

February 13, 2017

Digital Challenges & Opportunities

E&M Magazine – Launch Event

Rafael Maman
Partner, PwC Israel



<http://www.pwc.com/il>

About PwC

PwC in Numbers

\$35.9B Gross Revenues
223,468+ people

Advisory

\$11.5B
53,632+ people

Assurance

\$15.3B
98,326+ people

Tax

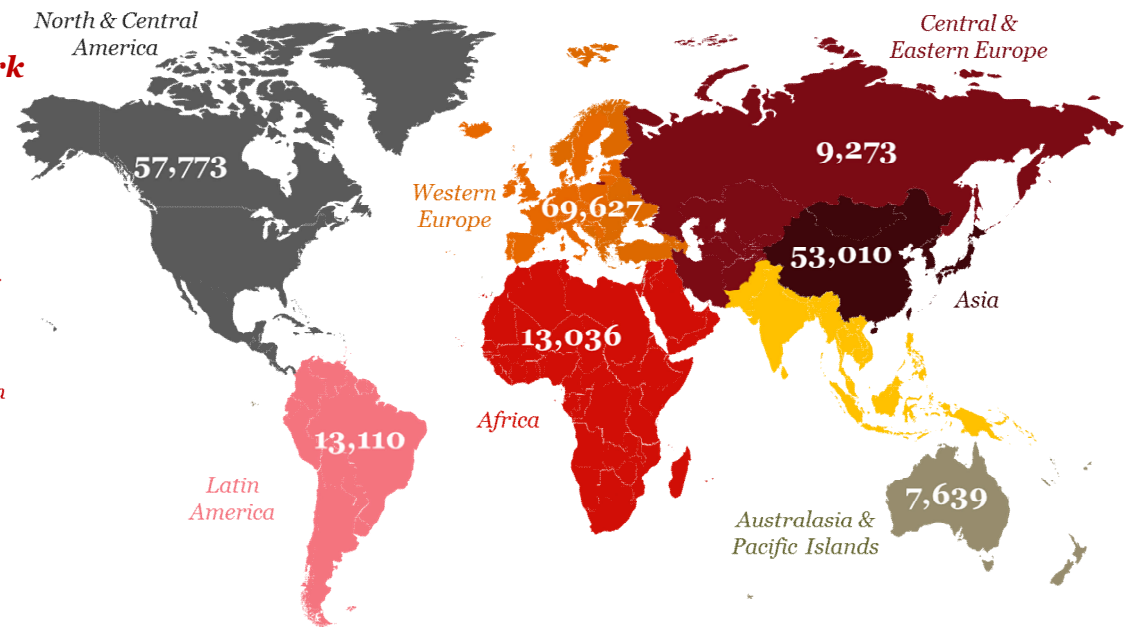
\$9.1B
44,694+ people

A Global Network

We are present in 157 countries across 743 locations. Our over 223,468 experienced experts across the globe will assist you in the world's growth markets.

With our local and regional teams we can provide a full suite of consulting services, from strategy to execution

**...with
profound
expertise**



No. 1
Advisory firm
IDC & Kennedy Information

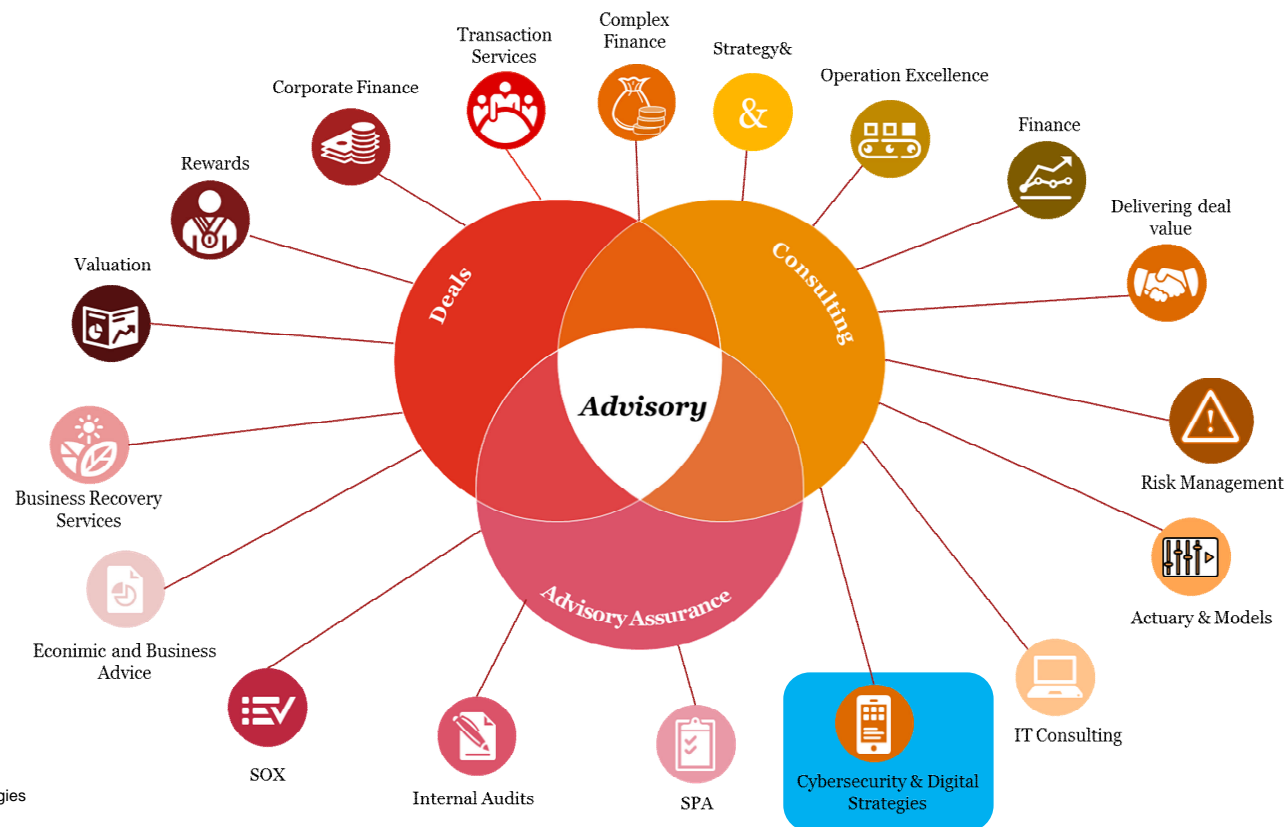
No. 1
For product & services launch operations
Kennedy Information

85%
Fortune Global 500 are PwC clients

1 out of the 8 nominated firms for the Kennedy Vanguard on Supply Chain
Kennedy Information

No. 1
M&A Advisor
Kennedy Information

About PwC Israel - Advisory





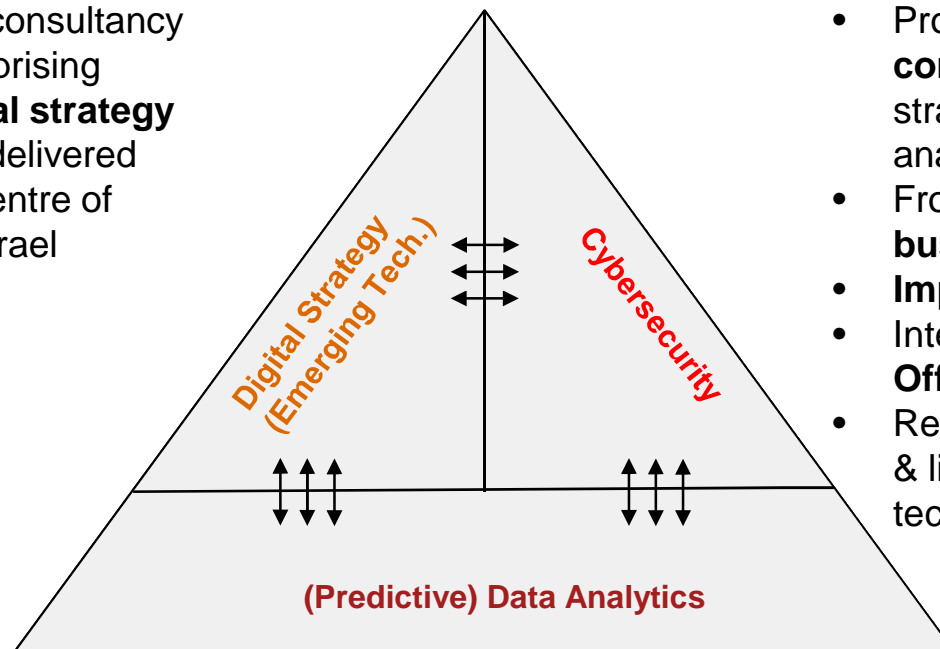
PwC

Cybersecurity & Digital Strategies

About PwC Israel – Cybersecurity & Digital Strategies

Our raison d'etre:

An integrated digital consultancy service offering, comprising **cybersecurity, digital strategy** and **data analytics**, delivered from a single DCS Centre of Excellence in PwC Israel



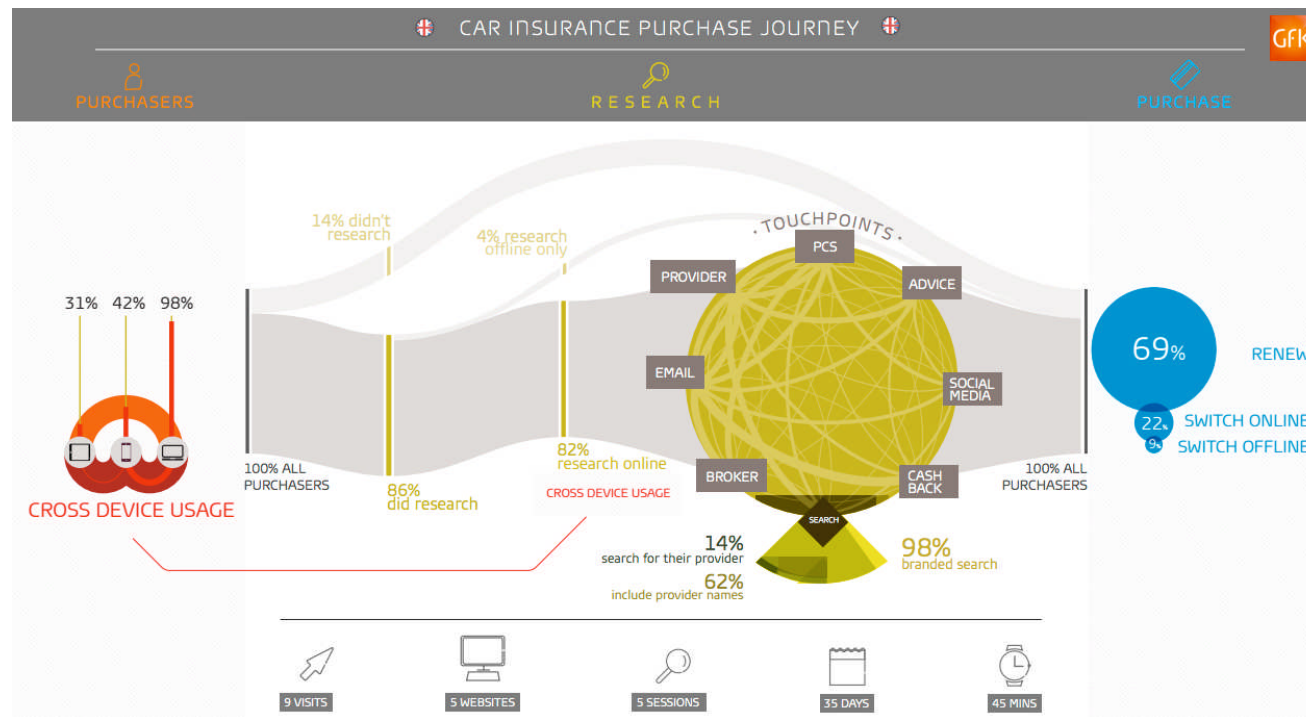
Objectives:

- Provide a world-class, **integrated consulting framework** for digital strategy, cybersecurity and data analytics to the modern enterprise
- From **strategy** development to **business transformation**
- **Impact Centre** in the PwC Network
- Integrated into the firm's **Global Offerings**
- Recognised **Centre of Excellence** & liaison to emerging digital technologies

Data Analytics

The Challenge: Move AI from the Drawing Board to Operations

Data Analytics – And Example from Long Time Ago (3-4 Years Ago...)



Data Analytics – Underpinnings & Forecast

- Current market-size, globally: \$420 billion (subscription + advertisement)
- 2017: milestone in digital advertising
 - **Digital spending will surpass that of TV**
- Move to **OTT** (Over The Top) subscription
 - 80% of US consumers subscribe to an OTT service
- New trends:
 - **Direct to Consumer, “fan-centric”**
 - From eyeballs x (subscriptions+ advertisement) to **fan-centric business**
- **Influencer Marketing** moves to centre-stage
 - Focus on individuals/groups rather than market



Artificial Intelligence

- Current trends and advances in data analytics identify applicable AI solutions as a way for:
 1. **Marketers** to target individuals in **Influencer Marketing** modus operandi
 2. **Consumers** to navigate in an increasingly complex world
- 2017 will be the year when AI will move **from the drawing board to operations**, in a big way
- This will mark a shift from advanced electronics applications, to **pinpoint analytics** that predict consumer needs as they arise
- **The challenge:** How best to leverage it and measure it from the perspective of business results and attribution modeling

A black and white photograph of a person's face, wearing Google Glass. The person is looking slightly to the right. The background is dark. The text is overlaid on the image.

Digital Strategy

The Challenge: Deploy & optimise what you know already works
and prepare for what you think will work

Digital Strategy – Underpinnings & Forecast: 1. Conversational Experience

- We are at the explosion-point of the **exponential growth curve**
 - Approaching Teotwawki (in a positive sense...)
- In E&M **mobile** has taken the lead
 - Already occupies two thirds of digital media time
- And in mobile – **the app is king**
 - 70% of mobile media time is in using apps
- Among the apps, **the gorillas dominate**
 - The 5 top apps get 88% of user-time
- **Messaging platforms** are prevalent
 - Billions interact daily and are **used to engage with brands in the feeds**
- **Chatbots** came of age, after many years in childhood, thanks to **Machine Learning**



Conversational Experience

- **Conversational Experience** will emerge as the key differentiator
- **Messaging** will scale creative one-to-one engagement, enhancing the Conversational Experience
- **Chatbots will be deployed as the main tool for managing apps** (& get smarter with each conversation)
- In parallel, **Virtual Agents** and **Avatars** will make inroads into mainstream communication
- Jointly they will bring us to a new period of truly **optimising omnichannel**

Digital Strategy – Underpinnings & Forecast: 2. Immersive Content

- 2010-2015: Virtual Reality
 - 2016: Augmented Reality
 - 2017: Mixed Reality
- **Virtual Reality** takes you to another place
 - **Augmented Reality** can make a Pikachu appear in your living room
 - **Mixed Reality** keeps you where you are – and makes that Pikachu come to life
- When Mixed Reality becomes reality, we can eventually start talking about truly **Immersive Content**



Watch Magic Leap – and Watch Carefully

- “**Magic Leap** is a US startup company (from Dania Beach, FL) that is working on a head-mounted virtual retinal display which superimposes 3D computer-generated imagery over real world objects, by projecting a digital light field into the user's eye”
- **Raised nearly \$1.4 billion** in venture capital
- **Valued at \$4.5 billion** in its latest round of financing
- **Every blue-chip tech investor** has a chunk, including Andreessen Horowitz, Kleiner Perkins, Google, JPMorgan, Fidelity and Alibaba
- When it arrives – my personal guess is in late 2017 – it could usher in **a new era of computing – a next-generation interface** we'll use for decades to come

Digital Strategy – Underpinnings & Forecast: 2. Immersive Content



Cybersecurity

The Challenge: Prepare! ... And then Prepare Again!



Cybersecurity – Prepare for

Identity and Information Theft

the guardian

all opinion culture business lifestyle fashion environment tech travel

Yahoo hack: 1bn accounts compromised by biggest data breach in history

The latest incident to emerge - which happened in 2013 - is probably distinct from the breach of 500m user accounts in 2014



Yahoo have said the stolen user account information may have included dates of birth and telephone numbers. Photograph: Dado Ruvic/Reuters

Yahoo said on Wednesday it had discovered another major cyber attack, saying data from more than 1bn user accounts was compromised in August 2013, making it the largest such breach in history.

The number of affected accounts was double the number implicated in a 2014 breach that the internet company disclosed in September and blamed on hackers working on behalf of a government.

"An unauthorised party" broke into the accounts, Yahoo said in a statement posted on its website. The company believes the hacks are connected and that the breaches are "state-sponsored".

Advertisement



mobilitypro

Most popular in US

Krebs on Security
In-depth security news and investigation



BLOG ADVERTISING

14 Yahoo: One Billion More Accounts Hacked

DEC 16

Just months after disclosing a breach that compromised the passwords for a half billion of its users, **Yahoo** now says a separate incident has jeopardized data from at least a billion more user accounts. The company also warned attackers have figured out a way to log into targeted Yahoo accounts without even supplying the victim's password.



On September 22, Yahoo warned that a security breach of its networks affected more than 500 million account holders. Today, the company said it uncovered a separate incident in which thieves stole data on more than a billion user accounts, and that the newly disclosed breach is separate from the incident disclosed in September.

Advertisement



GET YOUR

My New Book



Cybersecurity – Prepare for

Ransomware – and IoT Ransomware


the guardian

all opinion culture business lifestyle fashion environment tech travel

browse all sections

Los Angeles hospital paid \$17,000 in bitcoin to ransomware hackers

Hollywood Presbyterian Medical Center had lost access to its computer systems since 5 February after hackers installed a virus that encrypted their files



“The quickest and most efficient way to restore our systems ... was to pay the ransom,” said Allen Stefanel, president and chief executive of Hollywood Presbyterian Medical Center. Photograph: Mario Anzuino/Reuters

A Los Angeles hospital hit by ransomware swallowed the bitter pill; it paid off the hackers.

Hollywood Presbyterian Medical Center had lost access to its computer systems since 5 February after hackers installed a virus that encrypted their computer files. The only out was if the hospital paid the hackers \$17,000 worth of bitcoins, the digital currency.

On Wednesday, the hospital announced that it had relented.

“The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom,” Allen Stefanel, president and chief executive of Hollywood Presbyterian, said in a letter Wednesday. “In the best interest of restoring normal operations, we did this.”

The move is one of the most high-profile examples of a hacking victim paying the fee for so-called ransomware, a money-making favorite of eastern European hackers these days.

Most popular

- Alec Baldwin's Donald Trump impersonation fools Dominican newspaper
- Immigration crackdown: travel ban and Russia links intrude on Trump weekend
- I thought I was smarter than almost everybody: my double life as a KGB agent

BBC Sign in News Sport Weather Shop Earth Travel

NEWS

Home Video World UK Business Tech Science Magazine Entertainment & Arts


100 DAYS
MAKE SENSE OF THE EVENTS
SHAPING OUR WORLD

Technology

University hit 21 times in one year by ransomware

By Zoe Kleinman
Technology reporter, BBC News

24 August 2016 | Technology



Universities and NHS trusts in England have been hit hard by ransomware in the last year, according to Freedom of Information requests carried out by two cybersecurity firms.

Bournemouth University, which boasts a cybersecurity centre, has been hit 21 times in the last 12 months.

Twenty-eight NHS Trusts said they had been affected.

Ransomware is a form of computer malware which encrypts files and then demands a ransom for their release.

The New York Times

SEARCH

SuccessFactors Training Made Easy

EUROPE

Hackers Use New Tactic at Austrian Hotel: Locking the Doors

By DAN BILEFSKY JAN. 30, 2017

The ransom demand arrived one recent morning by email, after about a dozen guests were locked out of their rooms at the lakeside Alpine hotel in Austria.

The electronic key system at the picturesque [Romantik Seehotel Jaegerwirt](#) had been infiltrated, and the hotel was locked out of its own computer system, leaving guests stranded in the lobby, causing confusion and panic.

“Good morning?” the email began, according to the hotel’s managing director, Christoph Brandstaetter. It went on to demand a ransom of two Bitcoins, or about \$1,800, and warned that the cost would double if the hotel did not comply with the demand by the end of the day, Jan. 22.

Mr. Brandstaetter said the email included details of a “Bitcoin wallet” — the account in which to deposit the money — and ended with the words, “Have a nice day!”

With the 111-year-old hotel brimming with eager skiers, hikers and vacationers, some having paid about \$530 for a suite with a panoramic view and sauna, Mr. Brandstaetter said he decided to cave in.

Guests had already complained that their electronic room keys were not working, and receptionists’ efforts to create new ones had proved futile. Bashing down the doors was not an option.

A worrying trend...

FBI: Ransomware events quadrupled between 2015 and 2016, to 4,000/day. Cost to the victims went up almost 1000% in the same period, from \$24M to \$209M

Cybersecurity – Prepare for

And ... Influence Campaigns

Russia's Cyber Kompromat Playbook

1. **Mark the targets:** pick close election contests
2. **Gather intelligence:** know your audience
 - Thousands of gov. officials, media personalities and national security experts
3. **Hack**
 - The Fancy Bear (APT28) & The Cozy Bear (APT29)...
4. **Craft manipulated truths**
5. **Propagate & Amplify**
 - Release “information nukes” into “dumpsites”
 - Use automated bots to comment/retweet/share
 - Turn hashtags into twitter trends
6. **Trigger mainstream media outlets**
 - Artificial volumes entices media outlets to engage on the trending issue, further amplifying the narrative
7. **Electorates cannot distinguish fact from fiction, eroding integrity**



Cyberwar in Media:

- Start early and be persistent
- Try everything; stick with what works
- Use brute force to overwhelm adversaries (remember the Soviet military doctrine?)

2017: Here we go...

Germany, France, Netherlands, Norway, Czech Rep., Hungary, Serbia, Slovenia
Iran, Lebanon
South Korea
Chile

PwC Israel

<http://www.pwc.com/il>

THANK YOU!



Cybersecurity

Digital Strategies

Data Analytics