CHANGE: CHALLENGE TODAY'S SECURITY THINKING.

ETDA's report

RSA Images

RSA

Topics of interest

- General themes
- Cybersecurity workforce updates
- Government-led cybersecurity framework
- Cybersecurity fundamentals – An unknown factor & Outside in and Inside out monitoring
- Legal issues
- Visiting Google and Microsoft

RSA Conference 2015

San Francisco | April 20-24 | Moscone Center

HIGHLIGHTS IN RSA 2015

#RSAC

ETDA สพธอ
www.etda.or.th

ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA

RSA Conference 2015

April 2015

Venue : Moscone Center,

San Francisco

RSA 2015 - Bigger Security Conference than last year

- > 30,000 Attendees
- > 400 Exhibitors and Sponsors
- > 550 Speakers

Exhibitions

Two expo halls, hundreds of solutions featuring threat-centric security solutions to

- provide visibility and security management services,
- deliver threat Intelligence,
- and protect from advanced threats (IoT, Cloud)
- Big Data

Passes

ETDA www.etda.or.th

ThaiCERT Thailand Computer Emergency Response Team a member of ETDA

Compare Passes

ACCESS/BENEFITS	Full Conference	Explorer Expo Plus (Sold Out)	Explorer Expo	Tutorial Only
MONDAY EVENTS				
Orientation	YES			
Innovation Sandbox	YES	YES	YES	
Seminars ▲	YES	YES	YES	
SANS Tutorials	$	$	$	YES
(ISC)² Certification Training	$	$	$	
KEYNOTES & SESSIONS				
Keynotes: Tuesday	YES	YES		
Keynotes: Wednesday - Friday	YES	YES	YES	YES
The Viewing Point	YES	YES	YES*	YES*
Track Sessions	YES	■		

Breakout Sessions

ETDA www.etda.or.th ThaiCERT Thailand Computer Emergency Response Team a member of ETDA

More than 20 concurrent tracks covering

- Analytics & Forensics
- Application Security
- Association Special Topics
- Breaking Research
- C-suite View (New)
- Cloud Security & Virtualization
- Cryptography
- Data Security & Privacy
- Governance, Risk & Compliance
- Hackers & Threats
- Hackers & Threats Advanced
- Human Element
- Identity (New)
- Industry Experts
- Keynotes
- Law
- Mobile Security
- Policy & Government
- Professional Development
- Security Strategy
- Securing the Ecosystem (New)
- Security Trends & Innovation
- Technology Infrastructure & Operations

Internet of Me

- Internet of Things is coming to your organization whether you want it or not
  - Things are about you as a consumer and sensors
  - Compute Power (Cloud)
  - Network Connectivity (Internet, LTE, WIFI)
  - Proximity Communication (NFC, Bluetooth)
- Implication
  - Hard to define your enterprise network perimeter
  - Patch management is impossible (things use too many Oses and Apps)
  - Goal of Security is damage containment to minimize adverse impact
  - Require timely detection and response

Cybersecurity Readiness Goals

ETDA www.etda.or.th ThaiCERT Thailand Computer Emergency Response Team a member of ETDA

Goal #1: Understand Lines of Authority and Roles

- Responsibility
- Organizational view/approach to cyber incidents
- Communication

Goal #2: Increase Preparedness

- Understand effects of plans and procedures
- Create level of confidence and prevent future panic

Goal #3: Increase Awareness of Gaps and Vulnerabilities

- Investigative Capabilities
- Detection & Reporting (Process & Communication)
- Vendor management
- Security Awareness buy-in and commitment of resources

Goal #4: Identify Points of External Interaction

- Individuals
- Agencies
- Press & Social Media
- Vendors

Operations when network is compromised

If you have not detected an attack/compromise in the last 6 month, it is not because it is not happening – it is because you are not looking in the right areas

Protection is Ideal
But
Detection is a Must

Detection ingress traffics -> source of attacks
Detection egress traffics -> cause of damages

Focus on outbound traffics:

- Number of connections
- Length of connections
- Amount of data
- Percent that is encrypted
- Destination IP Addresses

Talk to management:
What percentage of your budget are you spending on coffee and maid service compared to on cybersecurity?

US Government Information Sharing

STIX/TAXII

ECS

ISAC

ISAO

CISCP

NCCIC

STIX/TAXII : Structure Threat Information Expression/Trusted Automated Exchange of Indicator Information

CISCP : Cyber Information Sharing and Collaboration Program ->Threat sharing

ECS : Enhanced Cybersecurity Services -> Provide confidential data to ISPs

NCCIC : National Cybersecurity & Communication Integration Center (NCCIC) -> US-CERT & ICS-CERT

ISAC/ISAO : Information Sharing and Analysis Center/Organization

ISACs in US

NCC
AVIATION ISAC
IT ISAC
ONG-ISAC
SC ISAC
HEALTH ISAC
ST-ISAC
REN-ISAC
APTA
EMR-ISAC
MARITIME ISAC
NEI
Real Estate ISAC
ES-ISAC
FINANCIAL SERVICES ISAC
WaterISAC
DIB ISAC
DEFENSE INDUSTRIAL BASE
MULTI-STATE ISAC

CI in US

INFORMATION SHARING AND ANALYSIS CENTERS (ISACS) OPERATE WITHIN SECTORS
U.S. DEPARTMENT OF HOMELAND SECURITY
16
Critical
Infrastructure
Sectors
INFORMATION SHARING DATA FLOWS

RSA 2015 Slides and Keynote VDOs

Presentation Slides

http://www.rsaconference.com/events/us15/agenda or

Search with keywords "*rsa 2015 agenda*"

Keynote VDOs

http://www.rsaconference.com/events/us15/agenda/keynotes

Seach with keywords "*rsa 2015 keynotes*"

CYBERSECURITY WORKFORCE UPDATES

ผลการสำรวจเรื่อง Global Information Security Workforce Study ประจำปี 2015 โดย (ISC)2

http://www.isc2cares.org

Status of the Industry: 2015 Global Information Security Workforce Study

หลักการ

- เนื่องจากขณะนี้หลายประเทศให้ความสนใจด้านการรับมือภัยคุกคามไซเบอร์มากขึ้น และช่องโหว่ในแอปพลิเคชั่นมีมากเกินกว่าการแก้ไขปัญหาให้ทัน รวมทั้งความพร้อมด้านความมั่นคงปลอดภัยยังอยู่ในระดับคงที่แม้ว่าจะจัดสรรงบประมาณเพิ่มขึ้นแล้วก็ตาม

ผลลัพธ์

- จำนวนบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ยังขาดแคลน และเป็นอัตราเพิ่มขึ้นต่อเนื่องทุกปี เนื่องจากบุคลากรด้านความมั่นคงปลอดภัยต้องใช้เวลาพัฒนาค่อนข้างมาก แม้ว่ามีความต้องการเพิ่มขึ้นแต่จำนวนบุคลากรที่มีก็ยังเท่าเดิม การปัญหาในขณะนี้คือ การ Outsource งานด้านความมั่นคงปลอดภัยไปยังหน่วยงานภายนอก แต่สิ่งที่เรามองไม่เห็นคือ เราได้ผลักงานด้านความมั่นคงปลอดภัยไปให้บุคลากรด้าน IT ที่ไม่ได้เชี่ยวชาญมากนักด้านความมั่นคงปลอดภัย รวมทั้งบางกิจกรรมด้านความมั่นคงปลอดภัยยังไม่ได้ดำเนินการ หรือดำเนินการแค่บางส่วน
- สิ่งที่หลายหน่วยงานร่วมกันแก้ไขปัญหา คือการพัฒนาหลักสูตรเพื่อฝึกอบรมบุคลากร โดยเริ่มจากในมหาวิทยาลัย และการฝึกอบรมภายในหน่วยงาน รวมทั้งควรมีการสร้างความร่วมมือระหว่างสถาบันการศึกษา หน่วยงานอิสระ และภาครัฐเพื่อจัดเตรียมหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์โดยเฉพาะ หรืออาจเป็นมหาวิทยาลัยด้านไซเบอร์ การกระตุ้นให้เกิด Talent โดยใช้การแข่งขัน Hackatron การจูงใจบุคลากร เช่น การยืดหยุ่นด้านเวลาการเข้างาน การทำงานจากที่ใดก็ได้ การให้ทุน/จัดอบรมอย่างต่อเนื่อง

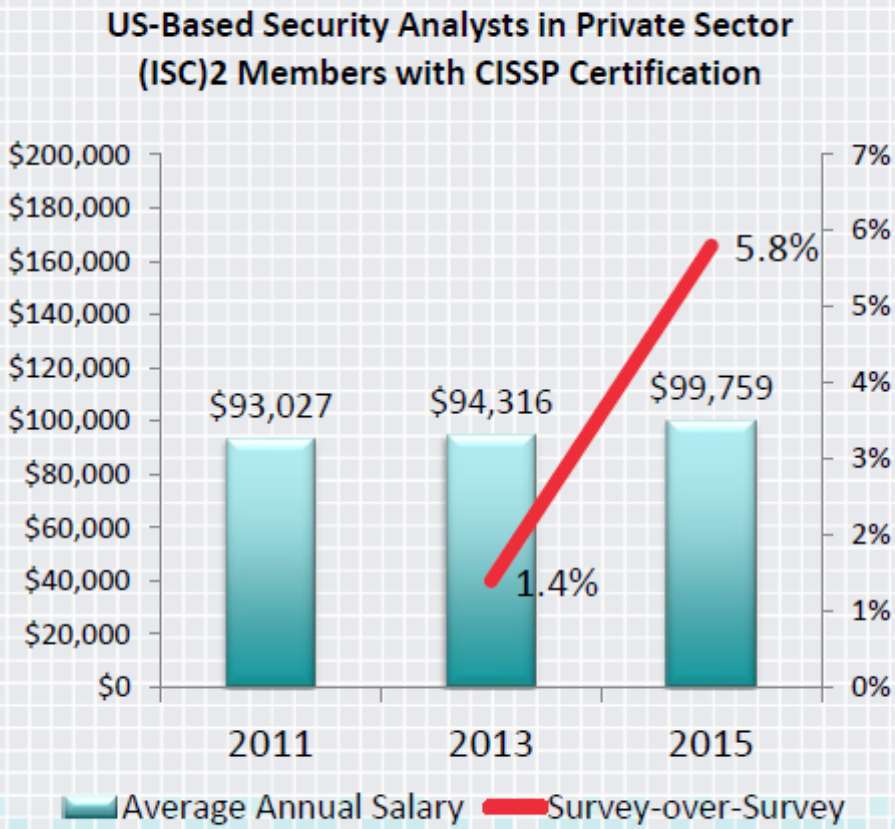
ข้อมูลสถิติอื่นๆ ที่น่าสนใจ ได้แก่

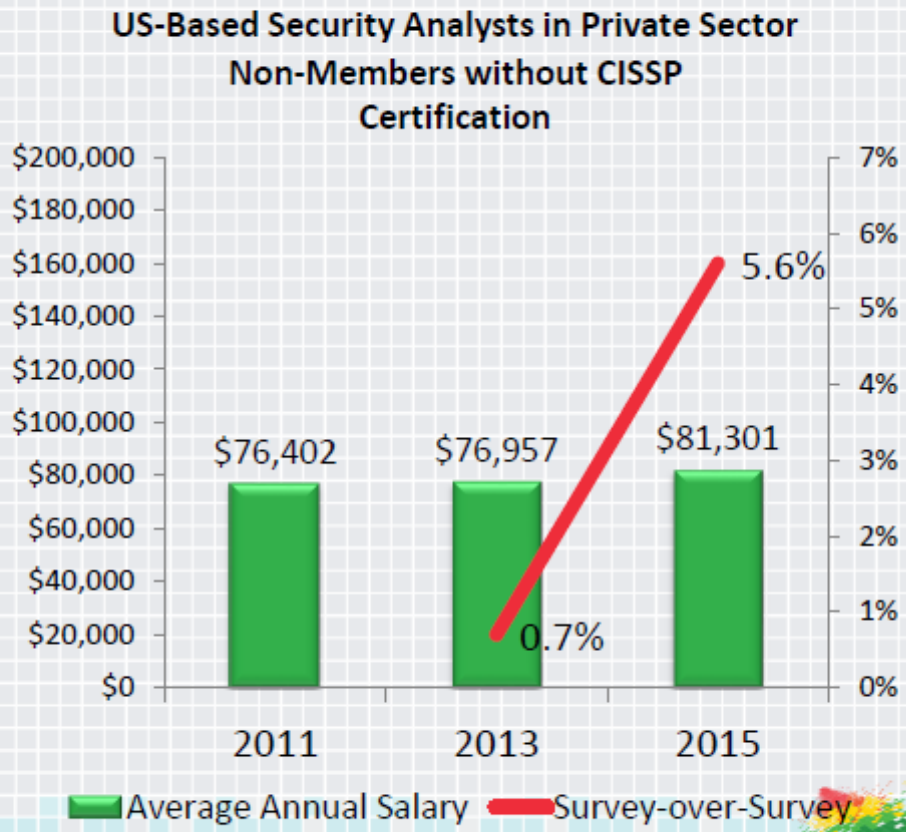
- บุคลากรกว่า 20% เปลี่ยนงานภายใน 3 ปี
- ค่าตอบแทนเฉลี่ยต่อปีของบุคลากรสายความมั่นคงปลอดภัยในปี 2015 อยู่ที่ 99,000 USD หรือ 3.16 ล้านบาท

CISSP vs non-CISSP !!!

Let's talk about why you are here: Study Shows Salaries Increasing!

#RSAC

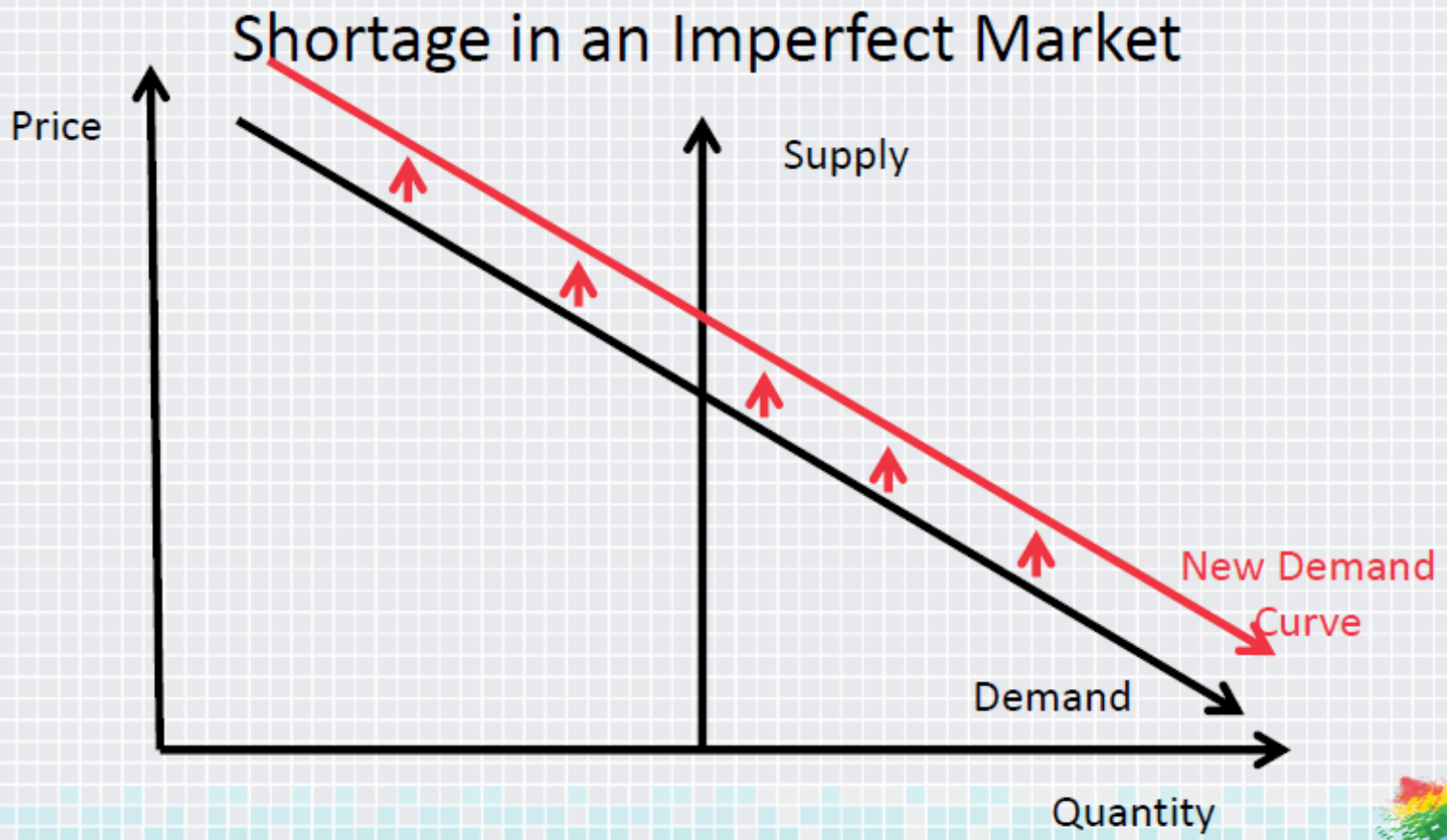




Cybersecurity workforce shortage

What is Shortage?

#RSAC



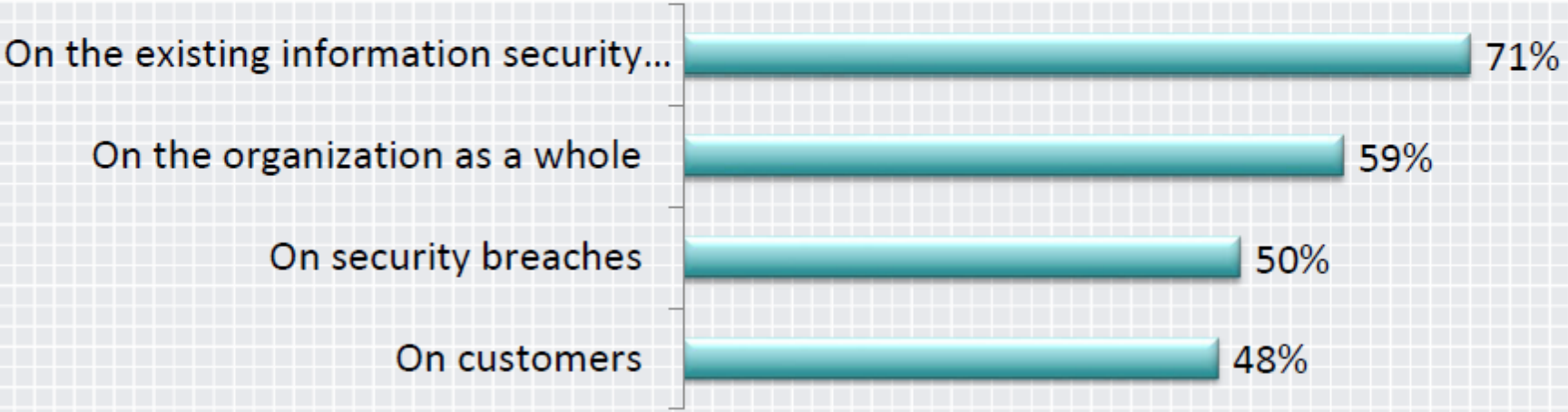
Workforce shortage impacts

#RSAC

Workforce Shortage Effects

What is the impact of your organization's shortage of information security workers on each of the following?

(Selected as Top 2 on a 5-point Very Great Impact-to-No Impact at All Scale)



Workforce shortage impacts

Workforce Shortage Effects

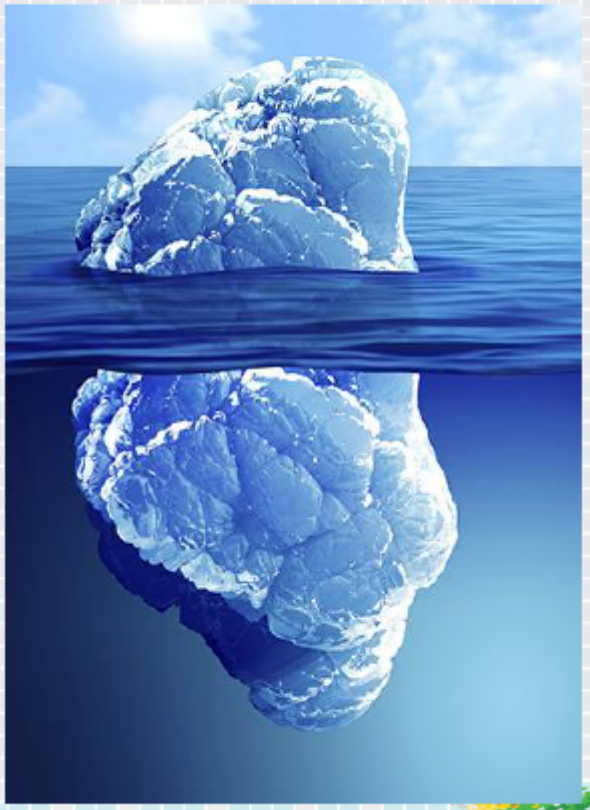
#RSAC

What you can see

- Security professional efficiency & Outsourcing
- Technology leverage to reduce security professional workload

What you can't see

- Pushing security tasks to IT professionals, a force multiplier
- Security tasks are getting left undone or performed sub-optimally



Opposing Perspectives on InfoSec Hiring and Interviewing

- บุคลากรด้านความมั่นคงปลอดภัยไซเบอร์มีการแข่งขันในการจ้างงานค่อนข้างสูง อาจเป็นเรื่องยากที่จะมองหาคนที่ใช่เข้ามาทำงานในองค์กร สิ่งที่ทำได้คือการสัมภาษณ์ที่มีประสิทธิภาพเท่านั้น
- หากมองในมุมผู้สมัครงาน ต้องยอมรับว่า Resume เสมือนเป็นใบเบิกทาง (Marketing Document) ก่อนที่ผู้ว่าจ้างจะเรียกสัมภาษณ์ ดังนั้น Resume ส่วนใหญ่จึงมีการอธิบายค่อนข้างเกินจริง ดังนั้นการเขียน Resume ที่ดีควรเขียนให้กระชับ และมีคำสำคัญที่ต้องการสื่อสาร ในการอธิบายประสบการณ์ทำงานควรหลีกเลี่ยงการระบุจำนวน เช่น เคยดูแล Server กี่ตัวหรือทำงานร่วมกับคนกี่คน เนื่องจากแต่ละหน่วยงานมีขนาดไม่เท่ากัน
- หากมองในมุมผู้ว่าจ้าง การเขียนใบบรรยายคุณลักษณะงาน (Job Description: JD) ควรระบุสิ่งที่ต้องการให้ชัดเจน เช่น คุณสมบัติ/ประสบการณ์/Certification ที่มี และควรเขียนเนื้องานให้จูงใจผู้สมัครงาน (Intellectual Curiosity/ Passion) ไม่ควรเขียนสิ่งที่ทำในปัจจุบันซึ่งอาจจะไม่ถูกต้องนัก รวมถึงการกำหนดชื่อตำแหน่งงานก็ควรจูงใจด้วย ชื่อเสียงของหน่วยงานผู้ว่าจ้างก็เป็นปัจจัยสำคัญที่ทำให้มีผู้สนใจมาทำงานมากขึ้น ซึ่งเป็นเรื่องยากและใช้เวลานานในการสร้าง และง่ายที่จะทำลาย ดังนั้น ผู้ว่าจ้างอาจพิจารณาสื่อต่างๆ โดยเฉพาะใน Social Media เพื่อให้หน่วยงานเป็นที่รู้จักในตลาดมากขึ้น
- ความรู้ทางเทคนิคเป็นเพียงจุดเริ่มต้นที่ควรมีในการทำงานเท่านั้น ต้องมีความรู้ด้านการบริหารจัดการ/ความรู้ใน Industry นั้นๆ ด้วย เช่น สายงานโรงพยาบาล นอกจากนี้ ทักษะด้านการสื่อสารกับลูกค้า กับทีมเทคนิค และการพูดในที่สาธารณะ ก็เป็นปัจจัยสำคัญที่ทำให้ก้าวขึ้นไปในตำแหน่งที่สูงขึ้น อย่างไรก็ตาม ผู้ปฏิบัติงานบางคนก็ไม่ได้ต้องการจะทำงานระดับบริหาร

GOVERNMENT-LED CYBERSECURITY FRAMEWORK

Framework for Improving Critical Infrastructure Cybersecurity

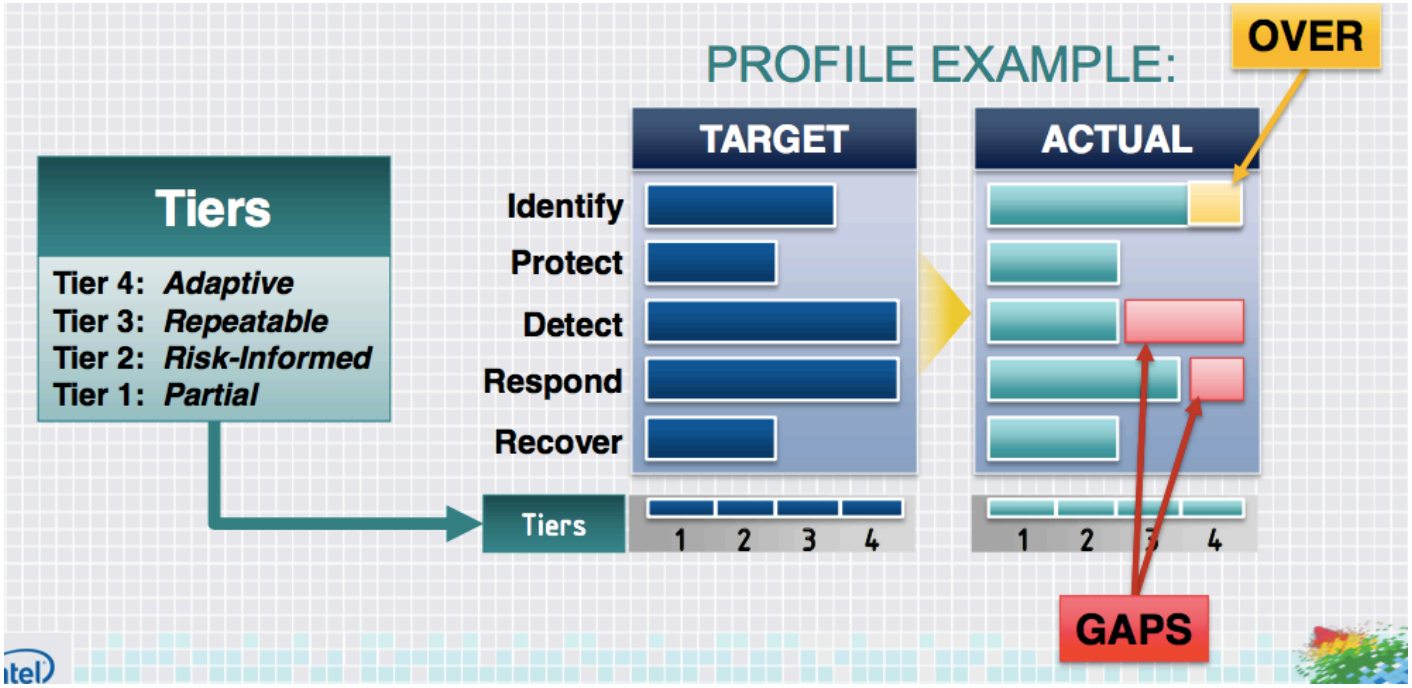
http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

About the Framework

- Framework for Improving Critical Infrastructure Cybesecurity กำหนดโดย NIST และเผยแพร่เป็นเวอร์ชันที่ 1.0 เมื่อวันที่ 12 กุมภาพันธ์ 2014 ซึ่งเป็นการทำตาม Presidential Executive Order 13636 เรื่อง Improving Critical Infrastructure Cybersecurity ออกในเดือนกุมภาพันธ์ 2013 Framework นี้เกิดจากความร่วมมือระหว่างภาคอุตสาหกรรมและหน่วยงานของรัฐโดยใช้เวลา มากกว่า 1 ปี ในการจัดทำ
- Framework ซึ่งอยู่บนหลักการของการบริหารจัดการความเสี่ยง ประกอบด้วย 3 ส่วนคือ ส่วนของ Framework core ได้แก่ รายการของกิจกรรมและผลลัพธ์ด้านความมั่นคงปลอดภัย ที่คาดว่าจะได้รับ จัดตามลักษณะฟังก์ชันงาน 5 ประเภทในวงจรการบริหารจัดการความเสี่ยงไซเบอร์ คือidentify, protect, detect, respond และ recover

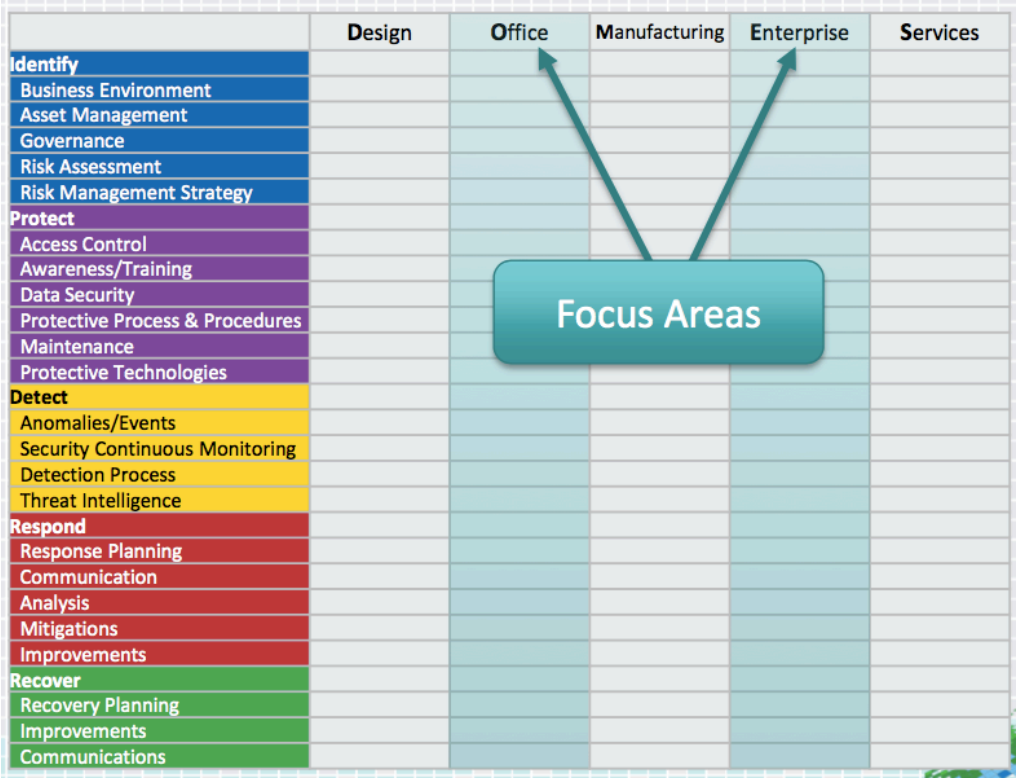
Maturity model for Improving Cybersecurity

- Framework implementation tiers กำหนดแนวทางการจัดระดับการบริหารจัดการความเสี่ยงไซเบอร์ขององค์กร ตั้งแต่ระดับ 1 (partial) – 4 (adaptive)
- Framework profile ซึ่งสะท้อนผลลัพธ์ด้านความมั่นคงปลอดภัยที่ได้จากการนำกิจกรรมใน Framework core ไปปฏิบัติ



CSF Implementation – Intel Case

- บริษัทอินเทลฯ ได้เริ่มมีส่วนร่วมใน Framework มาตั้งแต่ต้นในเดือนกุมภาพันธ์ 2013
- แต่เนื่องจากขนาดของบริษัทที่ใหญ่มาก มี business unit และ computing platform จำนวนมาก (มากกว่าสามแสน platforms) จึงเลือกที่จะทำโครงการนำร่องครอบคลุมงาน Office และ Enterprise เนื่องจากงานส่วนนี้บริษัทดูแลเองและเป็นงานที่ทีมหลักมีความคุ้นเคยมากที่สุด
- โดยเลือกกิจกรรมมา 21 categories และเพิ่มอีกหนึ่ง category เรื่อง Threat intelligence ซึ่งไม่มีใน Framework



CSF Implementation – Intel Case

จากดำเนินโครงการนำร่อง บริษัทอินเทลฯ พบว่า Framework เป็นเครื่องมือสำคัญที่กระตุ้นให้เกิดการสื่อสารภายในเกี่ยวกับความเสี่ยง การควบคุมภายใน การบริหารจัดการความเสี่ยง และการทำงานไปในทิศทางเดียวกัน Framework ทำให้หลายส่วนงานสื่อสารโดยใช้ภาษาเดียวกัน

Our Final Result

NOTIONAL / EXAMPLE ONLY

Category	Actual	Target	Delta
Identify	3	3	0
Business Environment	2	2	0
Asset Management	2	2	0
Governance	4	3	1
Risk Assessment	2	2	0
Risk Management Strategy	2	4	-2
Protect	2	2	0
Access Control	1	1	0
Awareness/Training	2	3	-1
Data Security	2	2	0
Protective Process & Procedures	2	2	0
Maintenance	3	4	-1
Protective Technologies	2	2	0
Detect	1	1	0
Anomalies/Events	3	2	1
Security Continuous Monitoring	4	4	0
Detection Process	2	2	0
Threat Intelligence	3	4	-1
Respond	2	2	0
Response Planning	1	1	0
Communication	3	3	0
Analysis	2	2	0
Mitigations	2	2	0
Improvements	3	4	-1
Recover	3	3	0
Recovery Planning	2	4	-2
Improvements	2	2	0
Communications	4	4	0

CYBERSECURITY FUNDAMENTALS:

AN UNKNOWN FACTOR & OUTSIDE IN AND INSIDE OUT MONITORING

> There are known knowns. These are things we know that we know. There are known unknowns. That is to say, there are things that we know we don't know. But there are also unknown unknowns. There are things we don't know we don't know.

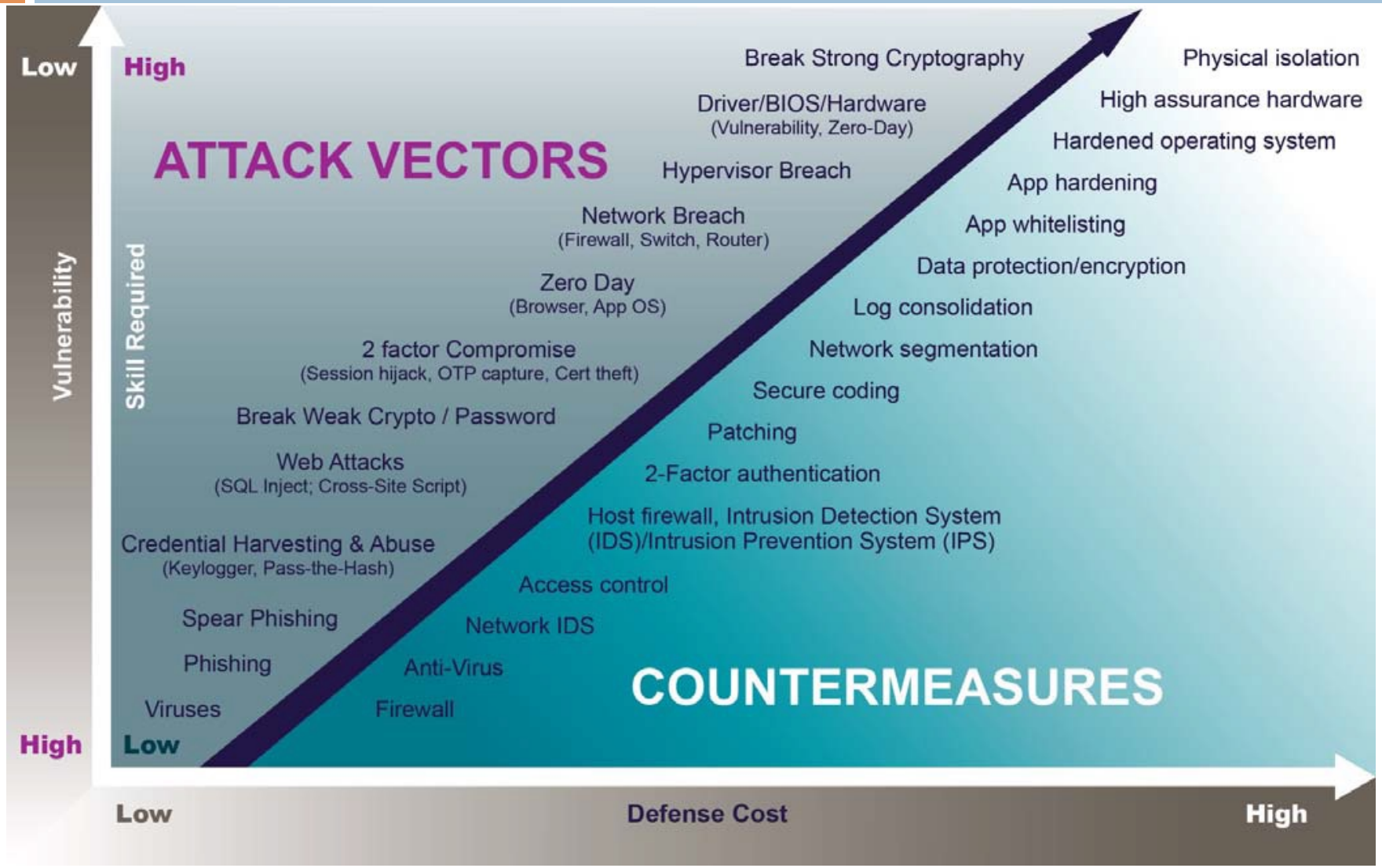
Donald Rumsfeld

An unknown Factor in Cyber Security

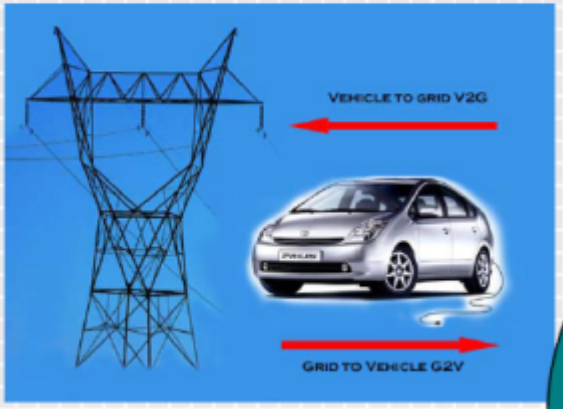
- แนวคิดในการประเมินความเสี่ยงของ Cyber Security ในโลกวันนี้เปลี่ยนแปลงไปจากเดิมมาก
  - อดีต Risk = Threads * Vulnerability * Impact
  - ปัจจุบัน Risk = Threads * Vulnerability * Impact + Unknown factor
- ในทุกองค์กรย่อมมสิ่งที่เราเองละเลยหรือไม่กระทั่งทราบว่ามีมาก่อน เช่น
  - คนในองค์กรทำงานที่ถูกต้องแต่บนวิธีการที่มีช่องโหว่ทาง Cyber Security
  - คนนอกเข้ามาใช้ระบบของเรา
  - Technology เปลี่ยนไป พัฒนาขึ้น
  - IT Supply Chain (ระบบที่ติดต่อกัน) ซับซ้อนจนเกิดความผิดพลาด
  - รัฐ พยามยามเจาะข้อมูล
  - คู่แข่งโจมตี

  และสิ่งที่เราไม่รู้นี่เองเป็นสิ่งที่เราป้องกันไม่ได้และมักจะเป็นที่มาของ security breach
- ใน Internet Security นั้นแม้เราหาจะป้องกันแค่ไหน ที่ต้องยอมรับว่า risk ก็ยังมีอยู่เพียงแต่ชั้นการป้องกันที่มากขึ้นย่อมทำให้ risk นั่นลดลง

Countermeasures Paring is Enough?



Need to Anticipate Future Use (and Abuse) Cases



...and energy theft

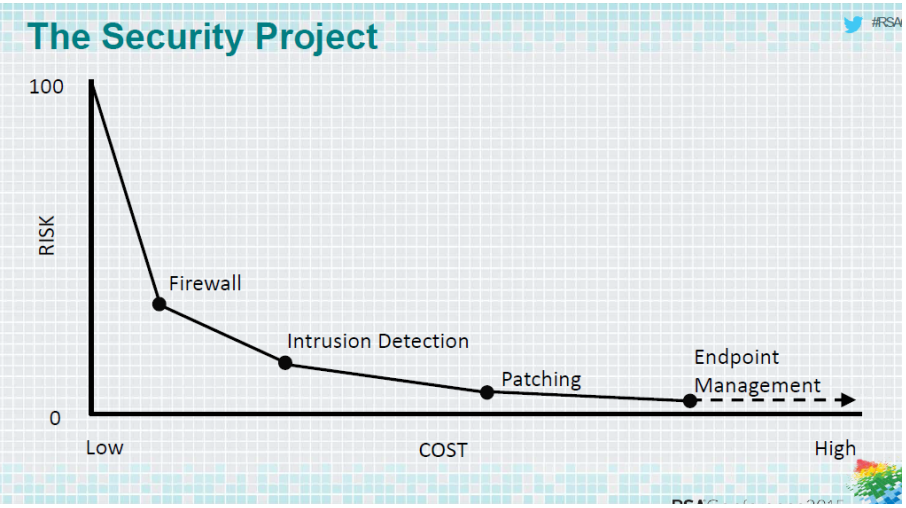
Home automation
... and stalking

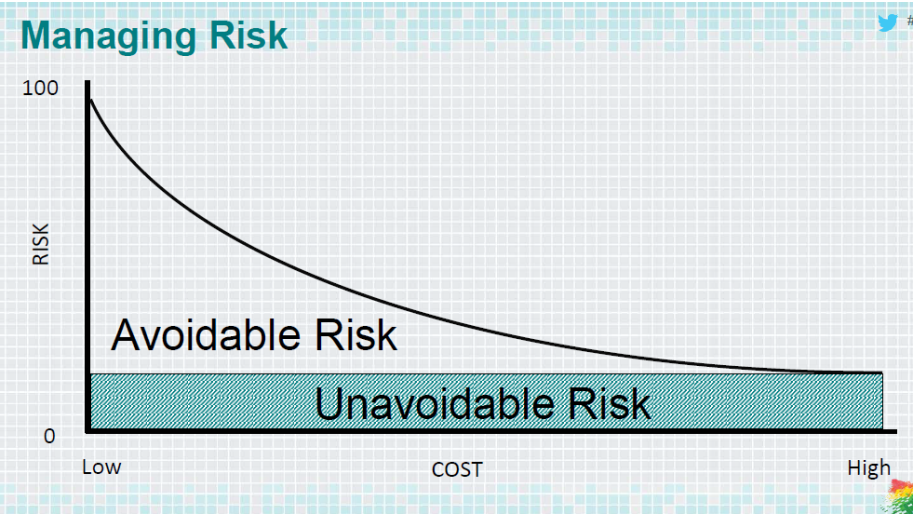
Vehicle to vehicle communication
.... and road rage hacking

Risk Management

ความซับซ้อนของการป้องกันที่มากย่อมทำให้ Risk นั้นลดลง (ซึ่งจะตามมาด้วยค่าใช้จ่ายด้วย) แต่อย่างไรก็ดี risk นั้นก็จะไม่มีทางลดลงจนถึง 0 ดังนั้นการประเมินความเสี่ยงยอมต้องแบ่งออกเป็น 2 ประเภท คือ

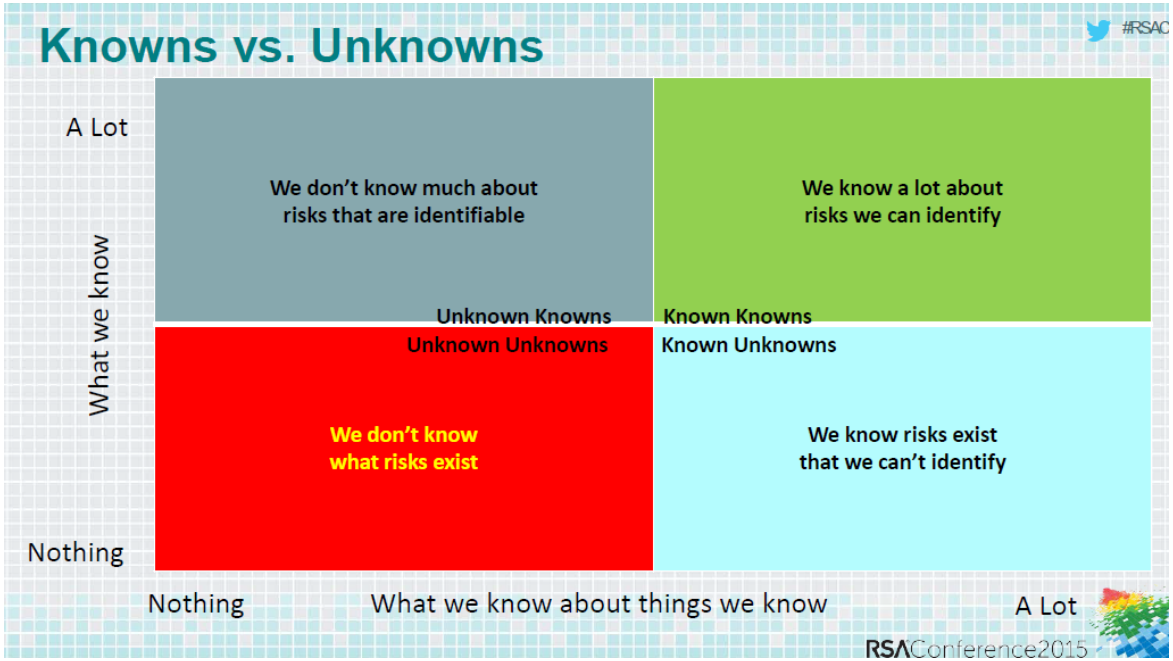
- Avoidable Risk (ป้องกันได้)
- Unavoidable Risk (ป้องกันไม่ได้ หรือองค์กรอาจจะไม่รู้ด้วยซ้ำ ว่ามี Risk อันนี้อยู่)





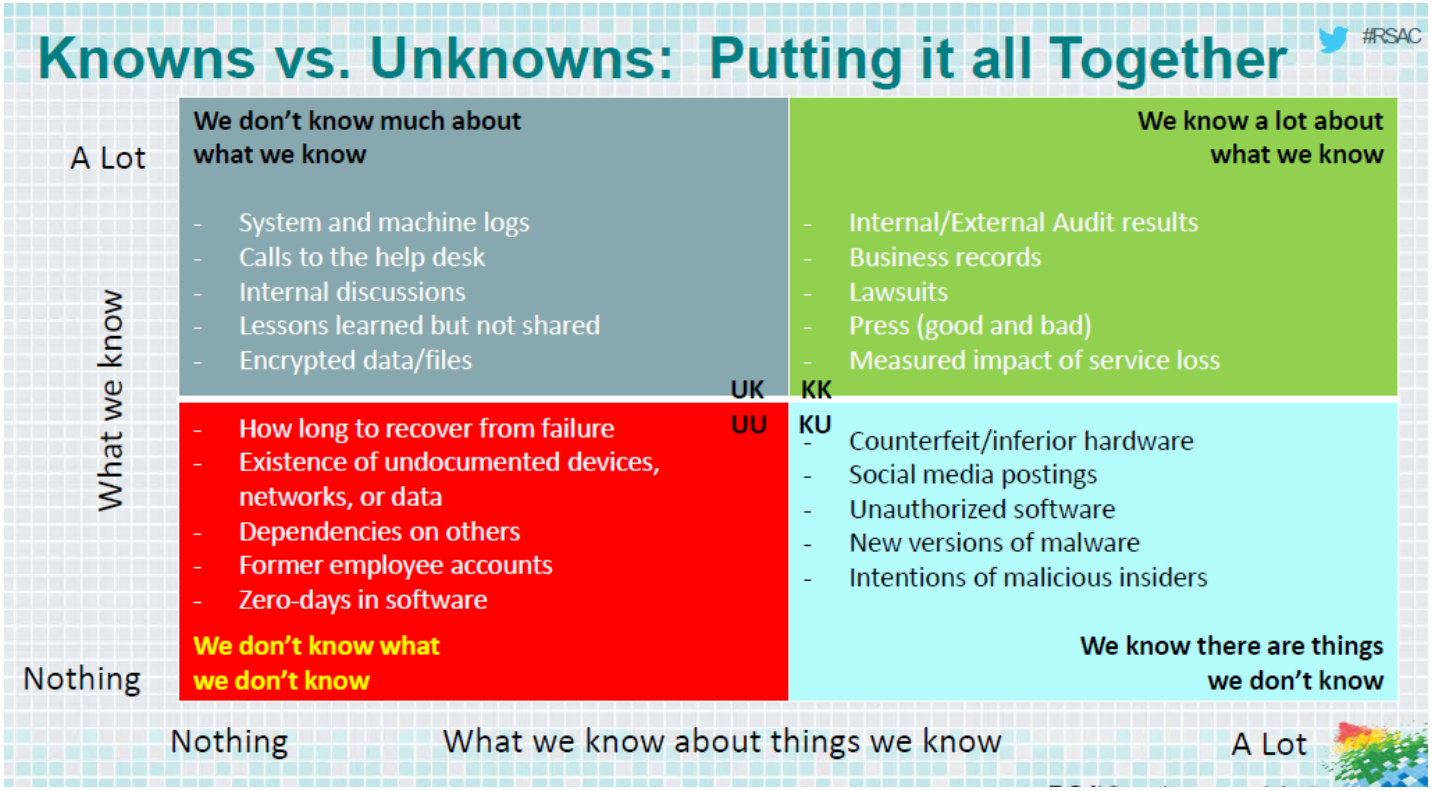
Risk Categories

- หากมองภาพรวมแล้วจะพบว่า Risk น่าจะแบ่งเป็น 4 Quadrant คร่าวๆคือ
  - Risk ที่เราระบุได้แต่ยังหาทางป้องกันได้ไม่ดีนัก
  - Risk ที่เราระบุได้และสามารถป้องกันได้
  - Risk ที่เราไม่สามารถระบุได้แต่ตระหนักว่ามีอยู่
  - Risk ที่เราไม่สามารถระบุได้และไม่ตระหนักด้วยมีอยู่

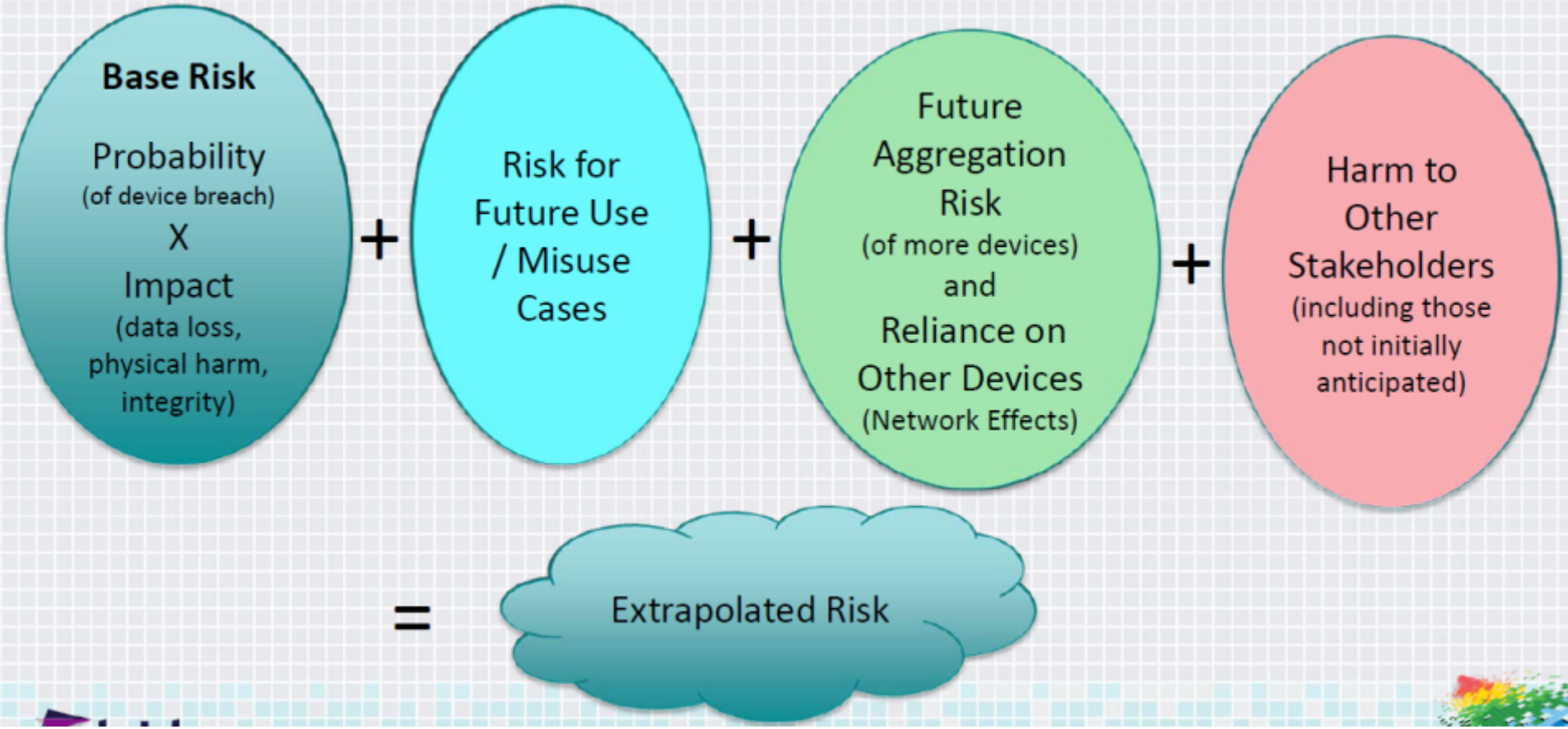


Challenges

- สิ่งอันตรายที่สุดคือ quadrant ที่ 3 (What don't know what risks exists) โดยเราต้องพยามให้องค์กรเคลื่อนไปยัง quadrant ที่ 2 (we know a lot about risks we can identify)



Internet of Things Risk Formula



Lessons Learned

- วิธีแก้ไขโดยหลักการคือการ focus ในสิ่งที่เรารู้อยู่แล้วและพยายามขยายจากจุดนั้นออกไปมากขึ้น
  - A monthly incident report (basic เพียงในเชิง quantitative เท่านั้น)
  - Quarterly statement of risk (update risk ที่ค้นพบใหม่ๆ)
  - Monthly vulnerability report
  - Monthly exception report
  - Access review summary (จาก logต่างๆ เพื่อนำมาวิเคาะห์หาความเสี่ยง)

LEGAL ISSUES

Privacy issues

- ด้วยการที่มีเทคโนโลยีใหม่ๆ ก็จำเป็นต้องมีการพัฒนากฎหมายเพื่อให้รองรับเทคโนโลยีนั้นๆ นอกจากนี้เรื่องของเทคโนโลยีใหม่ๆ ก็ไม่ได้จำกัดวงเฉพาะเรื่องภายในประเทศเท่านั้น ส่วนใหญ่จะเกี่ยวข้องกับต่างประเทศ ซึ่งแต่ละประเทศก็มีเขตอำนาจศาลภายใต้กรอบอำนาจอธิปไตยของตัวเอง และกฎหมายที่แต่ละประเทศใช้บังคับอยู่ก็มีความแตกต่างกัน จึงทำให้เกิดปัญหาในการประสานหรือร้องขอข้อมูลกัน เป็นต้น
- การคุ้มครองข้อมูลส่วนบุคคลของ EU นั้นเข้มงวดมาก ซึ่ง US ประสบปัญหาในการร้องขอพยานบุคคล/เอกสาร/วัตถุ จากประเทศในกลุ่ม EU ซึ่งใช้กฎนี้เป็น immunity ถึง 28 ประเทศ นอกจากนี้ยังต้องวิเคราะห์ว่าเป็นข้อมูลประเภทใดที่มีการเรียกเข้ามาเป็นพยานหลักฐาน เช่น หากไม่เป็นข้อมูล PII ก็ไม่มีปัญหา เพราะไม่เป็นข้อมูลที่ sensitive นอกจากนี้ยังต้องประเมินบุคคลที่เกี่ยวข้องด้วย
  - ได้มีการเสนอ case ที่ดำเนินการสำเร็จ คือ กระทรวงการคลังสหรัฐอเมริกาขอให้อีเบย์ในแคนาดาส่งข้อมูล เพราะเซิฟเวอร์เก็บข้อมูลอยู่ในแคนาดา
  - ในการร้องขอให้ส่งพยานหลักฐานที่ได้รับการคุ้มครองภายใต้ EU Legal Framework อาจมีการ negotiate กับประเทศที่เกี่ยวข้อง ว่าจะดำเนินการกับข้อมูลในแนวทางที่ไม่เปิดเผยและดำเนินการด้วยความระมัดระวัง

VISITING GOOGLE AND MICROSOFT

Google and Microsoft