Cybersecurity

Facts, Perception and Considerations to Move Forward

Harvard Business Turkey Webinar

Ümit Yalçın Şen, Partner, KPMG Turkey

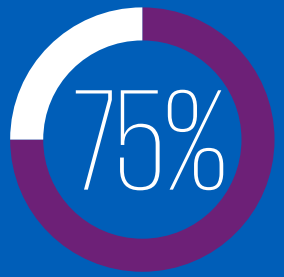
27 September 2022

Agenda

- Global considerations
- Facts and Figures
  - Perception: Is it not working?
- Mindset shift needed

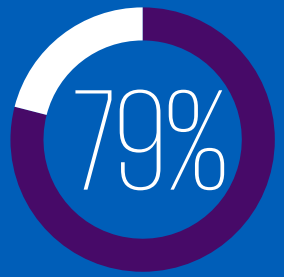
Cyber is the #1 risk to growth

Cyber security risk tied with today's burning environmental and supply chain issues as the top threat to organizational growth over the next three years.



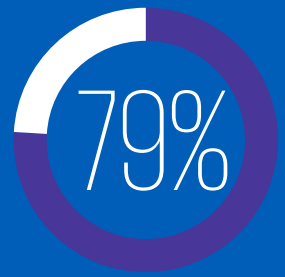
Building cyber trust

Majority of CEOs believe a strong cyber strategy is critical to engender trust with key stakeholders.



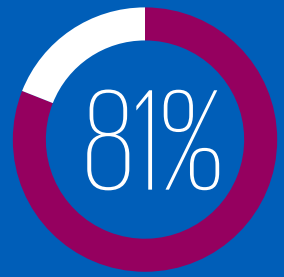
Grasping the supply chain security challenge

CEOs now see the challenge of protecting their partner ecosystem and supply chains as being just as important as building their own organization's cyber defenses.



Cyber security — a competitive advantage

CEOs view information security as a strategic function and as a potential source of competitive advantage.



Building a cyber security culture

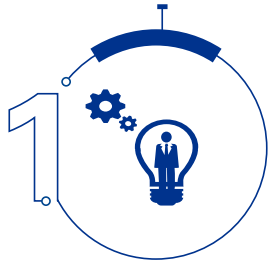
CEOs say that "building a cyber security culture" is just as important as building technological controls.

Source: KPMG 2021 CEO Outlook.

Eight key cyber security considerations for 2022+

Expanding the strategic security conversation

Change the conversation from cost and speed to effective security to help deliver enhanced business value and user experience.



Achieving the x-factor: Critical talent and skillsets

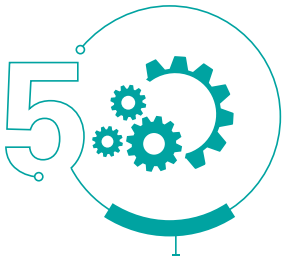
Transform the posture of CISOs and their teams from cyber security enforcers to influencers.

Adapting security for the cloud

Enhance cloud security through automation — from deployment and monitoring to remediation.

Placing identity at the heart of zero trust

Put IAM and zero trust to work in today's hyperconnected workplace.



Exploiting security automation

Use smart deployment of security automation to help realize business value and gain a competitive advantage.

Protecting the privacy frontier

Move to a multidisciplinary approach to privacy risk management that embeds privacy and security by design.

Securing beyond the boundaries

Transform supply chain security approaches — from manual and time consuming to automated and collaborative.

Reframing the cyber resilience conversation

Broaden the ability to sustain operations, recover rapidly and mitigate the consequences when a cyberattack occurs.

Yet, cost of breaches are increasing (I)

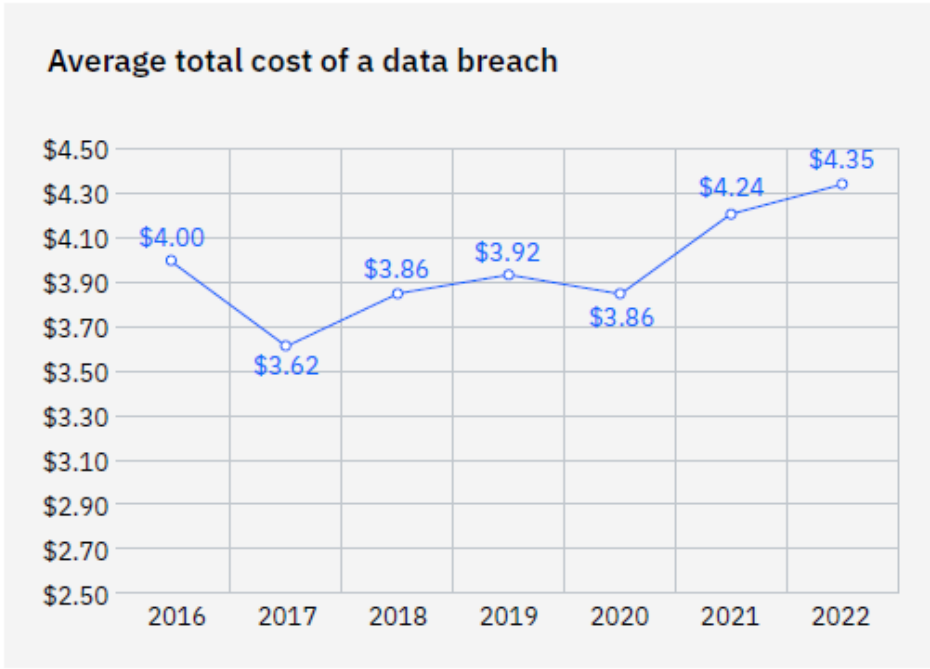


Figure 1: Measured in USD millions

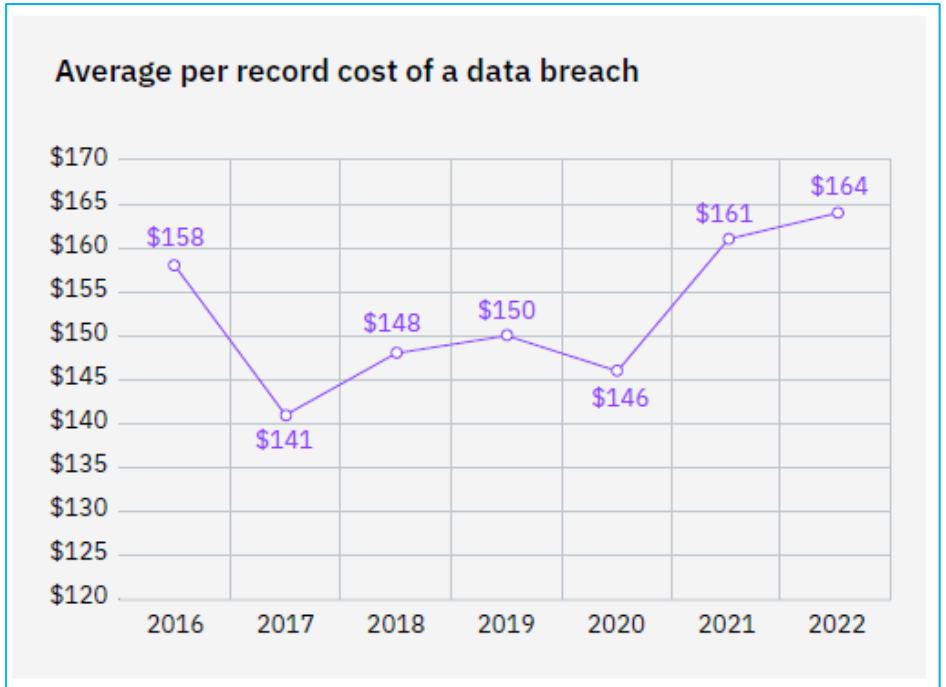


Figure 2: Measured in USD

- 83% of organizations had data breaches
- 60% of them reflected some costs to prices (to customers)
- 79% of orgs in critical organizations have no Zero Trust policy

277

days needed to identify and respond to a breach

Source: Cost of a Data Breach Report 2022, IBM

Yet, cost of breaches are increasing (II)

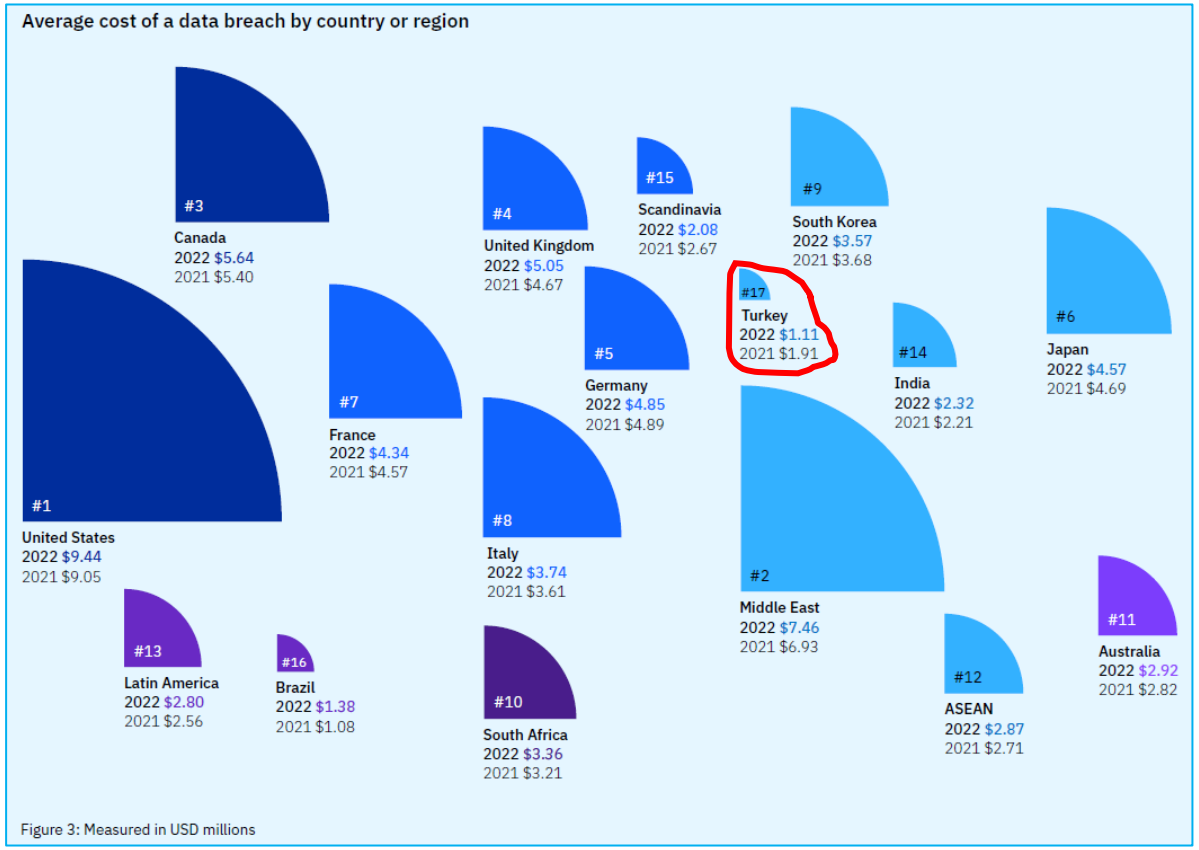


Figure 3: Measured in USD millions

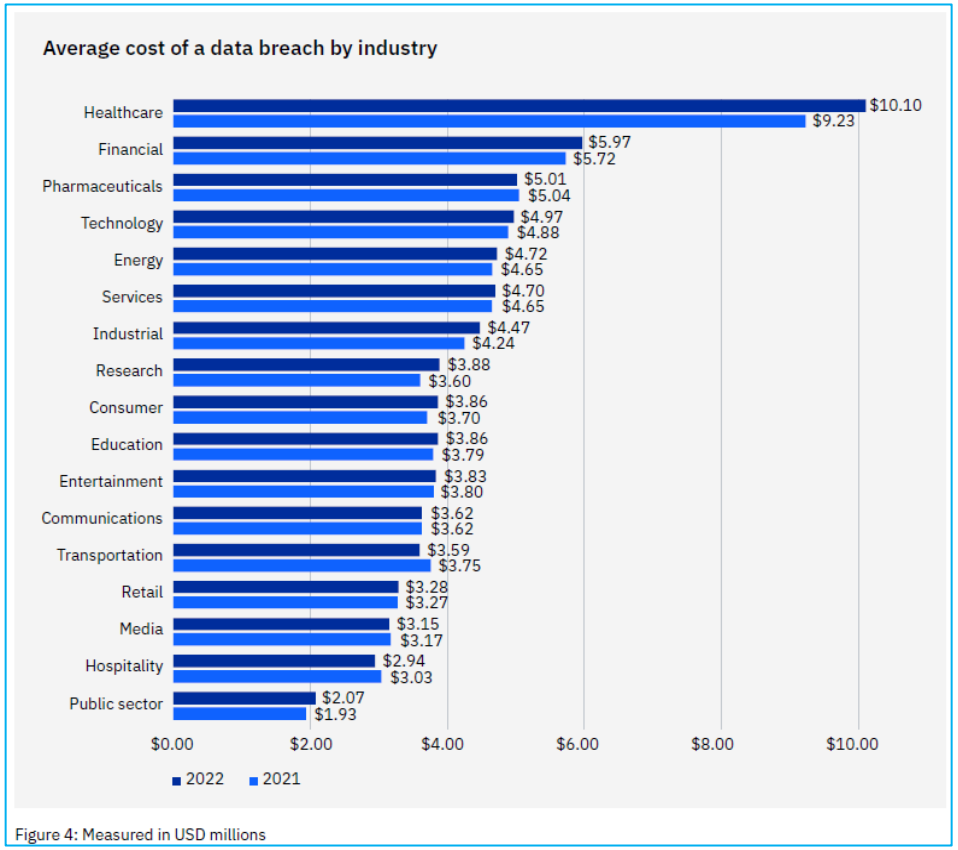


Figure 4: Measured in USD millions

Source: Cost of a Data Breach Report 2022, IBM

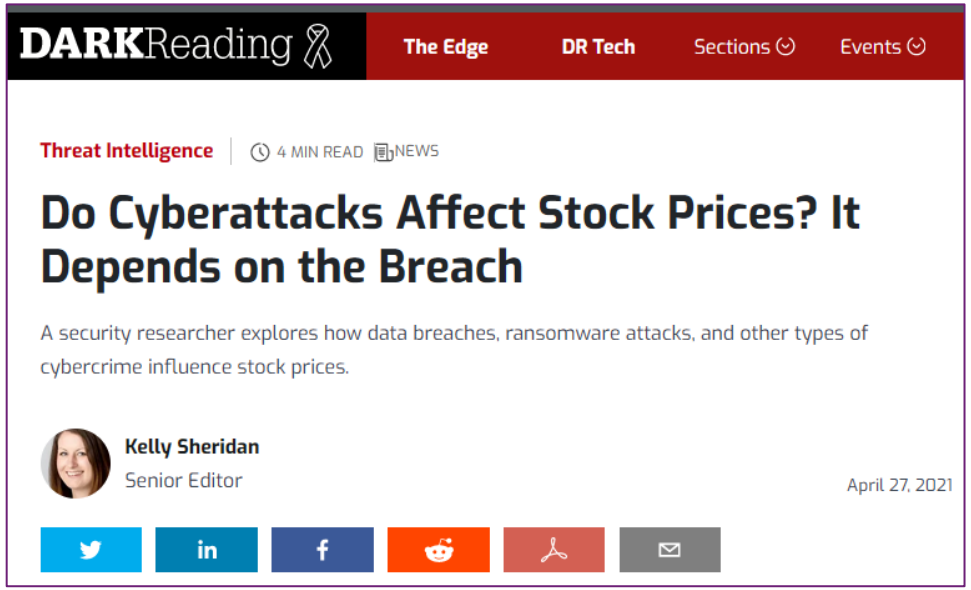
...and more; stock share prices (almost) not impacted by cyber attacks / breaches

Cybersecurity And Digital Privacy

A Cyberattack Doesn't Have to Sink Your Stock Price

by Keman Huang and Stuart Madnick

August 14, 2020 https://hbr.org/2020/08/a-cyberattack-doesnt-have-to-sink-your-stock-price



DARKReading | The Edge | DR Tech | Sections | Events

Threat Intelligence | 4 MIN READ | NEWS

Do Cyberattacks Affect Stock Prices? It Depends on the Breach

A security researcher explores how data breaches, ransomware attacks, and other types of cybercrime influence stock prices.

Kelly Sheridan
Senior Editor

April 27, 2021

*"Stock prices suffer following a breach, but **perhaps not as much as one might assume**. After 14 market days, or roughly three weeks, share prices drop -3.5% on average. In the six months leading up to a breach, average share price grew +2.6%, compared to -3.0% following a breach."*

Comparitech.com (https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis/)

Thus, a mindset change may be a need…

(No) Return on investment

- Limited or no visibility on realization
- Difficult to calculate/estimate impact of cyber incidents on financials and brand

Focus on revenue and brand protection

- Cyber resilience (part of business resilience)
- Security by design / default (new investments, business change, cloud migration etc.)
- Expansion to whole organization (top to bottom)

Non-deterrent fines / penalties

- Investment vs fines mostly favors no-investments
- No stakeholder trust to the system (by public, customers, etc.)

Use regulation as a leverage

- Put RISK at the forefront of each conversation
- Produce compliance as byproduct
- Workload management (get support from Internal Control, Internal Audit, etc.)

Complex/distributed protection technology

- Too many vendors, tools and integrators
- Limited # of trusted service providers
- Lack of required level expertise and support

Automation and vendor consolidation

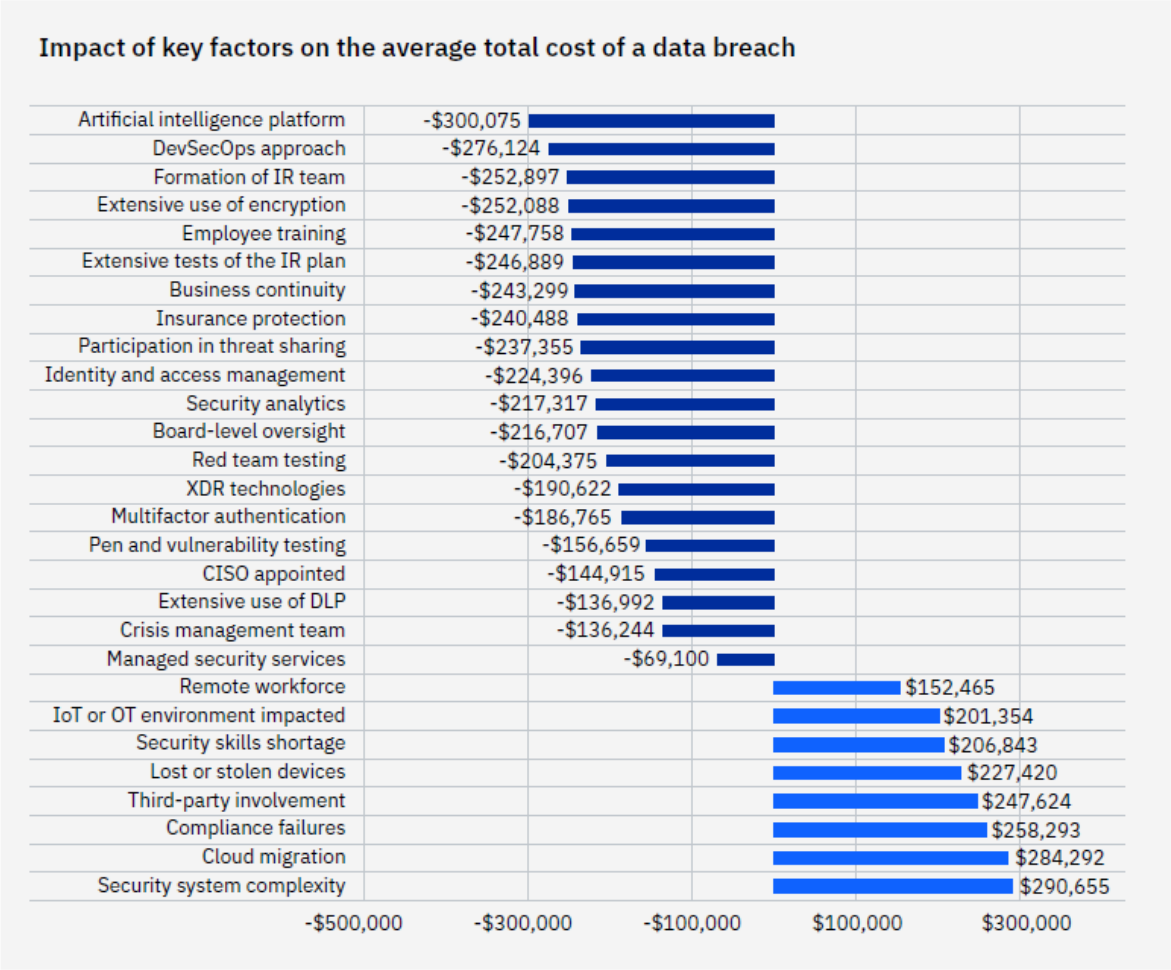
- Utilize more AI/Automation
- Reduce # of vendors, simplify cybersecurity tech
- Consider sourcing model alternatives - accreditate trusted service providers

Talent & Workforce

Main focus!!

KPMG

Mindset change to protect revenue and brand



- **Think from a revenue assurance perspective (proactive vs reactive)**
- **Automation and talent/workforce management is key**
- **Cyber resilience is current/next strategic move**
- **Risk awareness and focus must increase on third-parties, remote work and system complexity**

Source: Cost of a Data Breach Report 2022, IBM