



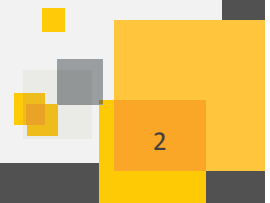
Facing Up to the Threats of Cyber Attacks in a 5G World

Zoltan Precsenyi CIPP/E, CIPM

Senior Manager Government Affairs EMEA

Agenda

1	What threats?
2	What security?
3	What EU policies?



Reminder: The 5G Vision

5G Vision

What 5G is about



Source: <http://ec.europa.eu/digital-agenda/en/towards-5g>

1	What threats?
2	What security?
3	What policies?



5G Vision

What 5G is about



Source: <http://ec.europa.eu/digital-agenda/en/towards-5g>

WEARABLES AND SELF-TRACKING DEVICES

A large and growing market...
...with big security problems

Surveillance

Data Breach

Stalking

Safety

Privacy

ID Theft

60%
US Adults
Self-Track
(Pew Research)



485 million

Wearable
Computing Devices
to Ship in 2018
(ABI Research)

SELF-TRACKING IS RISKY FOR USERS

Your digital footprint will be everywhere!



52%

Do not have a
privacy policy

20%

Login
credentials in
clear text

*(Apps that require
login)*

14

Domains
contacted by
apps

INSTALLING APPS ON ANDROID WEAR

ANDROID WEAR APPS ARE INSTALLED THROUGH A PAIRED ANDROID PHONE OR TABLET



#smartwatch



@threatintel | www.symantec.com

5G Vision

What 5G is about



Source: <http://ec.europa.eu/digital-agenda/en/towards-5g>

THE CONNECTED CAR

Symantec Has Demonstrated Numerous Vulnerabilities in Different Vehicles

RISK

Transmission Control Unit (TCU)
Engine Control Unit (ECU)



Telematics



Anti-Theft
System

On-Board
Diagnostic



Tire Pressure
Monitoring
Systems

Keyless
Entry



5G Vision

What 5G is about



Source: <http://ec.europa.eu/digital-agenda/en/towards-5g>

Security Community Blog

Hospitals Breached via Medical Devices?

By: **Brian Witten**  **SYMANTEC EMPLOYEE**

Created 24 Jun 2015

Of course, any PC in the hospital, just like your laptop, has countless defenses against such malware. Well-patched machines running effective, up-to-date anti-virus software are well protected against such malware and hacker attacks. Unfortunately though, for regulatory or policy reasons, hospitals are not allowed to patch medical devices, even medical devices running Windows or other commercial software. Similarly, hospitals are not allowed to install any additional software on these medical devices, even security software essential for protection. The original logic stems from good reason. Medical equipment, including its software, must undergo formal testing and be determined safe for patients. Changing the software in any way, including patches, or adding software without explicit approval by the manufacturer can change the behavior of the device in ways that could endanger patients. For such reasons, regulatory restrictions prohibit tampering with medical equipment, even if the tampering is intended to protect the equipment and ultimately protect the patients.

5G Vision

What 5G is about

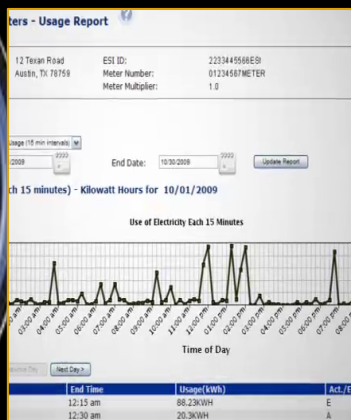


Source: <http://ec.europa.eu/digital-agenda/en/towards-5g>

FUTURE OF ELECTRICITY: SMART METERS/SMART GRID

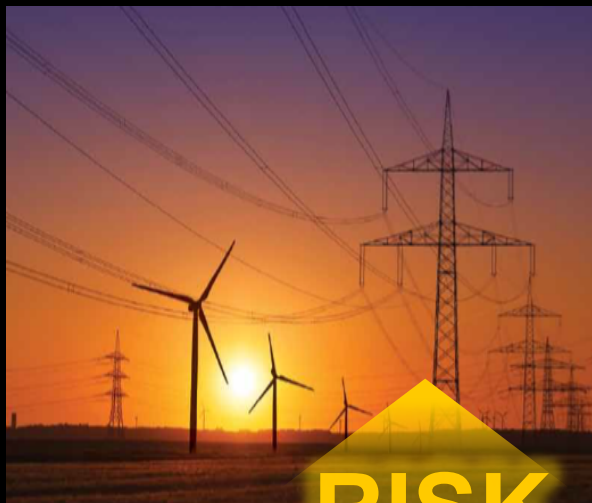
Millions of connected (critical) things – including SCADA Control Systems

RISK



Known unknowns:

- Vulnerabilities and cross-vulnerabilities
- Time and process to develop patches
- Time and process to deploy patches
- Threat propagation patterns
- Resilience of failover solutions
- Real risk of systemic failure



RISK



The Overall Threat Landscape

Attackers Moving Faster



5 of 6
large
companies
attacked



317M
new
malware
created



1M
new
threat
s daily



60% of
attacks
targeted
SMEs

Digital extortion on the rise



113%
increase in
ransomware



45X
more
devices
hostage

Malware gets smarter



28% of malware
was Virtual
Machine Aware

Zero-Day Threats



24
all-
time
high



Top 5
unpatched
for **295**
days

Many Sectors Under Attack



Healthc
are
+ 37%



Retail
+11%



Education
+10%



Govern
ment
+8%



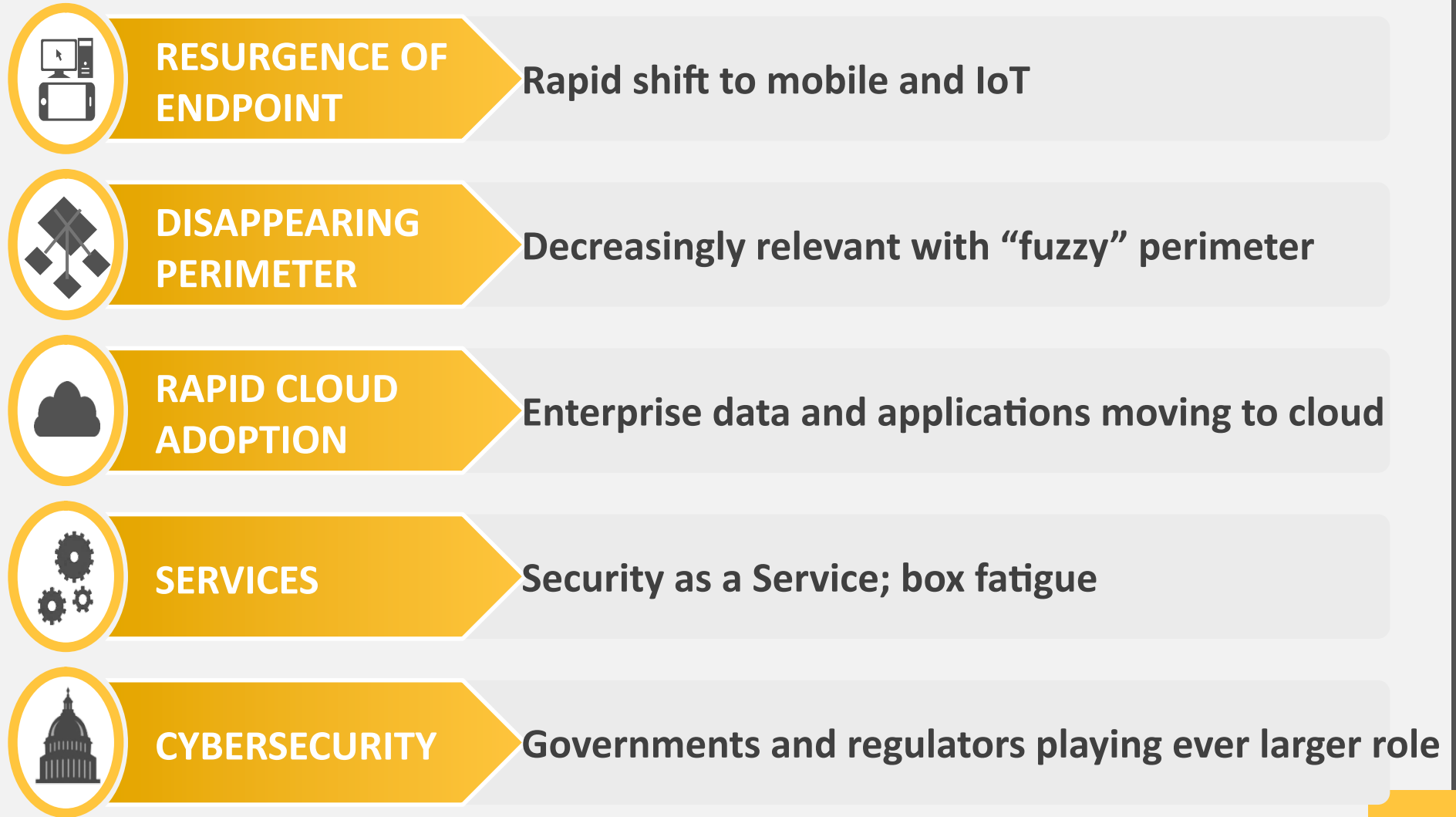
Financial
+6%

Source: Symantec Internet Security Threat Report 2015

Copyright © 2015 Symantec Corporation

1	What threats?
2	What security?
3	What policies?

Key Trends Reshaping the Enterprise Security Market



Symantec Enterprise Security | TECHNOLOGY STRATEGY



Cyber Security Services

Monitoring, Incident Response, Simulation, Adversary Threat Intelligence

Threat Protection



ENDPOINTS



DATA
CENTER



GATEWAYS

- Advanced Threat Protection Across All Control Points
- Built-In Forensics and Remediation
- Integrated Protection On-Premise, Virtual, and Cloud
- Cloud-based Mgmt for Endpoints, Datacenter, Gateways

Information Protection



DATA



IDENTITIES

- Integrated Data and Identity Protection
- Cloud Security Broker for Apps
- User and Behavioral Analytics
- Cloud-based Encryption and PKI



Unified Security Analytics Platform



Log and
Telemetry
Collection



Integrated
Threat and
Behavioral
Analysis



Unified Incident
Management and
Customer Hub

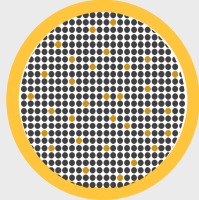


Inline Integrations
for Closed-loop
Actionable
Intelligence



Regional and
Industry
Benchmarking

Symantec Enterprise Security | **UNIQUE VISIBILITY**



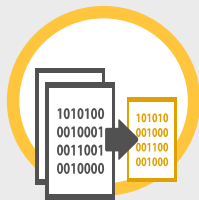
175M
endpoints



57M attack
sensors in **157**
countries



182M web
attacks blocked
last year



3.7T
rows of telemetry

100 Billion
more/month



30% of world's
enterprise email
traffic scanned/day

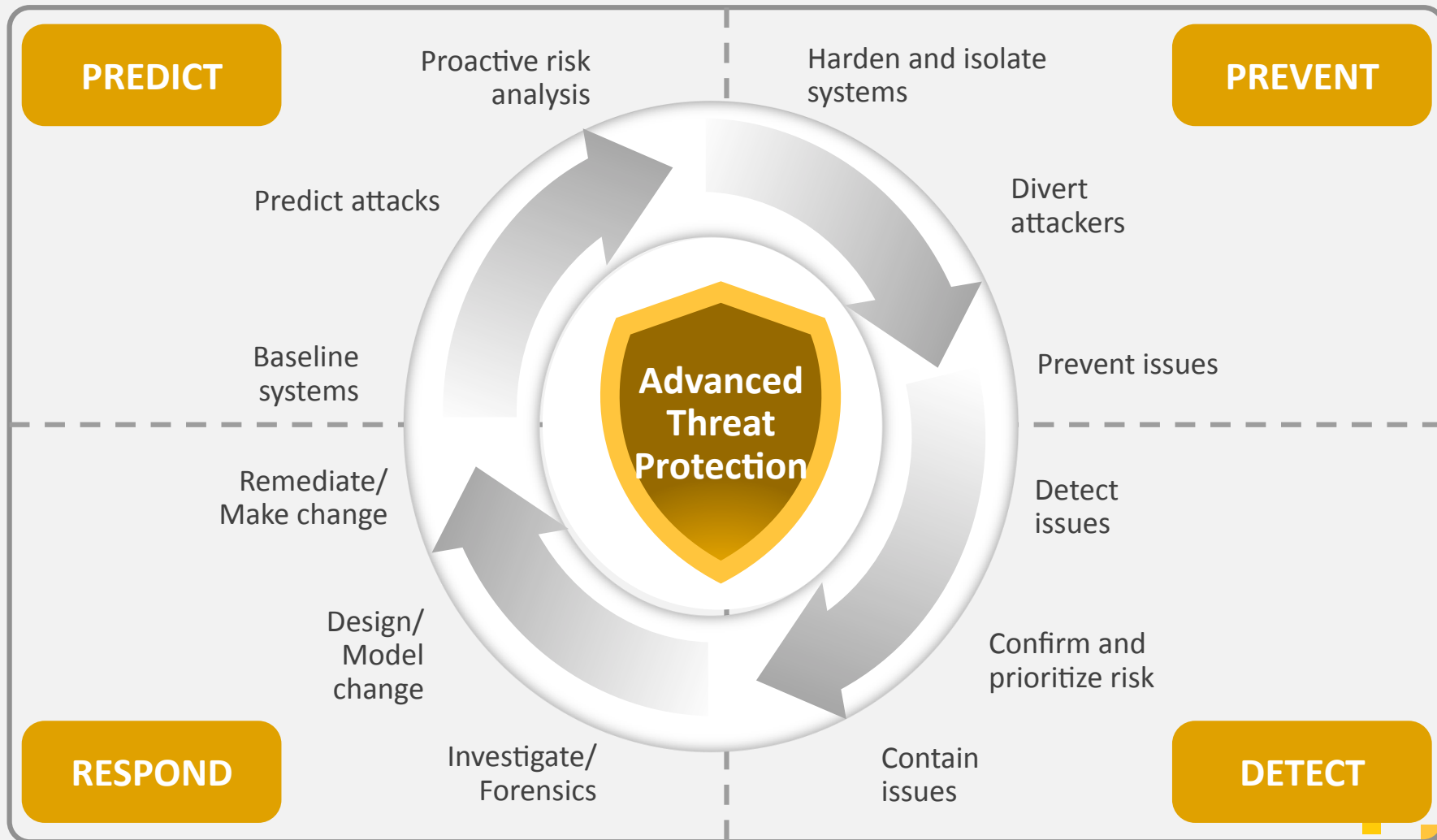
1.8 Billion
web requests



9
response centers

500+
rapid security response team

Threat Protection Requirements | **FULL THREAT LIFE-CYCLE**



Source: Gartner

Copyright © 2015 Symantec Corporation

1

What threats?

2

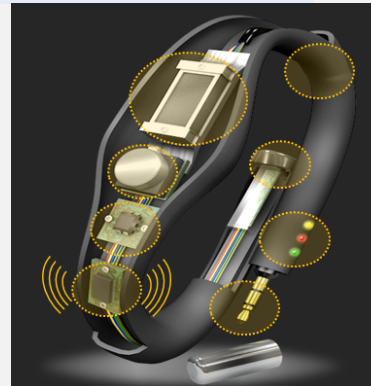
What security?

3

What public policies?

Security must be built into 5G upfront

- **5G Security is about:**
 - Identities
 - Information
 - Infrastructure
- **5G Security must be:**
 - By Design
 - Embedded
 - End-to-End
 - 24/7/365
- **5G Security will require:**
 - More data collection and processing
 - Automated processing and decision making
 - Uninterrupted international data flows



What regulatory framework?

- **Privacy Law:**

- GDPR will have **enhanced security** provisions.



- But only **personal data** is covered.

What regulatory framework?

- **Telecom Framework:**

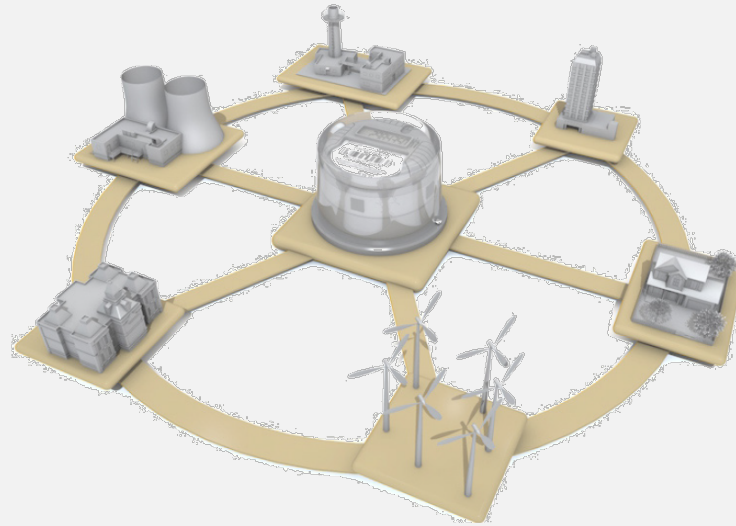
- Network **security and resilience** are covered.



- But only applies to **publicly available networks**.

What regulatory framework?

- **NIS Directive:**
 - Risk management, incident response are in.



- But only a limited set of sectors is covered.

What regulatory framework?

- **eIDAS Regulation:**

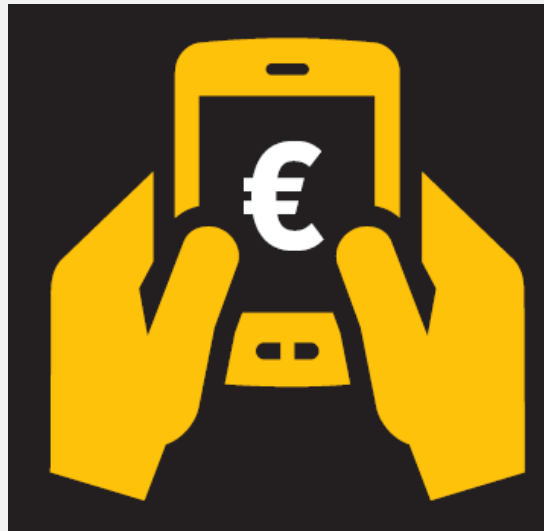
- Risk management, incident response, reporting are dealt with.



- But novel trust services are likely to emerge.

What regulatory framework?

- **Payment Services Directive:**
 - **Enhanced security rules** coming for e-, m- and online payments.



- But these won't cover **non-monetary transactions**.

What regulatory framework?

- **E-Commerce Directive:**
 - Still a **sound legal basis** for e-commerce in general.



- But the **liability regime for online content** won't be relevant or suitable to many IoT applications of 5G.

What regulatory framework?

- **New or recast legislation might be necessary at some point.**
 - Loads of **consultations** are underway.
 - Now is the time to **brainstorm**.

LET'S BE CREATIVE!





Thank you!

Zoltan Precsenyi CIPP/E, CIPM

zoltan_precsenyi@symantec.com

Copyright © 2015 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.