Managing Technology Risks in a Globally Competitive World

Prof. Frank Yam

Chairman & CEO – Focus Strategic Group Inc

CISA, CIA, CFSA, FHKCS, FHKIoD, FFA, FIPA, FHKITJC, CFE, CCP, CSP, CDP

Warning!!!

- All information discussed in this seminar is the personal opinion of the Seminar Leader and is meant to stimulate new ideas from the participants.

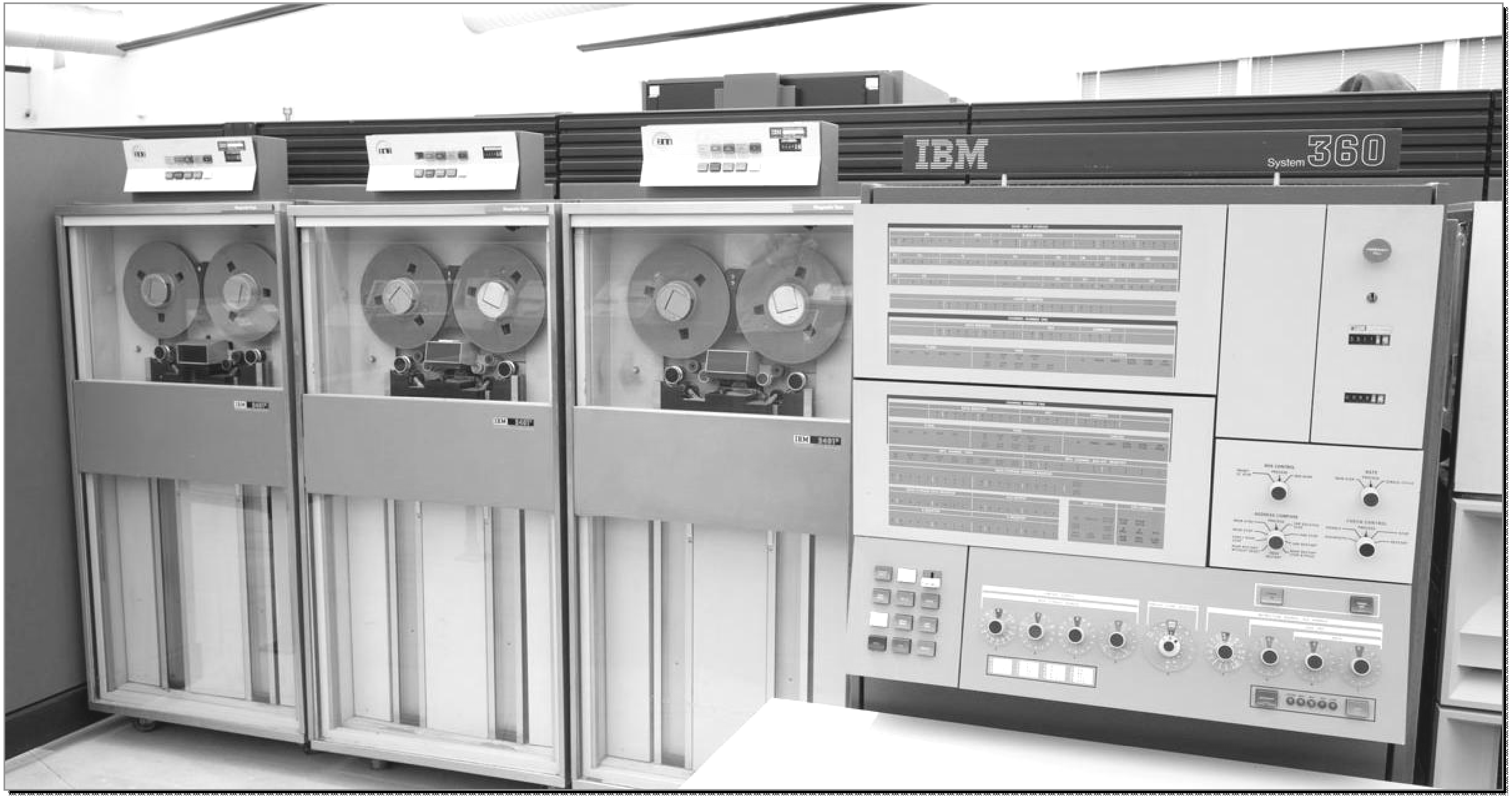
- Under no circumstances should any of the opinion be relied upon for decision making or used for any other purposes.

- The Seminar Leader does not assume any liabilities for the opinion expressed in this seminar.

- Audio, video, or any other form of electronic recording is strictly prohibited.

Evolution – "First Computer"

Evolution – Mainframe Computer

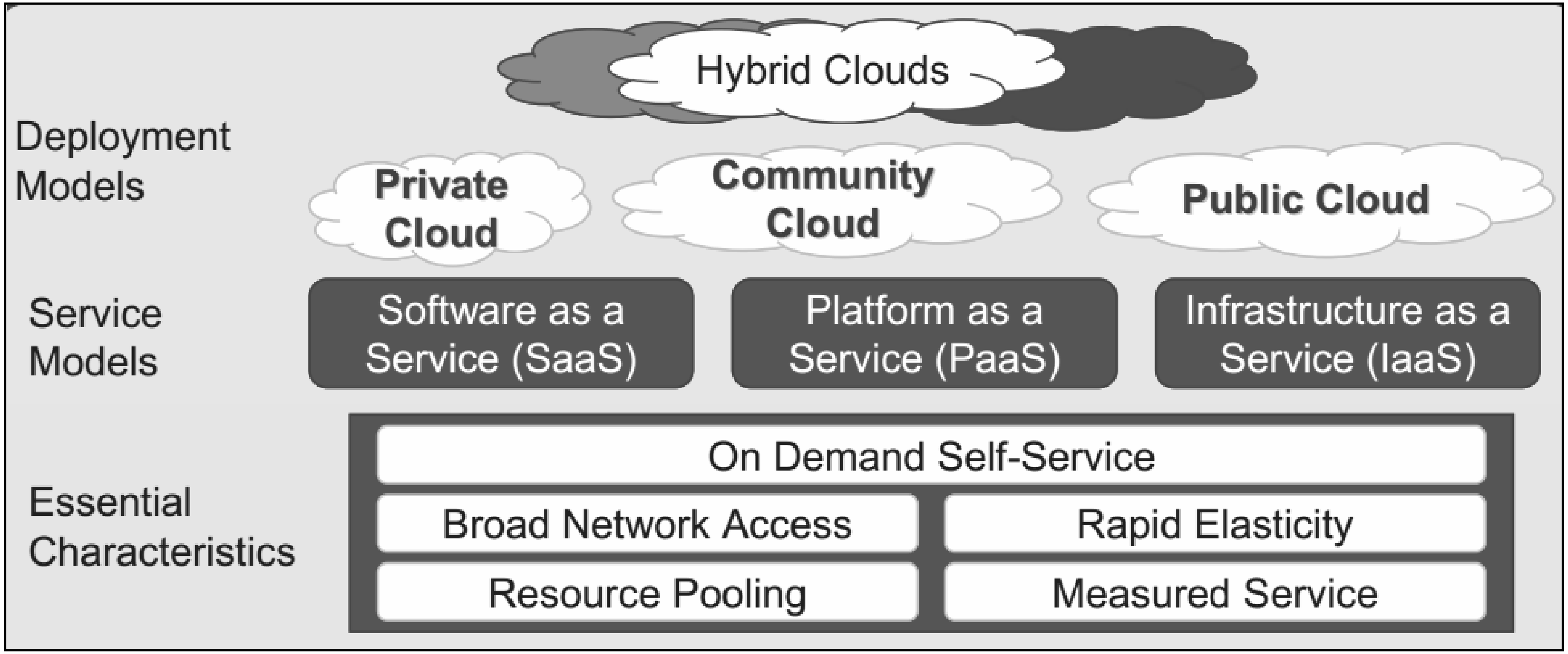


Evolution – Mini Computer, PC and Internet

Evolution - Cloud Computing

Credit : Ching Yiu

Understanding Cloud Computing



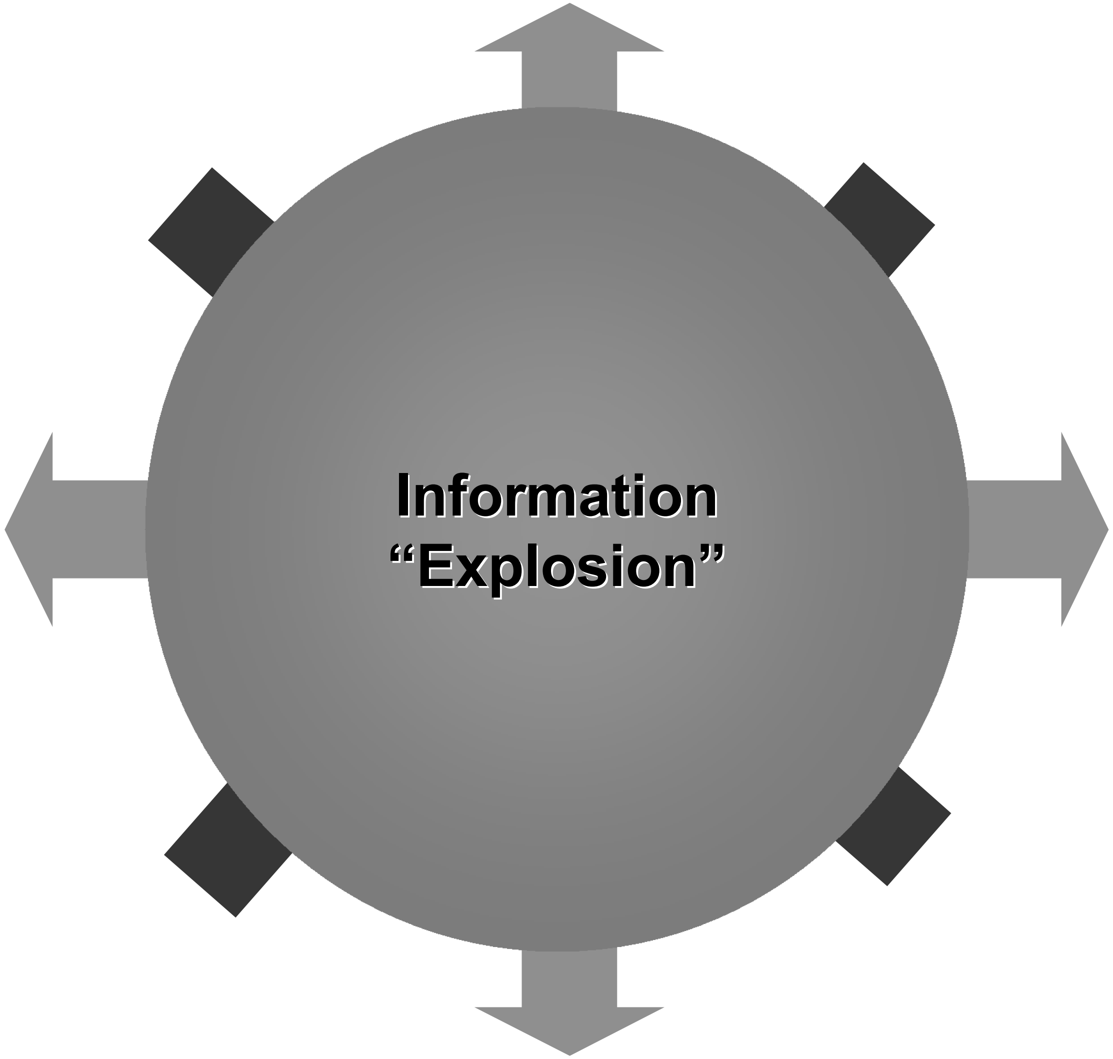
NIST Visual Definition of Cloud Computing

Understanding Cloud Computing

You will also hear other associated service models in the future, for example:

- Security as a Service (SecaaS)
- Storage as a Service (StaaS)
- Disaster Recovery as a Service (DRaaS)
- Identity as a Service (IDaaS)

Do we understand the Information Challenge



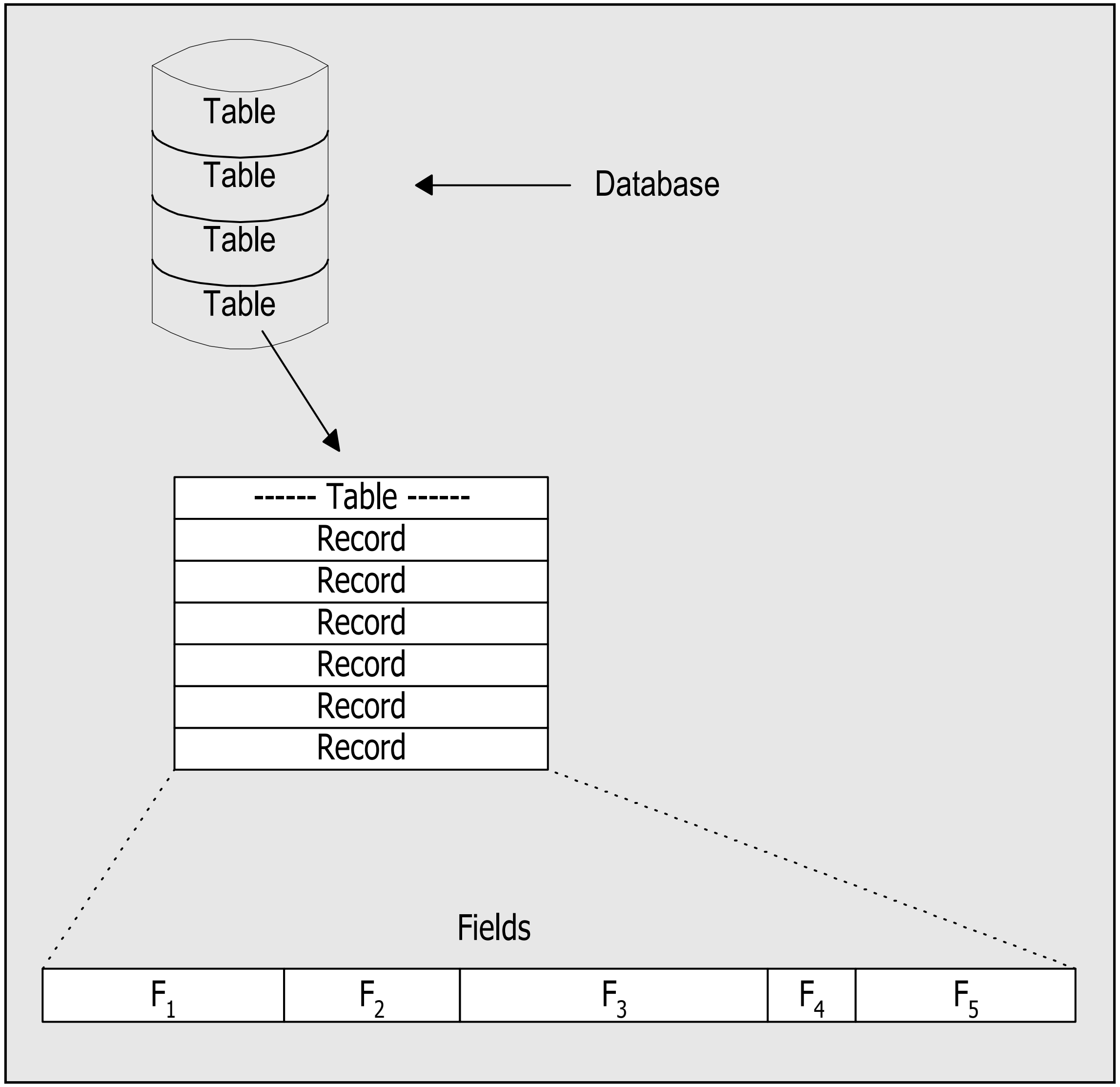
© Frank Yam 2015

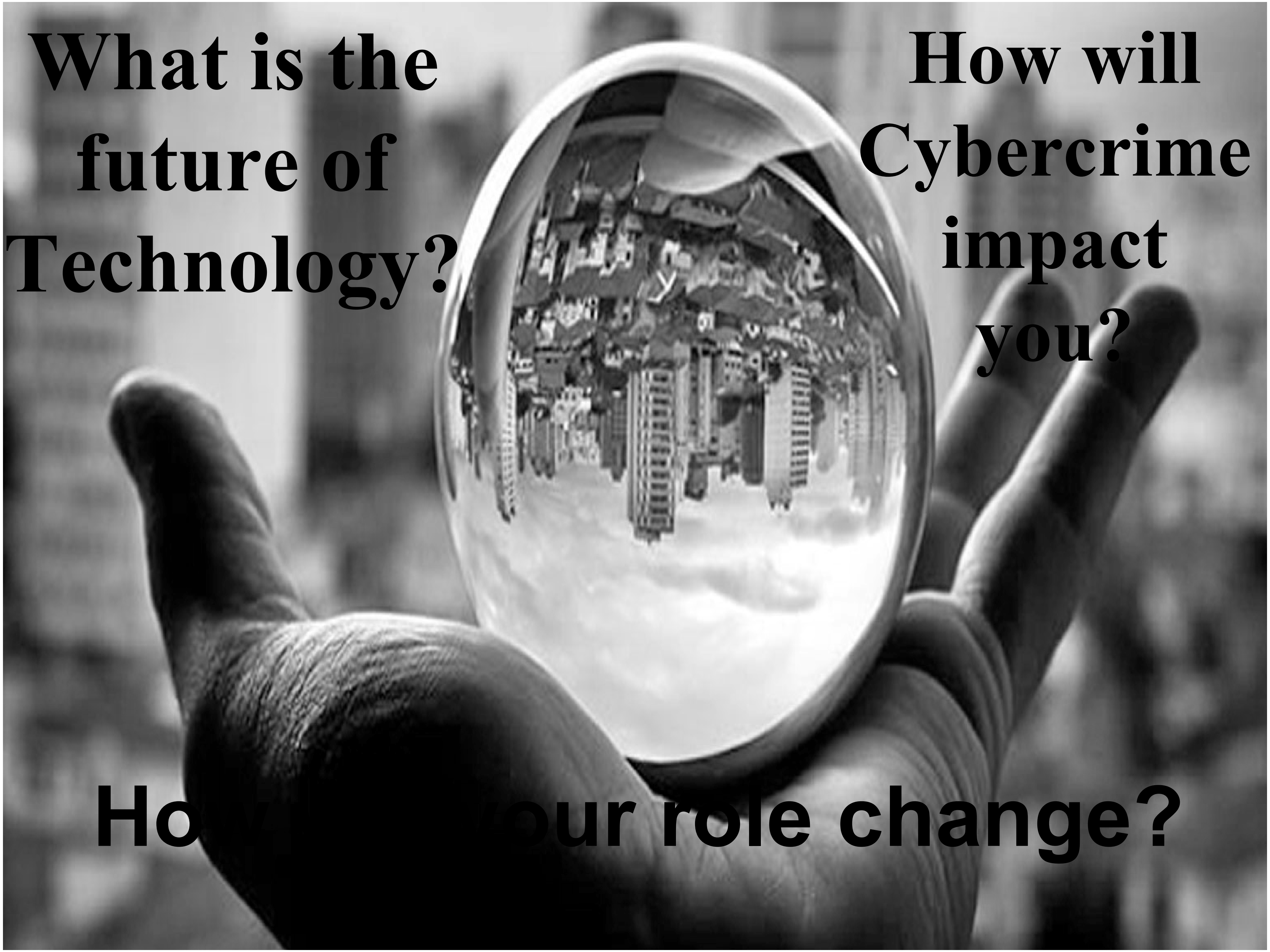
The Information Challenge
Can we trust our data?

- What data is there?
- Where is the data stored?
- Who owns the data?
- How is the data being used?
- Who has access to data?
- What is the value of the data?

Simplified Schematic of a Database

- **Database**
- **Table**
- **Record**
- **Field**



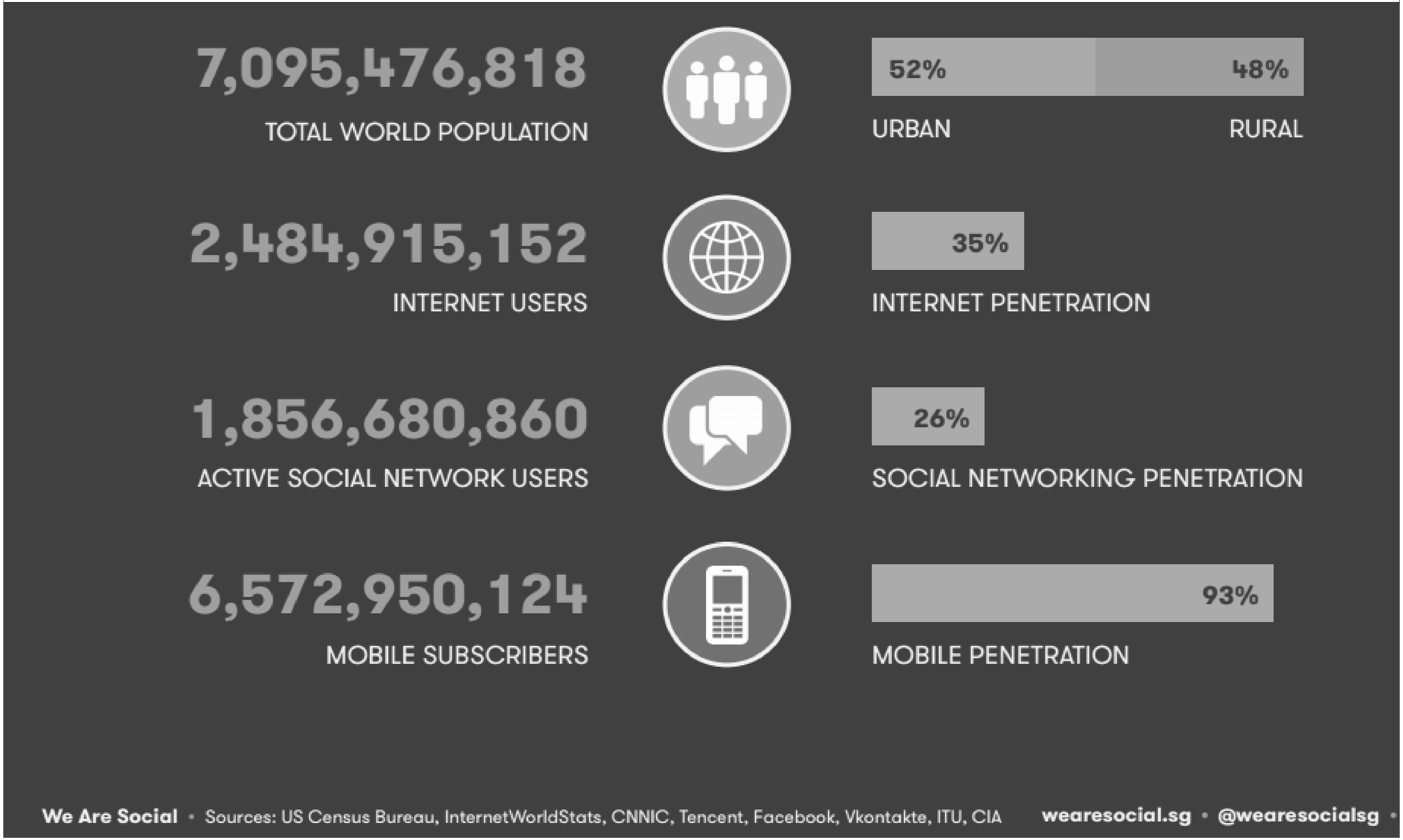


What is the future of Technology?

How will Cybercrime impact you?

How will your role change?

THE NEW WORLD ORDER



7,095,476,818

TOTAL WORLD POPULATION

52% 48%

URBAN RURAL

2,484,915,152

INTERNET USERS

35%

INTERNET PENETRATION

1,856,680,860

ACTIVE SOCIAL NETWORK USERS

26%

SOCIAL NETWORKING PENETRATION

6,572,950,124

MOBILE SUBSCRIBERS

93%

MOBILE PENETRATION

We Are Social • Sources: US Census Bureau, InternetWorldStats, CNNIC, Tencent, Facebook, Vkontakte, ITU, CIA wearesocial.sg • @wearesocialsg •

The Importance of Knowing What is Coming (or Already Here)

What came in
What went out

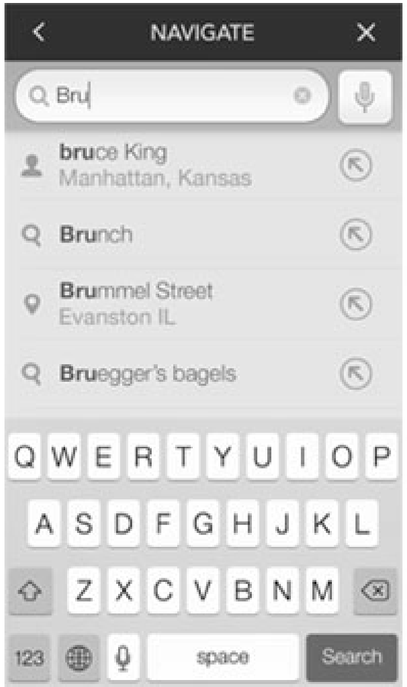
NEW TAXI EXPERIENCE

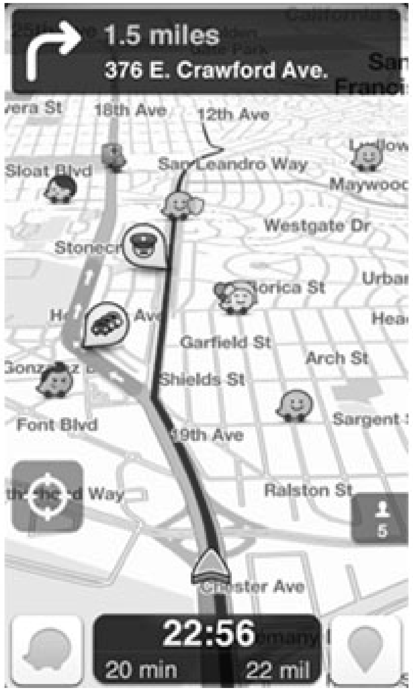
NEW DRIVING EXPERIENCE

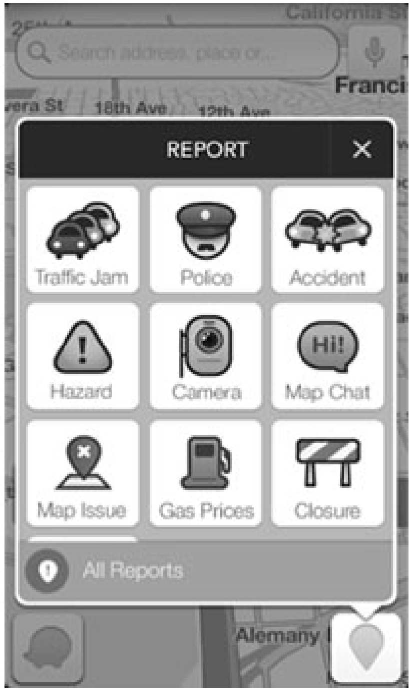
- Community-based navigation
- Report conditions you see
- Dynamically updated turn-by-turn directions

waze

OUTSMARTING TRAFFIC, TOGETHER.

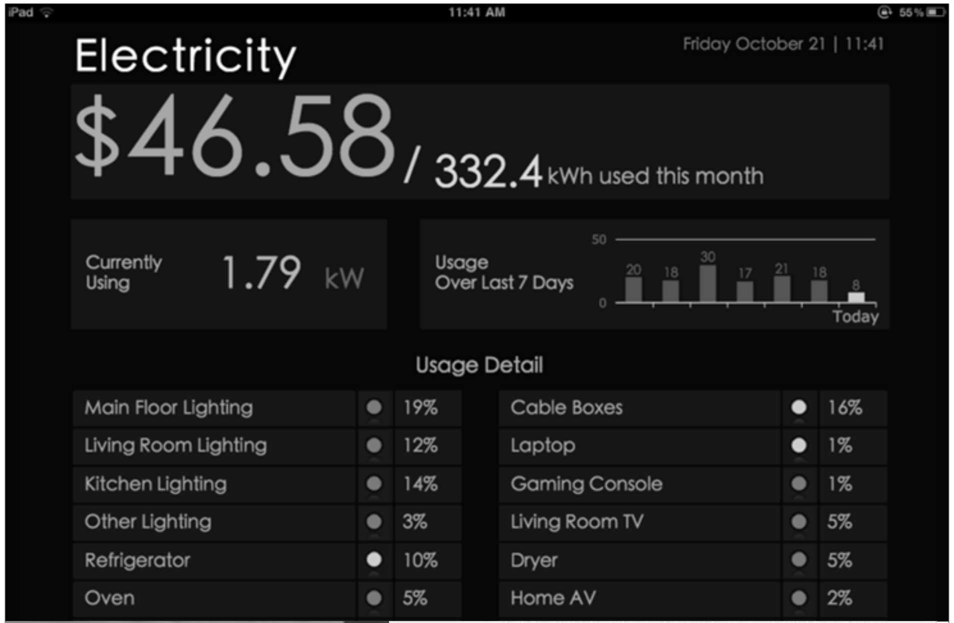






NEW UTILITY BILL

- **Minimally invasive, single outlet plug**
- **Customer-controlled profiling and tracking**
- **Fact-driven behaviors**
- **Changing behavior**



Electricity

Friday October 21 | 11:41

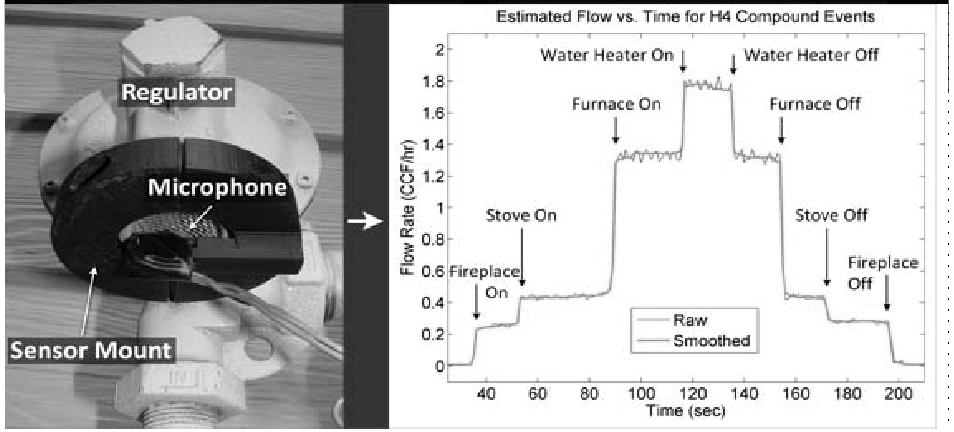
$46.58 / 332.4 kWh used this month

Currently Using 1.79 kW

Usage Over Last 7 Days

Usage Detail

Main Floor Lighting	●	19%	Cable Boxes	●	16%
Living Room Lighting	●	12%	Laptop	●	1%
Kitchen Lighting	●	14%	Gaming Console	●	1%
Other Lighting	●	3%	Living Room TV	●	5%
Refrigerator	●	10%	Dryer	●	5%
Oven	●	5%	Home AV	●	2%



© Frank Yam 2015

NEW NURSES

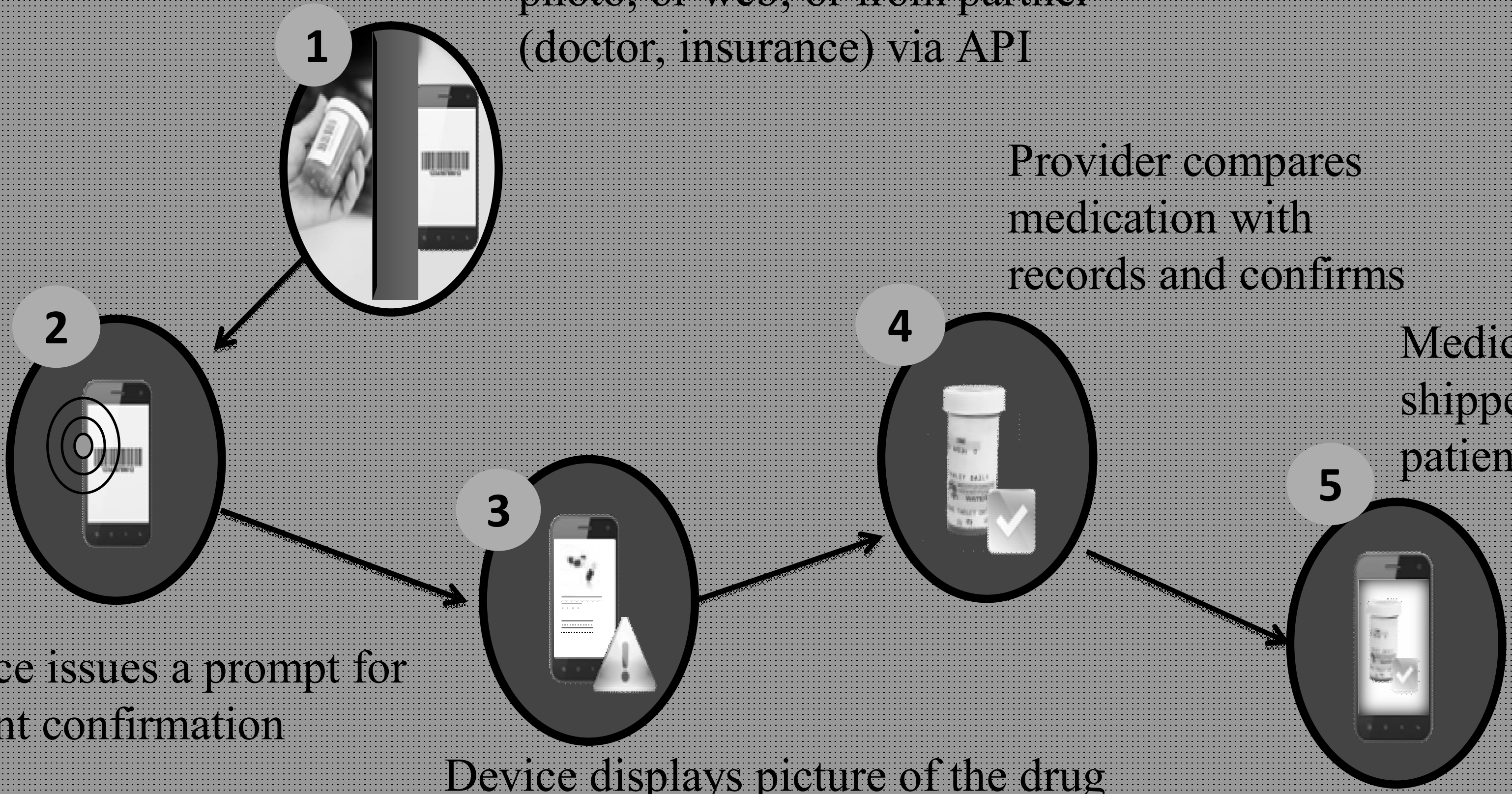
12:00
Fri, Jan 31
139
9'22"/mi
871
6:30
Fri, Jan 31
Rise and Shine
12:00
Fri, Jan 31
Healthbook
72 BPM
At Rest
7534 Steps
Great Job!
7.4
Hours of Sleep
12:00
Fri, Jan 31

%
97
73

NEW DOCTORS

Mobile Cough Tracking

NEW HEALTHCARE



Old prescription captured from patient via bar code, RFID, NFC, photo, or web; or from partner (doctor, insurance) via API

Device issues a prompt for patient confirmation

Device displays picture of the drug and other medical information

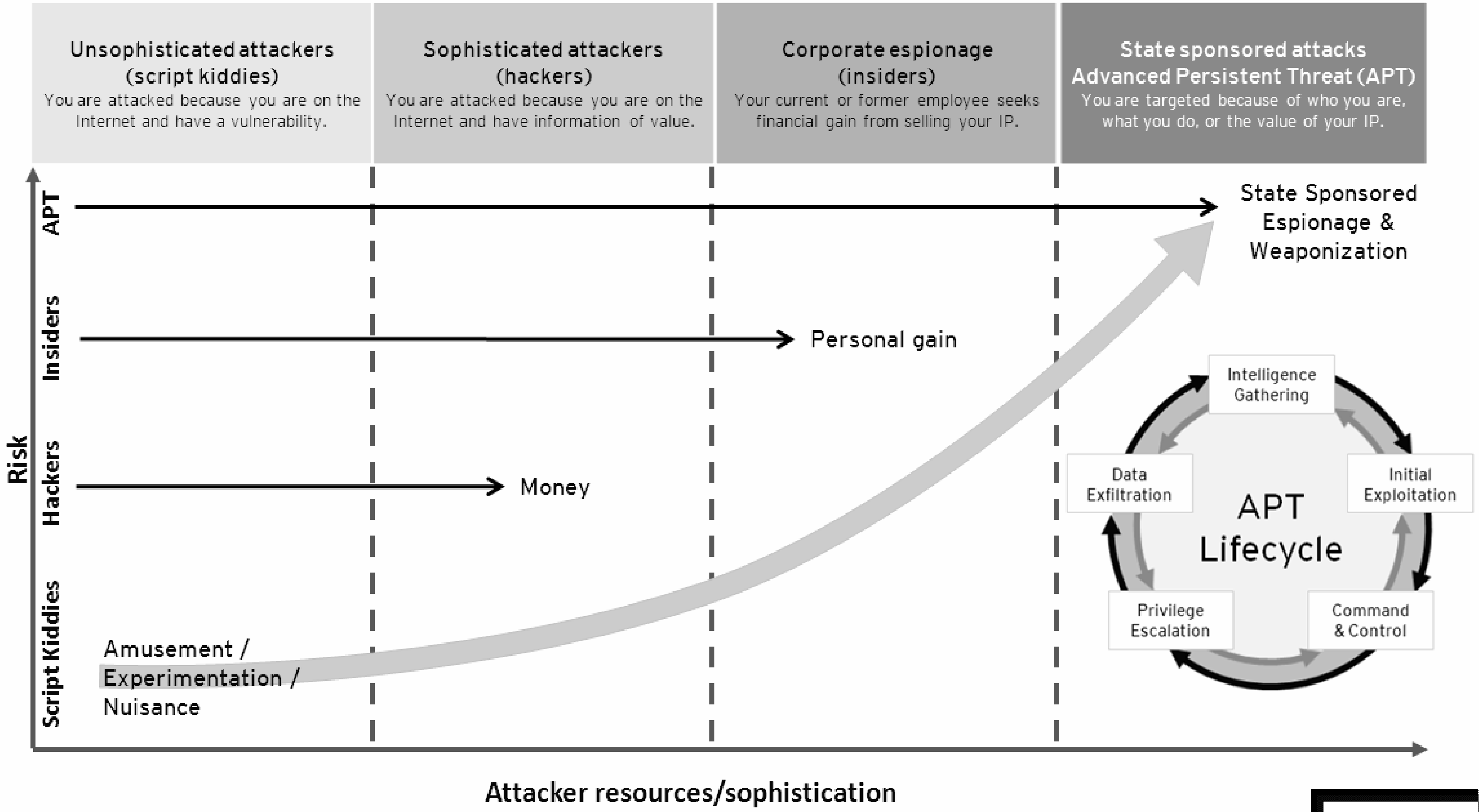
Provider compares medication with records and confirms

Medication is shipped to patient

NEW SPY

CURRENT STATE OF SECURITY

EVOLUTION OF ATTACKS



Unsophisticated attackers (script kiddies)
You are attacked because you are on the Internet and have a vulnerability.

Sophisticated attackers (hackers)
You are attacked because you are on the Internet and have information of value.

Corporate espionage (insiders)
Your current or former employee seeks financial gain from selling your IP.

State sponsored attacks Advanced Persistent Threat (APT)
You are targeted because of who you are, what you do, or the value of your IP.

Risk

APT: State Sponsored Espionage & Weaponization

Insiders: Personal gain

Hackers: Money

Script Kiddies: Amusement / Experimentation / Nuisance

APT Lifecycle: Intelligence Gathering, Initial Exploitation, Command & Control, Privilege Escalation, Data Exfiltration

Attacker resources/sophistication

1980s/1990s

2015

- BrainBoot/Morris Worm
- polymorphic viruses
- Michelangelo

- Concept Macro Virus
- Melissa
- "I Love You"

- Anna Kournikoiva
- Sircam
- Code Red & Nimda

- SQL Slammer
- Blaster
- Sobig

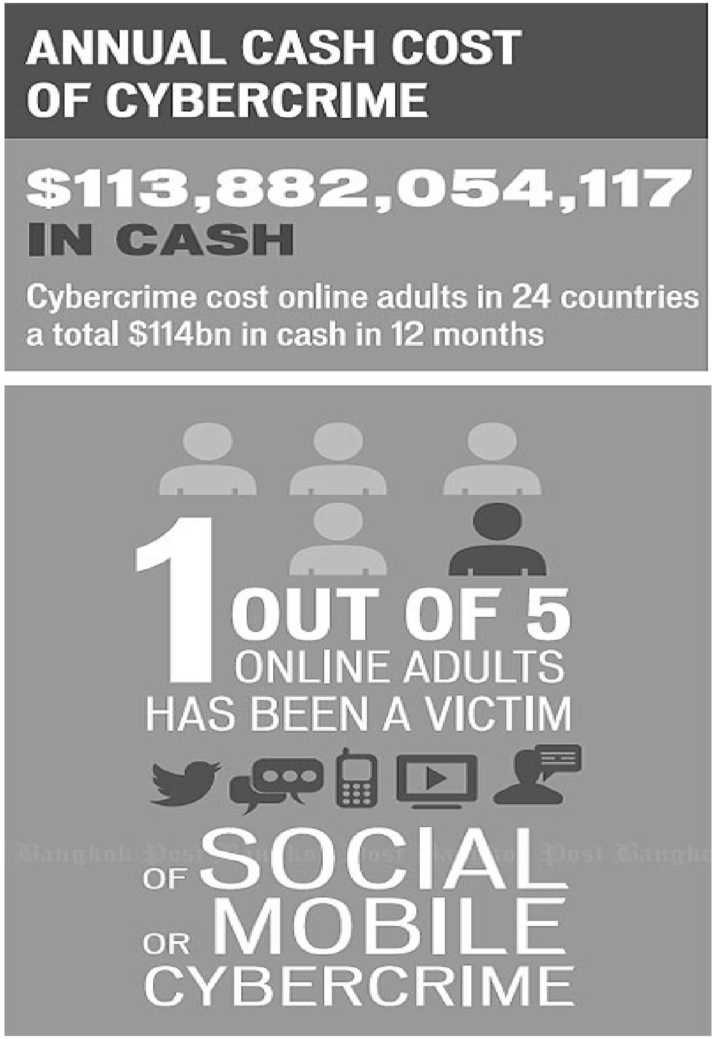
- MyDoom
- NetSky
- Sasser

- Storm botnet
- Koobface
- Conflicker

- Aurora
- Mariposa
- Stuxnet

- WikiLeaks
- Anonymous
- LulzSec

- SpyEye/Zeus
- Duqu
- Flame

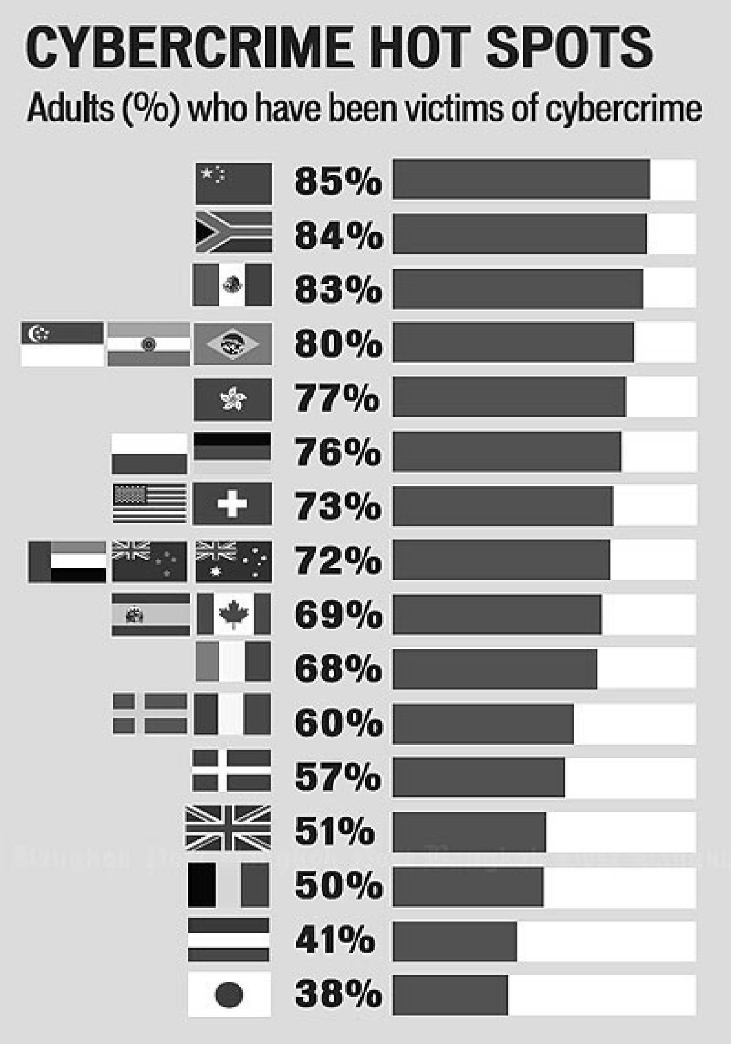


ANNUAL CASH COST OF CYBERCRIME

$113,882,054,117 IN CASH

Cybercrime cost online adults in 24 countries a total $114bn in cash in 12 months

1 OUT OF 5 ONLINE ADULTS HAS BEEN A VICTIM OF SOCIAL OR MOBILE CYBERCRIME

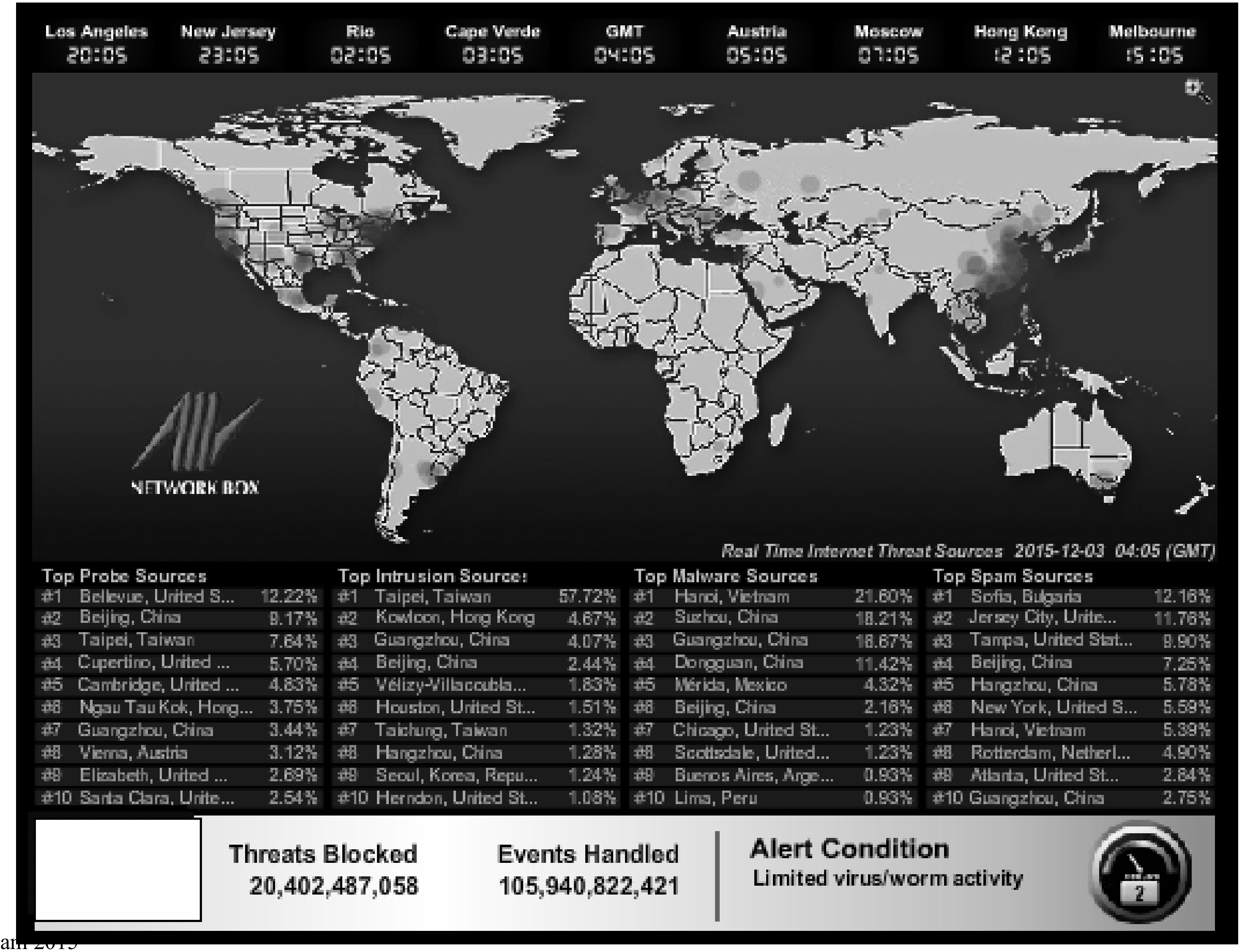


CYBERCRIME HOT SPOTS

Adults (%) who have been victims of cybercrime

http://www.bangkokpost.com/print/389343/
International Telecommunications Union, the United Nations specialized agency for information and communications technology

Real Time Cyber Threats



Los Angeles	New Jersey	Rio	Cape Verde	GMT	Austria	Moscow	Hong Kong	Melbourne
20:05	23:05	02:05	03:05	04:05	05:05	07:05	12:05	15:05

Real Time Internet Threat Sources 2015-12-03 04:05 (GMT)

Top Probe Sources		
#1	Bellevue, United S...	12.22%
#2	Beijing, China	8.17%
#3	Taipei, Taiwan	7.64%
#4	Cupertino, United ...	5.70%
#5	Cambridge, United ...	4.83%
#6	Ngau Tau Kok, Hong...	3.75%
#7	Guangzhou, China	3.44%
#8	Vienna, Austria	3.12%
#9	Elizabeth, United ...	2.69%
#10	Santa Clara, Unite...	2.54%

Top Intrusion Source:		
#1	Taipei, Taiwan	57.72%
#2	Kowloon, Hong Kong	4.67%
#3	Guangzhou, China	4.07%
#4	Beijing, China	2.44%
#5	Vélizy-Villacoubla...	1.83%
#6	Houston, United St...	1.51%
#7	Taichung, Taiwan	1.32%
#8	Hangzhou, China	1.28%
#9	Seoul, Korea, Repu...	1.24%
#10	Herndon, United St...	1.08%

Top Malware Sources		
#1	Hanoi, Vietnam	21.60%
#2	Suzhou, China	18.21%
#3	Guangzhou, China	18.67%
#4	Dongguan, China	11.42%
#5	Mérida, Mexico	4.32%
#6	Beijing, China	2.16%
#7	Chicago, United St...	1.23%
#8	Scottsdale, United...	1.23%
#9	Buenos Aires, Arge...	0.93%
#10	Lima, Peru	0.93%

Top Spam Sources		
#1	Sofia, Bulgaria	12.16%
#2	Jersey City, Unite...	11.76%
#3	Tampa, United Stat...	8.90%
#4	Beijing, China	7.25%
#5	Hangzhou, China	5.78%
#6	New York, United S...	5.59%
#7	Hanoi, Vietnam	5.39%
#8	Rotterdam, Netherl...	4.90%
#9	Atlanta, United St...	2.84%
#10	Guangzhou, China	2.75%

Threats Blocked
20,402,487,058

Events Handled
105,940,822,421

Alert Condition
Limited virus/worm activity

Lessons learnt from recent incidents

Recent Security Breaches

- Home Depot
- Target
- Army National Guard
- Ebay
- J.P. Morgan Chase
- Michaels
- VTech

- SONY
- Anthem
- BlueCross BlueShield
- Harvard University
- Kaspersky Lab
- LastPass
- US Postal Service

Lessons Learnt
Target

- 70 million customer email addresses stolen
- 40 million debit and credit card numbers stolen from Nov-Dec 2013
- Via a hacked vendor – a heating and air conditioning subcontractor in Pennsylvania that was relieved of remote network access credentials after someone inside the company opened a virus-laden email attachment
- It is common for large retail operations to have a team that routinely monitors energy consumption and temperatures in stores to save on costs and to detect fluctuation outside of the acceptable range
- Failed to separate from the payment system network

Lessons Learnt
Home Depot

- 56 million debit and credit card numbers stolen from April to Sep 2014
- Entered the network via a hacked vendor’s user name and password
- Then gained access to the POS devices via a vulnerability in MS Windows

Lessons Learnt
Ashley Madison

Get started by telling us your relationship status:

Over 37,610,000 anonymous members!

IF YOU HAVE IP YOU ARE A TARGET!

THE INTERNET OF THINGS AT WORK

NORTH AMERICA

WWW.ISACA.ORG/RISK-REWARD-BAROMETER

ISACA®

Trust in, and value from, information systems

As wearables and other connected devices increasingly make their way into the workplace, IT professionals still see more risk than benefit. Yet with sound preparation, education and governance, enterprises can be well-positioned to embrace the benefits of the Internet of Things (IoT) .

BIG CHALLENGES

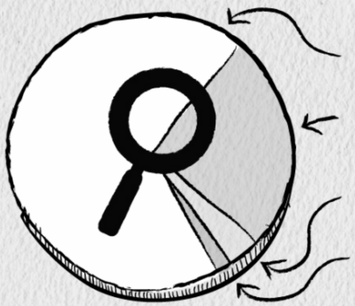
Challenge	%
INCREASED SECURITY THREATS	50%
DATA PRIVACY	24%
IDENTITY AND ACCESS MANAGEMENT	7%
COMPLIANCE REQUIREMENTS	6%
OWNERSHIP OF TECH AND/OR DATA OUTSIDE OF IT	6%

40%

SAY ORGANIZATION ALREADY HAS OR EXPECTS TO CREATE PLANS FOR INTERNET OF THINGS WITHIN NEXT 12 MONTHS

63% VS.

BELIEVE “BRING YOUR OWN WEARABLE” AND “BRING YOUR OWN DEVICE” ARE EQUALLY RISKY

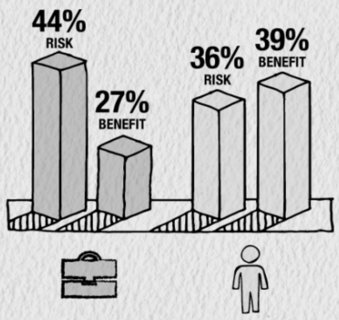


71%	VERY CONCERNED
24%	SOMEWHAT CONCERNED
3%	NOT CONCERNED
1%	DON’T BELIEVE IT’S DECREASING

IS PRIVACY DEAD?

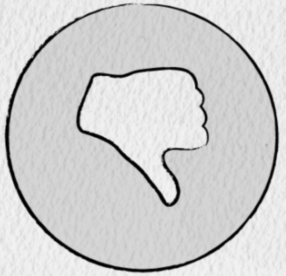
Attitude toward decreasing level of personal privacy

INTERNET OF THINGS RISK VS. BENEFIT



	ENTERPRISES	INDIVIDUALS
RISK	44%	36%
BENEFIT	27%	39%

WORKPLACE BYOD POLICY ADDRESSES WEARABLE TECH



60% NO

18% DON’T HAVE A BYOD POLICY

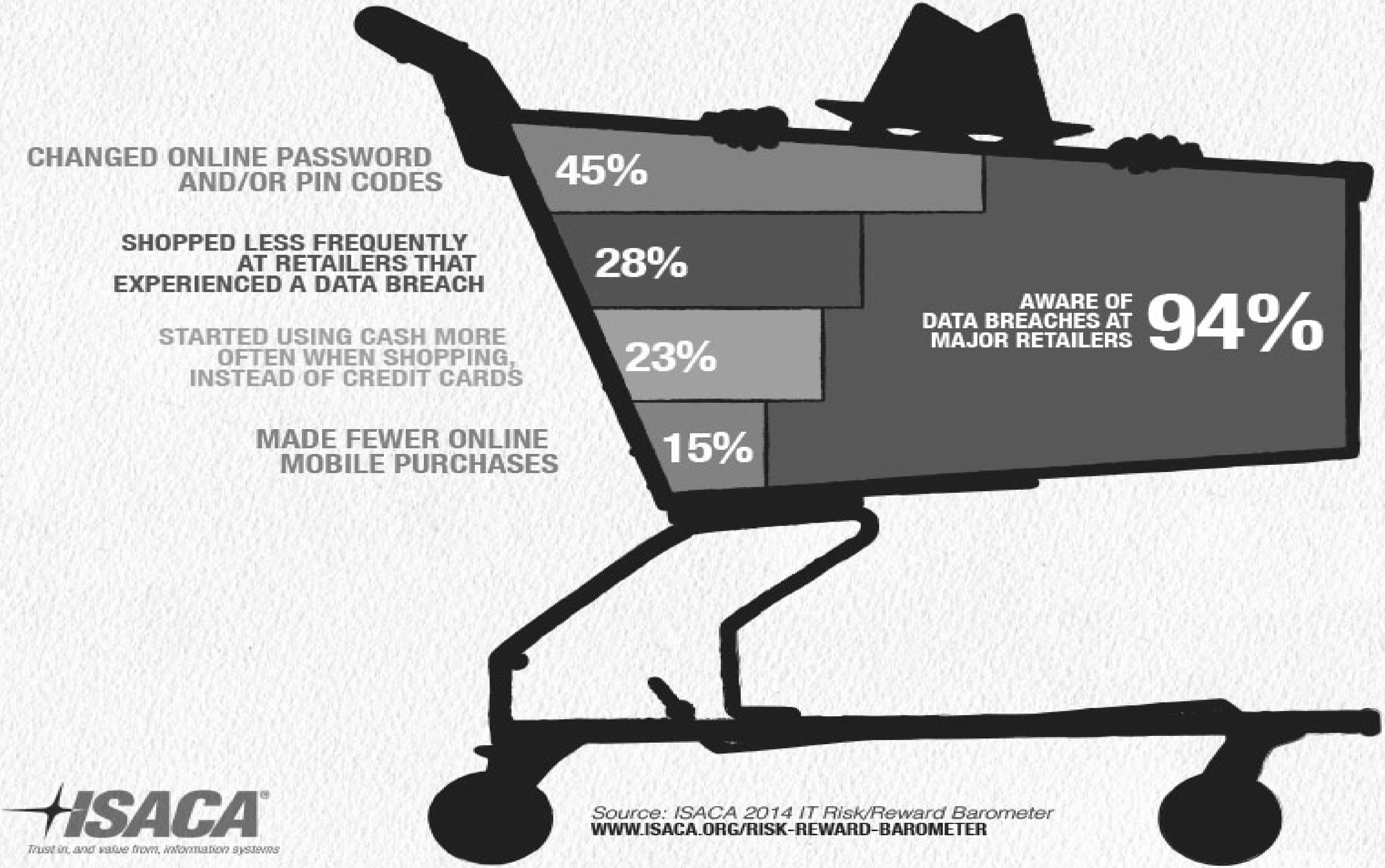
12% YES

10% UNSURE

Source: 2014 ISACA IT Risk/Reward Barometer

DO SHOPPERS CARE ABOUT DATA BREACHES?

Most US consumers are aware of the data breaches at major retailers over the past year. A substantially smaller number changed their shopping behaviors as a result.



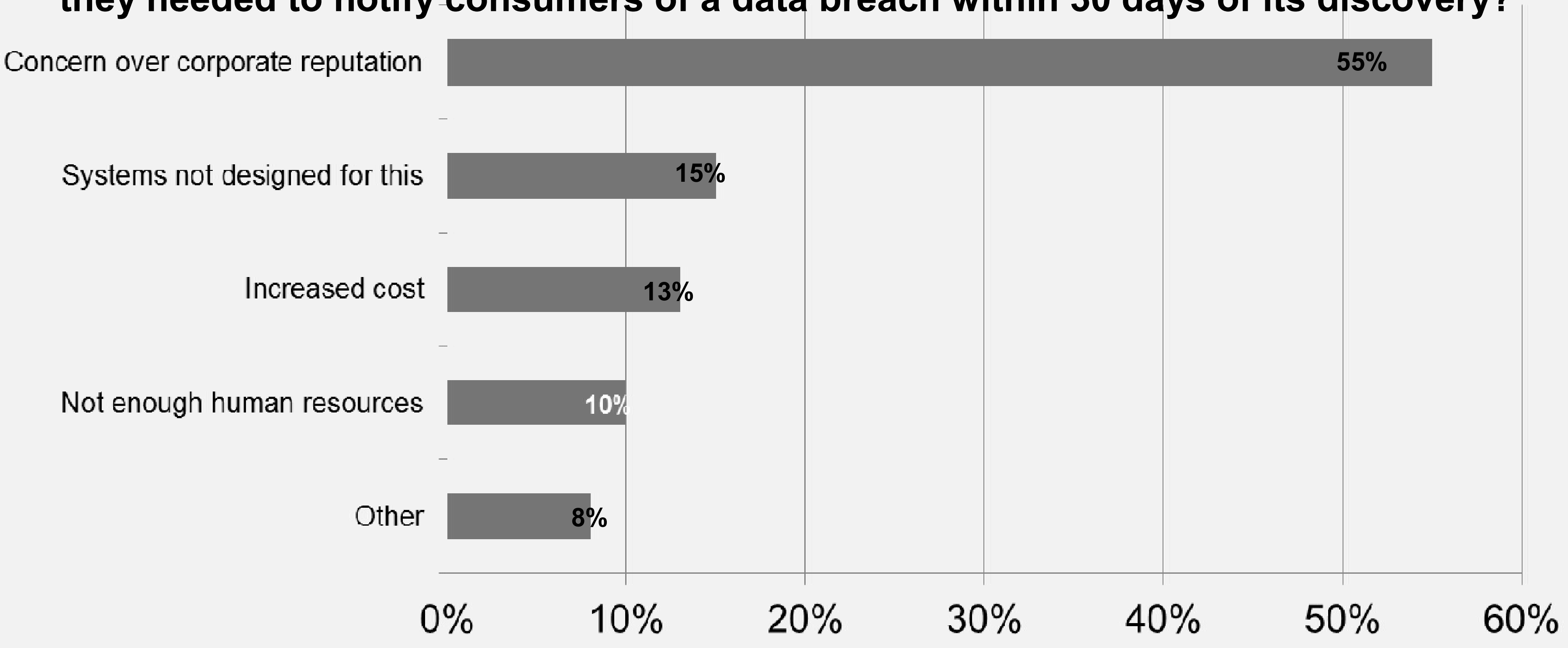
ISACA®
Trust in, and value from, information systems

Source: ISACA 2014 IT Risk/Reward Barometer
WWW.ISACA.ORG/RISK-REWARD-BAROMETER

DATA BREACH NOTIFICATION SUPPORT

76% **agree or strongly agree with United States President Obama’s proposal to require companies to notify consumers of a data breach within 30 days**

Of the following, what do you think is the greatest challenge companies would face if they needed to notify consumers of a data breach within 30 days of its discovery?



CYBERSECURITY: MARKET NEED

- **Cybersecurity is a top global concern. 82% of enterprises expect to experience a cyber incident in 2015**

- **69% say certification is required for cybersecurity jobs**

- **There is a cybersecurity skills crisis: 1 million unfilled jobs (source: Cisco)**

- **The research is clear. Cybersecurity has evolved from critical topic into a public safety issue**

CSX™

CYBERSECURITY NEXUS

Cybersecurity Skills Crisis

Too Many Threats

62% INCREASE IN BREACHES **IN 2013**[1]

1 IN 5 ORGANIZATIONS HAVE **EXPERIENCED AN APT ATTACK**[4]

US $3 TRILLION TOTAL GLOBAL IMPACT OF **CYBERCRIME**[3]

8 MONTHS IS THE AVERAGE TIME **AN ADVANCED THREAT GOES UNNOTICED** ON VICTIM'S NETWORK[2]

2.5 BILLION **EXPOSED RECORDS** AS A RESULT OF A DATA BREACH IN THE PAST 5 YEARS[5]

Too Few Professionals

62% OF ORGANIZATIONS **HAVE NOT INCREASED SECURITY TRAINING IN 2014**[6]

1 OUT OF 3 SECURITY PROS ARE **NOT FAMILIAR WITH ADVANCED PERSISTENT THREATS**[7]

<2.4% GRADUATING STUDENTS **HOLD COMPUTER SCIENCE DEGREES**[8]

1 MILLION UNFILLED SECURITY JOBS WORLDWIDE[9]

83% **OF ENTERPRISES** CURRENTLY LACK THE RIGHT SKILLS AND HUMAN RESOURCES TO PROTECT THEIR IT ASSETS[10]

Enterprises are under siege from **a rising volume of cyberattacks.**

At the same time, the global demand for skilled professionals sharply outpaces supply. Unless this gap is closed, organizations will continue to face major risk. Comprehensive educational and networking resources are required to meet the needs of everyone from entry-level practitioners to seasoned professionals.

SOURCES: 1. *Increased Cyber Security Can Save Global Economy Trillions*, McKinsey/World Economic Forum, January 2014; **2.** *M-Trends 2013: Attack the Security Gap*, Mandiant, March 2013; **3.** *Increased Cyber Security Can Save Global Economy Trillions*, McKinsey/World Economic Forum, January 2014; **4.** *ISACA's 2014 APT Study*, ISACA, April 2014; **5.** *Increased Cyber Security Can Save Global Economy Trillions*, McKinsey/World Economic Forum, January 2014; **6.** *ISACA's 2014 APT Study*, ISACA, April 2013; **7.** *ISACA's 2014 APT Study*, ISACA, April 2014; **8.** *Code.org*, February 2014; **9.** *2014 Cisco Annual Security Report;* **10.** *Cybersecurity Skills Haves and Have Nots*, ESG, March 2014

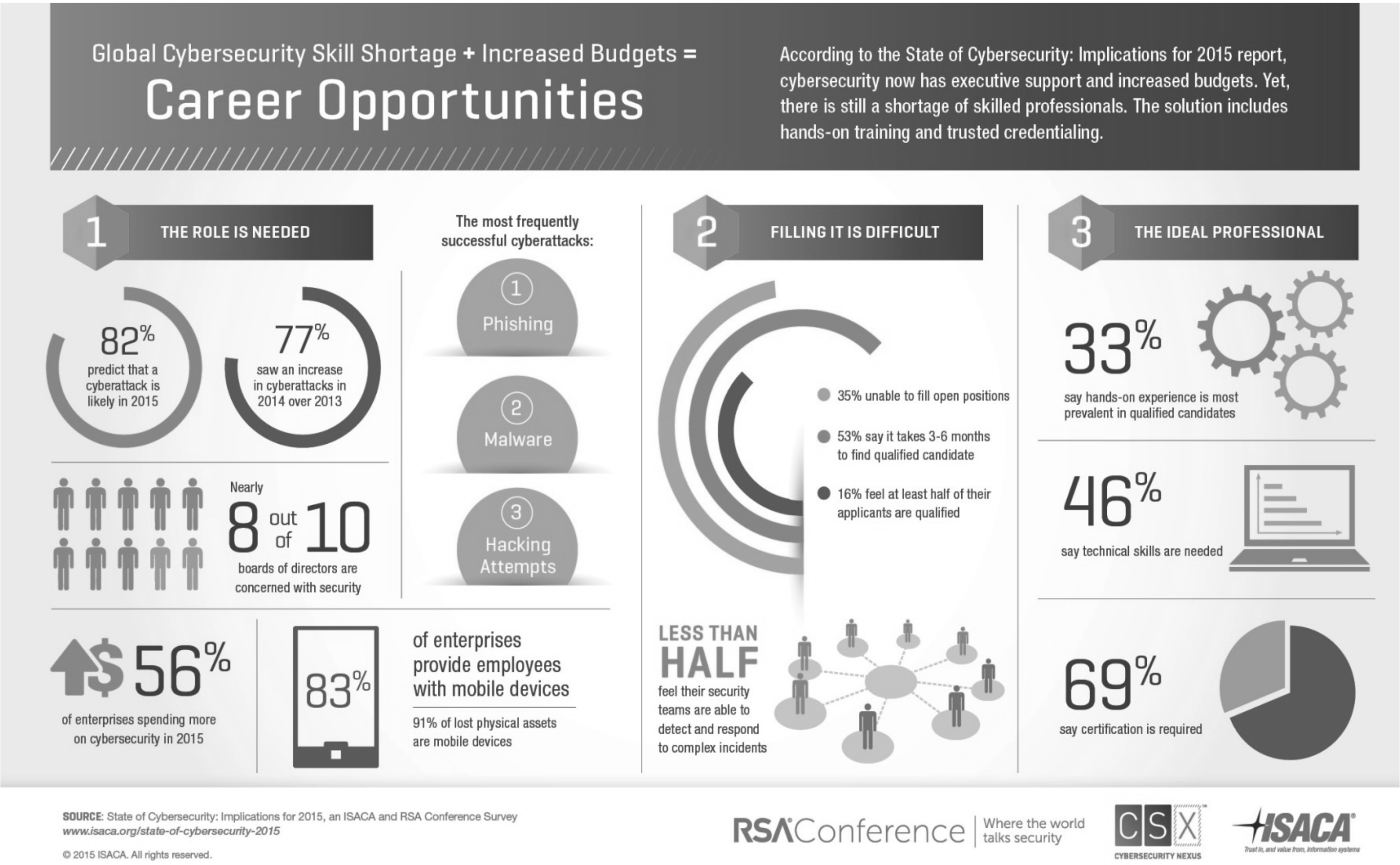
CSX™ CYBERSECURITY NEXUS

ISACA

Trust in, and value from, information syste

STATE OF CYBERSECURITY: IMPLICATIONS FOR 2015

ISACA and RSA CONFERENCE JOINT SURVEY—649 RESPONDENTS WORLDWIDE



Global Cybersecurity Skill Shortage + Increased Budgets =

Career Opportunities

According to the State of Cybersecurity: Implications for 2015 report, cybersecurity now has executive support and increased budgets. Yet, there is still a shortage of skilled professionals. The solution includes hands-on training and trusted credentialing.

1 THE ROLE IS NEEDED

82% predict that a cyberattack is likely in 2015

77% saw an increase in cyberattacks in 2014 over 2013

Nearly 8 out of 10 boards of directors are concerned with security

56% of enterprises spending more on cybersecurity in 2015

83% of enterprises provide employees with mobile devices

91% of lost physical assets are mobile devices

The most frequently successful cyberattacks:

1. Phishing
2. Malware
3. Hacking Attempts

2 FILLING IT IS DIFFICULT

- 35% unable to fill open positions
- 53% say it takes 3-6 months to find qualified candidate
- 16% feel at least half of their applicants are qualified

LESS THAN HALF feel their security teams are able to detect and respond to complex incidents

3 THE IDEAL PROFESSIONAL

33% say hands-on experience is most prevalent in qualified candidates

46% say technical skills are needed

69% say certification is required

SOURCE: State of Cybersecurity: Implications for 2015, an ISACA and RSA Conference Survey
www.isaca.org/state-of-cybersecurity-2015

RSAConference | Where the world talks security

CSX CYBERSECURITY NEXUS

ISACA Trust in, and value from, information systems

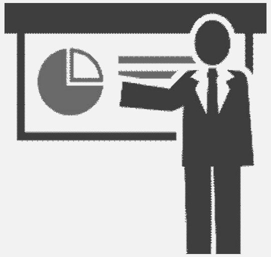
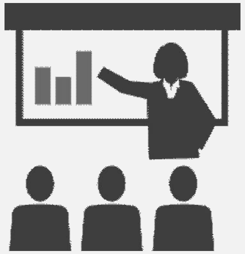
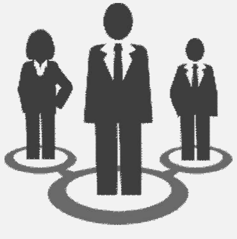
www.isaca.org/state-of-cybersecurity-2015

THE ISACA SOLUTION

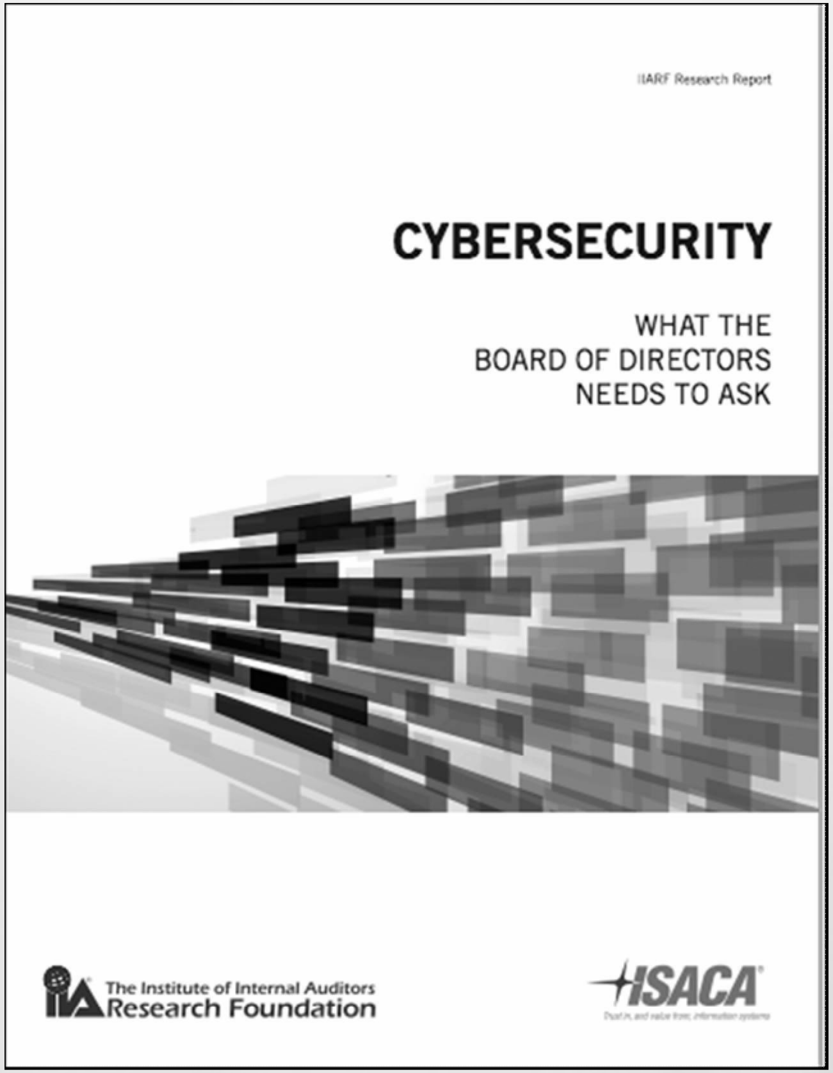
CSX Is Providing a Single Source for Cybersecurity Professionals:

Our holistic program will be the first and only “one stop shop” providing a complete solution and covering the full career lifecycle.

ISACA collaborates with leading global governments and organizations at the center of cybersecurity

Credentialing and Training	Education/ Conferences	Membership	Resources/ Publications	Career Management
				

ISACA Publications on Cybersecurity



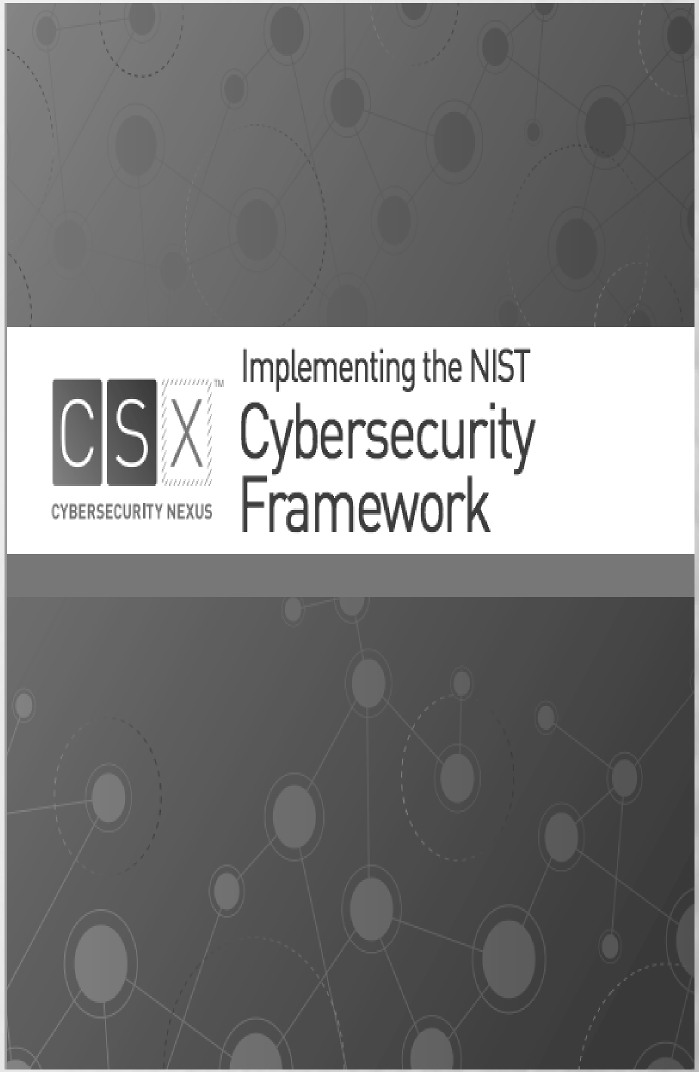
IIARF Research Report

CYBERSECURITY

WHAT THE
BOARD OF DIRECTORS
NEEDS TO ASK

The Institute of Internal Auditors
Research Foundation

ISACA
Trust in, and value from, information systems



CSX
CYBERSECURITY NEXUS

Implementing the NIST
Cybersecurity
Framework

NEW CYBERSECURITY CERTIFICATIONS

CSX Practitioner —Demonstrates ability to serve as a first responder to a cybersecurity incident following established procedures and defined processes. (1 certification, 3 training courses; prerequisite for CSX Specialist)

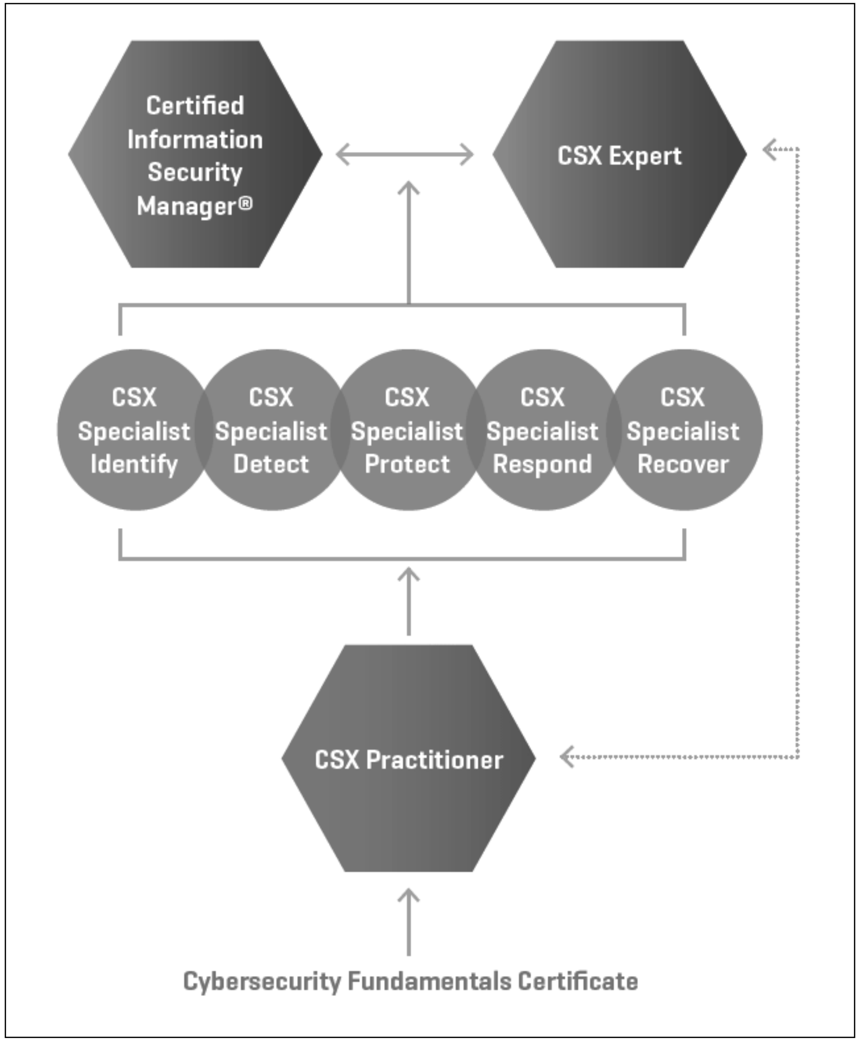
CSX Specialist —Demonstrates effective skills and deep knowledge in one or more of the five areas based closely on the NIST Cybersecurity Framework: Identify, Detect, Protect, Respond and Recover. (**5 certifications**, 5 training courses; requires CSX Practitioner)

CSX Expert —Demonstrates ability of a master/expert-level cybersecurity professional who can identify, analyze, respond to, and mitigate complex cybersecurity incidents. (1 certification, 1 training course; no prerequisites required)

NEW CYBERSECURITY CERTIFICATIONS

CSX
CERTIFICATIONS

CSX training and certifications offered for skill levels and specialties throughout a professional's career.



Certified Information Security Manager®

CSX Expert

CSX Specialist Identify

CSX Specialist Detect

CSX Specialist Protect

CSX Specialist Respond

CSX Specialist Recover

CSX Practitioner

Cybersecurity Fundamentals Certificate

www.isaca.org/csx-certifications

Seminar Summary

Key Points

- **Organisations (and individuals) will rely more and more on Technologies and Cloud Computing**
- **We should anticipate more Cybersecurity and Cloud-related risks (and frauds)**
- **Auditors and security professionals will be expected to understand Cybersecurity and Cloud-related risks, and to recommend appropriate controls**
- **Train all "Auditors" to become "IT Auditors"**
- **Focus on acquiring the right PEOPLE and CULTURE**

Remember ……
Attitudes are Contagious

Together, we can change the world, one audit at a time!

We appreciate your contributions to IIA!

THANK YOU!