Cybersecurity in Catalonia

September 2018

Technology Snapshot

Catalonia Trade & Investment

Generalitat de Catalunya
Government of Catalonia

Cybersecurity in Catalonia: Technology Snapshot

Catalonia Trade & Investment
Government of Catalonia

Elaborated by
sOwlers

Coordination and Supervision
Catalonia Trade & Investment. Strategy and Competitive Intelligence Unit

Collaboration
Secretary for Telecommunications, Cibersecurity and Digital Society

Barcelona, September 2018

Contents

1. Definition of Cybersecurity and Its Importance for Industry

Definition of Cybersecurity

WHAT IS CYBERSECURITY?

Cybersecurity includes the set of physical, logical and administrative measures taken to digitally protect companies, people and systems from digital attacks against their devices, applications and data that could compromise the confidentiality, availability and/or integrity of their data.

WHAT DOES IT CONSIST OF?

Cyber-physical systems equipped with Internet technology require reliable concepts and technologies to guarantee the security, privacy and protection of the data they contain. **Reliable, secure communications** are therefore crucial, along with a sophisticated identity and machine access control systems.

These cyber-physical systems and communications are used to define and implement different layers and levels of protection while preventing attacks and increasing system resilience. A combination of different measures can therefore be used to effectively prevent and mitigate attacks.

HOW IMPORTANT IS IT?

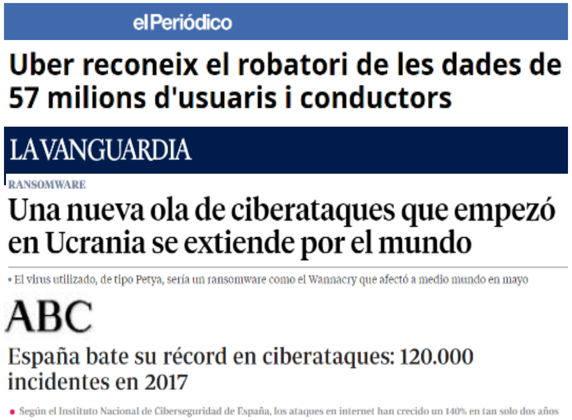
Today's companies have a strong digital presence, largely due to public exposure on the Internet and the use of computer systems to manage data and internal processes. Companies' inability to effectively protect themselves against new threats exposes them to the loss of confidential information, a negative public reaction to their brand and not being able to run their own business, not to mention infringing specific laws such as the new data protection regulation, which includes severe sanctions for infringement.

Source: Industry 4.0 Mapping and Palo Alto Networks.

The Importance of Cybersecurity to Industry

CYBERCRIME IS ON THE RISE:

- The global cost of cybercrime was $6 trillion in 2017, considerably higher than the 2016 figure of $3 trillion.
- 49% of Spanish senior executives acknowledge that their companies lack a comprehensive cybersecurity strategy.
- Because of cyberattacks, companies are forced to stop operations for an average of 17 hours a year.
- In 2017, 29.4% of user devices suffered at least one cyberattack.



elPeriódico

Uber reconeix el robatori de les dades de 57 milions d'usuaris i conductors

LA VANGUARDIA

RANSOMWARE

Una nueva ola de ciberataques que empezó en Ucrania se extiende por el mundo

• El virus utilizado, de tipo Petya, sería un ransomware como el Wannacry que afectó a medio mundo en mayo

ABC

España bate su récord en ciberataques: 120.000 incidentes en 2017

• Según el Instituto Nacional de Ciberseguridad de España, los ataques en internet han crecido un 140% en tan solo dos años

MAIN NEGATIVE IMPACTS OF A CYBERATTACK FOR COMPANIES:

- 40% of cyberattacks force operations and invoicing to be interrupted
- 39% involve the loss of confidential information
- 32% have a negative impact on product quality
- 29% of cyberattacks cause damage to hardw are
- 22% cause damage to human life

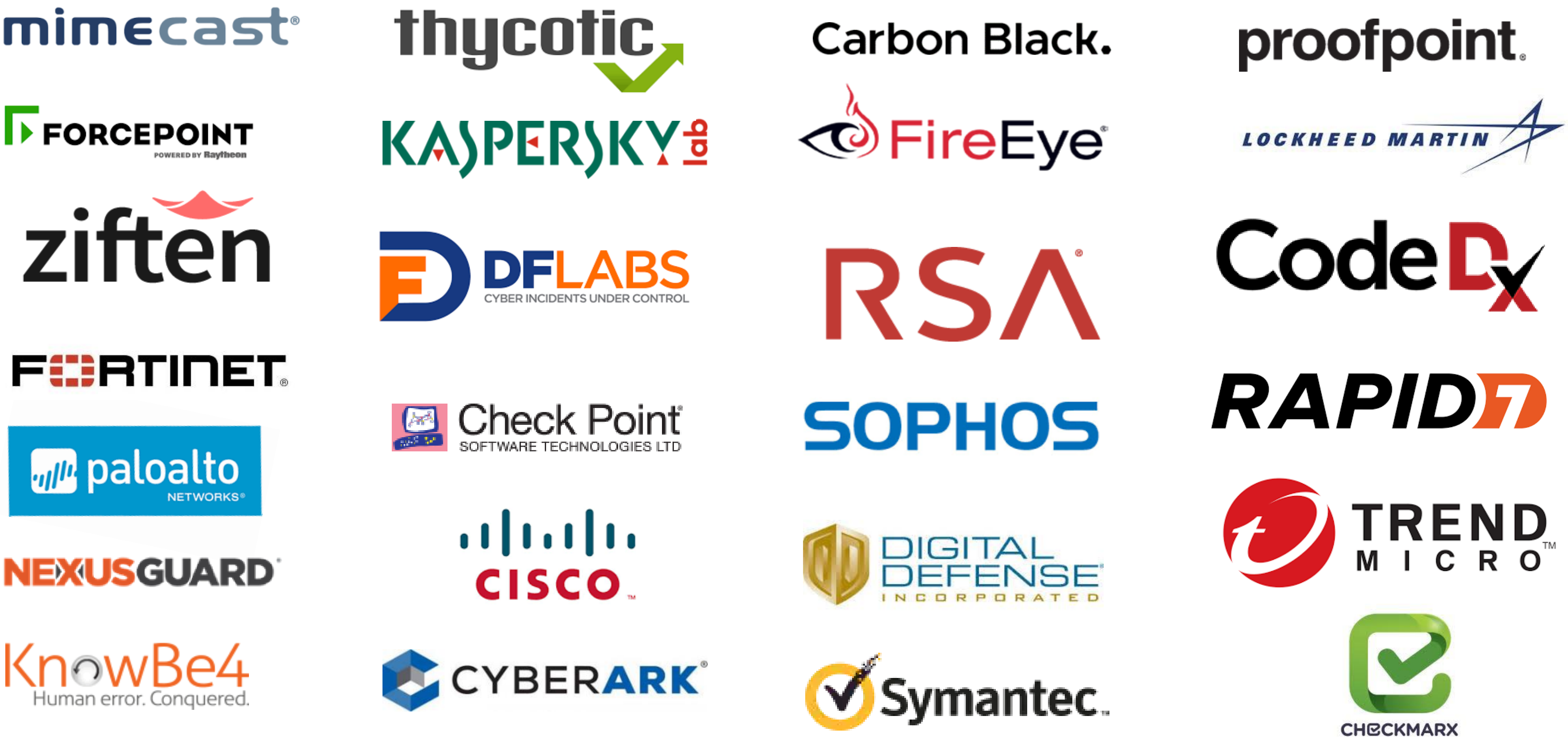
MOST COMMON WAYS USED BY CYBERCRIMINALS TO MAKE MONEY:

- Cloning credit cards
- Bank transfers
- Insurance and medical services fraud
- Internet identity theft for commercial purposes
- Crime as a service and pay per installs (PPI)
- Theft of cryptocurrencies
- Sale of information to third parties: intellectual property and confidential information

Source: Industry 4.0 Mapping and Palo Alto Networks; Press items and Raconteur.net

2. Key Global Dimensions

World's Leading Companies in Cybersecurity



Note: The use of these trademarks is for informative purposes only. Trademarks mentioned in this document are the registered trademarks of the companies to which they belong and are not owned by ACCIÓ. This is a partial and illustrative representation of companies that form part of the cybersecurity ecosystem in Catalonia; however, there may exist other companies that have not been included in the study.

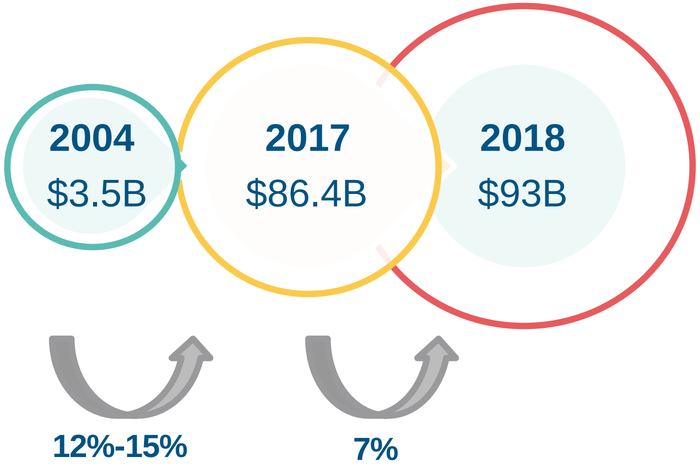
Source: Cybersecurity Ventures.

World Cybersecurity Market

SIZE OF THE CURRENT MARKET

In 2004, the global cybersecurity market was valued at $3.5 billion. **By 2017**, it had reached the figure of $86.4 billion, which represents annual growth of between 12% and 15%. **In 2018**, it is expected to increase to $93 billion.

However, this market is concentrated in very few countries, particularly the United States and, in Europe, the United Kingdom.



EXPECTED DATA

Cybercrime is on the rise

Total global spending on cybersecurity in the 2017-2021 period is expected to amount to $1 trillion.

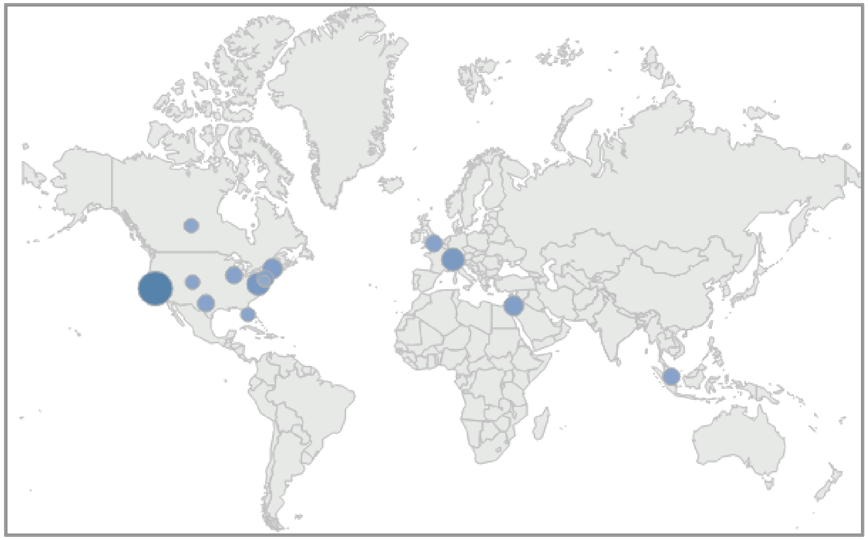
Also of note is that the global spend on user training and awareness raising on how to recognize and defend against cyberattacks is expected to amount to $10 billion by 2027.

It is also becoming increasingly more difficult to know how much companies spend on cybersecurity because this information is highly sensitive.

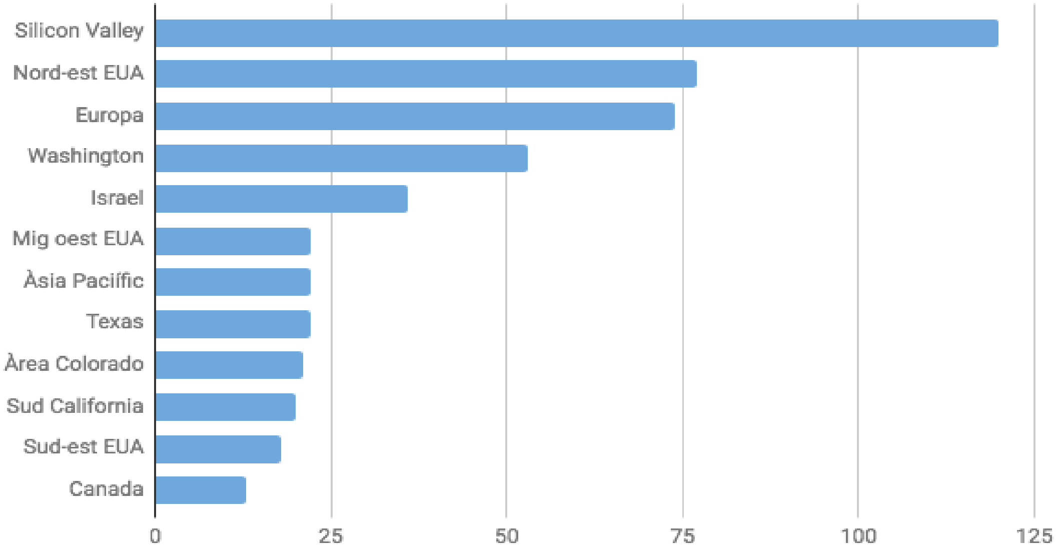
Source: Gartner Statistics / ACCIÓ / Cybersecurity Ventures

Important World Regions and Hubs

The cybersecurity market is concentrated in very few countries. In particular, in the United States, there are several top hubs, including Silicon Valley (24% of global share), the Northeast, which includes New England, New York and New Jersey (15%), and Washington, D.C. (10%). Outside the United States, the United Kingdom stands out with a 5% share of the sector (32% of European companies), as does Israel with 7%.



Number of cybersecurity hubs



Source: Cybersecurity Ventures.

3. Cybersecurity in Catalonia

Main Mapping Conclusions

Cybersecurity in Catalonia

352 companies

5,898 employees work in cybersecurity

€806 million in turnover directly related to cybersecurity

Cybersecurity accounts for 0.36% of Catalan GDP

37.5% of companies are less than 10 years old

95% of companies are SMEs

41.5% of companies recorded turnover of more than €1 million and 49% recorded turnover of less than €500,000

6.5% of companies have an affiliate company abroad

35% of companies are exporters

Font: Authors' own data based on Orbis, INCIBE, ACCIÓ directories and Barcelona & Catalonia Start-up Hub. For company turnover and employee data, estimates were made based on company business lines.

The Cybersecurity Ecosystem in Catalonia

* Partial illustrative table

Technology and research centres

i2cat, CD6, eurecat, CVC, CYBER[]CAT, easy, ICFO The Institute of Photonic Sciences, CTTC

Technology parks

TecnoCampus, La Salle

Knowledge providers (research groups and institutes)

Crises, ISG Information Security Group – Universitat Politècnica de Catalunya, Institut d'Investigació en Intel·ligència Artificial – IIIA

Company incubators

Barcelona Activa

Technology transfer

otri

Universities

Universitat Rovira i Virgili, UPC, UAB, UOC Universitat Oberta de Catalunya, Universitat de Lleida, upf.

COMPANIES

indra, semic, DELL EMC, panda, EY, 4id, LOGICALIS, Scytl, ABAST, NECSIA, MICRO BR, víntegris, THALES, hp, SIDE, accenture, SIEMENS, T-Systems, it now, avanade, IBM, LOGITEK, IThink, OMEGA Peripherals, LightEyes, VALORA DATA, exoClick, ca technologies, ID Grup, Informática El Corte Inglés, grupo SIRT, Deloitte., GRUPO SPEC, IMPALA network solutions, DSA, minsait, TÜV Rheinland, evollum, Red Points, S21 sec, SAFELAYER, Applus+, Iteuve, dimension data, SATINFO, gmv, firmaprofesional, FLYTECH, davinci, castinfo, DIAGONAL INFORMATICA, icar, nexica, NexTReT, internet security auditors, SPAMINA, zemsania Global Group, gemalto, Concatel, zhilabs, TechData, microblau, a2secure, a3kcent cybersecurity, digital dimension, advancegroup_, Bitdefender, open3s, Kimaldi, swhosting, herta, sayoscarrera global IT engineers, MAZARS, dagram, claranet

START-UPS

redcorus., bioaccez controls, blueliv, CDE, FileCircles File Transfer Analytics, MEDIATG, ID, Talaia, biid Your Mobile ID, a3kcent cybersecurity, boonder, xairk, elebia., ECOBAM, DrS, openprovider, Certifydoc, tranxfer, Altanetica, Atlantis, Konodrac, VD, herta, ncrumbs, e-movilia, Cellcrypt, ADRENALINA marketing digital

Public administration

ACCIÓ, Generalitat de Catalunya, apdcat, cesicat, AOC Consorci Administració Oberta de Catalunya, Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació, CATCert Agència Catalana de Certificació

EU/SP entities

enisa, NESSI, red.es, España, E-Sec, incibe, ens Esquema Nacional de Seguridad, CCN

Professional associations

SINERGIA, AMETIC, ciac, Associació de Professionals TIC de Catalunya

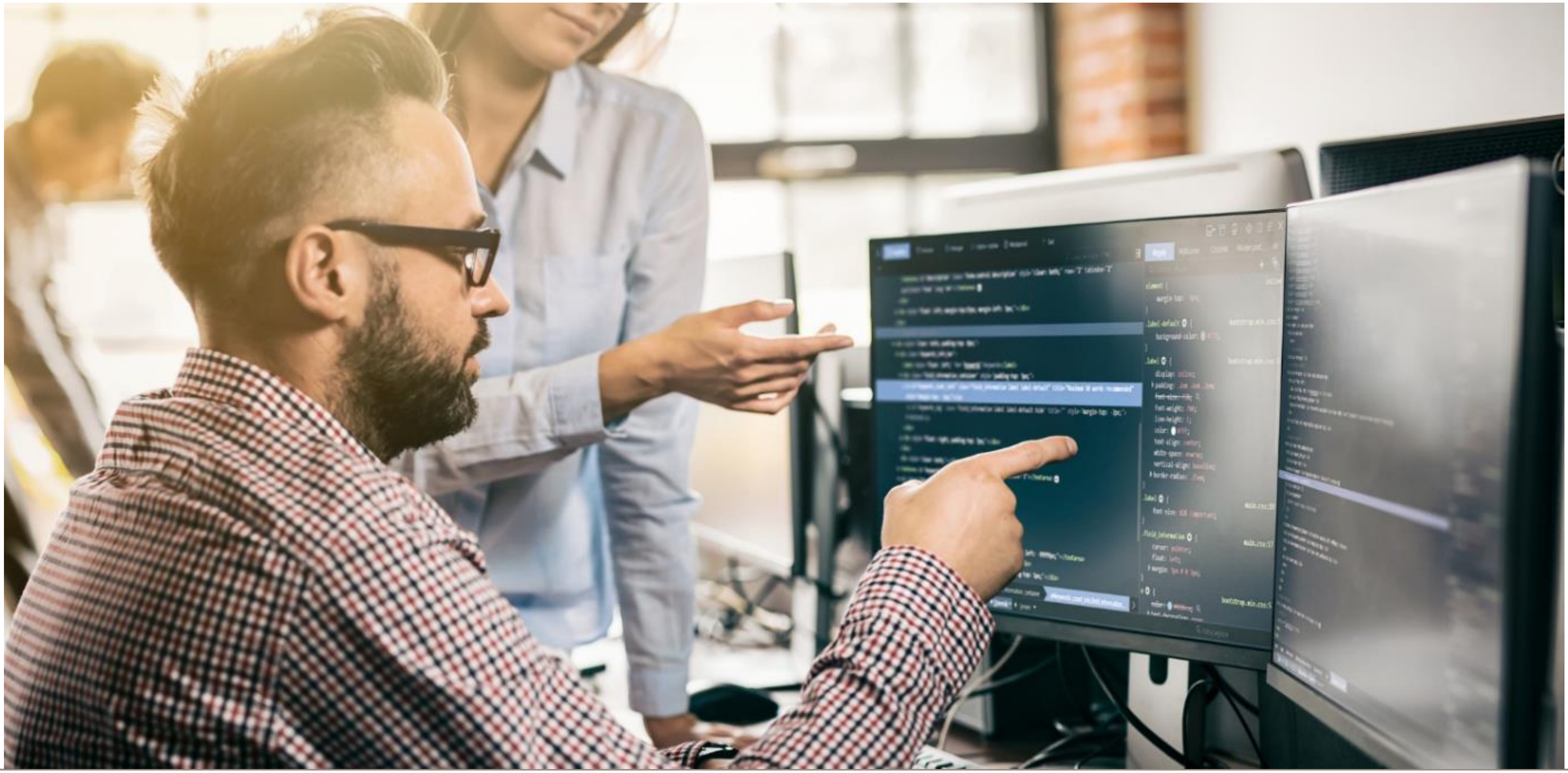
CSIRT/CERT

CSUC, cesicat, ESCERT, CaixaBank, Ingenia, mossos d'esquadra

Note: The use of these trademarks is for informative purposes only. Trademarks mentioned in this document are the registered trademarks of the companies to which they belong and are not owned by ACCIÓ.
This is a partial and illustrative representation of companies that form part of the cybersecurity ecosystem in Catalonia; however, there may exist other companies that have not been included in the study.

Source: ACCIÓ, Barcelona & Catalonia Start-up Hub

4. Trends and Applications by Demand Sector



Key Cybersecurity Trends

According to a study by the University of Barcelona and the EY consulting firm published in *Business Insights*, **60% of Catalan companies invest in cybersecurity.** Likewise, 83% of companies acknowledge that they are immersed in the digital transformation process. Cybersecurity is the top priority of Catalan companies within their own digital transformation process.

An increasingly more digital and connected **globalized society** generates huge amounts of data.

Cybersecurity trends are based on the impact of ICTs on today's society

A new generation of components and systems: **The Internet of Things**

The future Internet: new 5G architecture, cloud and fog computing, and critical services

The digital transformation of industry, sensorization, robotics and intelligence, the concept of **Industry 4.0**

The power of data: **big data and artificial intelligence**

Advanced computing and **Cloud Computing**

Facilitating technologies through innovations in **quantum photonics and nano-electronics**

A new, more secure computing and encryption system: **quantum security**

Cyberthreats are a trend on the rise that can affect any kind of **industrial company**. The advances that have driven productivity and business efficiency are also what have made organizations vulnerable to cyberattacks.

The following factors are behind this massive growth in the cybersecurity market:

Industrial Trends Requiring Cybersecurity

Threat complexity is increasing steadily and rapidly

Production chains are becoming increasingly **more interconnected**

The trend is for **greater transparency and access to company information**

Digitalization processes and online migration are delving deeper into companies and institutions

The **use of cyber-physical systems** in production that are susceptible to cyberattacks

Font: Authors' own data / Industry 4.0 Mapping / Business Achievers

Recent Applications by Demand Sector (I)

Industry

Industry: Smart Grids, Industry 4.0, Critical Infrastructure, Utilities

- Resilient cyber-systems for critical infrastructure
- Cybersecurity in industrial control systems: ICS/SCADA
- Protection of industrial networks
Smart Grids

Mobility

Transport and Communications: Smart cars, aviation, satellites

- Security of self-driving and connected vehicles
- Security and protection of unmanned aerial vehicles (drones)
- Protection of satellite communication systems

Financial services

Finance and Insurance: Online banking, fintech

- Big Data Analytics: detection of banking and insurance fraud
- Security information and event management (SIEM)
- Services security
Fintech

Health

Healthcare and Pharmacy: eHealth, Pharmacy

- Protection of connected medical devices
- Encryption for medical and pharmaceutical research
- Secure storage of medical data

Source: INCIBE

Recent Applications by Demand Sector (II)

Education

Training: training on security, employment, e-learning

Cyber-education and cybersecurity labs

Government

Public administration: e-government, defence and participation

Distribution of cyber intelligence

Simulation of incidents and cyber-exercises

ICTs

Digitalization: The Internet of Things, cloud computing, security services

Security services in the cloud

Real-time encryption

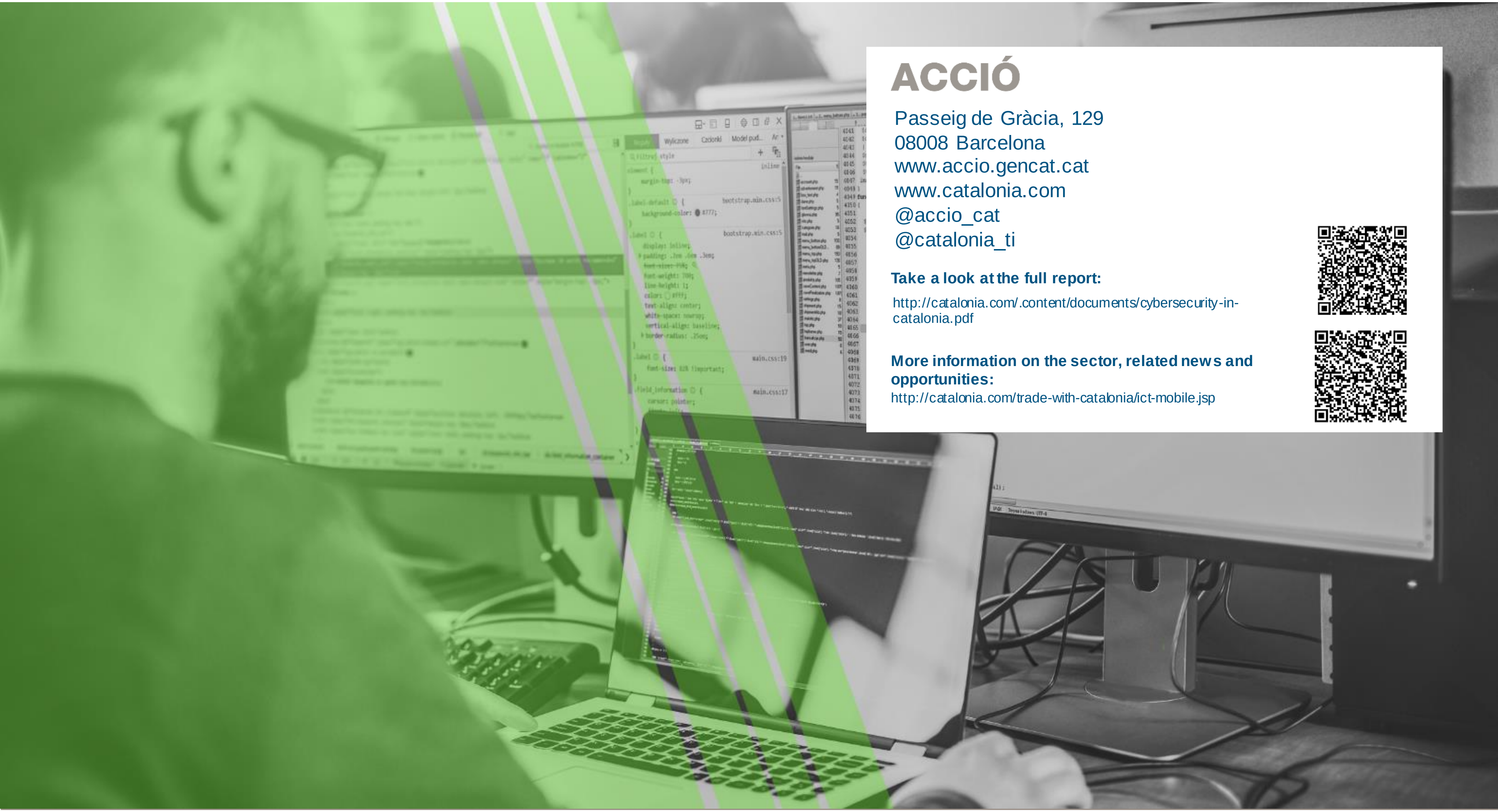
Homomorphic encryption

Ethical hacking

The Internet of Things

Certificate of digital trust

Source: INCIBE



ACCIÓ

Passeig de Gràcia, 129
08008 Barcelona
www.accio.gencat.cat
www.catalonia.com
@accio_cat
@catalonia_ti

Take a look at the full report:

http://catalonia.com/.content/documents/cybersecurity-in-catalonia.pdf

More information on the sector, related news and opportunities:

http://catalonia.com/trade-with-catalonia/ict-mobile.jsp

Catalonia Trade & Investment

Generalitat de Catalunya
Government of Catalonia