

— Banking IT and FinTech

Cybersecurity

Szabolcs Szalay

February 2025



The Bangladesh heist

<https://www.youtube.com/watch?v=-IZDNAkna5c>

Fraud and insider threats



- Internal and external threats
- Retail and nonretail threats
- Insider threats
- Market abuse and misbehavior

Cyber breaches



- Confidentiality
- Integrity
- Systems availability

Financial crimes



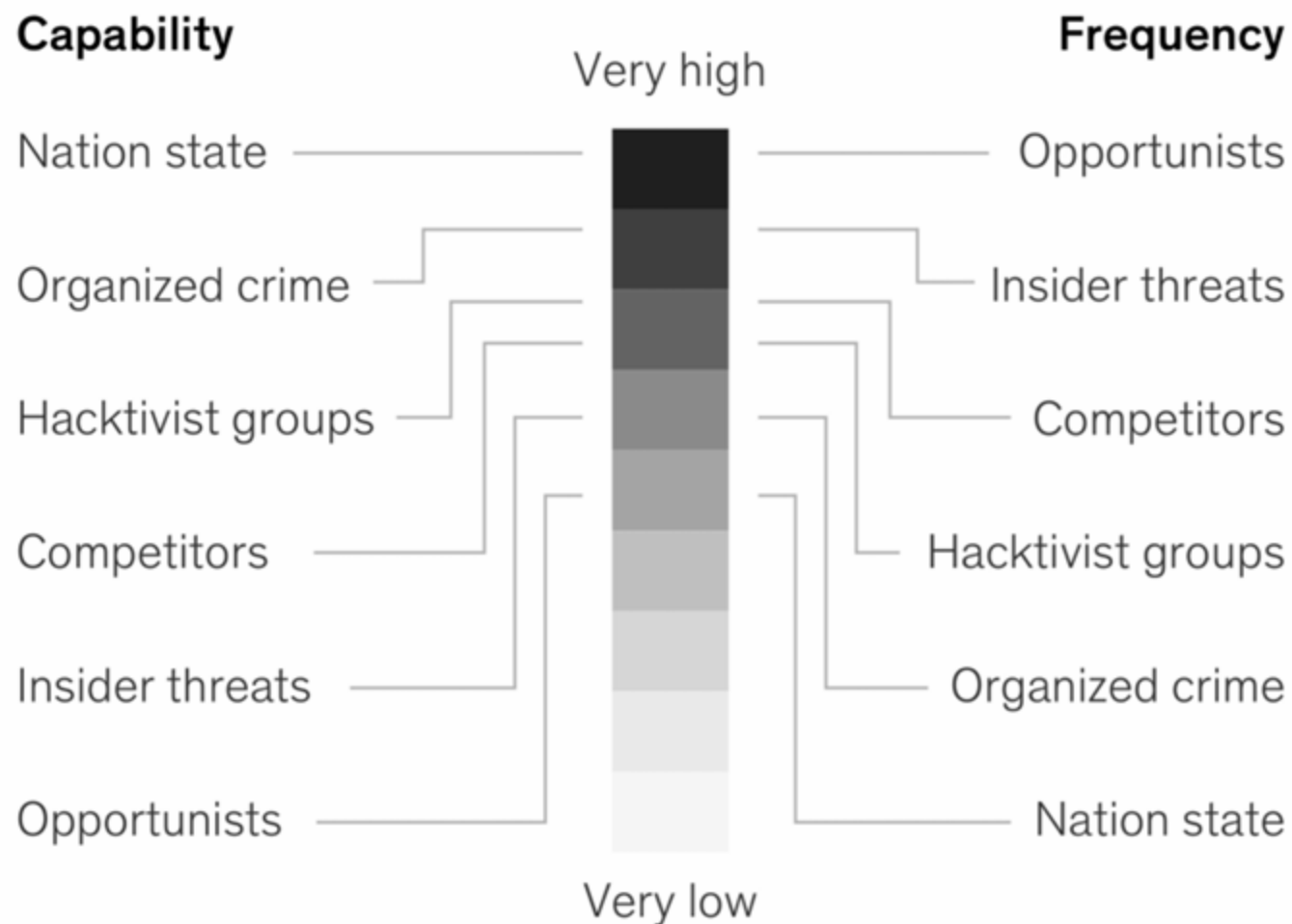
- Money laundering
- Bribery and corruption
- Tax evasion and tax fraud

Example: cyberattack on a central bank

- Bank employee's SWIFT¹ credentials stolen with the help of insiders
- Malware surreptitiously installed on the bank's computers to prevent discovery of withdrawals
- Funds routed from bank's account at a branch of another country's central bank to a third bank (on a weekend to ensure staff absence)
- Withdrawals were made at the third bank through multiple transactions that were not blocked until too late
- Attacks may have been linked to a known sanctioned entity

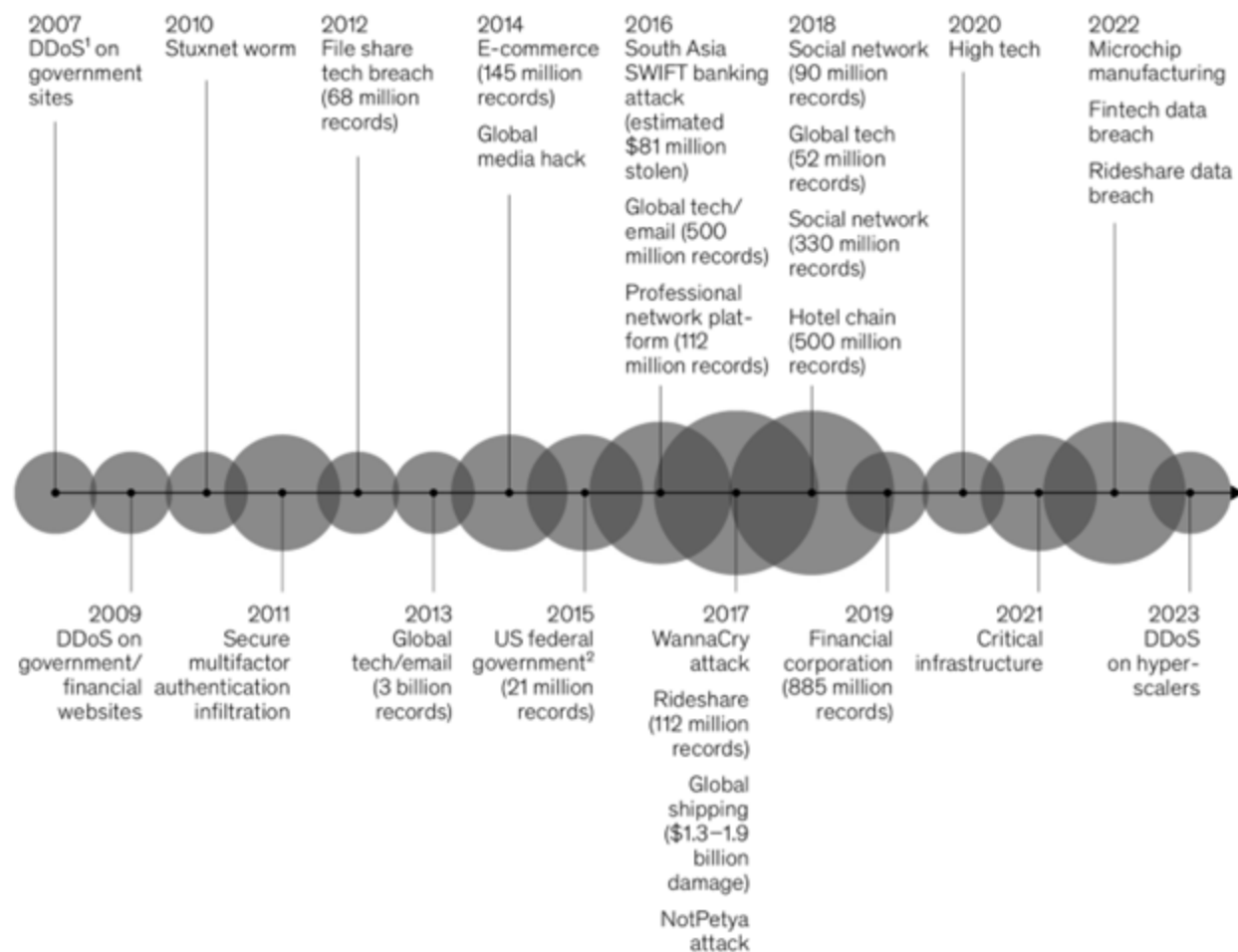
— **Crime categories are converging**

Proliferation of cybercriminals



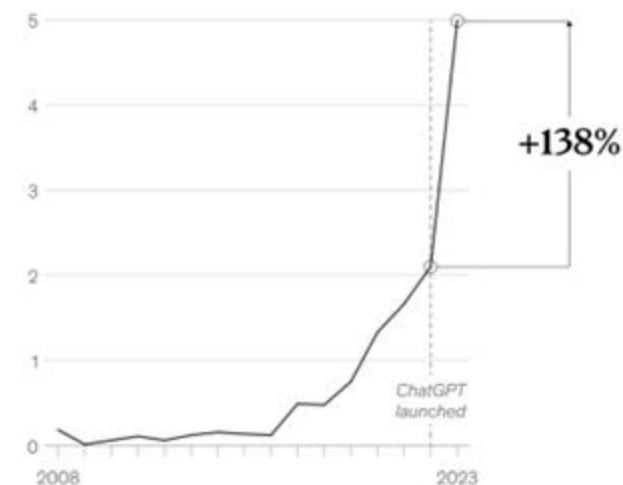
Frequency and severity of attacks increasing

Major cyberincidents, 2007–23



Source: McKinsey

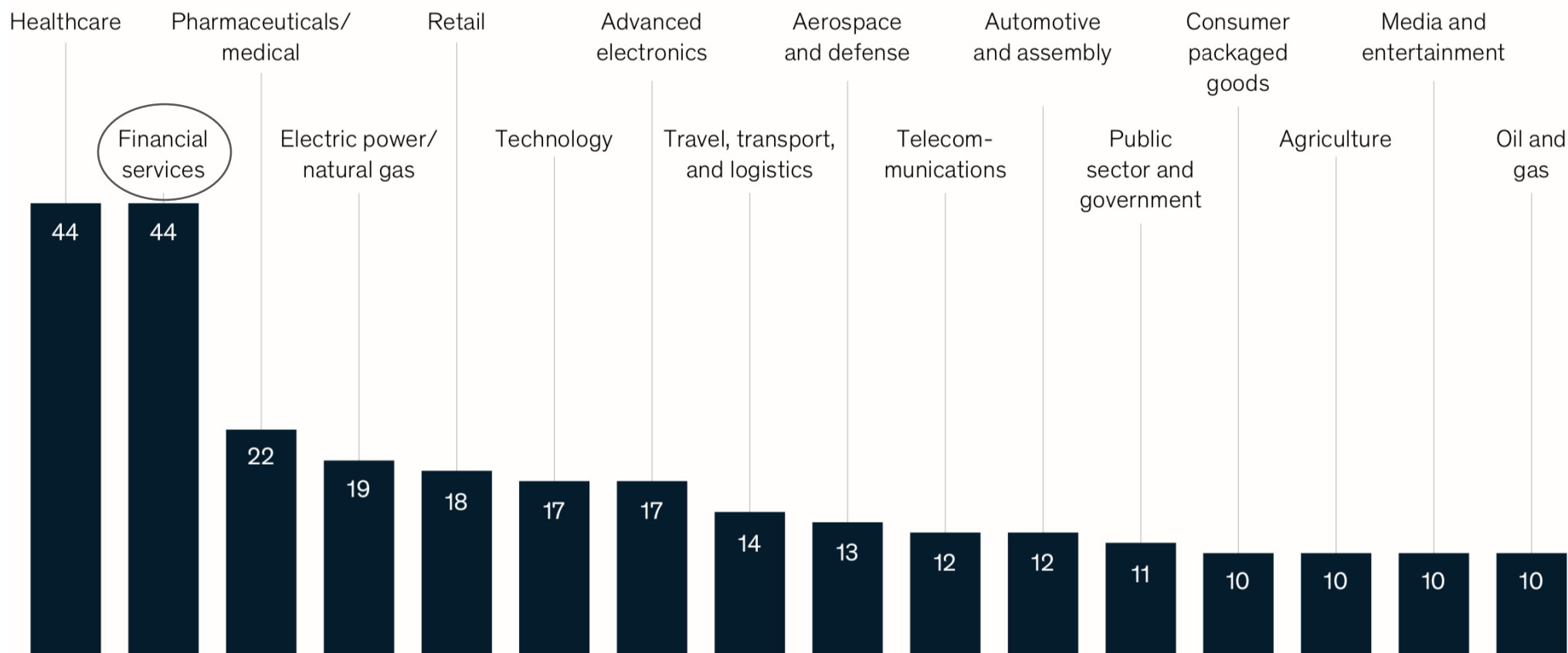
Annual number of phishing sites detected, million



Source: State of the Phish Report, Proofpoint, 2023

Financial services are trustworthy businesses





Respondents choosing a particular industry as most trusted in protecting of privacy and data, % (n = 1,000)



Source: McKinsey Survey of North American Consumers on Data Privacy and Protection, 2019

Many potential fraud attack opportunity in a customer journey

(retail bank example)

Customer-initiated actions				
	Open an account	Change account	Make a payment	Make a deposit
	Customer opens a new account or adds another account through online, mobile, branch, or ATM channels	Customer updates existing account, eg, adding a beneficiary or changing address	Customer pays self or third party through wire, credit or debit card, or online transaction	Customer makes a transfer or deposit into their account
	Attack channel			
	ATM			
	<ul style="list-style-type: none"> • Identity theft • Synthetic ID • Employee-generated account • Malware 	<ul style="list-style-type: none"> • Malware 	<ul style="list-style-type: none"> • Card skimming or trapping • Fake PIN pad • Cash trapping • Shoulder surfing • Duplicate card • Malware • Transaction reversal 	<ul style="list-style-type: none"> • Money laundering or terror financing • Malware (balance multiplier)
	Cards and e-commerce			
		<ul style="list-style-type: none"> • Account takeover • Address change • Secondary card • Malware 	<ul style="list-style-type: none"> • Card-not-present fraud • Card skimming • Malware • Cyberattack 	
	E-banking and wire			
		<ul style="list-style-type: none"> • Addition of false beneficiary • Account takeover • Malware 	<ul style="list-style-type: none"> • Cyberattack • Malware • Employee-driven transaction 	
	Branch			
		<ul style="list-style-type: none"> • Account takeover 	<ul style="list-style-type: none"> • n/a 	



1. Spear phishing

Employee in targeted organization receives email with the Carbanak backdoor as an attachment



2. Backdoor executed: credentials stolen

Upon opening attachment, employee activates the Carbanak backdoor



3. Machines infected in search for admin PC

Carbanak searches network and finds admin PC; embeds and records



4. Admin PC identified, clerk screens intercepted

Attacker watches admin screen to mimic admin behavior for the bank's cash-transfer systems



5. Balances inflated and inflated amount transferred

Attackers alter balances, pocket extra funds (\$1k account enlarged to \$10k, then \$9k transferred)



6. ATM programmed to dispense cash

Attackers program ATMs to issue cash to waiting accomplices at specific times



7. Cash moved through channels by wire transfers, e-payments

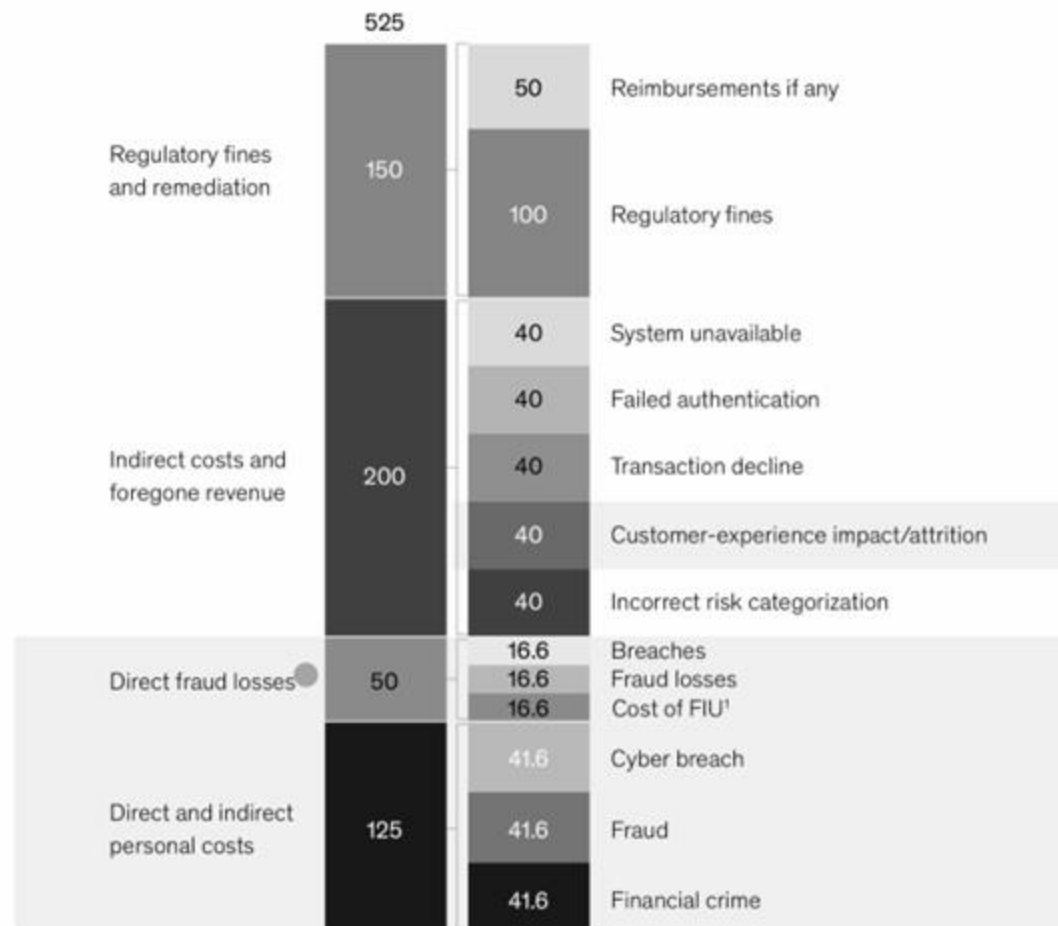
Attackers use online and e-payments to transfer extracted funds

The Carbanak attack

One of the most sophisticated and successful cyber heists in banking history

Banks often underestimate the total cost of financial crime

Example of financial-crime, fraud, and cybersecurity costs, \$ million



- Bank is in second quartile on customer satisfaction for fraud cards
- Satisfied customers are twice as likely to spend more on their cards than are unsatisfied customers

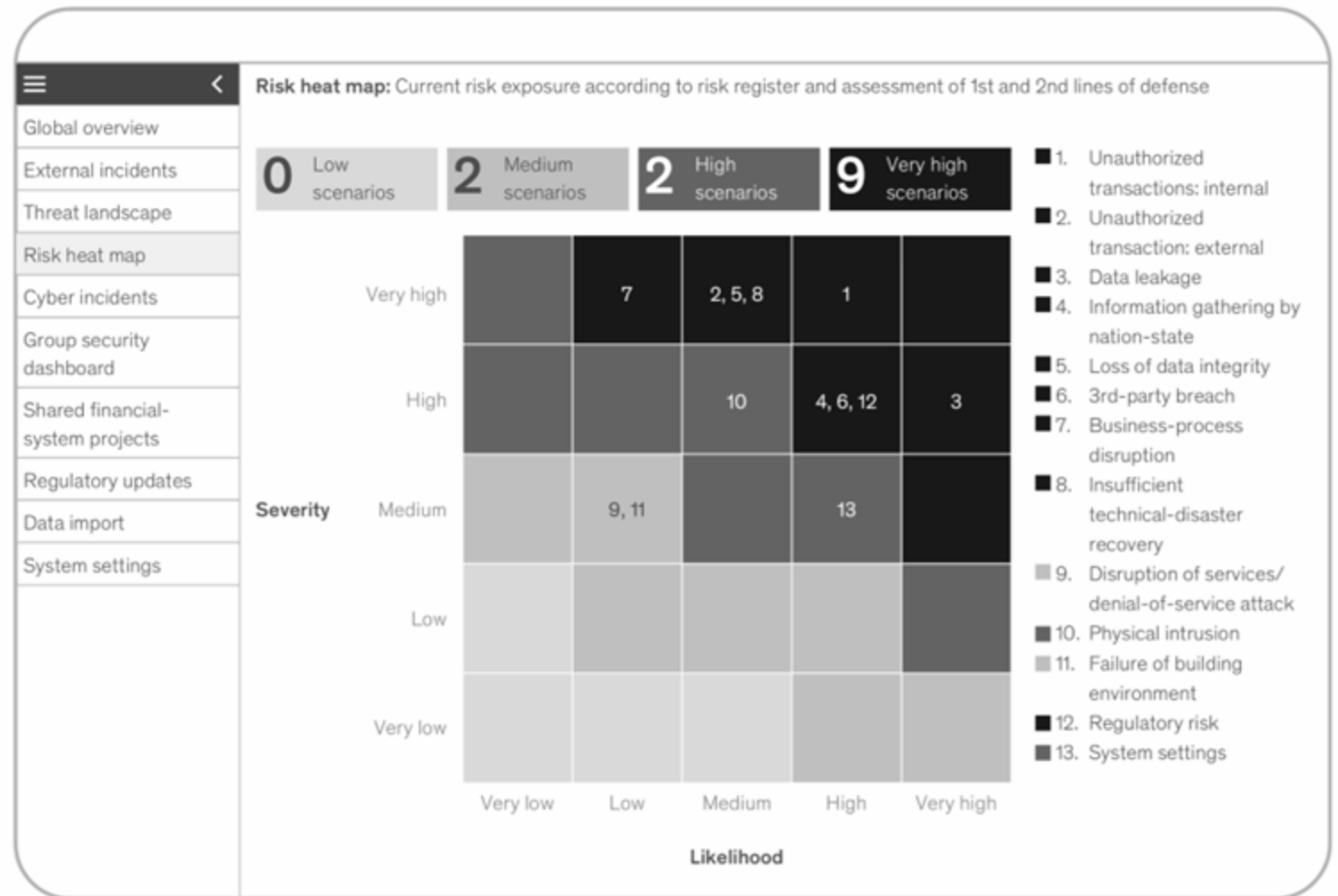
Bank focus areas

- Costs of all three lines of defense
- Much of the cost is in the first line
- Banks in this region typically spend 20 to 40 basis points of revenue on anti-money laundering

¹ Financial intelligence unit.

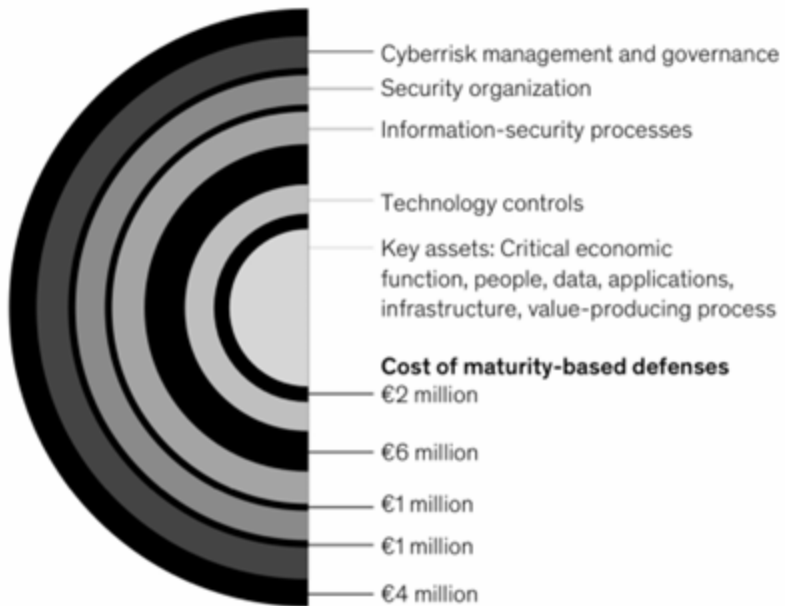
Best practice: risk-based approach to controls

Cyber risk dashboard, example



— Risk based approach is more budget conscious

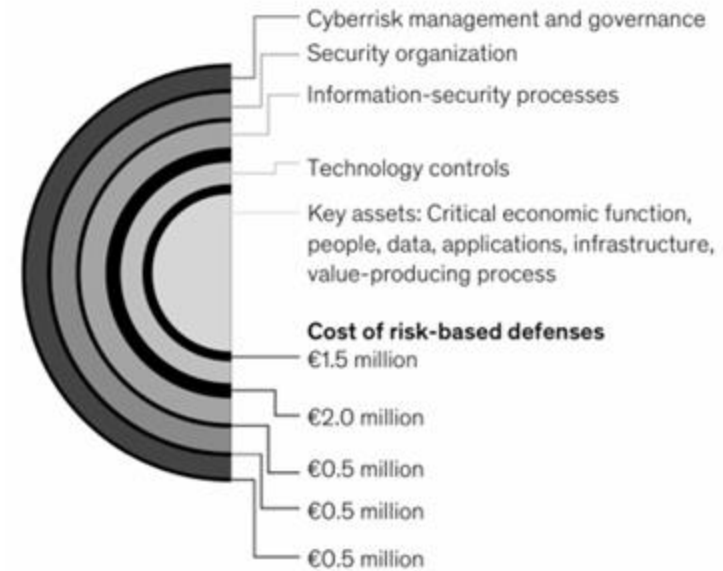
Maturity-based approach: Builds highest level of defense around everything.



Total cost

€14 million

Risk-based approach: Optimizes defensive layers for risk-reduction and cost. Critical assets are highly protected, but at less expense and in ways that improve productivity.



Total cost

€5 million

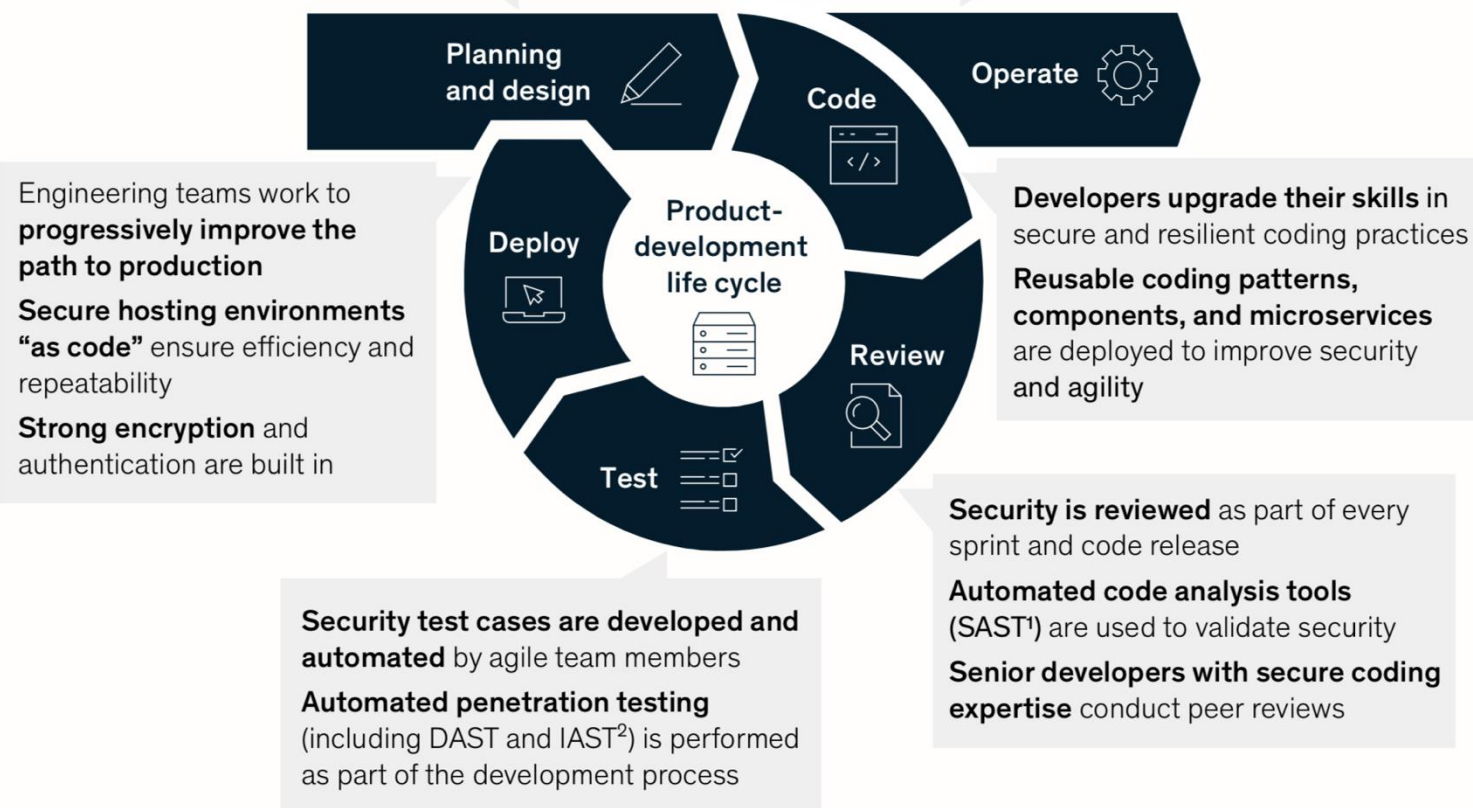
Note: Costs are illustrative but extrapolated from real-world examples and estimates.

DevSecOps

Security is integrated into every step in the product development life cycle.

Agile teams are aware of their security responsibilities from the outset; security champions are embedded in teams
Teams quickly model threats for all significant efforts
Backlog items are created, prioritized, and tracked to meet security and reliability requirements
Secure architecture designs are preapproved for implementation

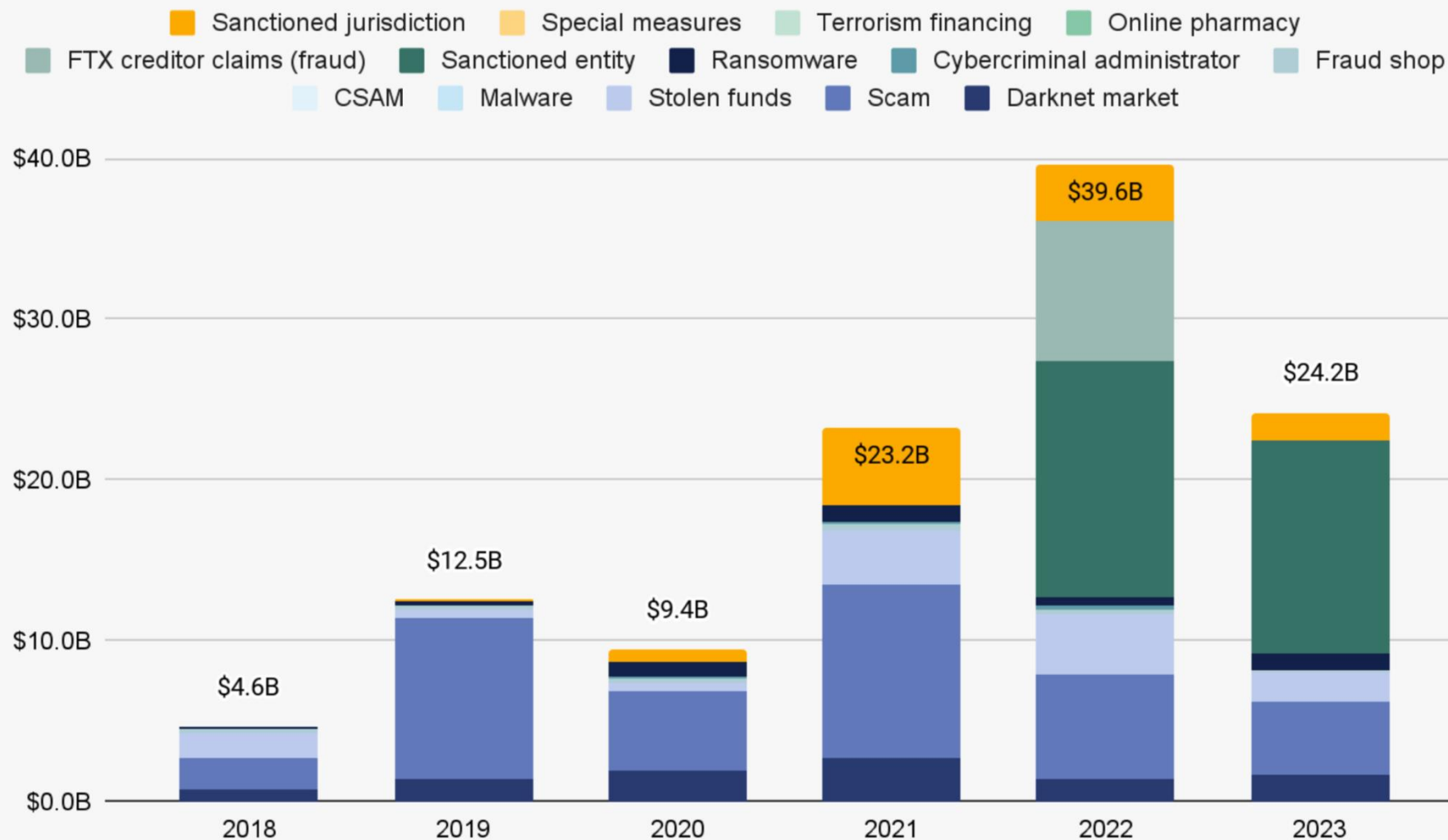
Real-time monitoring of app run time ensures potential security issues are identified
Host and network-based intrusion detection is implemented
Compliance validation and evidence gathering are automated



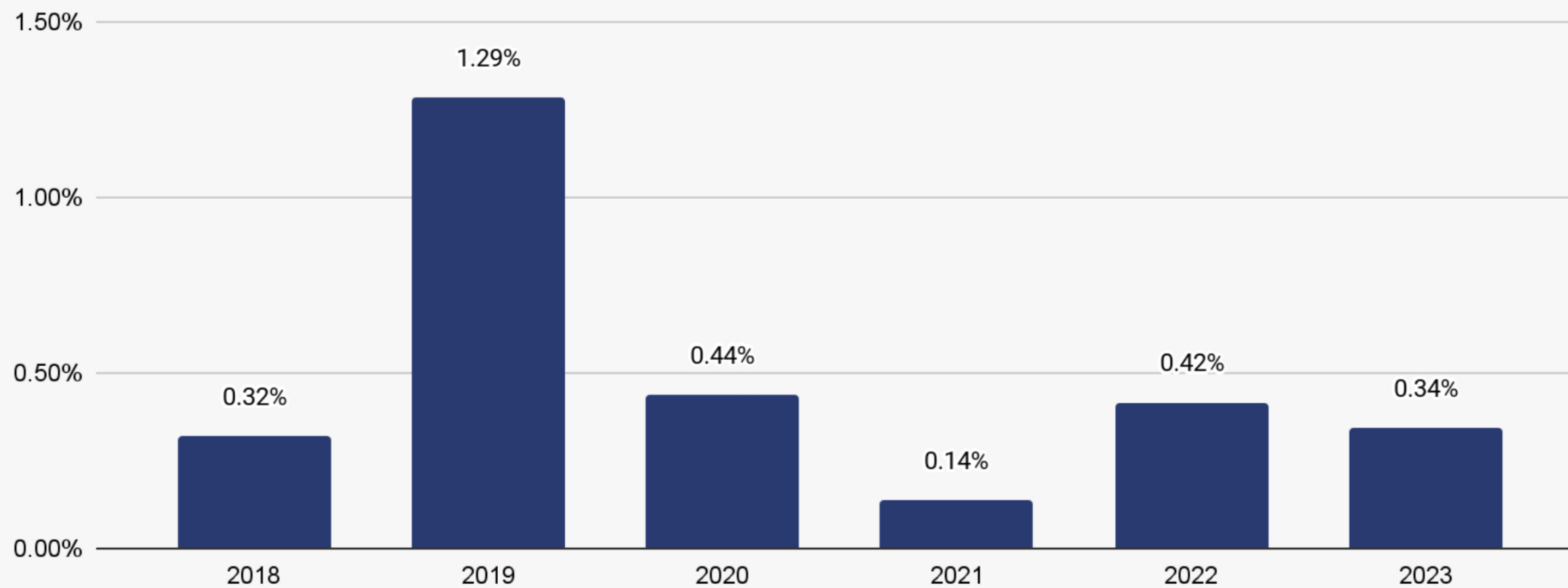
— **Coming next: Zoom into crypto crime...**

Total cryptocurrency value received by illicit addresses

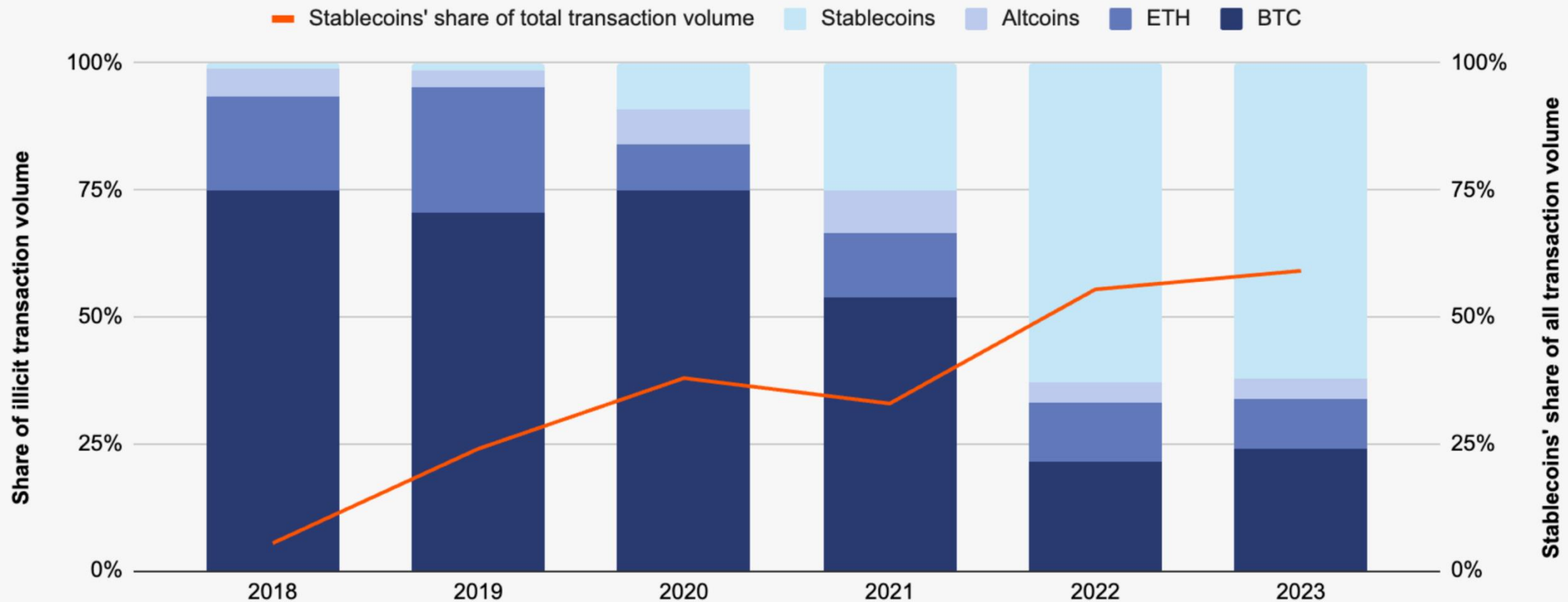
2018 - 2023



Illicit share of all cryptocurrency transaction volume 2018 - 2023

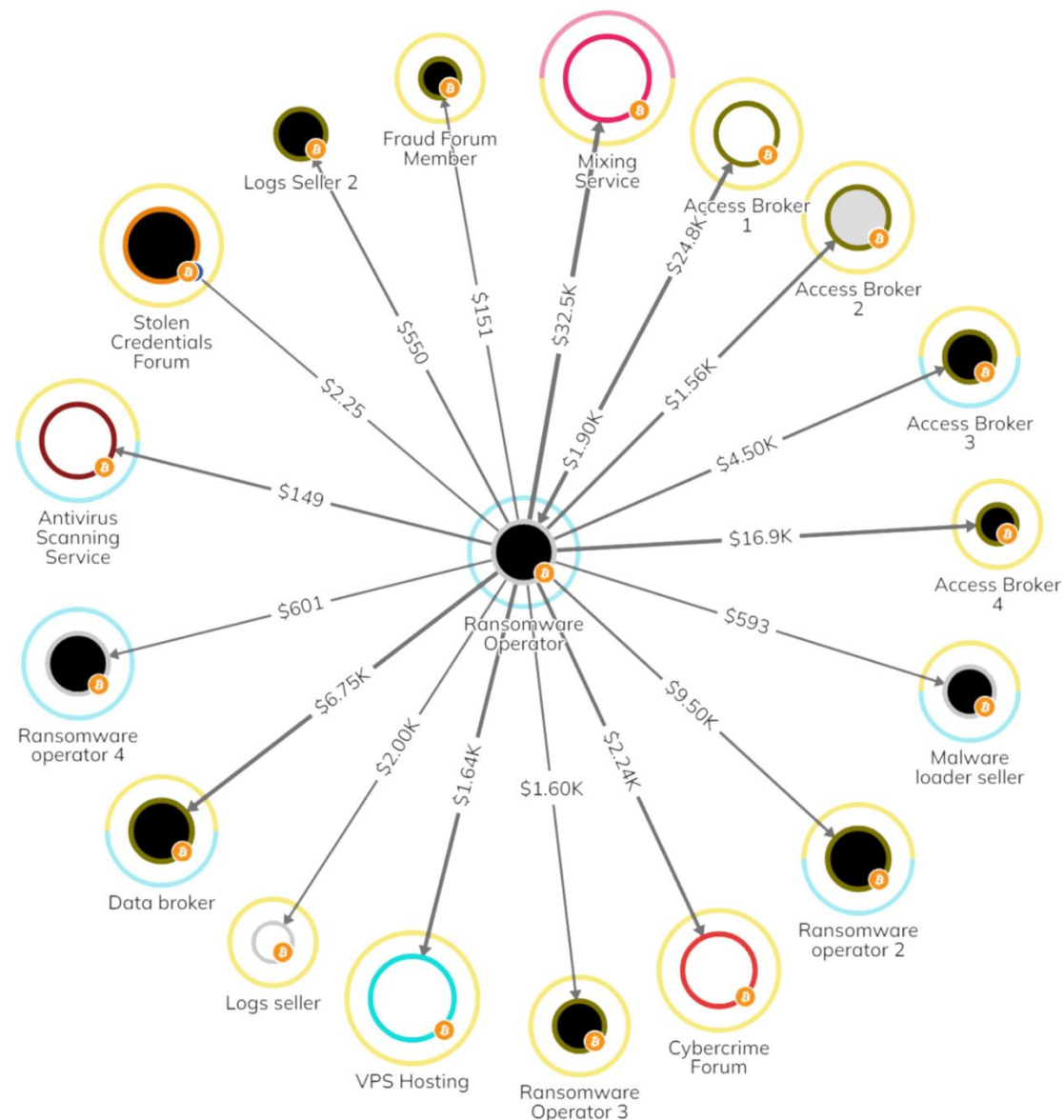


Illicit transaction volume by asset type 2018 - 2023

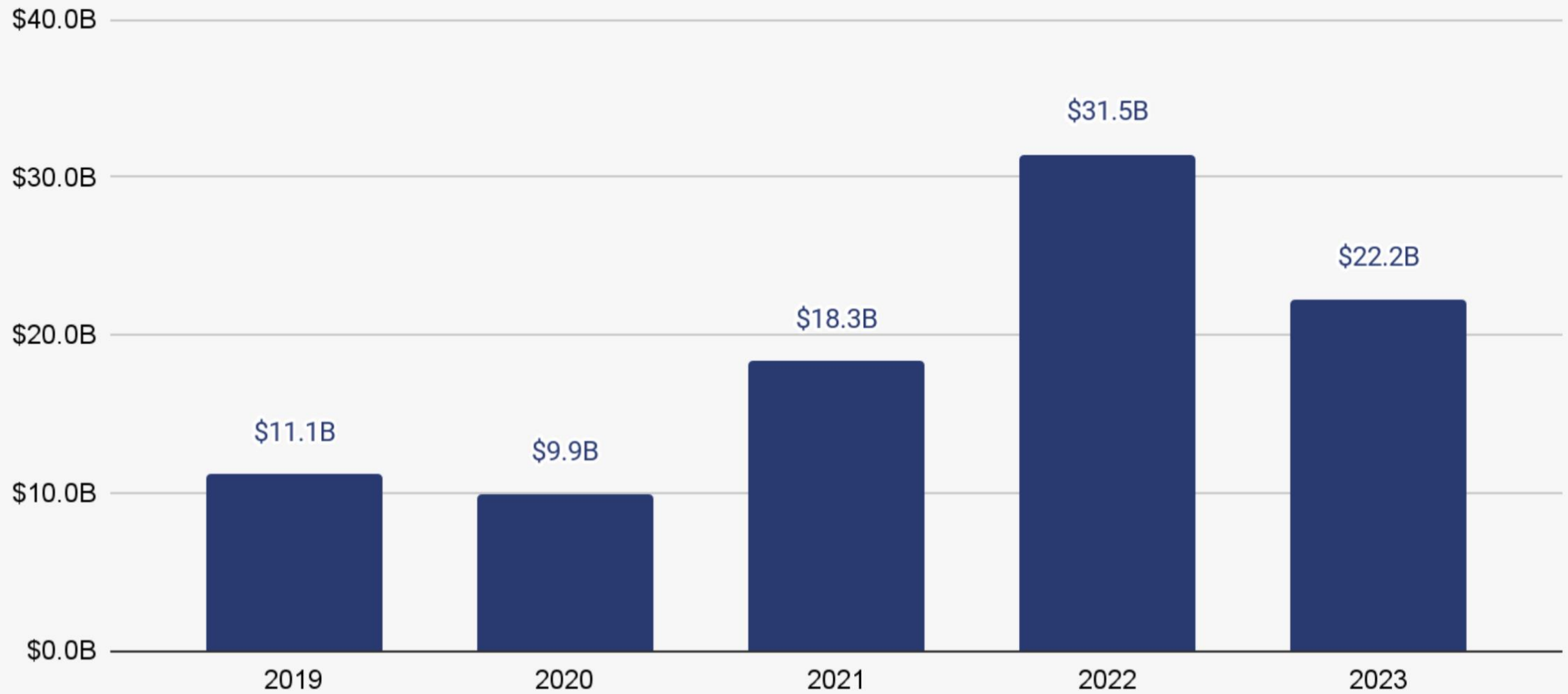


The spread of Ransomware-as-a-Service (RaaS)

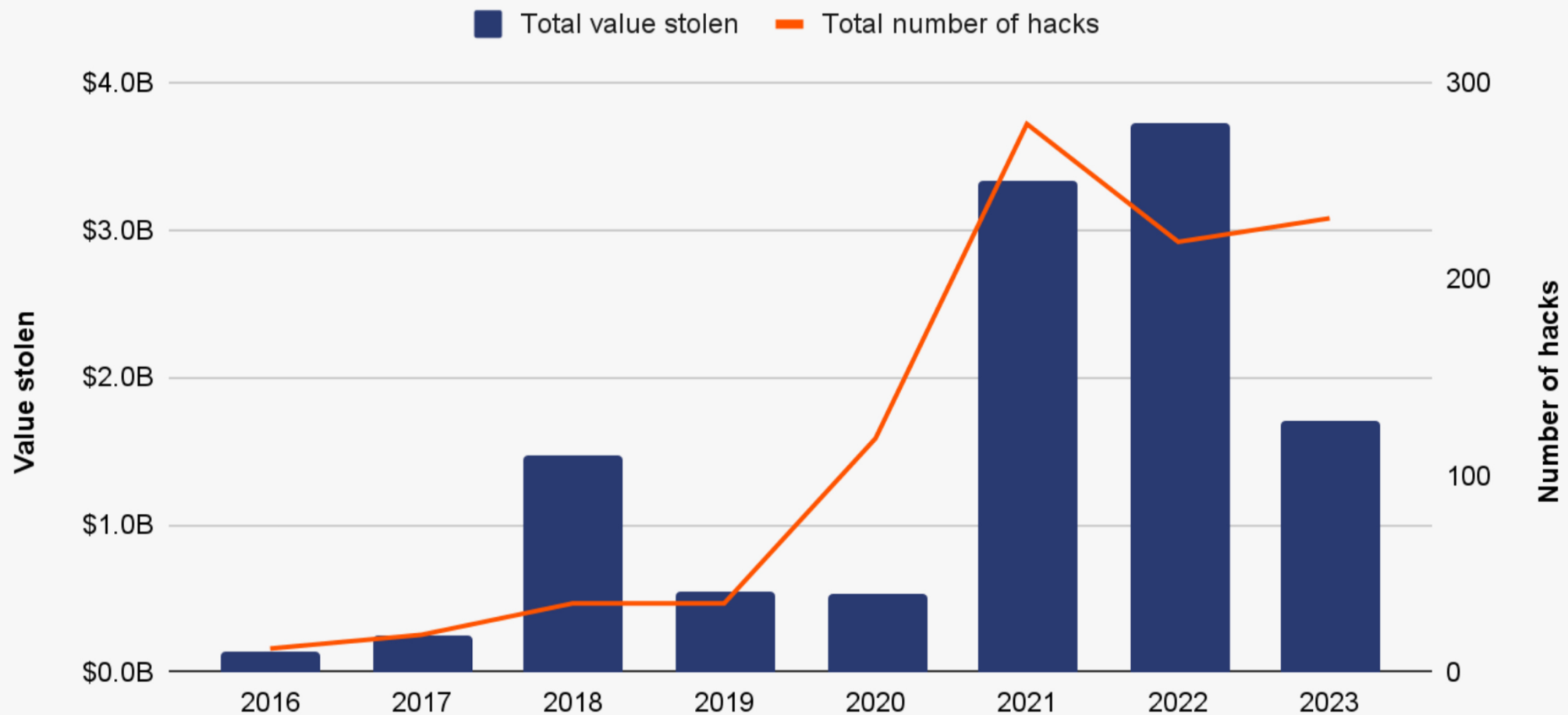
The Reactor graph on the right size shows a ransomware operator sending funds to several initial access brokers and other purveyors of tools useful for ransomware attacks



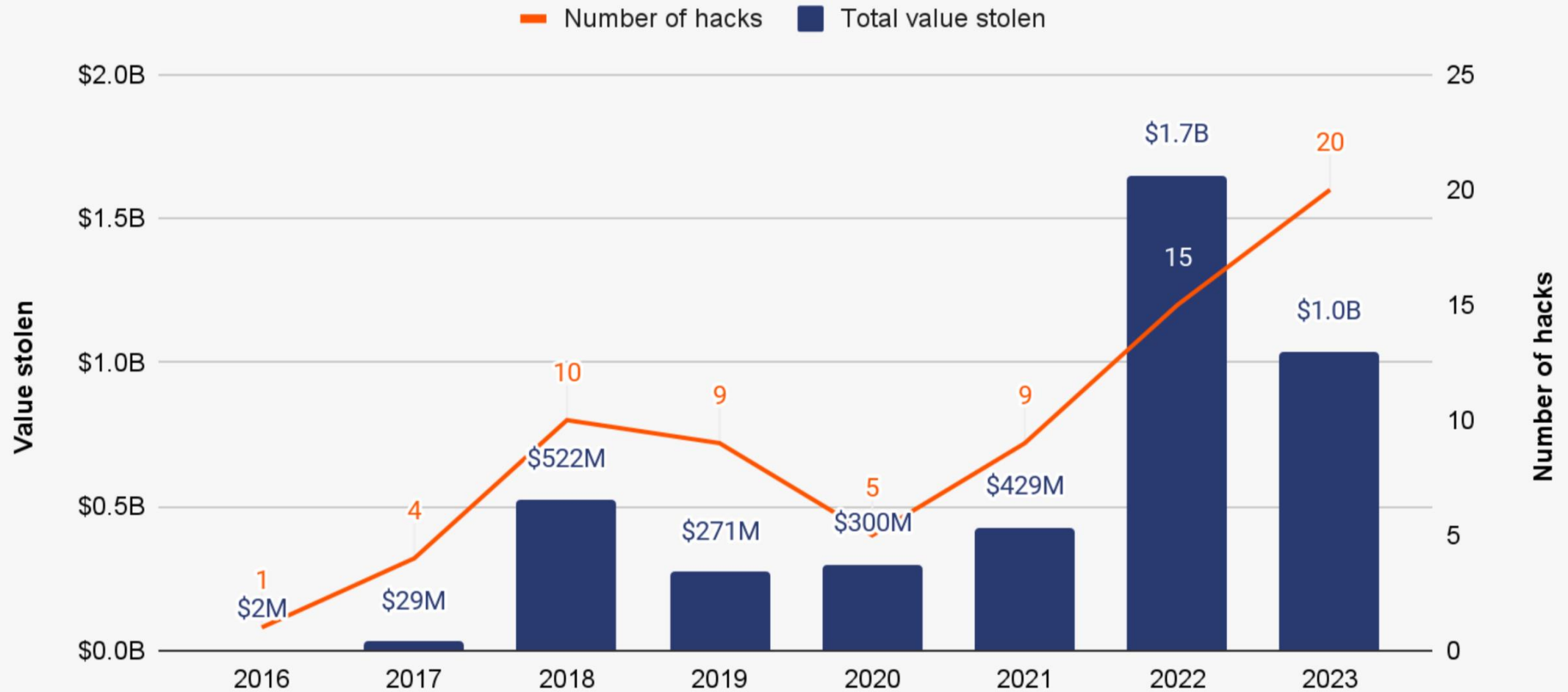
Total cryptocurrency laundered by year 2019 - 2023



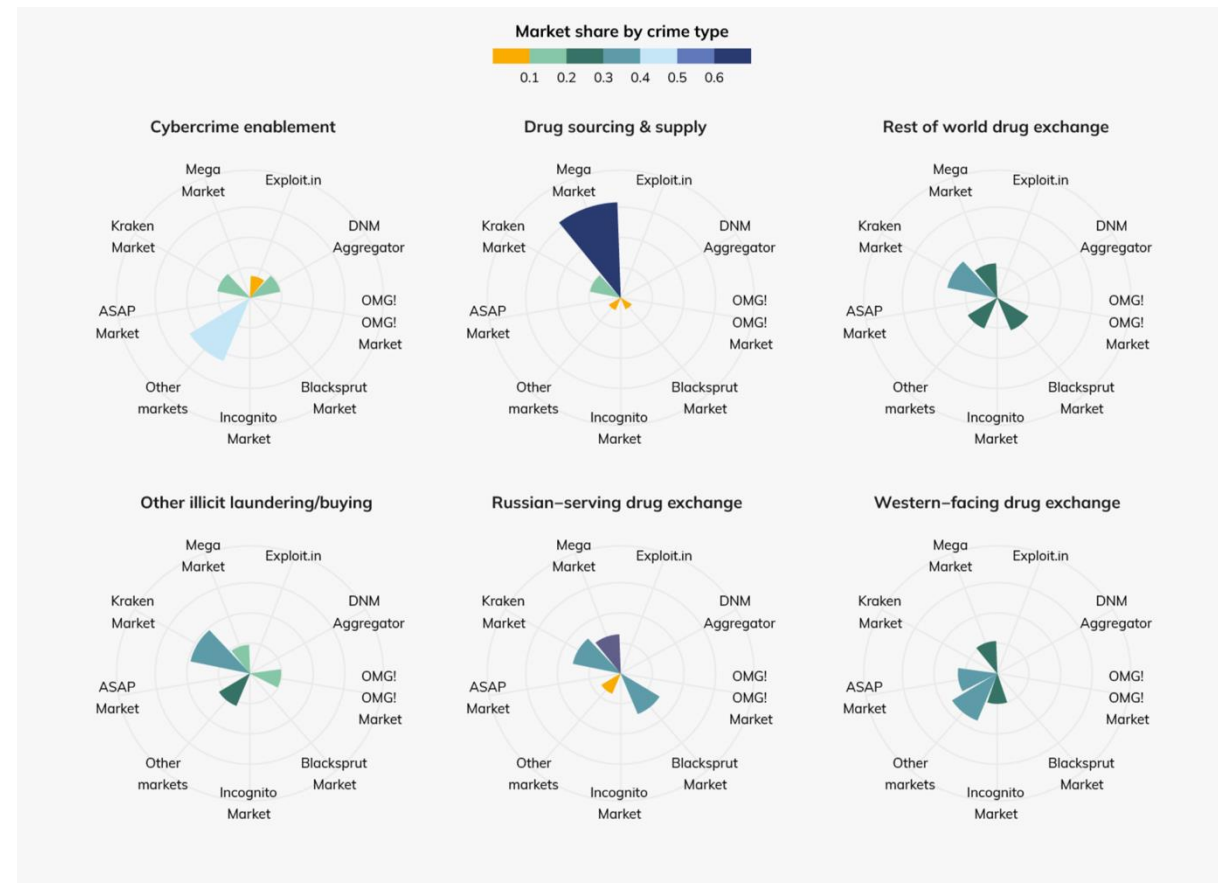
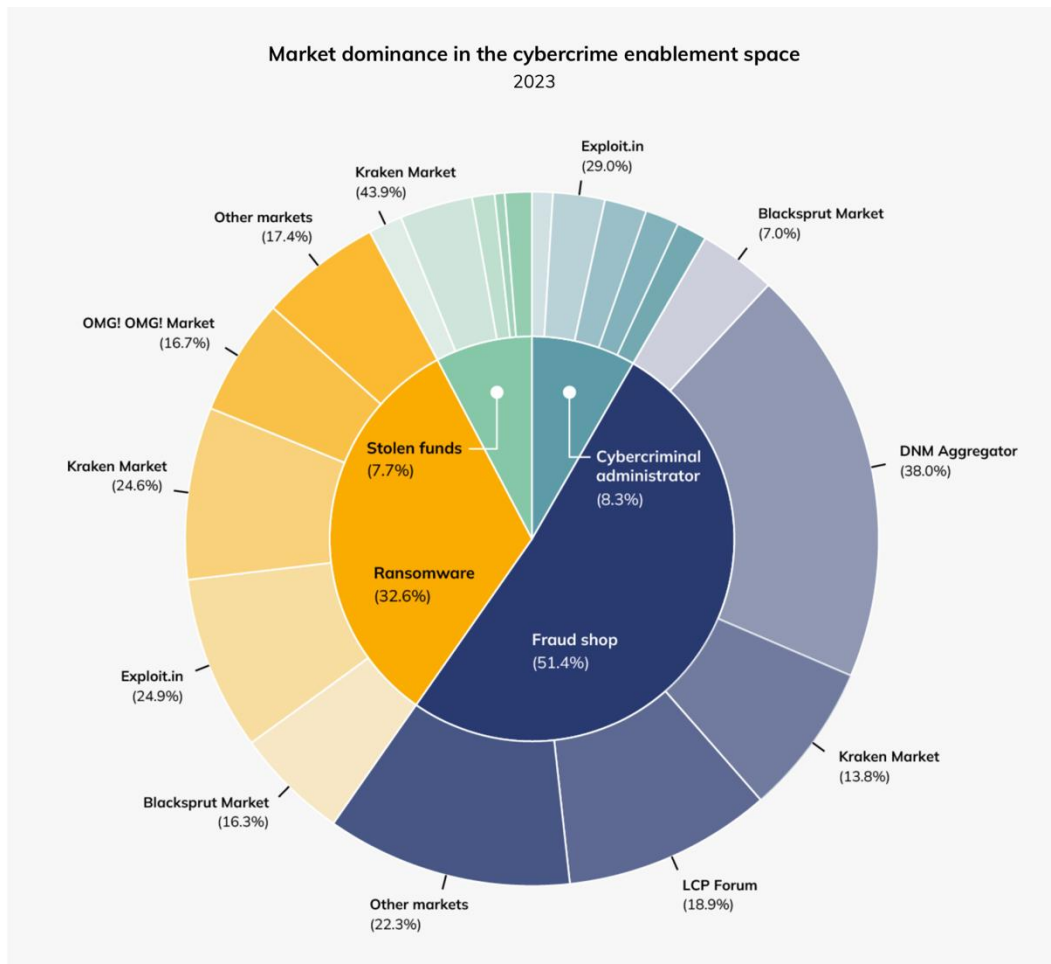
Yearly total value stolen in crypto hacks and number of hacks 2016 - 2023



Estimated value stolen by DPRK-linked hackers 2016 - 2023



Honey pot for the class' data analysts 😊



— Thank you

Szabolcs Szalay
February 2025