Global State of Information Security & Standards

SGS

Khawaja Faisal Javed, *CISA,CRISC,CBCP,ISMS LA, BCMS LA ITSM LA*
Manager of Operations & ICT Products
SGS Pakistan (P) Ltd.
President, ISACA Lahore Chapter

ISACA
Serving IT Governance Professionals
Lahore Chapter

Khawaja Faisal Javed

Manager Operations & ICT Products
SGS Pakistan (Pvt) Limited

President - ISACA Lahore Chapter
Member of International GRA Committee - ISACA, USA

Kh. Faisal Javed - Profile

- **Manager Operations & ICT Products (SGS Pakistan)**
- President of ISACA Lahore Chapter
- **Showcase Honoree Award for the Senior Information Security Professional– Asia-Pacific by (ISC)2, USA - 2012 -** https://www.isc2.org/isla-showcased-projects.aspx
- **20+ years of ICT, GRC, Info Sec, BPR, IT Services BCP/DRP**
- Member of Int'l Committees in **IT GRC** for organizations – **ISACA, IRCA, DRI**
- Member of the Team **developed ISO 27007** Standard (Auditing ISMS Guideline)
- Number of Certifications :
  - **CISA, CRISC, CBCP**
  - **IRCA, UK registered Lead Auditor and Lead Trainer for ISMS, ITSMS, BCMS, QMS, EMS, OHSAS etc.**
- **Only IRCA, UK approved Lead Auditor/Trainer for ISO 20000 & ISO 22301 in Pakistan**
- **900+** third party Audits & **4500+ HRS** of Training in **32 countries...**
  - (USA/Australia/Turkey/Malaysia/Indonesia/ Japan/ Taiwan/ Saudi Arabia / India/ Egypt/ Philippines/Jordon/ Kuwait / Qatar / Oman / UAE etc.)

WHEN YOU NEED TO BE SURE

SGS

SGS Profile

- Established in **1878 -** Head Office in Geneva, Switzerland
- **78'000+** employees incl. **1'000+** full-time lead auditors
- **1'200+** offices Laboratories in **140+** countries
- SGS is recognized as the **global benchmark in quality and integrity leader**
- **1'10'000+** certified organizations worldwide
- **UKAS** accredited **ISO 27001** Certification Body
- ***APMG*** accredited **ISO 20000** Certification body
- **UKAS** accredited **BS 25999 / ISO 22301** Certification body

No1

Certification body*

100’000+ certificates

in 130+ countries

ISACA®

Serving IT Governance Professionals

ISACA Serving IT Governance Professionals Lahore Chapter

Kh. Faisal Javed, CISA,CRISC,CBCP,IRCA / 2013

SGS

What is ISACA?

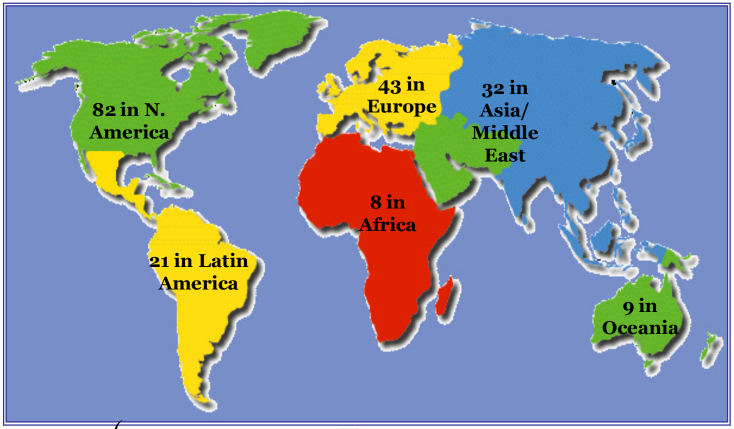
- **Non-profit association of individual members:**
  - IT auditors
  - IT security professionals
  - IT risk and compliance professionals
  - IT governance professionals and more!
- **Nearly all industry categories**: financial, public accounting, government/public sector, technology, utilities and manufacturing.

What is ISACA?
Structure

One International Headquarters Office

200+ Chapters in **75+ Countries**

Over **95,000 members** in **100+ countries**



(*Source: ISACA International data*)

ISACA Certifications

www.isaca.org/certification

CISA® Certified Information Systems Auditor® An ISACA® Certification

CGEIT® Certified in the Governance of Enterprise IT® An ISACA® Certification

CISM® Certified Information Security Manager® An ISACA® Certification

CRISC™ Certified in Risk and Information System Controls An ISACA® Certification

ISACA® NEXT EXAM DATE 8 JUNE 2013 Get Certified>

CISA Certified Information Systems Auditor · CISM Certified Information Security Manager · CGEIT Certified in the Governance of Enterprise IT · CRISC Certified in Risk and Information Systems Control™

ISACA® Serving IT Governance Professionals Lahore Chapter

Kh. Faisal Javed, CISA,CRISC,CBCP,IRCA / 2013

SGS

Agenda

- Trends
- Shifting Dimensions of the Global Threat?
- Facts About Intrusions
- What’s the Challenge ?
- A Way Ahead…..
- Standards /Frameworks available
- Q & A

ISACA® Serving IT Governance Professionals Lahore Chapter

Kh. Faisal Javed, CISA,CRISC,CBCP,IRCA / 2013

SGS

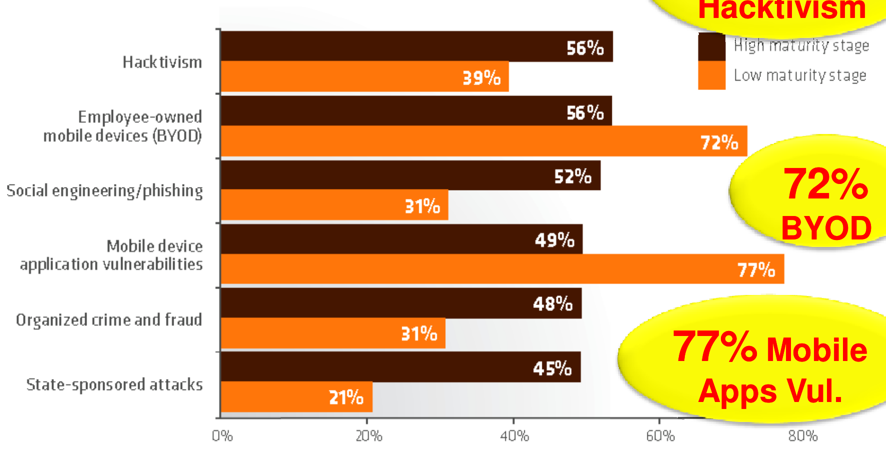
The Heart Of the Matter

For many businesses, security has become a game that is almost impossible to win. The rules have changed, and opponents–old & New - are armed with Xpert technology skills & risks are greater than ever!

Threats to Info Sec. Org. Face

FIGURE 27. Threats to information security that organizations face

Concerned and Very concerned response combined



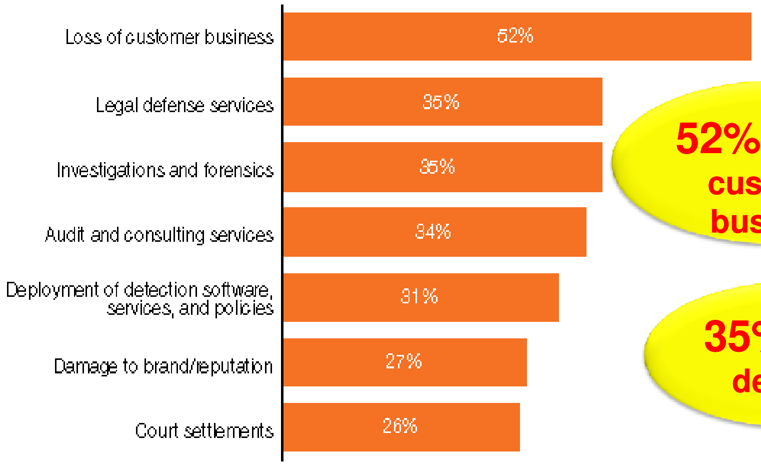
56% Hacktivism

72% BYOD

77% Mobile Apps Vul.

Source: Ponemon Institute study - 2013

Factors in financial losses from security breaches



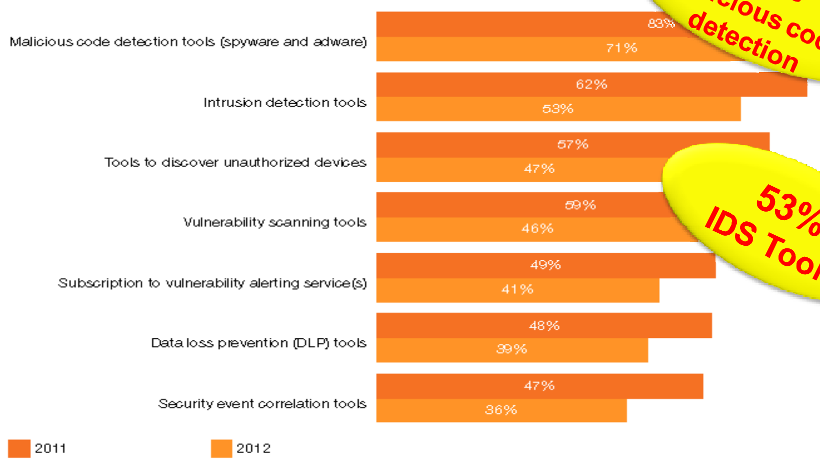
52% Loss of customer business

35% Legal defence

Source: PWC – Global state of InfoSec-2013

Which -Technology as Safeguard?

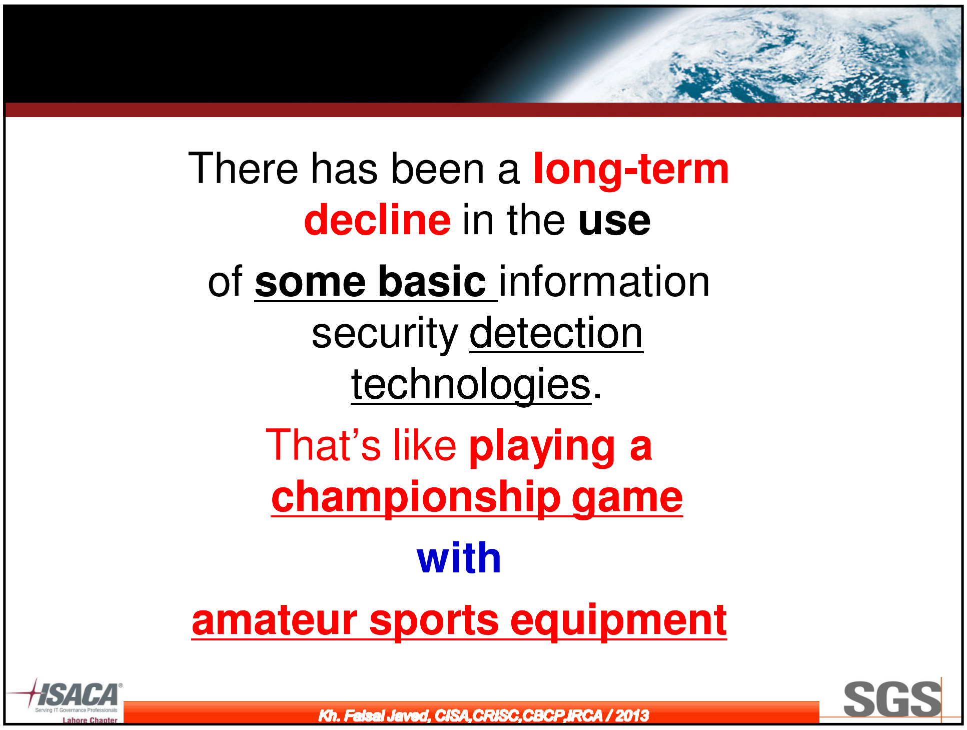
Technology information security sa
currently in place



71% Malicious code detection

53% IDS Tools

Source: PWC – Global state of InfoSec-2013



There has been a **long-term decline** in the **use** of **some basic** information security detection technologies.

That's like **playing a championship game**

with

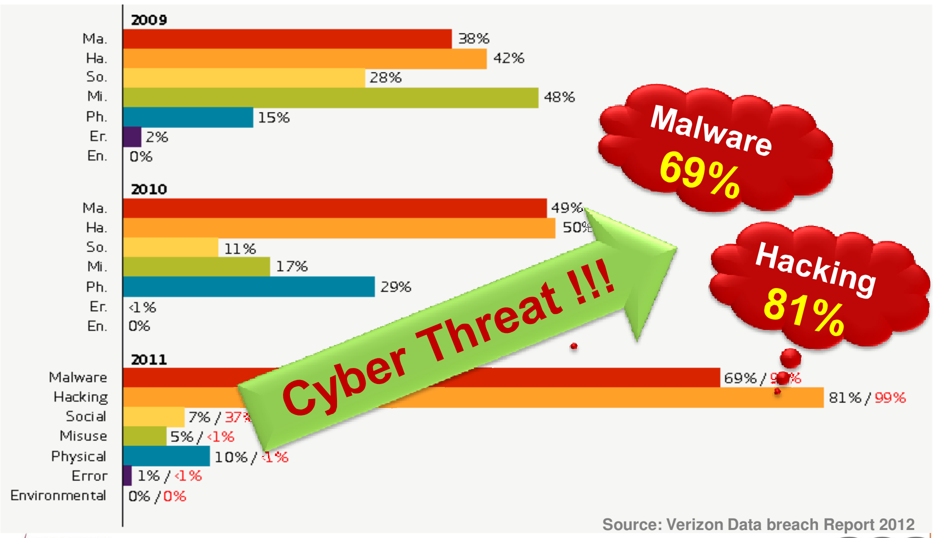
amateur sports equipment

ISACA
Serving IT Governance Professionals
Lahore Chapter
SGS

New Dimensions of the Global Threats

ISACA
Serving IT Governance Professionals
Lahore Chapter
SGS

Threat action categories over time by %age of breaches and %age of records



Source: Verizon Data breach Report 2012

Shifting Dimensions of the Global Threat

Has the Threat Fundamentally Changed in 2011-12?

Event	Why it's significant
CISCO (Counterfeit	CISCO Product Integrity Damaged…$145M seized by FBI
	nClassified Systems
Google	Publicly Identified An Intrusion, Asked for Government Help
Stuxnet / FLAME	High Level Of Sophistication and Target Specific – Cyber Espionage
Wiki Leaks	Insider Threat, Activists Empowered

APTs & Zero-Days Attacks

Lesson: lack of vigilance in a changing landscape increases risk

What Was The Cost Of Being Insecure $$$$

Cyber Threats – *What & Who* ?

- A Cyber Attack on the Specific Database of the Critical System
- A Cyber Attack for the purpose of Espionage
- A Cyber Attack for the purpose of Critical System Shutting down Service : DDoS

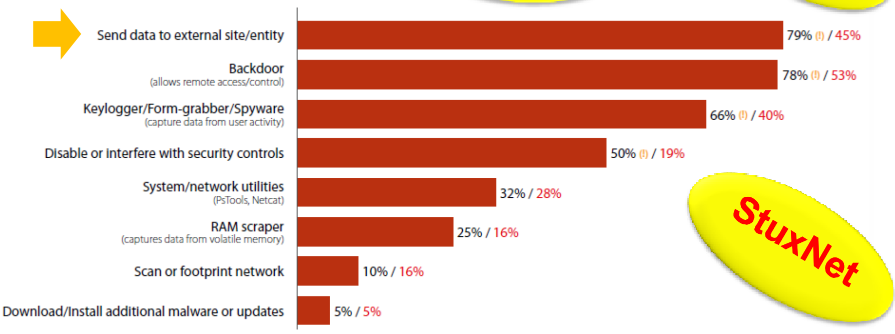
APTs – a Real Threat !

- **Advanced Persistent Threat (APT)** is very real
  - **Malware is now a tool for hacker**
  - **They are stealing data...**

Duqu

Flame

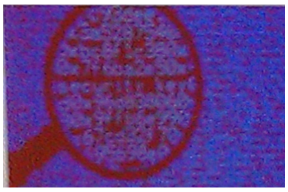
StuxNet



Reference: *2011 Data Breach Investigations Report*, Verizon

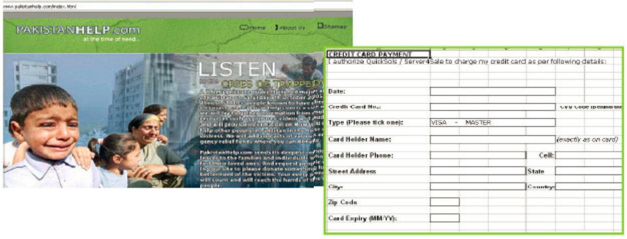
Main Targets

- Military Cyber Structure
- National Critical Infrastructure
  1) Telecommunications
  2) Electronic Power
  3) Gas & Oil
  4) Banking & Finance
  5) Transportation
  6) Water
  7) Emergency Services
  8) Continuity of Government



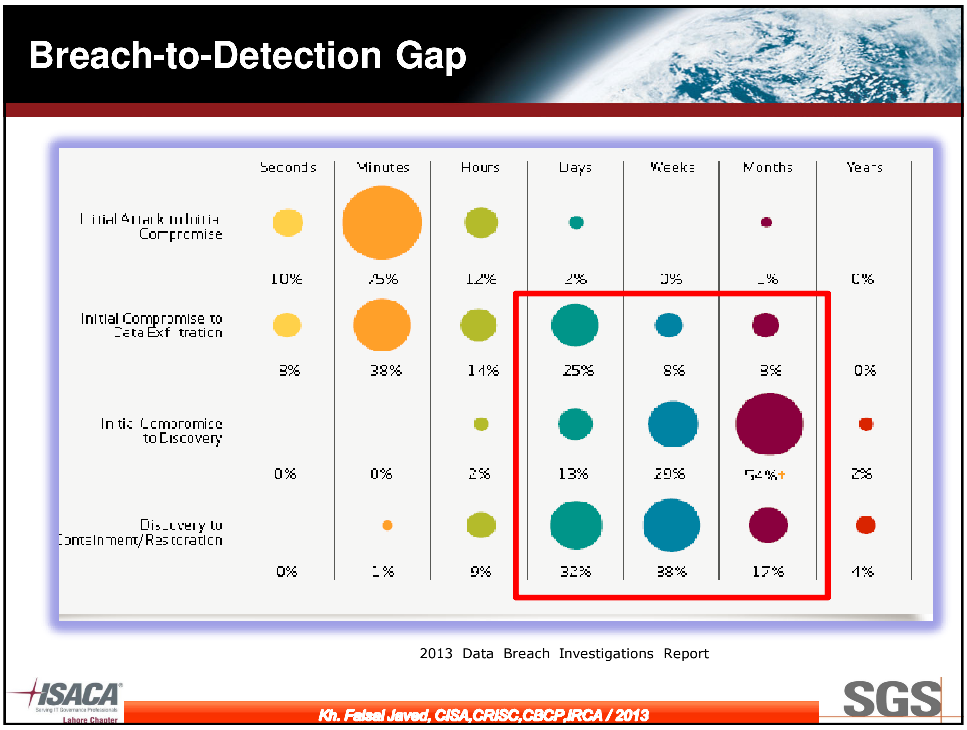
Example – Phishing & Scam

- Pakistan Earthquake – We found the URL http://pakistanhelp.com
- In this case, the '**help**' options include the download of an Excel file to be sent by fax
- A real and legal organization would never do this….



CREDIT CARD PAYMENT
I authorize QuickSols / Server4Sale to charge my credit card as per following details:

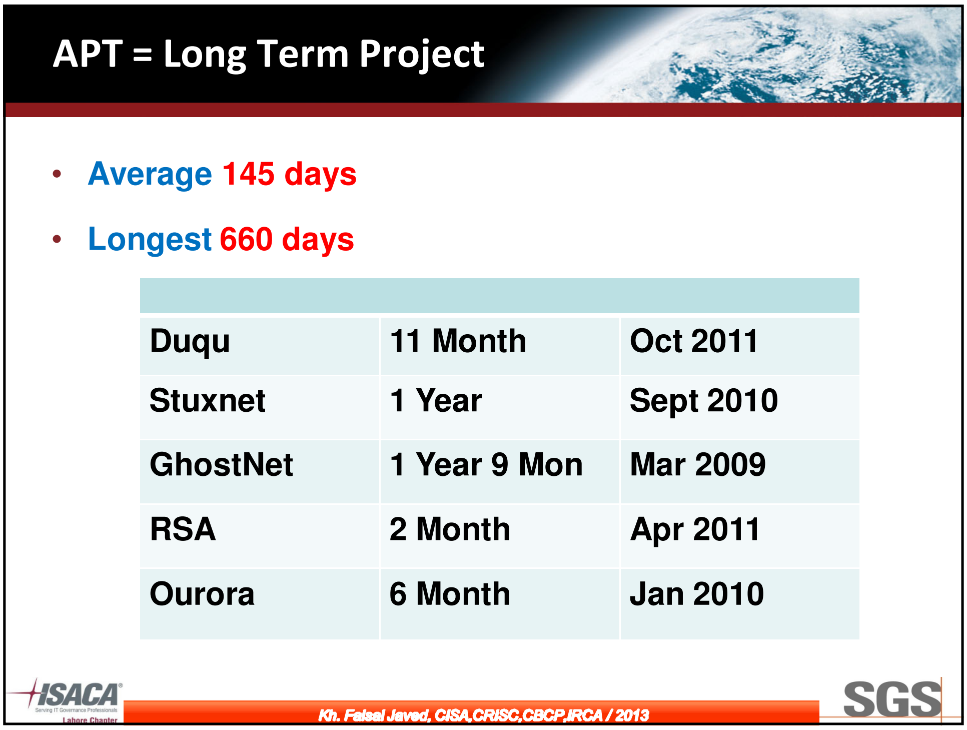
Date:
Credit Card No.:
Type (Please tick one): VISA - MASTER
Card Holder Name: (exactly as on card)
Card Holder Phone: Cell:
Street Address State
City: Country:
Zip Code
Card Expiry (MM/YY):



Breach-to-Detection Gap

	Seconds	Minutes	Hours	Days	Weeks	Months	Years
Initial Attack to Initial Compromise	10%	75%	12%	2%	0%	1%	0%
Initial Compromise to Data Exfiltration	8%	38%	14%	25%	8%	8%	0%
Initial Compromise to Discovery	0%	0%	2%	13%	29%	54%+	2%
Discovery to Containment/Restoration	0%	1%	9%	32%	38%	17%	4%

2013 Data Breach Investigations Report



APT = Long Term Project

- Average 145 days
- Longest 660 days

Duqu	11 Month	Oct 2011
Stuxnet	1 Year	Sept 2010
GhostNet	1 Year 9 Mon	Mar 2009
RSA	2 Month	Apr 2011
Ourora	6 Month	Jan 2010

Flame/ Flamer

- The most Sophisticated & complex Malware encountered – *by Kaspersky Lab*.
- Identified first by MAHER Centre of Iranian National CERT - *Kaspersky Lab in 2012*
- **Aimed at** targeted Cyber Espionage in Middle Eastern countries

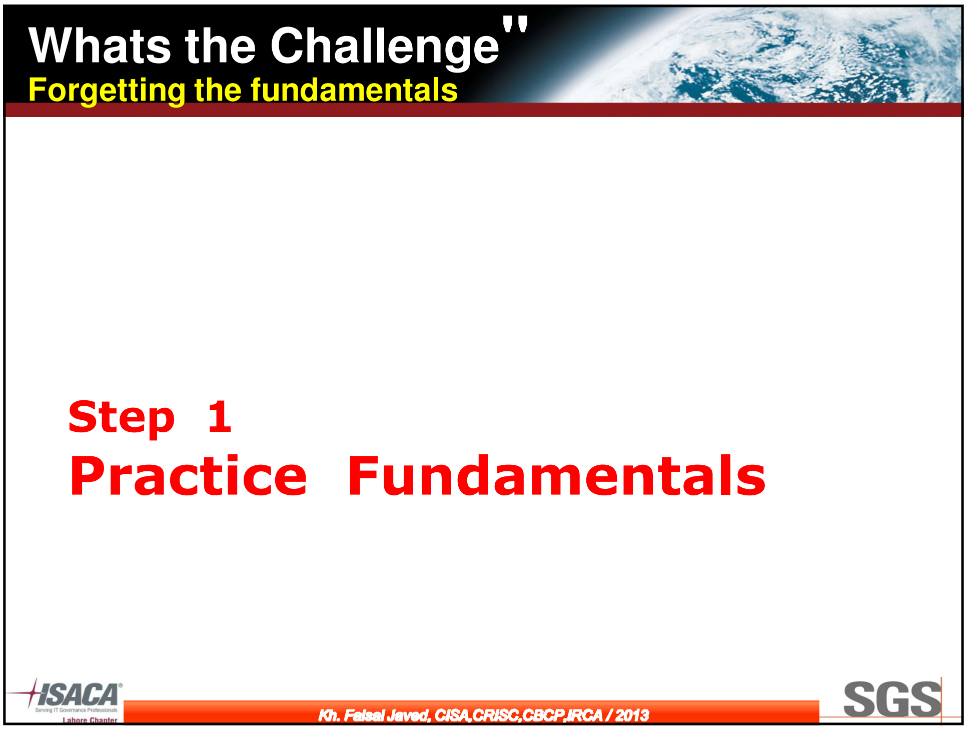
Washington Post

“ the massive piece of malware secretly mapped and monitored Iran’s computer networks, sending back a steady stream of intelligence to prepare for a cyber warfare campaign”s

this is preventable: ***The 80/20 Rule for Cyber Defense***

96 percent of data breaches examined were preventable if companies would have followed security basics.

2011 Data Breach Report V*erizon Business*

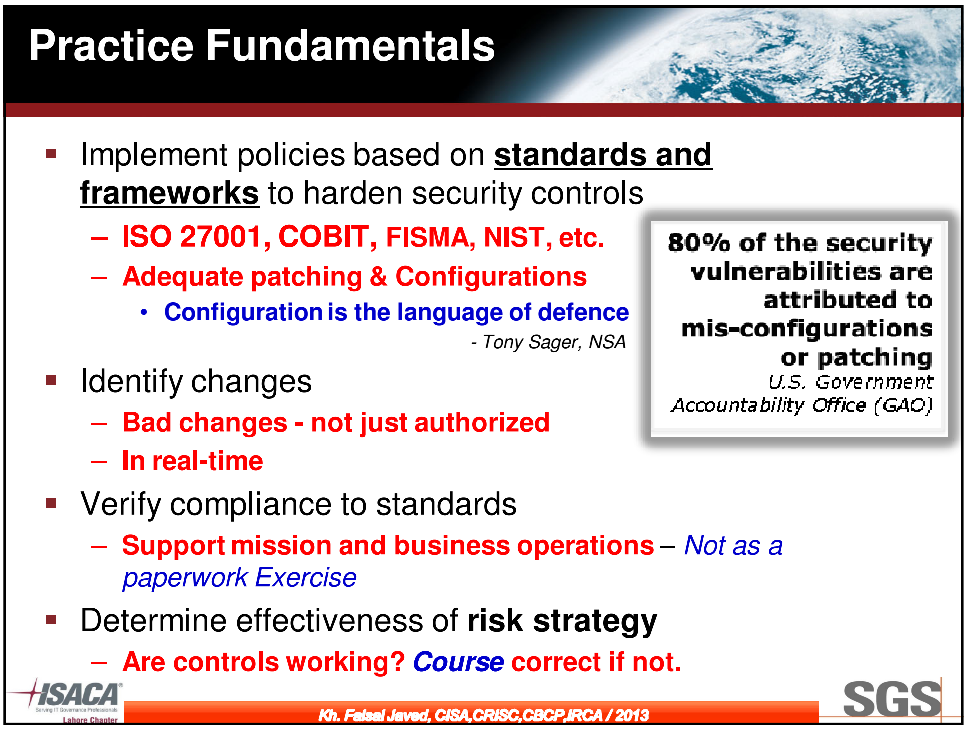


Whats the Challenge"

Forgetting the fundamentals

Step 1

Practice Fundamentals



Practice Fundamentals

- Implement policies based on **standards and frameworks** to harden security controls
  - **ISO 27001, COBIT, FISMA, NIST, etc.**
  - **Adequate patching & Configurations**
    - **Configuration is the language of defence**

      - Tony Sager, NSA
- Identify changes
  - **Bad changes - not just authorized**
  - **In real-time**
- Verify compliance to standards
  - **Support mission and business operations** – *Not as a paperwork Exercise*
- Determine effectiveness of **risk strategy**
  - **Are controls working? *Course* correct if not.**

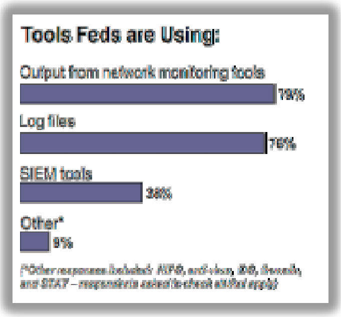
80% of the security vulnerabilities are attributed to mis-configurations or patching

U.S. Government Accountability Office (GAO)

Step 2
Monitor Continuously

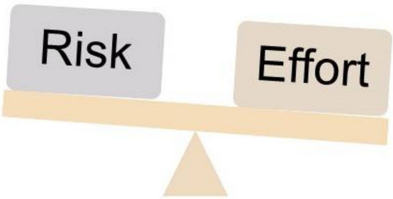
Monitor Continuously

- Categorize assets
  - Prioritize critical not all assets
- Determine level of control
  - Based on criticality of asset
- Make risk-based decisions
  - Answers “what is my security state”



Monitoring

- Comes down to **value of data**



Step 3

Detect Threats fast

Detect Threats Faster

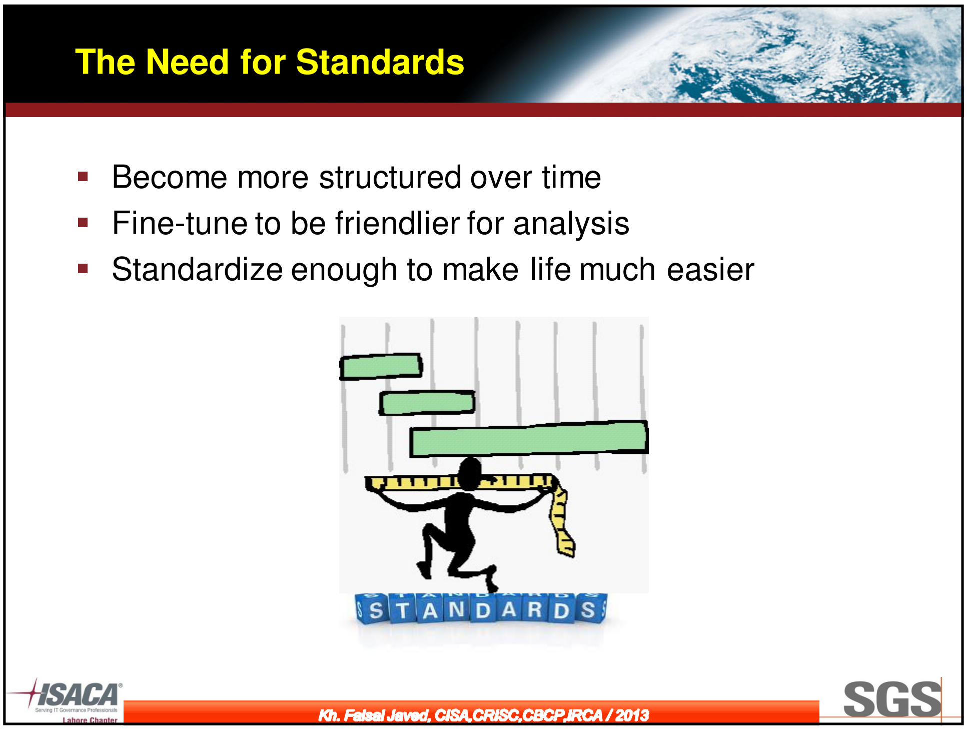
- Reduce massive volume of data
  - Correlate (bad) changes and (suspicious) events
- Dis-till intelligent information
- Respond immediately
  - Get information into the right hands
  - Make risk-based decision

87% of organizations had evidence of the breach in their log files, yet missed it.

2010 Data Breach Report From Verizon Business, U.S. Secret Service)

Standards & Frameworks *Why?*

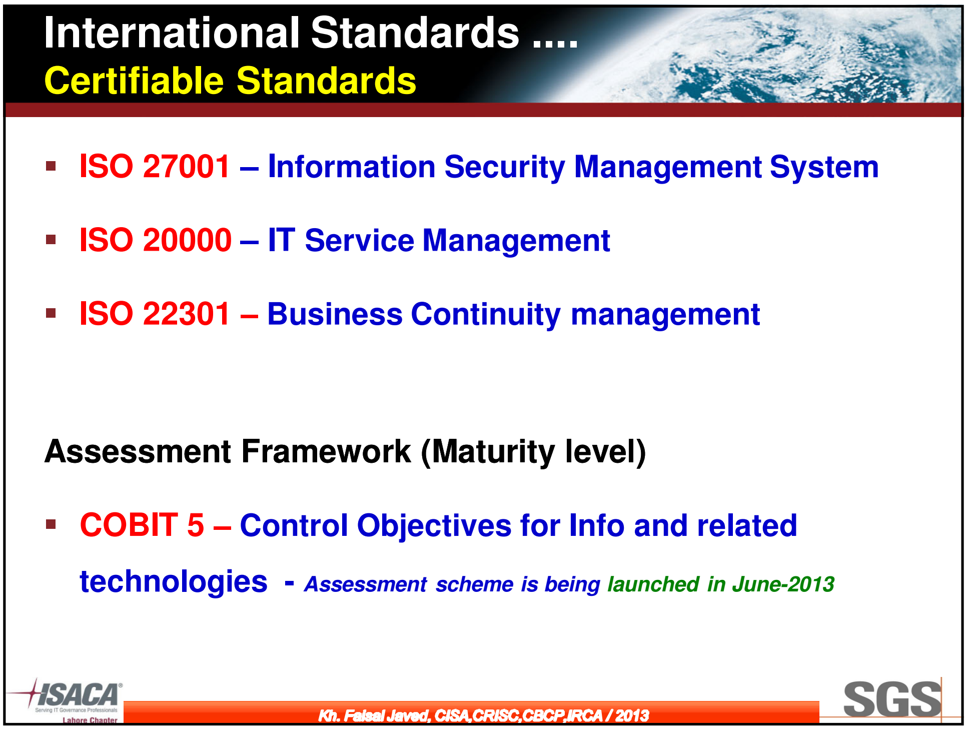
Kh. Faisal Javed, CISA,CRISC,CBCP,IRCA / 2013



The Need for Standards

- Become more structured over time
- Fine-tune to be friendlier for analysis
- Standardize enough to make life much easier

Kh. Faisal Javed, CISA,CRISC,CBCP,IRCA / 2013

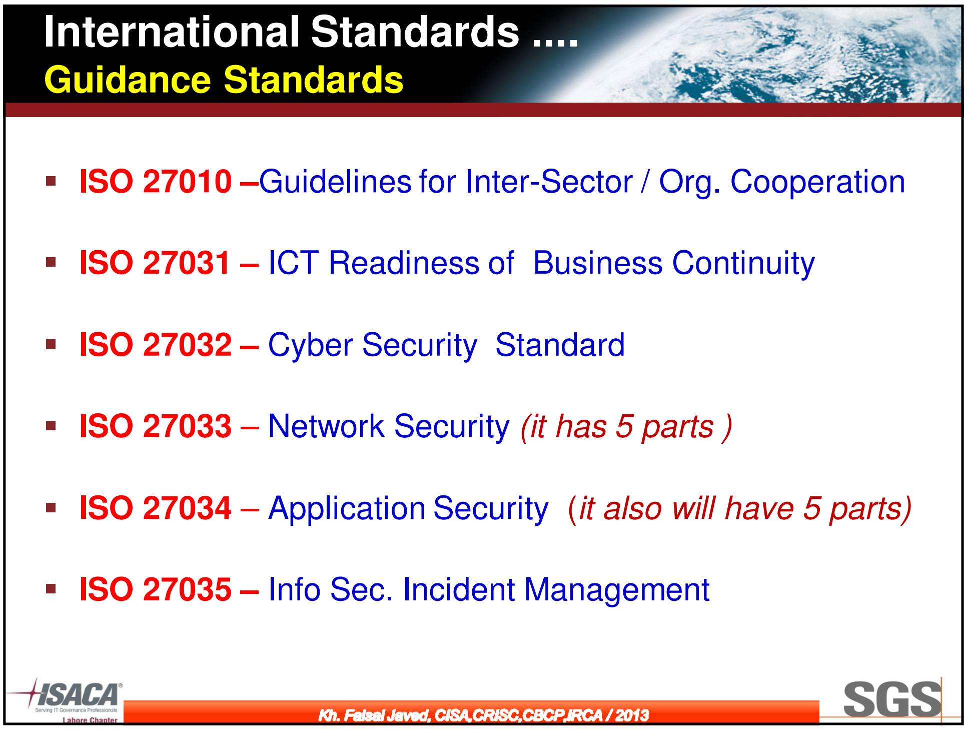


International Standards ....
Certifiable Standards

- **ISO 27001 – Information Security Management System**
- **ISO 20000 – IT Service Management**
- **ISO 22301 – Business Continuity management**

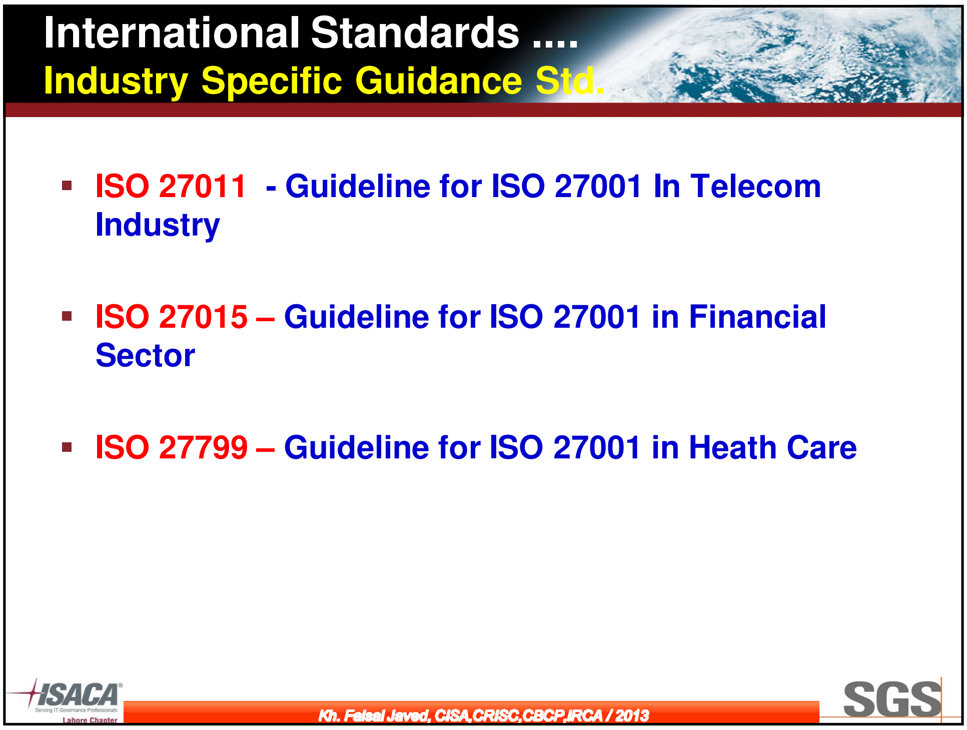
Assessment Framework (Maturity level)

- **COBIT 5 – Control Objectives for Info and related technologies** - ***Assessment scheme is being launched in June-2013***



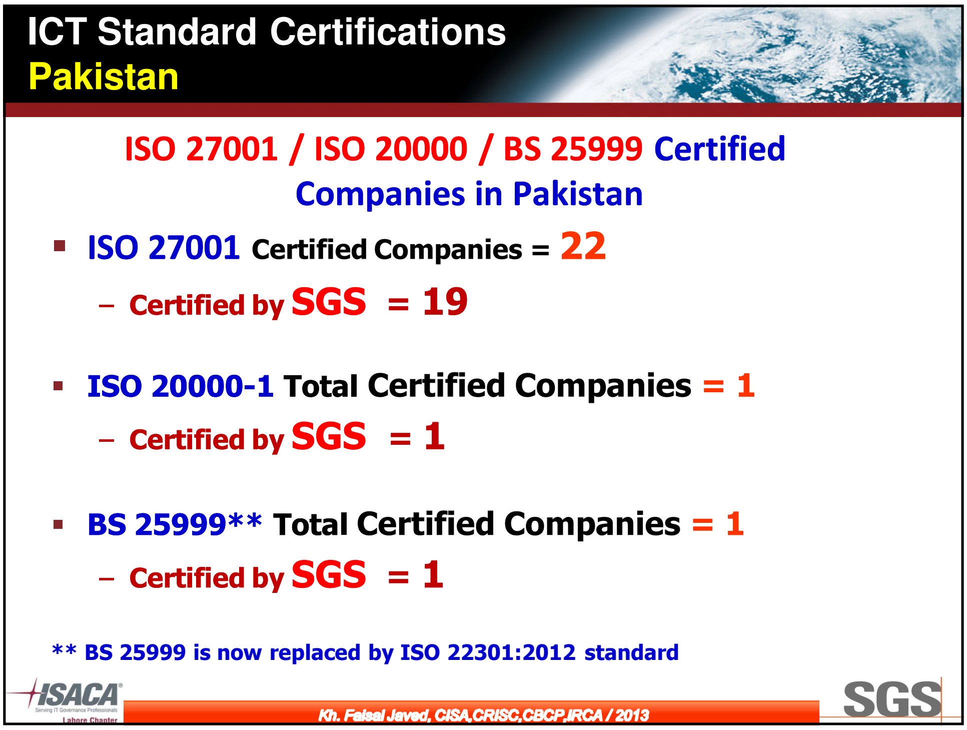
International Standards ....
Guidance Standards

- **ISO 27010 –**Guidelines for Inter-Sector / Org. Cooperation
- **ISO 27031 –** ICT Readiness of Business Continuity
- **ISO 27032 –** Cyber Security Standard
- **ISO 27033** – Network Security *(it has 5 parts)*
- **ISO 27034** – Application Security (*it also will have 5 parts)*
- **ISO 27035 –** Info Sec. Incident Management



International Standards ....
Industry Specific Guidance Std.

- ISO 27011 - Guideline for ISO 27001 In Telecom Industry
- ISO 27015 – Guideline for ISO 27001 in Financial Sector
- ISO 27799 – Guideline for ISO 27001 in Heath Care



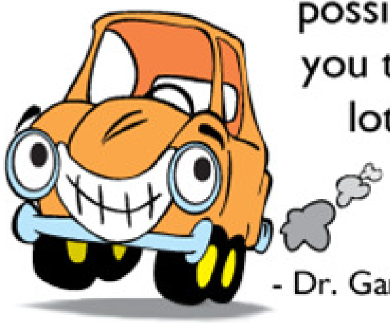
ICT Standard Certifications
Pakistan

ISO 27001 / ISO 20000 / BS 25999 Certified Companies in Pakistan

- ISO 27001 Certified Companies = 22
  - Certified by SGS = 19
- ISO 20000-1 Total Certified Companies = 1
  - Certified by SGS = 1
- BS 25999** Total Certified Companies = 1
  - Certified by SGS = 1

** BS 25999 is now replaced by ISO 22301:2012 standard

Security is like the brakes in your car. It slows you down, but it also make it possible for you to go a lot faster.



- Dr. Gary Hinson

WINNING IS AN ATTITUDE

THANK YOU, AND WISH YOU AHEAD OF THE GAME!

Mr. Khawaja Faisal Javed

Manager of Operations & ICT Products

Email: khawaja.faisal@sgs.com