# From Harm to Healing: Understanding Individual Resilience after Cybercrimes

**Xiaowei Chen**, Mindy Tran, Yue Deng,

Bhupendra Acharya, Yixin Zou

MAX PLANCK INSTITUTE
FOR SECURITY AND PRIVACY

香港科技大學
THE HONG KONG
UNIVERSITY OF SCIENCE
AND TECHNOLOGY

UNIVERSITY of
LOUISIANA
LAFAYETTE

# Cybercrime Surge: Complaints and Losses


Fig 1: Complaints and loss trends since 2020 (FBI, IC3 Report).

## Background: Impact of Cybercrimes

Cybercrimes impact: financial loss, compromised personal data, disrupted routine, and psychological distress [1]

Victim support resources: close ones, online forums, law enforcement, and victim support organizations[2];

[1] Luke Balcombe. 2025. The Mental Health Impacts of Internet Scams. *Int. J. Environ. Res. Public Health*.
[2] Nott et al. 2021. Double, triple or quadruple hits? Exploring the impact of cybercrime on victims in the Netherlands. *Int. Rev. Vic.*

## *What is individual cyber resilience?*

Individuals who have had prior data loss experiences were more inclined to implement data backup practices [1].

Joinson et al. [2] developed "human cyber resilience" scale: *self-efficacy, social support, learning and growth*, and *helplessness* (reverse-scored).

[1] Wunder et al. 2025. Achieving Resilience: Data Loss and Recovery on Devices for Personal Use in Three Countries. *CHI25*.
[2] Joinson et al. 2023. Development of a new 'human cyber-resilience scale'. *J Cybersecurity*.

**Research Questions:**

**RQ1**: How do individuals recover after experiencing cybercrimes?

**RQ2**: Which aspects support their recovery process and contribute to individual cyber resilience?

## Trauma-informed interview

- “Trauma-informed Design Research” workshop.
- Interview protocol was reviewed by a psychologist (trauma research).
- We hired an on-call psychotherapist.
- Prior to the interview, we informed participants that they can skip/stop as they want. During the interview, we chose not to ask further if they showed hesitance.

## Interveiw protocol

Section 1: **Elicit a detailed account of the incident**

*e.g., "Can you tell us your story of the cybercrime? Feel free to share as much as you like. This might be difficult to talk about, and you can stop whenever you want"*

Section 2: **Individual's recovery process**

e.g., *How did you try to resolve the issue, if any?*

Section 3: **Lesson learned**

*e.g., What advice would you offer to others who might fall into this incident based on your experience?*

# Participant demographic (n = 18)

**Recruitment**: Prolific (180 respondents → 27 eligible → 11); Word-of-mouth recruitment (7)

**Countries**: UK (9); Germany, France, Sweden, Luxembourg & Denmark (9)

**Gender & Age**: 10 female, 8 male; 22–65 years (M = 37.8, SD = 11.7)

**Crime types**:

- Unauthorized payments, account takeovers, malware
- Scams: romance, investment, rental, buyer, task
- Impersonations(banks, crypto services, delivery companies, social platforms)

| Recognition of cybercrimes | Different coping approaches | Processing the incidents | Indicators of recovery |
| --- | --- | --- | --- |
| Emotional distress;<br>Losses (time, personal data, and money);<br>Behavioral changes | Emotion-focused;<br>Problem-focused;<br>Avoidant;<br>Misinformed coping | Rationalization;<br>Adaptation;<br>Integration | Monetary recovery;<br>Emotional calm;<br>Behavioral adjustment;<br>Reconciliation |

Fig 2: Four common stages after cybercrime victimization: recognition, coping, processing, and recovery.

## Recognition

- Most participants self-reported quite confident in managing their digital devices and online accounts.
- Situational factors, e.g., stress, distraction, and coincidental triggers, seemed to make them vulnerable to attacks.
- Some participants were able to promptly recognize the fraud and mitigate its impact, while others were warned by banks or friends.
- Half of participants experienced financial loss, almost all of them contacted their bank/crypto wallet for assistance. Leak of Personal info caused continuous attack attempts.

# Coping


Fig 3: Word Cloud to visualize the subcodes of ”crime impact” category: 88 segments of negative emotions, 13 self-blame and 8 blame from others, 10 inconvenience.

## Coping

- Cybercrimes triggered high-arousal negative emotions (panic, stress, anxiety, & angry) and low arousal negative emotions (wary, sadness, embarrassment, & annoyance).
- Half of our participants expressed self-blame or blame from external parties, indicating varied regret, self-criticism, and frustration following their victimization experiences.
- Experiences with banks varied by participant. Interactions with digital platforms exploited by attackers were limited.
- Avoidant and misinformed coping.

## Processing

- *Reconstructing their sense of security and control: rationalization, adaptation, and integration.*
- *A few participants highlighted how this incident has prompted them to exchange security-related topics with their family and friends.*
- *Participants highlighted the role of emotion, technological adaptation, and learning in protecting against online risks.*

## Recovery

- *Recovery not just in financial terms but also through psychological and behavioral aspects.*
- *Safe spaces helped victims feel less isolated and more empowered to move forward.*
- *Being able to cope with and process cybercrime to reconcile with oneself was a recurring theme mentioned by participants.*
- Security knowledge does not make participants immune to cybercrime, but it helps them recover quickly and effectively.

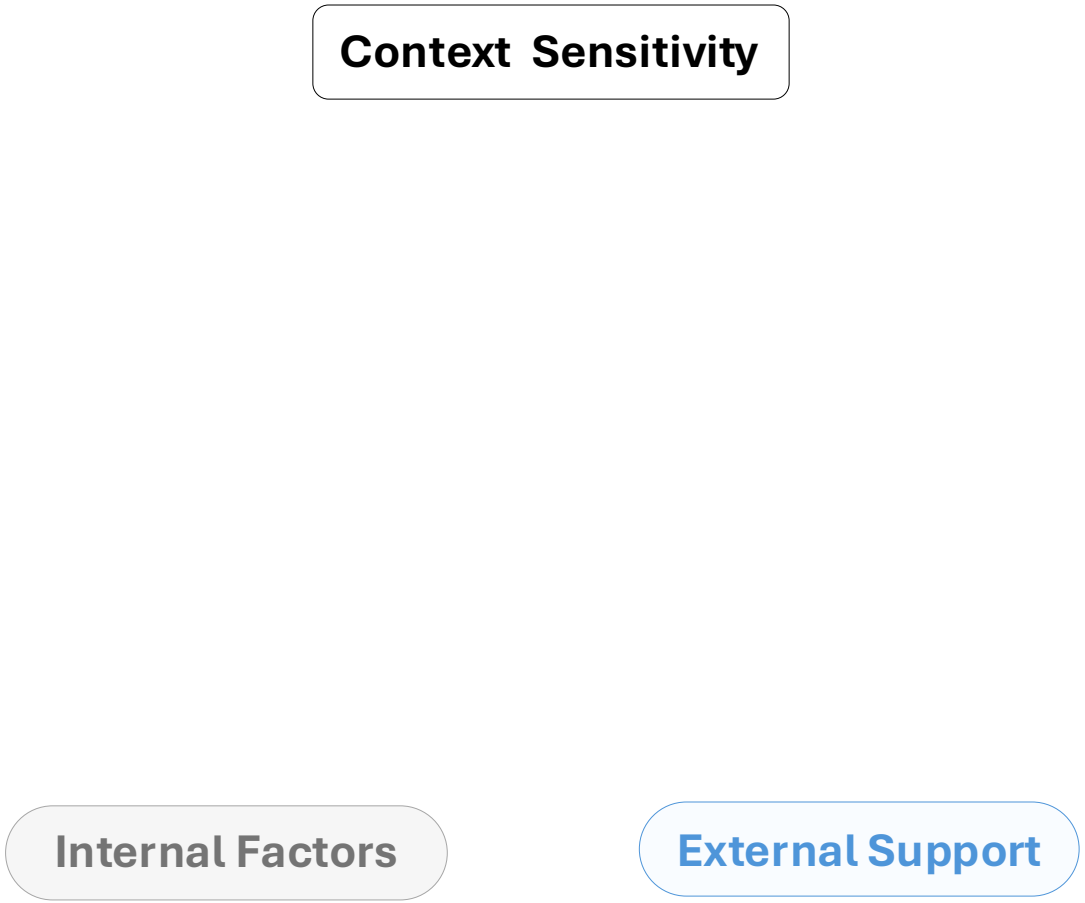


Fig 4: Visualization of Individual Cyber Resilience.

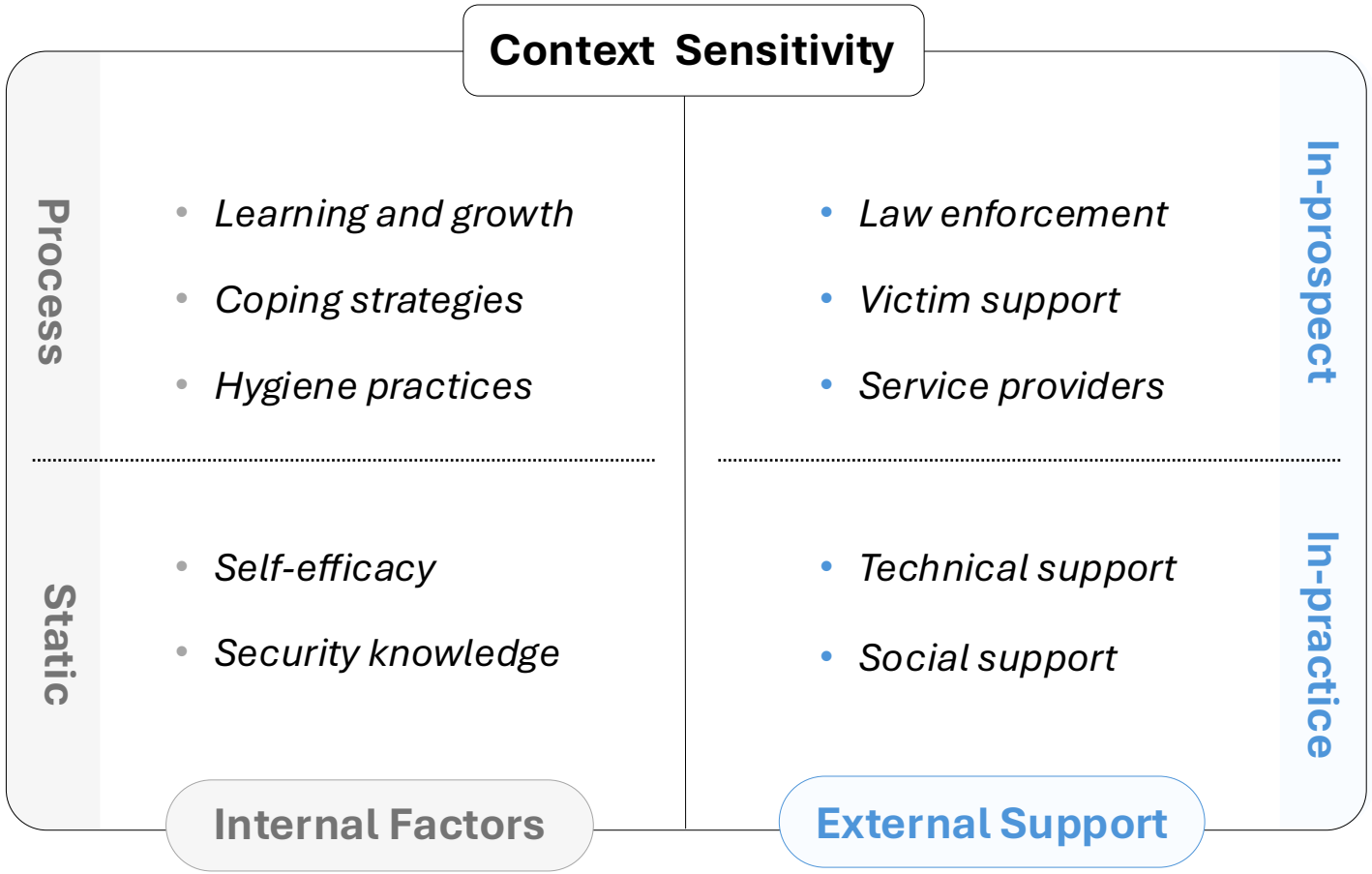


Fig 4: Visualization of Individual Cyber Resilience.

## Gaps in Victims' Needs and Institutional Actions:

- Low engagement with law enforcement;
- No participant engaged with victim support organizations, despite availability;
- Perceived indifferent or ineffective responses from service providers; however, they are the key to financial recovery.

## Future Directions:

edu.lu/w7ry6

- How can we design a reporting system to reduce victims' traumatization and facilitate their recovery?
- Can we integrate supportive interfaces into service providers' contact page?
- How can we promote trauma-informed services among cybercrime victims' first points of contact?

**Xiaowei Chen, Mindy Tran, Yue Deng**, Bhupendra Acharya, & **Yixin Zou**. (2026). From Harm to Healing: Understanding Individual Resilience after Cybercrimes. CHI 26.