Applying Privacy by Design as a Strategy to Reduce Your Attack Surface

Chuck Georgo, NOWHERETOHIDE.ORG

IJIS Institute National Symposium – January 23/24, 2019

You want me to be a good CISO?

SANS MANAGEMENT

CYBER LEADER

CURRICULUM

Get the right training to build and lead a world-class security team.

FOUNDATIONAL

MGT512
SANS Security Leadership Essentials for Managers with Knowledge Compression™
GSLC

MGT414
SANS Training Program for CISSP® Certification
GISP

SEC566
Implementing and Auditing the Critical Security Controls – In-Depth
GCCC

MGT525
IT Project Management, Effective Communication, and PMP® Exam Prep
GCPM

CORE

MGT514
IT Security Strategic Planning, Policy, and Leadership

MGT415
A Practical Introduction to Cybersecurity Risk Management

NEW
MGT517
Managing Security Operations: Detection, Response, and Intelligence

LEG523
Law of Data Security and Investigations
GLEG

SPECIALIZATION

AUD507
Auditing & Monitoring Networks, Perimeters, and Systems
GSNA

MGT433
Securing the Human: How to Build, Maintain, and Measure a High-Impact Awareness Program

MGT305
Technical Communication and Presentation Skills for Security Professionals

SANS

Security Leadership

POSTER

CISO Mind Map
Version 1.0

AND

Security Operations Center (SOC) Essential Functions

For Cyber Leaders of Today and Tomorrow

sans.org/curricula/management

CISO MIND MAP

Security Operations

□ Prevention
- Data Protection
  - Encryption, PKI, TLS
  - Data Loss Prevention (DLP)
  - Email Security
- Network Security
  - Firewall, IDS/IPS, Proxy Filtering
  - VPN, Security Gateway
  - DDoS Protection
- Application Security
  - Threat Modeling
  - Design Review
  - Secure Coding
  - Static Analysis
  - Web App Scanning
  - WAF, RASP
- Endpoint Security
  - Antivirus, Anti-malware
  - HIDS/HIPS, FIM
  - App Whitelisting
- Secure Configurations
- Active Defense
- Patching

□ Detection
- Log Management/SIEM
- Continuous Monitoring
- Network Security Monitoring
- NetFlow Analysis
- Advanced Analytics
- Threat Hunting
- Penetration Testing
- Red Team
- Vulnerability Scanning
- Human Sensor
- Data Loss Prevention (DLP)
- Security Operations Center (SOC)
- Threat Intelligence
- Threat Information Sharing
- Industry Partnerships

□ Response
- Incident Handling Plan
- Breach Preparation
- Tabletop Exercises
- Forensic Analysis
- Crisis Management
- Breach Communications

Legal and Regulatory

□ Compliance
- PCI
- SOX
- HIPAA
- FFIEC, CAT
- FERPA
- NERC CIP
- NIST SP 800-37 and 800-53

□ Privacy
- Privacy Shield
- EU GDPR

□ Audit
- SSAE 16
- SOC 2
- ISO 27001
- FISMA and FedRAMP
- NIST SP 800-53A
- COSO

□ Investigations
- eDiscovery
- Forensics

□ Intellectual Property Protection

□ Contract Review

□ Customer Requirements

□ Lawsuit Risk

Business Enablement

□ Product Security
- Secure DevOps
- Secure Development Lifecycle
- Bug Bounties
- Web, Mobile, Cloud AppSec

□ Cloud Computing
- Cloud Security Architecture
- Cloud Guidelines

□ Mobile
- Bring Your Own Device (BYOD)
- Mobile Policy

□ Emerging Technologies
- Internet of Things (IoT)
- Augmented Reality (AR)
- Virtual Reality (VR)

□ Mergers and Acquisitions
- Security Due Diligence

CYBER LEADER

Identity and Access Management

□ Provisioning/Deprovisioning

□ Single Sign On (SSO)

□ Federated Single Sign On (FSSO)

□ Multi-Factor Authentication

□ Role-Based Access Control (RBAC)

□ Identity Store (LDAP, ActiveDirectory)

Risk Management

□ Risk Management Frameworks

□ Risk Assessment Methodology

□ Business Impact Analysis

□ Risk Assessment Process

□ Risk Analysis and Quantification

□ Security Awareness

□ Vulnerability Management

□ Vendor Risk Management

□ Physical Security

□ Disaster Recovery (DR)

□ Business Continuity Planning

□ Cyber Insurance

□ Policies and Procedures

□ Risk Treatment
- Mitigation Planning, Verification
- Remediation, Cyber Insurance

Governance

□ Strategy

□ Business Alignment

□ Risk Management

□ Program Framework
- NIST CSF
- ISO 27000

□ Control Frameworks
- NIST 800-53
- Critical Security Controls (CSC)

□ Program Structure

□ Program Management

□ Communications Plan

□ Roles and Responsibilities

□ Workforce Planning

□ Resource Management

□ Data Classification

□ Security Policy

□ Creating a Security Culture

□ Security Training
- Awareness Training
- Role-Based Training

□ Metrics and Reporting

□ IT Portfolio Management

□ Change Management

□ Board Communications

Leadership Skills

□ Business Strategy

□ Industry Knowledge

□ Business Acumen

□ Communication Skills

□ Presentation Skills

□ Strategic Planning

□ Technical Leadership

□ Security Consulting

□ Stakeholder Management

□ Negotiations

□ Mission and Vision

□ Values and Culture

□ Roadmap Development

□ Business Case Development

□ Project Management

□ Employee Development

□ Financial Planning

□ Budgeting

□ Innovation

□ Marketing

□ Leading Change

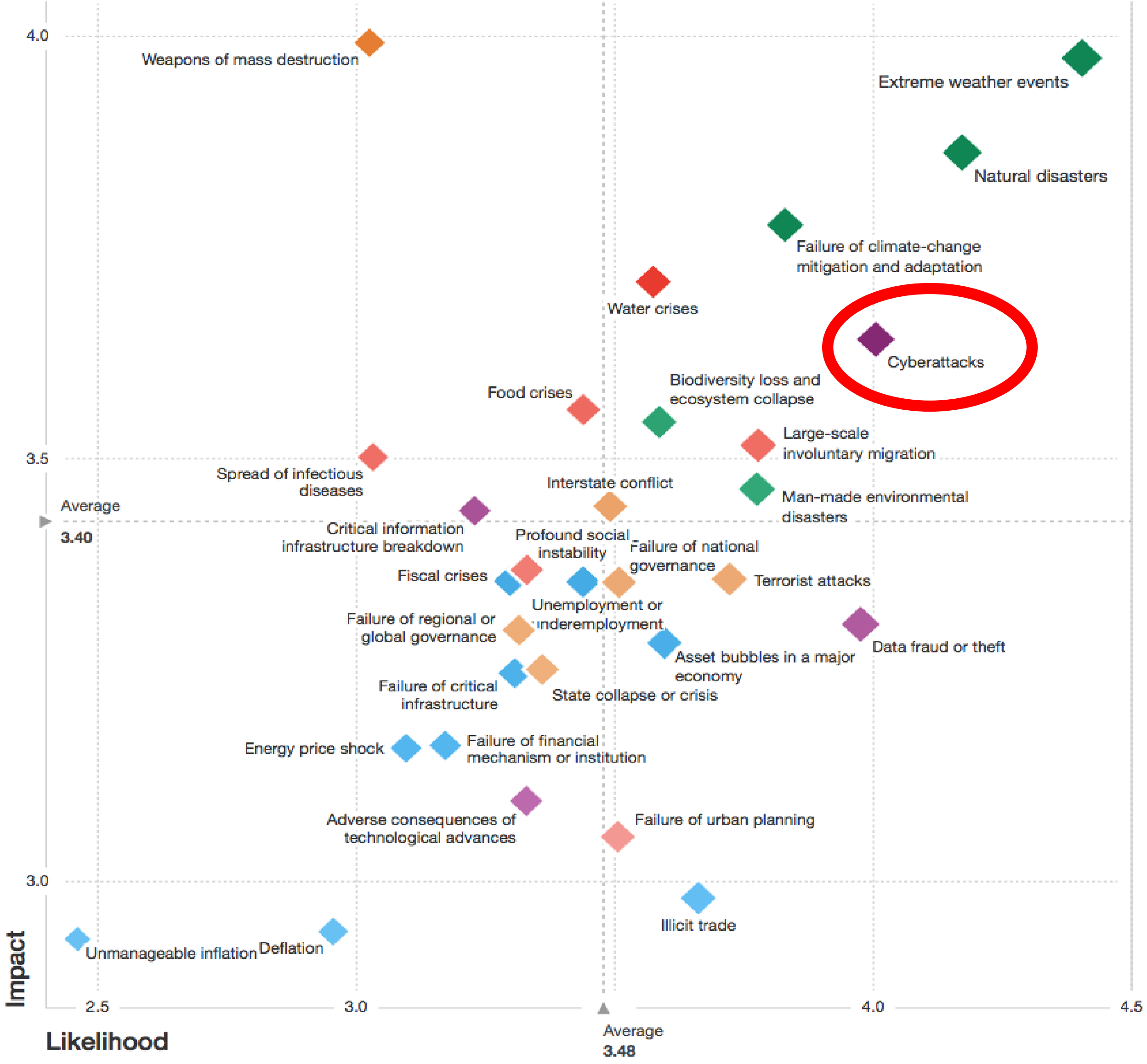
□ Customer Relationships

□ Team Building

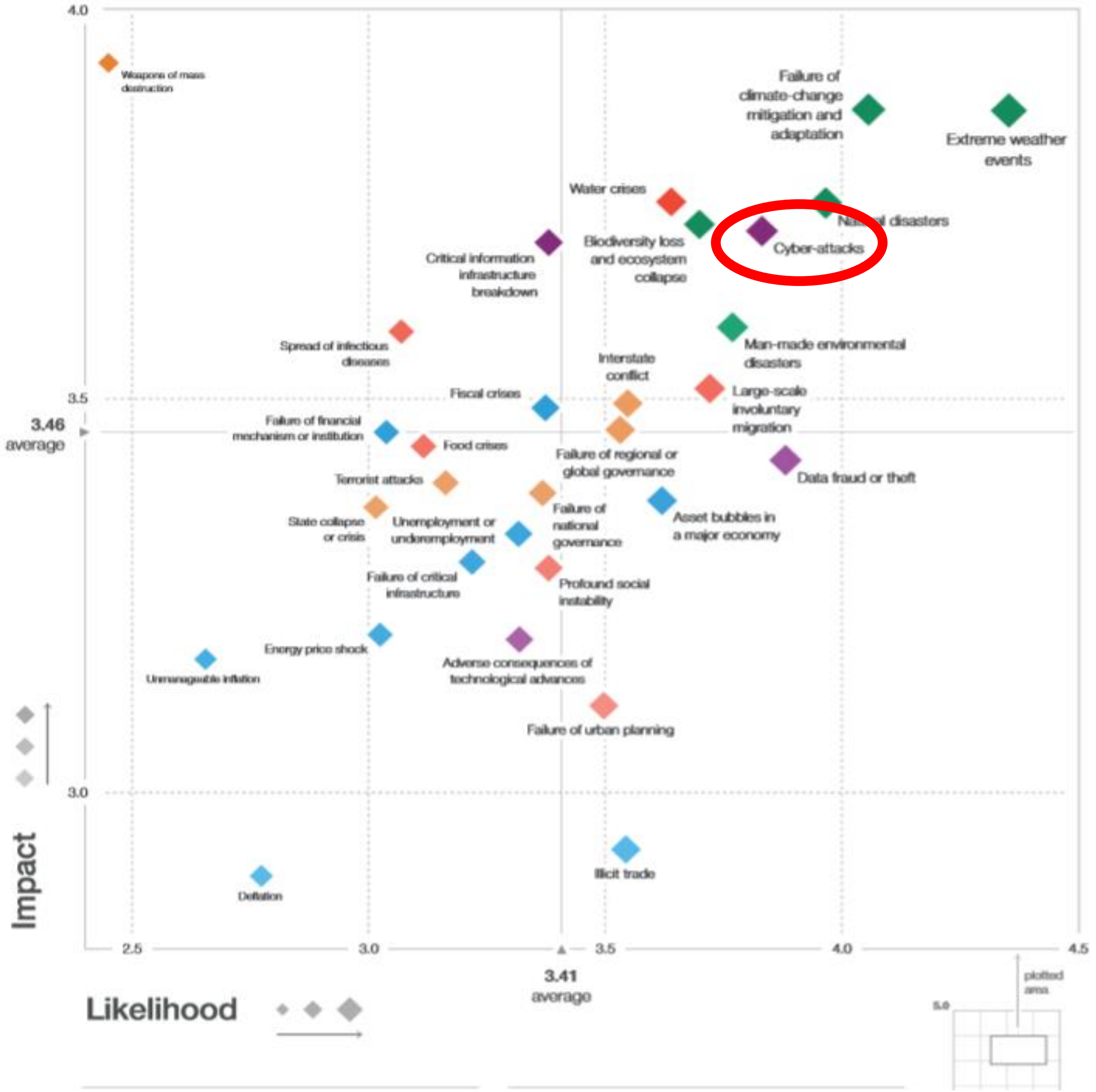
□ Mentoring

Based on CISO MindMap by Rafeeq Rehman @rafeeq_rehman http://rafeeqrehman.com Used with permission.

Global Risks Report 2018
World Economic Forum



Global Risks Report 2019
World Economic Forum



Number of users on the internet is blowing up

Sizing Legend

□ = 5M Internet Users

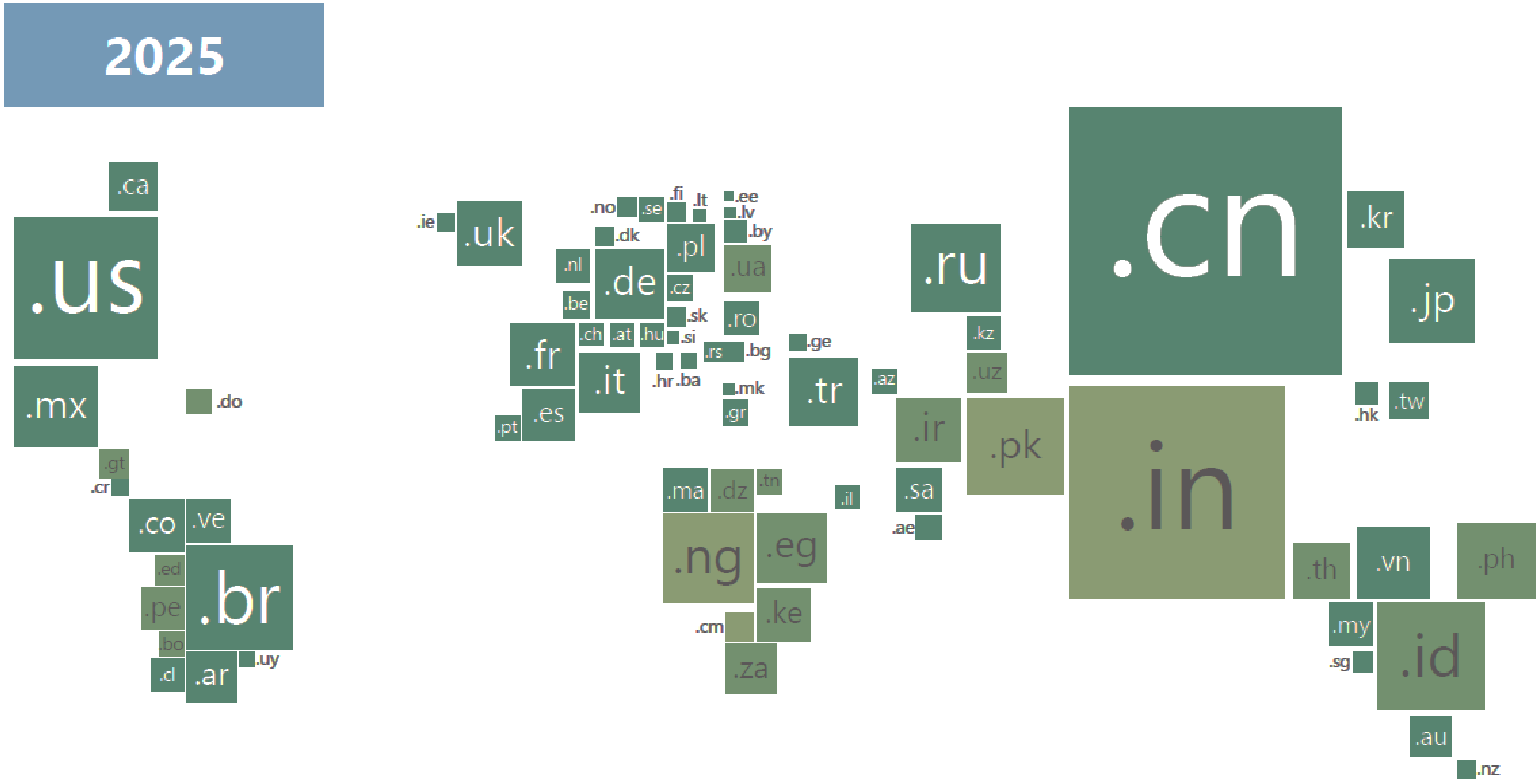
□ = 10M Internet Users

Percent Penetration of Internet Users

🟩	🟩	🟩	🟩	🟩
0-20	21-40	41-60	61-80	81-100

Number of Internet Users

	Brazi	China	France	Germany	India	Japan	Mexico	Nigeria	Russia	USA
2015	127M	751M	54M	72M	283M	109M	68M	66M	90M	287M
2025	173M	1.1B	62M	74M	708M	111M	106M	126M	124M	317M

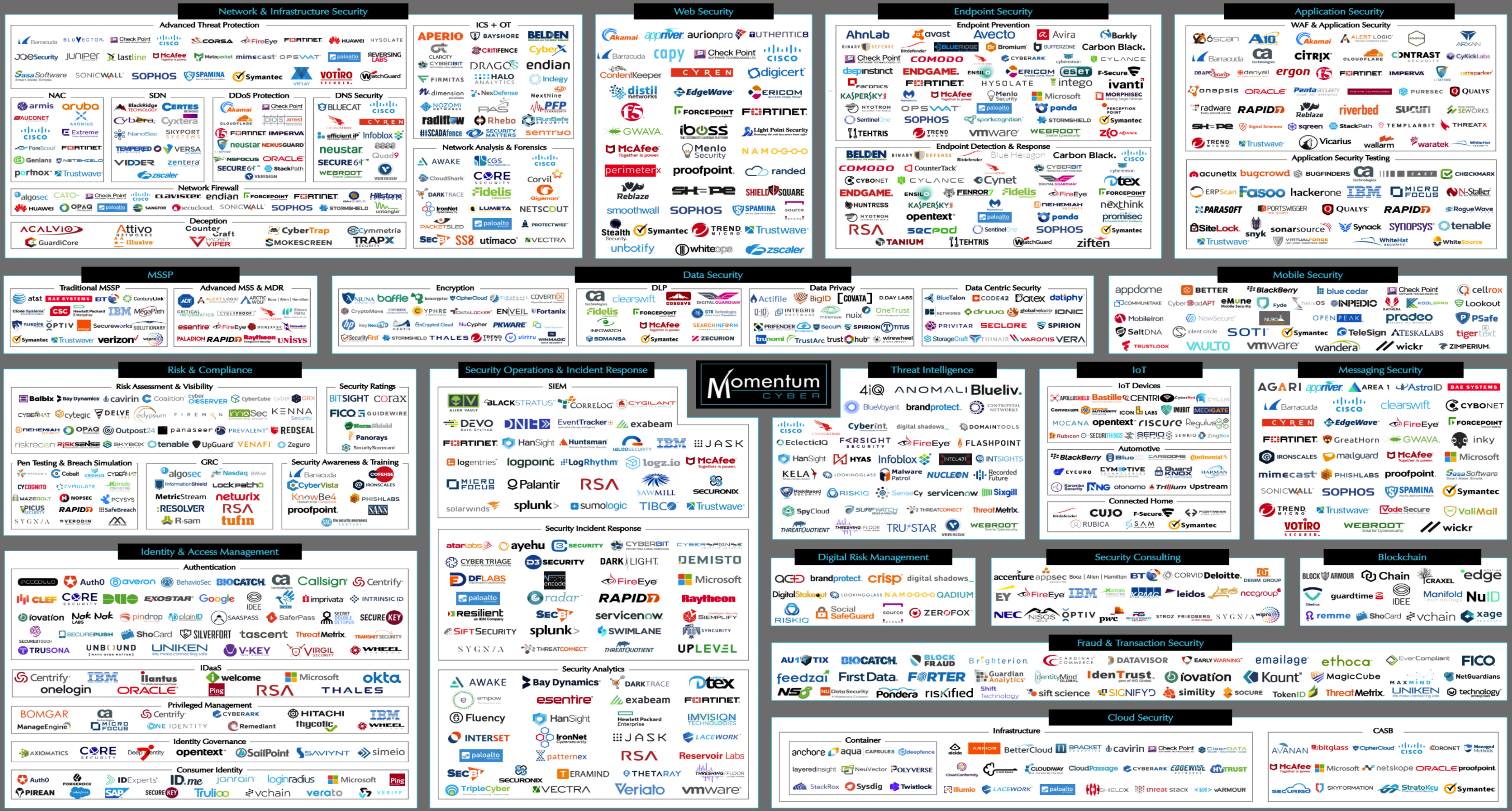


Map concept derived from Geographies of the World's Knowledge, Graham, M., Hale, S.A. and Stephens, M. (Convoco! Edition, London, 2011).

Identity & Access Control	Application and Data	Cloud, Internet and Online	Network and Infrastructure	Governance, Risk, Compliance	Neutralization	Remediation	Mobile and IOT
ca technologies Cisco Citrix HID Entrust F5 RSA ForeScout Fortinet LogRhythm The Security Intelligence Company LANDesk Software Symantec FireEye	McAfee Fortinet Verint Citrix Blue Coat Alien Vault Trend Micro F5 MobileIron Check Point Software Technologies Ltd. mimecast LANDesk Software Symantec WatchGuard	Fortinet F5 Blue Coat 360 FireEye RSA Bitdefender McAfee Citrix Trend Micro mimecast MobileIron LANDesk Software Cisco Verint paloalto networks Alien Vault Check Point Software Technologies Ltd.	MobileIron WatchGuard Cisco paloalto networks ForeScout 360 RSA FireEye Fortinet F5 Juniper Networks LANDesk Software Blue Coat Trend Micro Citrix Verint VeriSign McAfee vmware HID BAE Systems corero Check Point Software Technologies Ltd.	360 FireEye Alien Vault LANDesk Software Check Point Software Technologies Ltd. F5 RSA Verint mimecast Trend Micro Cisco Citrix Symantec ca technologies MobileIron	Cisco Trend Micro BAE Systems Blue Coat Alien Vault Fortinet corero mimecast RSA Verint MobileIron LANDesk Software 360 McAfee	Verint Blue Coat LockPath Citrix FireEye Alien Vault BAE Systems Bitdefender Cisco paloalto networks LANDesk Software Trend Micro LogRhythm The Security Intelligence Company McAfee Fortinet Juniper Networks corero RSA Symantec mimecast	ca technologies MobileIron Citrix Blue Coat Symantec vmware Check Point Software Technologies Ltd. Alien Vault FireEye HID Juniper Networks Symantec LANDesk Software McAfee 360
Securonix Security Analytics. Delivered. Early Warning digicert beyondtrust Veritas okta Blue Coat elastica CyberArk illumio Ping Identity Bromium Centrify Wallix	syncplicity Singtel Bromium CipherCloud Allegro Entrust iboss cybersecurity Checkmarx hiperos LogRhythm The Security Intelligence Company Blue Coat elastica illumio Threat Connect CyberArk Early Warning	ProtectWise Early Warning CipherCloud Singtel Trustwave Centrify PhishLabs Bromium PhishMe Malwarebytes Blue Coat elastica Webroot netskope Pulse Secure CyberArk	Arbor Networks illumio iboss cybersecurity Agiliance LogRhythm The Security Intelligence Company Early Warning HyTrust ProtectWise Lancope exabeam beyondtrust Veritas Securonix CyberArk Blue Coat elastica ForeScout Bromium cybereason Malwarebytes	LockPath Early Warning netskope Blue Coat elastica illumio TRUSTe Click to verify Agiliance iboss cybersecurity hiperos syncplicity CyberArk beyondtrust Veritas Securonix Centrify LogRhythm The Security Intelligence Company	Veracode cybereason exabeam Early Warning Bromium CrowdStrike Malwarebytes iboss cybersecurity skybox security	Malwarebytes Arbor Networks Carbon Black Agiliance CipherCloud Lancope exabeam TRUSTe Click to verify Webroot CrowdStrike iboss cybersecurity Singtel Veracode netskope illumio Securonix beyondtrust Veritas Blue Coat elastica syncplicity	Bromium Centrify iboss cybersecurity TRUSTe Click to verify Checkmarx Webroot Early Warning Singtel Veracode Malwarebytes syncplicity Blue Coat elastica Pulse Secure
SecuredTouch SecureAuth QuoVadis Dome9 Cylance ThreatMetrix onelogin iovation BehavioSec FireLayers hydrantid dashlane Dyadic When security means secured	enSilo Covertix keep x safe ThreatMetrix LightCyber Cyberint BufferZone invincea GuardiCore iovation Prevalent Dyadic When security means secured	Prevalent Zenedge Cyberint Menlo Security Cylance Skycure Reblaze Votiro Secured ThreatMetrix wombat security technologies PhishLine BufferZone Hexadite esentire Zimperium Mobile Defense invincea iovation ThetaRay ironscales LightCyber Cyphort algosec GuardiCore Dyadic FireLayers	BufferZone esentire Cylance illusive Hexadite LightCyber messageware Cyphort Skycure FortScale Dome9 GuardiCore ThetaRay Votiro Secured Menlo Security algosec Threat Connect Zenedge invincea Cyberint wirex	swimlane LightCyber SecureAuth Avanan KnowBe4 Prevalent R-sam BehavioSec esentire algosec illusive Dome9 Hexadite Skycure Votiro Secured ThetaRay BlackStratus BufferZone ayehu iovation Threat Connect Cyberint SafeBreach FireLayers	BufferZone Cylance CyberArk Cyphort SentinelOne LightCyber Forter riskified Threat Connect invincea iovation Zenedge Hexadite Votiro Secured BehavioSec ThreatBook ThetaRay ThreatMetrix esentire Dome9 Skycure FortScale illusive GuardiCore Cyberint	SafeBreach Prevalent CyberArk Cylance Cyphort R-sam iovation Siemplify Threat Connect invincea Skycure Hexadite appthority esentire Dome9 illusive FortScale Menlo Security GuardiCore Cyberint BufferZone comilion	R-sam ThetaRay Skycure SecuredTouch iovation ThreatMetrix Votiro Secured Menlo Security Zimperium Mobile Defense Dyadic When security means secured

: Marlin & Associates, 2016

CYBERscape v2.5



Network & Infrastructure Security

Advanced Threat Protection

NAC

SDN

DDoS Protection

DNS Security

Network Firewall

Deception

ICS + OT

Network Analysis & Forensics

Web Security

Endpoint Security

Endpoint Prevention

Endpoint Detection & Response

Application Security

WAF & Application Security

Application Security Testing

MSSP

Traditional MSSP

Advanced MSS & MDR

Data Security

Encryption

DLP

Data Privacy

Data Centric Security

Mobile Security

Risk & Compliance

Risk Assessment & Visibility

Security Ratings

Pen Testing & Breach Simulation

GRC

Security Awareness & Training

Security Operations & Incident Response

SIEM

Security Incident Response

Security Analytics

Identity & Access Management

Authentication

IDaaS

Privileged Management

Identity Governance

Consumer Identity

Threat Intelligence

IoT

IoT Devices

Automotive

Connected Home

Messaging Security

Digital Risk Management

Security Consulting

Blockchain

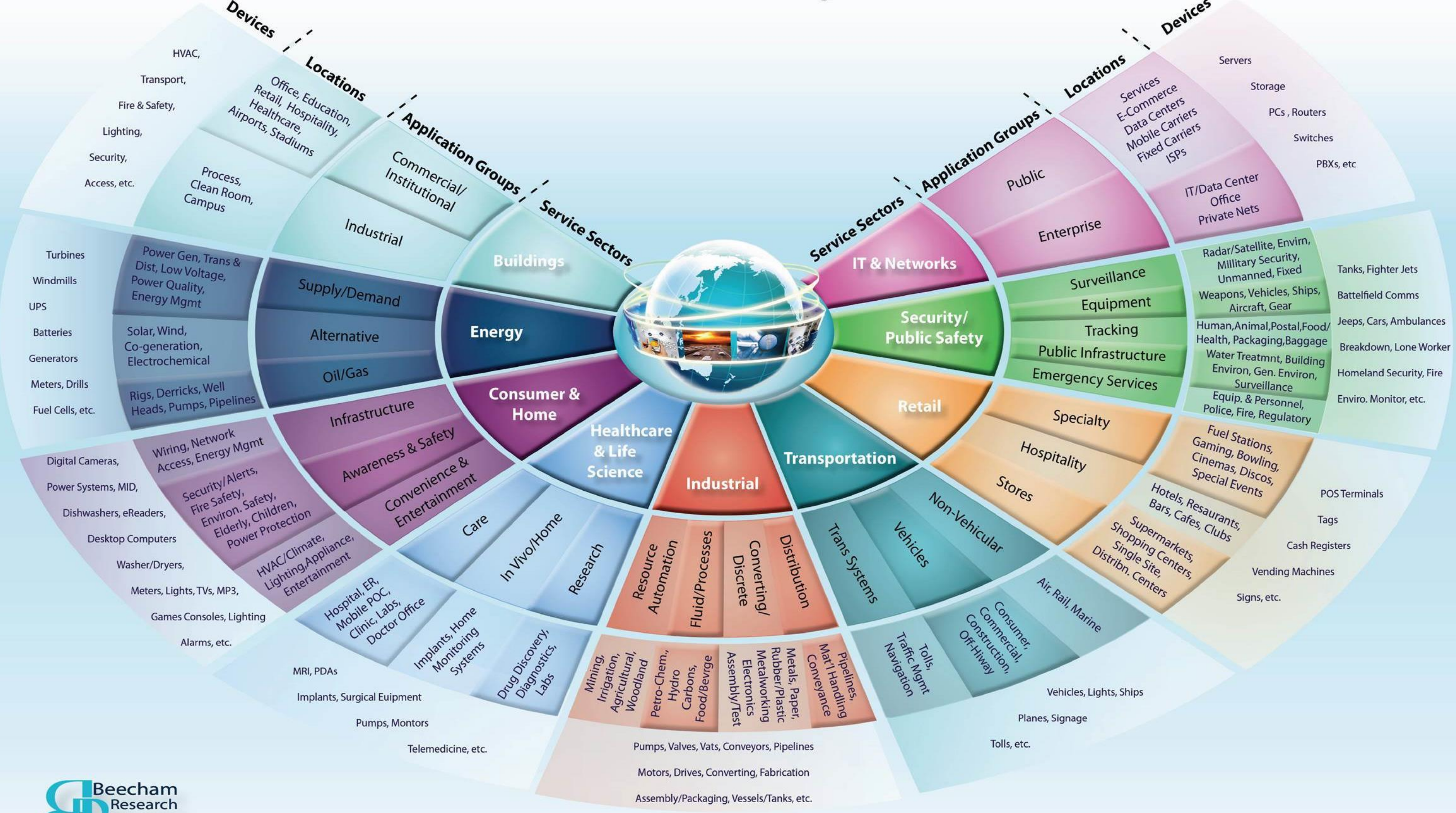
Fraud & Transaction Security

Cloud Security

Infrastructure

Container

CASB



Service Sectors
Application Groups
Locations
Devices

Buildings
Commercial/ Institutional
Office, Education, Retail, Hospitality, Healthcare, Airports, Stadiums
Industrial
Process, Clean Room, Campus
HVAC, Transport, Fire & Safety, Lighting, Security, Access, etc.

Energy
Supply/Demand
Power Gen, Trans & Dist, Low Voltage, Power Quality, Energy Mgmt
Alternative
Solar, Wind, Co-generation, Electrochemical
Oil/Gas
Rigs, Derricks, Well Heads, Pumps, Pipelines
Turbines
Windmills
UPS
Batteries
Generators
Meters, Drills
Fuel Cells, etc.

Consumer & Home
Infrastructure
Wiring, Network Access, Energy Mgmt
Awareness & Safety
Security/Alerts, Fire Safety, Environ. Safety, Elderly, Children, Power Protection
Convenience & Entertainment
HVAC/Climate, Lighting,Appliance, Entertainment
Digital Cameras, Power Systems, MID, Dishwashers, eReaders, Desktop Computers, Washer/Dryers, Meters, Lights, TVs, MP3, Games Consoles, Lighting, Alarms, etc.

Healthcare & Life Science
Care
Hospital, ER, Mobile POC, Clinic, Labs, Doctor Office
In Vivo/Home
Implants, Home Monitoring Systems
Research
Drug Discovery, Diagnostics, Labs
MRI, PDAs
Implants, Surgical Euipment
Pumps, Montors
Telemedicine, etc.

Industrial
Resource Automation
Mining, Irrigation, Agricultural, Woodland
Fluid/Processes
Petro-Chem., Hydro Carbons, Food/Bevrge
Converting/ Discrete
Metals, Paper, Rubber/Plastic
Metalworking Electronics Assembly/Test
Distribution
Pipelines, Mat'l Handling Conveyance
Pumps, Valves, Vats, Conveyors, Pipelines
Motors, Drives, Converting, Fabrication
Assembly/Packaging, Vessels/Tanks, etc.

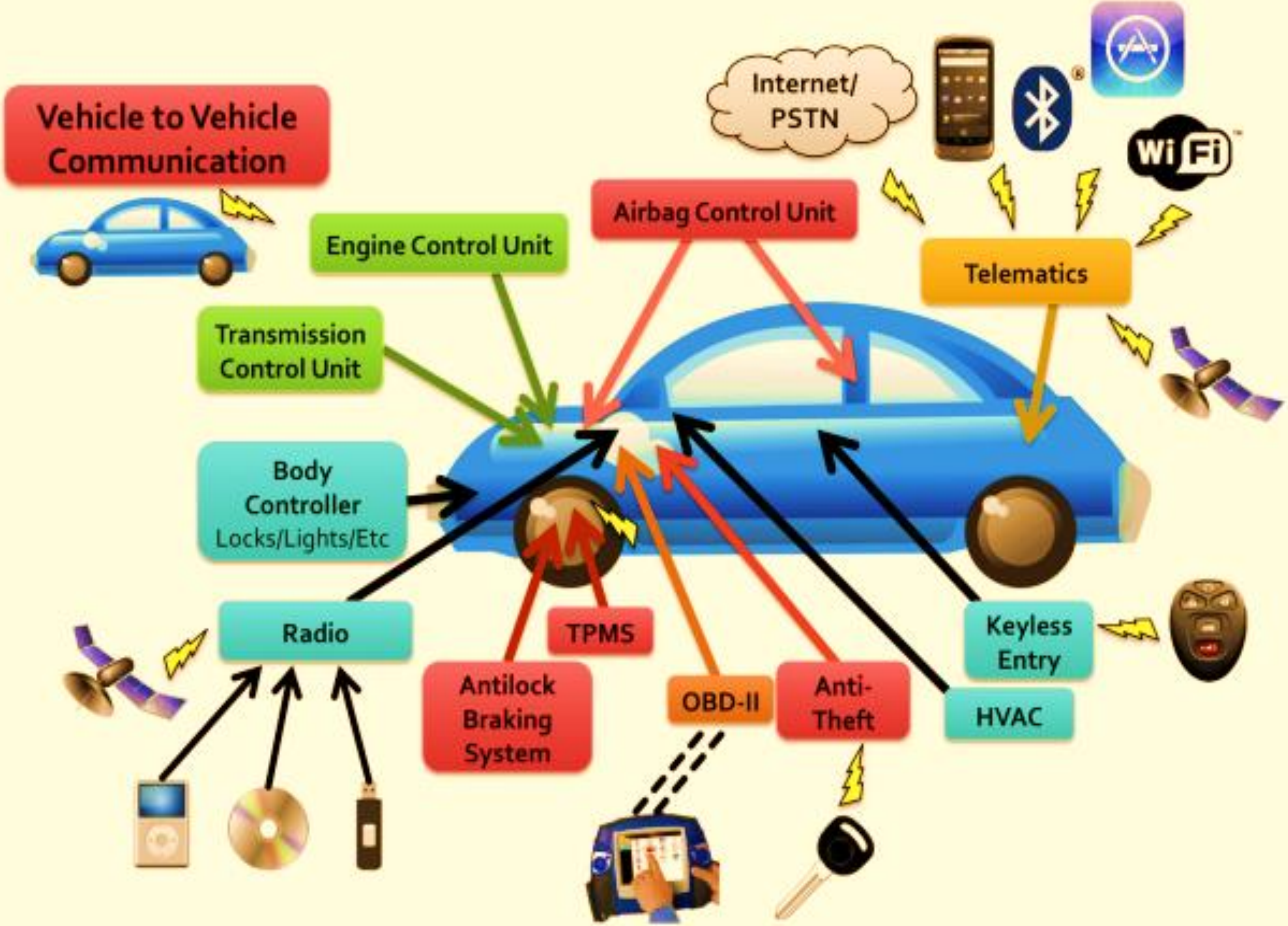
Transportation
Trans Systems
Tolls, Traffic Mgmt Navigation
Vehicles
Consumer, Commercial, Construction, Off-Hiway
Non-Vehicular
Air, Rail, Marine
Vehicles, Lights, Ships
Planes, Signage
Tolls, etc.

Retail
Specialty
Fuel Stations, Gaming, Bowling, Cinemas, Discos, Special Events
Hospitality
Hotels, Resaurants, Bars, Cafes, Clubs
Stores
Supermarkets, Shopping Centers, Single Site, Distribn. Centers
POS Terminals
Tags
Cash Registers
Vending Machines
Signs, etc.

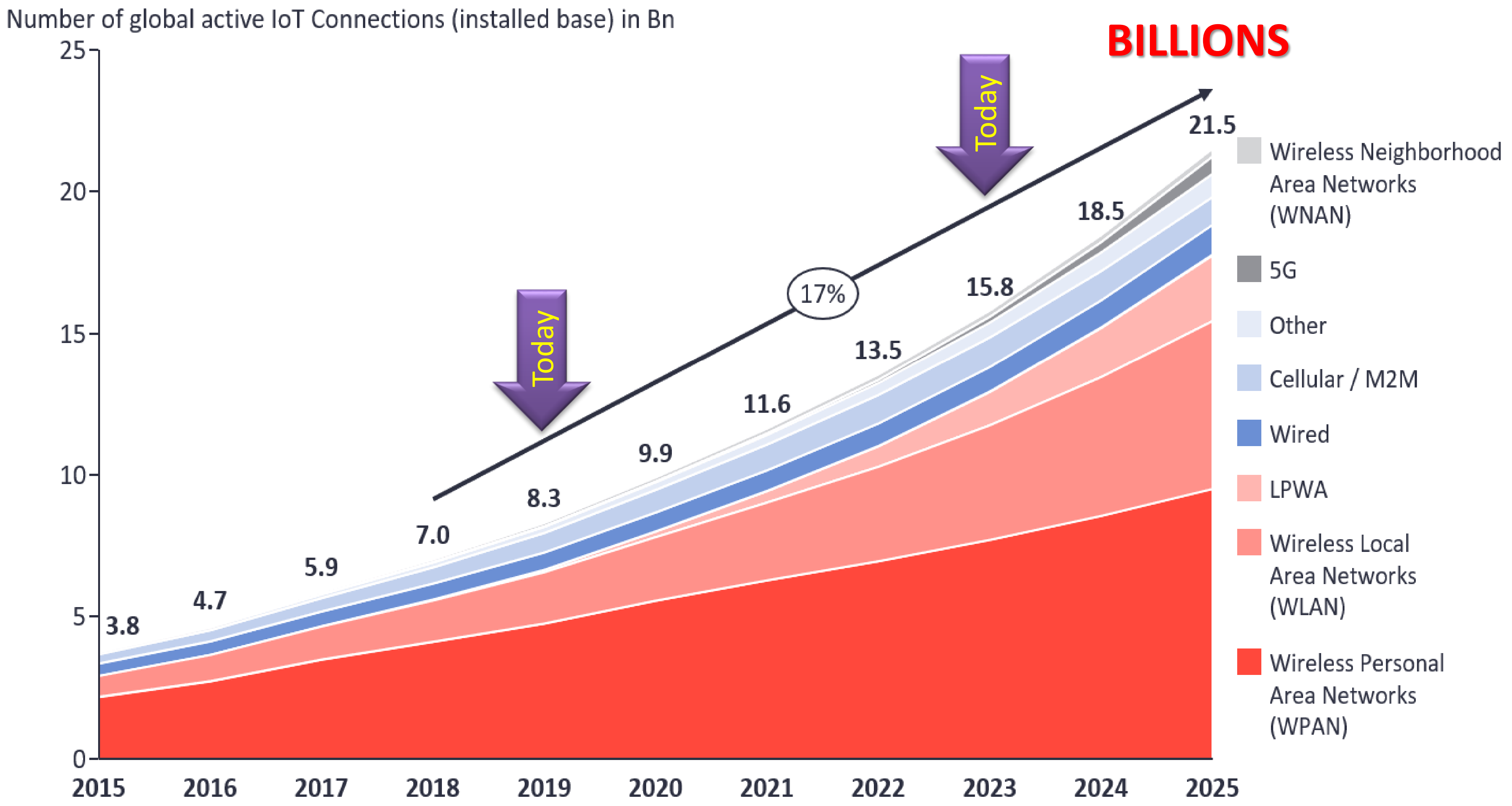
Security/ Public Safety
Surveillance
Radar/Satellite, Envirn, Millitary Security, Unmanned, Fixed
Equipment
Weapons, Vehicles, Ships, Aircraft, Gear
Tracking
Human,Animal,Postal,Food/ Health, Packaging,Baggage
Public Infrastructure
Water Treatmnt, Building Environ, Gen. Environ, Surveillance
Emergency Services
Equip. & Personnel, Police, Fire, Regulatory
Tanks, Fighter Jets
Battlefield Comms
Jeeps, Cars, Ambulances
Breakdown, Lone Worker
Homeland Security, Fire
Enviro. Monitor, etc.

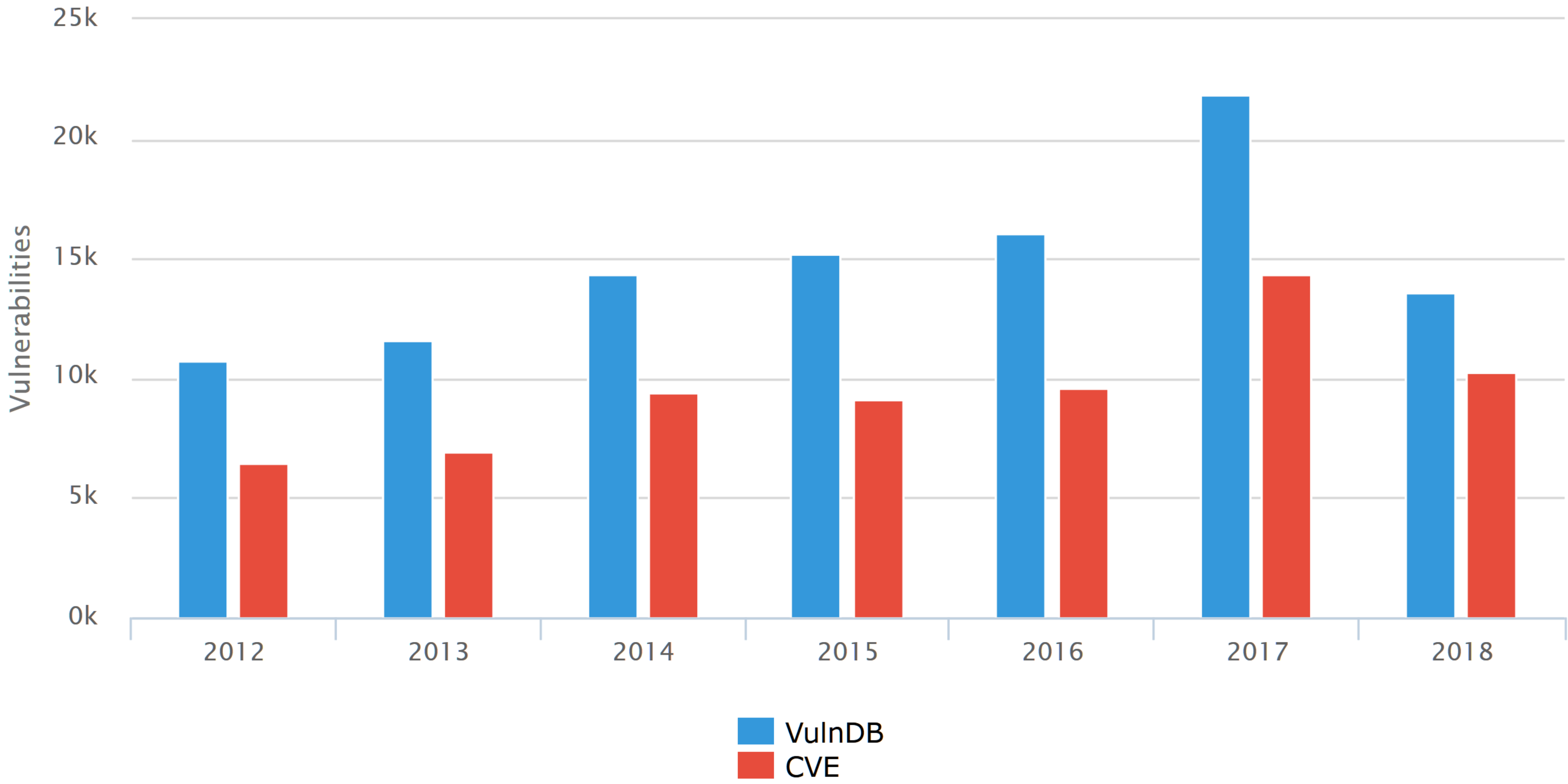
IT & Networks
Public
Services E-Commerce Data Centers Mobile Carriers Fixed Carriers ISPs
Enterprise
IT/Data Center Office Private Nets
Servers
Storage
PCs , Routers
Switches
PBXs, etc

Beecham Research


Vehicle to Vehicle Communication
Internet/ PSTN
Engine Control Unit
Airbag Control Unit
Telematics
Transmission Control Unit
Body Controller Locks/Lights/Etc
Radio
TPMS
Antilock Braking System
OBD-II
Anti-Theft
Keyless Entry
HVAC

Global Number of Connected IoT Devices



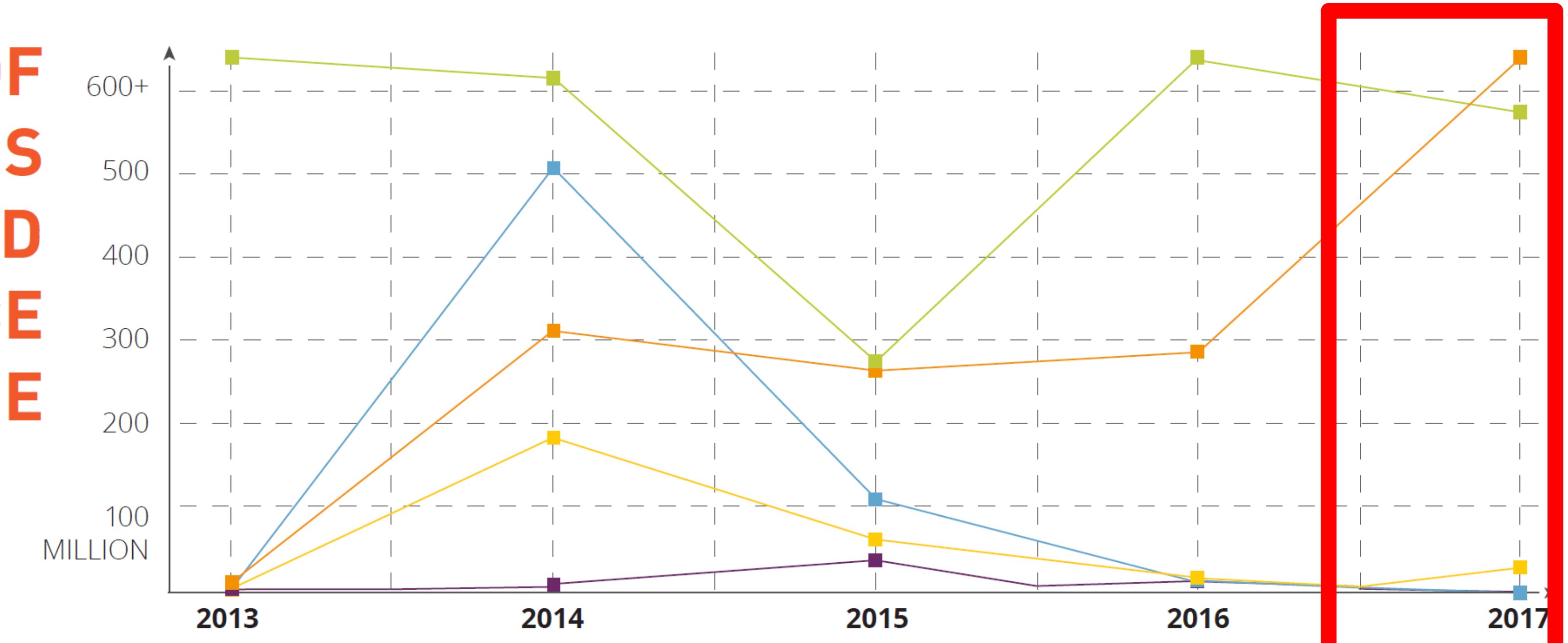


25k
20k
15k
10k
5k
0k
Vulnerabilities
2012
2013
2014
2015
2016
2017
2018
VulnDB
CVE

Cyber Threat	Motive	Targets of Opportunity	Methodologies	Capabilities
Nation States ~ Peace Time	Economic, Military, Political	Commercial Enterprises, Intelligence, National Defense, Governments, National Infrastructure	Military & Intel specific cyber doctrine, hacktivists	Asymmetric use of the cyber domain short of kinetic
Nation States ~ War Time	Economic, Military, Political	Commercial Enterprises, Intelligence, National Defense, Governments, National Infrastructure	Military & Intel specific cyber doctrine, hacktivists	Asymmetric use of the cyber domain including kinetic
Cyber Terrorists & Insurgents	Political	Infrastructure, Extortion and Political Processes	Combination of advanced persistent threats (APT)	Developing – will be a concern in 2012
Cyber Criminals – Grey & Black Markets	Financial	Intellectual Property Theft, Fraud, Theft, Scams, Hijacked Network & Computer Resources, Cyber Crime for Hire	Exploits, Malware Botnets, Worms & Trojans	Cell-based structure as an APT
Criminal Organizations – RBS	Financial		Use of above with distinct planning	Highly professional, dangerous
Rogue Organizations – Anonymous, LulzSec	Financial	Intellectual Property Theft, Direct & Indirect pressure on OGA Resources	Organic hacking capabilities unsurpassed	Organized yet de-centralized

Red-DragonRising.com ©

NUMBER OF RECORDS BREACHED BY SOURCE OVER TIME



BREACH SOURCE	2013	2014	2015	2016	2017
Malicious Outsider	2,081,285,434	674,544,208	274,762,361	1,057,189,069	585,502,201
Accidental Loss	15,068,756	309,823,689	265,209,847	292,246,026	1,985,095,967
Malicious Insider	10,371,810	185,738,742	64,791,635	13,963,040	30,348,328
Hacktivist	875,946	8,182,103	30,573,822	12,371,864	21,784
State Sponsored	165,053	509,928,563	108,076,636	10,797,581	0
Unknown	77,525	1,307	591	950,000	0
TOTALS	2,107,844,524	1,688,218,612	743,414,892	1,387,517,580	2,600,968,280

Source: BREACHLEVELINDEX.COM

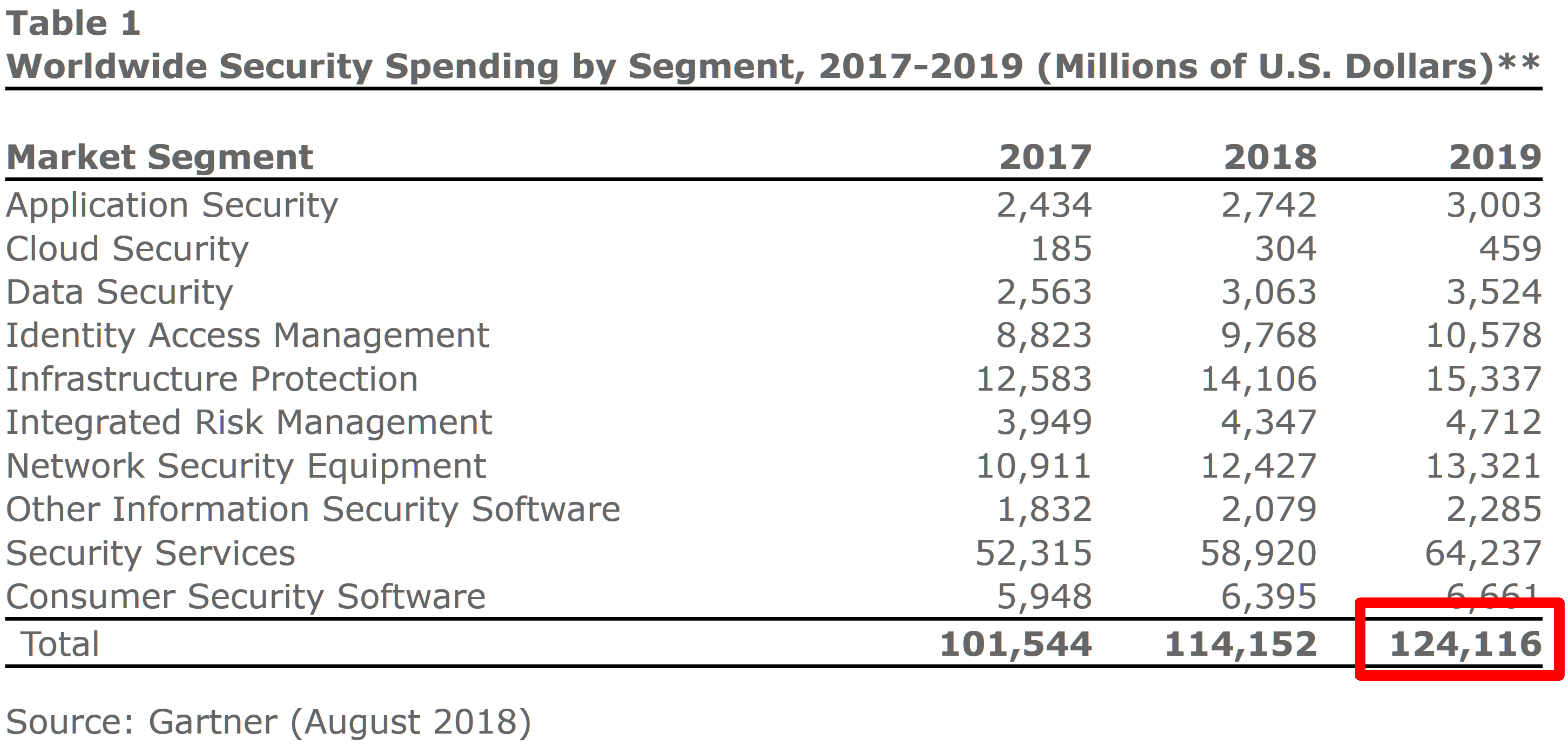


Table 1
Worldwide Security Spending by Segment, 2017-2019 (Millions of U.S. Dollars)**

Market Segment	2017	2018	2019
Application Security	2,434	2,742	3,003
Cloud Security	185	304	459
Data Security	2,563	3,063	3,524
Identity Access Management	8,823	9,768	10,578
Infrastructure Protection	12,583	14,106	15,337
Integrated Risk Management	3,949	4,347	4,712
Network Security Equipment	10,911	12,427	13,321
Other Information Security Software	1,832	2,079	2,285
Security Services	52,315	58,920	64,237
Consumer Security Software	5,948	6,395	6,661
Total	**101,544**	**114,152**	**124,116**

Source: Gartner (August 2018)

We cannot solve our problems with the same thinking we used when we created them.

Albert Einstein

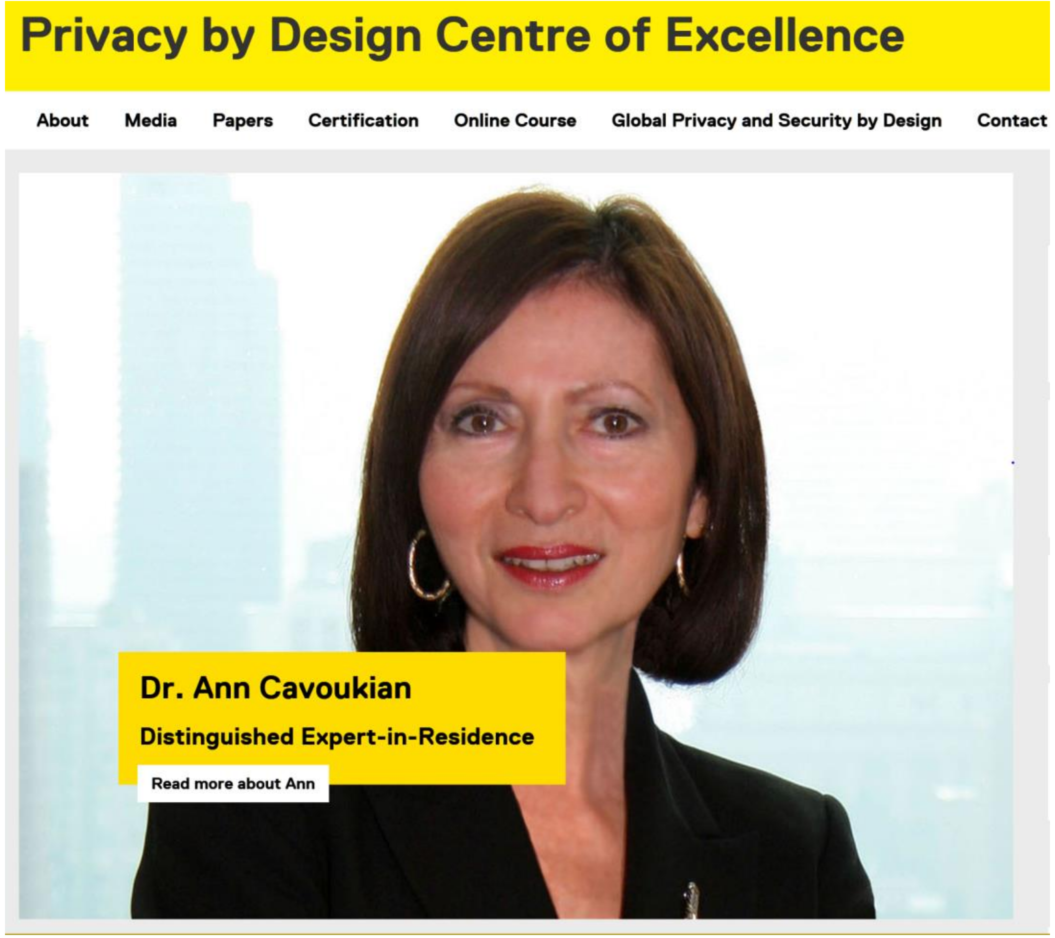
This is your attack surface…

- Company strategy
- Financial data
- Personnel data
- Health data
- Customer data
- Product data
- R&D data
- Partner/vendor data
- Application databases
- Customer history
- Government data
- Other documents
- Spreadsheets
- Presentations
- Photos/diagrams

This is what the bad guys are after...

- Name and alias
- Social security number
- National identification number
- Driver's license/history data
- Other government identifiers
- Citizenship/legal status
- Gender, race, ethnicity
- Birth date, place of birth
- Home, work and cell numbers
- Personal email address
- Religious preference
- Sexual preference
- Security clearance
- Mailing and home address
- Mother's maiden names
- Spouse information
- Child information
- Emergency contact information
- Biometric data
- Financial/credit card data
- Medical/disability information
- Emergency contact information
- Biometric data
- Financial/credit card data
- Medical/disability information
- Law enforcement records
- Employment records
- Educational records
- Military records
- Law enforcement records
- Employment records
- Educational records
- Military records

Introducing Privacy by Design



Privacy by Design Centre of Excellence

Dr. Ann Cavoukian

Distinguished Expert-in-Residence

Privacy by Design Asserts:

- Privacy cannot be assured by regulatory frameworks alone.
- Protecting privacy must become your default mode of operation.
- To include accountable business practices and information systems.
- It must protect all types of personally identifiable information (PII).

* http://www.ryerson.ca/pbdce/

7 Principles of Privacy by Design

1. **Proactive** not Reactive; **Preventive** not Remedial
2. Privacy as the **Default** Setting
3. Privacy **Embedded** into Design
4. Full Functionality — **Positive-Sum**, not Zero-Sum
5. **End-to-End** — Full Lifecycle Protection
6. Visible and **Transparent** — Keep it Open
7. **User-Centric** — Focus is on respect for User Privacy

1. Proactive not Reactive; Preventive not Remedial

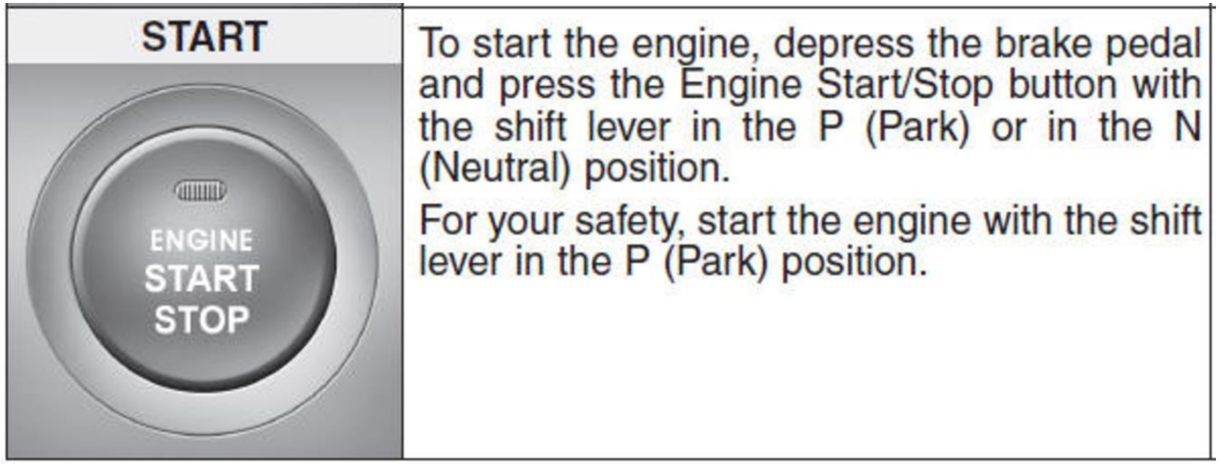
- **Anticipates** and prevents privacy invasive events *before they happen*.
- It does not wait for privacy risks to materialize, it **aims to prevent** them from occurring.
- PbD comes **before-the-fact**, not after.

2. Privacy as the Default Setting

- Helps to ensure personal **data are automatically protected** in any system or business practice.
- If an individual does nothing, their **privacy still remains intact**.

3. Privacy Embedded into Design

- **Baked into design** of information systems and business practices; not bolted on after the fact.
- PbD becomes an component of the functionality being delivered, **without diminishing that functionality**.



START

ENGINE
START
STOP

To start the engine, depress the brake pedal and press the Engine Start/Stop button with the shift lever in the P (Park) or in the N (Neutral) position.

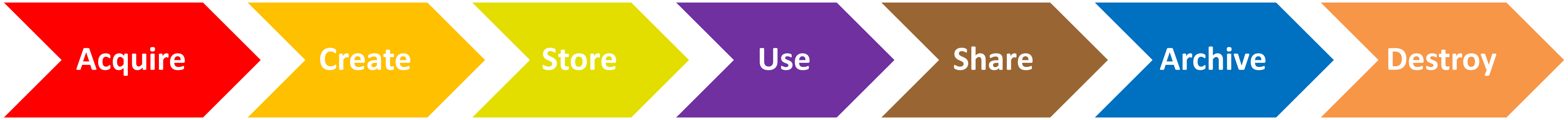
For your safety, start the engine with the shift lever in the P (Park) position.

4. Full Functionality; Positive-Sum, not Zero-Sum

- PbD **accommodates all interests** and objectives in a “win-win” manner, not zero-sum approach.
- It avoids the conflict between privacy vs. security, and **works to achieve both**.

5. End-to-End, Full Lifecycle Protection

- Addresses security **before first element of information is collected**.
- Ensures **cradle to grave**, protections throughout information lifecycle, end-to-end.


Acquire → Create → Store → Use → Share → Archive → Destroy

6. Visibility and Transparency; Keep it Open

- PbD assures **everyone is operating according to the stated (privacy) promises** and objectives.
- PbD component parts, processes and operations remain **visible and transparent** to users and stakeholders.

7. Respect for User Privacy; Keep it User-Centric

- Requires everyone to **keep the interests of individual users the highest priority** by offering:
  - Strong privacy default settings.
  - Appropriate notice about what you hold and how you are using their data
  - User-friendly options for them to control their privacy.

10 Steps towards implementing Privacy by Design

1. Document an INVENTORY of the sensitive and PII data you hold.

2. REVALIDATE where the data came from and WHY you are holding it.

3. If you don’t know data provenance, or can’t revalidate why you hold it, DELETE it

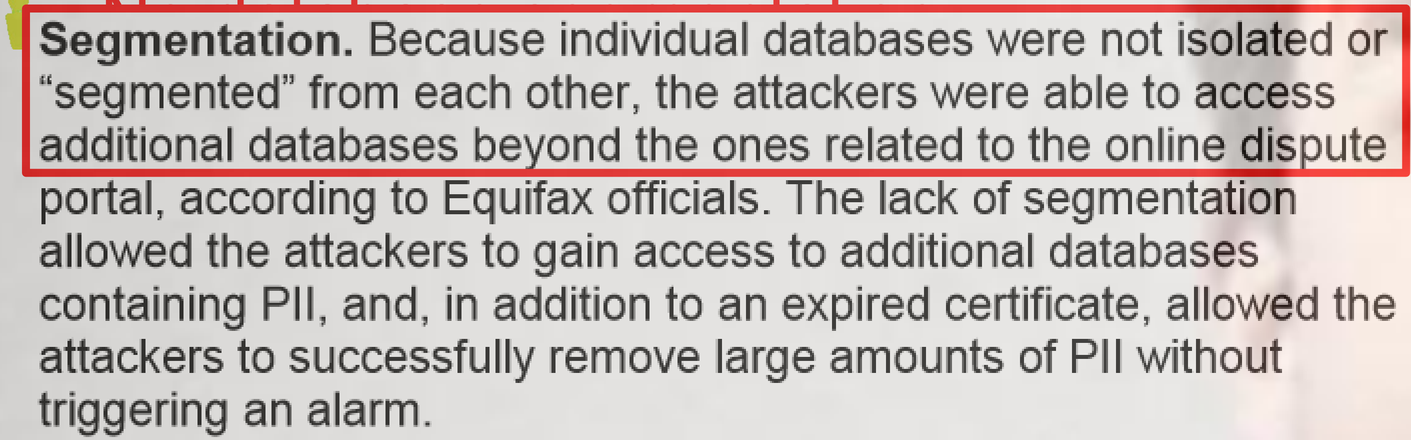
4. If you must hold it, get PERMISSION from the data owner(s) to hold and use it.

5. Where possible, DE-IDENTIFY the data you hold.

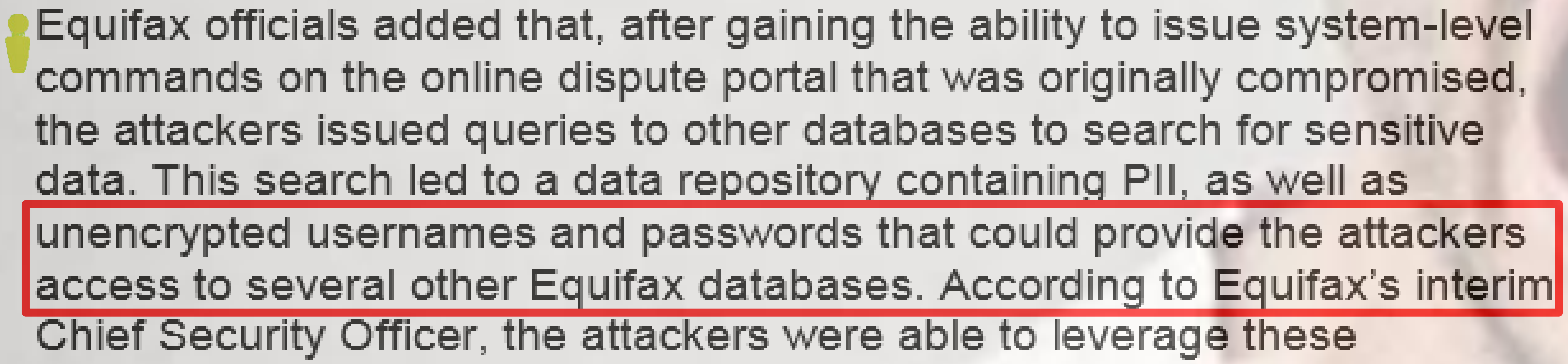
6. SEGMENT/PARTITION the data you hold; logically/physically

7. ENCRYPT all data, in motion and at rest.

Equifax hack – two internal weaknesses



- **Segmentation.** Because individual databases were not isolated or "segmented" from each other, the attackers were able to access additional databases beyond the ones related to the online dispute portal, according to Equifax officials. The lack of segmentation allowed the attackers to gain access to additional databases containing PII, and, in addition to an expired certificate, allowed the attackers to successfully remove large amounts of PII without triggering an alarm.



- Equifax officials added that, after gaining the ability to issue system-level commands on the online dispute portal that was originally compromised, the attackers issued queries to other databases to search for sensitive data. This search led to a data repository containing PII, as well as unencrypted usernames and passwords that could provide the attackers access to several other Equifax databases. According to Equifax's interim Chief Security Officer, the attackers were able to leverage these

8. Establish retention policies and expunge data; from ALL stores.

9. Use different authentication methods between presentation and data layers.

10. As soon as you no longer need to hold sensitive/PII data, DELETE IT.

BONUS: Go through these steps quarterly; to verify compliance with business units.

Thank you

Chuck Georgo

chuck@nowheretohide.org

410-903-6289

NOWHERE TO HIDE.ORG