Cyber Security in the GCC:
Are we doing The Best We Can?

Varun Kukreja
Sr. Security Consultant
CISA, CISSP, ITIL
GBM

A Brief History of Hacking

2010s

- Stuxnet worm attacks Irans Nuclear Facility
- Bank of America website hacked, 85000 credit cards and accounts stolen
- Playstation Network taken offline, with 77 Million PII leaked
- Bangladeshi hacker made a record in defacement history by hacking 700,000 websites
- Saudi hacker, published over 400,000 credit cards online
- Foxconn is hacked. Massive data leaked online
- Elite hacker sl1nk announced that he has hacked a total of 9 countries SCADA systems.
- Qatar National Bank Hacked, data leaked

2000s

- ILOVEYOU Worm introduced, affecting millions of computers
- DOS attacks introduced targeting domain servers
- Anna Kournikova virus is released
- Hacktivist group Anonymous was formed
- Turkish hacker iSKORPiTX successfully hacks 21,549 websites
- FBI Finds 1 Million Botnet Victims
- Anonymous attacks Scientology website servers around the world
- Google reveals of their IP theft

1990s

- 1260 or V2PX - First virus is created
- $10 Million were siphoned from Citibank and transferred to multiple accounts throughout the world
- AOHell is released resulting in readymade application for script kiddies
- Hackers alter the websites of US DOJ, CIA and Air Force
- Yahoo notifies users that they may have downloaded a logic bomb

1980s

- New York Times describers the term hacker
- Ian Murphy is convicted as first felon for breaking into AT&T Computers
- The term 'Trojan Horse' is coined as security exploit
- Computer Fraud and Abuse Act is released
- First National Bank of Chicago is subjected to a $70 Million Dollar computer theft
- CERT is formed

1940s / 1960s

- René Carmille, hacked the punched card machines to save countless jews from death camp
- Phreaking boxes emerge
- Password vulnerability in IBM 7094 is found

1939

- Bombe Machnine is developed. Enigma is broken by Brute force attack

1903

- Nevil Maskelyne disrupts John Ambrose Fleming's demonstration by sending insulting Morse code messages through the auditorium's projector.

GBM

Motivations

Espionage

Corporate / Government espionage is one of the biggest factors for hacking today, rival organization's or governments pay money to hackers to compromise critical information

EXAMPLE: STUXNET HACK

Money

Many hackers perform hacking related activities only to gain financial information that they can either use for themselves or sell it to a buyer at a price

EXAMPLE: BANKING HACKS

Challenge

Some hackers create malwares and perform hacking activities for gaining knowledge on the organization and to face new challenges that they want to overcome

EXAMPLE:

Social Issues

Many hacker groups have emerged that constitutes of various hacktivists that want to address social issues and target various companies and governments

EXAMPLE : ANONYMOUS GROUP

Fame

Hackers are known for openly claiming hacks conducted by them on social media websites and various other forums

EXAMPLE:

Destruction

Some hackers are fueled by revenge and just intend to destruct the opponent

EXAMPLE: ASHLEY MADISON HACK

Curiosity

Many hackers start as 'Script Kiddies' by using various tools freely available on the Internet
EXAMPLE: AOHELL Tool used by Newbies

GBM

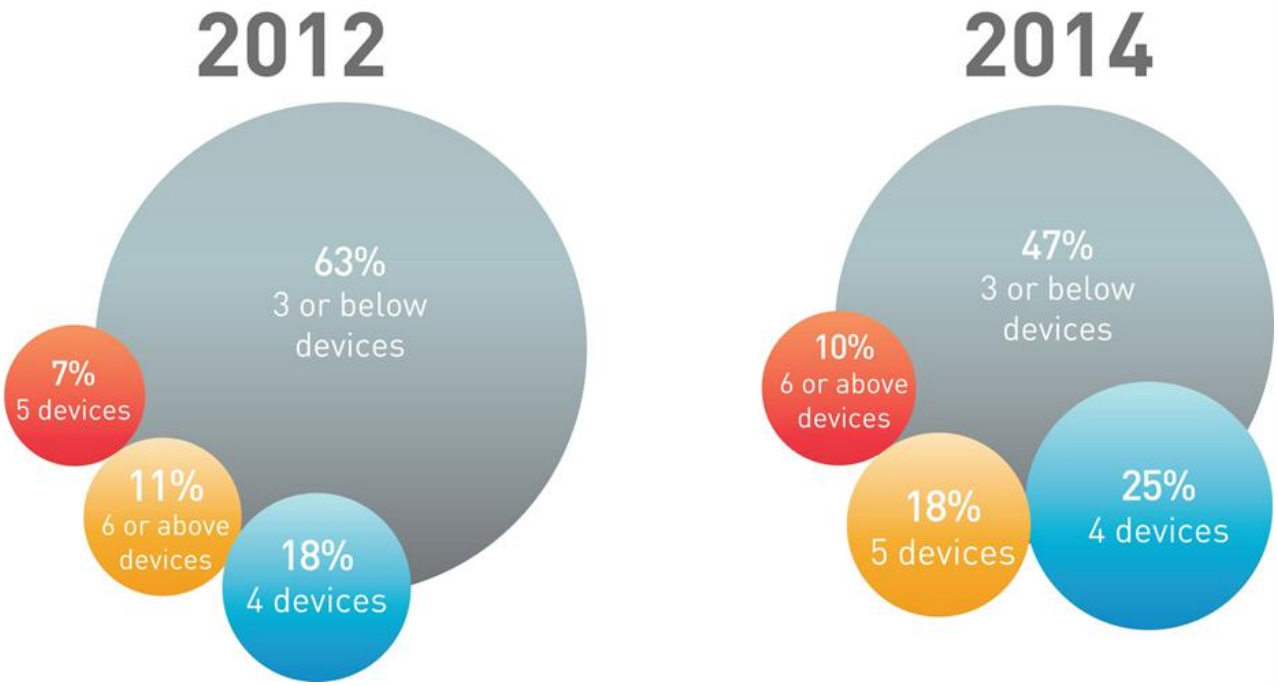
More Connected Devices / Services, More Hacks

- Around 40% of the world population has an internet connection today. In 1995, it was less than 1%
- The number of internet users has increased tenfold from 1999 to 2013.
- The **first billion** was reached in 2005. The **second billion** in 2010. The **third billion** in 2014.
- Gartner report suggests that it will increase to 20 Billion Devices by 2021

GBM

Your Logo

Personal Connected Devices in the GCC



70% of Professionals in the **GCC** carry more than 3 connected smart devices

Source: GBM

Digital Empowerment in Bahrain Education

GBM

Changes in the Threat Landscape in the Middle East

South African university website hacked by Anonymous

A South African university's website has been hacked by a group associating itself with Anonymous's #OpAfrica campaign.

Hacker holds UAE bank to ransom, demands $3m - Gulf News

Iran struck by cyberattack similar to April's oil hit

Iran's national CERT has warned of a new type of data-wiping malware that bears some of the hallmarks of a cyberattack that severely disrupted the country's oil industry earlier this year.

Hackers steal $1bn in series of online bank thefts says report

Cyber-warfare in the Middle East is no game

Triska Hamid

Nov 14, 2012

Report: Iranian hackers hit Qatar during two-year campaign ...

dohanews.co/report-iranian-**hackers**-hit-**qatar**-two-year-campaign/

Cyber attacks rob $45m from Gulf Banks

Faked RAKBANK and Bank Muscat credit cards used to take cash from ATMs in 27 countries in two co-ordinated attacks

Tags: Bank Muscat (www.bankmuscat.com), Credit card, Cyber crime, Mastercard, National Bank of Ras Al Khaimah, Oman, USA, United Arab Emirates

'Sophisticated' attack on Twitter

Twitter hammered by a cyber attack similar to those on major Western news outlets

Twitter says hackers compromise 250K accounts

Hacker attack shuts down Twitter

THE BLOG

5 Colleges With Data Breaches Larger Than Sony's in 2014

01/15/2015 09:40 am ET | Updated Mar 17, 2015

35 percent of all security breaches take place in higher education

By *Ian Barker* | Published 1 year ago | Follow @IanDBarker

GBM

New Challenges in Security

GBM

Key IT Security Challenges

Hackers & Attack Sophistication

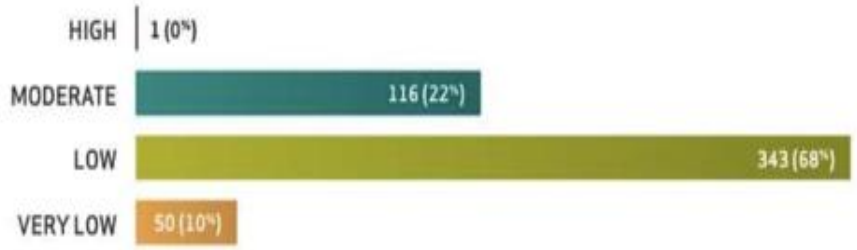
IT Security Compliance & Risk Mitigation

Security Intelligence, Monitoring & Management

People	Data	Application	Infrastructure	
BYOD	Leakage & Loss	Webification	Remote Access	Virus, Zero Day Malware
Roles & Responsibilities	Eavesdropping	Source code bugs	Guest Access	Secured Connectivity
Recruitment, Training & Awareness	Data in Rest / Motion	Spam	Internet Security	Physical Access

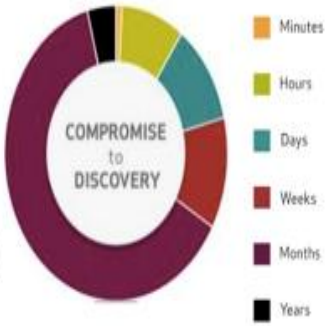
GBM

78% OF ATTACKS WERE LOW OR VERY LOW IN DIFFICULTY



EVEN ESPIONAGE LEVERAGED BASIC TECHNIQUES:
95% OF ESPIONAGE RELIED ON PHISHING

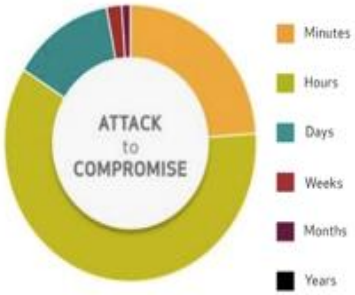
66% OF CASES WEREN'T DISCOVERED FOR MONTHS OR EVEN YEARS.



UP FROM 56% THE YEAR BEFORE

verizon

IN 84% OF CASES, INITIAL COMPROMISE TOOK HOURS OR LESS.



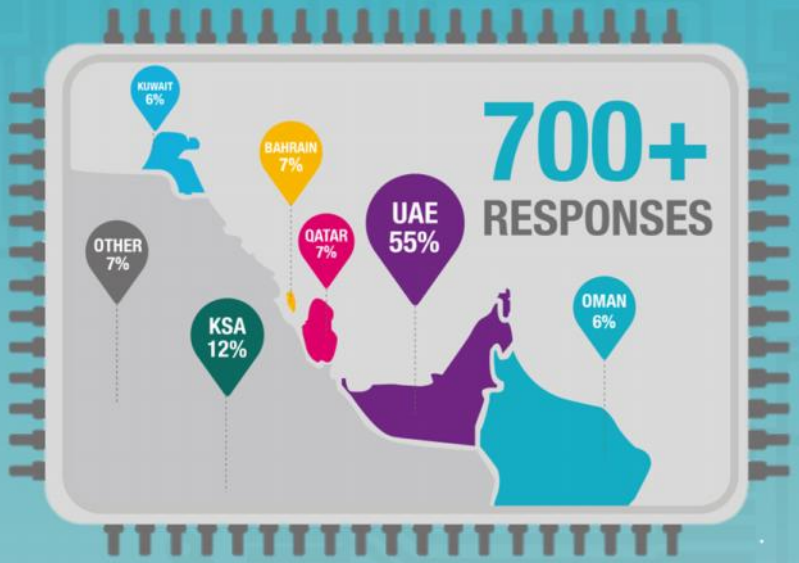
ALMOST A QUARTER TOOK JUST MINUTES OR LESS

69% OF BREACHES SPOTTED BY AN EXTERNAL PARTY

9% DISCOVERED BY CUSTOMERS

GBM

GBM 5TH ANNUAL SECURITY SURVEY 2016

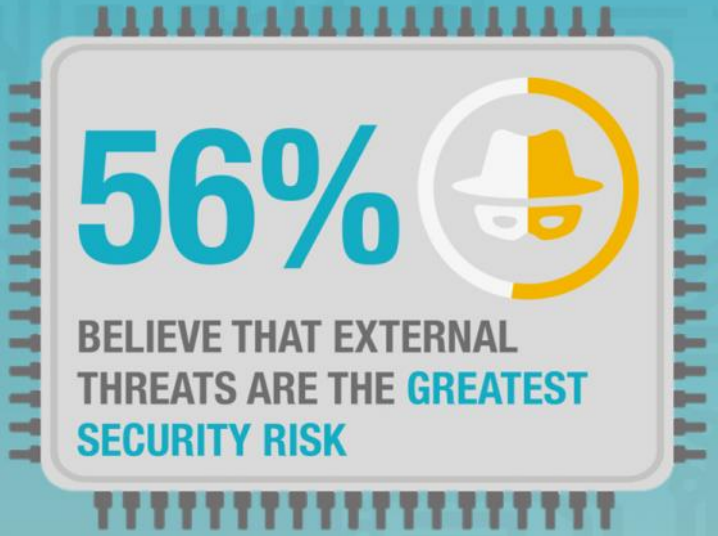

KUWAIT
6%
BAHRAIN
7%
QATAR
7%
UAE
55%
OMAN
6%
KSA
12%
OTHER
7%
700+
RESPONSES


ORGANIZATION SAMPLE
50%
SMALL & MEDIUM
ENTERPRISES
50%
LARGE
ENTERPRISES

GBM

Mixed Confidence

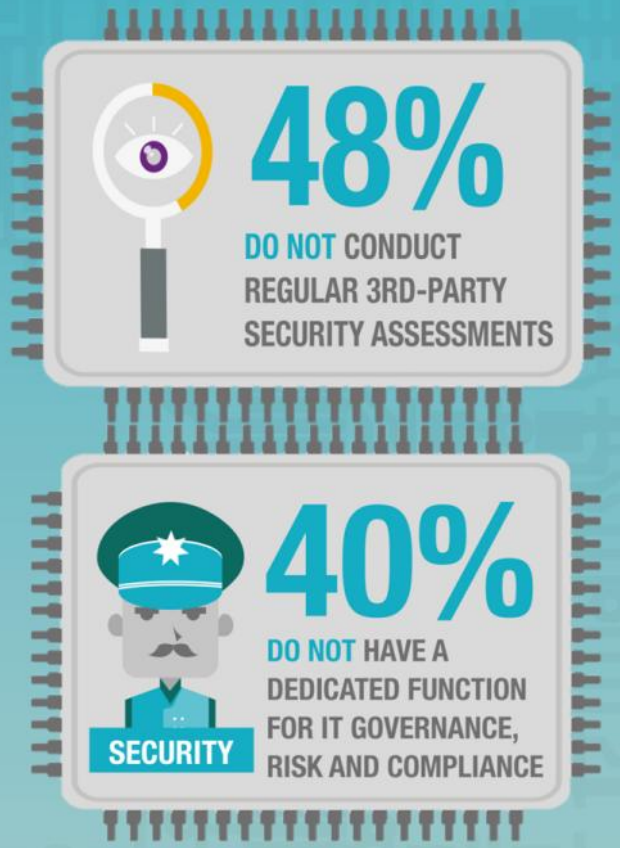
Executives Not Sure in Ability to Contain Compromise



GBM

Even the basics aren’t covered.

Less than half security practitioners leverage security tools



- Identify Admin and Provisioning
- Patching and configuration
- Technical Assessments
- Quarantine malicious apps

GBM

Public Breaches Can Improve Security.

More organizations conduct security training after an incident

GBM

Maturity: Budget Constrains Rank High

GBM

Problems that we have observed

- Cyber Security is still considered a part of IT
- The blind belief “This cannot happen to me”
- Lack of Security awareness campaigns in organizations
- Security is “Plug – And – Play” like an appliance
- Not investing enough in Business Continuity
- Reactive approach than Proactive

What can you do?

Proactive Vs Reactive

- Define Baselines
- Process and policies

Security Ownership

- CISO
- Risk and Compliance team
- Management focus

Identify Vulnerabilities

- By People, Processes and Technology
- Periodic external assessment

Remediation Program

- Risk Management
- Impact Analysis
- 'Fix' the risks

Plan Improvements

- Ensure regular and repeatable process

Continued Focus

- Monitor and Measure
- Identify new trends and adjust approach accordingly

Security Awareness

- Spread awareness on how to be more secure
- Via various medium like poster, newsletters etc


GBM
Varun Kukreja
Sr. Security
Consultant