



MIGUEL GARCIA-MENENDEZ

iTTi | The [Digital] Accountability Think Tank
Spain

- Former control engineer and management consultant for some 20 years
- Currently runs iTTi | The [Digital] Accountability Think Tank
- Former member of the Board of the Industrial Cybersecurity Center (CCI)

@MGarciaMenendez

An [almost] global Industrial Cybersecurity regulatory landscape



**Industrial
Cybersecurity 2018:**
Opportunities and challenges
in Digital Transformation

KASPERSKY

Kaspersky Lab's 6th Industrial Cybersecurity Conference
Sochi (Russia). September, 20th, 2018

iTTi



Miguel Garcia-Menendez (ES)

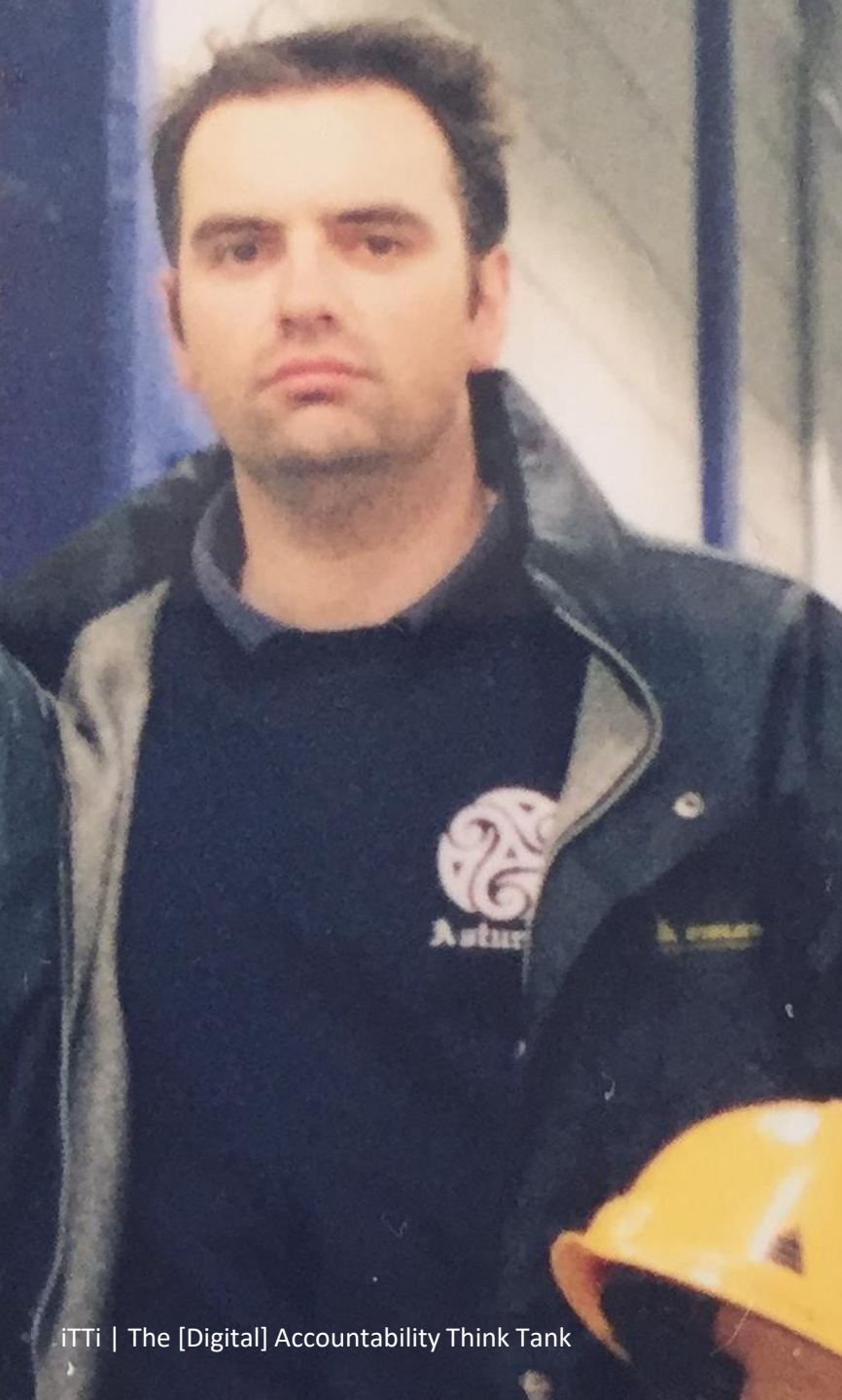
Co-Founder & Chairman

iTTi | The [Digital] Accountability Think
Tank

@MGarciaMenendez



iTTi | The [Digital] Accountability Think Tank



Miguel Garcia-Menendez

Co-Founder & Chairman

iTTi | The [Digital] Accountability Think Tank

A 2+ decades' career veteran, Miguel's first job was in the steel Industry as Head of MES & HMI at an engineering firm, where he soon became CIO. This let him know, first hand, the problems bound to Information/Operational Technology integration.

He has also been a consultant, auditor, lecturer and popularizer in management consultancy firms, universities and forums from which he has helped other executives to fulfill their digital obligations.

Today, Miguel aims to help corporate Directors & Officers to understand their digital | cyber accountability.

You can follow Miguel's professional interests as well as his musings via his Twitter account, [@MGarciaMenendez](https://twitter.com/MGarciaMenendez).





Reino Unido

Irlanda

Liverpool

Londres

Países Bajos

Bruselas

Belgica

Paris

Colonia

Luxemburgo

Francia

Golfo de Vizcaya

Oporto

Portugal

España

Madrid

Barcelona

Valencia

Sevilla

Granada

Gibraltar

Argel
مدينة الجزائر

Casablanca
الدار البيضاء

Marruecos

Agadir
أكادير

Túnez
تونس

Túnez

Tripoli
طرابلس

Malta

Mar Mediterráneo

Dinamarca

Hamburgo

Berlín

Polonia

Varsovia

Alemania

Praga

Chequia

Múnich

Viena

Eslovaquia

Budapest

Hungria

Austria

Suiza

Milán

Mónaco

Eslovenia

Zagreb

Croacia

Belgrado
Београд

Bosnia y
Herzegovina

Sarajevo

Serbia

Podgorica
Подгорица

Kosovo

Macedonia
(ARYM)

Tirana

Albania

Rumanía

Bucarest

Bulgaria

Grecia

Atenas
Αθήνα

Esmirna

Estambul

Bursa

Ankara

Turquía

Antalya

Adana

Chipre

Beirut
بيروت

Damasco
دمشق

Siria

Libano

Jerusaléne

Jordania

Israel

Alejandro
الإسكندرية

El Cairo
القاهرة

Egipto

Kuwait

Bagdad
بغداد

Irak

Georgia
თბილისი

Azerbaiyán

Bakú

Krasnodar
Краснодар

Rostov del Don
Ростов-на-Дону

Ucrania

Járkov
Харків

Vorónezh
Воронеж

Kiev
Київ

Bielorrusia

Minsk
Мінск

Vilna

Lituania

Letonia

Moscú
Москва

Samara
Самара

Orengburgo
Оренбург

Saratov
Саратов

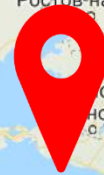
Volgogrado
Волгоград

Mar Caspio

Mar Negro



Novorossiysk (RU)



Gijón (ES)

Novorossiysk (RU)





Gijon (ES)



Novorossiysk (RU)



Are we going to have a
digitally-transformed
industry to protect?

Castillo de San Marcos



THE **digital** industrial company?

Why So Many High-Profile Digital Transformations Fail

by Thomas H. Davenport and George Westerman

MARCH 09, 2018

 SUMMARY  SAVE  SHARE  COMMENT ²⁰  TEXT SIZE  PRINT **\$8.95** BUY COPIES



Prof. Thomas H.
Davenport

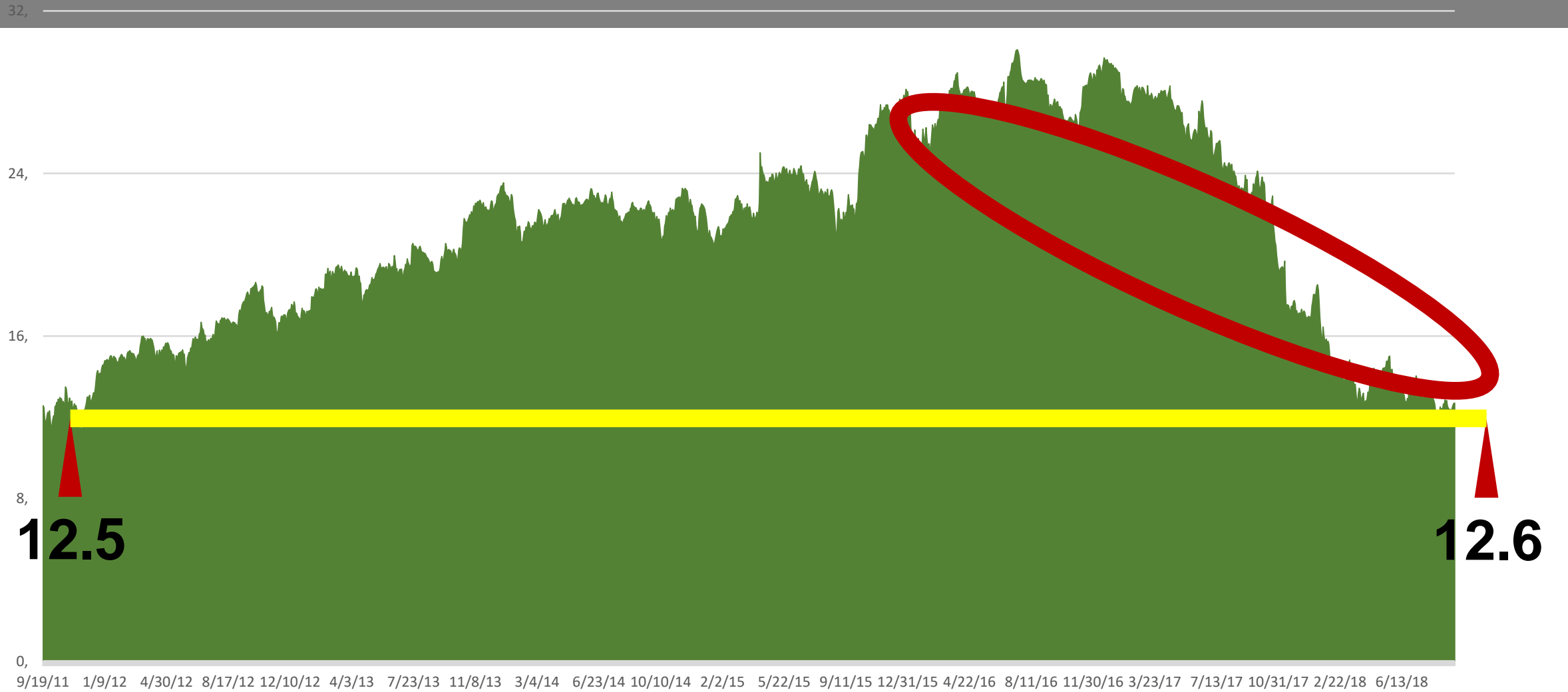


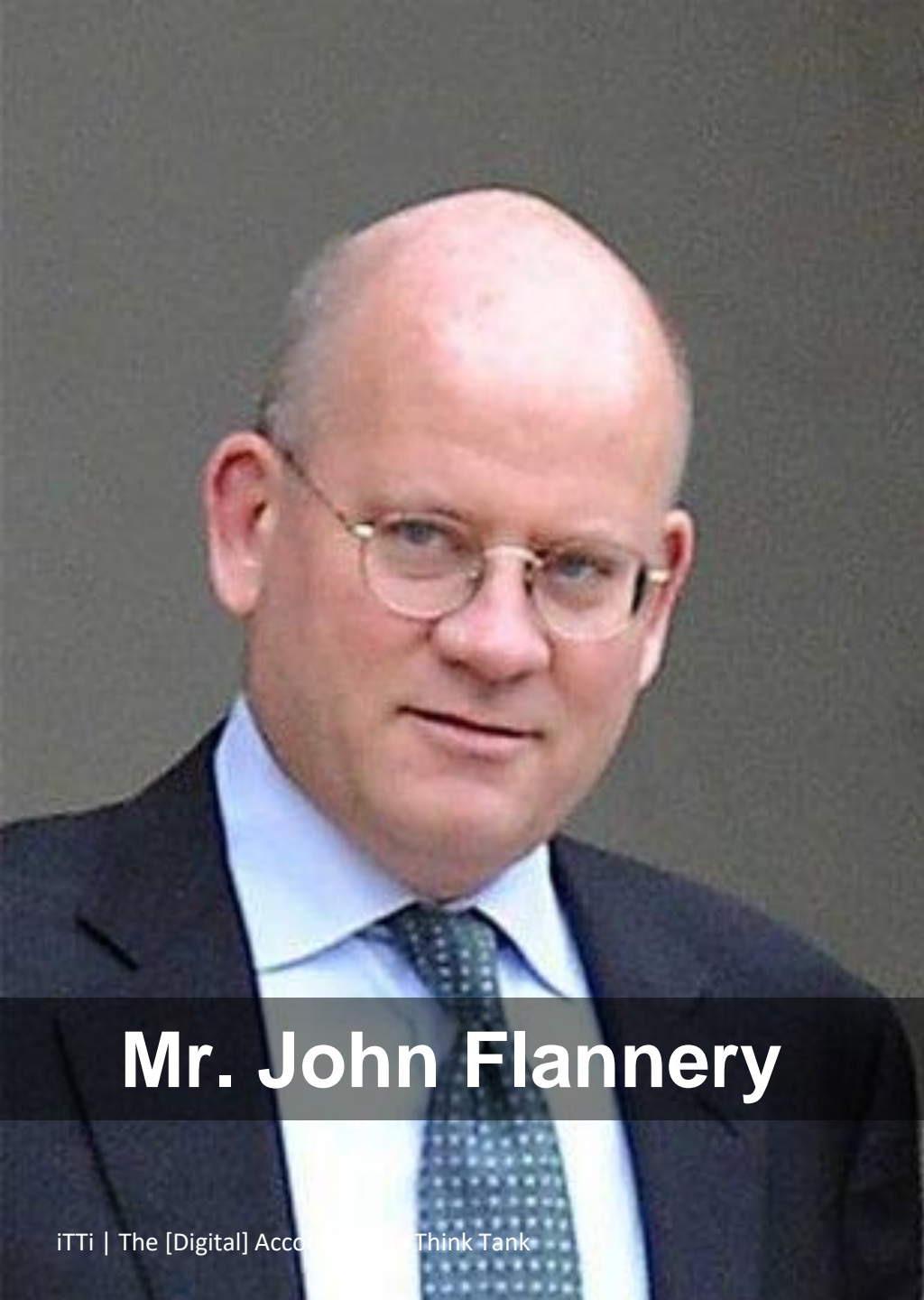
Prof. George
Westerman



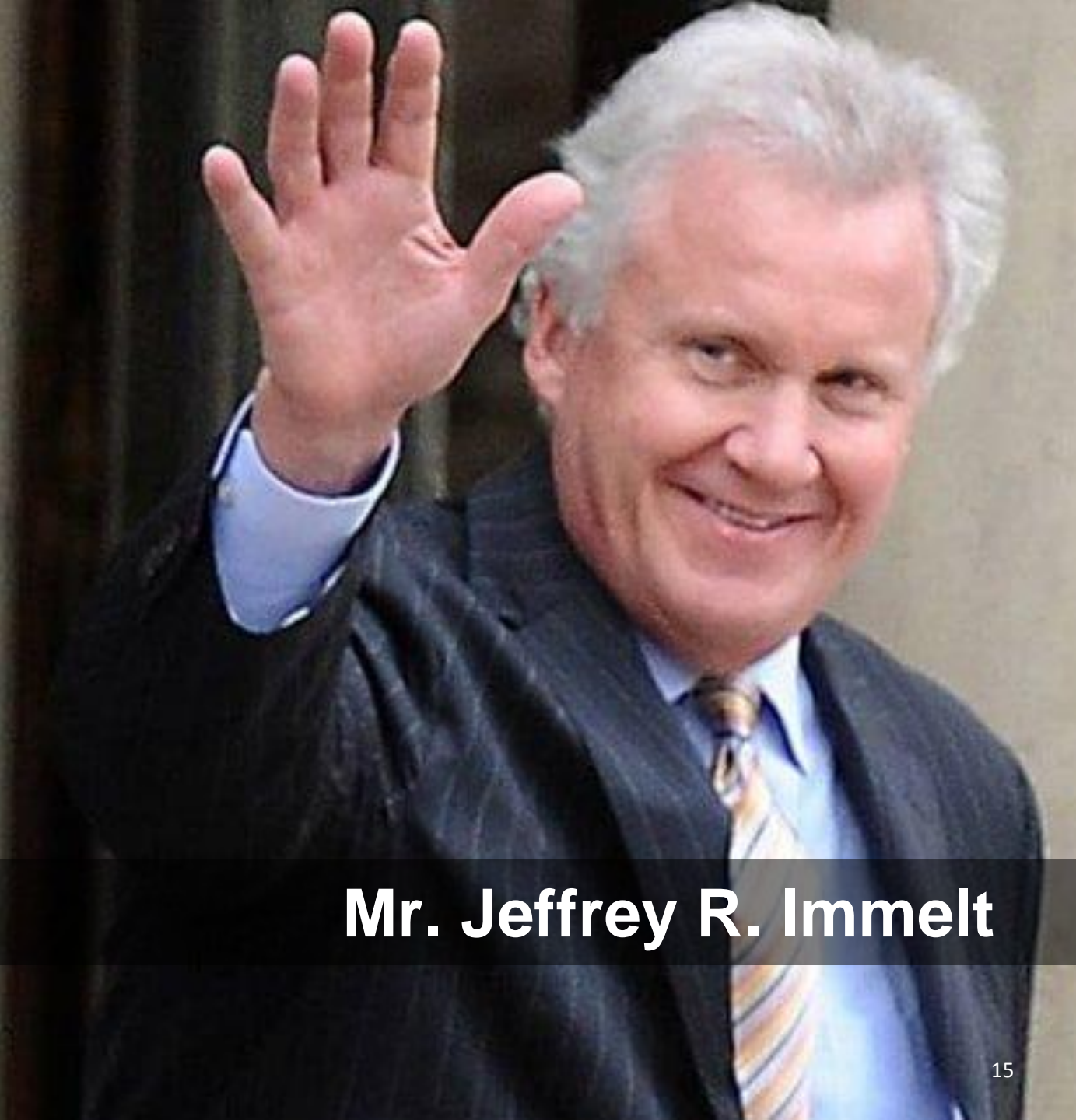
YAGI STUDIOS/GETTY IMAGES

GE's stock price 2011-2018 (USD)





Mr. John Flannery



Mr. Jeffrey R. Immelt

Security is hardly
digitally-transformed
Industry's 1st challenge.
[Neither yours].

**The economy,
the desirability of your
products & your
investors' patience are.**

AGILE

FRAGILE

digital. *Fragility*

d. $F =$

$f(\text{digital Density}) =$

$f(\text{digital Dependence}) =$

$f(dD, \text{lack of awareness})$

digital. *Fragility*

Quality of an organization that determines its susceptibility to suffer an incident, of digital nature, which disturbs its activity (besides causing other consequences for people, assets or the environment); and of whose possible materialization there is not always *consciousness*.

**Protection:
everyone's primary
[& primitive] need.**

Castillo de San Marcos

Fort Alexandria

Планъ форта Александрия.
Возведеннаго на северо-восточномъ берегу Чернаго моря
при устьи реки Соти-Лема.
1838 года.



Объясненіе.

- 1 Казарма на 350 человекъ
- 2 Госпиталь на 64 койки.
- 3 Связь для жительства офицеровъ
- 4 Кухня съ навесомъ поварной аппаратуры.
- 5 Второговоя пещеръ
- 6 Сарай для скота и коней
- 7 Цейхаузъ для зарядной аппаратуры.
- 8 Госпитальный цейхаузъ
- 9 Духовныя печи
- 10 Запасный пороховой погребъ
- 11 Госпитальная баня.
- 12 Кухня маршантъ и конюшня для 10 лошадей.

Ковчегъ

--- -- вѣнчательная для стѣнъ

Г фронтъ-портъ

О солончакъ бассейны

“National” Cyber Security Strategies (CSS)



Source: ENISA, European Network & Information Security Agency

«**NATIONAL**»?

Think twice ...

“National” Cyber Security Strategies (CSS)



Source: ENISA, European Network & Information Security Agency

... and stop calling your
CSS «**NATIONAL**», in a
borderless [cyber] space.



European Industrial Cybersecurity Regulatory Landscape

A multi-lateral perspective

[almost] global

-  **BE**
-  **DE**
-  **ES**
-  **FR**
-  **IT**
-  **NL**
-  **PT**
-  **RO**
-  **TR**
-  **UK**

 **ZA**

-  **CN**
-  **SG**
-  **US**

[ **RU**]

15

COUNTRIES

not an easy task!

100 10

DOCUMENTS

LANGUAGES



CS

STRATEGIES

CTP

REGULATIONS

CG

CODES

CS strategies analyzed

	CYBER SECURITY STRATEGIES (CSS)													
Country Name	BE - Belgium Cyber Security Strategy .be: Securing Cyberspace	DE - Germany Cyber-Security Strategy for Germany 2016	ES - Spain National Cyber Security Strategy 2013	FR - France French National Digital Security Strategy	IT - Italy National Strategic Framework for Cyberspace Security	NL - The Netherlands National Cyber Security Strategy 2. From awareness to capability	PT - Portugal National Cyberspace Security Strategy. Portugal	RO - Romania Cyber Security Strategy of Romania	TR - Turkey 2016-2019 National Cyber Security Strategy	UK - United Kingdom National Cyber Security Strategy 2016-2021	CN - China National Cybersecurity Strategy	SG - Singapore Singapore's Cybersecurity Strategy	US - United States Executive Order 13800 - Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure	
Year	2012	2016	2013	2015	2013	2013	2015	2013	2016	2016	2016	2016	2017	
Generation	1st	2nd (prev. 2011)	1st	1st	1st	2nd (prev. 2011)	1st	1st	2nd (prev. 2013)	2nd (prev. 2011)	1st	1st	(prev. 2003, 2008, 2013)	
Rationale	scientific & economic potential	enormous opportunities and potentials	economic potential & competitiveness	economic prosperity	prosperity	social-economic benefits	economic & social benefits	undeniable social benefits	economic growth and efficiency	economy and privacy	big opportunities social, economic and cultural	economic & social development	economic prosperity	
Protection of fundamental values, rights & duties	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	generic [create a secure cyberspace for businesses and communities]	Yes	
D&D accountability / awareness	No	No	Yes (objective)	No	No	Yes (approach)	No	No	Yes (specific action)	Yes (implementation plan)	No	partially Yes (make cyber a biz priority through Trade Associations & Chambers)	partially Yes (promote market transparency of cybersecurity risk management practices)	
Int'l Split	generic/cooperation	specific/leadership	specific/cooperation	specific/cooperation	specific/cooperation	specific/leadership	specific / cooperation	specific/cooperation	generic/competitive power & cooperation	specific/partnership-leadership	specific/cooperation & assistance	specific/partnership	specific/cooperation	
Promotion of national cyber-industry	Yes (stimulation)	Yes (strengthening)	Yes (int'l-ization)	Yes (promotion & int'l-ization)	Yes (development)	Yes (innovation)	Yes (innovation)	No	No (cooperative ecosystem, at most)	Yes (stimulation [of growth, innovation & int'l-ization])	Yes (stimulation [of growth])	Yes (boosting growth, int'l-ization & innovation)	No	
CIP regulation	specific / Law of 1 July 2011 on the security and protection of critical infrastructures	specific / The IT Security Act of 2015	generic / regulations on the protection of critical infrastructures	specific / Law No. 2013-1168 of 18 December 2013 relating to military programming for the years 2014 to 2019 and containing various provisions concerning defense and national security	generic / Council Directive 2008/114/EC, of 8 December 2008, on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection	generic / (There is no formal legislation -i.e., laws- on CIP in the Netherlands. There are public policies, instead)	generic / [Decree-Law 62/2011 NOT MENTIONED within the Strategy]	generic / national strategy for the protection of critical infrastructure (formally "Government Decision no. 718 of 13 July 2011")	specific / Resolution No. 2 of 20 June 2013 of the Cyber Security Council	generic / right regulatory framework (There is no formal legislation -i.e., laws- on CIP in the United Kingdom. There are public policies, instead)	specific / Cybersecurity Law	specific / new Cybersecurity Act	specific / Presidential Policy Directive/PPD-21, of February 12, 2013, on Critical Infrastructure Security and Resilience	
OT cybersec	specific: SCADA /ICS	generic: Industry 4.0	generic: industrial sector	generic: Industrial accident / industrial activity	specific: SCADA / industrial processes	-	generic: Industry	-	-	specific: Industrial control systems / ICS	specific: automated control systems	-	-	
KPI's	-	-	-	-	-	-	-	-	-	Yes	-	-	-	
Budget	-	-	-	-	-	-	-	-	-	GBP 1.9 Bn	-	8% of Gov.'s ICT budget (SG\$2.4 Bn->SG\$192 M)	33	

avoid the “I-want-my-own-strategy” presidential syndrome



Country Name	BE - Belgium	DE - Germany	ES - Spain	FR - France	IT - Italy	NL - The Netherlands	PT - Portugal	RO - Romania	TR - Turkey	UK - United Kingdom	CN - China	SG - Singapore	US - United States
Year	2012	2016	2013	2013	2013	2013	2013	2013	2016	2016	2016	2016	2017
Generation	1st	2nd (prev. 2011)	1st	1st	1st	2nd (prev. 2011)	1st	1st	2nd (prev. 2013)	2nd (prev. 2011)	1st	1st	(prev. 2003, 2008, 2013)
Rationale	scientific & economic potential	enormous opportunities and potentials	economic potential & competitiveness	economic prosperity	prosperity	social-economic benefits	economic & social benefits	undeniable social benefits	economic growth and efficiency	economy and privacy	big opportunities, social, economic and cultural	economic & social development	economic prosperity
Protection of fundamental rights & freedoms	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	generic [create a secure cyberspace for businesses and communities]	Yes
D&O accountability / awareness	Yes (objective)	Yes (objective)	Yes (objective)	Yes (objective)	Yes (objective)	Yes (objective)	Yes (objective)	Yes (objective)	Yes (specific action)	Yes (implement a plan)	No	partially Yes (make cyber a biz priority through Trade Associations & Chambers)	partially Yes (promote market transparency of cybersecurity risk management practices)
Int'l Spirit	generic/cooperation	specific/leadership	specific/cooperation	specific/cooperation	specific/cooperation	specific/leadership	specific / cooperation	specific/cooperation	generic/competitive power & cooperation	specific/partnership- leadership	specific/cooperation & assistance	specific/partnership	specific/cooperation
Promotion of national cyber-industry	Yes (stimulation)	Yes (strengthening)	Yes (int'l-ization)	Yes (promotion & int'l-ization)	Yes (development)	Yes (innovation)	Yes (innovation)	No	No (cooperative ecosystem, at most)	Yes (stimulation [of growth, innovation] & int'l-ization)	Yes (stimulation [of growth])	Yes (boosting growth, int'l-ization & innovation)	No
CIP regulation	Yes (the security and protection of critical infrastructures)	Yes (2015)	Yes (protection of critical infrastructures)	Yes (18 December 2013 relating to military programming for the years 2014 to 2019 and containing various provisions relating to military programming)	Yes (2008, on the identification and designation of European critical infrastructures)	Yes (legislation - i.e., on CIP in the Netherlands. There are public policies, instead)	Yes (NOT MENTIONED within the Strategy)	Yes (protection of critical infrastructure (formally "Government Decision no. 738 of 13 July 2011")	Yes (June 2013 of the Cyber Security Council)	Yes (right regulatory framework (There is no formal legislation - i.e. laws - on CIP in the United Kingdom. There are public policies, instead)	Yes (specific / Cybersecurity Law)	Yes (specific / new Cybersecurity Act)	Yes (specific / Presidential Policy Directive/PPD-21, of February 12, 2013, on Critical Infrastructure Security and Resilience)
OT cybersecurity	-	-	-	-	-	-	-	-	-	specific: industrial control systems / ICS	specific: automated control systems	-	-
KPI's	-	-	-	-	-	-	-	-	-	Yes	-	-	-
Budget	-	-	-	-	-	-	-	-	-	GBP 1.1 B	-	8% of Gov.'s ICT budget (SG\$2.4 Bn->SG\$192 M)	-

Until recently [May, 15th, 2018], the **US** had **no specific formal cybersecurity strategy** [despite having been a CSS pioneer in 2003].

There have been several public policies, instead.

 **Russia** started its InfoSec journey in 2000.

An updated doctrine was approved in 2016.

an example for the rest of us

Country Name	BE - Belgium	DE - Germany	ES - Spain	FR - France	IT - Italy	NL - The Netherlands	PT - Portugal	RO - Romania	TR - Turkey	UK - United Kingdom	CN - China	SG - Singapore	US - United States
Year	2012	2016	2013	2015	2013	2013	2015	2013	2016	2016	2016	2016	2017
Generation	1st	2nd (prev. 2011)	1st	1st	1st	2nd (prev. 2011)	1st	1st	2nd (prev. 2013)	2nd (prev. 2011)	1st	1st	(prev. 2003, 2008, 2013)
Rationale	potential	competitiveness	competitiveness				benefits	benefits			economic and cultural	development	
Protection of fundamental values, rights & duties	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	generic [create a secure cyberspace for businesses and communities]	Yes
D&D accountability / awareness	No	No	Yes (objective)	No	No	Yes (approach)	No	No	Yes (specific action)	Yes (implementation plan)	No	partially Yes (make cyber a biz priority through Trade Associations & Chambers)	partially Yes (promote market transparency of cybersecurity risk management practices)
Int'l Split	generic/cooperation	specific/leadership	specific/cooperation	specific/cooperation	specific/cooperation	specific/leadership	specific/cooperation	specific/cooperation	generic/competitive	specific/partnership-leadership	specific/cooperation & assistance	specific/partnership	specific/cooperation
Promotion national cyber industry CIP regulati				Law No. 2013-1168 of 18 December 2013 relating to military programming for the years 2014 to 2019 and containing various provisions relating to the security and protection of critical infrastructures	Council Directive 2006/114/EC, of 8 December 2008, on the identification and designation of European critical infrastructures and the obligation of member states to take appropriate measures to protect them	(There is no formal legislation - i.e., laws - on CIP in the Netherlands. There are public policies, instead)	(Decree-Law 62/2011 NOT MENTIONED within the Strategy)	national strategy for the protection of critical infrastructure (formally "Government Decision no. 738 of 13 July 2011")	Resolution No. 2 of 20 June 2013 of the Cyber Security Council	right regulatory framework (There is no formal legislation - i.e., law - on CIP in the United Kingdom. There are public policies, instead)	specific / Cybersecurity Law	specific / new Cybersecurity Act	specific / Presidential Policy Directive/PPD-21, of February 12, 2013, on Critical Infrastructure Security and Resilience
OT cyberse										specific/ industrial control systems / ICS	specific: automated control systems		
KPI's										Yes			
Budget										GBP 1.9 Bn		8% of Gov.'s ICT budget (SG\$2.4 Bn -> SG\$192 M)	

Germany, The Netherlands, Turkey, the UK and the US, the most veteran countries (more than 1 iteration) in developing CSS's.

Russia introduced the concept of Cyber Security Strategy for the first time in a draft released in 2014.

corporate directors are not in the policy-makers' agendas

Country Name	BE - Belgium	DE - Germany	ES - Spain	FR - France	IT - Italy	NL - The Netherlands	PT - Portugal	RO - Romania	TR - Turkey	UK - United Kingdom	CN - China	SG - Singapore	US - United States
Year	2012	2016	2013	2015	2013	2013	2015	2013	2016	2016	2016	2016	2017
Generation	1st	2nd (prev. 2011)	1st	1st	1st	2nd (prev. 2011)	1st	1st	2nd (prev. 2013)	2nd (prev. 2011)	1st	1st	(prev. 2003, 2008, 2013)
Rationale	scientific & economic potential	enormous opportunities and potentials	economic potential & competitiveness	economic prosperity	prosperity	social-economic benefits	economic & social benefits	undeniable social benefits	economic growth and efficiency	economy and privacy	big opportunities social, economic and cultural	economic & social development	economic prosperity
Protection of fundamental values, rights & duties	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	generic [create a secure cyberspace for businesses and communities]	Yes
D&D accountability / awareness	No	No	Yes (objective)	No	No	Yes (approach)	No	No	Yes (specific action)	Yes (implementation plan)	No	partially Yes (make cyber a biz priority through Trade Associations & Chambers)	partially Yes (promote market transparency of cybersecurity risk management practices)
Int'l Split									power & cooperation	leadership	assistance	Yes (boosting growth, int'l-ization & innovation)	No
Promotion of national cyber-industry	Yes (stimulation)	Yes (strengthening)	Yes (int'l-ization)	Yes (promotion & int'l-ization)	Yes (development)	Yes (innovation)	Yes (innovation)	No	No (cooperative ecosystem, at most)	Yes (stimulation [of growth, innovation & leadership])	Yes (stimulation [of growth])	Yes (boosting growth, int'l-ization & innovation)	No
CIP regulation	specific / Law of 1 July 2011 on the security of information systems	specific / The IT Security Act of 2015	generic / regulations on the protection of critical infrastructures	specific / Law No. 2013-1168 of 18 December 2013	generic / Council Directive 2005/61/EC of 8 October 2005	generic / [There is no formal regulation in the Netherlands]	generic / [Decree-Law 62/2011 NOT MENTIONED within the CSS]	generic / national strategy for the protection of critical infrastructures	specific / Resolution No. 2 of 20 July 2013 of the Cyber Security Council	generic / night regulatory work on CIP in the United Kingdom. There are no formal laws on CIP in the United Kingdom. There are public policies, instead	specific / Cybersecurity Law	specific / new Cybersecurity Act	specific / Presidential Policy Directive/PPD-21, of February 12, 2013, on Critical Infrastructure Security and Resilience
OT cybersecurity													
KPI's													
Budget												8% of Gov.'s ICT budget (SG\$2.4 Bn->SG\$192 M)	

Only **Spain, The Netherlands, Turkey** and the **UK** have specific objectives or actions targeting **BoD's members w/in their CSS's.**

ICS cybersecurity is not in the policy-makers' agendas

The Netherlands, Romania, Turkey and the US's CSS do not include specific mention to Operational Technology at all.

Russia's InfoSec doctrine does not include any reference to ICS cybersecurity, too.

Country Name	BE - Belgium	DE - Germany	ES - Spain	FR - France	IT - Italy	NL - The Netherlands	PT - Portugal	RO - Romania	TR - Turkey	UK - United Kingdom	CN - China	SG - Singapore	US - United States
Year	2012	2016	2013	2015	2013	2013	2015	2013	2016	2016	2016	2016	2017
Generation	1st	1st	1st	1st	1st	1st	1st	1st	1st	2nd (prev. 2013)	1st	1st	(prev. 2003, 2008, 2013)
Rationale	potential	and potentials	competitiveness	economic and social benefits	economic and social benefits	economic and social benefits	economic and social benefits	economic and social benefits	economic and social benefits	economic and social benefits	economic and social benefits	economic and social benefits	economic and social benefits
Protection of fundamental rights & duties	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
D&D accountability / awareness	Yes	Yes	(objective)	No	No	Yes (approach)	No	No	Yes (specific action)	Yes (implementation plan)	No	partially Yes (make cyber a biz priority through Trade Associations & Chambers)	partially Yes (promote market transparency of cybersecurity risk management practices)
Int'l Split	specific/leadership	specific/leadership	specific/cooperation	specific/cooperation	specific/cooperation	specific/leadership	specific / cooperation	specific/cooperation	generic/competitive ecosystem, at most	specific/partnership	specific/cooperation & assistance	specific/partnership	specific/cooperation
Promotion of national cyber industry CIP regulation	Yes (stimulation [of growth])	Yes (stimulation [of growth])	Yes (stimulation [of growth])	Yes (stimulation [of growth])	Yes (stimulation [of growth])	Yes (stimulation [of growth])	Yes (stimulation [of growth])	Yes (stimulation [of growth])	Yes (stimulation [of growth])	Yes (stimulation [of growth])	Yes (stimulation [of growth])	Yes (stimulation [of growth])	No
OT cybersecurity	specific: SCADA / ICS	generic: Industry 4.0	generic: industrial sector	generic: Industrial accident / industrial activity	specific: SCADA / industrial processes	-	generic: Industry	-	-	specific: Industrial control systems / ICS	specific: automated control systems	-	-
KPI's	-	-	-	-	-	-	-	-	-	Yes	-	-	-
Budget	-	-	-	-	-	-	-	-	-	GBP 1.9 Bn	-	8% of Gov.'s ICT budget (SG\$2.4 Bn -> SG\$192 M)	37

CIP regulations analyzed [pre-EU NIS Directive]

	CRITICAL INFRASTRUCTURE PROTECTION												
Country	BE - Belgium	DE - Germany	ES - Spain	FR - France	IT - Italy	NL - The Netherlands	PT - Portugal	RO - Romania	TR - Turkey	UK - United Kingdom	CN - China	SG - Singapore	US - United States
Legal basis	Law of 1 July 2011 on the security and protection of critical infrastructures	IT security act of 2015	Law 8/2011, of 28 April, establishing measures for the protection of critical infrastructures	Law No. 2013-1168 of 18 December 2013 relating to military programming for the years 2014 to 2019 and containing various provisions concerning defense and national security	Legislative decree no. 61 of 11 April 2011 implementing Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection	No specific formal legislation -i.e., laws-on CIP (public policies, instead)	Decree-Law no. 62/2011, of 9 May	Emergency Ordinance no. 98 of 3 November 2010 regarding the identification, designation and protection of critical infrastructures	Resolution No. 2 of 20 June 2013 of the Cyber Security Council	No specific formal legislation -i.e., laws-on CIP (public policies, instead)	Cybersecurity Law	Cybersecurity Act (draft)	Presidential Policy Directive/PPD-21, of February 12, 2013, on Critical Infrastructure Security and Resilience
Year	2011	2015	2011	2013	2011	-	2011	2010	2010	-	2017	2018 (expected)	2013
Total # of sectors	(4)	(9)	(12)	(12)	(2)	(12)	(2)	(10)	(6)	(13)	(12)	(11)	(16)
Sectors	e-communications; energy; finance and transportation	drinking water supply & sewage disposal; emergency and rescue services & disaster control and management; finance and insurance business; Government, Parliament, Public Administration and law enforcement agencies; ICT; media and cultural assets; energy supply & distribution; public health & food and transportation	chemical industry; energy; financial & tax system; food; health; ICT; nuclear industry; Public Administration; research facilities; space; transportation and water	civilian activities; communication, technologies & broadcasting; energy; finance; food; health; industry; legal activities; military activities; space & research; transportation and water management	energy and transportation	chemical & nuclear industries; drinking water; energy; financial sector; food; health; legal order; Public Administration; public order & safety; surface water management; telecommunication & ICT and transport	energy and transportation	chemical & nuclear industries; energy; food supply; health; ICT; national security; Public Administration; space & research; transportation and water supply	banking & finance; e-communications; energy; public services; transportation and water management	chemicals; civil nuclear; communications; defence; emergency services; energy; finance; food; Government; health; space; transport and water	communications and digital services; education; energy; environmental protection; finance; industrial manufacturing [defence, large equipment, chemical engineering, food and pharmaceuticals]; healthcare & social welfare; Government; media; scientific research; transportation; water	aviation; banking & finance; energy; Government; healthcare; land transport; maritime; media; security & emergency services; info_communications; water	chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food & agriculture; Government facilities; healthcare & public health; information technology; nuclear reactors, materials and waste; transportation systems; water and wastewater systems

“less regulation, better regulation” might apply here

Country	BE - Belgium	DE - Germany	ES - Spain	FR - France	IT - Italy	NL - The Netherlands	PT - Portugal	RO - Romania	TR - Turkey	UK - United Kingdom	CN - China	SG - Singapore	US - United States
Legal basis	Law of 1 July 2011 on the security and protection of critical infrastructures	IT security act of 2015	Law 8/2011, of 28 April, establishing measures for the protection of critical infrastructures	Law No. 2013-1168 of 18 December 2013 relating to military programming for the years 2014 to 2019 and containing various provisions concerning defense and national security	Legislative decree no. 6 of 11 April 2011 implementing Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection	No specific formal legislation -i.e., laws- on CIP [public policies, instead]	Decree-Law no. 62/2011, of 9 May	Emergency Ordinance no. 98 of 3 November 2010 regarding the identification, designation and protection of critical infrastructures	Resolution No. 2 of 20 June 2013 of the Cyber Security Council	No specific formal legislation -i.e., laws- on CIP [public policies, instead]	Cybersecurity Law	Cybersecurity Act (draft)	Presidential Policy Directive/PPD-21, of February 12, 2013, on Critical Infrastructure Security and Resilience

Year	2011	2015	2011	2013	2011	-	2011	2010	2010	-	2017	2018 (expected)	2013
Total # of sectors	(4)	(9)	(13)	(11)	(9)	(13)	(13)	(10)	(6)	(13)	(13)	(11)	(16)
Sectors	e-communications; energy; finance and insurance; health; information and communication technology; media and cultural assets; energy supply & distribution; public health & food and transportation	drinking water supply & sewage disposal; energy; financial & tax services; health; information and communication technology; media and cultural assets; energy supply & distribution; public health & food and transportation	chemical industry; energy; financial & tax services; health; information and communication technology; media and cultural assets; energy supply & distribution; public health & food and transportation	civilian activities; communication; energy and transportation; health; information and communication technology; media and cultural assets; energy supply & distribution; public health & food and transportation	energy and transportation; health; information and communication technology; media and cultural assets; energy supply & distribution; public health & food and transportation	chemical & nuclear industries; drinking water supply & sewage disposal; energy; financial & tax services; health; information and communication technology; media and cultural assets; energy supply & distribution; public health & food and transportation	chemical & nuclear industries; drinking water supply & sewage disposal; energy; financial & tax services; health; information and communication technology; media and cultural assets; energy supply & distribution; public health & food and transportation	energy and transportation; health; information and communication technology; media and cultural assets; energy supply & distribution; public health & food and transportation	chemical & nuclear industries; energy; food and agriculture; health; information and communication technology; media and cultural assets; energy supply & distribution; public health & food and transportation	banking & finance; e-communications; energy; financial & tax services; health; information and communication technology; media and cultural assets; energy supply & distribution; public health & food and transportation	chemicals; civil nuclear; communications; energy; financial & tax services; health; information and communication technology; media and cultural assets; energy supply & distribution; public health & food and transportation	communications and digital services; energy; financial & tax services; health; information and communication technology; media and cultural assets; energy supply & distribution; public health & food and transportation	aviation; banking & finance; energy; financial & tax services; health; information and communication technology; media and cultural assets; energy supply & distribution; public health & food and transportation

A **specific regulation** rules CIP in every country, **except for The Netherlands** and the **UK**. The EU NIS Directive has come to change this.



Russia started its CIP journey in the early 2000s. Today **Russia's CIP policy** is part of its national security strategy.

another example for the rest of us

Romania and Turkey (again) are among the most veteran (2010) countries when it comes to formally define their CIP policy.

Country	BE - Belgium	DE - Germany	ES - Spain	FR - France	NL - Netherlands	PT - Portugal	RO - Romania	TR - Turkey	UK - United Kingdom	CN - China	SG - Singapore	US - United States	
Legal basis	Law of 1 July 2011 on	IT security act of 2015	Law 8/2004, of 28 April,	Law No. 2013-1168 of	legislative decree no. 51	No specific formal	Decree-Law no. 201/2010	Emergency Ordinance	Resolution No. 2 of 20	No specific formal	Cybersecurity Act (draft)	Presidential Policy	
Year	2011	2015	2011	2013	2011	-	2010	2010	-	2017	2018 (expected)	2013	
Total # of sectors	10	10	10	10	10	10	10	10	10	10	10	10	
Sectors	e-communications; energy; finance and transportation	drinking water supply & sewage disposal; emergency and rescue services & disaster control and management; finance and insurance business; Government, Parliament, Public Administration and law enforcement agencies; ICT; media and cultural assets; energy supply & distribution; public health & food and transportation	chemical industry; energy; financial & tax system; food; health; ICT; nuclear industry; Public Administration; research facilities; space; transportation and water	civilian activities; communication, technologies & broadcasting; energy; finance; food; health; industry; legal activities; military activities; space & research; transportation and water management	energy and transportation	chemical & nuclear industries; drinking water; energy; financial sector; food; health; legal order; Public Administration; public order & safety; surface water management; telecommunication & ICT and transport	energy and transportation	chemical & nuclear industries; energy; food health; ICT; security; Public Administration; space & research; transportation and water supply	banking & finance; communications; energy; public order & safety; transportation; water management	communications; energy; emergency services; finance; food; Government; health; space; transport and water	communications and digital services; education; energy; environmental protection; finance; industrial manufacturing [defence, large equipment, chemical engineering, food and pharmaceuticals]; healthcare & social welfare; Government; media; scientific research; transportation; water	aviation; banking & finance; energy; Government; healthcare; land transport; maritime; media; security & emergency services; info_communications; water	chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food & agriculture; Government facilities; healthcare & public health; information technology; nuclear reactors, materials and waste; transportation systems; water and wastewater systems



would less disparity benefit interdependencies someway?

Italy and **Portugal** have opted for extrictly following EU's CIP Directive of 2008. Their **critical sectors** are only **energy & transportation**. A situation that the EU NIS Directive has come to change.

Country	Law	Year
China	Security Law	2015
SG - Singapore	Cybersecurity Act (draft)	2017
US - United States	Presidential Policy Directive/PPD-21, of February 12, 2013, on Critical Infrastructure Security and Resilience	2013

Year	2011	2015	2011	2013	2011	2011	2010	2010	2011	2012	2018 (expected)	2013	
Total # of sectors	(4)	(9)	(12)	(12)	(2)	(12)	(2)	(10)	(6)	(13)	(12)	(11)	(16)
Sectors	e-communications; energy; finance and transportation	drinking water supply & sewage disposal; emergency and disaster services & disaster control and management; finance and insurance business; Government, Parliament, Public Administration and law enforcement agencies; ICT; media and cultural assets; energy supply & distribution; public health & food and transportation	chemical industry; energy; financial & tax system; food; health; ICT; nuclear industry; Public Administration; research facilities; space; transportation and water	civilian activities; communication, technologies & broadcasting; energy; finance; food; health; industry; legal activities; military activities; research; transportation and water management	energy and transportation	chemical & nuclear industries; drinking water; energy; financial sector; food; health; legal order; Public Administration; public order & safety; surface water management; telecommunication & ICT and transport	energy and transportation	chemical & nuclear industries; energy; food supply; health; ICT; security; Public Administration; space & transportation; water supply	banking & finance; e-communications; energy; public services; transportation and water management	chemicals; civil nuclear; communications; defence; emergency services; energy; finance; food; Government; health; space; transport and water	communications and digital services; education; energy; environmental protection; finance; industrial manufacturing [defence, large equipment, chemical engineering, food and pharmaceuticals]; healthcare & social welfare; Government; media; scientific research; transportation; water	aviation; banking & finance; energy; Government; healthcare; land transport; maritime; media; security & emergency services; info_communications; water	chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food & agriculture; Government facilities; healthcare & public health; information technology; nuclear reactors, materials and waste; transportation systems; water and wastewater systems

The post-EU NIS Directive picture

-  **BE**
-  **DE**
-  **ES**
-  **FR**
-  **IT**
-  **NL**
-  **PT**
-  **RO**
-  **TR**
-  **UK**












9

COUNTRIES
affected [w/in our study]

only

The post-EU NIS Directive picture

-  BE
-  **DE**
-  ES
-  FR
-  **IT**
-  NL
-  PT
-  RO
-  **UK**

as of May, 9th, 2018

3

**COUNTRIES
complied** [on due
date]

The post-EU NIS Directive picture



Castillo de San Marcos

17

out of

28

COUNTRIES

were urged to transpose the NIS Directive [on July, 20th, 2018]

Source: European Commission

MITI | The [Digital] Accountability Think Tank

Google

The post-EU NIS Directive picture



... as of today.

4

**COUNTRIES
still pending**

Source: European Commission

MITI | The [Digital] Accountability Think Tank

Google

Are companies taking cybersecurity seriously?

“National” Cyber Security Strategies (CSS)



Source: ENISA, European Network & Information Security Agency

of countries that already have their own CSS



1

out of

4

Source: ENISA, European Network & Information Security Agency

MITI | The [Digital] Accountability Think Tank

Google

**25% of countries already
have a CSS!
Does companies have?**

TalkTalk

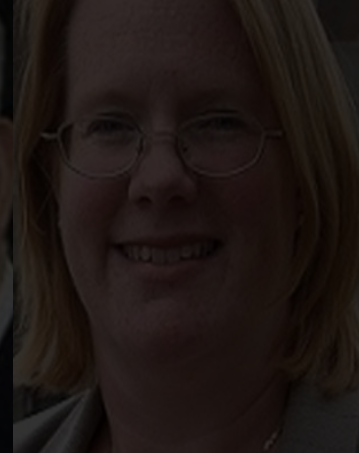
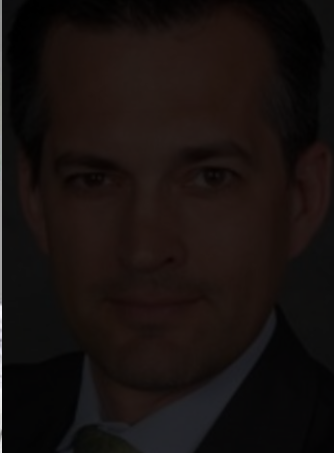
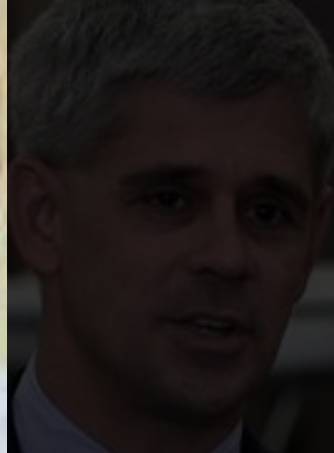


“Although ultimate responsibility for cyber security within a company lies with the CEO, it would be highly unusual for the CEO of a company to have to resign over an attack”.

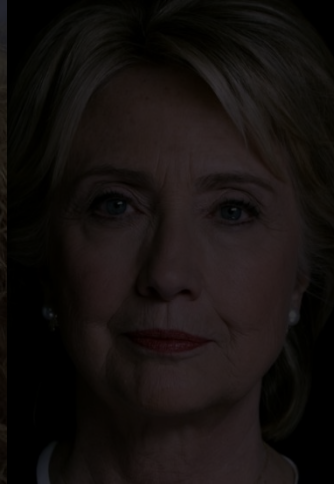
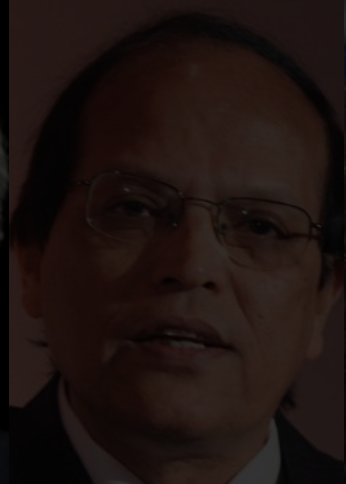
**UK Parliament (@UKParliament)
House of Commons**

Culture, Media & Sport Committee

“Cyber Security: Protection of Personal Data Online” report



Oil & Gas





Air Transport & Aeronautics



Digital Security



Financial Services



Healthcare



Public Sector





Retail

A grid of 24 portrait photos of various people, arranged in a 4x6 grid. The central portrait, of a woman with brown hair, is highlighted in color, while all other portraits are in grayscale. The text "Leisure & entertainment" is overlaid in large white font across the center of the grid.

Leisure & entertainment



Automotive



Policy Making



1999



2004



2010



2011



2011



2012



2012



2013



2014



2015



2015



2015



2015



2016



2016



2016



2016



Digital is not my biz!



Who's been next?



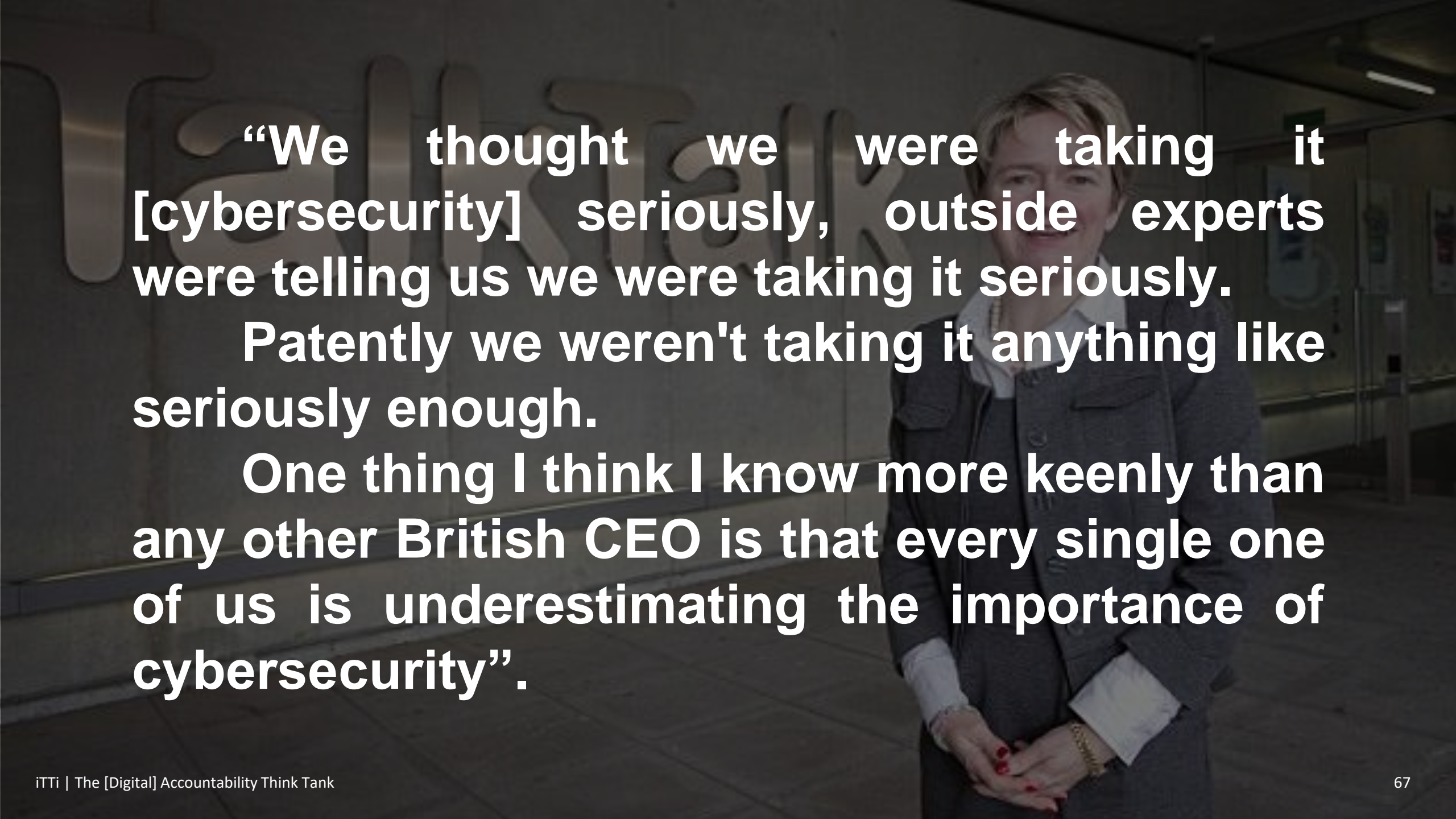
talkTalk



A woman with short blonde hair, wearing a grey suit and a pearl necklace, stands in front of a wall with large, metallic, 3D letters spelling 'WalkTalk'. She is smiling and has her hands clasped in front of her. The background shows a modern office interior with glass doors and a hallway.

WalkTalk

“... sometimes it's OK to admit to your fallibility”.

A woman with short blonde hair, wearing a grey suit and a white shirt, stands in a modern office hallway. She is smiling slightly and has her hands clasped in front of her. The background features large, stylized, metallic letters on the wall, possibly spelling out 'iTTi'. The lighting is soft and even.

“We thought we were taking it [cybersecurity] seriously, outside experts were telling us we were taking it seriously.

Patently we weren't taking it anything like seriously enough.

One thing I think I know more keenly than any other British CEO is that every single one of us is underestimating the importance of cybersecurity”.

CG codes analyzed

Country	Corporate Governance Code	Source	Nature	Governance Structure	Compliance Framework	Risk Oversight by BoD thru	Cyber
BE Belgium	"The 2009 Belgian Code on Corporate Governance" (2009)	Corporate Governance Committee	Self-regulatory	1-Tier	comply or explain	Audit Committee	non-explicit
DE Germany	"German Corporate Governance Code" (2017)	Govt. Commission of the German Corporate Governance Code	Self-regulatory	2-Tier	comply or explain	Audit Committee	non-explicit
ES Spain	"Good Governance Code of Listed Companies" (2015)	Stock Market National Committee (CNMV)	Govt-promoted	1-Tier	comply or explain	Audit Committee	non-explicit
FR France	"Corporate governance code of listed corporations" (2016)	AFEP/MEDEF	Self-regulatory	1-Tier	comply or explain	Audit Committee / Risk Committee	non-explicit
IT Italy	"Corporate Governance Code" (2015)	Corporate Governance Committee	Self-regulatory	1-Tier / both	comply or explain	Control & Risk Committee	non-explicit
NL The Netherlands	"The Dutch Corporate Governance Code" (2016)	Corporate Governance Code Monitoring Committee (MCCG)	Self-regulatory	2-Tier	comply or explain	Audit Committee / Risk Committee	explicit
PT Portugal	"Corporate Governance Code" (2017)	Portuguese Corporate Governance Institute (IPCG)	Self-regulatory	both	comply or explain	Monitoring Board	non-explicit
RO Romania	Code of Corporate Governance (2015)	Bucharest Stock Exchange (BVB)	Self-regulatory	both	comply or explain	Audit Committee	non-explicit
TR Turkey	Principles of Corporate Governance (2014)	Capital Markets Board (CMB)	Govt-promoted	1-Tier	comply or explain	Early Detection of Risk Committee	non-explicit
UK United Kingdom	The UK Corporate Governance Code (2016)	Financial Reporting Council (FRC)	Self-regulatory	1-Tier	comply or explain	Audit Committee / Risk Committee	non-explicit
ZA South Africa	King Report on Corporate Governance for South Africa 2016 (2016)	Institute of Directors in Southern Africa (IoDSA)	Self-regulatory	1-Tier	apply and explain	Risk committee / Audit Committee	explicit
CN China	Code of Corporate Governance for Listed Companies in China (2001)	China Securities Regulatory Commission (CSRC)	Govt-promoted	2-Tier	comply or explain	Audit Committee	non-explicit
SG Singapore	Code of Corporate Governance (2012)	Monetary Authority of Singapore (MAS)	Govt-promoted	1-Tier	comply or explain	Audit Committee	non-explicit
US United States	Sarbanes-Oxley Act of 2002 (2002)	Securities and Exchange Commission (SEC)	Govt-promoted	1-Tier	comply or else	Audit Committee	non-explicit

does it make sense?

Corporate Governance codes are mandatory, while its recommendations are not (“comply-or-explain” principle).

Exception: US (the Sarbanes-Oxley Act of 2002 is not a code, it is a law).

Country	Corporate Governance Code	Source	Nature	Governance Structure	Compliance Framework	Risk Oversight by BoD thru	Cyber
Belgium	The 2009 Belgian Code on Corporate Governance (2009)	Corporate Governance Committee	Self-regulatory	1-Tier	comply or explain	Audit Committee	non-explicit
Denmark	Guidelines on Corporate Governance (2015)	Corporate Governance Institute (CGI)	Self-regulatory	2-Tier	comply or explain	Audit Committee	non-explicit
Spain	Good Governance Code of Listed Companies (2014)	Stock Market National Committee (CNMV)	Govt-promoted	1-Tier	comply or explain	Audit Committee	non-explicit
France	Corporate governance code of listed corporations (2016)	AFEP/MEDEF	Self-regulatory	1-Tier	comply or explain	Audit Committee / Risk Committee	non-explicit
Italy	Principles of Corporate Governance (2014)	Italian Corporate Governance Committee	Self-regulatory	1-Tier / both	comply or explain	Control & Risk Committee	non-explicit
Netherlands	The Dutch Corporate Governance Code (2016)	Corporate Governance Code Monitoring Board (CGCB)	Self-regulatory	2-Tier	comply or explain	Audit Committee / Risk Committee	explicit
Portugal	Corporate Governance Code (2017)	Portuguese Corporate Governance Institute (IPCG)	Self-regulatory	both	comply or explain	Monitoring Board	non-explicit
Romania	Code of Corporate Governance (2015)	Bucharest Stock Exchange (BVB)	Self-regulatory	both	comply or explain	Audit Committee	non-explicit
Taiwan	Principles of Corporate Governance (2015)	Capital Markets Board (CMB)	Govt-promoted	1-Tier	comply or explain	Early Detection of Risk Committee	non-explicit
United Kingdom	The UK Corporate Governance Code (2016)	Financial Reporting Council (FRC)	Self-regulatory	1-Tier	comply or explain	Audit Committee / Risk Committee	non-explicit
Zimbabwe	Guiding Principles for Corporate Governance (2015)	Association of Banks of Zimbabwe (ABZ) / Zimbabwe Stock Exchange (ZSE)	Self-regulatory	1-Tier	apply and explain	Risk committee / Audit Committee	explicit
China	Corporate Governance for Listed Companies in China (2001)	China Securities Regulatory Commission (CSRC)	Govt-promoted	2-Tier	comply or explain	Audit Committee	non-explicit
Singapore	Code of Corporate Governance (2012)	Monetary Authority of Singapore (MAS)	Govt-promoted	1-Tier	comply or explain	Audit Committee	non-explicit
US	Sarbanes-Oxley Act of 2002 (2002)	Securities and Exchange Commission (SEC)	Govt-promoted	1-Tier	comply or else	Audit Committee	non-explicit



shouldn't every Audit/Risk Committee act early, too?

Risk oversight is BoD's biz (usually through an Audit or Risk Committee).

Turkish listed companies have an **Early Detection of Risk Committee**.



In the case of **Russia**, its Corporate Governance Code also refers to an Audit Committee.



Country	Corporate Governance Code	Source	Nature	Governance Structure	Compliance Framework	Risk Oversight by BoD thru	Cyber
BE Belgium	THE 2003 Belgian Code on Corporate Governance (2003)	Corporate Governance Committee	Self-regulatory	1-Tier	comply or explain	Audit Committee	non-explicit
DE Germany	Corporate Governance Code	Corporate Governance Committee (CNMV)	Self-regulatory	1-Tier	comply or explain	Audit Committee	non-explicit
ES Spain	Corporate Governance Code	Corporate Governance Committee (CNMV)	Govt-promoted	1-Tier	comply or explain	Audit Committee	non-explicit
FR France	"Corporate governance code of listed corporations" (2016)	AFEP/MEDEF	Self-regulatory	1-Tier	comply or explain	Audit Committee / Risk Committee	non-explicit
IT Italy	"Corporate Governance Code" (2015)	Corporate Governance Committee	Self-regulatory	1-Tier / both	comply or explain	Control & Risk Committee	non-explicit
NL The Netherlands	"Corporate Governance Code" (2016)	Corporate Governance Committee (MCCG)	Self-regulatory	2-Tier	comply or explain	Audit Committee / Risk Committee	explicit
PT Portugal	"Corporate Governance Code" (2011)	Portuguese Corporate Governance Institute	Self-regulatory	both	comply or explain	Monitoring Board	non-explicit
RO Romania	Code of Corporate Governance (2015)	Bucharest Stock Exchange (BVB)	Self-regulatory	both	comply or explain	Audit Committee	non-explicit
TR Turkey	Principles of Corporate Governance (2014)	Capital Markets Board (CMB)	Govt-promoted	1-Tier	comply or explain	Early Detection of Risk Committee	non-explicit
UK United Kingdom	The UK Corporate Governance Code (2016)	Financial Reporting Council (FRC)	Self-regulatory	1-Tier	comply or explain	Audit Committee / Risk Committee	non-explicit
ZA South Africa	King III Report on Corporate Governance (2009)	King III Report on Corporate Governance	Self-regulatory	1-Tier	apply and explain	Risk committee / Audit Committee	explicit
CN China	Code of Corporate Governance for Listed Companies in China (2001)	China Securities Regulatory Commission (CSRC)	Govt-promoted	2-Tier	comply or explain	Audit Committee	non-explicit
SG Singapore	Code of Corporate Governance (2012)	Monetary Authority of Singapore (MAS)	Govt-promoted	1-Tier	comply or explain	Audit Committee	non-explicit
US United States	Sarbanes-Oxley Act of 2002 (2002)	Securities and Exchange Commission (SEC)	Govt-promoted	1-Tier	comply or else	Audit Committee	non-explicit

this probably explains everything

Only **The Netherlands** and **South Africa's** CG codes make an **explicit mention to cyber** [despite almost all of them were released after the **TARGET** case (2013)].

Of course, none of them mentions **industrial cybersecurity**.



Country	Corporate Governance Code	Source	Nature	Governance Structure	Compliance Framework	Risk Oversight by BoD thru	Cyber
BE Belgium	"The 2009 Belgian Code on Corporate Governance" (2009)	Corporate Governance Committee	Self-regulatory	1-Tier	comply or explain	Audit Committee	non-explicit
DE Germany	"German Corporate Governance Code" (2017)	Govt. Commission of the German Corporate Governance Code	Self-regulatory	2-Tier	comply or explain	Audit Committee	non-explicit
ES Spain	"Corporate Governance Code of listed companies" (2014)	Spanish Corporate Governance Institute	Self-regulatory	2-Tier	comply or explain	Audit Committee	non-explicit
FR France	"Corporate governance code of listed corporations" (2016)	FFP/MEDEF	Self-regulatory	1-Tier	comply or explain	Audit Committee / Risk Committee	non-explicit
IT Italy	"Corporate Governance Code" (2015)	Corporate Governance Committee	Self-regulatory	1-tier / both	comply or explain	Control & Risk Committee	non-explicit
NL The Netherlands	"Corporate Governance Code" (2017)	Portuguese Corporate Governance Institute	Self-regulatory	both	comply or explain	Audit Committee / Risk Committee	explicit
PT Portugal	"Corporate Governance Code" (2017)	Portuguese Corporate Governance Institute	Self-regulatory	both	comply or explain	Monitoring Board	non-explicit
RO Romania	Code of Corporate Governance (2015)	Bucharest Stock Exchange (BVB)	Self-regulatory	both	comply or explain	Audit Committee	non-explicit
TR Turkey	Principles of Corporate Governance (2014)	Capital Markets Board (CMB)	Govt-promoted	1-Tier	comply or explain	Early Detection of Risk Committee	non-explicit
UK United Kingdom	UK Corporate Governance Code (2016)	Financial Reporting Council (FRC)	Self-regulatory	1-Tier	comply or explain	Audit Committee / Risk Committee	non-explicit
ZA South Africa	King Report on Corporate Governance for South Africa 2016 (2016)	Institute of Directors in Southern Africa (IoDSA)	Self-regulatory	1-Tier	apply and explain	Risk committee / Audit Committee	explicit
CN China	Guidelines for Corporate Governance in China (2011)	China Securities Regulatory Commission (CSRC)	Govt-promoted	2-Tier	comply or explain	Audit Committee	non-explicit
SG Singapore	Code of Corporate Governance (2012)	Monetary Authority of Singapore (MAS)	Govt-promoted	1-Tier	comply or explain	Audit Committee	non-explicit
US United States	Sarbanes-Oxley Act of 2002 (2002)	Securities and Exchange Commission (SEC)	Govt-promoted	1-Tier	comply or else	Audit Committee	non-explicit

Definitely, it seems that companies are not taking cybersecurity seriously.

Castillo de San Marcos

2015



Good news

a change of behaviour: the “*Cybersecurity Disclosure Act*”

114TH CONGRESS
1ST SESSION

S. 2410

To promote transparency in the oversight of cybersecurity risks at publicly traded companies.



Sen. J. Reed (D)



Sen. S. M. Collins (R)

2017



Good news

a change of behaviour: the “*Cybersecurity Disclosure Act*”

115TH CONGRESS
1ST SESSION

S. 536

To promote transparency in the oversight of cybersecurity risks at publicly traded companies.



Sen. J. Reed (D)



Sen. S. M. Collins (R)



Sen. M. R. Warner (D)



Sen. J. McCain (R)

2018



Good news

a change of behaviour: the “*Cybersecurity Disclosure Act*”

115TH CONGRESS
2D SESSION

H. R. 6638

To promote transparency in the oversight of cybersecurity risks at publicly traded companies.



Rep. J. Himes (D)



Rep. T. Rooney (R)



Rep. G. Meeks (D)



Rep. D. Heck (D)

a change of behaviour: the “*Cybersecurity Disclosure Act*”

13 (3) the term “information system”—

14 (A) has the meaning given the term in sec-
15 tion 3502 of title 44, United States Code; and

16 (B) includes industrial control systems,
17 such as supervisory control and data acquisition
18 systems, distributed control systems, and pro-
19 grammable logic controllers;





**Industrial
Cybersecurity 2018:**
Opportunities and challenges
in Digital Transformation

KASPERSKY

iTTi

Thank you very much!!!