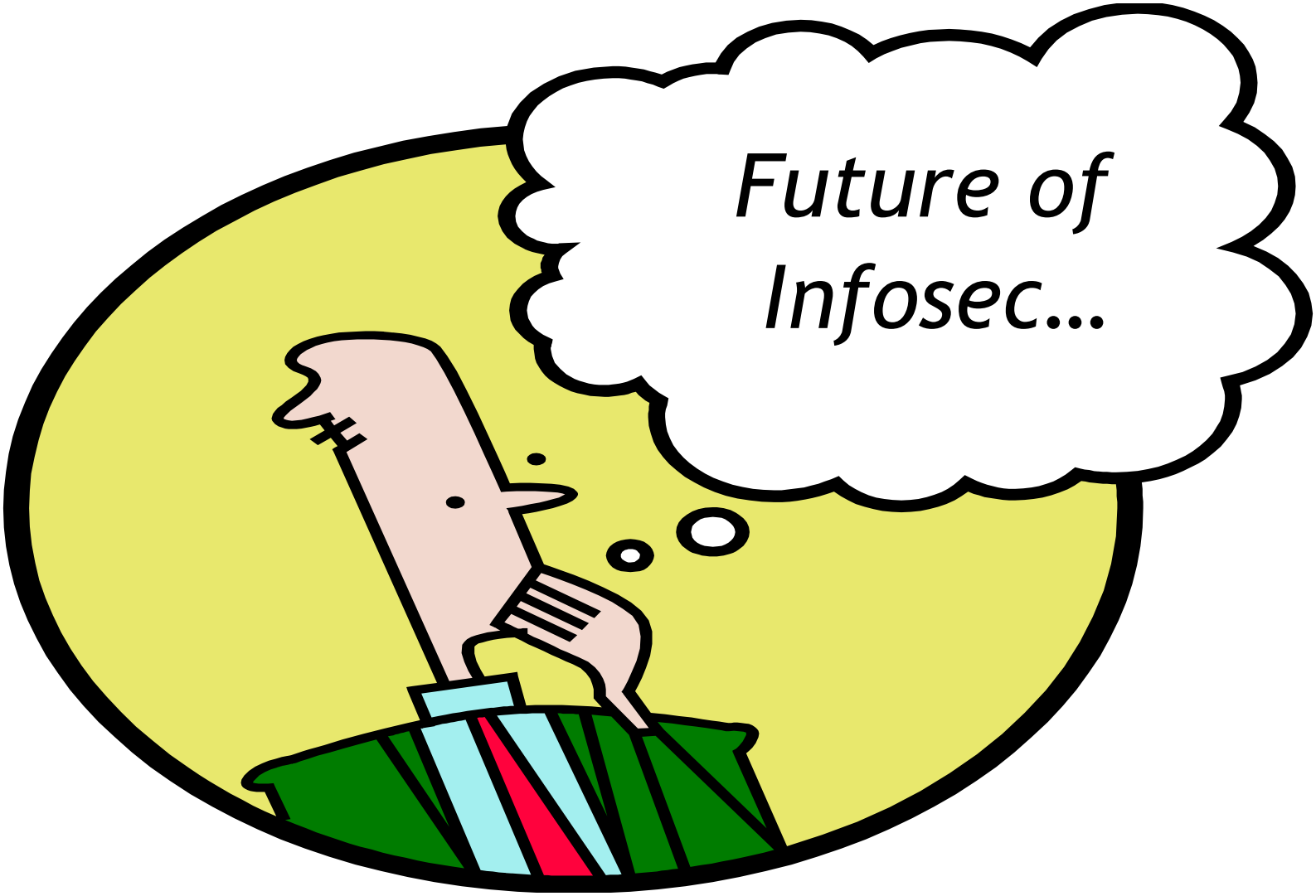
- Euro-centric appendix from Dutch HTCU

Table 15. Compromised data types by number and percent of breaches and percent of records

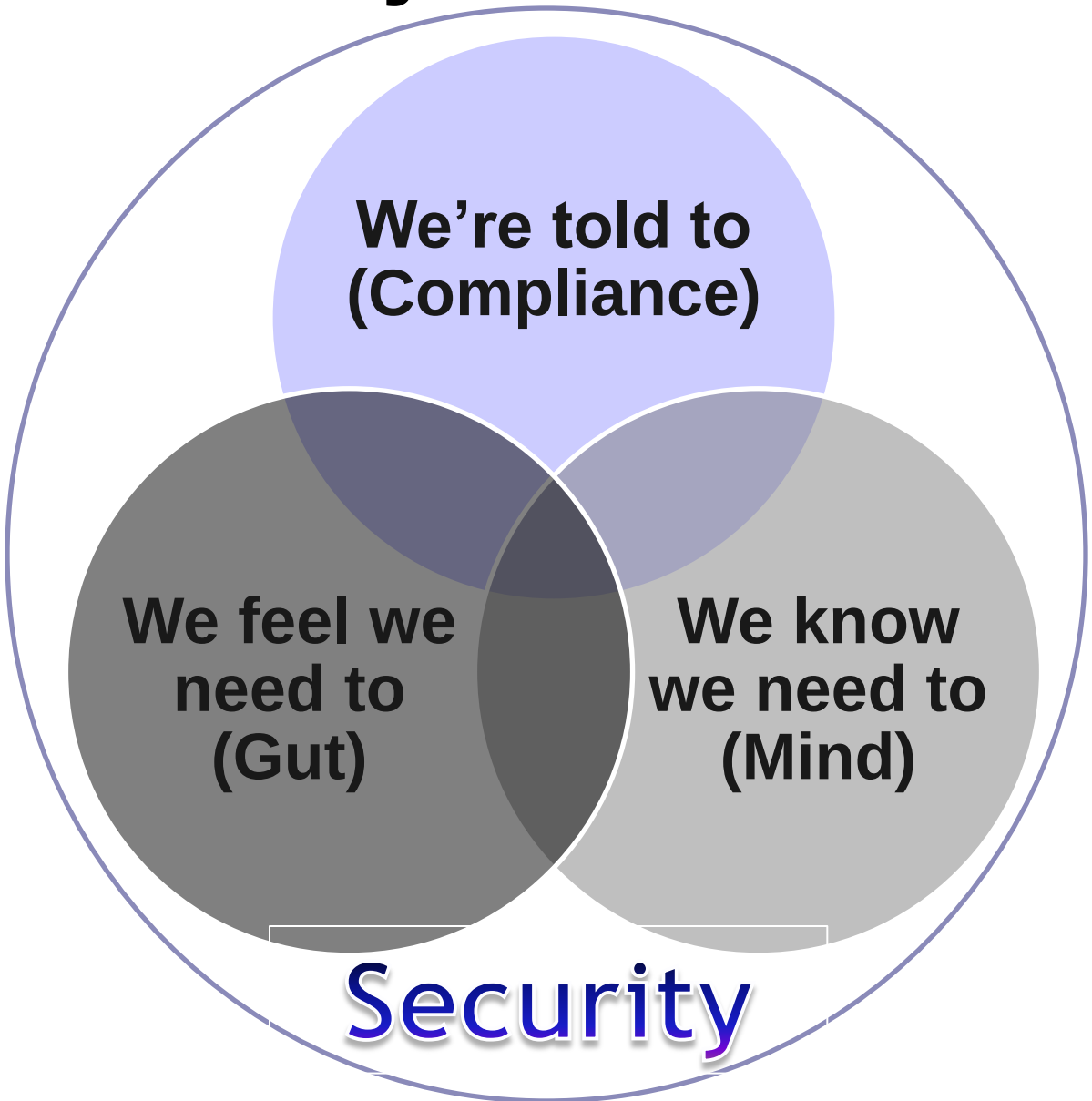
	Number of incidents	Percent of incidents	Percent of records
Payment card numbers/data	593	78%	96%
Authentication credentials (usernames, pwds, etc)	339	45%	3%
Personal Information (Name, SS#, Addr, etc)	111	15%	1%
Sensitive organizational data (reports, plans, etc)	81	11%	0%
Bank account numbers/data	64	8%	<1%
Intellectual property	41	5%	<1%
System information (config, svcs, sw, etc)	41	5%	unknown
Classified information	20	3%	unknown

Drop in Data Loss – Why?

- ~~Random caseload variation~~
- ~~Huge global improvement in security posture~~
- Prosecution and incarceration of “Kingpins”
- Change in criminal tactics
  - Away from massive breaches to smaller, less risky heists (Helps explain increase in breaches)
- Market forces (law of supply and demand)
- Targeting different (non-bulk) data types
- Better at evading detection


Future of Infosec…

Why Security?



Society of Information Risk Analysts

SIRA

http://societyinforisk.org/

Future Thoughts

"We don't have a silver bullet, but we do have silver buckshot."

Jay Jacobs

Future Thoughts

"The more things change, the more they stay the same."

"What we've got right now is what we'll have tomorrow."

Future Thoughts

Security is Risk Management

- Information Security Magazine, Looking Ahead (2005 & 2010)
- The evolution from it's current series of random incarnations to full, fledged information risk management. (boB Rudis)
- Prioritization based on risk using a battle hardened framework with industry benchmarks. (Phil Agcaoili)

Better Security Metrics

Figure 10. Compromised records by threat agent, 2010

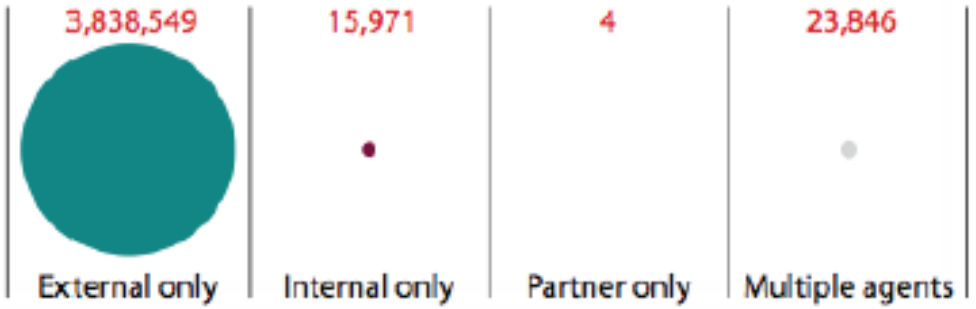
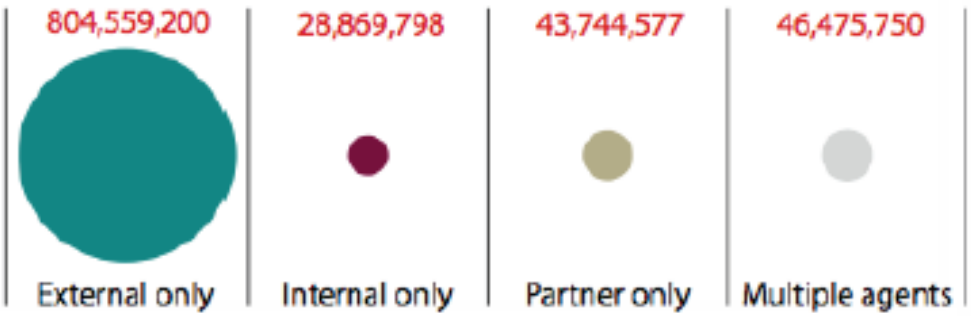


Figure 11. Compromised records by threat agent, 2004-2010



Security Silos

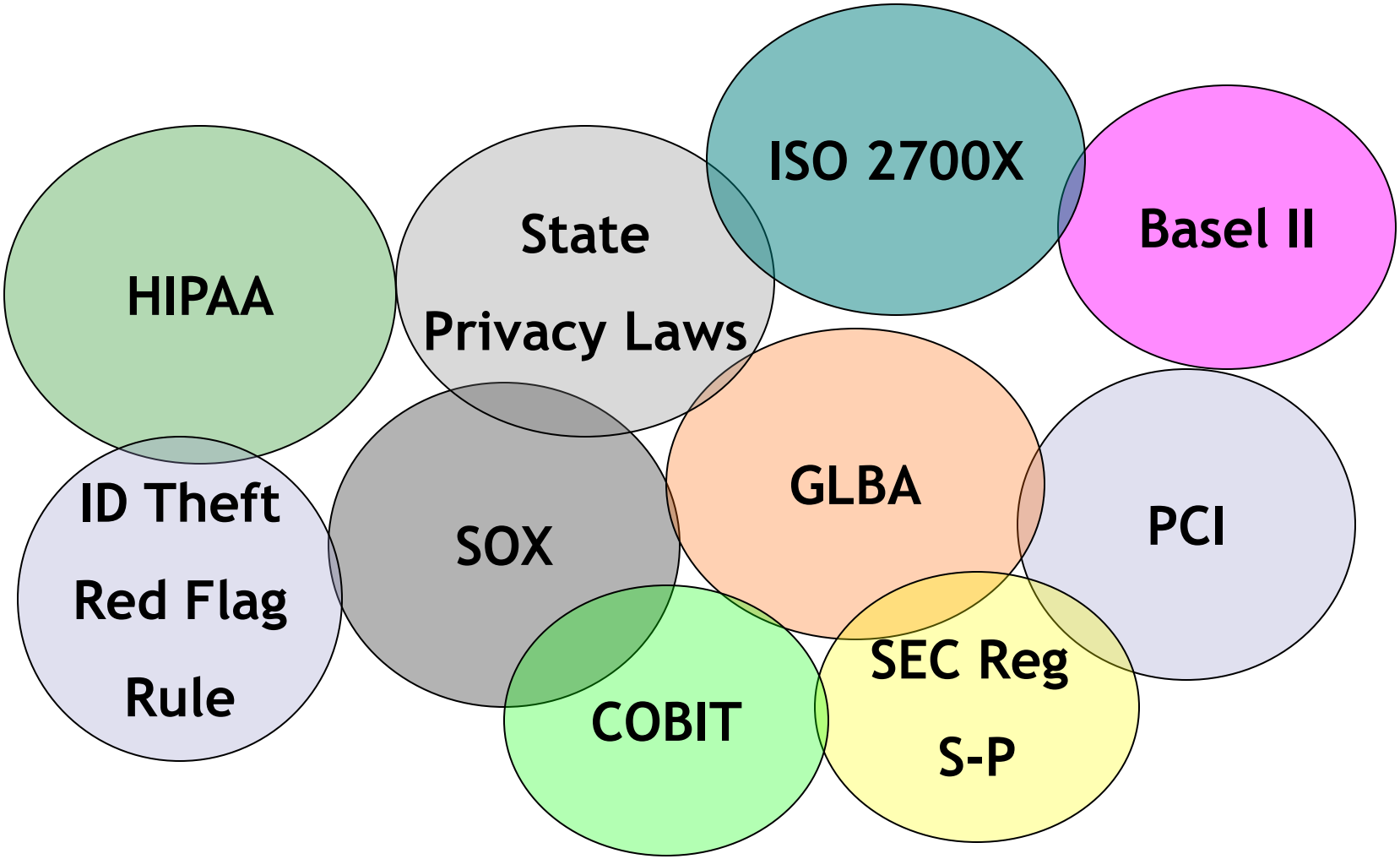
The transformation of it being a solely a dedicated discipline to an attribute/skill expected in all information workers.

Cylinders of Excellence

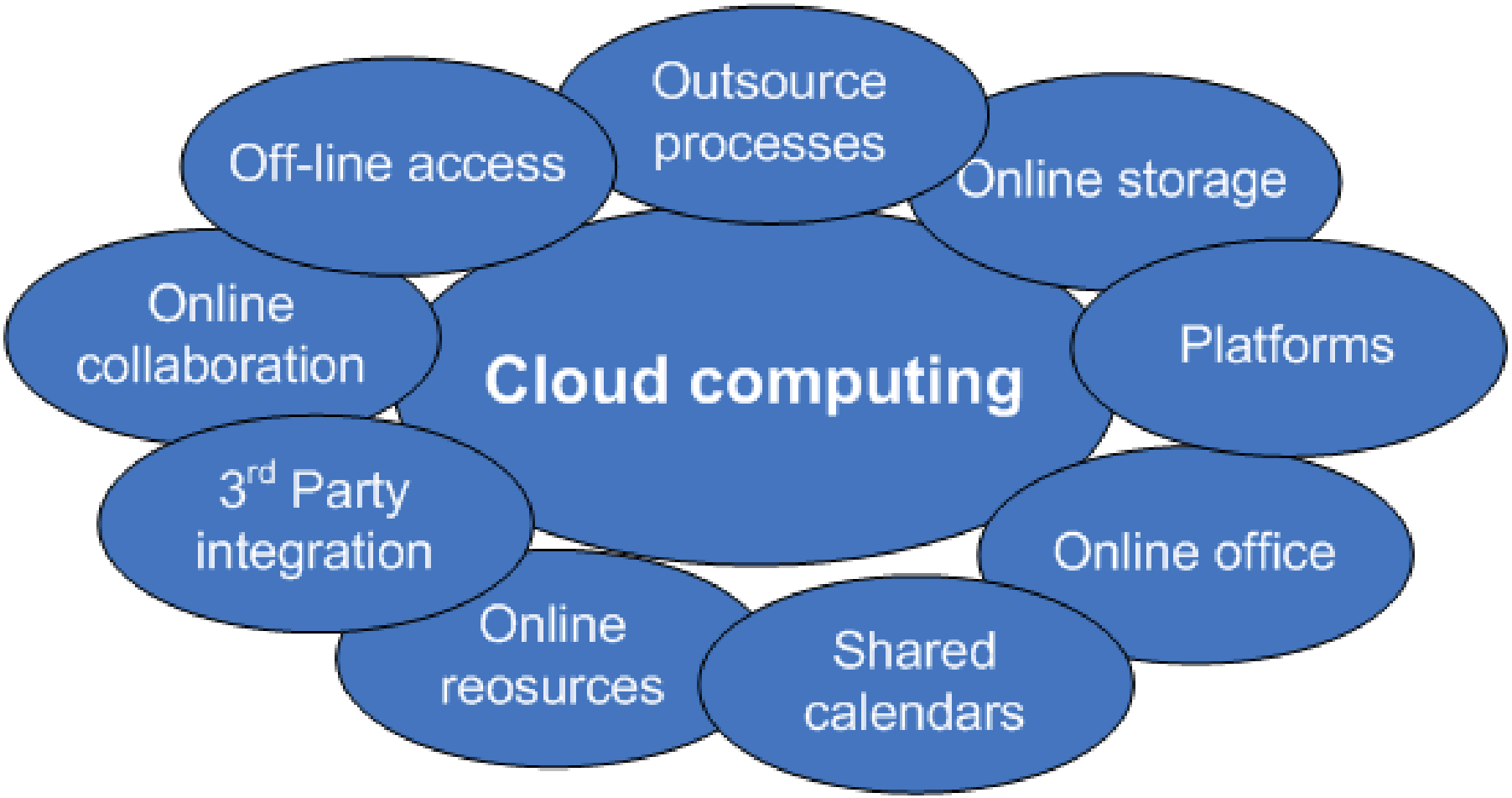
DEFENSE

- Security is driven by what abusers and misusers will do. (Donn Parker)
- Engineer for resiliency, not for absolute defense. (Ben Tomhave)
- Fail-safe security

Compliance


ISO 2700X
Basel II
HIPAA
State
Privacy Laws
ID Theft
Red Flag
Rule
SOX
GLBA
PCI
COBIT
SEC Reg
S-P

Web 3.0 – New Technologies



What do we do?

What can we do?

Administer the Obvious*

- Enforce the policies, standards & guidelines
- Find and fix holes
- Control access
  - Know who has access to what
  - Know who the administrators are
- Guide, assist & train
  - Managers, users and systems administrators
- Know what to do when you have an incident

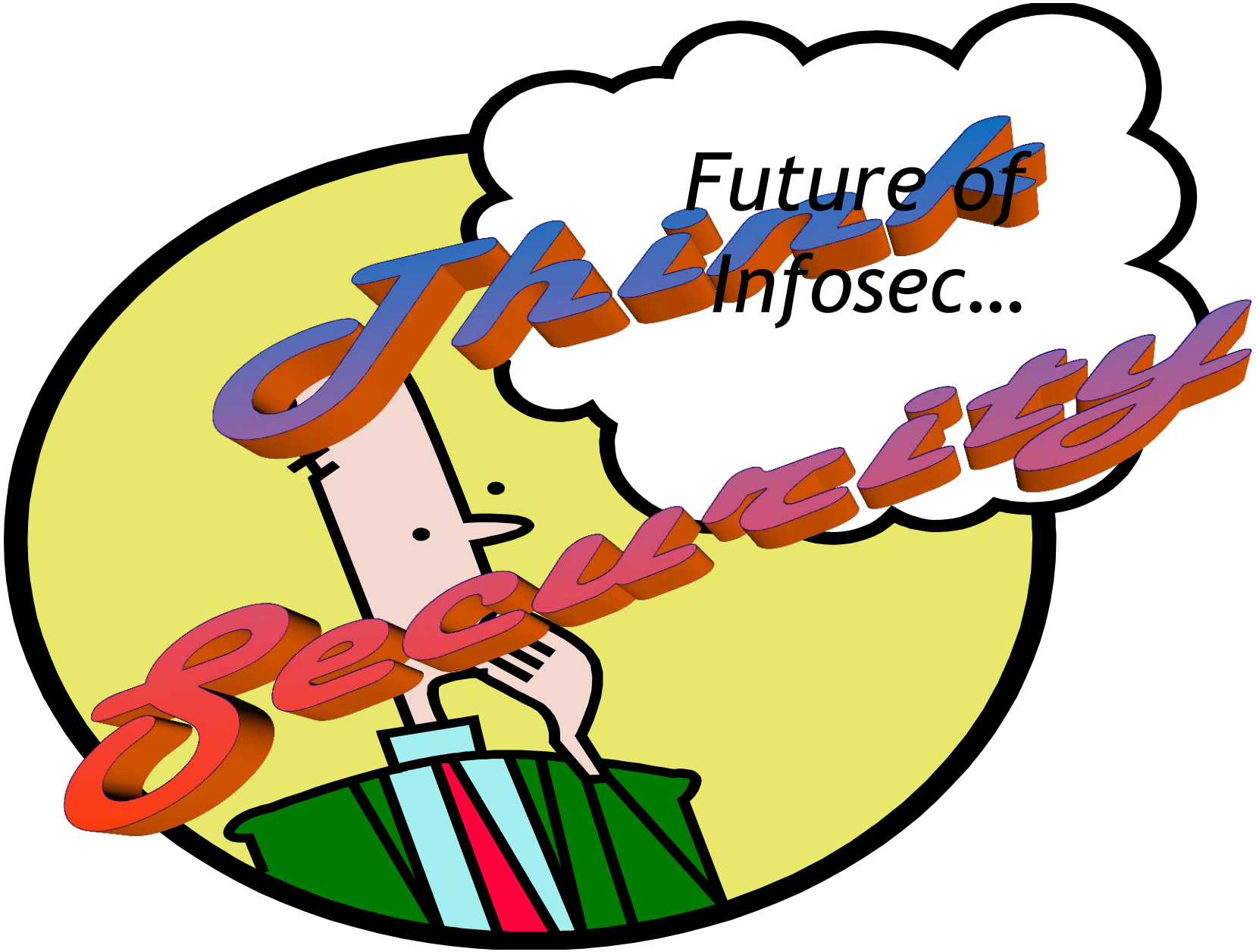
***From: Infotec 2004 – "Zen & The Art of Information Security**

Security Caveats

- These tasks won't close all of the holes.
- Everyone needs to take responsibility for information systems security.
- The intent is to make your environment much less inviting to those looking for easy pickings.
- This also establishes legal due diligence in protecting your organization.

Conclusion

- Understand the problem
- Plan solutions
- Be aware of what’s available
- Go out and play
- Security is all about percentages
- Join a community & Share with others
- Do no harm


Future of
Infosec...
Think
Security

HOMEWORK

Find your own security future

Ron Woerner

Ronw2007(at)gmail.com

Twitter: @ronw123