

Predicting the future
is easy ... getting it right is the
hard part. Version 2015.0





Introductie



- Ir.drs. J. van der Vlugt RE CISA CRISC CCX RCX
- Jurgen
- Maverisk Consultancy, IS Audit & Advisory services
- ICC Audit/Advies
- Blogblogblog – maverisk.wordpress.com
- ERM/ORM, (IS) Audit, (Info)Security

Gaarne discussie ..!



(Agenda)



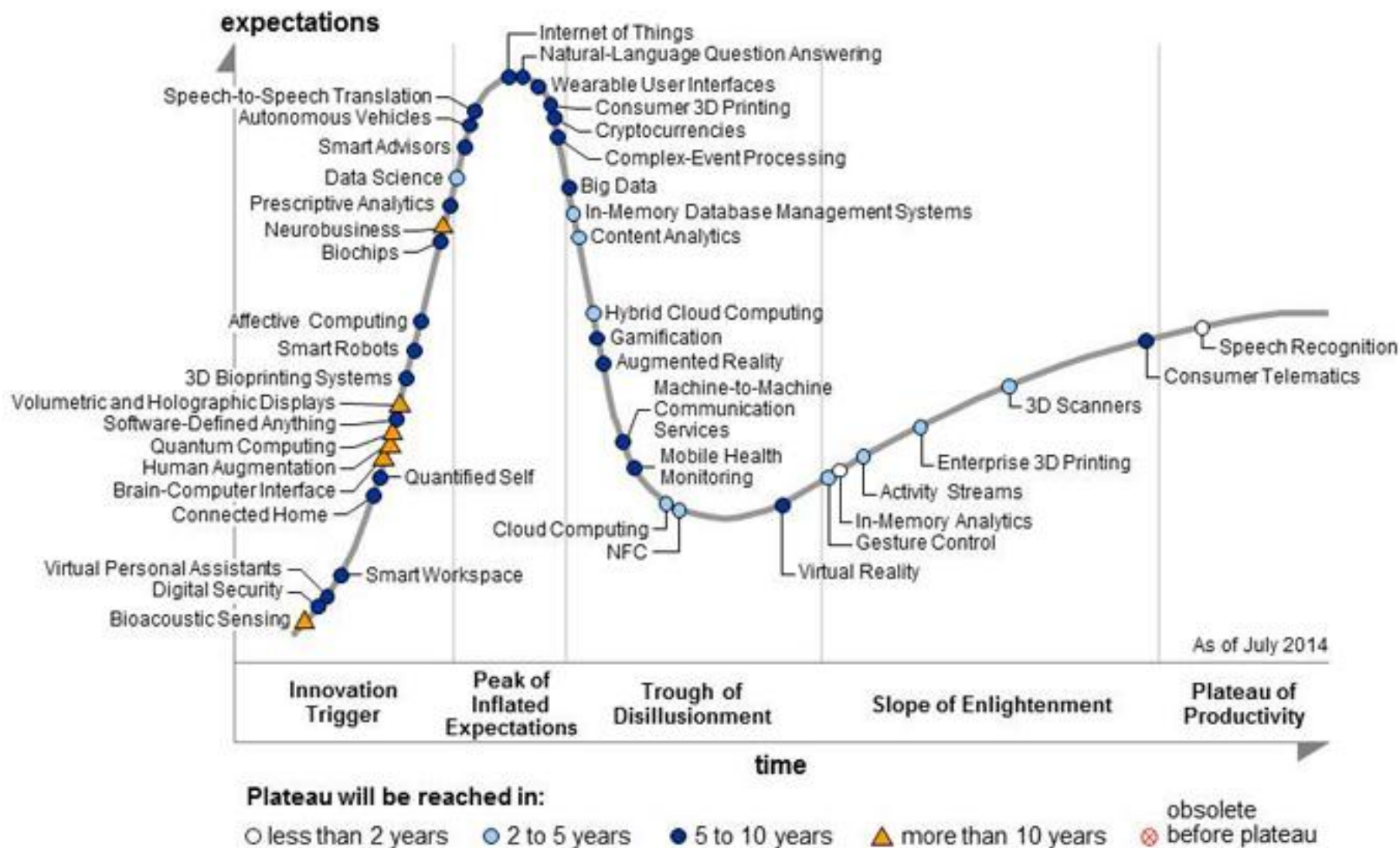
1. Terugblik
2. Governance
3. Business
4. IoT(A)
5. AI
6. ITSec
7. InfoSec
8. Conspectus

Terugblik



- Trust
 - Identity
 - Things
 - Social
 - Mobile
 - Analytics
 - Cloud
 - Demise of ERP
 - InfoSec
 - APTs
 - Certificaatkwestbaarheden
 - Crypto-breuken
 - Quantum Computing
 - New methodologies
 - Deflation of TLD
- ☒ Loopt door
 - ☒ Hoewel... Bitcoin et al! ☒
 - ☒ IoT ...
 - ☒ WhatsApp / Telegram / Ello / Viv / ...
 - ☒ Mehhh
 - ☒ → 'smart' / mensenwerk
 - ☒ Mehhh
 - ☒ Beetje uit-de-cloud, verder niks
 - ☒ Sony. En vele andere!
 - (☒)
 - ☒ NSA m.n.
 - ☒
 - ☒ OSSTMM
 - ☒ Gelukkig wel (BoE, Forbes, et al)

Cycle



End of Hipster

TRILBY



FEDORA



Governance

Governance



naar binnen gekeerde cultuur. In het provinciehuis zijn ambtenaren en politici elkaar al geruime tijd aan het feliciteren met de formidabele manier waarop zij werken. Woensdagochtend hielden ze er maar weer eens een bijeenkomst over. Of dat tot betere plannen leidt, maakt niet uit. Het provinciehuis is in handen gevallen van procesmanagers en consultants.

Het is dezelfde cultuur waarin het streven naar meer groene energie vooral betekent dat eindeloos veel discussiebijeenkomsten en congressen worden georganiseerd. Tot de productie van meer groene energie leidt dat nauwelijks. Niettemin heerst er grote tevredenheid.

“GRC”

THE DINOSAUR MUSEUM

DORCHESTER

WORLD HERITAGE MUSEUMS ▾

OPEN EVERY DAY 7 DAYS A WEEK

10.00am – 5.00pm (winter hours: 10.00am – 4pm)

[HOME](#) [VISITING US ▾](#) [SCHOOLS & GROUPS ▾](#) [SPECIAL EVENTS](#) [LEARN & PLAY ▾](#) [LATEST NEWS](#) [BUY TICKETS](#) [SHOP](#) [CONTACT US](#)



EXPLORE THE MUSEUM



▶ [MORE INFORMATION](#)

SAVE MONEY ON TICKETS

DOWNLOAD THIS VOUCHER

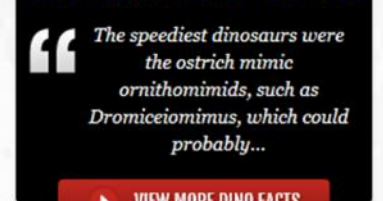
▶ [MORE INFORMATION](#)

DINOSAUR SHOP



▶ [MORE INFORMATION](#)

DID YOU KNOW THAT...



▶ [VIEW MORE DINO FACTS](#)



- SOx ↓
- “PDCA” ↓
 - Quod non!
 - Alles tegelijk
- Audit industry ↓
- Risk Analysis ↓
 - Quod non
 - Brugklas:

BRAUN OR APPLE?

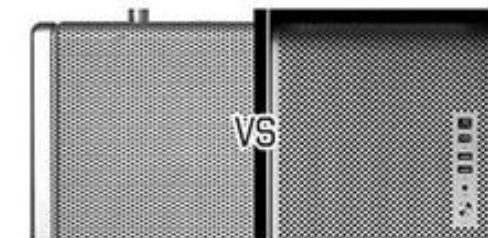
BRAUN T3 POCKET RADIO
(1959)

APPLE IPOD
(2001)



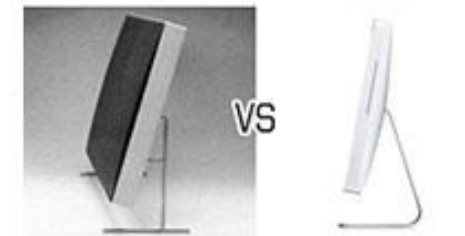
BRAUN T1000 RADIO
(1967)

POWERMAC GS/MAC PRO.
(2003)



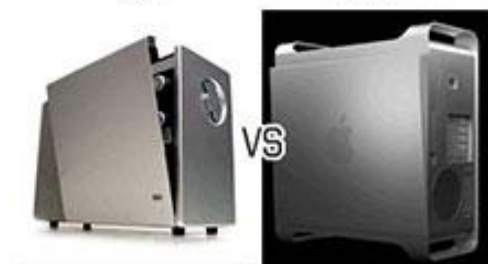
BRAUN LE1 SPEAKER
(1959)

APPLE IMAC
(2007)



BRAUN T1000 RADIO
(1967)

POWERMAC GS/MAC PRO
(2003)



Brugklas



‘GRC’ in 2015 (I)

- “...we hebben hier geen regels; we proberen wat te bereiken!”
- ‘Disruption’
Kaizen .. verbeterstapjes .. upgrade .. innovatie .. Disruptie



The infographic compares a flip phone (left) and a smartphone (right) across various metrics. The title 'CELL PHONES BEFORE & NOW' is centered at the top. The comparison table is as follows:

	Before (Flip Phone)	Now (Smartphone)
Battery life	3-4 days	3-4 hours
Impact limit	third floor (asphalt)	2 feet (hardwood floors)
Impact protection	Built-in	Needs add-ons
Software updates	Unnecessary	Approx. once a week
Life span	Still going	Max. 1-2 years
Typing speed	9 characters per second	Damn you autocorrect!

truthfacts.com

'GRC' in 2015 (II)

- Kippenhok / When the going gets tough, the Info(Sec) masters get going:
- ISO27001:2013, ISO15504(SPICE)
- OSSTMM (hopelijk)
- Risicoanalyse:
 - Doorbraak van Normaal Doen (hopelijk)
 - Be Prepared + Acceptatie

Business

Business

- Big IT
- IoT
- B2C 'Innovatie'
- (Hobbeltje InfoSec → ITSec)

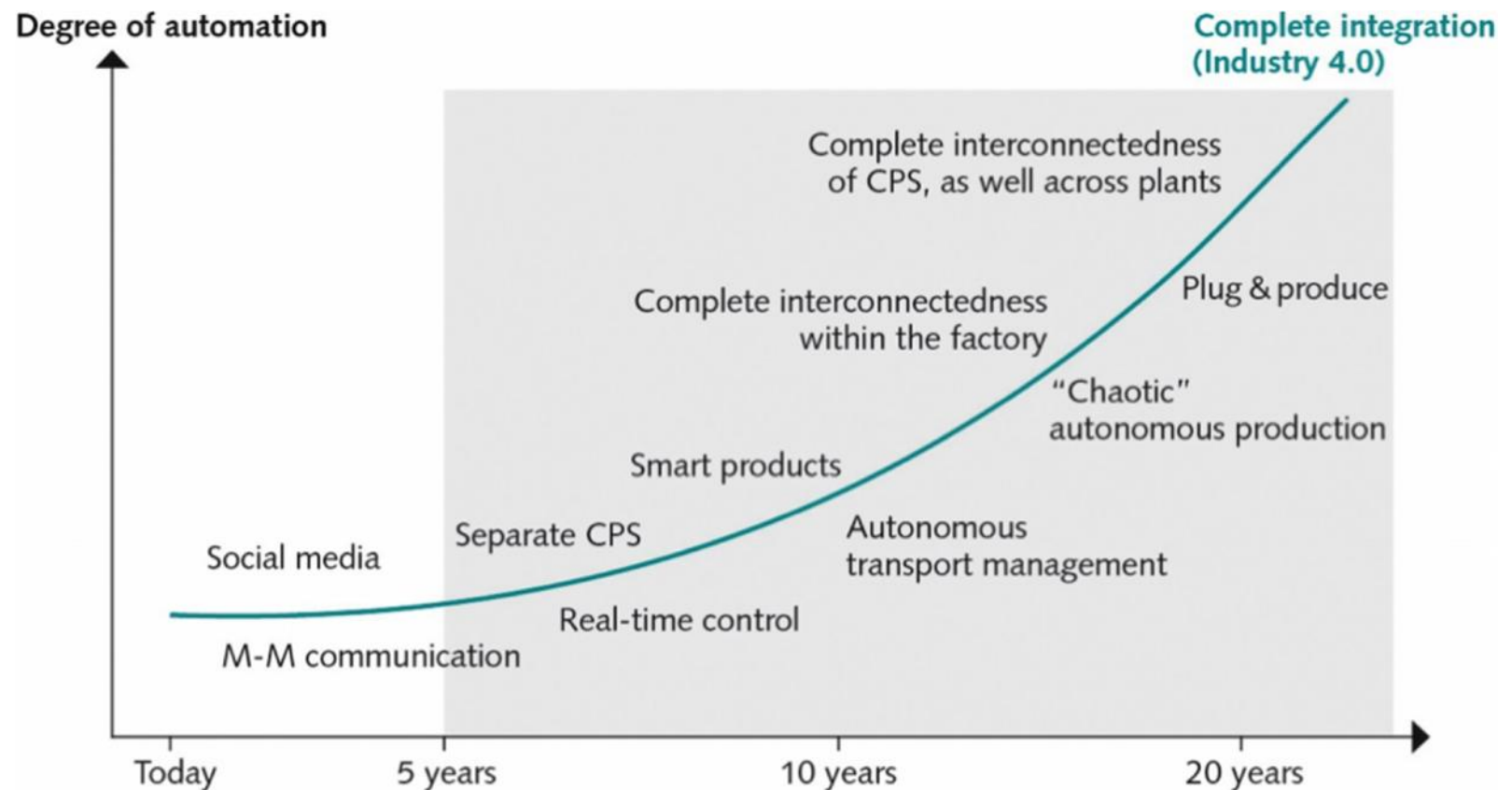
Business (Big IT 2015)



- Big Data segmentation
- Docker, Firebase
- e.v.a.
- SMACI(o)T
- (Google Docs, Klaut)

Business (IoT 2015)

- Convergence van APIs
- Stealth

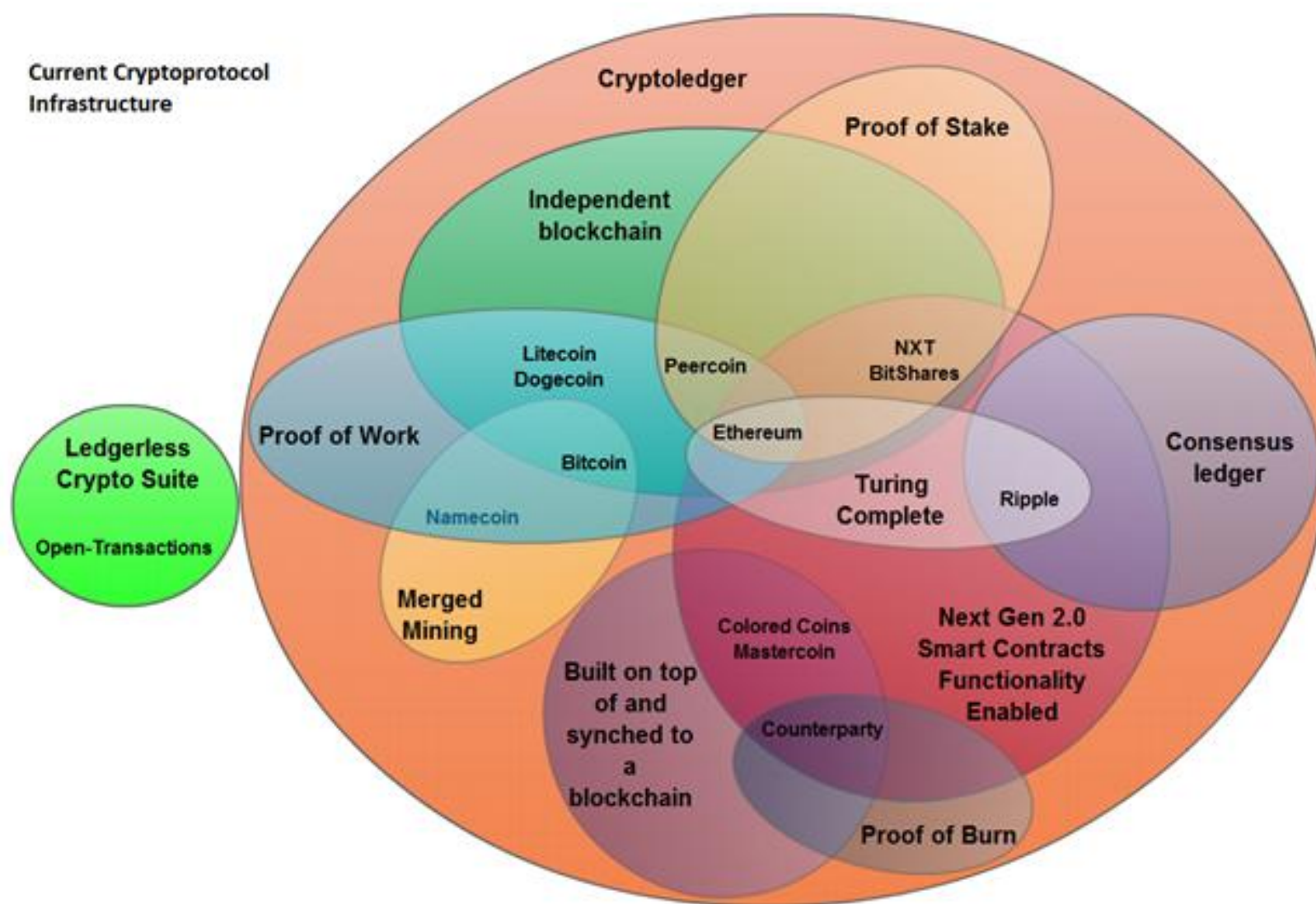


Nog wat B(2B, 2C)

- Bitcoin / Blockchain (onder water)
163 cryptocurrencies
- Webrooming → Showrooming
- Alibaba, Tencent, Baidu > Amazon+Ebay
- Mobile payments, NFC
- 3rd Platform / Fabric
- Drones
- Sharing Economy
- Virtual Reality ..?

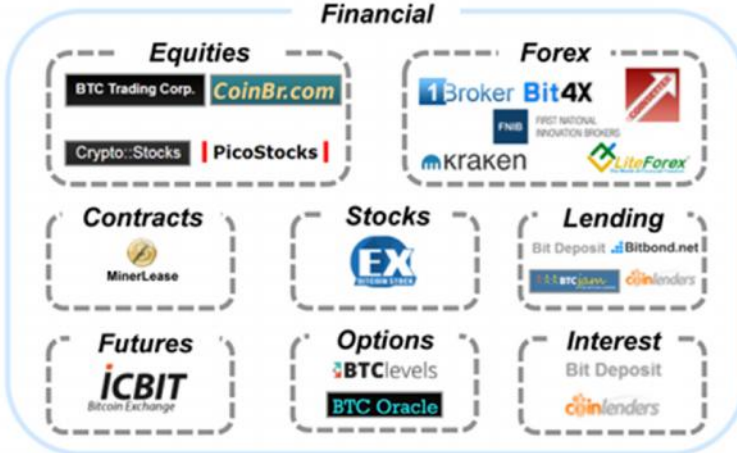


Blockchain trust



IT in business 2015 – finance

Financial



Payment Processing



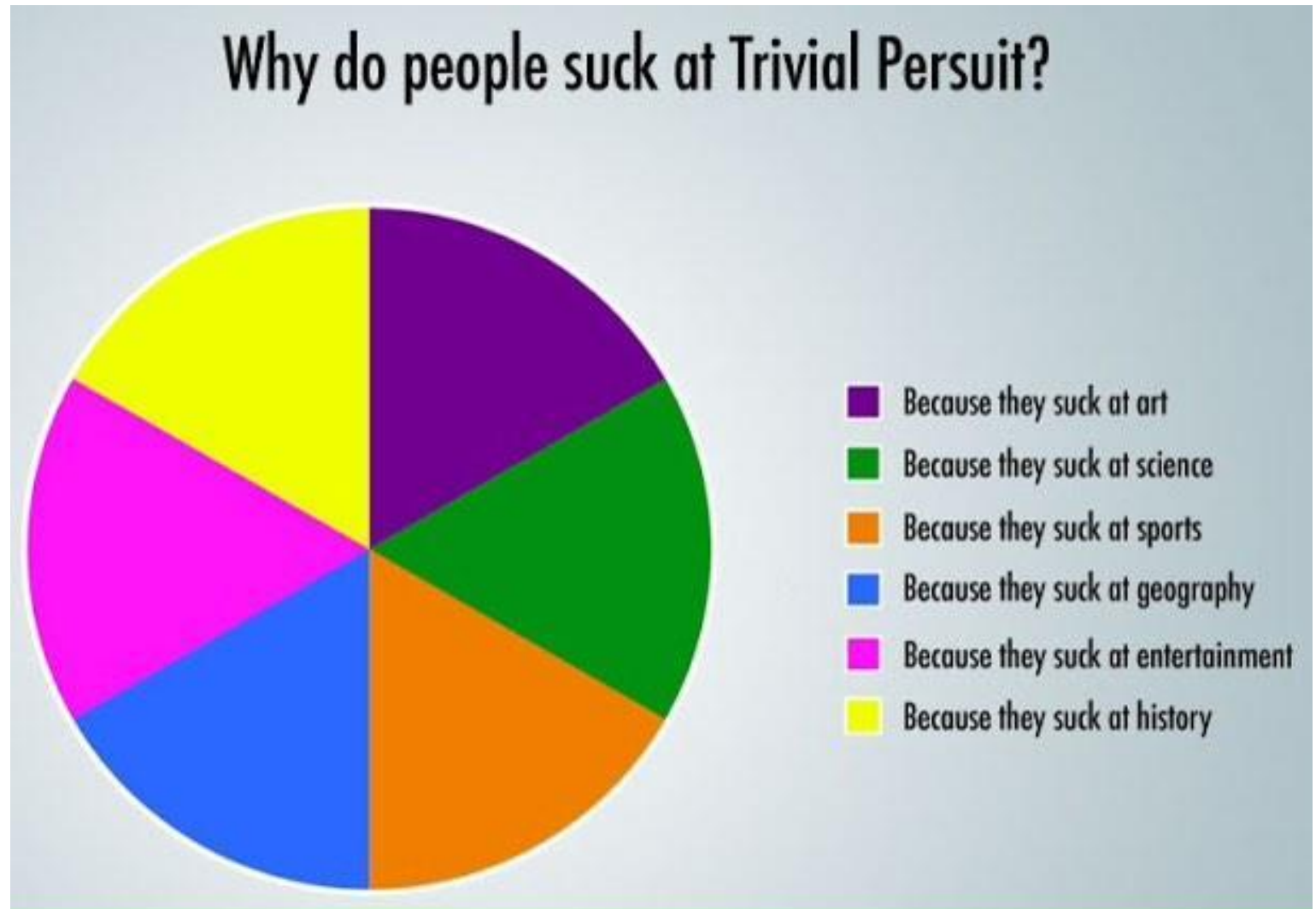
Banking & eWallets



Currency Exchanges



Business (B2C 'Innovatie' 2015)



IoT(A)

IoT(A) 2015

4 richtingen

- B-inhouse:
3D printing, robots, remote fabrieken
- C-inhouse:
Domotica (Nest e.v.a., setjes; alles-in-1),
Connected Cars
- B2B:
'SaaS', DACs?, groep/clubvorming.
Industrial Internet!
- B2C/C2B:
Smart Cities, lifelogging, wearables, tracking ..!

IoT(A)

The FTC Warns Internet Of Things Businesses To Bake In Privacy And Security

Posted 31 seconds ago by [Natasha Lomas \(@riptari\)](#)



The FTC has raised concerns about the complexity and privacy risks posed by the rise of an Internet of Things, with some 25 billion connected objects predicted to be online in 2015, and so-called smart home devices predicted to number around 25 million this year.

ADVERTISEMENT



Latest News, Celeb
Weather, Travel and S

Visit AOL

TC NEWSLETTERS

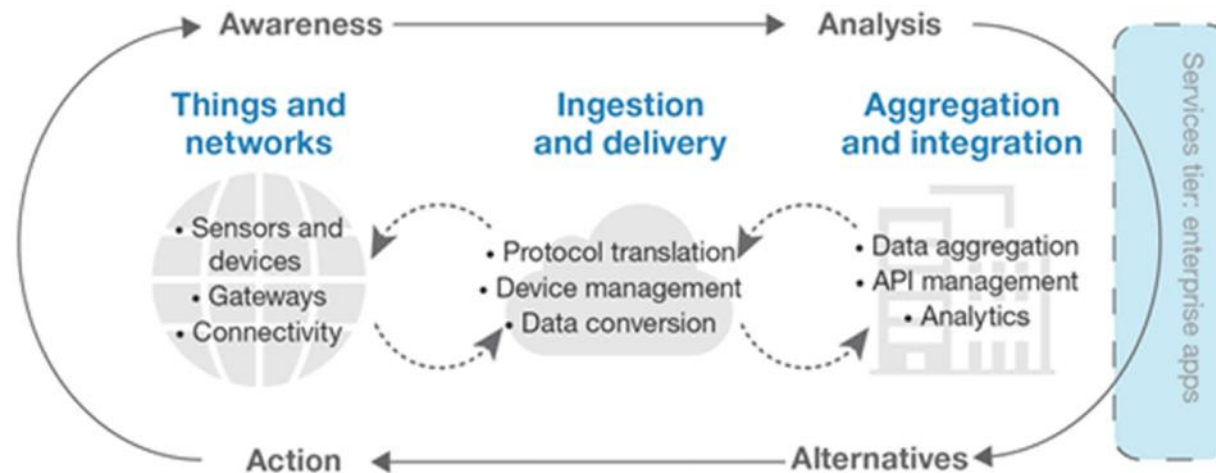
- ✓ **TechCrunch Daily** Top headl delivered daily
- ✓ **TC Week-in-Review** Most pr stories, delivered Sundays
- ✓ **CrunchBase Daily** Latest star fundings delivered daily

Security-boom →

Risico's (Stuxnet ↔ privacy) →

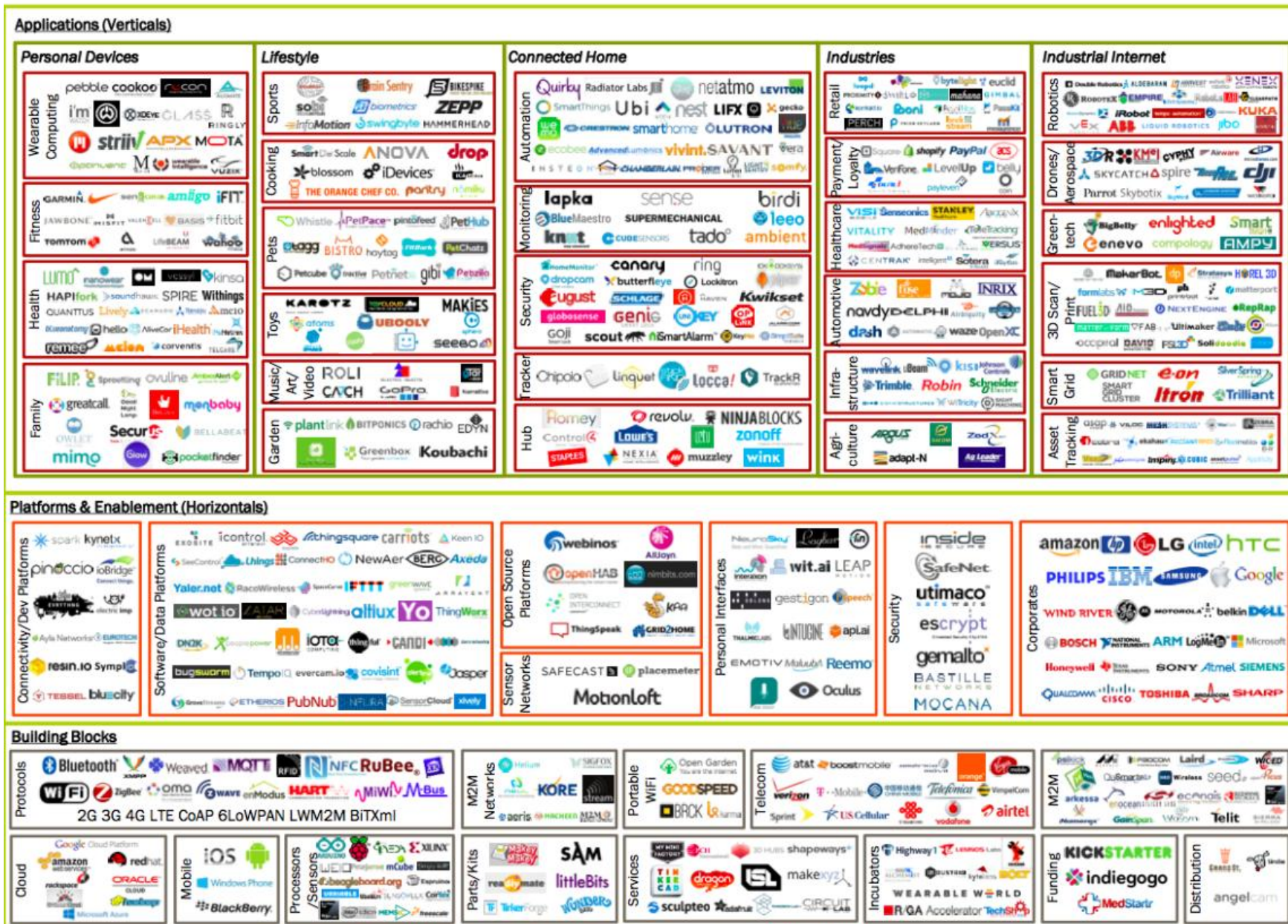
Auditprogramma's (Yours Truly)

Yours Truly (?)



	Things and networks	Ingestion and delivery	Aggregation and integration
Tech, protocols, and standards	Which short-range radio tech — ZigBee, Z-Wave, or others?	Use HTTP or IoT-specific standards such as MQTT or CoAP?	DIY API management or SaaS service?
Distributed data, analytics, and logic	Which programming language for proprietary edge devices?	How to extract and coordinate logic running in IoT platform?	How to document dependencies on third-party data?
New security challenges	How to ensure immutable device state?	How to prevent data monitoring by hackers?	How to guard against API hacking or denial of service?
New network demands	How to enable IoT on-site while guarding core network?	How to enable mix of high volume streaming and low latency?	How to monitor and protect with many partners and services?
Time series demand	Filter at edge, or transmit raw data in volume	Capture as time series or as event?	How to store so it's easy to transform as needed?

To watch



© Matt Turck (@mattturck), David Rogg (@davidjrogg) & FirstMark Capital (@firstmarkcap) FIRSTMARK

AI

AI



M|Δ®|{• |— Ø%û5 ✓
@markhoppus

True story. I'm flying right now but through wifi and an app on my phone I'm honking the horn on my car back home to annoy my family.

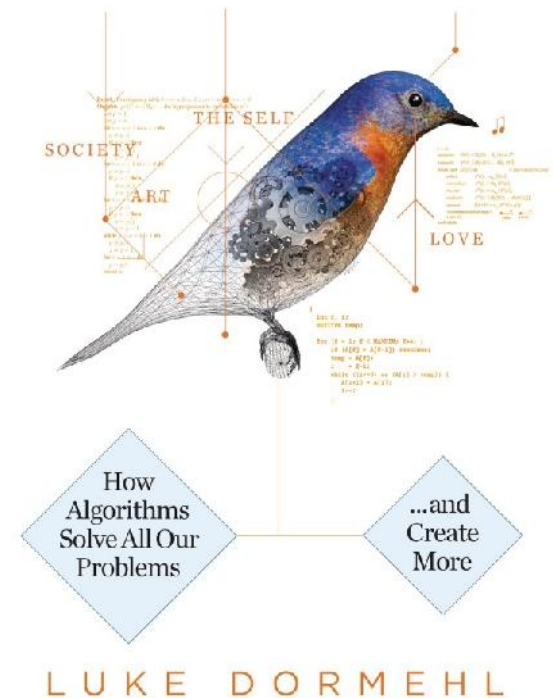
- Ethiek
 - Trolley problem
 - Vertrouwen/Singularity
- Veel AI-‘plugins’
 - [visual|speech]-naar-[tekst|interpretatie]-naar-[informatie|handeling]
 - Losse ideetjes t/m API-achtige tools
- Onder water: Nog veel meer

Reeds

"This important book deserves to be read, and digested, by all who wrestle with, and enjoy—or worry about—a world transformed by digital technology."

—KEN AULETTA, author of *GOOGLED*

The Formula



“The RMV itself was unsympathetic, claiming that it was the *accused individual's 'burden' to clear his or her name in the event of any mistakes*, and arguing that the pros of protecting the public far outweighed the inconvenience to the wrongly targeted few.”

Sluipend



Venture Capital Firm Appoints Machine Intelligence As Board Member



George Dvorsky

Filed to: FUTURISM 5/15/14 7:30am

26,884 🔥 6 ★



1

Hong Kong based venture capital firm Deep Knowledge Ventures (DKV) has appointed a machine learning program to its board. Called VITAL, it's an "equal member" that will uncover trends "not immediately obvious to humans" in order to make investment recommendations.

This is probably an attempt to attract media attention, but it could truly be the start of a larger trend; it's the world's first software program to be appointed as a board member. The move could also herald a new direction in the way venture capital is done.

The tool was developed by Aging Analytics UK who's licensing it out to DKV, a capital fund that focuses on companies developing therapies for age-related diseases and regenerative medicine.

And so it begins...

ITSec

ITSec

- Poodle, Beast, Heartbleed → Open Source ?
- Encryptie-by-default; Diaspora*, TORbrowser, PGP
- OSSTMM / ISO27k1:2013
- IoT Security / Audit → IAM ? / Analyse ?
- APTs

Droom (wiegeliedje?)



And so it begins...

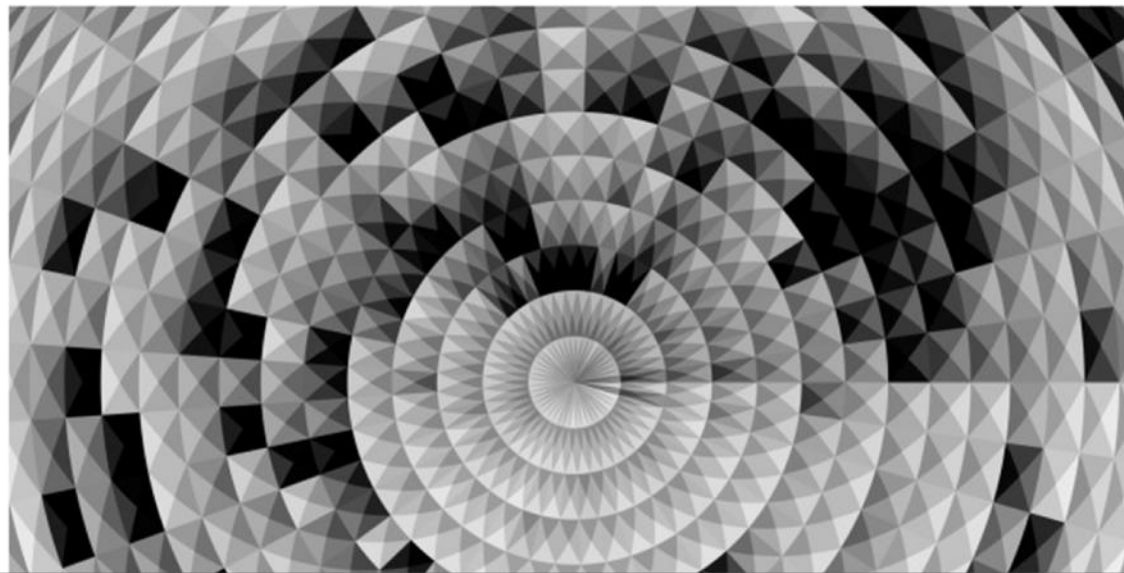


THREAT LEVEL | german steel mill | icymi | Sony | stuxnet | FOL

A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever

BY KIM ZETTER 01.08.15 | 5:30 AM | PERMALINK

[f Share](#) 46 [t Tweet](#) 306 [g+1](#) 10 [in Share](#) 27 [Pin it](#)



Van Vroeger Was Alles Beter naar Mordor

Dader \ Target	Individu	Gang	Organisatie	Land
	Individu	Gang	Organisatie	Land
Individu	Meh.	Ehhh	'Hacker'	'Hacker'
Gang	Meh.	Ah!	'Hacker'	'Hacker' / Defacing / Ideology driven
Organisatie	Meh. / Defacing de klokkenluider?	Infiltratie	APT's / Spionage	APT's / Spionage
Land	Meh. / Snowden	Politiewerk	APT's / Intel-werk	APT's / Spionage

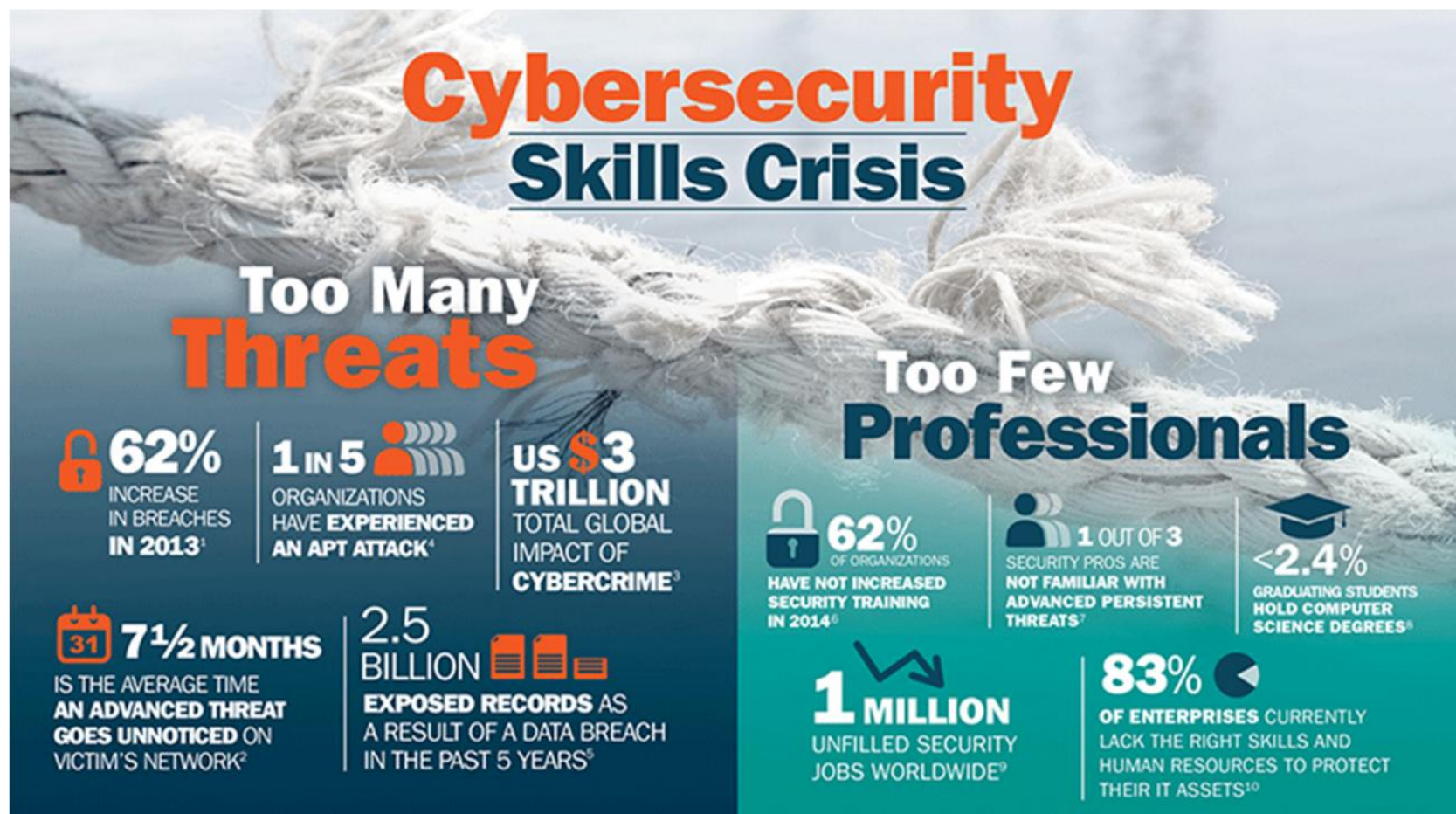
ITSec: into the hardcore mosh pit



Alle details doen ertoe

Threat	Target	Individual			Gang			Organisation			Country		
		Script kiddie	Loose cannon	Long-horizon activist	Loose, ad-hoc, bragging-motivated	Organised, Dispersed, Resilient	Business-oriented	Business	Interest group	State-backed	Rogue	Sophisticated, closed	Sophisticated, many-faceted
Individual	Script kiddie	LOLz	Calimero	Fly to be swatted	Fly to be swatted	Fly to be swatted	Fly to be swatted	Embarrasing nuisance	Embarrasing nuisance	Embarrasing nuisance	Danger's on you	Danger's on you	Danger's on you
	Loose cannon	Swat the fly	Battle of wits	<Undetermined>	<Undetermined>	Bets on the defence	Bets on the defence	Serious BCM needed	Serious BCM needed	Fly to be swatted	Fly to be swatted	Fly to be swatted	Fly to be swatted
	Long-horizon activist	Swat the fly	Battle of wits	<Undetermined>	War of attrition	War of attrition	War of attrition	BCM critical	BCM critical	War of attrition	<Undetermined>	Fly to be swatted	Fly to be swatted
Gang	Loose, ad-hoc, bragging-motivated	Swat the fly	Swat the fly	War of attrition	War of attrition	War of attrition	War of attrition	Serious BCM needed	Serious BCM needed	Fly to be swatted	Fly to be swatted	Fly to be swatted	Fly to be swatted
	Organised, Dispersed, Resilient	Swat the fly	Swat the fly	War of attrition	War of attrition	War of attrition	War of attrition	BCM critical	BCM critical	BCM critical	<Undetermined>	<Undetermined>	<Undetermined>
	Business-oriented	Swat the fly	Swat the fly	War of attrition	War of attrition	War of attrition	War of attrition	BCM critical	BCM critical	Serious BCM needed	War of attrition	War of attrition	War of attrition
Organisation	Business	Swat the fly	Battle of wits	Strike-back may be successful	Strike-back may be successful	Bets on the defence	Bets on the defence	<Undetermined>	<Undetermined>	Bets on the defence	No chance	No chance	No chance
	Interest group	Swat the fly	Battle of wits	Strike-back may be successful	Bets on the defence	Bets on the defence	Bets on the defence	Serious BCM needed	BCM critical	<Undetermined>	Bets on the defence	No chance	No chance
	State-backed	Swat the fly	Swat the fly	Strike-back may be successful	Strike-back bets on the offensive	Strike-back bets on the offensive	Strike-back bets on the offensive	BCM critical	BCM critical	<Undetermined>	<Undetermined>	<Undetermined>	<Undetermined>
Country	Rogue	Swat the fly (pathetic variant)	Swat the fly (pathetic variant)	Bets on the defence (w/gov't help)	Swat the fly (pathetic variant)	<Undetermined>	<Undetermined>	BCM critical	Swat the fly (pathetic variant)	<Undetermined>	<Undetermined>	<Undetermined>	<Undetermined>
	Sophisticated, closed	Swat the fly (pathetic variant)	Swat the fly (pathetic variant)	Swat the fly (pathetic variant)	Swat the fly	Swat the fly (hard effort)	Swat the fly (hard effort)	BCM critical	Swat the fly (pathetic variant)	<Undetermined>	<Undetermined>	<Undetermined>	<Undetermined>
	Sophisticated, many-faceted	Swat the fly (pathetic variant)	Swat the fly (pathetic variant)	Swat the fly (pathetic variant)	Swat the fly (pathetic variant)	Swat the fly (hard effort)	Swat the fly (hard effort)	Swat the fly (pathetic variant)	Swat the fly (pathetic variant)	<Undetermined>	<Undetermined>	<Undetermined>	<Undetermined>

Armageddon...! ..?

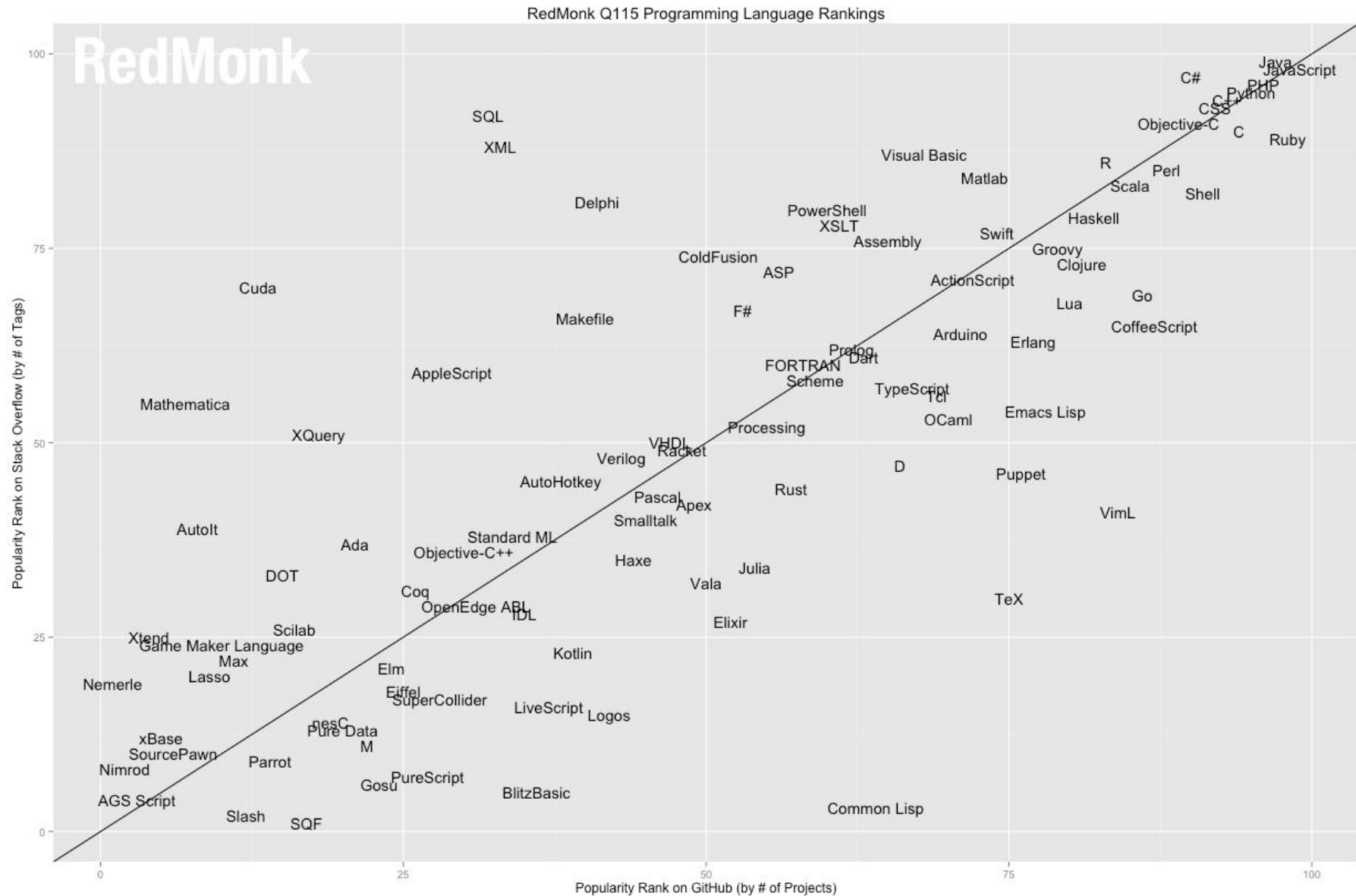


Enterprises are under siege from **a rising volume of cyberattacks.**

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. 2014 Internet Security Threat Report, Volume 19, Symantec, April 2014; 2. M-Trends 2014: Attack the Security Gap, Mandiant, April 2014; 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. An Executive's Guide to 2013 Data Breach Trends, Risk Based Security/Open Security Foundation, February 2014; 6. ISACA's 2014 APT Study, ISACA, April 2014; 7. ISACA's 2014 APT Study, ISACA, April 2014; 8. Code.org, February 2014; 9. 2014 Cisco Annual Security Report, Cisco, January 2014; 10. Cybersecurity Skills Haves and Have Nots, ESG, March 2014

L33t Skillz



InfoSec

InfoSec



- Info → Risico's →
All-in oplossingencomplexen + restrisico's!
- Kwetsbaarheden overal
 - 3rd parties
 - Open Source
 - Shadow IT, BYOD/CYOD
 - Complexiteit, veranderlijkheid
- (Mosh pit wordt de New Normal)

Doe iets!

"So many sit idle, thinking their self-assured mastery of computer and network will save them from the ills ahead.

I ask you, those in the audience today: What shielding does an intimate understanding of fission provide against the radiance of a nuclear blast?"

- Taylor Swift



Buiten de deur (?)



- Altijd-waakzaam publiek
 - Van socmed naar messaging
 - Snapchat, Telegram voorbij
 - Ello, Viv, YikYak, Tsu, Whisper, Kik, WeChat, Line, Viber, surespot, Whicker, Treema, KakaoTalk, Nimbuzz, Tango, MessageMe, Slack, HipChat, Peerio, Wizters, Secret, The Insider, Awkward, Cloaq, Chrends, Dropon ...
- Privacy ... (by design) (Q1, Q2)
- Blockchain trust

- Nation-state attacks ☒
- Extortion ☒
- Data destruction ☒
- Bank card breaches continue ☒
- 3rd party breaches ☒
- Critical infra ☒

Conspectus

- ✓ Terugblik
- ✓ Governance: Meh hh
- ✓ Business: As usual; fin-disruption
- ✓ IoT(A): Domotica, Ccars, ++
- ✓ AI: Tooltjes, ++
- ✓ ITSec: Hardcore strijd
- ✓ InfoSec: Alles tegelijk / privacy
- ✓ Conspectus: (Rekursie)

Wammoedikkermeej?

- Be a lert. The world needs more lerts.
 1. Voor uzelf
 2. Voor uw werkgever(s)
- Door met reeds ingezette verbeteringen
- Maar:
 - Oude plannen bijbuigen
 - Nieuwe plannen: 'Open' voor toekomst
- Spread The Word



Recommended Reading





Thank you



HTTP status 418 Contact details

- Jvdvlugt@maverisk.nl
- @jvdvlugt
- Maverisk.wordpress.com
- <http://nl.linkedin.com/in/jurgenvandervlugt/>
- (G+, etc.etc.)

