REPUTATION AT STAKE

58

Types of Data Breaches

The Hacking Attack	The Accidental Data Leak	The Inside Job
1	2	3
Cybercriminals break into a company's computer system and steal data.	An employee accidentally sends sensitive data to the wrong person or posts it online where anyone can access it.	A company employee steals data for their gain.

59

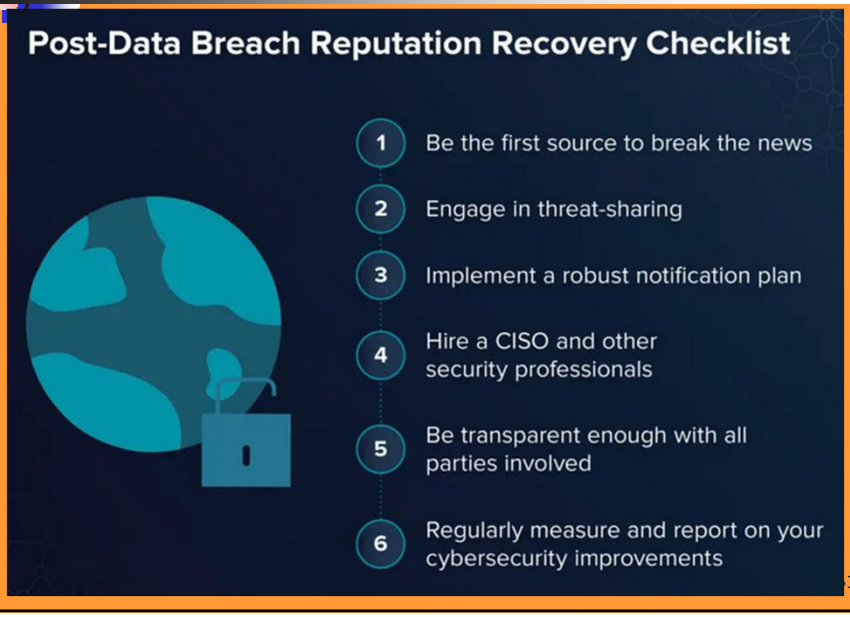
59

Prevent a Data Breach

- Restrict access to sensitive information to only those who need it.
- Install a firewall
- Install antivirus software on your computer.
- Keep software up to date.
- Regularly back up data.
- Impose password policies
  - strong passwords
  - change them regularly.
  - Don't use the same password for different accounts.
- Educate employees
  - Beware of spear-phishing attacks, emails that appear to be from a trusted source but are designed to steal your information.
  - Do not open attachments or click on links in.
  - Install a security plugin on your browser.
  - Be careful about what information you share online.

60

60



61

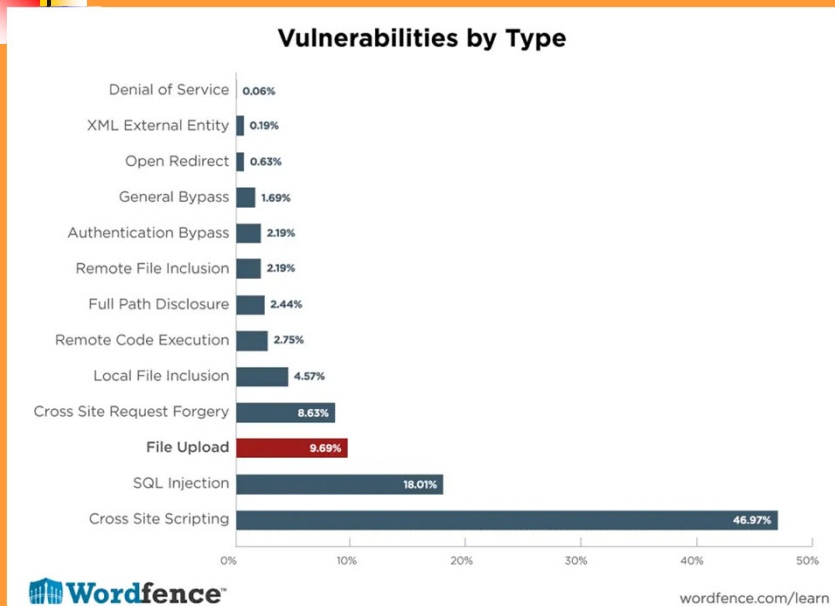
61

CyberReputation Recovery

- Be honest and upfront with customers and LE
  - Explain what happened,
  - Solutions being taken
  - Action for them to protect themselves.
- Improve your security.
  - Ensure your systems are up-to-date
  - "force" your employees to follow best practices.
- Establish a trust relation with your customers.
  - Tell them actions you're taking to protect their data,
  - remind them that you're a reputable company.

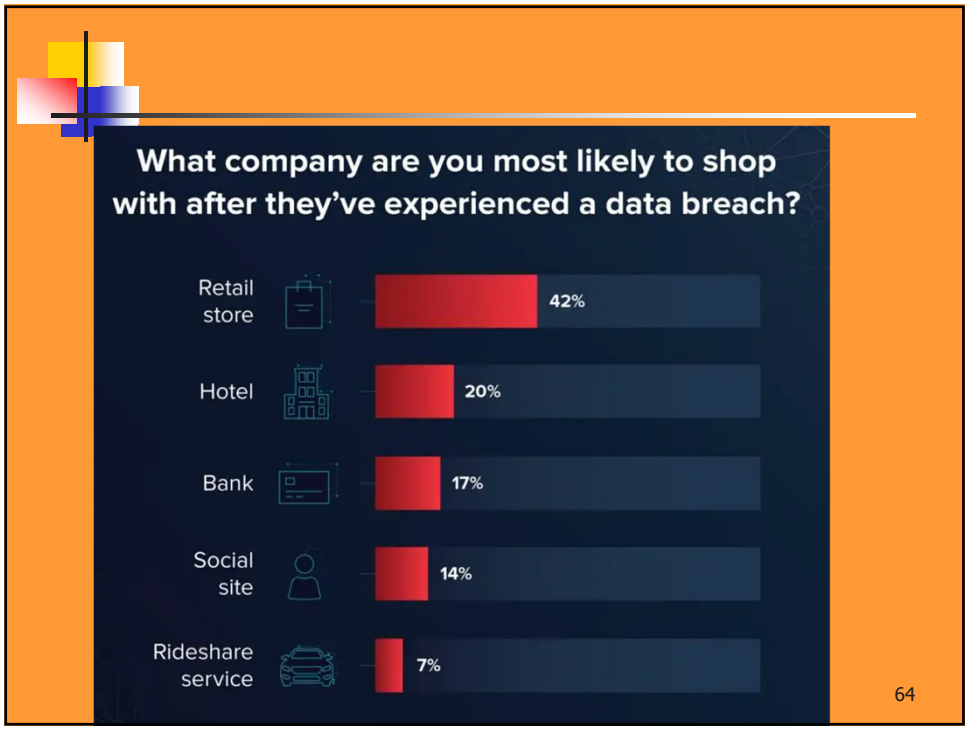
62

62

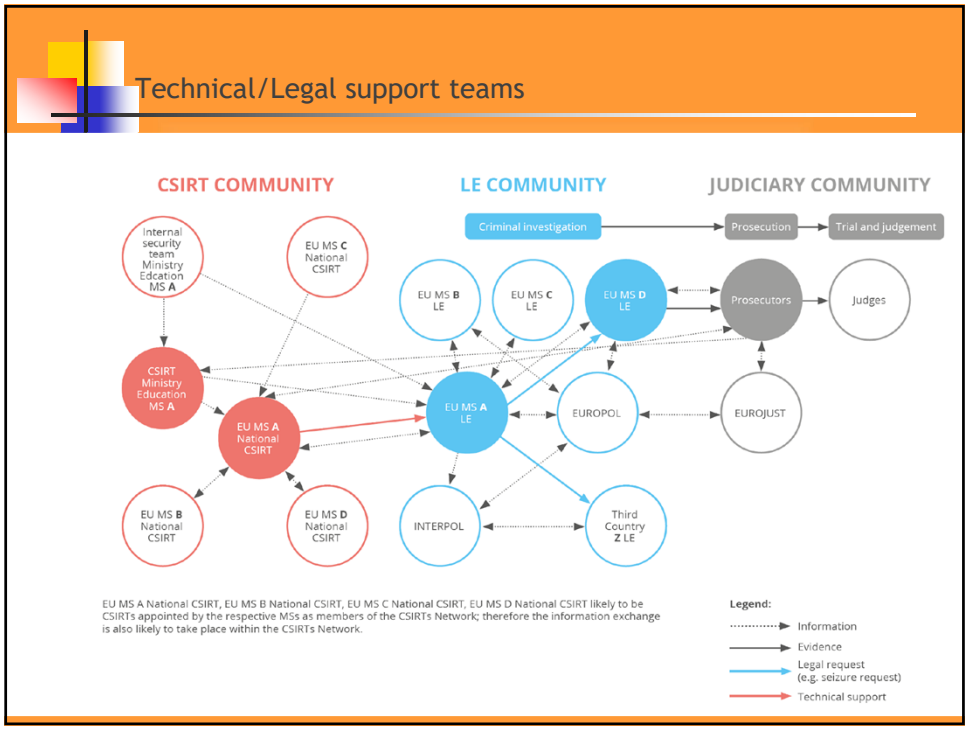


63

63

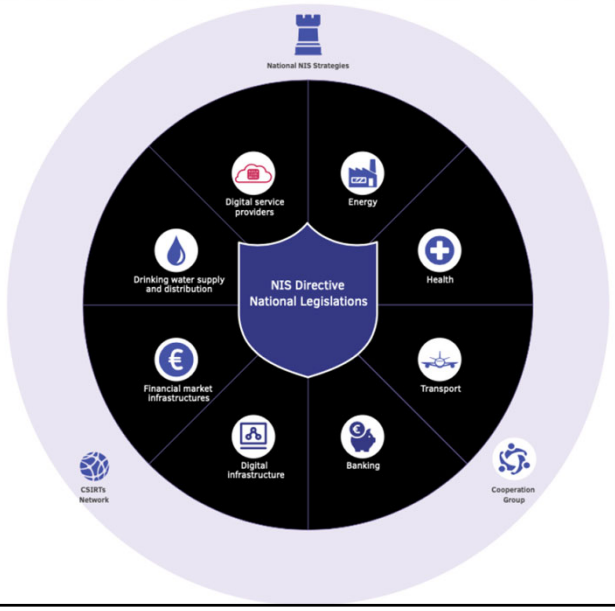

What company are you most likely to shop with after they've experienced a data breach?
Retail store
42%
Hotel
20%
Bank
17%
Social site
14%
Rideshare service
7%
64

64


Technical/Legal support teams
CSIRT COMMUNITY
LE COMMUNITY
JUDICIARY COMMUNITY
Criminal investigation
Prosecution
Trial and judgement
Internal security team Ministry Education MS A
EU MS C National CSIRT
EU MS B LE
EU MS C LE
EU MS D LE
Prosecutors
Judges
CSIRT Ministry Education MS A
EU MS A National CSIRT
EU MS A LE
EUROPOL
EUROJUST
EU MS B National CSIRT
EU MS D National CSIRT
INTERPOL
Third Country Z LE
EU MS A National CSIRT, EU MS B National CSIRT, EU MS C National CSIRT, EU MS D National CSIRT likely to be CSIRTs appointed by the respective MSs as members of the CSIRTs Network; therefore the information exchange is also likely to take place within the CSIRTs Network.
Legend:
Information
Evidence
Legal request (e.g. seizure request)
Technical support

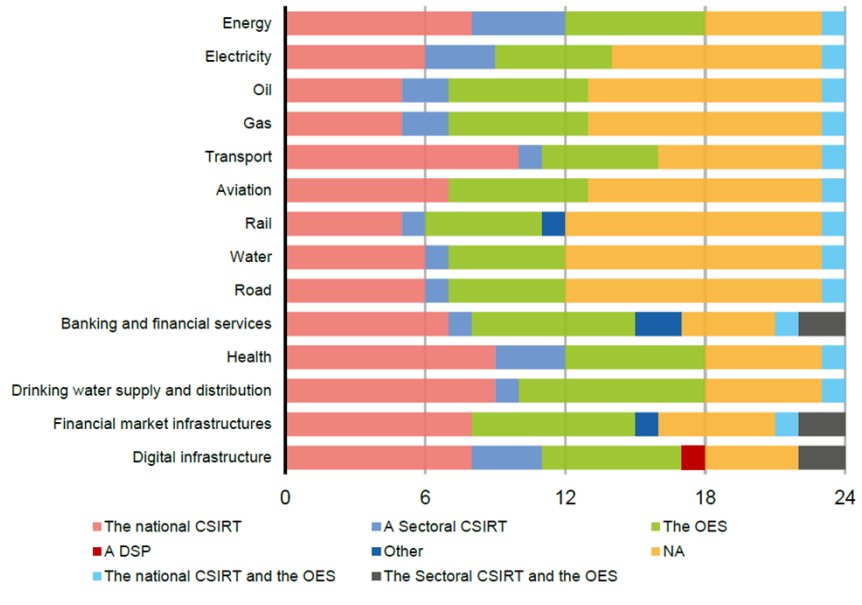
65

Legal and Regulatory Frameworks



66

66



67

CYBERSECURITY MARKET & ECOSYSTEM

68

Global Cybersecurity Market

173.5 USD BILLION 2022

266.2 USD BILLION 2027

CAGR of 8.9%

The global cybersecurity market is expected to be worth USD 266.2 Billion by 2027, growing at CAGR of 8.9% during the forecast period.

North America is estimated to hold the largest market share of the global cybersecurity market in 2022 and the Asia Pacific is also projected to grow at the highest CAGR during the forecast period.

The market growth can be attributed to the growing instances of target-based cyber attacks and increased adoption of cloud-based cybersecurity solutions.

The global hardware segment is estimated to grow from USD XX million in 2022 and reach USD XX million by 2027 to grow at the highest CAGR of XX%.

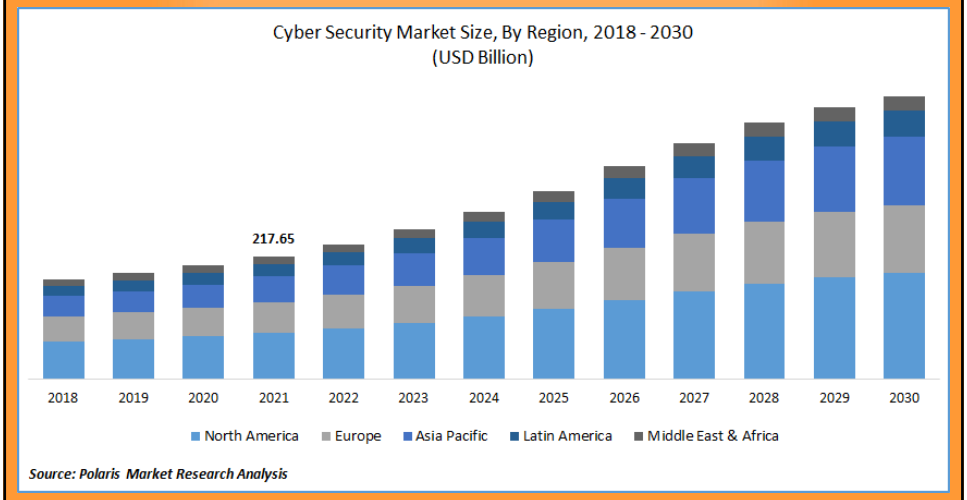
Countries are showing huge opportunities for the cybersecurity solutions due to the presence of key cybersecurity solutions market vendors, investments & innovations, strict regulatory environment, and high technology adoption rates.

The healthcare vertical offers great opportunities in the cybersecurity market and is expected to grow at the highest CAGR during the forecast period.

69

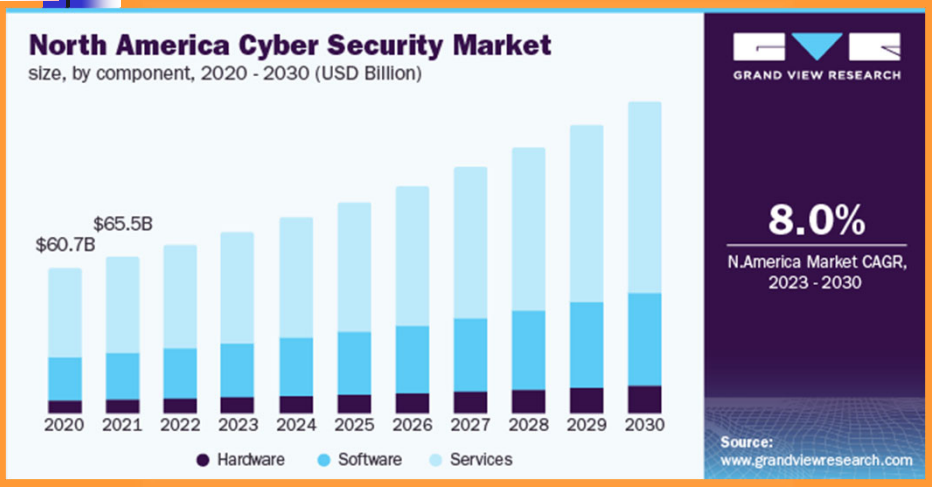
69

Market per Region



70

70



71

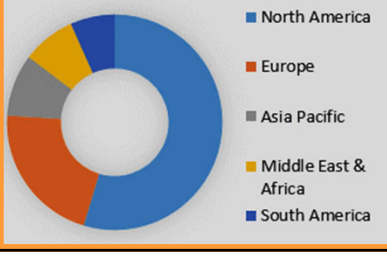
71

Cybersec Market

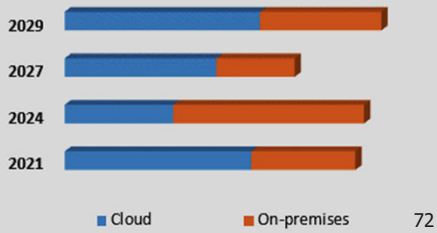
Key Players

Check Point Software Technologies Ltd.
Cisco Systems, Inc.
CyberArk Software Ltd.
Qualys, Inc.
Palo Alto Networks, Inc.
LogRhythm, Inc.
IBM Corporation
Hewlett Packard Enterprise
Webroot, Inc.
Fortinet, Inc.
Imperva, Inc.
McAfee LLC
Trend Micro, Inc.
F-Secure
Trustwave Holdings, Inc.
FireEye, Inc.
Sophos Ltd.

Regional Analysis in 2021 (%)



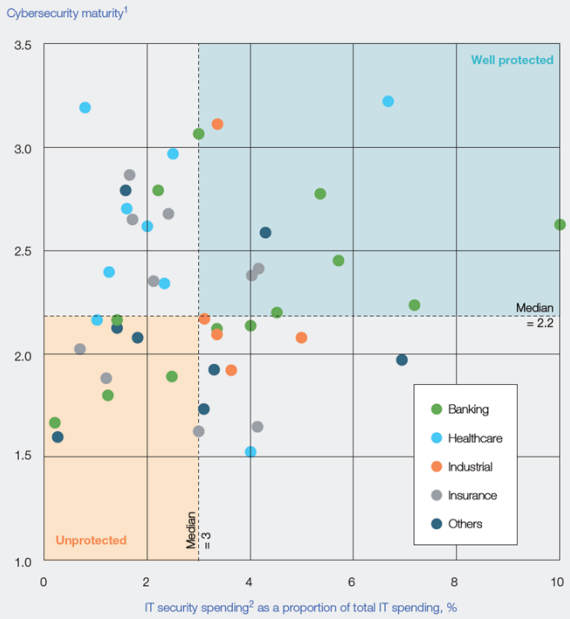
Deployment Mode Segment Overview



72

72

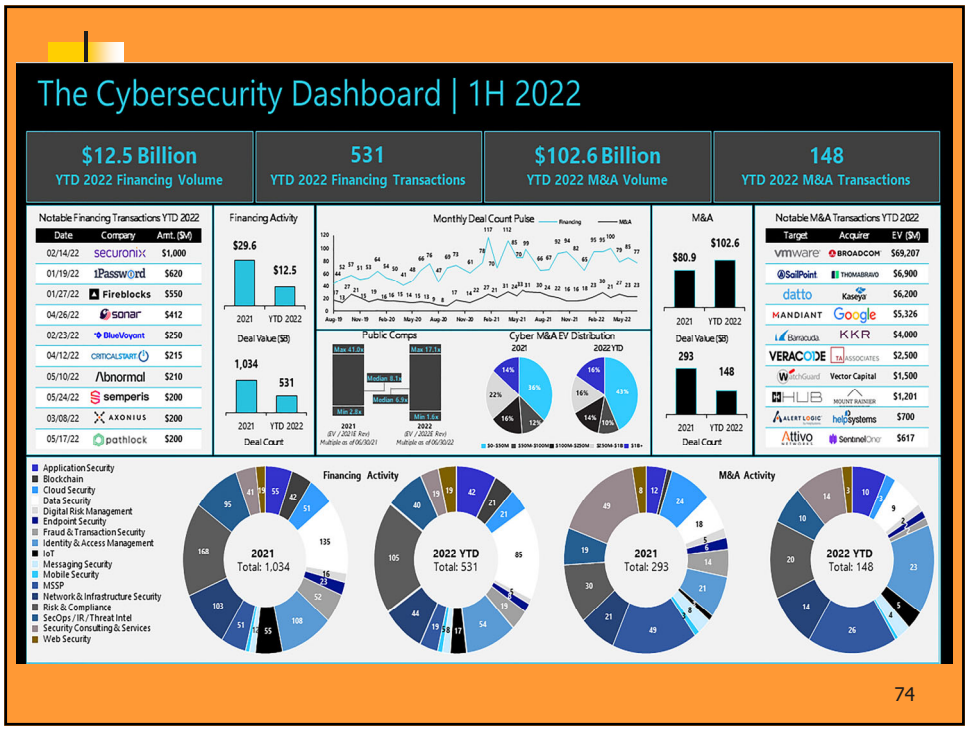
Companies' spending on cybersecurity does not necessarily correlate with level of protection.



Note: Reflects responses from 45 companies in the Global 500 about their cybersecurity spending and capabilities.

73

73

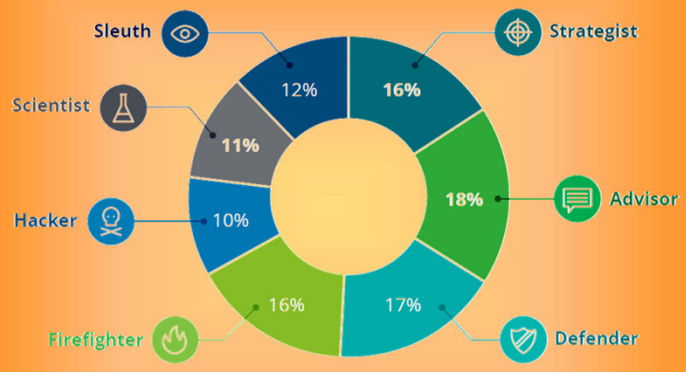

The Cybersecurity Dashboard | 1H 2022
$12.5 Billion
YTD 2022 Financing Volume
531
YTD 2022 Financing Transactions
$102.6 Billion
YTD 2022 M&A Volume
148
YTD 2022 M&A Transactions
Notable Financing Transactions YTD 2022
Date Company Amt. ($M)
02/14/22 securonix $1,000
01/19/22 1Password $620
01/27/22 Fireblocks $550
04/26/22 sonar $412
02/23/22 BlueVoyant $250
04/12/22 CRITICALSTART $215
05/10/22 Abnormal $210
05/24/22 semperis $200
03/08/22 AXONIUS $200
05/17/22 pathlock $200
Financing Activity
$29.6
$12.5
2021
YTD 2022
Deal Value ($B)
1,034
531
Deal Count
Monthly Deal Count Pulse
Financing
M&A
Public Comps
Cyber M&A EV Distribution
2021
2022 YTD
M&A
$80.9
$102.6
Deal Value ($B)
293
148
Deal Count
Notable M&A Transactions YTD 2022
Target Acquirer EV ($M)
vmware BROADCOM $69,207
SailPoint THOMABRAVO $6,900
datto Kaseya $6,200
MANDIANT Google $5,326
Barracuda KKR $4,000
VERACODE TA ASSOCIATES $2,500
WatchGuard Vector Capital $1,500
HUB MOUNT RAINIER $1,201
ALERT LOGIC helpsystems $700
Attivo SentinelOne $617
Application Security
Blockchain
Cloud Security
Data Security
Digital Risk Management
Endpoint Security
Fraud & Transaction Security
Identity & Access Management
IoT
Messaging Security
Mobile Security
MSSP
Network & Infrastructure Security
Risk & Compliance
SecOps / IR / Threat Intel
Security Consulting & Services
Web Security
Financing Activity
2021
Total: 1,034
2022 YTD
Total: 531
M&A Activity
2021
Total: 293
2022 YTD
Total: 148
74

74

Defender
Scientist
Sleuth
Hacker
Firefighter
Strategist
Advisor

75

In Canada…



Hardest to find today: Strategist, Scientist

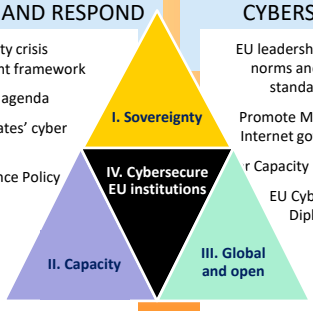
Expected to grow the most in importance: Strategist, Scientist, Advisor

76

76

The EU's Cybersecurity Strategy for the Digital Decade (16.12.2020); 3 instruments (regulatory, investment, policy initiatives) 3 to three pillars

RESILIENCE, TECHNOLOGICAL SOVEREIGNTY AND LEADERSHIP	BUILDING OPERATIONAL CAPACITY TO PREVENT, DETER AND RESPOND	COOPERATION TO ADVANCE A GLOBAL AND OPEN CYBERSPACE
Revised Directive on Security of Network and Information Systems (NIS 2)	Cybersecurity crisis management framework	EU leadership on standards, norms and frameworks in standardisation bodies
Cybersecurity Shield (CSIRT, SOC)	Cybercrime agenda	Promote Multi-Stakeholder Internet governance model
Secure Communication Infrastructure: Quantum, NG Mobile, IPv6, DNS	Member States' cyber intelligence	r Capacity Building Agenda
Competence Centre and Network of Coordination Centres (CCCN)	Cyber Defence Policy Framework	EU Cyber Dialogue and Diplomacy Network
EU workforce upskilling		



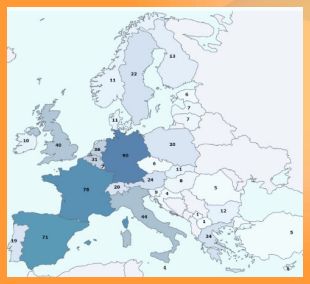
79

79

Cybersecurity knowledge and capabilities in the EU

The EU represents 26% of the global cybersecurity market

More than 660 expertise centres registered in the mapping of cybersecurity centres of expertise



CYBERSECURITY PRODUCTS AND SOLUTIONS

Up to 30% of the European demand is met by companies headquartered outside the EU.

Europe is the location for the corporate headquarters of only 14% of the top 500 global Cybersecurity providers, compared to 75% for the Americas, 7% for Israel and 4% for Asia.

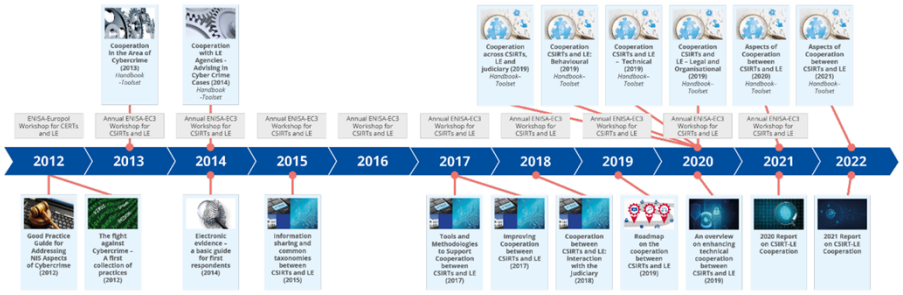
ECS EUROPEAN CYBER SECURITY ORGANISATION

ECSO has +/- 250 members

80

ENISA european union agency for cybersecurity

Figure 2: Overview of ENISA's work in the area of CSIRTs and LE cooperation



CSIRT - computer security incident response team

LE – Law enforcement

- Implements NIS (Directive (EU) 2016/1148), NIS2 (Directive (EU) 2022/2555) and Cybersecurity toolbox.

81

81