

Cyber Security Inside Out

Gurpreet Dhillon, PhD
Professor
Virginia Commonwealth University

Executive Director, The Information Institute

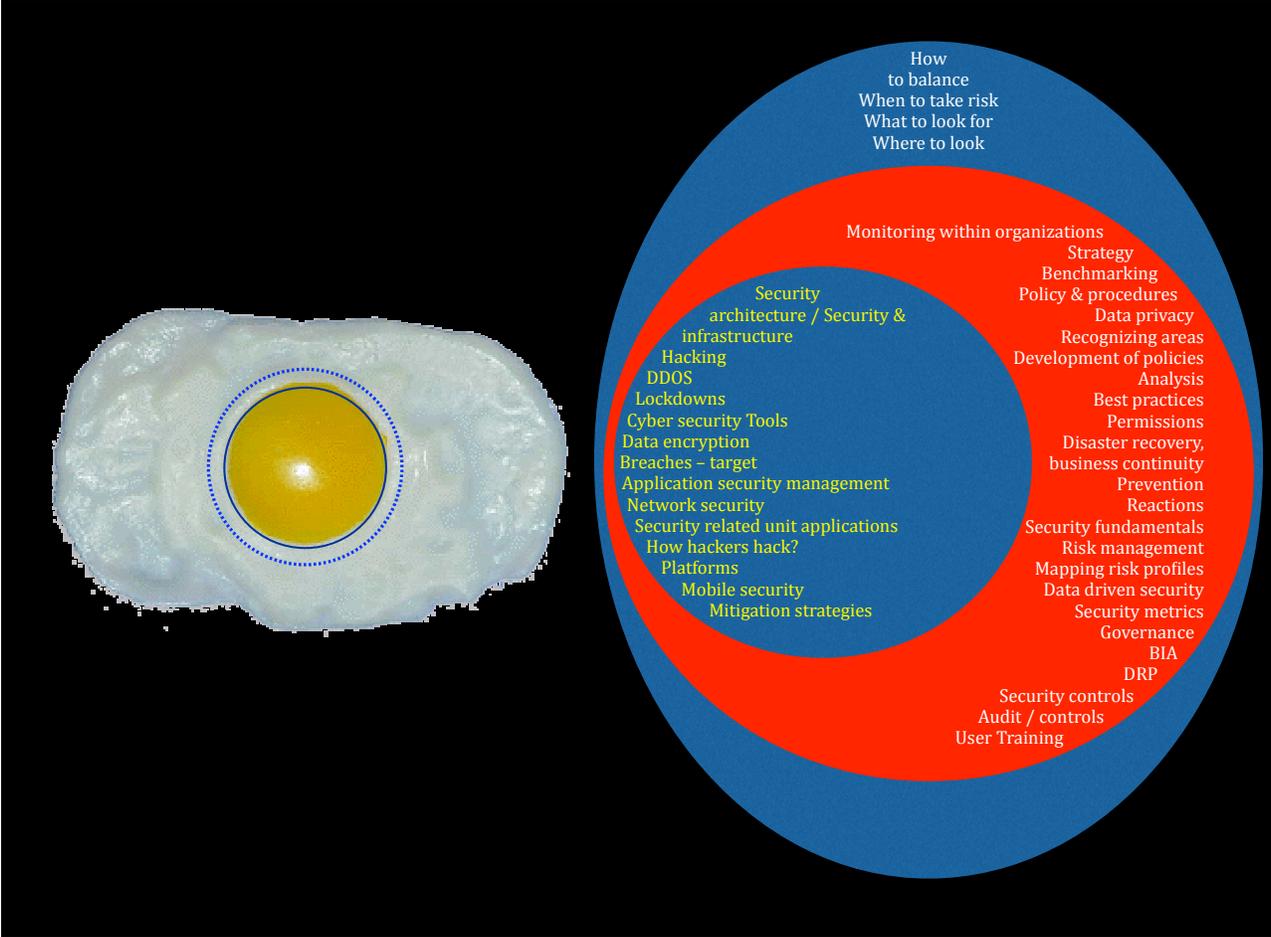
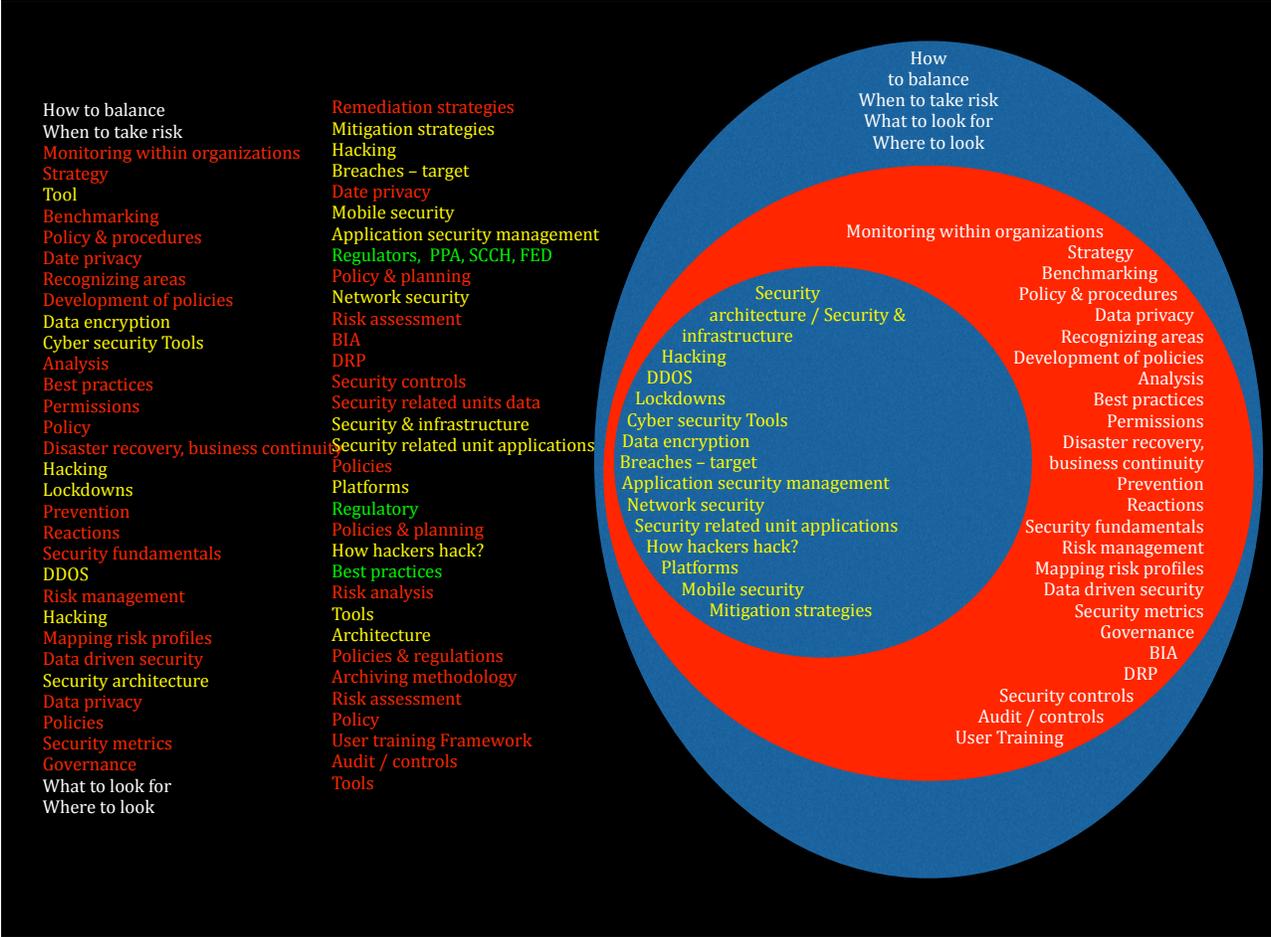
1

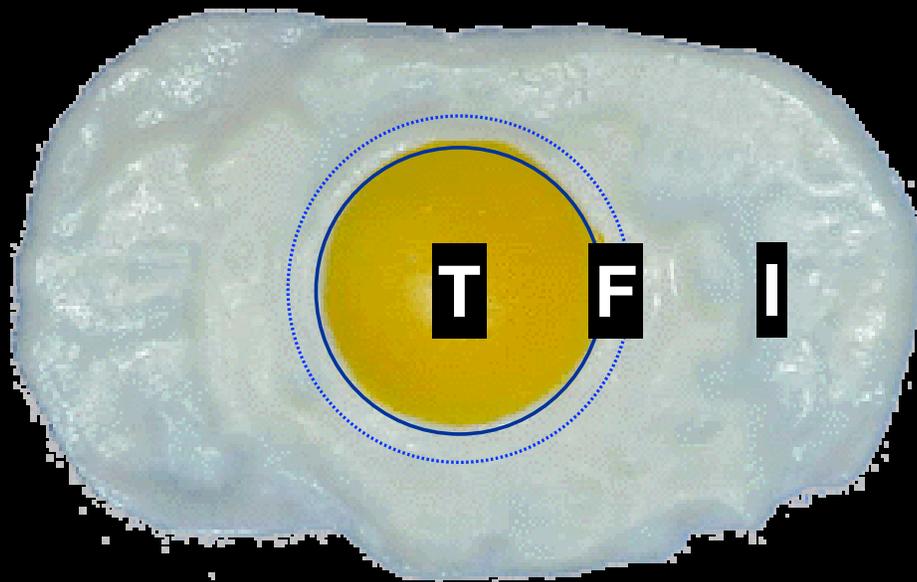
Security Challenges - April 23, 2015

How to balance	Remediation strategies		
When to take risk	Mitigation strategies		
Monitoring within organizations	Hacking		
Strategy	Breaches – target		
Tool	Date privacy		
Benchmarking	Mobile security		
Policy & procedures	Application security management		
Date privacy	Regulators, PPA, SCCH, FED		
Recognizing areas	Policy & planning		
Development of policies	Network security		
Data encryption	Risk assessment		
Cyber security Tools	BIA	Data priority	Hacking
Analysis	DRP	Ethical hacking	Roles / permissions
Best practices	Security controls	Recognize areas of importance	Tools
Permissions	Security related units data	Data encryption	Structure and architecture
Policy	Security & infrastructure	Development of policies	Team structure
Disaster recovery, business continuity	Security related unit applications	Security fundamentals	Risk assessment
Hacking	Policies	How hackers hack	Policy and planning
Lockdowns	Platforms	How to keep data secure	HIPAA
Prevention	Regulatory	Risk management	Data privacy
Reactions	Policies & planning	Auditing / controls	Security metrics
Security fundamentals	How hackers hack?	Standards	Mitigation strategies
DDOS	Best practices	Best practices	Remediation strategies
Risk management	Risk analysis	Policy	Apply practices, focus points
Hacking	Tools		
Mapping risk profiles	Architecture		
Data driven security	Policies & regulations		
Security architecture	Archiving methodology		
Data privacy	Risk assessment		
Policies	Policy		
Security metrics	User training Framework		
Governance	Audit / controls		
What to look for	Tools		
Where to look			

2

Security Challenges - April 23, 2015





The Challenge

- Just like a thief can easily steal a car with its doors open and engine running, the solution is not to ban cars. Instead, we use simple layered security procedures, locking the ignition, steering wheel, and doors to present series of problems to thieves.
- Likewise a layered approach to protecting computing environments needs to be developed.

The good news

- There is an increased level of awareness regarding information security. Security awareness typically figures relatively high on the corporate agenda and businesses are proactively engaged in getting the word out to their employees.

All rights reserved. Copyright held by Gurpreet Dhillon, PhD

7

Security Challenges - April 23, 2015

The bad news

- **Being aware** is NOT EQUAL to **being secure**. There is a problem with the nature and scope of security awareness training. Information security is complex.

All rights reserved. Copyright held by Gurpreet Dhillon, PhD

8

Security Challenges - April 23, 2015

However ...

- How many times have you been tempted to open the email with the following subject line:
 - “Returned mail: see transcript for details”

All rights reserved. Copyright held by Gurpreet Dhillon, PhD

#	Total Spam: August 2010 Top Subject Lines	No of Days	Total Spam: July 2010 Top Subject Lines	No of Days
1	Your wife photos attached	21	Blank Subject line	31
2	Blank Subject line	31	Delivery Status Notification (Failure)	31
3	Your Order with Amazon.com	12	You have received an Greeting eCard	12
4	Meet Local Girls	16	Amazon.com: Please verify your new e-mail address	11
5	Resume	10	Returned mail: see transcript for details	31
6	Your private photo attached	7	Undelivered Mail Returned to Sender	31
7	New Message	17	Nikki Sent You A Message	15
8	Join my network on LinkedIn	4	My Pics	14
9	You have notifications pending	22	failure notice	31
10	Best Sales 2010!	3	Give your partner a one-way ticket to ecstasy-land.	31

Earn Your M.E.

QualityCIALI

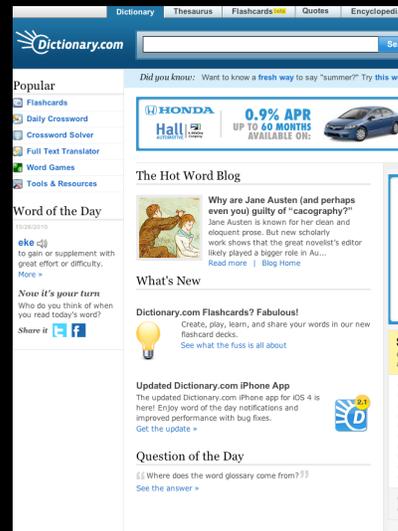
80

All rights reserved. Copyright held by Gurpreet Dhillon, PhD

Dictionary.com

- Single visit results in:

- 159 cookies
- 41 Beacon
- 11 First Party
- 168 No Opt Out
- 143 May share info
- 121 May collect Fin. Health data
- 133 Keep Info indefinitely



All rights reserved. Copyright held by Gurpreet Dhillon, PhD

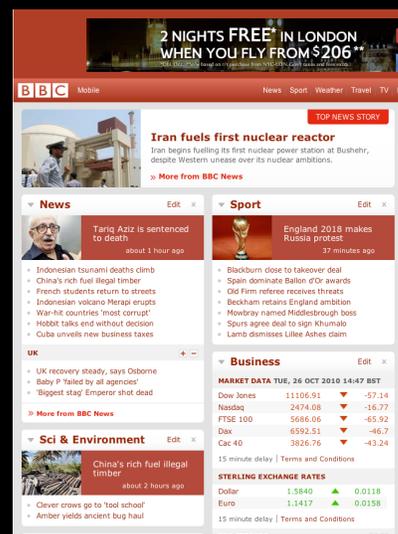
11

Security Challenges - April 23, 2015

bbc.co.uk

- Single visit results in:

- 22 cookies
- 17 Beacon
- 6 First Party
- 33 No Opt Out
- 20 May share info
- 15 May collect Fin. Health data
- 19 Keep Info indefinitely



All rights reserved. Copyright held by Gurpreet Dhillon, PhD

12

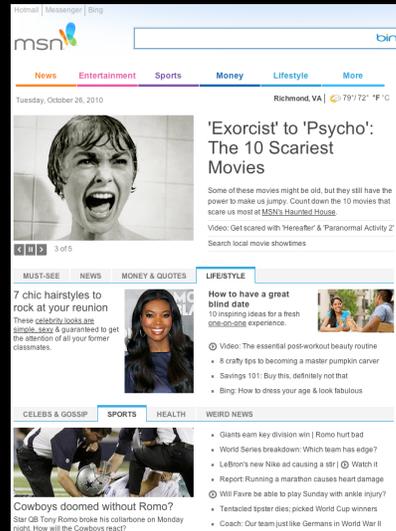
Security Challenges - April 23, 2015

msn.com

- Single visit results in:

- 131 cookies
- 23 Beacon
- 53 First Party

- 135 No Opt Out
- 52 May share info
- 46 May collect Fin. Health data
- 98 Keep Info indefinitely



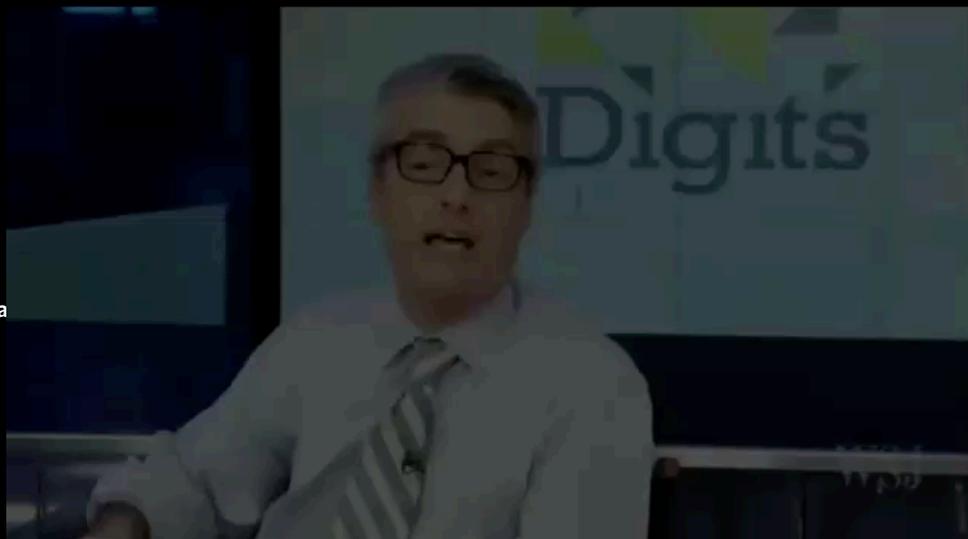
All rights reserved. Copyright held by Gurpreet Dhillon, PhD

13

Security Challenges - April 23, 2015

Consider this

Google a



All rights reserved. Copyright held by Gurpreet Dhillon, PhD

14

Security Challenges - April 23, 2015

Abacus Deal Is Quaint in Today's Data Era

New Ad Age Newsletter Will Cover How Marketers Tap 'Big Data' Like Never Before

By: Kate Kaye Published: January 14, 2013

72 | share this page



It was the first online ad-privacy scandal.

In 1999, DoubleClick bought catalog-data firm Abacus for \$1.7 billion. Privacy advocates flipped. They petitioned the Federal Trade Commission and scared DoubleClick into announcing it would not connect personal information from Abacus with online-browsing data.

If the deal happened today, the story would be different. It's not uncommon for offline data -- retail transactions, CRM data, loyalty-card data and more -- to be connected to digital data to enhance online targeting.

In pre-bust 1999, investor dollars were flowing and DoubleClick was years away from its acquisition by Google, still operating as a mere "ad network" -- an almost quaint term in light of today's data-driven marketplace and its behavioral targeting, social media and ad and data exchanges.

The concern when DoubleClick bought Abacus -- which it sold at a loss to Epsilon for \$435 million in 2006 -- was that personally identifiable information would be linked with online info.

The industry was young, and DoubleClick failed at first to acknowledge privacy concerns. "DoubleClick was tone deaf in how they handled it," said Dave Morgan, founder of one of the first successful behavioral-targeting firms, Tacoda, and CEO and founder of Simulmedia.

It wasn't clear exactly what DoubleClick wanted to do with Abacus data, and the privacy scare and subsequent FTC investigation essentially crimped its ability to exploit the full potential. (The FTC

In 2005 they had also bought DART email for \$9m

All rights reserved. Copyright held by Gurpreet Dhillon, PhD

15

Security Challenges - April 23, 2015

The Challenge

15% of US adults are still not online

2% of the 18-29 year olds are not online

92% of the 15% have no desire to go online

4 out of 10 nonconnected asked someone to go online

Ignore (I don't care)

Embrace (That's a way of life)

Stay informed (I need to know)

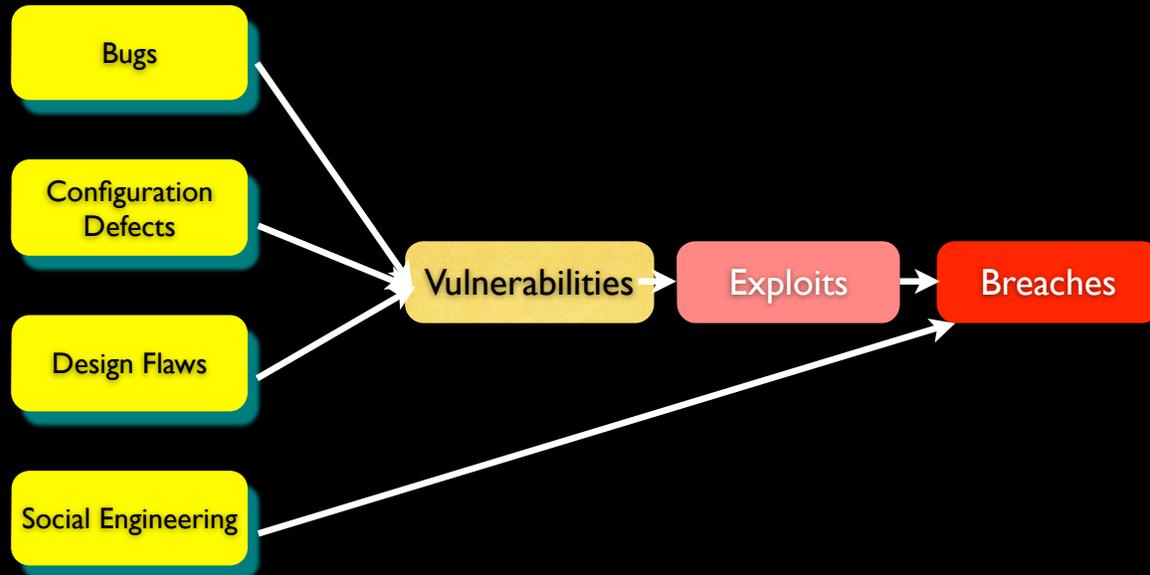
Learn (Proactively do something about it)

All rights reserved. Copyright held by Gurpreet Dhillon, PhD

16

Security Challenges - April 23, 2015

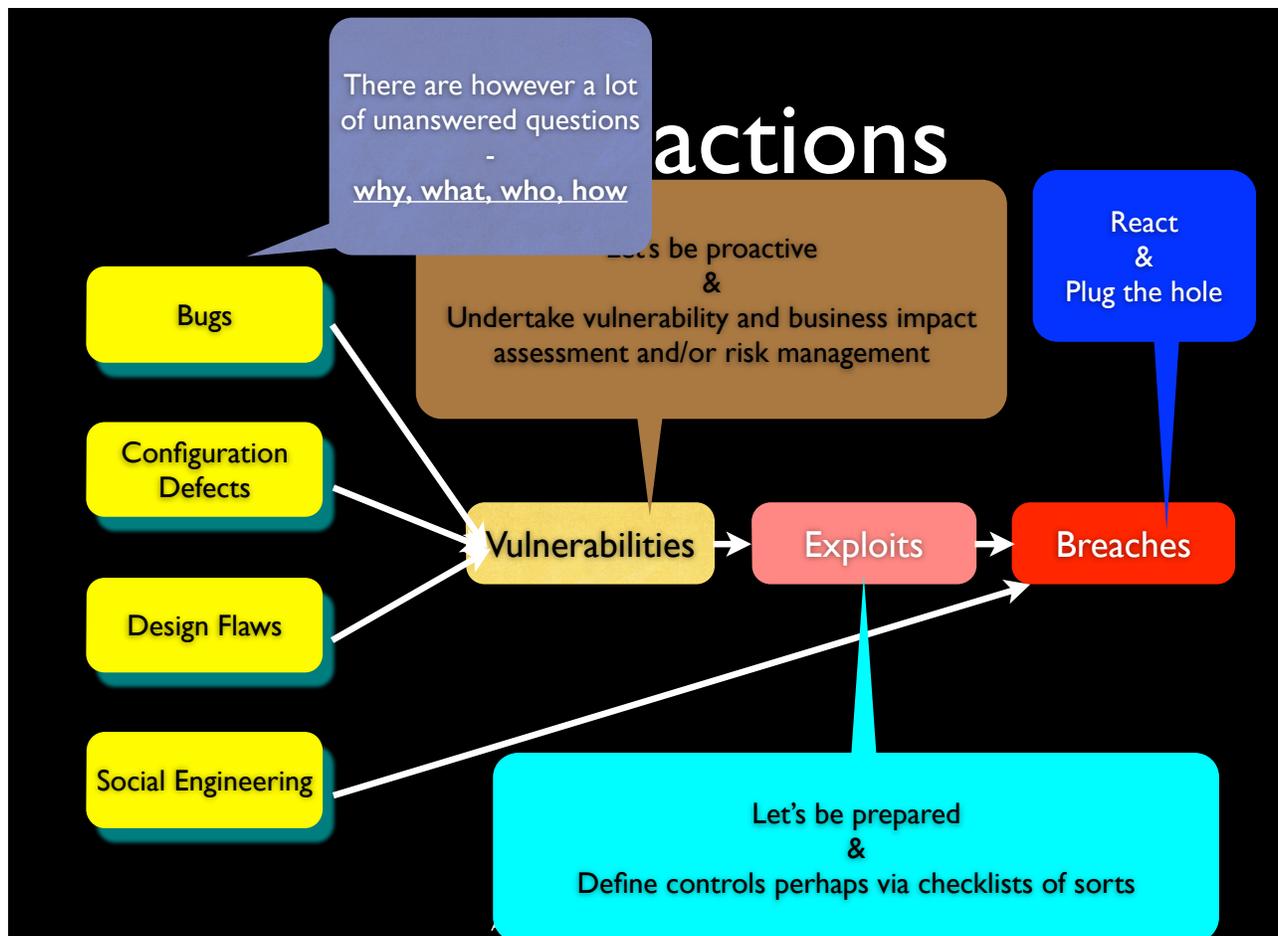
What are we dealing with?



All rights reserved. Copyright held by Gurpreet Dhillon, PhD

17

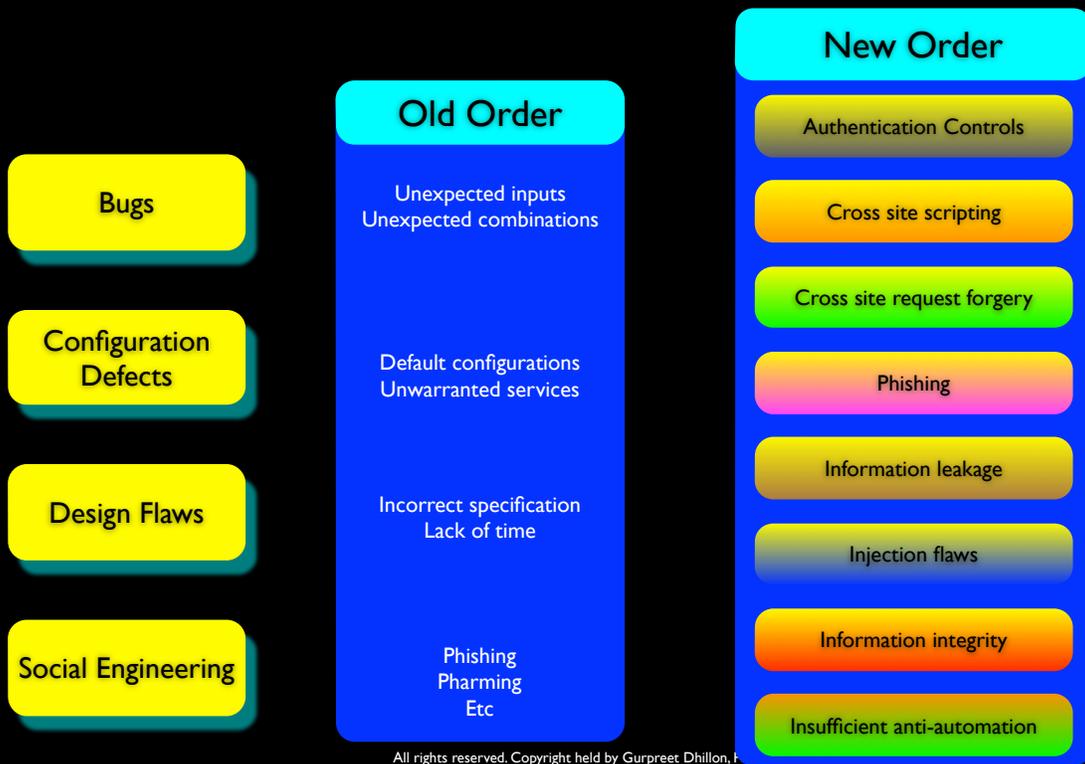
Security Challenges - April 23, 2015



18

Security Challenges - April 23, 2015

The new order



Management Myths



MYTH 1

WE HAVE A GOOD SECURITY
POLICY

All rights reserved. Copyright held by Gurpreet Dhillon, PhD

21

Security Challenges - April 23, 2015

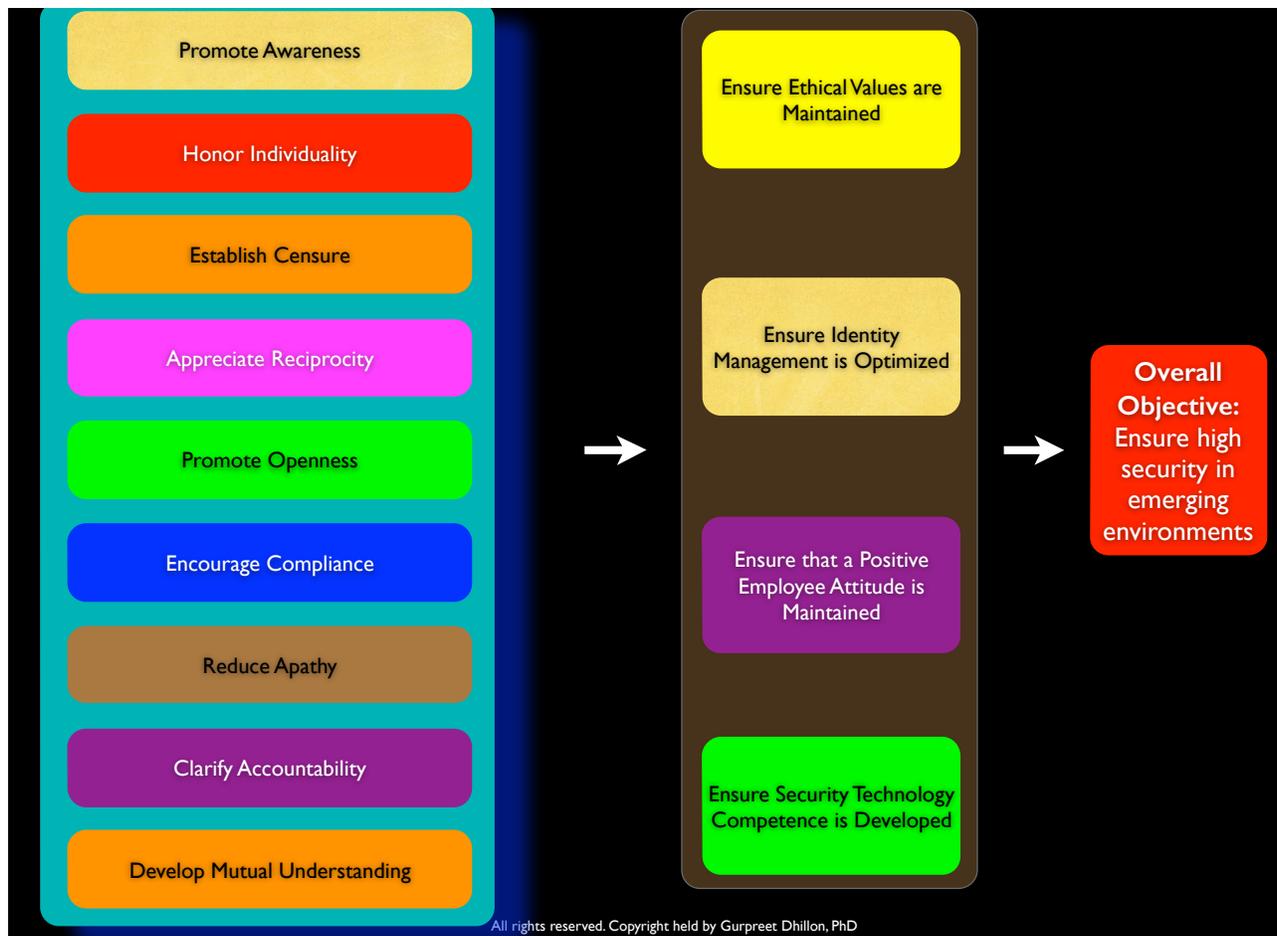
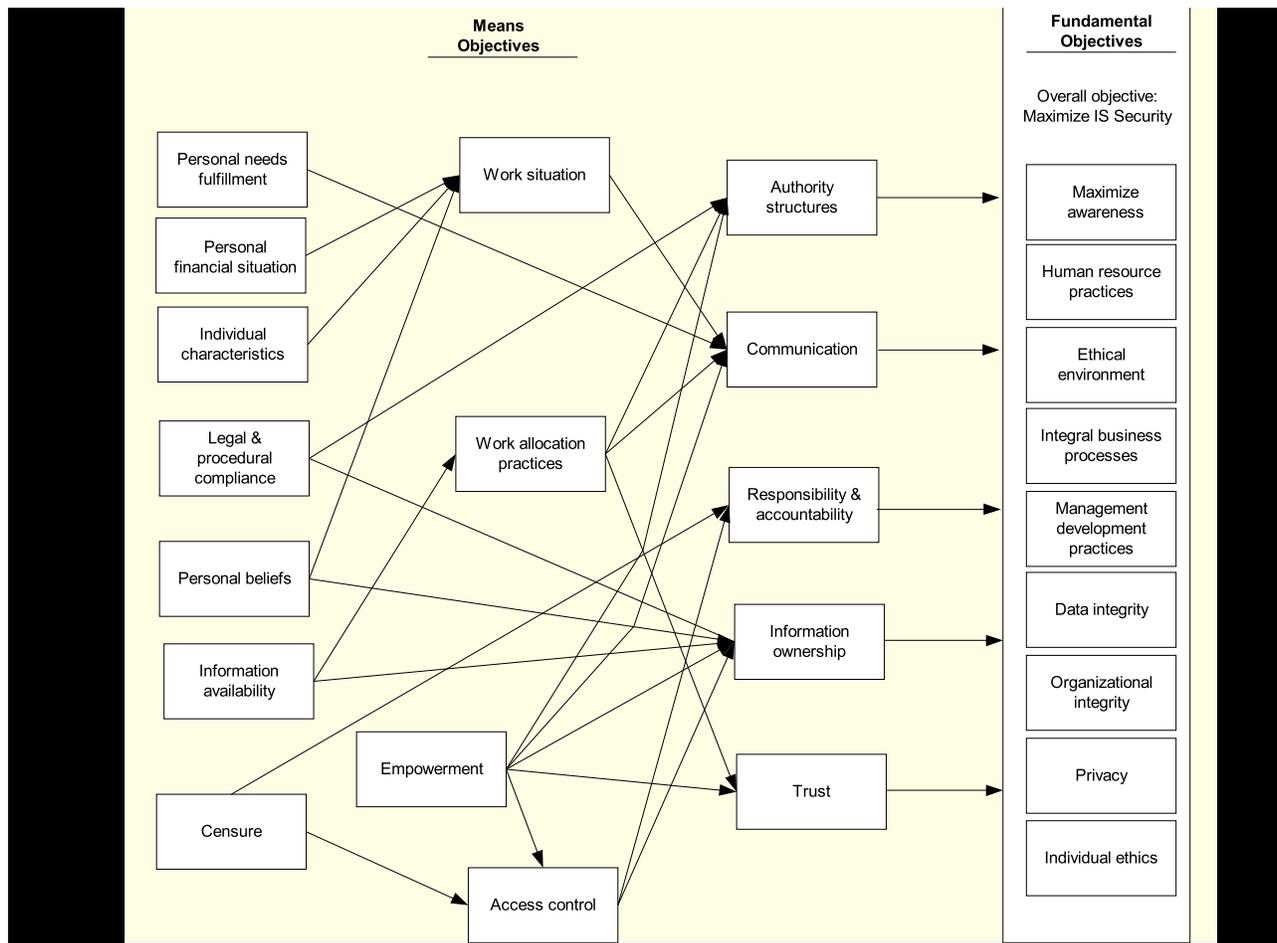
Security Policy??

- Think again.
 - Majority of organizations do not have one
 - Even if it is there, it's archaic, useless and does not fit the organization

All rights reserved. Copyright held by Gurpreet Dhillon, PhD

22

Security Challenges - April 23, 2015



Problem

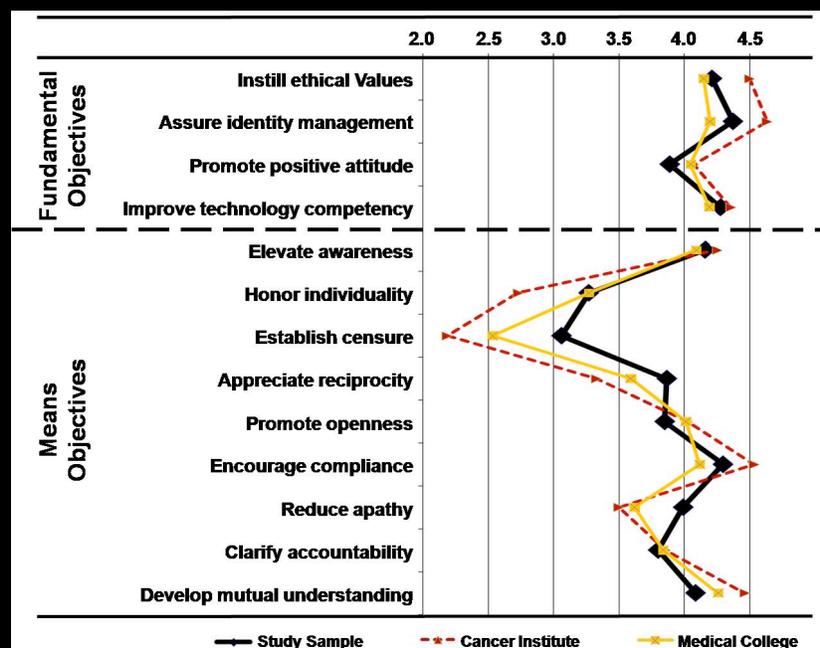
- Based on our work across Sweden (3 companies), Portugal (7 companies) and the US (23 companies), we found there to be a 30% correspondence between security objectives and what their security policies espoused.

All rights reserved. Copyright held by Gurpreet Dhillon, PhD

25

Security Challenges - April 23, 2015

Profiling Companies



All rights reserved. Copyright held by Gurpreet Dhillon, PhD

26

Security Challenges - April 23, 2015

Fortune Cookie Advice

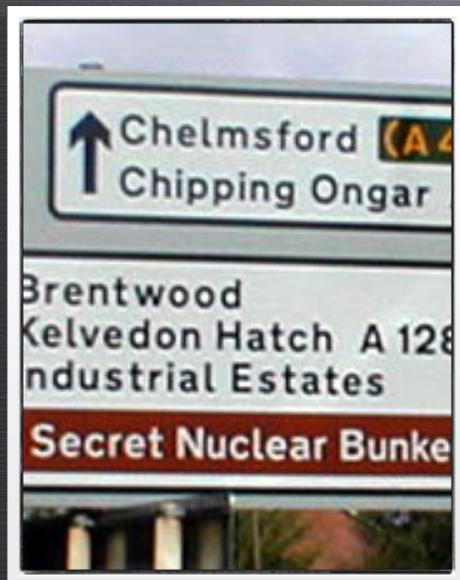
- Security policy is like a seatbelt. It will not protect you every time, but it is guaranteed to fail if you choose not to use it.
- Moreover, it needs constant evaluation and reassessment.



All rights reserved. Copyright held by Gurpreet Dhillon, PhD

27

Security Challenges - April 23, 2015



MYTH 2
WE HAVE STRICT
CONFIDENTIALITY RULES

All rights reserved. Copyright held by Gurpreet Dhillon, PhD

28

Security Challenges - April 23, 2015

Confidentiality Rules??

- You assume that there are strict confidentiality rules that are typically not broken.
- Surprise! Surprise! Confidentiality, as defined in the old environment, does not necessarily match the largely decentralized and virtualized org. structure of the new environment

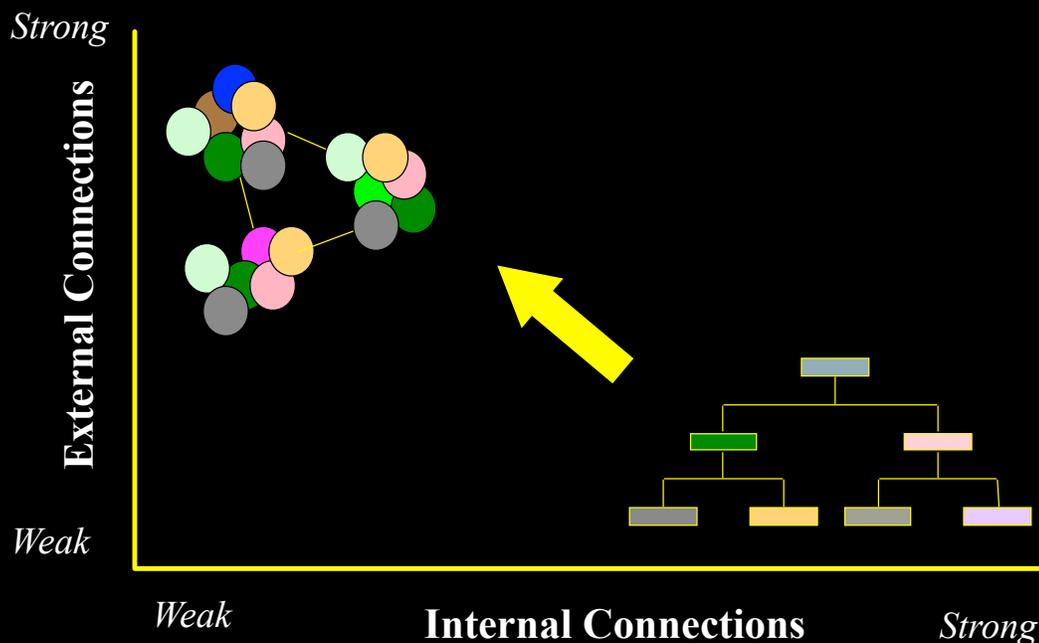
All rights reserved. Copyright held by Gurpreet Dhillon, PhD

29

Security Challenges - April 23, 2015

Confidentiality

in a web of an enterprise



All rights reserved. Copyright held by Gurpreet Dhillon, PhD

30

Security Challenges - April 23, 2015

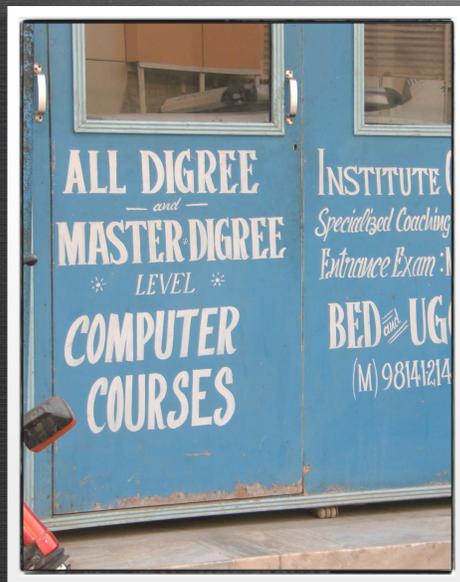
On the horizon...

- User-to-service authentication
- Service-to-service authentication
- Delegated authorization
- Emergence of the likes of OpenID and OAuth, albeit become a target of phishing attacks
- Individual trust

All rights reserved. Copyright held by Gurpreet Dhillon, PhD

31

Security Challenges - April 23, 2015



MYTH 3

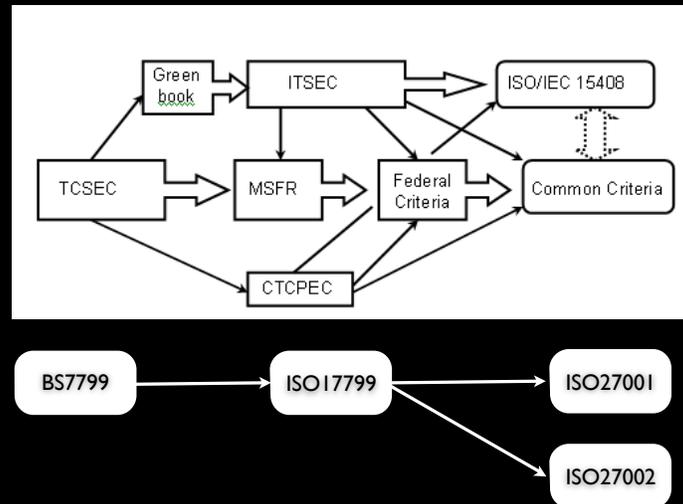
WE HAVE ADOPTED 'XYZ'
STANDARD

All rights reserved. Copyright held by Gurpreet Dhillon, PhD

32

Security Challenges - April 23, 2015

Which one?



All rights reserved. Copyright held by Gurpreet Dhillon, PhD

33

Security Challenges - April 23, 2015

Standardization??

- NIST 800 series
- ISO
- SSE-CMM
-

- Unfortunately these are all outdated ... even before the international community adopted them.

All rights reserved. Copyright held by Gurpreet Dhillon, PhD

34

Security Challenges - April 23, 2015

THEOREM

Every horse has an infinite number of legs.

PROOF

At the back a horse has two legs, and at the front a horse has fore legs.

So the total number of legs on any horse is two plus fore = six, an even number.

But six is an odd number of legs for a horse to have! Hence we have shown that a horse has a number of legs that is both even and odd.

The only number that is both even and odd is infinity, therefore a horse must have an infinite number of legs.

End of proof.

Flawed assumption

THEOREM
Every horse

Interpretation error

PROOF

At the back a horse has two legs, and at the front a horse has fore legs.

Computational error

So the total number of legs on any horse is two plus fore = six, an even number.

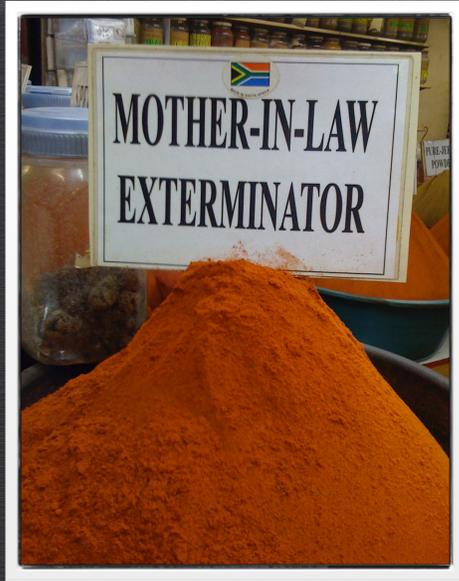
Derivation error

But six is an odd number of legs for a horse to have! Hence we have shown that a horse has a number of legs that is both even and odd.

Usefulness error

The only number that is both even and odd is infinity, therefore a horse must have an infinite number of legs.

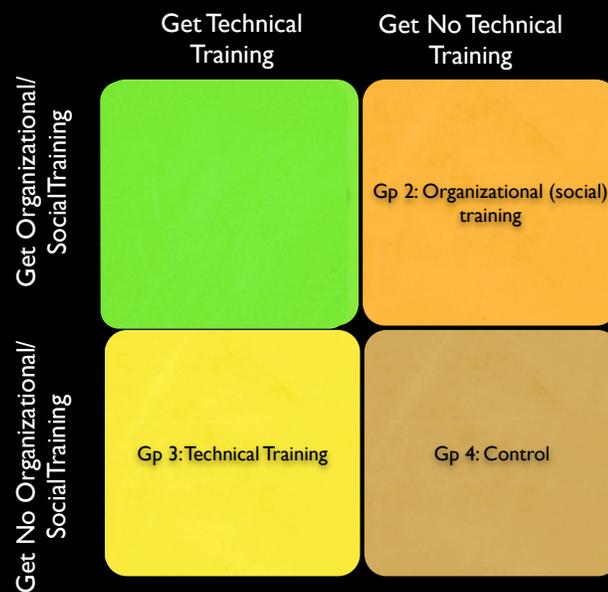
End of proof.



MYTH 4

WE HAVE A GOOD SECURITY AWARENESS PROGRAM

All rights reserved. Copyright held by Gurpreet Dhillon, PhD



All rights reserved. Copyright held by Gurpreet Dhillon, PhD

- (1) Ensure password protection is fully utilized
- (2) Ensure training covers employee integrity
- (3) Ensure data confidentiality policies are in place
- (4) Ensure a trust relationship between employees and the organization
- (5) Ensure appropriate ethics training
- (6) Ensure TECHNOLOGICAL competence

All rights reserved. Copyright held by Gurpreet Dhillon, PhD

What we learned...

1. Form vs. content
2. Type of content
3. Security training is like building a sub-culture

Opportunity

Nearly 80% of security breaches begin with an insider "tweaking" around with a business process control rather than a computer.

Used around 55% of the time.

All rights reserved. Copyright held by Gurpreet Dhillon, PhD

Questions

All rights reserved. Copyright held by Gurpreet Dhillon, PhD