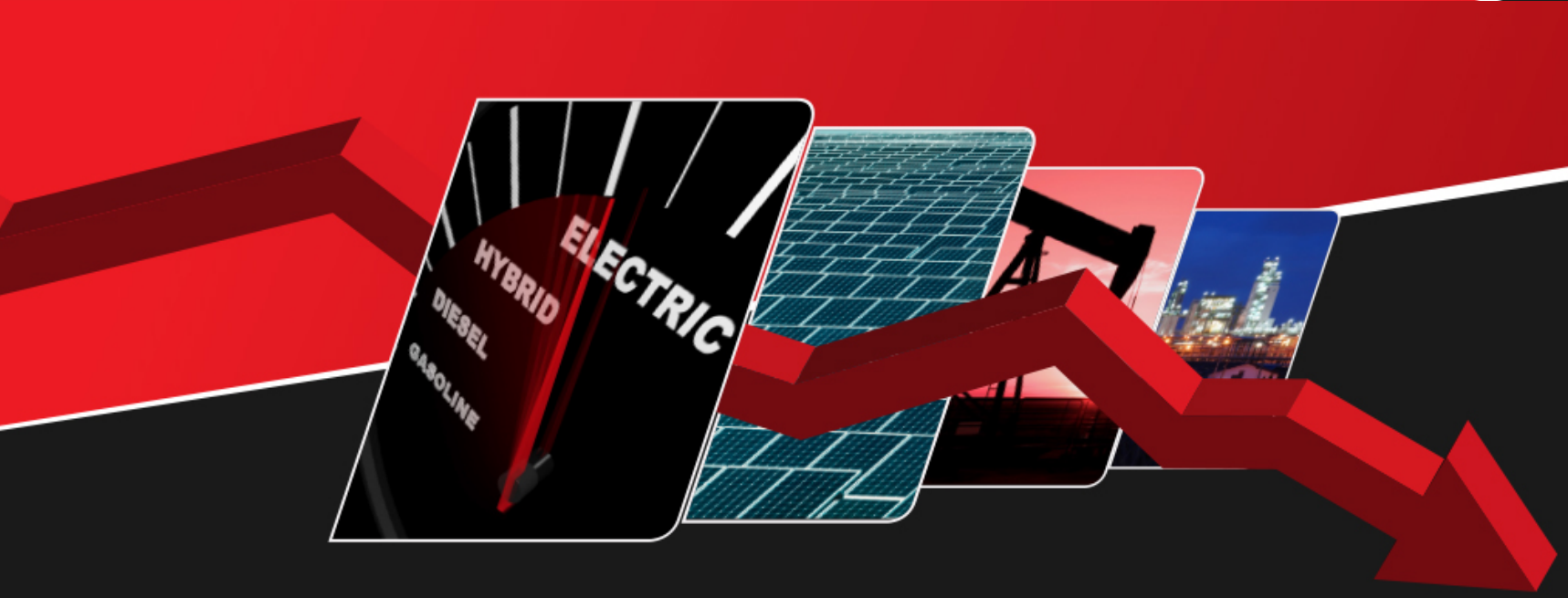

KUWAIT ENTERPRISE RISK MANAGEMENT CONFERENCE
4th Edition | 2017

Sourabh Sharma

Director, Cyber Security, EY Kuwait



Cyber Risks- The new normal

Agenda

Is Cyber Security a real issue???

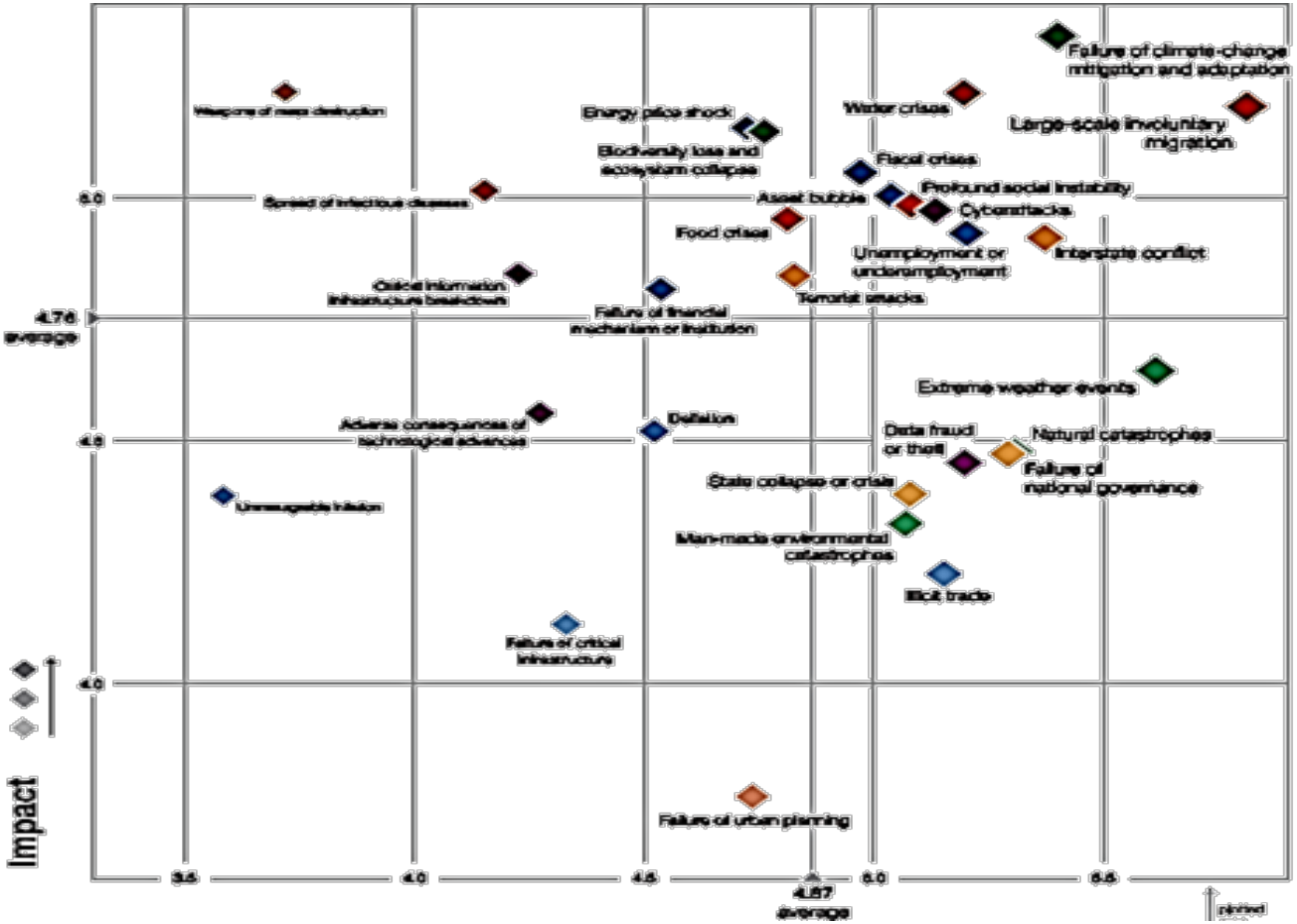
2017 cyber security trends

Why cyber security risks prevail??

Cyber Risk Mitigation

Cyber Risks, dominating for the past three years

- Economic risks
- Geopolitical risks
- Environmental risks
- Societal risks
- Technological risks



Source- Global Risk Landscape,2016

Some major cyber attacks - 2017

Database of 1.4 Billion Records leaked from World's Biggest Spam Networks

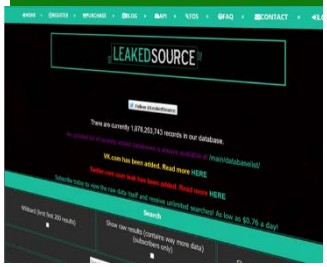
- A database of 1.4 billion email addresses combined with real names, IP addresses, and often physical address has been exposed in what appears to be one the largest data breach of this year
- The database contains sensitive information about the company's operations, including nearly 1.4 Billion user records, which was left completely exposed to anyone – even without any username or password.

Yahoo Hacked Once Again! Quietly Warns Affected Users About New Attack

- Yahoo sent out another round of notifications to its users on Wednesday, warning that their accounts may have been compromised as recently as last year after an ongoing investigation turned up evidence that hackers used forged cookies to log accounts without passwords

Popular PlayStation and Xbox Gaming Forums Hacked; 2.5 Million Users' Data Leaked

- Mostly gamers who look for free versions of popular games are members of these two gaming forums, which provide download links for gaming ISO files – digital copies of online video games lifted from physical game disks – to the owners of Microsoft's Xbox 360 and Sony's Playstation Portable.



Breach Database Site 'LeakedSource' Goes Offline After Alleged Police Raid

- The biggest mistake companies make with data security is leaving all their secrets unprotected at one place, which if attacked, they are all gone in one shot.
- An unnamed law enforcement agency has reportedly accessed billions of compromised usernames, email IDs, and their passwords, collected by LeakedSource, a popular breach notification service.

Some major cyber attacks contd..

1-Billion Yahoo Users' Database Reportedly Sold For $300,000 On Dark Web

- The new development in Yahoo!'s 2013 data breach is that the hacker sold its over Billion-user database on the Dark Web last August for $300,000, according to Andrew Komarov, Chief Intelligence Officer (CIO) at security firm InfoArmor.

Hackers shut down Ukraine power grid

- The same group of hackers that caused the power outage across several regions in Ukraine last Christmas holidays might have once again shut down power supply in northern Ukraine during the weekend.
- United States Cyber firm iSight Partners identified the perpetrator as a Russian group of hackers known as "Sandworm"

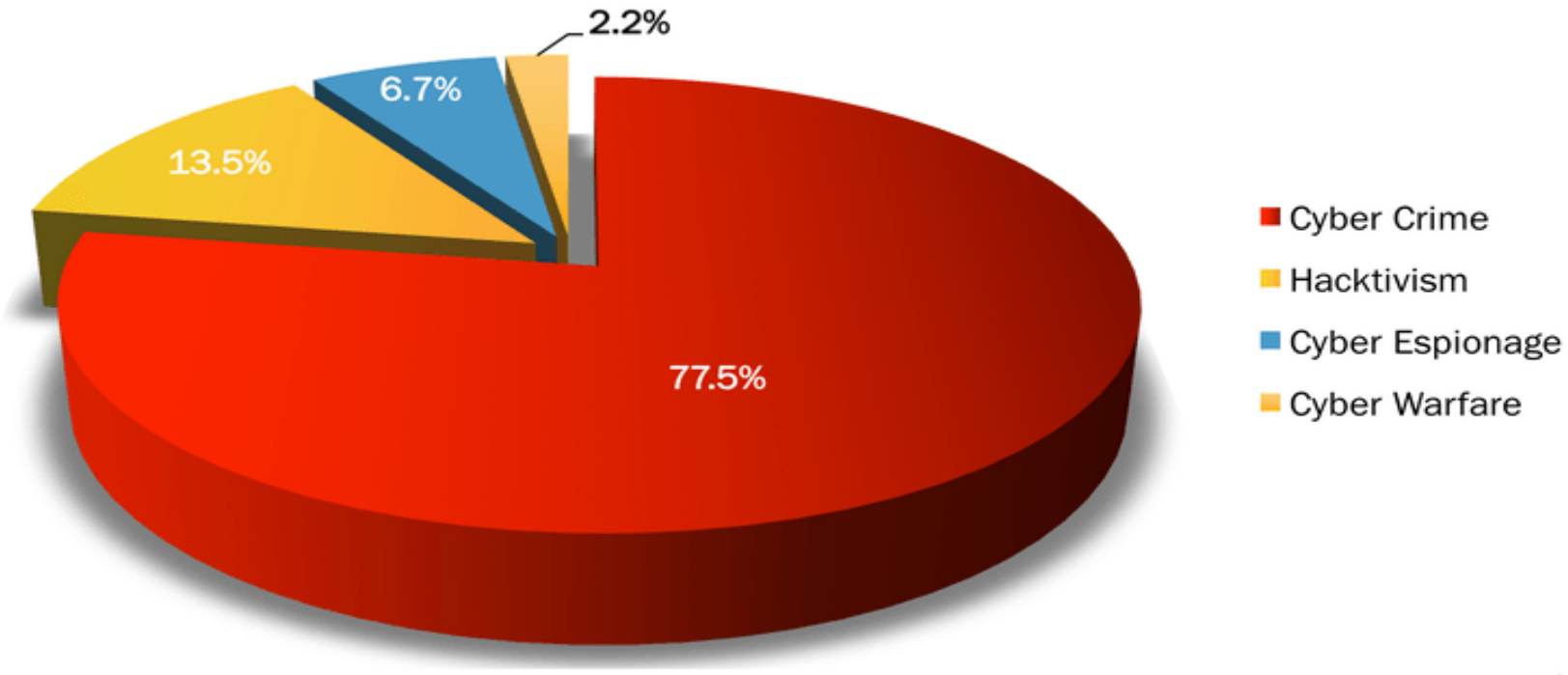
Shamoon Malware : Permanently wiping data from Energy Industry Computers (2nd Drill)

- A new disk wiping malware has been uncovered targeting a petroleum company in Europe, which is quite similar to the mysterious disk wiper malware Shamoon that wiped data from 35,000 computers at Saudi Arabia's national oil company in 2012.
- Shamoon 2.0 is the more advanced version of Shamoon malware that reportedly hit 15 government agencies and organizations across the world, wipes data and takes control of the computer's boot record, preventing the computers from being turned back on.

Massive ATM Hack Hits 3.2 Million Indian Debit Cards — Change Your PIN Now!

- Hackers allegedly used malware to compromise the Hitachi Payment Services platform — which is used to power country's ATM, point-of-sale (PoS) machines and other financial transactions — and stole details of 3.2 Million debit cards, reports The Economic Times.

Motivation's for Cyber Attacks Statistics- 2017



2017 cyber security trends

Increased regulations

More automation

IoT as the next Trojan

Increase in nationwide Cyber terror attacks

Data theft turning into data manipulation

Breaches will get more complicated and harder to beat

Attacks on public figures

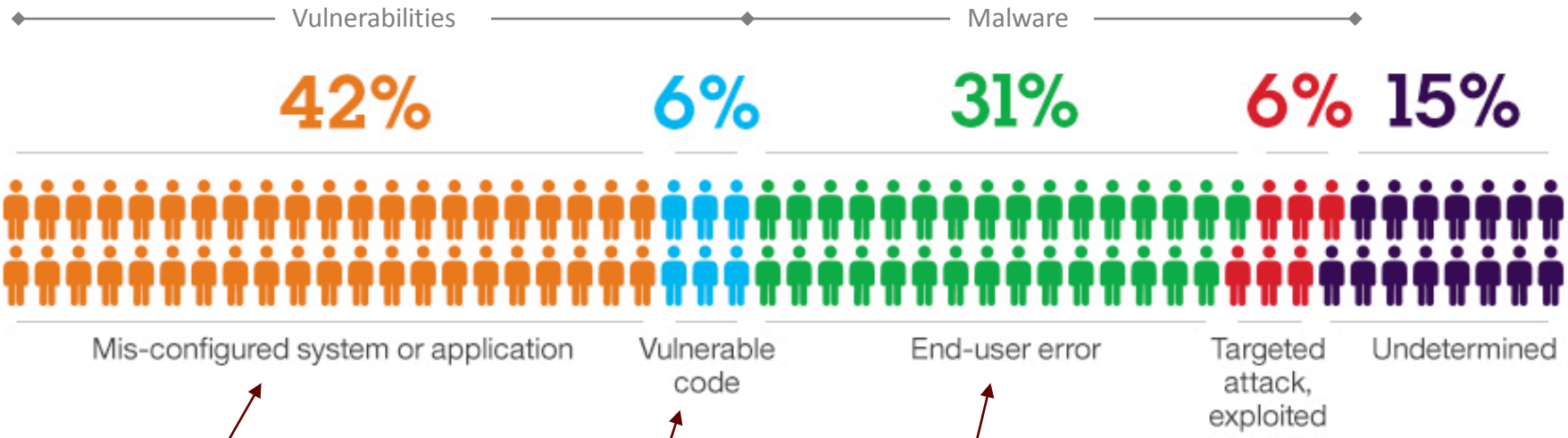
New job titles appearing – CCO (chief cybercrime officer)

Why cyber risk prevails??

	2003	2010	2015	2020
World Population	6.3 billion	6.8 billion	7.2 billion	7.6 billion
Connected Devices	500 million	12.5 billion	25 billion	50 billion
Connected Devices per person	0.08	1.84	3.47	6.58

More connected devices than people

Why do Breaches Happen?



- Configuration Errors
- "Weak" defaults
- Easy passwords

- "Bugs"
- Input validation

- Installing suspect applications
- Clicking malicious links

- Phishing Emails
- Watering Hole attacks

Cyber Risk Mitigation

Enable business performance

- Make security everyone's responsibility
- Don't restrict newer technologies; use the forces of change to enable them.
- Broaden the program to adopt enterprise-wide information risk management concepts
- Set security program goals and metrics that influence business performance

Sustain an enterprise program

- Get governance right – make security a board-level priority
- Allow good security to drive compliance, not vice versa
- Measure leading indicators to catch problems while they are still small
- Accept manageable risks that improve performance.

Protect what matters most

- Develop a security strategy focused on business drivers and protecting high-value data
- Assume breaches will occur – improve processes that plan, protect, detect and respond
- Balance fundamentals with emerging threat management
- Establish and rationalize access control models for applications and information

Identify the real risk

- Define the organization's overall risk appetite and how information risk fits
- Identify the most important information and applications, where they reside and who has or needs access
- Assess the threat landscape and develop predictive models highlighting your real exposures.

Optimize for business performance

- Align all aspects of security (information, privacy, physical and business continuity) with the business.
- Spend wisely in controls and technology – invest more in people and processes.
- Consider selectively outsourcing operational security program areas

Key Mitigation steps

Perform Current State Assessment across defense, detection and response domains

Baseline whether you have been compromised or not

Identify what are the crown jewels

Develop/Refresh Cyber strategy

Review security spend and align with current state assessment results

Thanks for Your Attention