

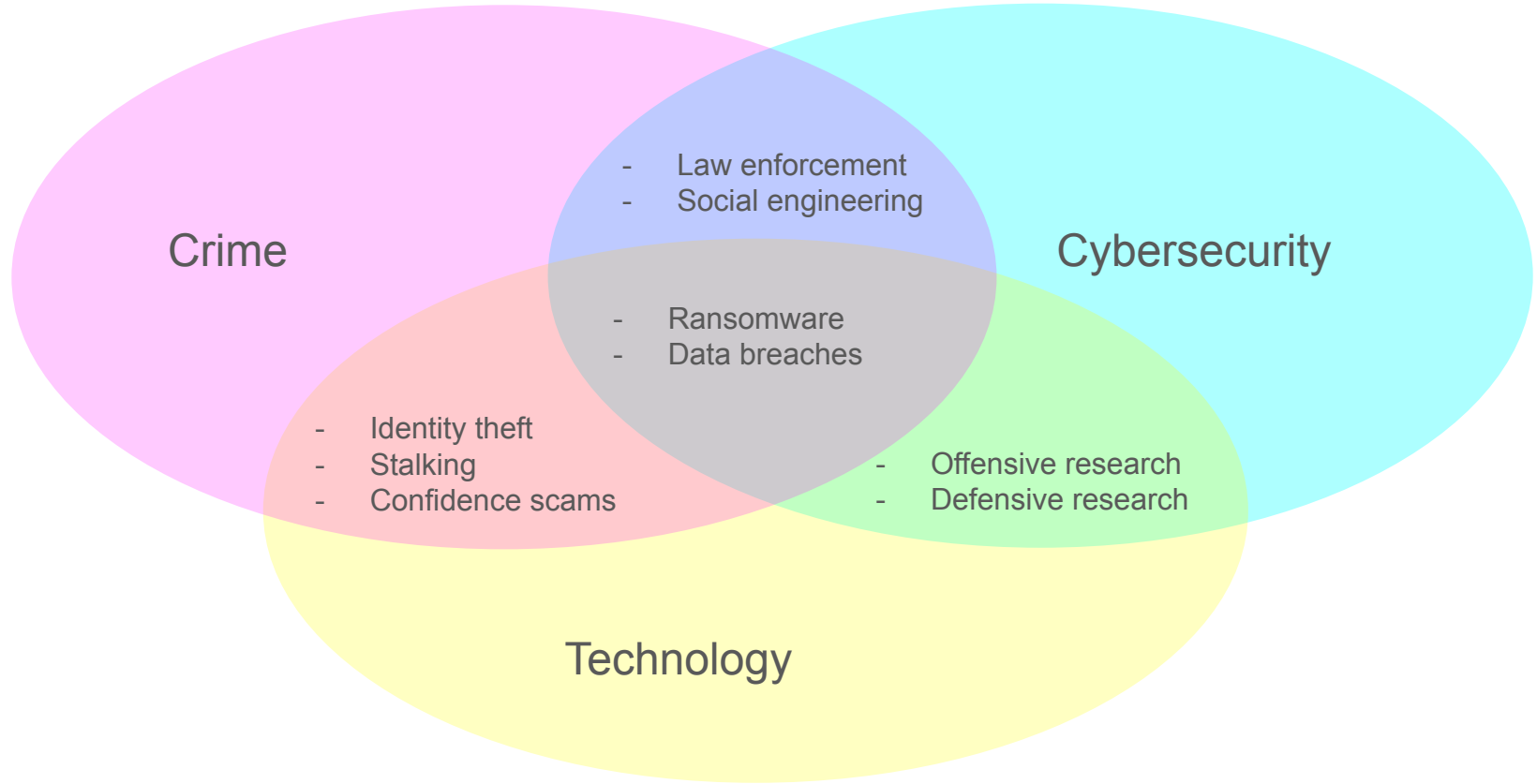
The Economics of cybercrime

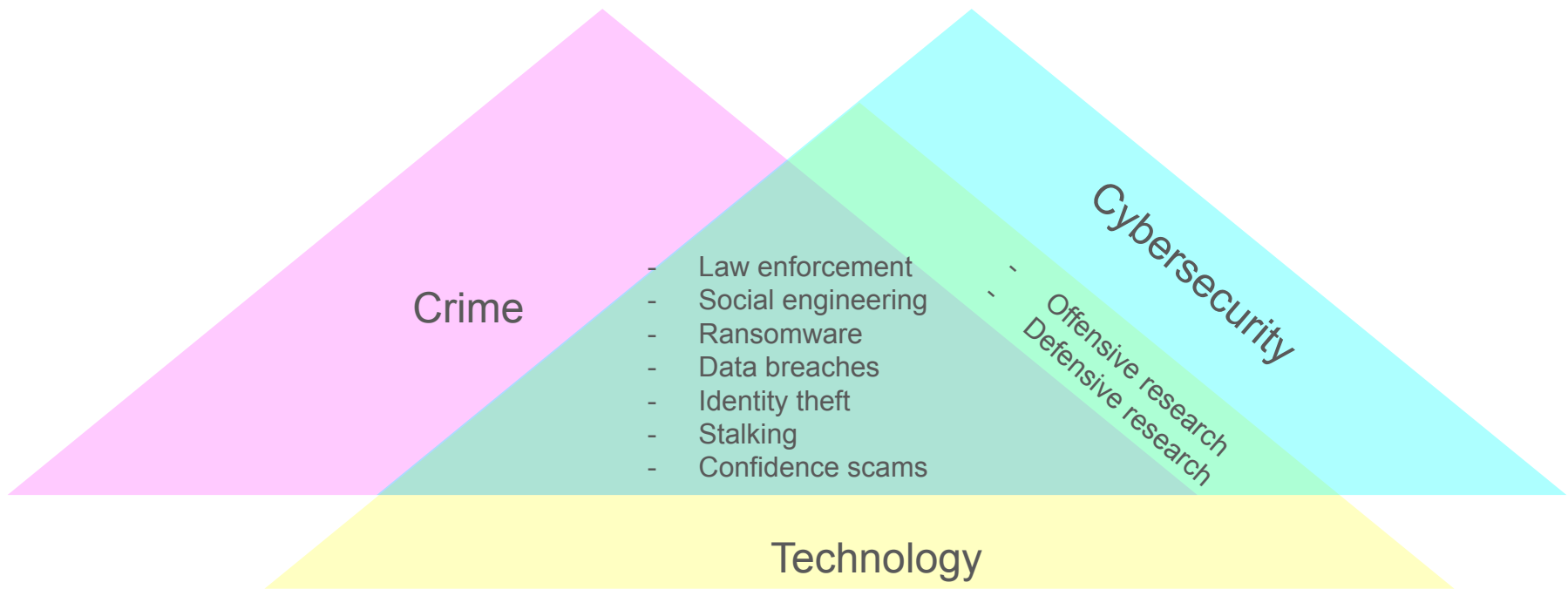


Agenda: Discuss three works on measuring cybercrime

1. Industry report
2. Government report
3. Academic paper

Goals: Face our intuitions and assumptions





SOPHOS

The State of Ransomware 2023

**Findings from an independent, vendor-agnostic survey
of 3,000 leaders responsible for IT/cybersecurity across
14 countries, conducted in January-March 2023.**



3,000
respondents



14
countries



100-5,000
employee organizations



Jan-Mar 2023
research conducted



<\$10M - \$5B+
annual revenue

1) What percentage of respondents were hit by ransomware?

- A. 0% to 25%
- B. 25% to 50%
- C. 50% to 75%
- D. 75% to 100%

1) What percentage of respondents were hit by ransomware?

- A. 0% to 25%
- B. 25% to 50%
- C. 50% to 75%
- D. 75% to 100%



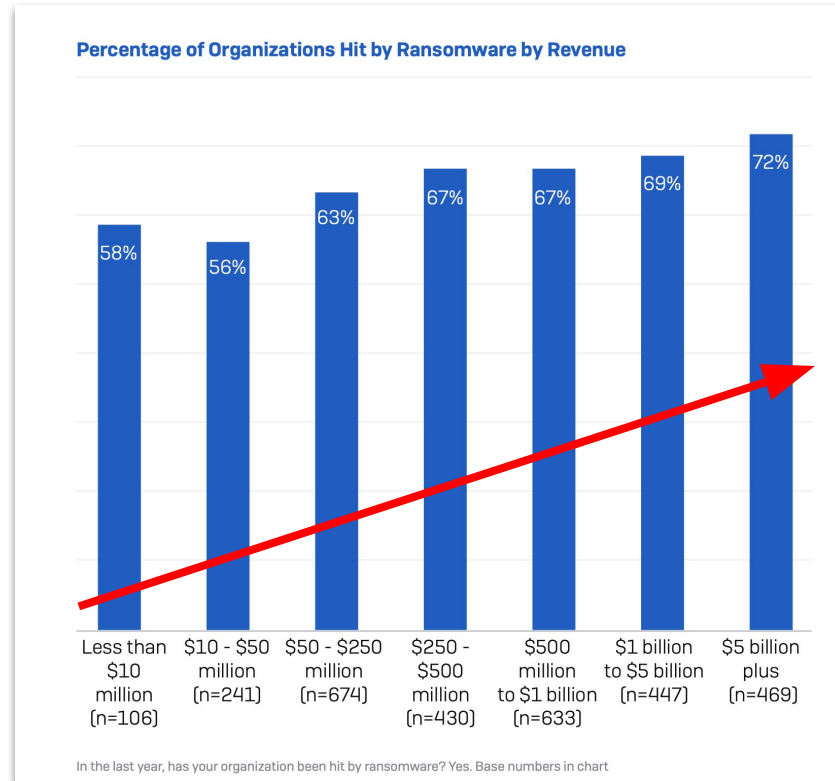
66%

2) Which group is more likely to be hit with ransomware?

- A. Small organizations
- B. Large organizations
- C. No difference

2) Which group is more likely to be hit with ransomware?

- A. Small organizations
- B. Large organizations**
- C. No difference



3) What percentage of ransomware attacks list “exploited vulnerability” as the root cause?

- A. 0% to 25%
- B. 25% to 50%
- C. 50% to 75%
- D. 75% to 100%

3) What percentage of ransomware attacks list “exploited vulnerability” as the root cause?

- A. 0% to 25%
- B. 25% to 50%
- C. 50% to 75%**
- D. 75% to 100%



What percentage of ransomware attacks list “exploited vulnerability” as the root cause?

- A. 0% to 25%
- B. 25% to 50%
- C. 50% to 75%**
- D. 75% to 100%

**40% due to
technological flaws**

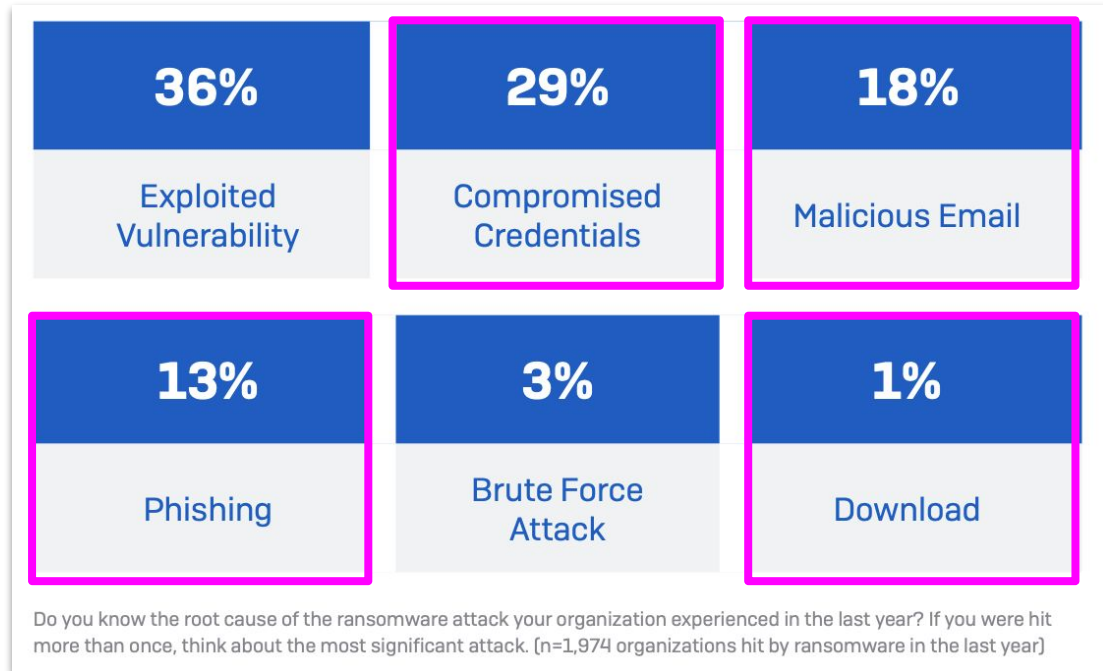


What percentage of ransomware attacks list “exploited vulnerability” as the root cause?

- A. 0% to 25%
- B. 25% to 50%
- C. 50% to 75%**
- D. 75% to 100%

40% due to technological flaws

60% due to social engineering!



4) What percentage of ransomware attacks are successful?

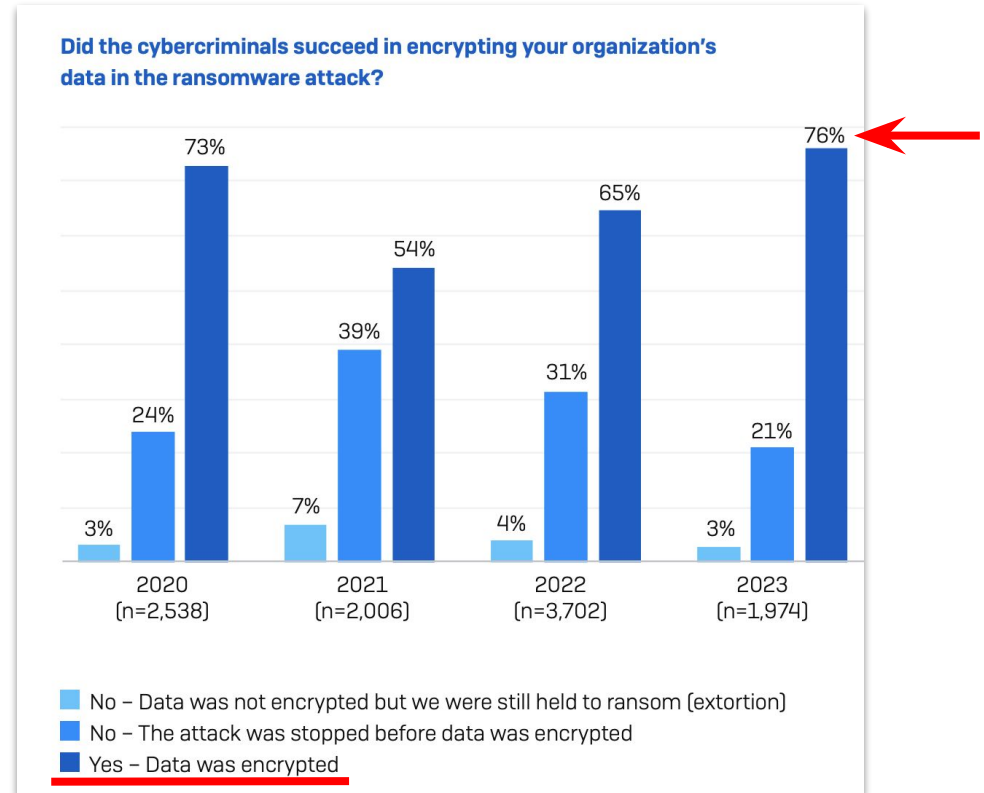
“Successful” = data is encrypted

- A. 0% to 25%
- B. 25% to 50%
- C. 50% to 75%
- D. 75% to 100%

4) What percentage of ransomware attacks are successful?

“Successful” = data is encrypted

- A. 0% to 25%
- B. 25% to 50%
- C. 50% to 75%
- D. 75% to 100%**



5) What percentage of victimized organizations paid ransom?

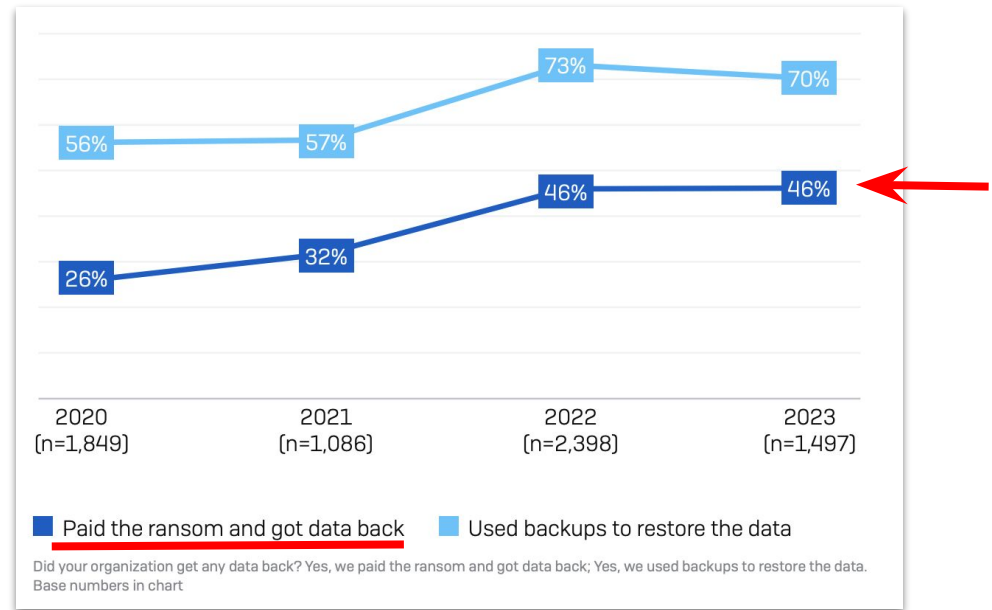
“Victimized” = had data encrypted
(97% of orgs recovered data)

- A. 0% to 25%
- B. 25% to 50%
- C. 50% to 75%
- D. 75% to 100%

5) What percentage of victimized organizations paid ransom?

“Victimized” = had data encrypted
(97% of orgs recovered data)

- A. 0% to 25%
- B. 25% to 50%**
- C. 50% to 75%
- D. 75% to 100%



5) What percentage of victimized organizations paid ransom?

“Victimized” = had data encrypted
(97% of orgs recovered data)

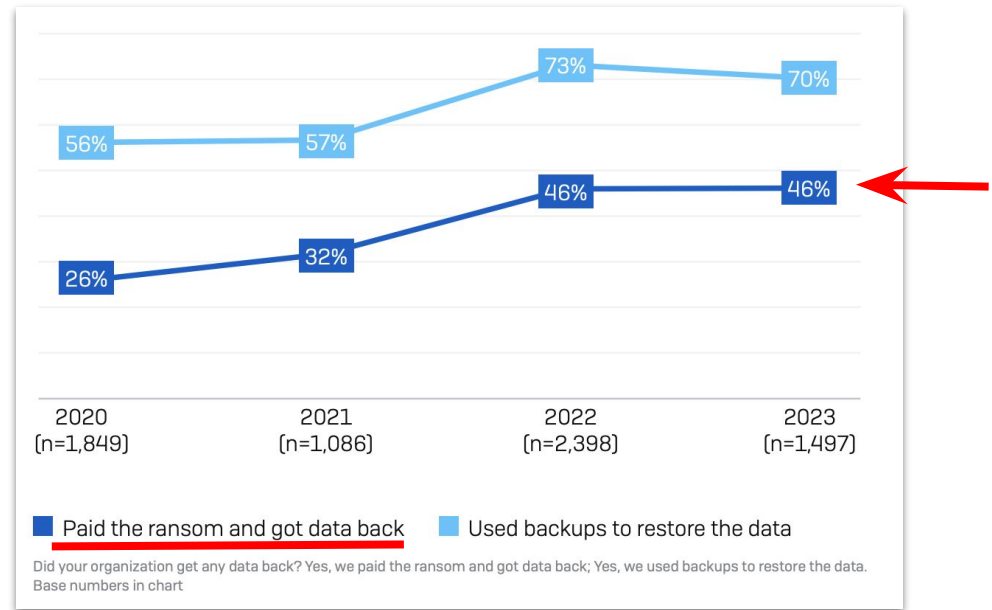
- A. 0% to 25%
- B. 25% to 50%**
- C. 50% to 75%
- D. 75% to 100%

% attacked = 0.66

% victimized = $0.76 * (\% \text{ attacked})$

% paid ransom = $0.46 * (\% \text{ victimized})$

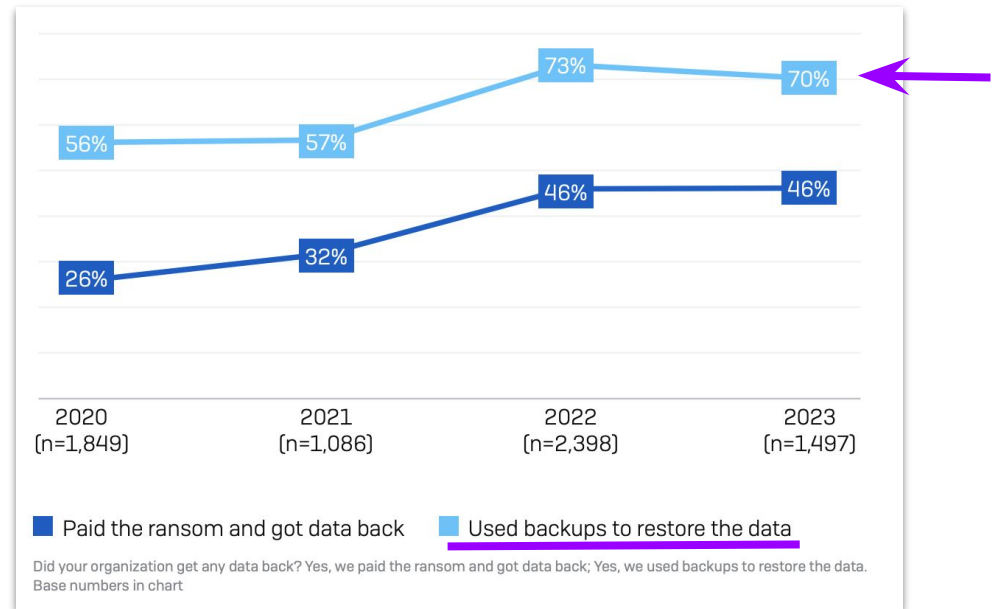
% paid ransom = 23% ???



5) What percentage of victimized organizations paid ransom?

“Victimized” = had data encrypted
(97% of orgs recovered data)

- A. 0% to 25%
- B. 25% to 50%**
- C. 50% to 75%
- D. 75% to 100%

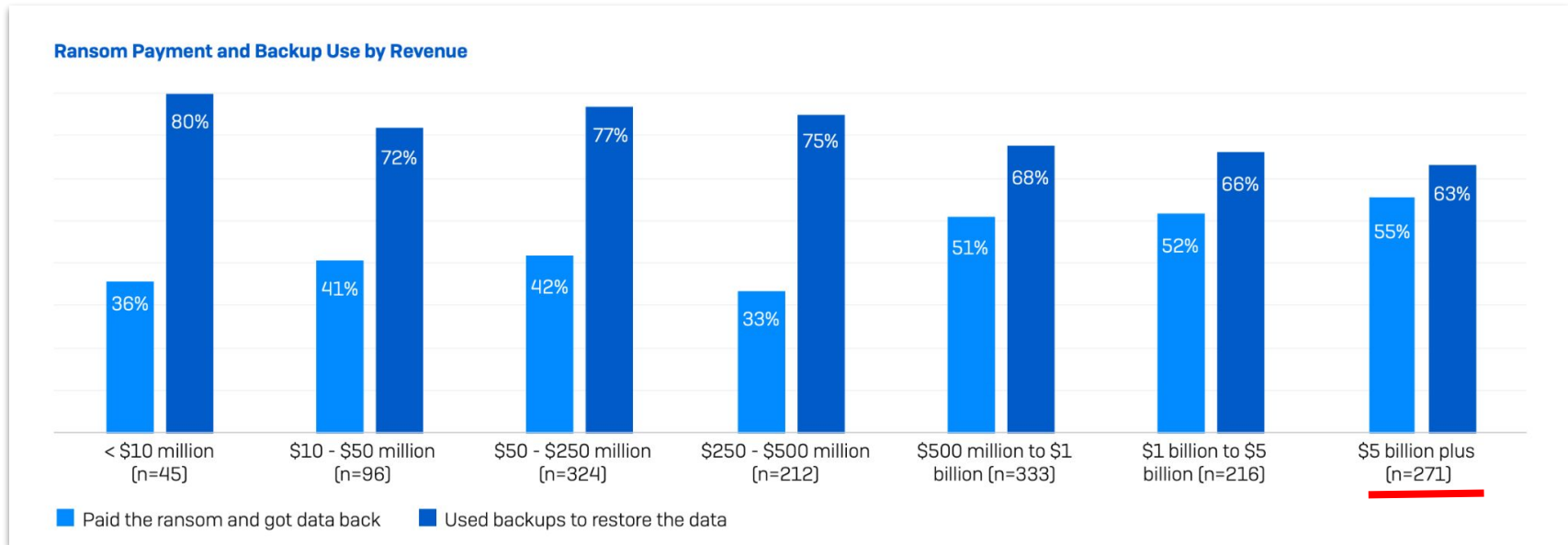


6) Which group is more likely to pay ransoms?

- A. Small organizations
- B. Large organizations
- C. No difference

6) Which group is more likely to pay ransoms?

- A. Small organizations
- B. Large organizations**
- C. No difference



7) Who is more likely to recover data?

- A. Organizations with cyber insurance
- B. Organizations without cyber insurance
- C. No difference

7) Who is more likely to recover data?

- A. Organizations with cyber insurance
- B. Organizations without cyber insurance
- C. No difference

Impact of insurance on propensity to pay ransom



Did your organization get any data back? Yes, we paid the ransom and got data back. n=1,497 organizations that were hit by ransomware in the last year and had data encrypted [771 standalone policy, 658 cyber as part of wider policy, 67 no cyber policy]

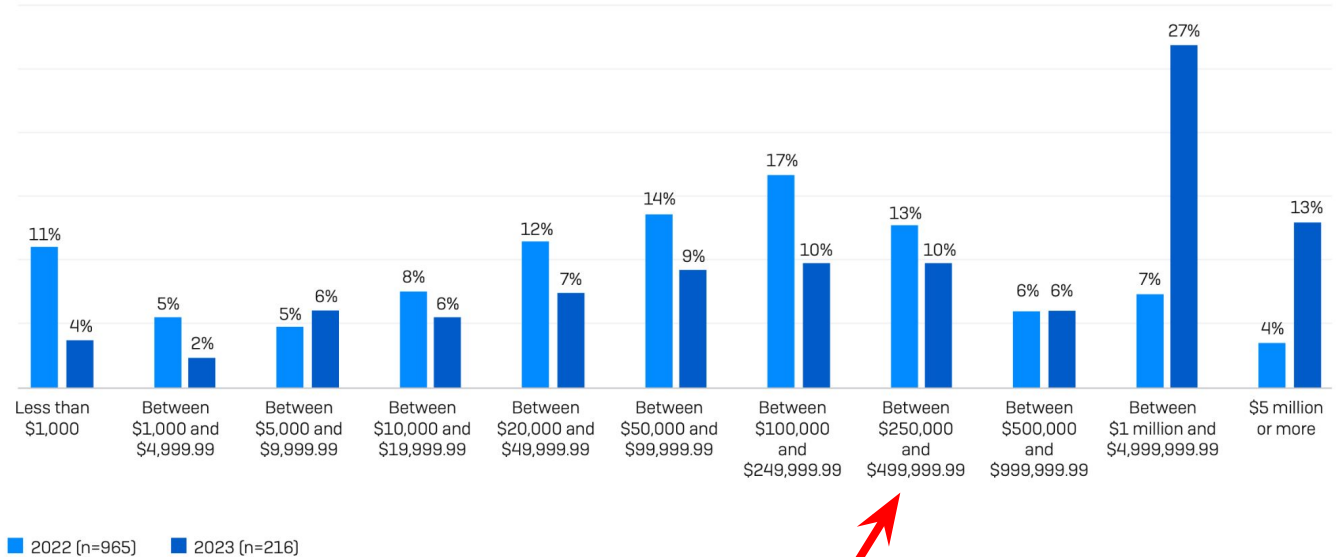
8) How much is the median ransom payment?

- A. \$400
- B. \$4,000
- C. \$40,000
- D. \$400,000
- E. \$4,000,000
- F. \$40,000,000

8) How much is the median ransom payment?

- A. \$400
- B. \$4,000
- C. \$40,000
- D. \$400,000**
- E. \$4,000,000
- F. \$40,000,000

Ransom Payments: 2023 vs 2022



■ 2022 (n=965) ■ 2023 (n=216)

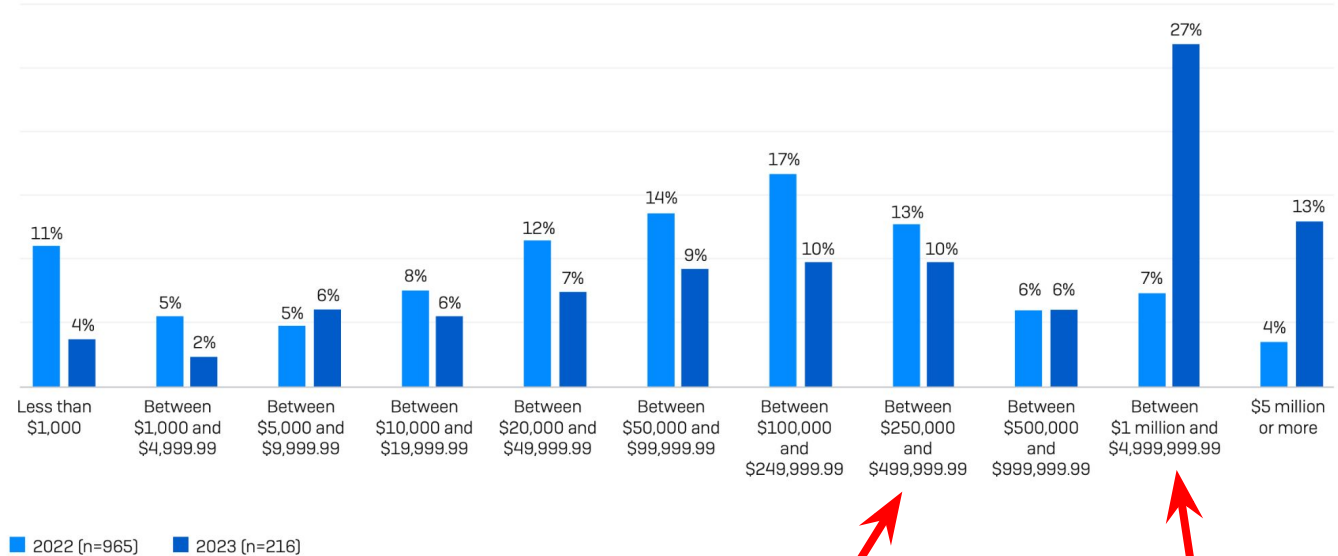
How much was the ransom payment that was paid to the attackers? Excluding "Don't know" responses.

Median = \$400K

8) How much is the median ransom payment?

- A. \$400
- B. \$4,000
- C. \$40,000
- D. \$400,000**
- E. \$4,000,000
- F. \$40,000,000

Ransom Payments: 2023 vs 2022



How much was the ransom payment that was paid to the attackers? Excluding "Don't know" responses.

Median = \$400K

Mean = \$1.5M

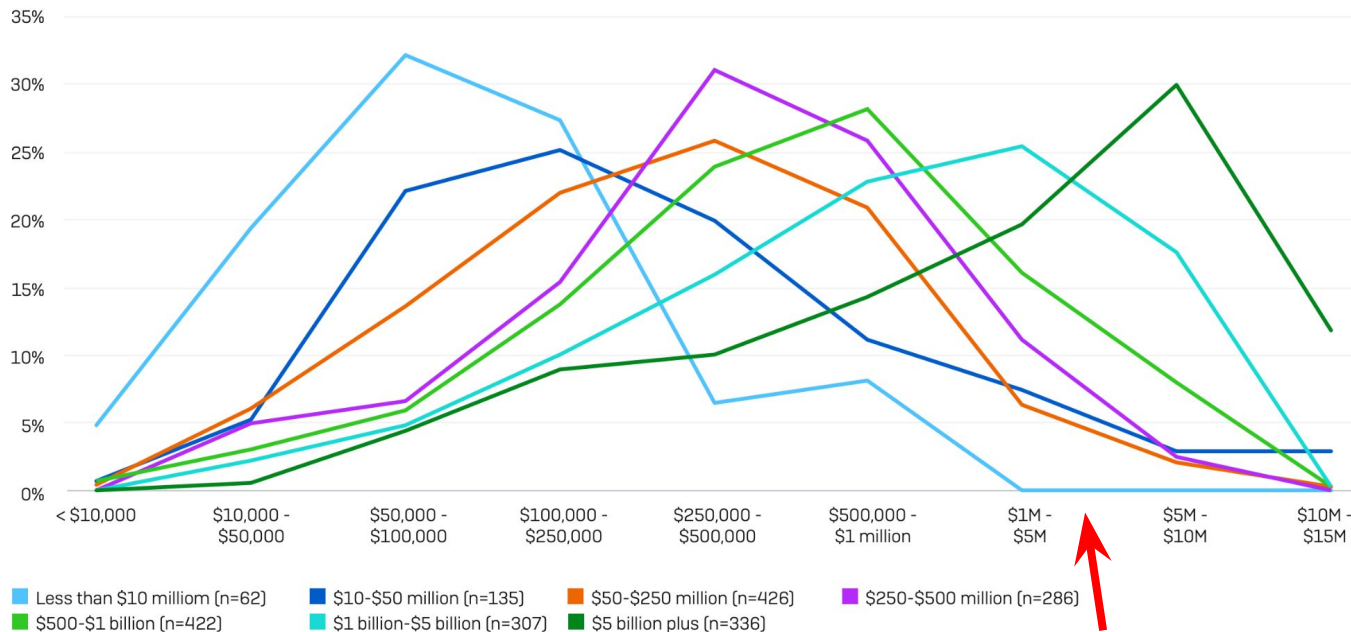
9) What is the mean recovery cost? (i.e. costs excluding the ransom)

- A. \$18
- B. \$180
- C. \$1,800
- D. \$18,000
- E. \$180,000
- F. \$1,800,000

9) What is the mean recovery cost? (i.e. costs excluding the ransom)

- A. \$18
- B. \$180
- C. \$1,800
- D. \$18,000
- E. \$180,000
- F. \$1,800,000

Recovery Cost by Revenue



What was the approximate cost to your organization to rectify the impacts of the most significant ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity etc)? Base numbers in chart

Mean = \$1.82M

10) What is the implied total cost of ransomware?

- A. \$2K
- B. \$2M
- C. \$2B
- D. \$2T

10) What is the implied total cost of ransomware?

A. \$2K

B. \$2M

C. \$2B

D. \$2T

median ransom = \$400K

median recovery cost = \$400K * (1.8M avg)

Cost per incident = \$400K + \$400K = \$800K

Victimization rate = 22%

of respondents = 13,000

victims = 22% of 13,000 = 2860

Total costs: = 2860 * \$800K = \$2.29B



FEDERAL BUREAU of INVESTIGATION
Internet Crime Report
2022



INTERNET CRIME COMPLAINT CENTER

2022 CRIME TYPES

[illegible]

2022 CRIME TYPES

By Victim Count

[illegible]

Phishing	300,497
----------	---------

2022 CRIME TYPES

By Victim Count

[illegible]

2022 CRIME TYPES

By Victim Count

[illegible]

2022 CRIME TYPES

By Victim Count

<i>Crime Type</i>	<i>Victims</i>
Phishing	300,497
Personal Data Breach	58,859
Non-Payment/Non-Delivery	51,679
Extortion	39,416

?

?

?

?

?

?

?

?

?

?

2022 CRIME TYPES

By Victim Count

Crime Type	Victims
Phishing	300,497
Personal Data Breach	58,859
Non-Payment/Non-Delivery	51,679
Extortion	39,416
Tech Support	32,538

?

?

?

?

?

?

?

?

?

2022 CRIME TYPES

By Victim Count

<i>Crime Type</i>	<i>Victims</i>
Phishing	300,497
Personal Data Breach	58,859
Non-Payment/Non-Delivery	51,679
Extortion	39,416
Tech Support	32,538
Investment	30,529
Identity Theft	27,922
Credit Card/Check Fraud	22,985
BEC	21,832
Spoofing	20,649
Confidence/Romance	19,021
Employment	14,946
Harassment/Stalking	11,779
Real Estate	11,727

2022 CRIME TYPES continued

By Victim Loss

<i>Crime Type</i>	<i>Loss</i>
-------------------	-------------

?

?

?

?

?

?

?

?

?

?

?

?

?

?

2022 CRIME TYPES continued

By Victim Loss

<i>Crime Type</i>	<i>Loss</i>
Investment	\$3,311,742,206

?

?

?

?

?

?

?

?

?

?

?

?

?

2022 CRIME TYPES continued

By Victim Loss

[illegible]

2022 CRIME TYPES continued

By Victim Loss

<i>Crime Type</i>	<i>Loss</i>
Investment	\$3,311,742,206
BEC	\$2,742,354,049
Tech Support	\$806,551,993

?

?

?

?

?

?

?

?

?

?

?

2022 CRIME TYPES continued

By Victim Loss

Crime Type	Loss
------------	------

Investment	\$3,311,742,206
------------	-----------------

BEC	\$2,742,354,049
-----	-----------------

Tech Support	\$806,551,993
--------------	---------------

Personal Data Breach	\$742,438,136
----------------------	---------------

?

?

?

?

?

?

?

?

?

?

2022 CRIME TYPES continued

By Victim Loss

<i>Crime Type</i>	<i>Loss</i>
Investment	\$3,311,742,206
BEC	\$2,742,354,049
Tech Support	\$806,551,993
Personal Data Breach	\$742,438,136
Confidence/Romance	\$735,882,192

?

?

?

?

?

?

?

?

?

2022 CRIME TYPES continued

By Victim Loss

<i>Crime Type</i>	<i>Loss</i>
Investment	\$3,311,742,206
BEC	\$2,742,354,049
Tech Support	\$806,551,993
Personal Data Breach	\$742,438,136
Confidence/Romance	\$735,882,192
Data Breach	\$459,321,859
Real Estate	\$396,932,821
Non-Payment/Non-Delivery	\$281,770,073
Credit Card/Check Fraud	\$264,148,905
Government Impersonation	\$240,553,091
Identity Theft	\$189,205,793
Other	\$117,686,789
Spoofing	\$107,926,252
Advanced Fee	\$104,325,444

OVERALL STATE STATISTICS

Count by Subject per State*

<i>Rank</i>	<i>State</i>	<i>Subjects</i>
1	California	43,970
2	Texas	14,449
3	New York	12,633
4	Connecticut	12,460
5	Florida	12,080
6	Ohio	5,694
7	Virginia	5,178
8	Maryland	4,941
9	Illinois	4,719
10	North Carolina	4,670

???

Measuring the Changing Cost of Cybercrime

Ross Anderson¹ Chris Barton² Rainer Böhme³ Richard Clayton⁴
Carlos Gañán⁵ Tom Grasso⁶ Michael Levi⁷ Tyler Moore⁸ Marie Vasek⁹

Abstract

In 2012 we presented the first systematic study of the costs of cybercrime. In this paper, we report what has changed in the seven years since. The period has seen major platform evolution, with the mobile phone replacing the PC and laptop as the consumer terminal of choice, with Android replacing Windows, and with many services moving to the cloud. The use of social networks has become extremely widespread. The executive summary is that about half of all property crime, by volume and by value, is now online. We hypothesised in 2012 that this might be so; it is now established by multiple victimisation studies. Many cybercrime patterns appear to be fairly stable, but there are some interesting changes. Payment fraud, for example, has more than doubled in value but has fallen slightly as a proportion of payment value; the payment system has simply become bigger, and slightly more efficient. Several new cybercrimes are significant enough to mention, including business email compromise and crimes involving cryptocurrencies. The move to the cloud means that system misconfiguration may now be responsible for as many breaches as phishing. Some companies have suffered large losses as a side-effect of denial-of-service worms released by state actors, such as NotPetya; we have to take a view on whether they count as cybercrime. The infrastructure supporting cybercrime, such as botnets, continues to evolve, and specific crimes such as premium-rate phone scams have evolved some interesting variants. The overall picture is the same as in 2012: traditional offences that are now technically 'computer crimes' such as tax and welfare fraud cost the typical citizen in the low hundreds of Euros/dollars a year; payment frauds and similar offences, where the *modus operandi* has been completely changed by computers, cost in the tens; while the new computer crimes cost in the tens of cents. Defending against the platforms used to support the latter two types of crime cost citizens in the tens of dollars. Our conclusions remain broadly the same as in 2012: it would be economically rational to spend less in anticipation of cybercrime (on antiviruses, firewalls, etc.) and more on response. We are particularly bad at prosecuting criminals who operate infrastructure that other wrongdoers exploit. Given the growing realisation among policymakers that crime hasn't been falling over the past decade, merely moving online, we might reasonably hope for better funded and coordinated law-enforcement action.

¹Computer Laboratory, University of Cambridge, Cambridge, UK. ross.anderson@cl.cam.ac.uk

²chris@nworks.net

³Department of Computer Science, Universität Innsbruck, Innsbruck, Austria. rainer.boehme@uibk.ac.at

⁴Computer Laboratory, University of Cambridge, Cambridge, UK. richard.clayton@cl.cam.ac.uk

⁵Faculty of Technology, Policy and Management, Delft University of Technology, Delft, Netherlands.

⁶C.HernandezGanan@tudelft.nl

⁷QinetiQ, Pittsburgh, PA, USA. con@qinetel.com

⁸School of Social Sciences, Cardiff University, Cardiff, UK. levi@cf.ac.uk

⁹Tandy School of Computer Science, The University of Tulsa, Tulsa OK, USA. tyler-moore@utulsa.edu

⁹Department of Computer Science, University of New Mexico, Albuquerque NM, USA. vasek@cs.unm.edu

Three types of costs

Direct losses

Three types of costs

Direct losses

Indirect losses

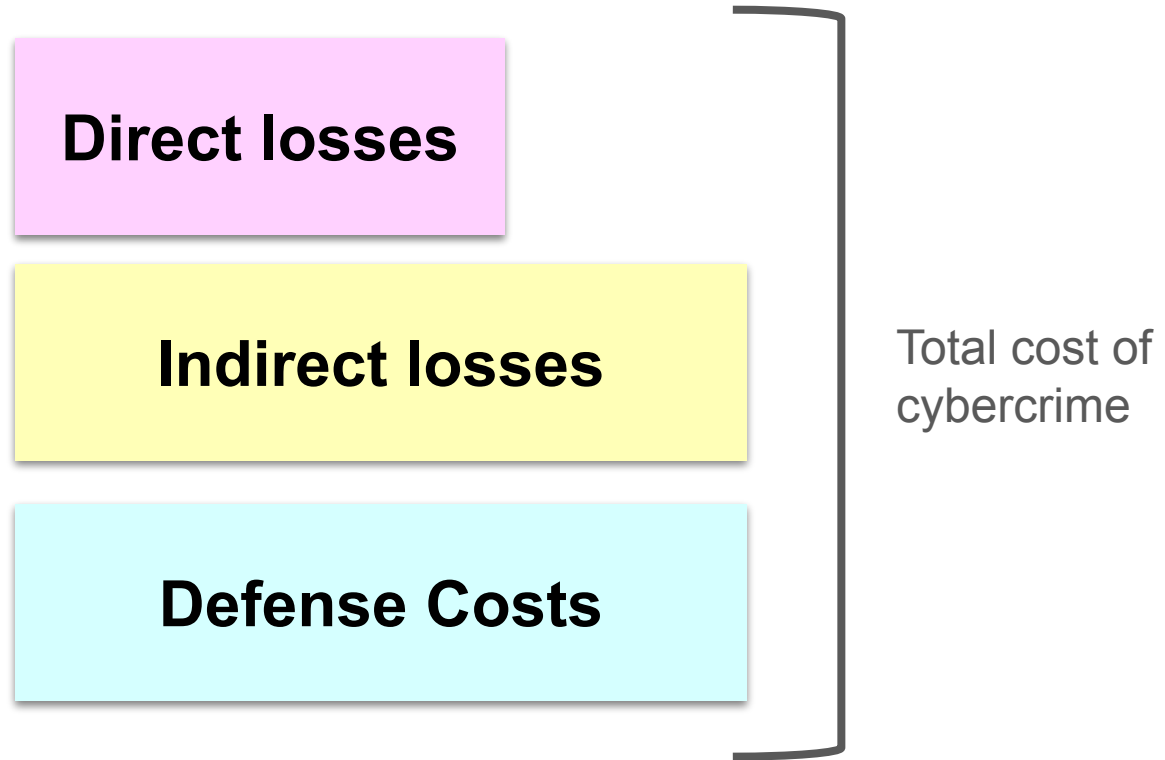
Three types of costs

Direct losses

Indirect losses

Defense Costs

Three types of costs



crime type	value
§3.1 Online credit card fraud	£731.8m (UK)
§3.2 Online bank fraud	£121.4m (UK)
§3.2 Authorised push payments	£236m (UK)
§3.3 In-person card fraud	£158m
§3.4 Ransomware	well over \$10m
§3.4 Cryptocrime	\$2bn
§3.5 Ad fraud	low \$billions
§3.5 Pharmaceuticals	tens of \$millions
§3.5 Coupon fraud	\$300m+ (US)
§3.5 Loyalty-program fraud	\$235m
§3.5 Travel fraud	\$1bn
§3.5 Counterfeit software	low \$millions
§3.5 Copyright theft	low \$10 millions
§3.6 Fake antivirus	\$7.1m (US)
§3.6 Tech support scams	\$39m (US)
§3.7 Compromised email	
§3.8 Fake companies	tens of \$millions
§3.9 Advance fee fraud	low \$100 millions
§3.10 Business email compromise	\$1.3bn (US)
§3.11 Telecoms fraud	\$7 billion
§3.12 Wannacry / NotPetya	\$1–2 billion
§3.13 Fiscal fraud	many \$billions
§3.14 Romance scams	\$143m (US)

crime type (2017)	value
§3.1 Online credit card fraud	£731.8m (UK)
§3.2 Online bank fraud	£121.4m (UK)
§3.2 Authorised push payments	£236m (UK)
§3.3 In-person card fraud	£158m
§3.4 Ransomware	well over \$10m
§3.4 Cryptocrime	\$2bn
§3.5 Ad fraud	low \$billions
§3.5 Pharmaceuticals	tens of \$millions
§3.5 Coupon fraud	\$300m+ (US)
§3.5 Loyalty-program fraud	\$235m
§3.5 Travel fraud	\$1bn
§3.5 Counterfeit software	low \$millions
§3.5 Copyright theft	low \$10 millions
§3.6 Fake antivirus	\$7.1m (US)
§3.6 Tech support scams	\$39m (US)
§3.7 Compromised email	
§3.8 Fake companies	tens of \$millions
§3.9 Advance fee fraud	low \$100 millions
§3.10 Business email compromise	\$1.3bn (US)
§3.11 Telecoms fraud	\$7 billion
§3.12 Wannacry / NotPetya	\$1–2 billion
§3.13 Fiscal fraud	many \$billions
§3.14 Romance scams	\$143m (US)

crime type (2017)	value
§3.1 Online credit card fraud	£731.8m (UK)
§3.2 Online bank fraud	£121.4m (UK)
§3.2 Authorised push payments	£236m (UK)
§3.3 In-person card fraud	£158m
§3.4 Ransomware	well over \$10m
§3.4 Cryptocrime	\$2bn
§3.5 Ad fraud	low \$billions
§3.5 Pharmaceuticals	tens of \$millions
§3.5 Coupon fraud	\$300m+ (US)
§3.5 Loyalty-program fraud	\$235m
§3.5 Travel fraud	\$1bn
§3.5 Counterfeit software	low \$millions
§3.5 Copyright theft	low \$10 millions
§3.6 Fake antivirus	\$7.1m (US)
§3.6 Tech support scams	\$39m (US)
§3.7 Compromised email	
§3.8 Fake companies	tens of \$millions
§3.9 Advance fee fraud	low \$100 millions
§3.10 Business email compromise	\$1.3bn (US)
§3.11 Telecoms fraud	\$7 billion
§3.12 Wannacry / NotPetya	\$1–2 billion
§3.13 Fiscal fraud	many \$billions
§3.14 Romance scams	\$143m (US)

2022 CRIME TYPES continued

By Victim Loss

Crime Type	Loss
Investment	\$3,311,742,206
BEC	\$2,742,354,049
Tech Support	\$806,551,993
Personal Data Breach	\$742,438,136
Confidence/Romance	\$735,882,192
Data Breach	\$459,321,859
Real Estate	\$396,932,821
Non-Payment/Non-Delivery	\$281,770,073
Credit Card/Check Fraud	\$264,148,905
Government Impersonation	\$240,553,091
Identity Theft	\$189,205,793
Other	\$117,686,789
Spoofing	\$107,926,252
Advanced Fee	\$104,325,444

crime type (2017)	value
§3.1 Online credit card fraud	£731.8m (UK)
§3.2 Online bank fraud	£121.4m (UK)
§3.2 Authorised push payments	£236m (UK)
§3.3 In-person card fraud	£158m
§3.4 Ransomware	well over \$10m
§3.4 Cryptocrime	\$2bn
§3.5 Ad fraud	low \$billions
§3.5 Pharmaceuticals	tens of \$millions
§3.5 Coupon fraud	\$300m+ (US)
§3.5 Loyalty-program fraud	\$235m
§3.5 Travel fraud	\$1bn
§3.5 Counterfeit software	low \$millions
§3.5 Copyright theft	low \$10 millions
§3.6 Fake antivirus	\$7.1m (US)
§3.6 Tech support scams	\$39m (US)
§3.7 Compromised email	
§3.8 Fake companies	tens of \$millions
§3.9 Advance fee fraud	low \$100 millions
§3.10 Business email compromise	\$1.3bn (US)
§3.11 Telecoms fraud	\$7 billion
§3.12 Wannacry / NotPetya	\$1–2 billion
§3.13 Fiscal fraud	many \$billions
§3.14 Romance scams	\$143m (US)

2022 CRIME TYPES continued

By Victim Loss

Crime Type	Loss
Investment	\$3,311,742,206
BEC	\$2,742,354,049
Tech Support	\$806,551,993
Personal Data Breach	\$742,438,136
Confidence/Romance	\$735,882,192
Data Breach	\$459,321,859
Real Estate	\$396,932,821
Non-Payment/Non-Delivery	\$281,770,073
Credit Card/Check Fraud	\$264,148,905
Government Impersonation	\$240,553,091
Identity Theft	\$189,205,793
Other	\$117,686,789
Spoofing	\$107,926,252
Advanced Fee	\$104,325,444

crime type (2017)	value
§3.1 Online credit card fraud	£731.8m (UK)
§3.2 Online bank fraud	£121.4m (UK)
§3.2 Authorised push payments	£236m (UK)
§3.3 In-person card fraud	£158m
§3.4 Ransomware	well over \$10m
§3.4 Cryptocrime	\$2bn
§3.5 Ad fraud	low \$billions
§3.5 Pharmaceuticals	tens of \$millions
§3.5 Coupon fraud	\$300m+ (US)
§3.5 Loyalty-program fraud	\$235m
§3.5 Travel fraud	\$1bn
§3.5 Counterfeit software	low \$millions
§3.5 Copyright theft	low \$10 millions
§3.6 Fake antivirus	\$7.1m (US)
§3.6 Tech support scams	\$39m (US)
§3.7 Compromised email	
§3.8 Fake companies	tens of \$millions
§3.9 Advance fee fraud	low \$100 millions
§3.10 Business email compromise	\$1.3bn (US)
§3.11 Telecoms fraud	\$7 billion
§3.12 Wannacry / NotPetya	\$1–2 billion
§3.13 Fiscal fraud	many \$billions
§3.14 Romance scams	\$143m (US)

2022 CRIME TYPES continued

By Victim Loss

Crime Type	Loss
Investment	\$3,311,742,206
BEC	\$2,742,354,049
Tech Support	\$806,551,993
Personal Data Breach	\$742,438,136
Confidence/Romance	\$735,882,192
Data Breach	\$459,321,859
Real Estate	\$396,932,821
Non-Payment/Non-Delivery	\$281,770,073
Credit Card/Check Fraud	\$264,148,905
Government Impersonation	\$240,553,091
Identity Theft	\$189,205,793
Other	\$117,686,789
Spoofing	\$107,926,252
Advanced Fee	\$104,325,444



crime type (2017)**value**

§3.1 Online credit card fraud	£731.8m (UK)
§3.2 Online bank fraud	£121.4m (UK)
§3.2 Authorised push payments	£236m (UK)
§3.3 In-person card fraud	£158m
§3.4 Ransomware	well over \$10m
§3.4 Cryptocrime	\$2bn
§3.5 Ad fraud	low \$billions
§3.5 Pharmaceuticals	tens of \$millions
§3.5 Coupon fraud	\$300m+ (US)
§3.5 Loyalty-program fraud	\$235m
§3.5 Travel fraud	\$1bn
§3.5 Counterfeit software	low \$millions
§3.5 Copyright theft	low \$10 millions
§3.6 Fake antivirus	\$7.1m (US)
§3.6 Tech support scams	\$39m (US)
§3.7 Compromised email	
§3.8 Fake companies	tens of \$millions
§3.9 Advance fee fraud	low \$100 millions
§3.10 Business email compromise	\$1.3bn (US)
§3.11 Telecoms fraud	\$7 billion
§3.12 Wannacry / NotPetya	\$1–2 billion
§3.13 Fiscal fraud	many \$billions
§3.14 Romance scams	\$143m (US)

2022 CRIME TYPES continued**By Victim Loss***Crime Type**Loss*

Investment	\$3,311,742,206
BEC	\$2,742,354,049
Tech Support	\$806,551,993
Personal Data Breach	\$742,438,136
Confidence/Romance	\$735,882,192
Data Breach	\$459,321,859
Real Estate	\$396,932,821
Non-Payment/Non-Delivery	\$281,770,073
Credit Card/Check Fraud	\$264,148,905
Government Impersonation	\$240,553,091
Identity Theft	\$189,205,793
Other	\$117,686,789
Spoofing	\$107,926,252
Advanced Fee	\$104,325,444

crime type (2017)	value
§3.1 Online credit card fraud	£731.8m (UK)
§3.2 Online bank fraud	£121.4m (UK)
§3.2 Authorised push payments	£236m (UK)
§3.3 In-person card fraud	£158m
§3.4 Ransomware	well over \$10m
§3.4 Cryptocrime	\$2bn
§3.5 Ad fraud	low \$billions
§3.5 Pharmaceuticals	tens of \$millions
§3.5 Coupon fraud	\$300m+ (US)
§3.5 Loyalty-program fraud	\$235m
§3.5 Travel fraud	\$1bn
§3.5 Counterfeit software	low \$millions
§3.5 Copyright theft	low \$10 millions
§3.6 Fake antivirus	\$7.1m (US)
§3.6 Tech support scams	\$39m (US)
§3.7 Compromised email	
§3.8 Fake companies	tens of \$millions
§3.9 Advance fee fraud	low \$100 millions
§3.10 Business email compromise	\$1.3bn (US)
§3.11 Telecoms fraud	\$7 billion
§3.12 Wannacry / NotPetya	\$1–2 billion
§3.13 Fiscal fraud	many \$billions
§3.14 Romance scams	\$143m (US)



2022 CRIME TYPES continued

By Victim Loss

Crime Type	Loss
Investment	\$3,311,742,206
BEC	\$2,742,354,049
Tech Support	\$806,551,993
Personal Data Breach	\$742,438,136
Confidence/Romance	\$735,882,192
Data Breach	\$459,321,859
Real Estate	\$396,932,821
Non-Payment/Non-Delivery	\$281,770,073
Credit Card/Check Fraud	\$264,148,905
Government Impersonation	\$240,553,091
Identity Theft	\$189,205,793
Other	\$117,686,789
Spoofing	\$107,926,252
Advanced Fee	\$104,325,444

crime type (2017)	value
§3.1 Online credit card fraud	£731.8m (UK)
§3.2 Online bank fraud	£121.4m (UK)
§3.2 Authorised push payments	£236m (UK)
§3.3 In-person card fraud	£158m
§3.4 Ransomware	well over \$10m
§3.4 Cryptocrime	\$2bn
§3.5 Ad fraud	low \$billions
§3.5 Pharmaceuticals	tens of \$millions
§3.5 Coupon fraud	\$300m+ (US)
§3.5 Loyalty-program fraud	\$235m
§3.5 Travel fraud	\$1bn
§3.5 Counterfeit software	low \$millions
§3.5 Copyright theft	low \$10 millions
§3.6 Fake antivirus	\$7.1m (US)
§3.6 Tech support scams	\$39m (US)
§3.7 Compromised email	
§3.8 Fake companies	tens of \$millions
§3.9 Advance fee fraud	low \$100 millions
§3.10 Business email compromise	\$1.3bn (US)
§3.11 Telecoms fraud	\$7 billion
§3.12 Wannacry / NotPetya	\$1–2 billion
§3.13 Fiscal fraud	many \$billions
§3.14 Romance scams	\$143m (US)

2022 CRIME TYPES continued

By Victim Loss

Crime Type	Loss
Investment	\$3,311,742,206
BEC	\$2,742,354,049
Tech Support	\$806,551,993
Personal Data Breach	\$742,438,136
Confidence/Romance	\$735,882,192
Data Breach	\$459,321,859
Real Estate	\$396,932,821
Non-Payment/Non-Delivery	\$281,770,073
Credit Card/Check Fraud	\$264,148,905
Government Impersonation	\$240,553,091
Identity Theft	\$189,205,793
Other	\$117,686,789
Spoofing	\$107,926,252
Advanced Fee	\$104,325,444

?

crime type (2017)	value
§3.1 Online credit card fraud	£731.8m (UK)
§3.2 Online bank fraud	£121.4m (UK)
§3.2 Authorised push payments	£236m (UK)
§3.3 In-person card fraud	£158m
§3.4 Ransomware	well over \$10m
§3.4 Cryptocrime	\$2bn
§3.5 Ad fraud	low \$billions
§3.5 Pharmaceuticals	tens of \$millions
§3.5 Coupon fraud	\$300m+ (US)
§3.5 Loyalty-program fraud	\$235m
§3.5 Travel fraud	\$1bn
§3.5 Counterfeit software	low \$millions
§3.5 Copyright theft	low \$10 millions
§3.6 Fake antivirus	\$7.1m (US)
§3.6 Tech support scams	\$39m (US)
§3.7 Compromised email	
§3.8 Fake companies	tens of \$millions
§3.9 Advance fee fraud	low \$100 millions
§3.10 Business email compromise	\$1.3bn (US)
§3.11 Telecoms fraud	\$7 billion
§3.12 Wannacry / NotPetya	\$1–2 billion
§3.13 Fiscal fraud	many \$billion
§3.14 Romance scams	\$143m (US)

2022 CRIME TYPES continued

By Victim Loss

Crime Type	Loss
Investment	\$3,311,742,206
BEC	\$2,742,354,049
Tech Support	\$806,551,993
Personal Data Breach	\$742,438,136
Confidence/Romance	\$735,882,192
Data Breach	\$459,321,859
Real Estate	\$396,932,821
Non-Payment/Non-Delivery	\$281,770,073
Credit Card/Check Fraud	\$264,148,905
Government Impersonation	\$240,553,091
Identity Theft	\$189,205,793
Other	\$117,686,789
Spoofing	\$107,926,252
Advanced Fee	\$104,325,444

Discussion

- Many of the costliest crimes (e.g. BEC and tech support scams) do not seem to be a priority for the security community. Why?