Why “WannaCry and PETYA" ought not to cause tears in your IT world.

September 7th 2017, Munich

Agenda

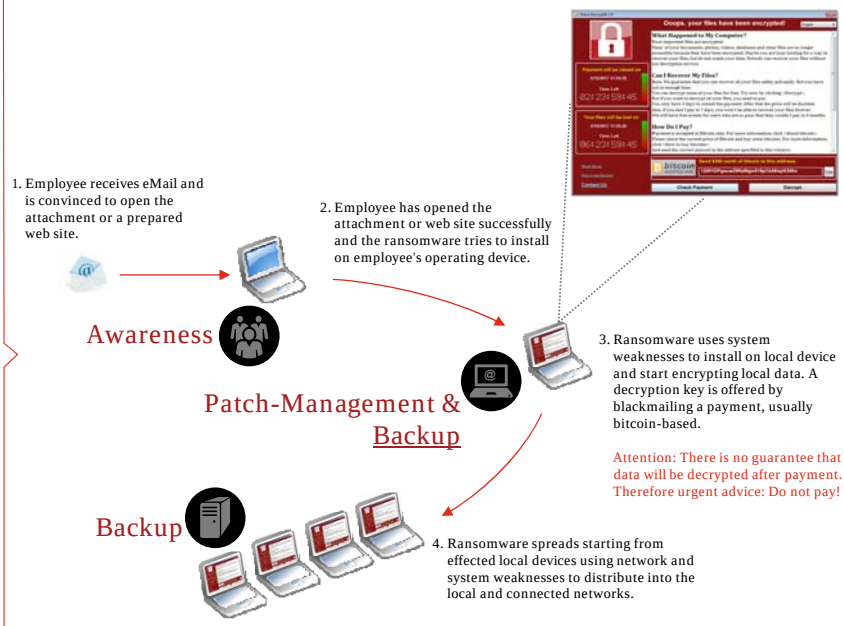
Contact: Dipl.-Math. Derk Fischer
Partner Cybersecurity & Privacy
Phone: +492119812192 | Mobile: +491707946797 | derk.fischer@pwc.com
PricewaterhouseCoopers GmbH WPG
Moskauer Str. 19, 40227 Düsseldorf

1 Understanding the invaders

How do WannaCry and NON-PETYA work?

WannaCry
It is so easy ...

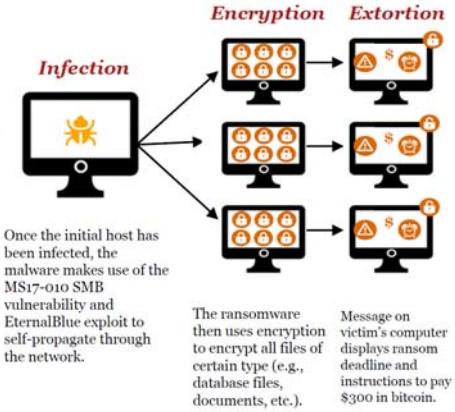
May 2017



„WannaCry", "Wanna Decryptor", "w-cry"
How it works

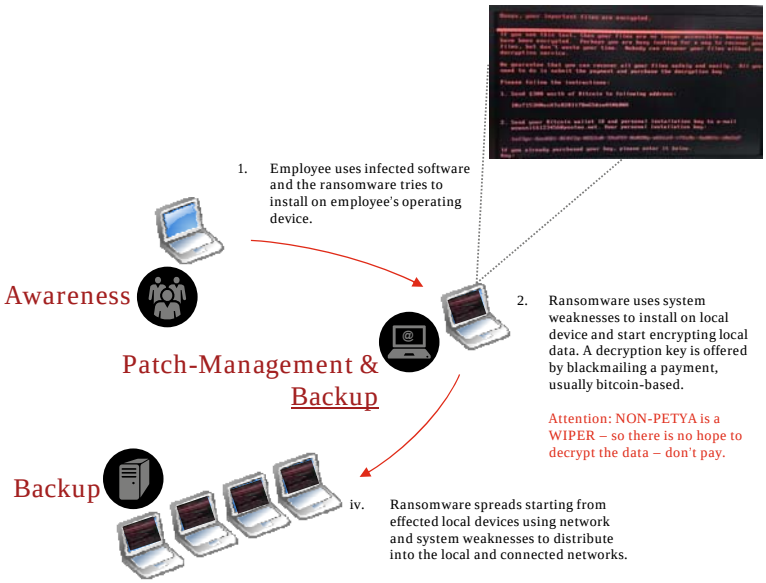
- Widespread ransomware campaign emerged on May 12, 2017
- Hitting hundreds of thousands of systems across over 100 countries within a timespan of 48 hours
- Quickly propagated across Europe, Russia and Asia (known victims: UK's National Health Service, Brazil's Foreign Ministry, Deutsche Bahn and Telefónica)
- Impact: locked computer, data encryption, displaying message demanding approximately $300 in bitcoin

- Short time frame to pay the ransom
- Very fast infection through self-propagation
- Availability of open SMB interfaces at network borders promoted cross network border propagation



NON-PETYA
Yet - it is so easy ...

June 2017



„PETYA", "NON-PETYA"
How it works

- Initial insertion: MEDoc, a tax and accounting software package. MEDoc is widely used in Ukraine, indicating that organizations in that country were the primary target.
- NON-PETYA renaming: The attack is based on a rebuild of Petya and Mischa!
- Information gathering:
  - All IP addresses and DHCP servers of all network adaptors
  - All DHCP clients of the DHCP server if ports 445/139 are open
  - All IP addresses within the subnet as defined by the subnet mask if ports 445/139 are open
  - All computers you have a current open network connection with
  - All computers in the ARP cache
  - All resources in Active Directory
  - All server and workstation resources in Network Neighborhood
  - All resources in the Windows Credential Manager (including Remote Desktop Terminal Services computers)
  - Gathers user names and passwords from Windows Credential Manager
  - Drops and executes a 32bit or 64bit credential dumper

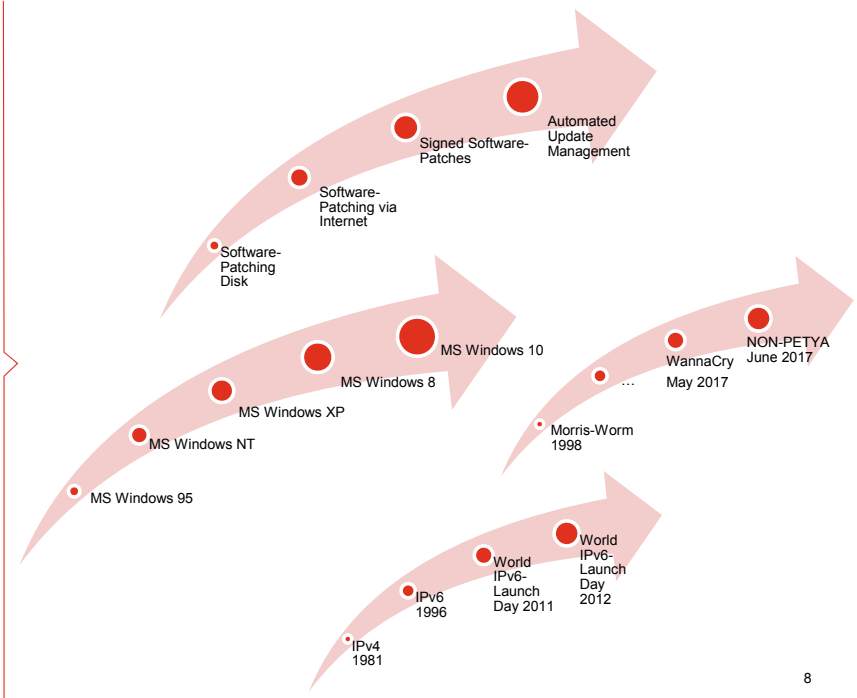
- Self-propagating worm:
  - Execution across network shares via PsExec or the Windows Management Instrumentation Command-line (WMIC) tool
  - SMB exploits (EternalBlue or EternalRomance)
- Attack is focusing on MS Windows systems -> urgent alert for all IT responsible operating systems at outdated patch levels
- Detailed analysis of encryption procedures showed

NON-PETYA is a WIPER

- MBR infection to add a custom loader which is used to load a CHKDSK simulator
- User-mode File encryption

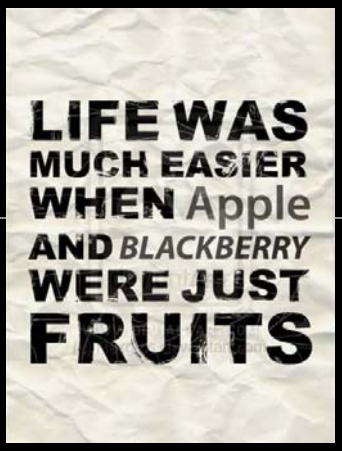
.3ds	.7z	.accdb	.ai	.asp	.aspx	.avhd	.back	.bak	.c	.cfg	.conf	.cpp	.cs
.ctl	.dbf	.disk	.djvu	.doc	.docx	.dwg	.eml	.fdb	.gz	.h	.hdd	.kdbx	.mail
.mdb	.msg	.nrg	.ora	.ost	.ova	.ovf	.pdf	.php	.pmf	.ppt	.pptx	.pst	.pvi
.py	.pyc	.rar	.rtf	.sln	.sql	.tar	.vbox	.vbs	.vcb	.vdi	.vfd	.vmc	.vmdk
.vmsd	.vmx	.vsdx	.vsv	.work	.xls	.xlsx	.xvd	.zip					

Why is this not new ?
... and what we should worry about?



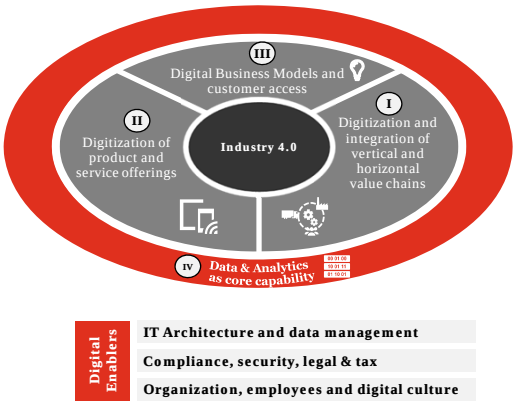
2 Looking for the root cause

What are the drivers we see for information security ?



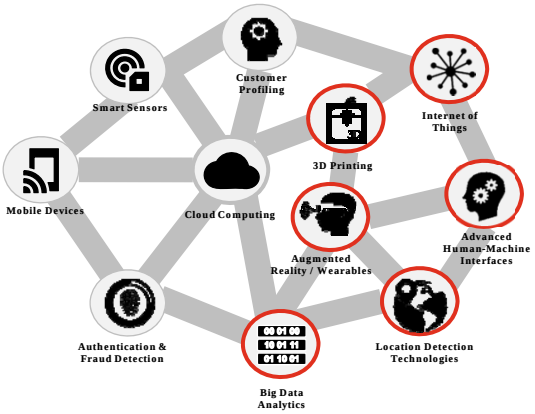
The digital enterprise comprises of digitized and integrated processes, products & business models

Core Application Fields

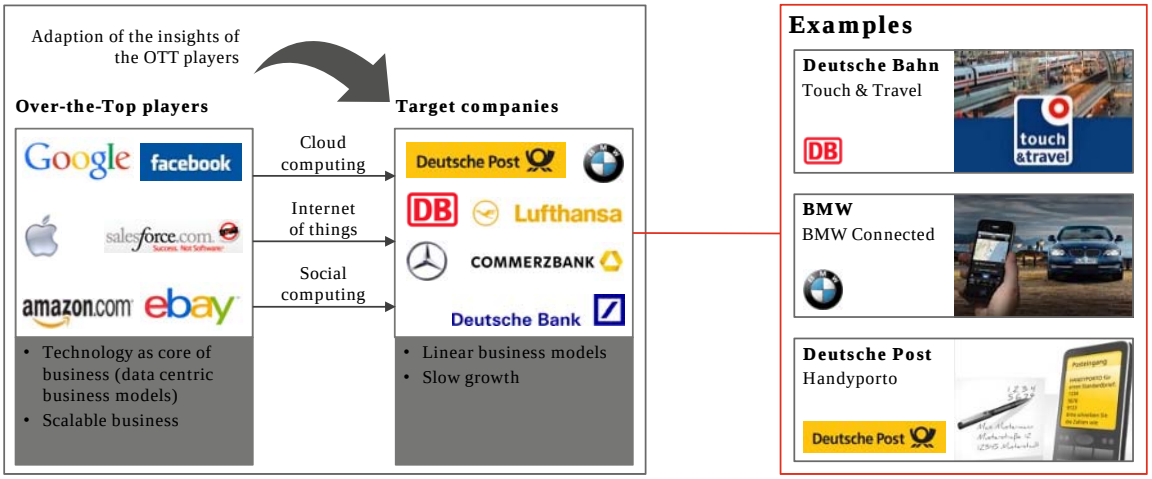


Digital Enablers	
	IT Architecture and data management
	Compliance, security, legal & tax
	Organization, employees and digital culture

Core technologies to provide innovative Industry 4.0 solutions



New player entered the rising digital market

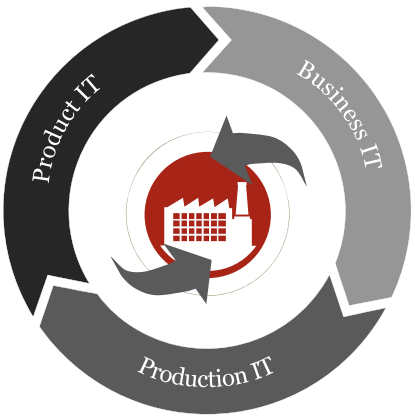


Digital is increasing complexity and need for change

Dimensions of change	Specific future topics
01 Business model	• Confrontation with new business models • New means of competition & new competitors • Focus on volumes with high impact on brand profile
02 Global-isation	• Increasing competition and complexity • Shift of sales markets (Europe vs. Emerging Markets) • Shift of production sites towards new sales markets
03 Data	• Big Data & Predictive Analytics • Cloud & Business Intelligence • Predictive Maintenance & individualized insurance premium
04 Technology	• Telematics & Internet of Things • Improved Infotainment Systems & Human Machine Interfaces • Increased personalization of the automobile, similar to smartphones
05 Security	• Autonomous Driving & eCall • Data protection & Cybersecurity • Automotive Security

Digital Transition drives the metamorphose of the value chain

The transformation drives the need of trust within the whole corporate IT



Investment

- The volume of investment in the different sectors of a company is very different and requires a differing prioritization of the topic of "security".

Evolution

- The development in the areas is based on deviating parameters. While the products are oriented towards the customer market, the production is based on efficiency and the business IT is based on functionality.

Organization

- All three areas are usually subdivided into different departments, which can follow divergent strategies.

Putting Cyber Security into perspective

Key characteristics and attributes of Cyber Security:

- Broader than just information technology and not limited to just the enterprise
- Increasing attack surface due to technology connectivity and convergence
- An 'outside-in view' of the threats and potential impact facing an organization
- Shared responsibility that requires cross functional disciplines in order to plan

It is no longer just an IT challenge – it is a business imperative!

Management of Cyber Security is a compliance issue for digital companies

Fundamentals

- National provisions
- International provisions
- Business specific provisions

„The executive board has to take appropriate measures, [...] , to detect early on developments jeopardizing the continued existence of companies. "[1]

A management system for information security is, in our opinion an important subsystem. Detailed requirements come from

- laws[2]/jurisprudence and
- norms/standards.

Correct implementation

Information security needs to be implemented company-wide and across sectors.
Needs-oriented, individual **design according to the current state of the art**
with regard to

- organization,
- structures and
- technologies.

Design

The **ISMS supports the executive board** in meeting its organizational duties in the subject of information security.

Appropriate measures are

- designed,
- implemented,
- sufficiently monitored,
- audited and
- adequately documented.

Outlook

Foreseeable, **more concrete regulatory requirements** in the course of the digitalization

- Car Spy Act
- IT security act
- EU-NIS-guideline

Tendency to increasingly exposed responsibility of the executive board in case of compliance and security violations.

- ISMS supports amongst others
- Effectiveness review,
- Documentation and
- Further development of requirements.

1 § 91 II AktG
2 Examples: protection of business secrets, Know-how ; protection of industrial property rights (z. B. Patents, brands in design and registration phase or UrhG); surveillance of third parties like e.g. suppliers for the purpose of third party compliance (e.g. BGB, ProdHG, PatG, UWG)

Unfortunately Cyber Security is identified as a hindrance, not a business imperative

The Decision gap

- Increase production capacity
- Lower production cost
- Risk & Security (sometimes later)

Function first – then (perhaps) Security

The Awareness gap

- Lack of Awareness regarding opportunities, risk and speed at all enterprise levels
- First and foremost effects (old-fashioned) management
- Scary excuses

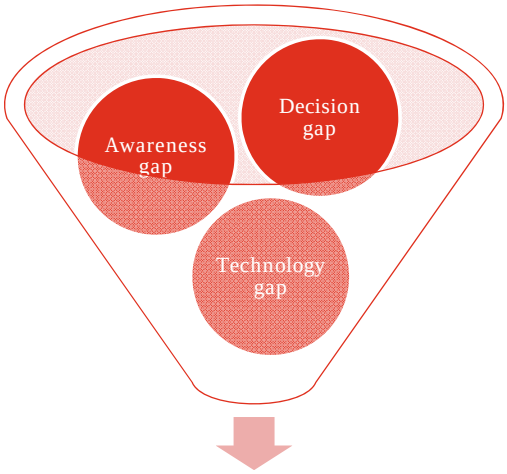
Management is not ready in mind for the digital age

The Technology gap

- Technology is behind state-of-the-art
- Risk management is behind best practice
- Management processes do not even exist

Company eco-system immature to transform into digital eco-system

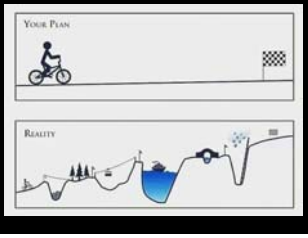
... and the logical conclusion is:



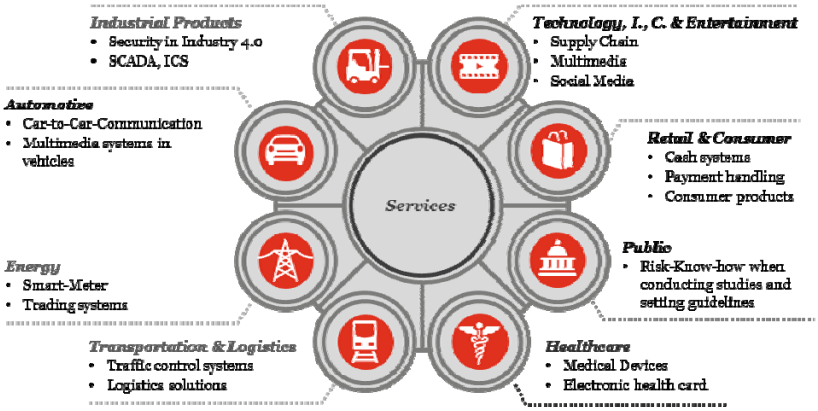
Security, risk and compliance increase costs and decrease speed into a companies digital future

3 Security principles

What to take care of when designing, building and operating information security ?



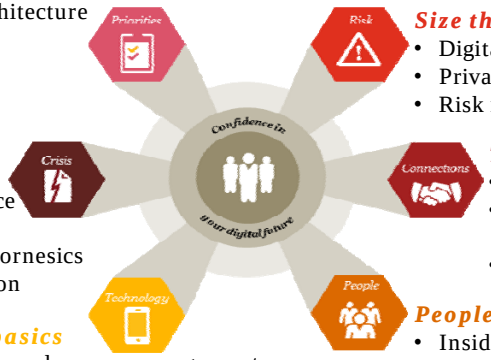
Industry specific topics and new trends



Cyber Security isn't just about technology

You can't secure everything
- Enterprise security architecture
- Protect what matters
- Strategy, organization and governance
- Threat intelligence

It's not if but when
- Continuity and resilience
- Crisis management
- Incident response and fornesics
- Monitoring and detection



Size the advantage
- Digital trust is embedded in the strategy
- Privacy and cyber security legal compliance
- Risk management and risk appetite

Their risk is your risk
- Digital channels
- Partner and supplier management
- Robust contracts

People matter
- Insider threat management
- People and 'moments that matter'
- Security culture and awareness

Fix the basics
- Identity and access management
- Information technology, operations technology and consumer technology
- IT security hygiene
- Security intelligence and analytics

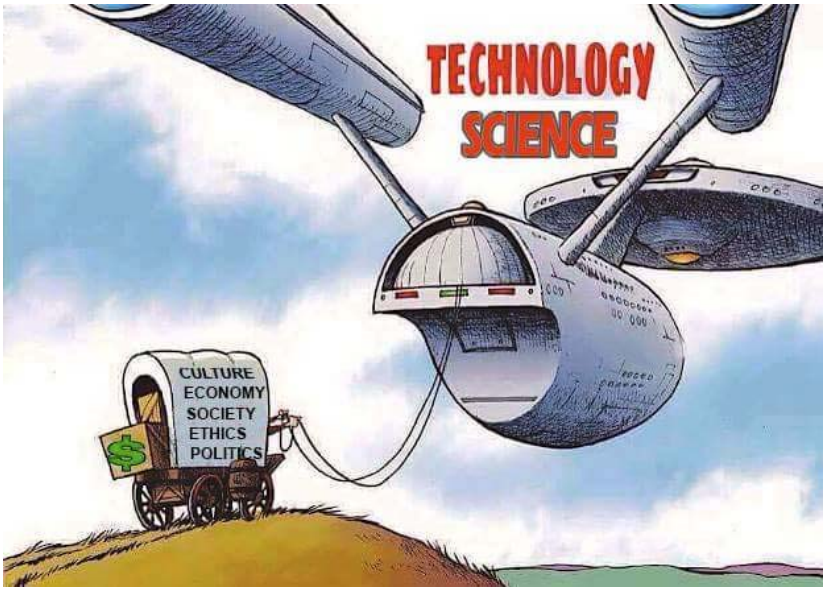
Cyber Security's basic principles

- Secure by Design
  Address security requirements during design and concept work
- Secure by Default
  Implement security measures, minimized access privileges and minimal functional features
- Secure in Development
  Implement a Secure Development Life Cycle
- Secure in Deployment
  Support admin to install and customize software an a security optimized way
- Communications (Software)
  Open communication of security leakages and fast implementation of patches and workarounds
- Privacy by Design
  Consider data privacy during design and concept work
- Privacy by Default
  Conservative of-the-shelf privacy settings
- Privacy in Development
  Implement compliant data privacy controls
- Privacy in Deployment
  Disclosure of data privacy functions
- Communications (Privacy)
  Transparent data privacy statements; dedicated team for data privacy incident handling

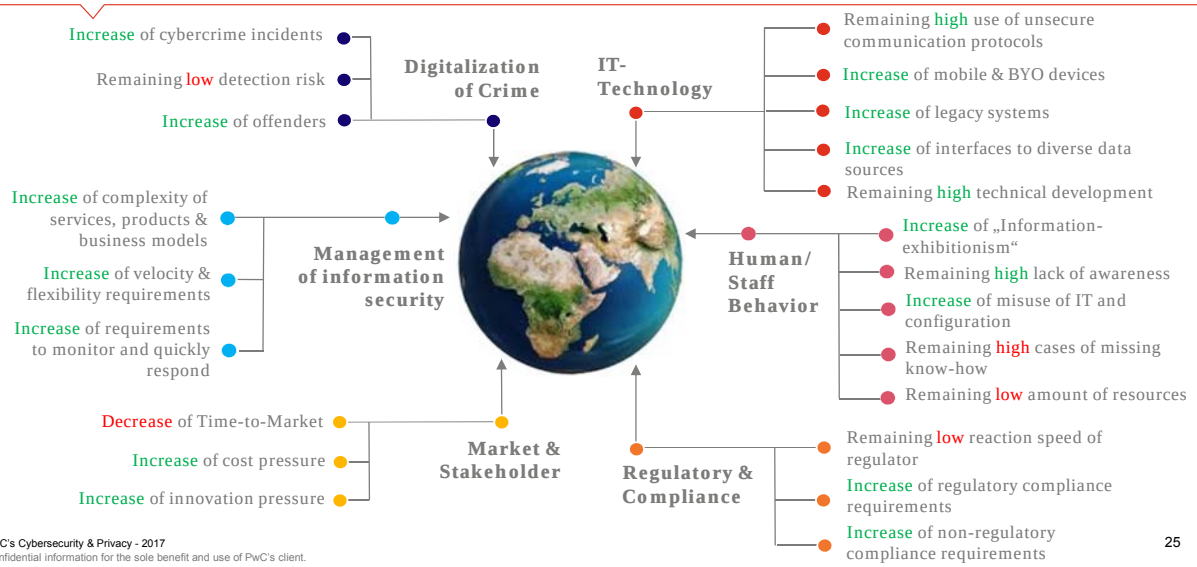
4 Challenges in a digital world

How do digital eco-systems influence our view on cyber security?

Timely development mismatch



Challenges of information security in a digital world



5 Cyber Resilience is the future

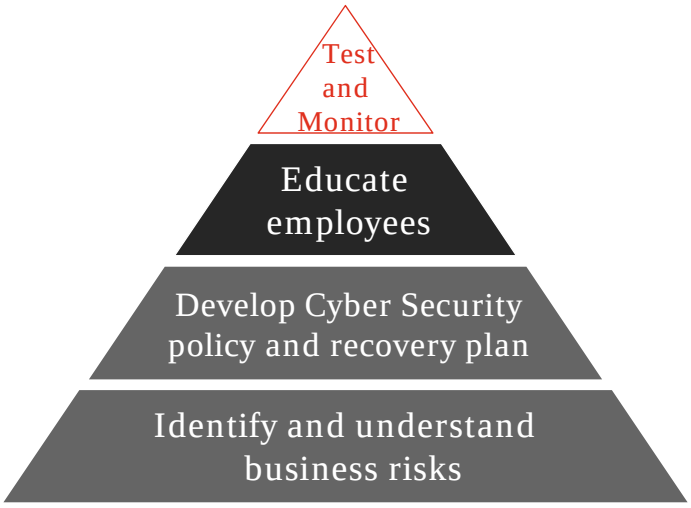
Why cyber security is not sufficient any more …

359,420,698	MySpace accounts		530,270	Battlefield Heroes accounts
164,611,595	LinkedIn accounts		518,966	vBulletin accounts
152,445,165	Adobe accounts		458,155	WIIU ISO accounts
112,005,531	Badoo accounts		453,427	Yahoo accounts
93,338,602	VK accounts		447,410	PS3Hax accounts
68,648,009	Dropbox accounts		442,166	Team SoloMid accounts
65,469,298	tumblr accounts		432,943	Acne.org accounts
49,467,477	iMesh accounts		432,552	Xbox-Scene accounts
40,767,652	Fling accounts		422,959	Avast accounts
30,811,934	Ashley Madison accounts		341,118	PSX-Scene accounts
29,020,808	Tianya accounts		327,314	Plex accounts
27,393,015	Mate1.com accounts		285,191	Sumo Torrent accounts
26,892,897	Neopets accounts		281,924	Seedpeer accounts
22,281,337	R2Games accounts		269,548	MajorGeeks accounts
13,545,468	000webhost accounts		252,751	myRepoSpace accounts
8,243,604	Gamigo accounts		252,216	Foxy Bingo accounts
8,089,103	Heroes of Newerth accounts		228,605	COMELEC (Philippines

Implement a Cyber Resilience Program

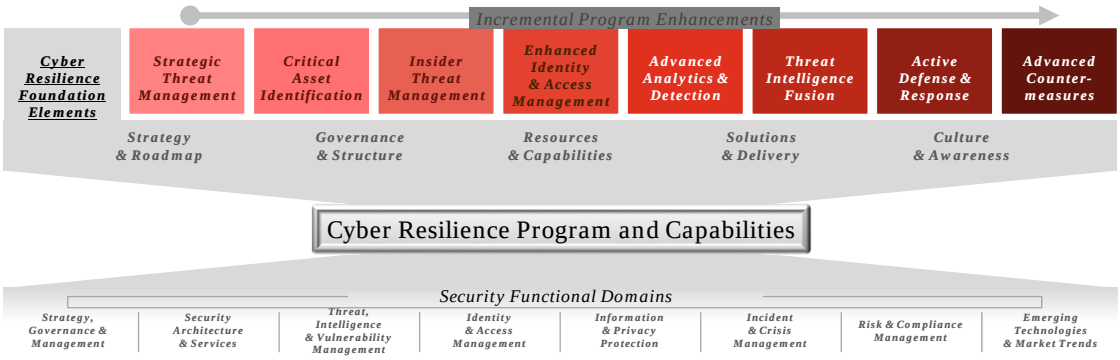
PwC's Cyber Resilience Program approach encompasses both defense and prevention components.

It is designed to adequately react in a moment of a Cyber Crisis.



A Cyber Resilience Program

Once an organization has established stable and **effective foundational IT security** practices, **incremental Cyber Security solutions and Cyber Resilience capabilities** should be pursued.



Finally: 9 Cyber Resilience focus areas

1 Understand the risk landscape.

2 Set the right risk strategy, aligned to the digital age.

3 Assess the upside and downside by making risk-aware business decisions.

4 Design and implement the most efficient and cost effective controls.

5 Harness the power of GRC technologies and other tools to monitor and manage risks and incidents.

6 Gain confidence that technology programs have built in the right controls to the end solution.

7 Promote and measure the right culture and behaviors to succeed.

8 Establish the right boundaries and ways of working across the lines of defense.

9 Build the right monitoring and assurance program for the clients' key risks.

Derk Fischer
Partner
Cybersecurity &Privacy
PricewaterhouseCoopers GmbH WPG
Moskauer Straße 20
40227 Düsseldorf
Tel. +49 211 981 2192
Mobile +49 170 7946 797
derk.fischer@pwc.com