Understanding human nature

Disgruntled
Definitely cause intentional harm

Disgruntled
Likely to cause intentional harm

12%

Not engaged at work
Unlikely to cause intentional harm

Fully engaged at work
Unlikely to cause intentional harm

12 out of 100 humans are likely to cause intentional harm

Source: Gallup- http://www.gallup.com/strategicconsulting/164735/state-global-workplace.aspx
Source: CERT - https://insights.sei.cmu.edu/insider-threat/2015/07/handling-threats-from-disgruntled-employees.html

Trust humans at your own

RISK

Cyber attacks are increasing ↑ day by day

We all know this

The Insecurity of things

Medical Devices
Potentially deadly vulnerabilities

Smart TVs
Internet-connected TVs are vulnerable to click fraud, botnets, data theft and even ransomware
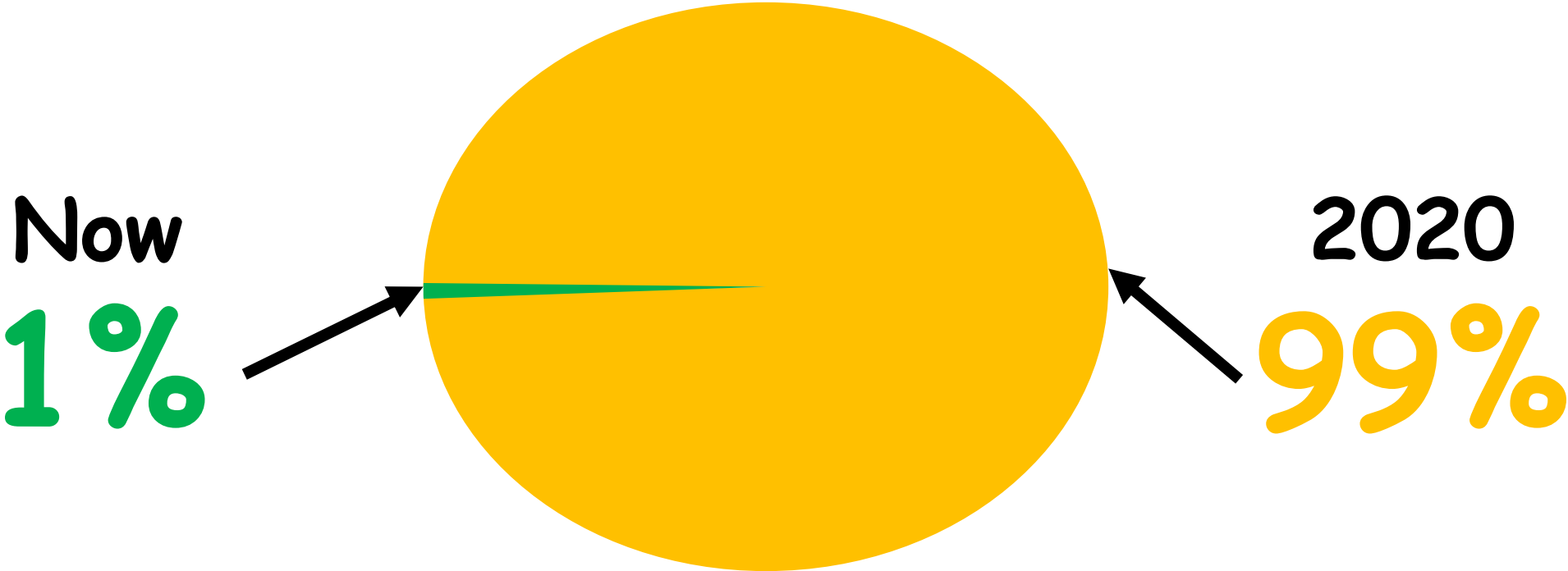
Driverless Cars
Fiat Chrysler recalled 1.4 million vehicles after a proof of concept attack to take control of the vehicle remotely.
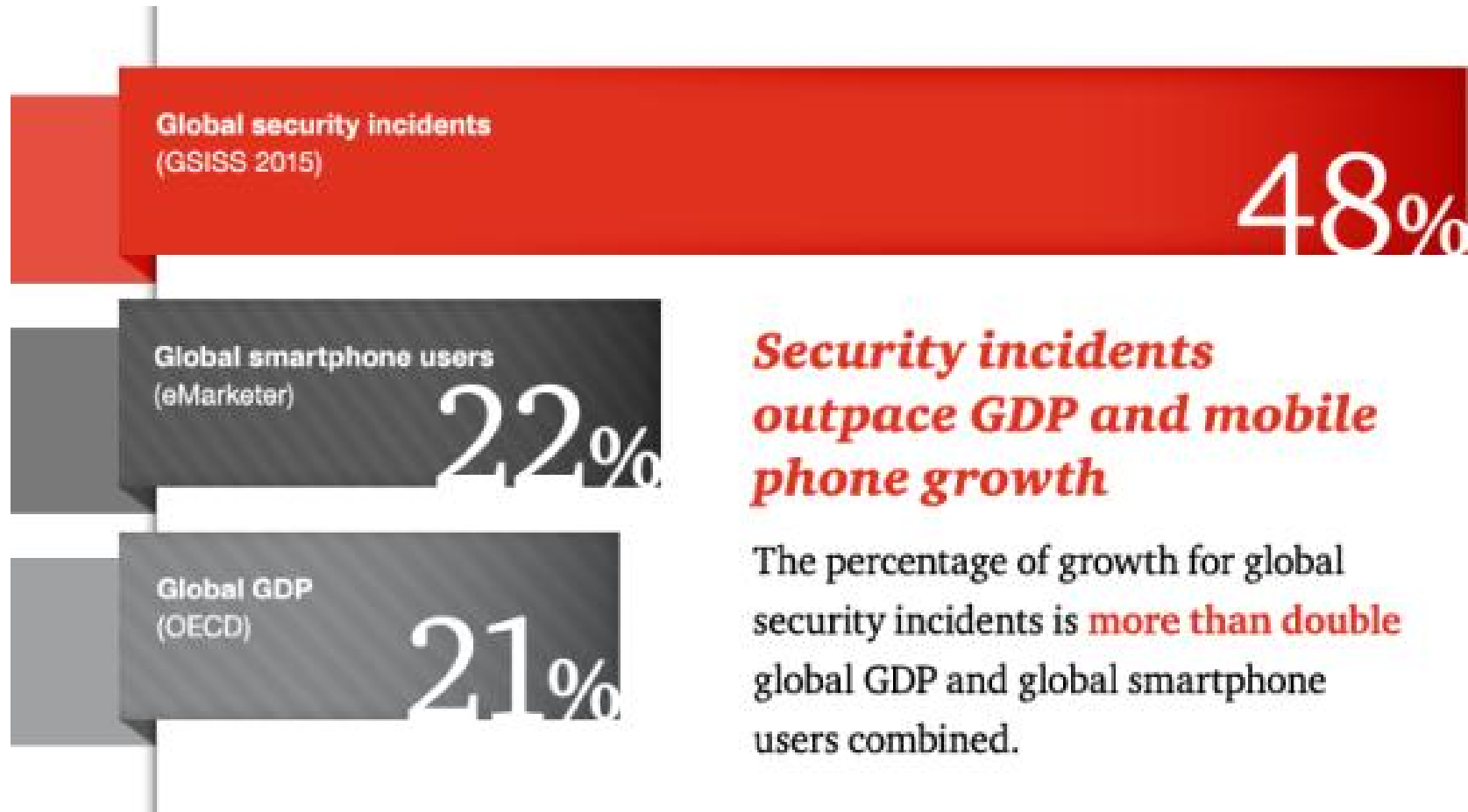
Smart Homes
Home automation systems – vulnerable?

Number of devices connected to Internet

Now
1%

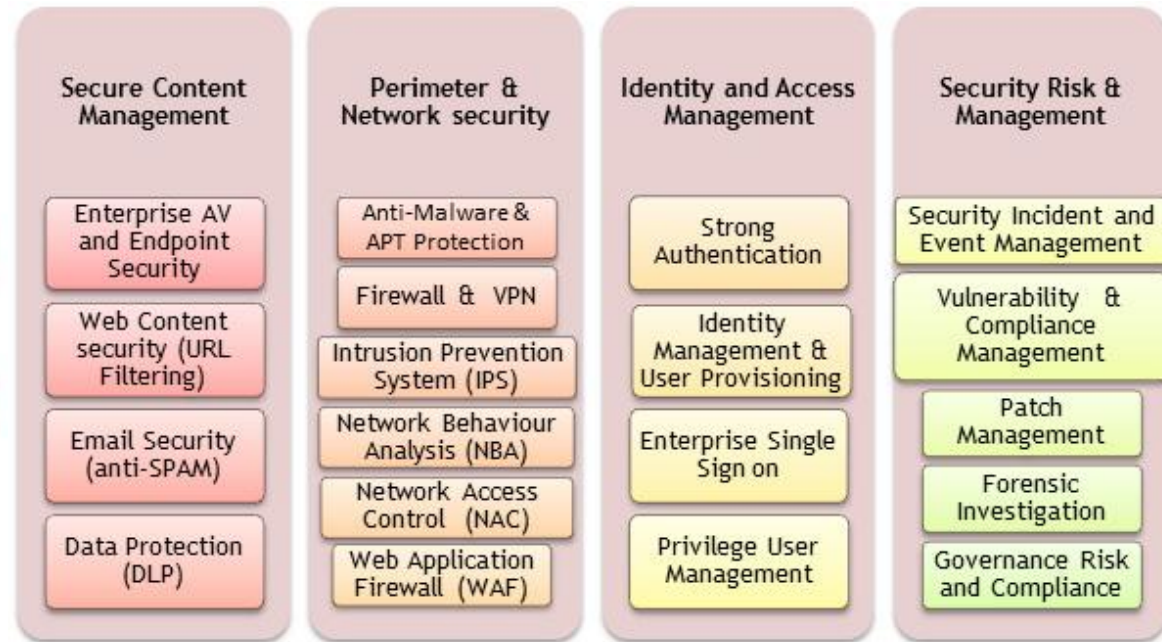2020
99%

Are we ready for this?

And increasing number of devices, leads to increasing number of security incidents…

Global security incidents (GSISS 2015)	**48%**
Global smartphone users (eMarketer)	**22%**
Global GDP (OECD)	**21%**

Security incidents outpace GDP and mobile phone growth

The percentage of growth for global security incidents is **more than double** global GDP and global smartphone users combined.

Cyber solutions

Cyber Security Solutions

- Information Security Policy
- Comprehensive Cyber Security Solution
- Access Control Solutions
- Cyber investigation
- Vulnerability Analysis
- Cyber Hygiene
- Gap Analysis
- Data Leak Prevention Solutions
- Penetration Testing
- Cyber Security Surveys
- Web Application Security Testing
- Security Products Identification
- Information Security Policy Design
- Log Analysis / Network Traffic Analysis

Secure Content Management
- Enterprise AV and Endpoint Security
- Web Content security (URL Filtering)
- Email Security (anti-SPAM)
- Data Protection (DLP)

Perimeter & Network security
- Anti-Malware & APT Protection
- Firewall & VPN
- Intrusion Prevention System (IPS)
- Network Behaviour Analysis (NBA)
- Network Access Control (NAC)
- Web Application Firewall (WAF)

Identity and Access Management
- Strong Authentication
- Identity Management & User Provisioning
- Enterprise Single Sign on
- Privilege User Management

Security Risk & Management
- Security Incident and Event Management
- Vulnerability & Compliance Management
- Patch Management
- Forensic Investigation
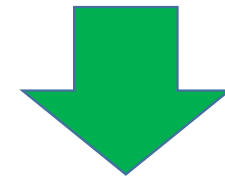- Governance Risk and Compliance

Advanced Cyber
Security Solution

+

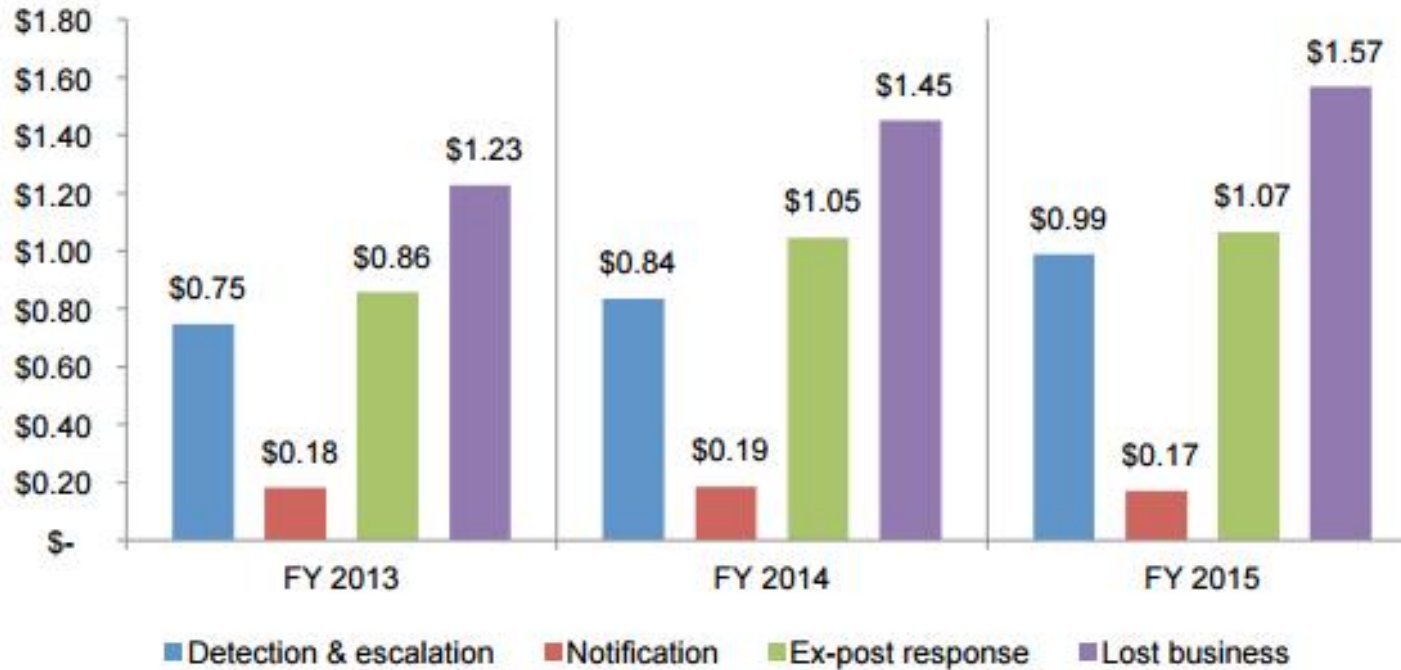Increased budget for
cyber security solutions

Should result in

Reduced Cyber Incidents???

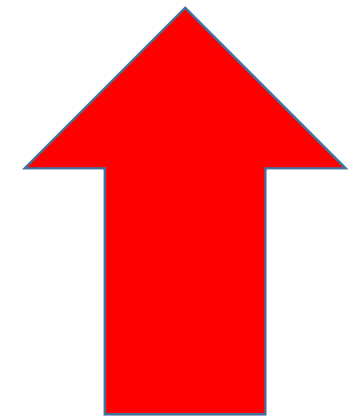# Figure 13. Trends in four data breach cost components over three years

Consolidated view (FY 2015 = 350, FY 2014 = 315, FY 2013 = 277)
Measured in US$ (millions)

	FY 2013	FY 2014	FY 2015
Detection & escalation	$0.75	$0.84	$0.99
Notification	$0.18	$0.19	$0.17
Ex-post response	$0.86	$1.05	$1.07
Lost business	$1.23	$1.45	$1.57

■ Detection & escalation   ■ Notification   ■ Ex-post response   ■ Lost business

Source: IBM - http://www-03.ibm.com/security/data-breach/

Cyber crimes are increasing

Reduced Cyber Incidents???

Cyber Threat Is

Technology + Humans

Fool-Proof Technology

Speed limit on accelerators: The vehicle will never violate the speed limit

Fool-Trap Technology
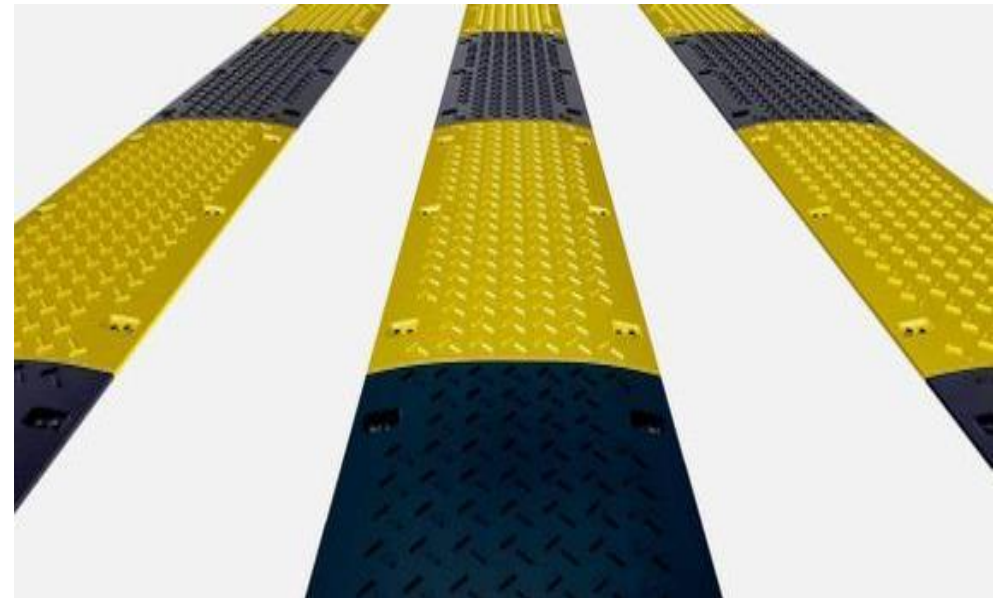
Speed breakers on the road: Driver may violate the speed limit and get injured before hitting someone else

# Most plane crashes in the world have happened due to human/pilot error

*According to Boeing, **close to 80% percent of accidents caused by pilot error**. The other 20% are mainly due to faulty equipment and unsafe, weather-related flying conditions.*

Causes of fatal accidents (1950-2009)

Cause	1950s	1960s	1970s	1980s	1990s	2000s	Total
Pilot error	58%	57%	42%	44%	53%	46%	50%
Other human error	0%	8%	9%	6%	8%	8%	6%
Weather	16%	10%	13%	15%	9%	9%	12%
Mechanical failure	21%	20%	23%	21%	21%	28%	22%
Sabotage	5%	5%	11%	13%	10%	9%	9%
Other	0%	2%	2%	1%	0%	1%	1%

Source: www.planecrashinfo.com. Taken from database of 1,300 fatal accidents involving commercial aircraft with more than 10 people on board, for which a specific cause is known. "Other human error" includes air traffic controllers and improper maintenance. "Sabotage" includes explosive devices and hijackings.

Technology is no match for Human **Errrur**..

95%
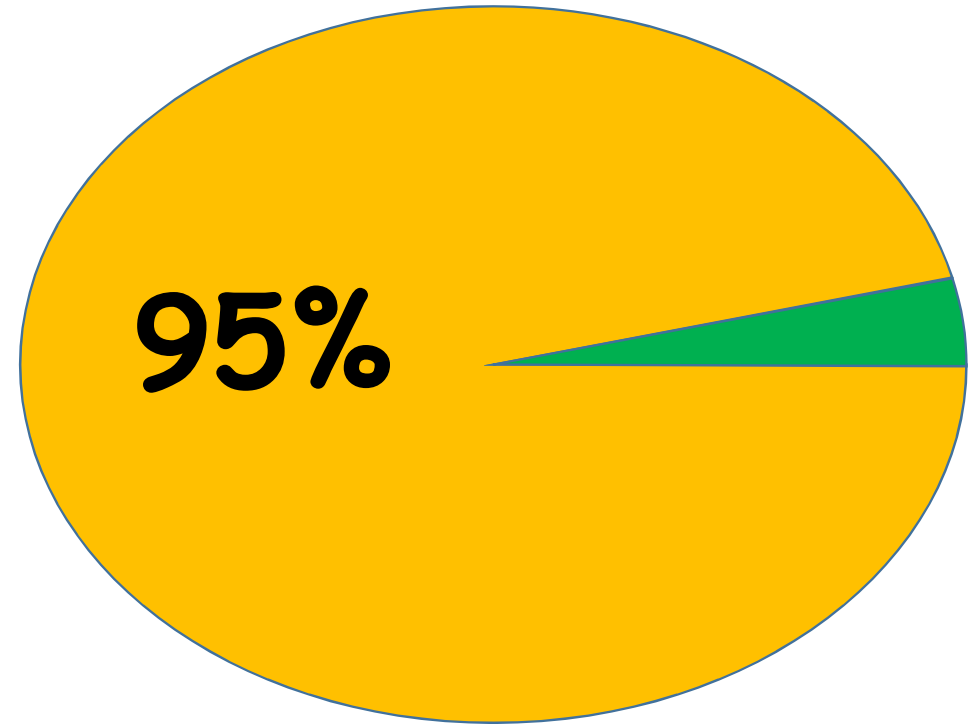
95% of all security incidents involve **human error**.

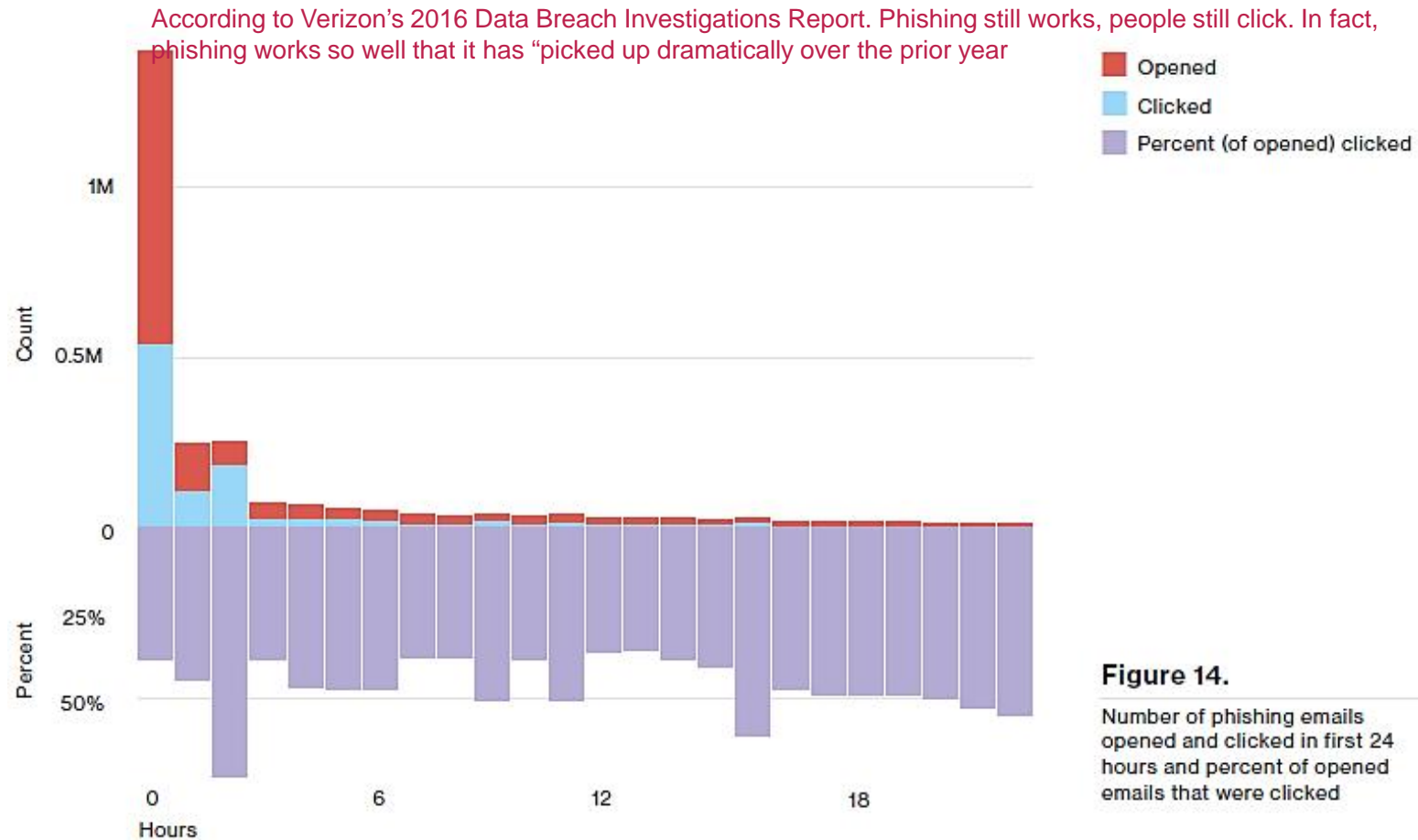# 30% of phishing emails are opened by the intended target

According to Verizon's 2016 Data Breach Investigations Report. Phishing still works, people still click. In fact, phishing works so well that it has "picked up dramatically over the prior year

Figure 14.

Number of phishing emails opened and clicked in first 24 hours and percent of opened emails that were clicked

Source: Verizon – 2016 Data breach investigations report

Human factors

Human error

Fraud

Document Classification: KPMG Confidential

Types of human risks

Intentional   **Accidental**

- Malicious intent
- Stealing
- Damaging
- Misuse
- Disgruntled
- ……

- Lack of awareness
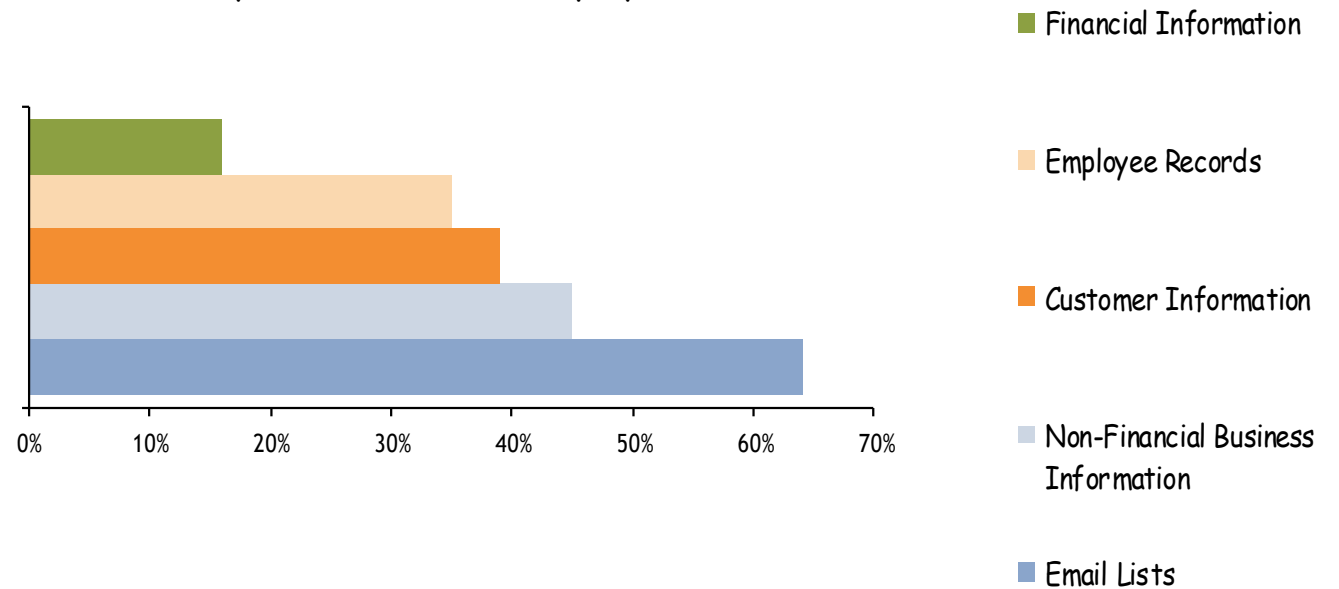- Mishap
- Thoughtlessness
- Neglect
- Irresponsibility
- ……

Let's make some choices

Economist.com

Option #1:

Print only subscription   **14%** $59

Option #2:

Internet only subscription   **0%** $125

Option #3:

Print + Internet subscription   **86%** $125

Economist.com

Option #1:

Print only subscription   **66%** $59

Option #2:

Print + Internet subscription   **32%** $125
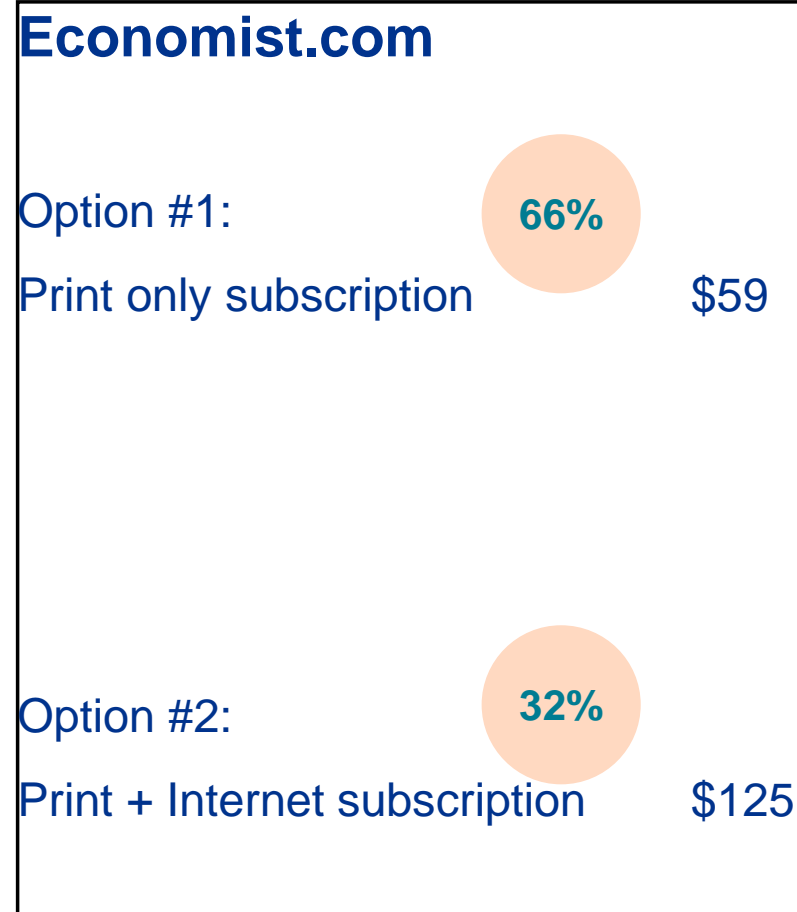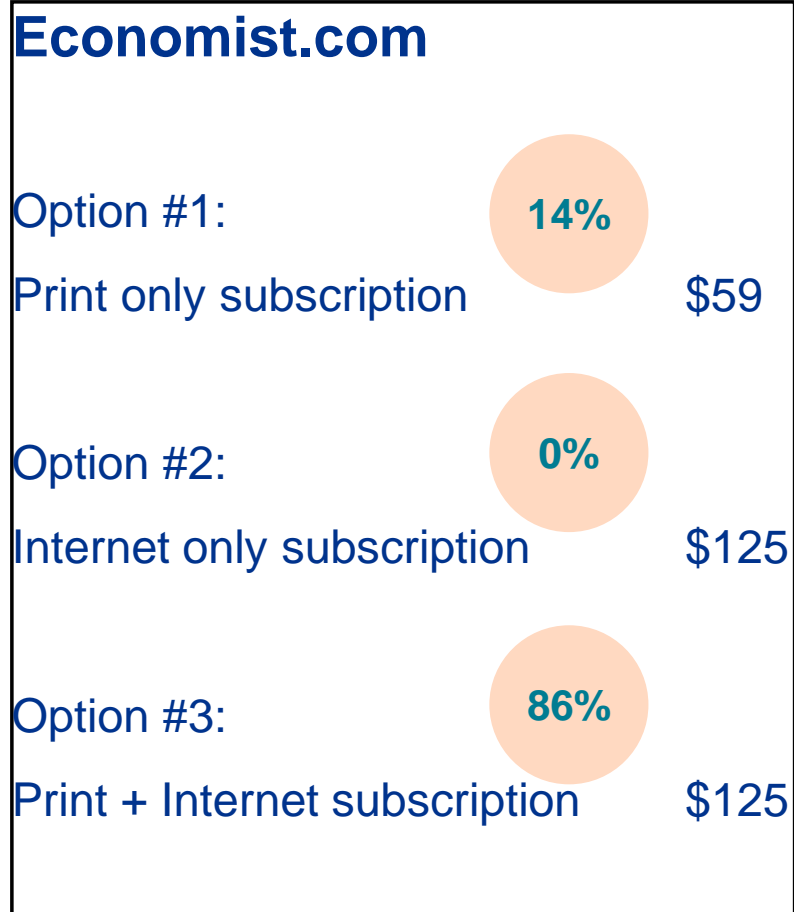
Irrespective of what you do, **69%** of all Ex-Employees Leave with Organizational Data

Data Most Likely Stolen from Ex-Employers

- Financial Information
- Employee Records
- Customer Information
- Non-Financial Business Information
- Email Lists

Let's investigate honesty

The highlighter pen syndrome
And
Coke vs $1 bill

Let's investigate honesty

20 question test

❖ Experiment #1

  – Fill out answer sheet

  – Transfer scores on bubble sheet

  – Hand over both sheets to examiner

  – Examiner scores

  – Receive money

❖ Experiment #2

  – Fill out answer sheet

  – Transfer scores on bubble sheet having right answers ticked already

  – Shred the answer sheet

  – Hand over bubble sheet to examiner

  – Examiner counts right answers

  – Receive money

❖ Experiment #3

  – Fill out answer sheet

  – Transfer scores on bubble sheet having right answers ticked already

  – Shred the answer sheet

  – Count the correct answers

  – Collect token from examiner

  – Collect money in exchange of token

Let's investigate honesty – new dimension

Experiment #	Description	Scores
#1	Control group – direct cash	3.5
#2	Self check + shredding – direct cash	6.2
#3	Self check + shredding – token – then cash	9.4

Cash experiment

Total cheating : 4 out of 2,000

Token experiment

Total cheating : 320 out of 2,000

Conclusions:

❑ Take the cash just one step away and people may cheat wildly

❑ Imagine the risks of frauds in truly digital cash economy!

Cyber Security
...Myths

Clearly, Neither **Positive** Motivation
nor **Negative** Message is helping

Knowledge ≠ Action

subtle to **direct**

Messages have gone from

Result?
1. Number of smokers increased
2. Number of deaths increased

If knowledge meant action,
whole world would be a healthy place ☺

Humans are essentially

Machine + Mind
Technology + Trust

Easier to control

Difficult to control

Humans are difficult to control and understand

God as guard: Bank opens 'lockless' branch

Shani Shingnapur attracts about 40,000 devotees each day due to its remarkable 300-year-old legend.

By Swati Jain
31 May 2016

Imagine a village where homes have no front doors, shops are always left unlocked and locals never feel unsafe.
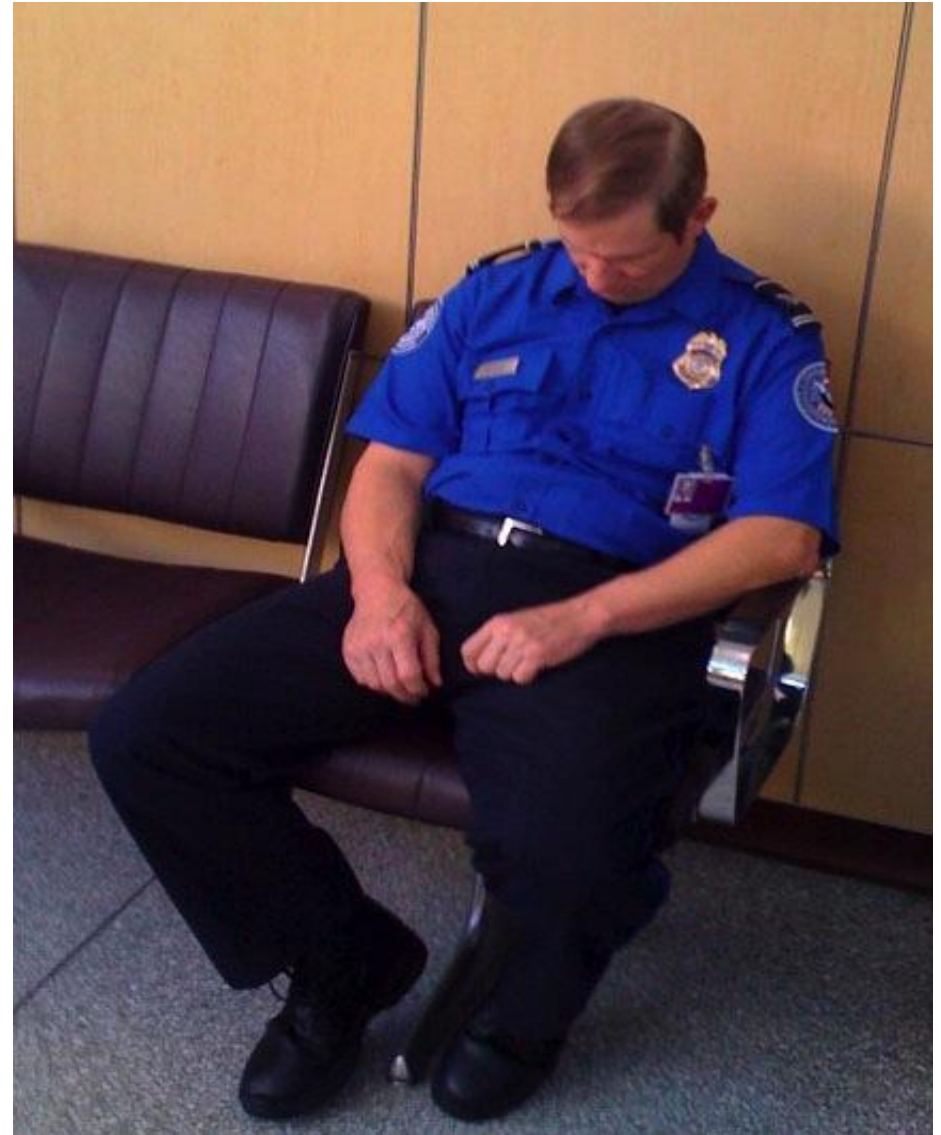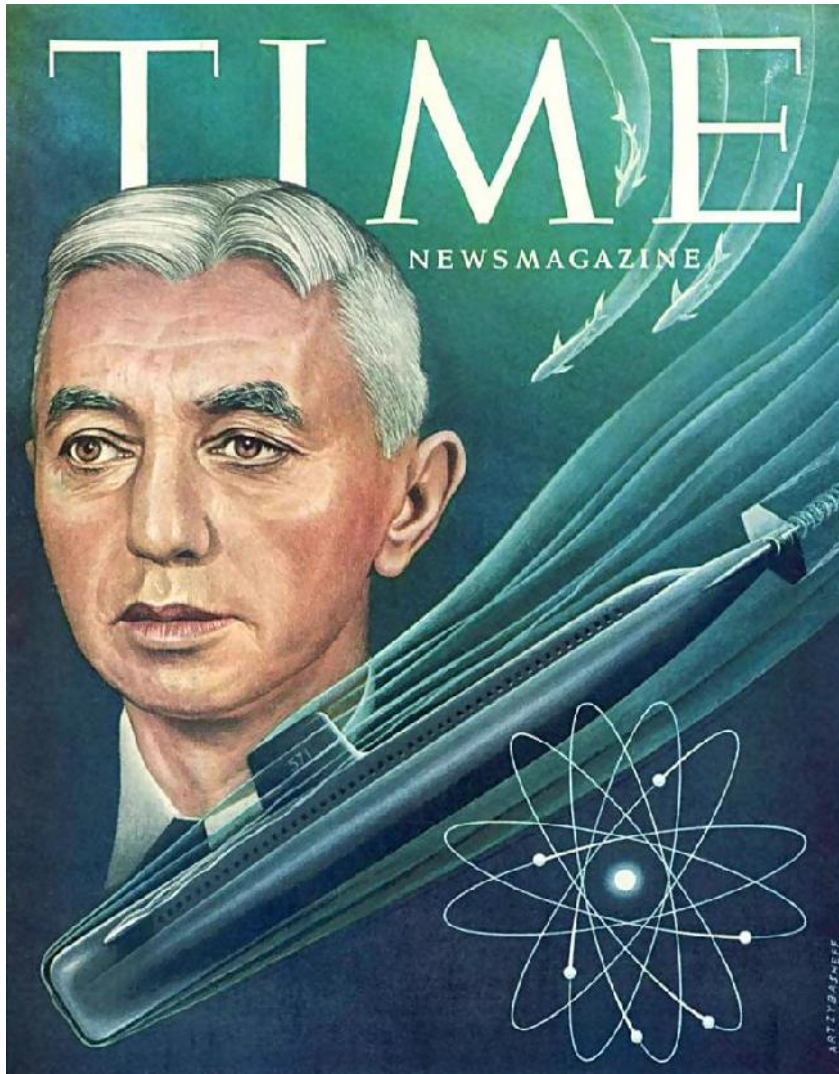
Are we ready for the

NEW WORLD?

The story of AJ & Bobby

What Is the
Solution?
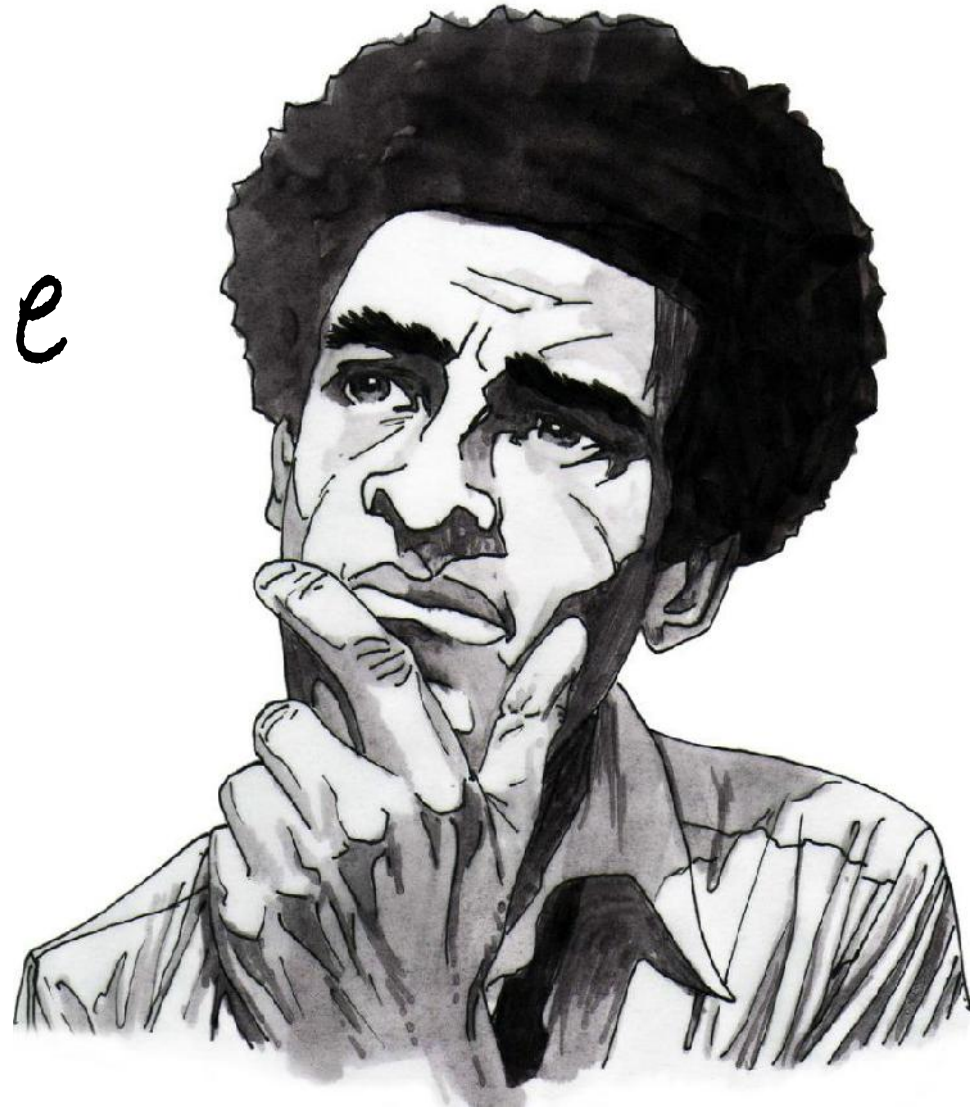
Traditional security measures are not enough

Admiral Hyman Rickover
"Father of the Nuclear Navy"

launched
The nuclear-propulsion program

No accident in 60 years

Rickover focused intensely on the human factor, U.S. Department of Defense for its cyber security had adopted similar protocol.

Human factors fundamentals adopted from Rickover

Integrity and continuous awareness	Making everyone accountable	Procedural compliance	An unquestionable attitude
Technical Capability Human Excellence	Check up on your defenses	Institute uniform standards and centrally managed training and certification	
Eliminate fear of honesty and increase the consequences of dishonesty		Depth of knowledge	Formality in communication

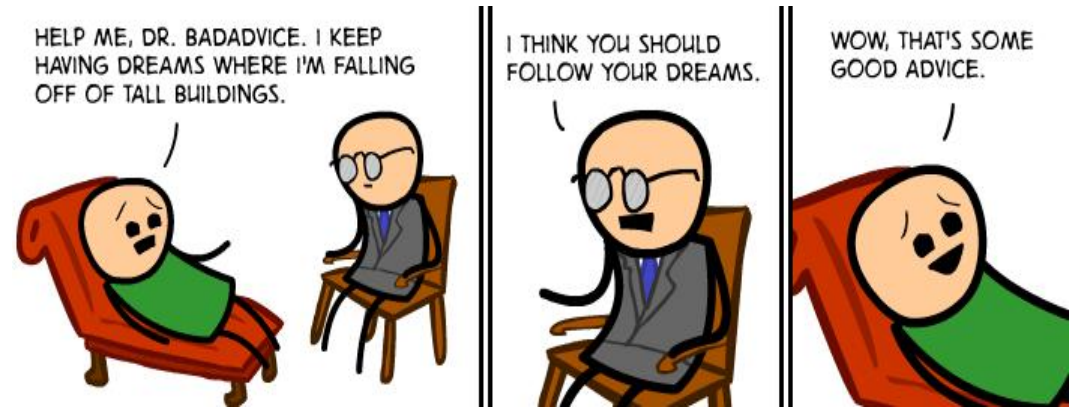"We have to get beyond focusing on just the tech piece. It's about ethos. It's about culture."

- Admiral Mike Rogers, U.S. Cyber Command

Awareness

We Know

+

Behavior

We do

=

Culture

We know
&
We do

Change in behavior is required to take action

ADVOCATE

Should Consultants Advice (Knowledge)?

Should Consultants Advocate (action)?

Cyber security consultants are approaching to handle human risks by understanding the **environment** and causing change in **culture and behavior**...

Doing without doing…

Once people adopt the right behavior, complying with cyber security will become second nature!

Leonard Bernstein
Haydn Symphony No 88

Akhilesh Tuteja

KPMG Global Cyber Security Co-Head
Building No. 10, 8th Floor, Tower B & C, DLF Cyber
City, Phase II Gurgaon Haryana - 122 002
Phone: +919871025500
E-mail: atuteja@kpmg.com