



Is it time to
**rethink our
investments?**



Who am I?

Michalis Kamprianis

MBA, MSc

1.

The Game Rules
Frameworks

Which
framework is
your favorite?

The SMB darling: NIST CyberSecurity Framework



Controls per function

- ▶ Identify: 29
- ▶ Protect: 39
- ▶ Detect: 18
- ▶ Respond: 16
- ▶ Recover: 6



2.

The Numbers

How much
money do you
have to spend?

Investment trends

FIGURE 1

Companies continue to spend more on cybersecurity

Overall cybersecurity spending benchmarks

■ 2019 ■ 2020



Sources: FS-ISAC/Deloitte Cyber & Strategic Risk Services CISO survey reports, 2019 and 2020; Deloitte Center for Financial Services analysis.

Deloitte Insights | deloitte.com/insights

- ▶ Reshaping the cybersecurity landscape, Deloitte Insights, 2020

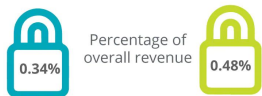
Investment trends

FIGURE 1

Companies continue to spend more on cybersecurity

Overall cybersecurity spending benchmarks

■ 2019 ■ 2020

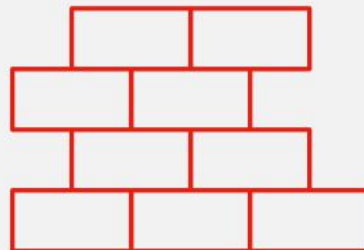


Sources: FS-ISAC/Deloitte Cyber & Strategic Risk Services CISO survey reports, 2019 and 2020; Deloitte Center for Financial Services analysis.

Deloitte Insights | deloitte.com/insights

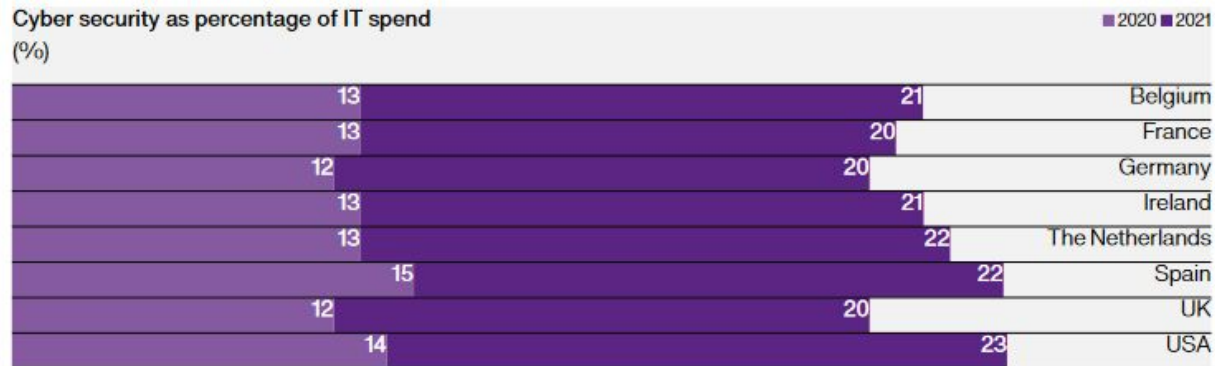
IT budgets reorient to cyber

The average firm now devotes more than a fifth (21%) of its IT budget to cyber security – a jump of 63%.

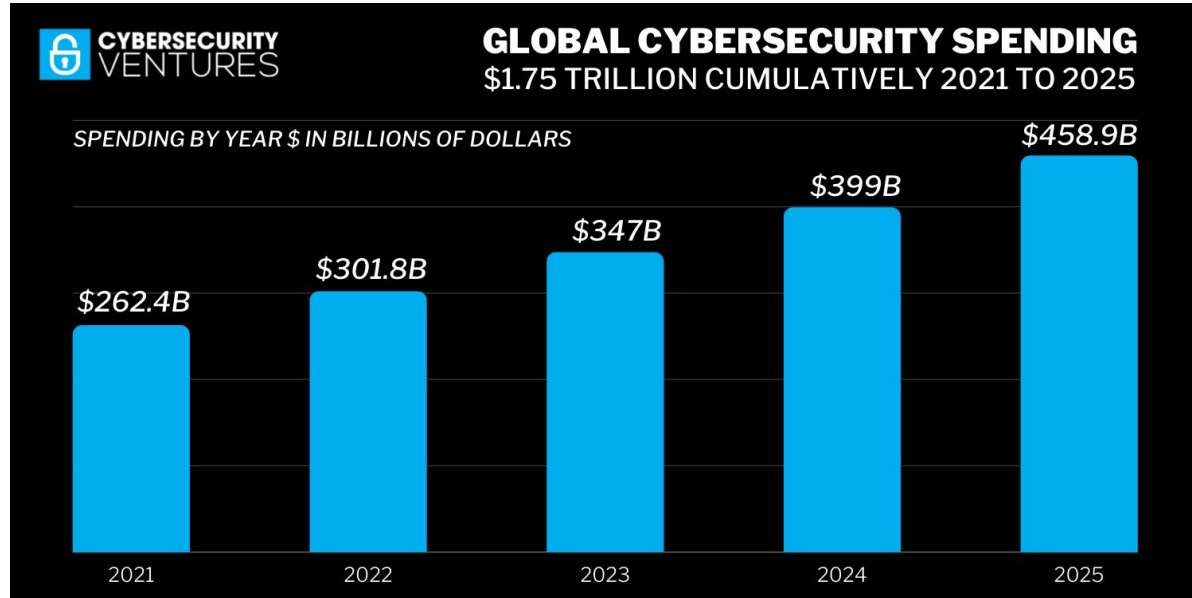


- ▶ Reshaping the cybersecurity landscape, Deloitte Insights, 2020
- ▶ Hiscox Cyber Readiness Report, 2021

Investment trends



Investment trends



Estimated annual growth: 15%

- ▶ Global Cybersecurity Spending To Exceed \$1.75 Trillion From 2021-2025, CyberSecurity Ventures, September 2021

The ambivalent CISO



We can spend more money



It is still not enough

3.

The distribution

What do we
invest on?

Trends in investment distribution

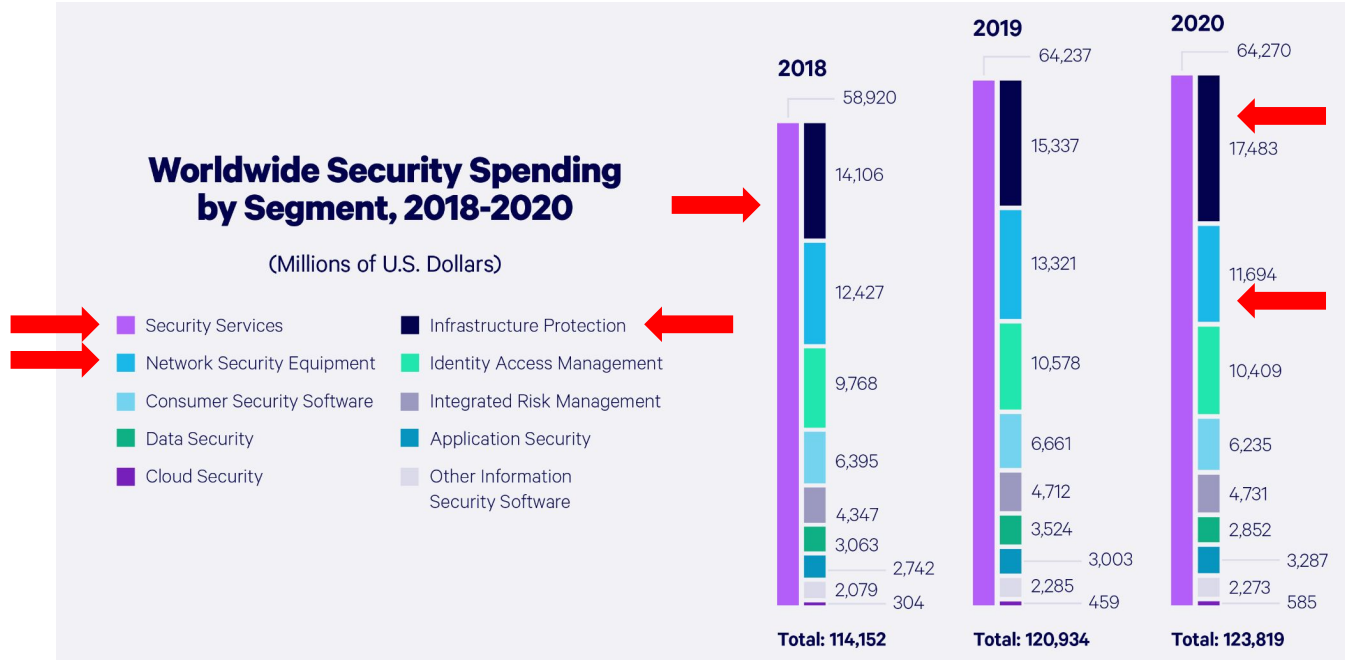


Controls per function

- ▶ Identify: 29 → 27%
- ▶ Protect: 39 → 36%
- ▶ Detect: 18 → 17%
- ▶ Respond: 16 → 15%
- ▶ Recover: 6 → 5%

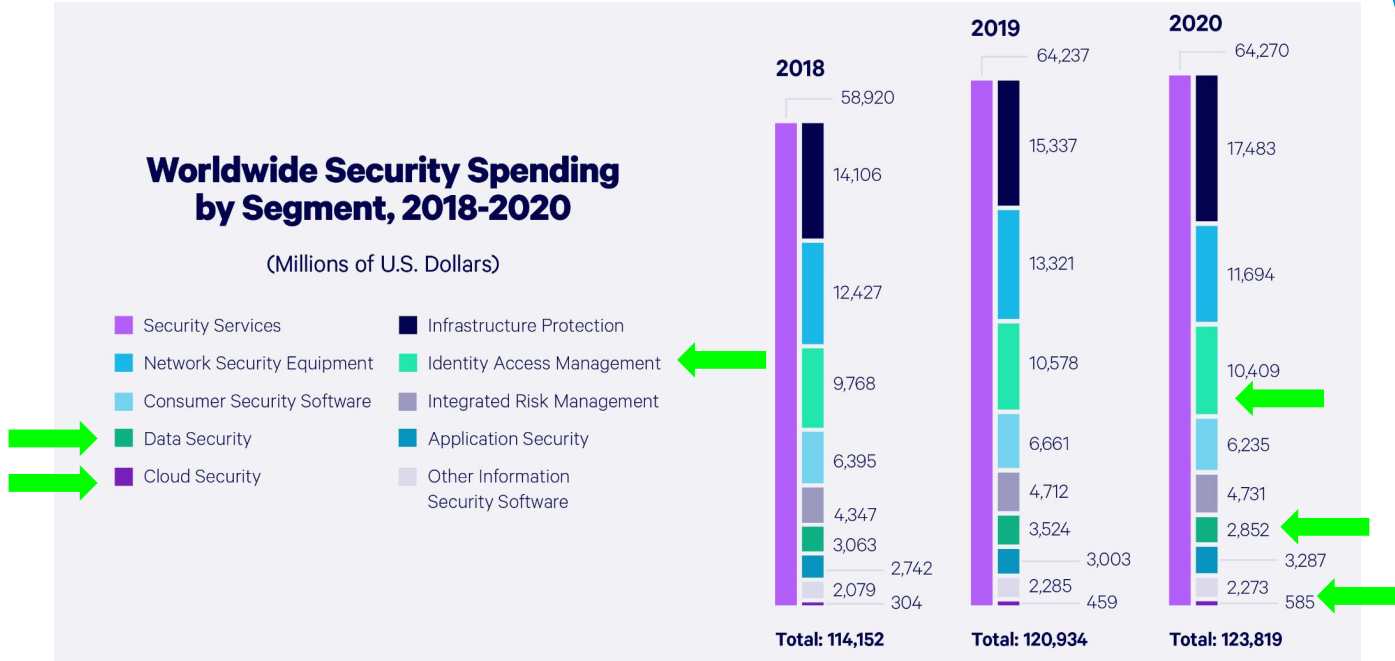
Trends in investment distribution

What are we doing?



Trends in investment distribution

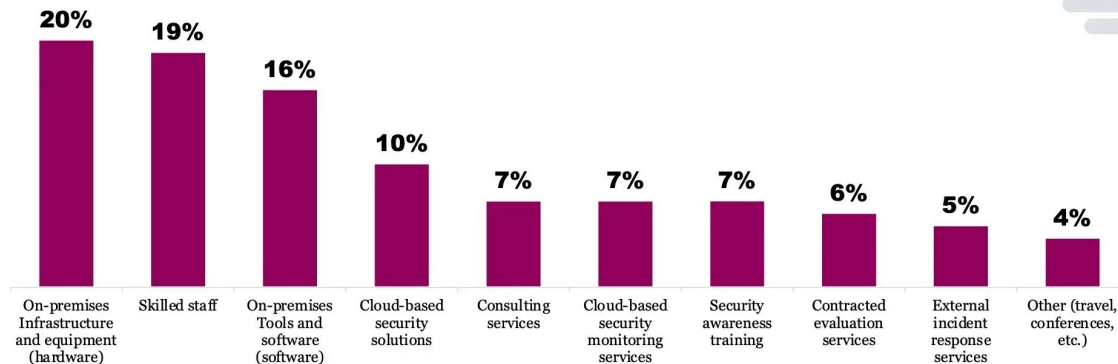
What should we be doing?



► 2022 Must-Know Cyber Attack Statistics and Trends, Embroker, January 2022

Trends in investment distribution

Allocation of Security Budgets



Q. With the total equal to 100%, approximately what percent of your annual budget for IT security will be allocated to the following areas over the next 12 months?

Is our allocation correct?

- ▶ Cybersecurity spending trends for 2022: Investing in the future, December 2021

Trends in investment distribution

Should we change our focus?

Information Security & Risk Management End User Spending by Segment, 2020-2021
(Millions of U.S. Dollars)

Market Segment	2020	2021	Growth (%)
Application Security	3,333	3,738	12.2
Cloud Security	595	841	41.2
Data Security	2,981	3,505	17.5
Identity Access Management	12,036	13,917	15.6
Infrastructure Protection	20,462	23,903	16.8
Integrated Risk Management	4,859	5,473	12.6
Network Security Equipment	15,626	17,020	8.9
Other Information Security Software	2,306	2,527	9.6
Security Services	65,070	72,497	11.4
Consumer Security Software	6,507	6,990	7.4
Total	133,776	150,409	12.4



Source: Gartner (May 2021)

- ▶ Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed \$150 Billion in 2021 (May, 2021)

4.

The questionable

Do these controls
still provide the
intended value?

Consider the value of these controls

Modern environment

- Containers, Serverless computing
- Cloud services, O365
- Cloud applications, Serverless computing

Value needs to be re-assessed

- ❑ Anti-malware (on servers)
 - ❑ DE.CM-4: Malicious code is detected
- ❑ Everything on access
 - ❑ PR.AC-3: Remote access is managed
 - ❑ PR.AC-2: Physical access to assets is managed and protected
- ❑ Vulnerability scans
 - ❑ ID.RA-1: Asset vulnerabilities are identified and documented

How will you address these controls?

NIST control

- PR.DS-5: Protections against data leaks are implemented
- PR.IP-4: Backups of information are conducted, maintained, and tested
- PR.IP-6: Data is destroyed according to policy

Challenges

- Do you know where your data is?
- Do you have one (or more tools) for DLP?
- Can you even do a test restore in e.g. SFDC or O365?
- Can you even delete data from O365?



THANK YOU!

Any questions? Ask me now or

On Twitter: @kamprianism

By email: michalis.kamprianis@gmail.com

At my blog: <https://kamprianis.eu/michalis/i.think>

On LinkedIn: <https://www.linkedin.com/in/michaliskamprianis>



Resources and data

<https://www.nist.gov/cyberframework>

<https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html>

<https://www.hiscox.co.uk/sites/default/files/documents/2021-04/21486-Hiscox-Cyber-Readiness-Report-2021-UK.pdf>

<https://cybersecurityventures.com/cybersecurity-spending-2021-2025/>

<https://www.embroker.com/blog/cyber-attack-statistics/>

<https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem>

<https://www.csoonline.com/article/3645091/cybersecurity-spending-trends-for-2022-investing-in-the-future.html>