Universitat Pompeu Fabra Barcelona

MANCHESTER 1824 The University of Manchester

UNIVERSITAS Miguel Hernández

When do businesses report cybercrime? Findings from a UK study

S. Kemp[1], D. Buil-Gil[2], F. Miró-Llinares[3] and N. Lord[2]

[1] Pompeu Fabra University, Spain
[2] University of Manchester, UK
[3] Miguel Hernández University of Elche, Spain

Introduction: businesses and cybercrime

1. Cybercrime poses a growing threat to organisations

Steep rises in cyber-enabled fraud against organisations during pandemic (Kemp et al., 2021)

£500 million reported losses in last 12 months (Action Fraud UK, 2021)

“small or medium-sized enterprises have around 1 in 2 chance of cyber security breach” (UK NCSC, 2020)

Lack of data
(Buil-Gil et al. 2021)

Low reporting
(Lavorgna, 2020)

Reporting is key for prevention and response
(Kemp et al. 2021)

Understand reporting, improve, get better data

What do we know about crime reporting by business?

- Crime reporting by businesses can be predicted by:
  - crime type, impact, characteristics of the organisation, perceived efficacy (e.g. Isenring et al. 2016; Taylor, 2002)
- Little research on cybercrime reporting by businesses (Rantala, 2008; van de Weijer et al., 2021):
  - lower to police than non-police
  - may depend on ability to resolve internally
  - relevance of impact
  - insurance
  - reputation

The Present Project

Research Question 1:
Are the characteristics of businesses (size, sector, digital activity) associated with cybercrime reporting?

Research Question 2:
Are the attitudes of businesses towards cyber security and the cyber security practices instituted by businesses associated with cybercrime reporting?

Research Question 3:
Are the characteristics of the cybercrime event associated with reporting?

Present study

- Business participants in 2018, 2019 and 2020 waves of CSBS (n = 4,433)
- Reweighted according to size and sector: representative.
- Companies that suffered at least one incident in previous 12 months (n = 1,965)
- Reporting to :
    - police and other public authorities
    - external private and non-profit organisations

Department for
Digital, Culture,
Media & Sport

Cyber Security
Breaches Survey
2021

Descriptive overview

- Cybersecurity incidents:
  - “staff receiving fraudulent emails or being directed to fraudulent websites” (34.5%)
  - “people impersonating your organisation in emails or online” (12.0%)
  - “computers becoming infected with other viruses, spyware or malware” (8.8%)
  - “computers becoming infected with ransomware” (5.0%)
  - “hacking of computers, networks or servers by people outside your organisation” (4.2%)
  - ‘attacks that try to take down your website or online services’ (3.4%)
  - “hacking or attempted hacking of online bank accounts” (3.3%)

- Reporting rates:
  - 39.5% reported to someone
  - 8% reported to a public authority

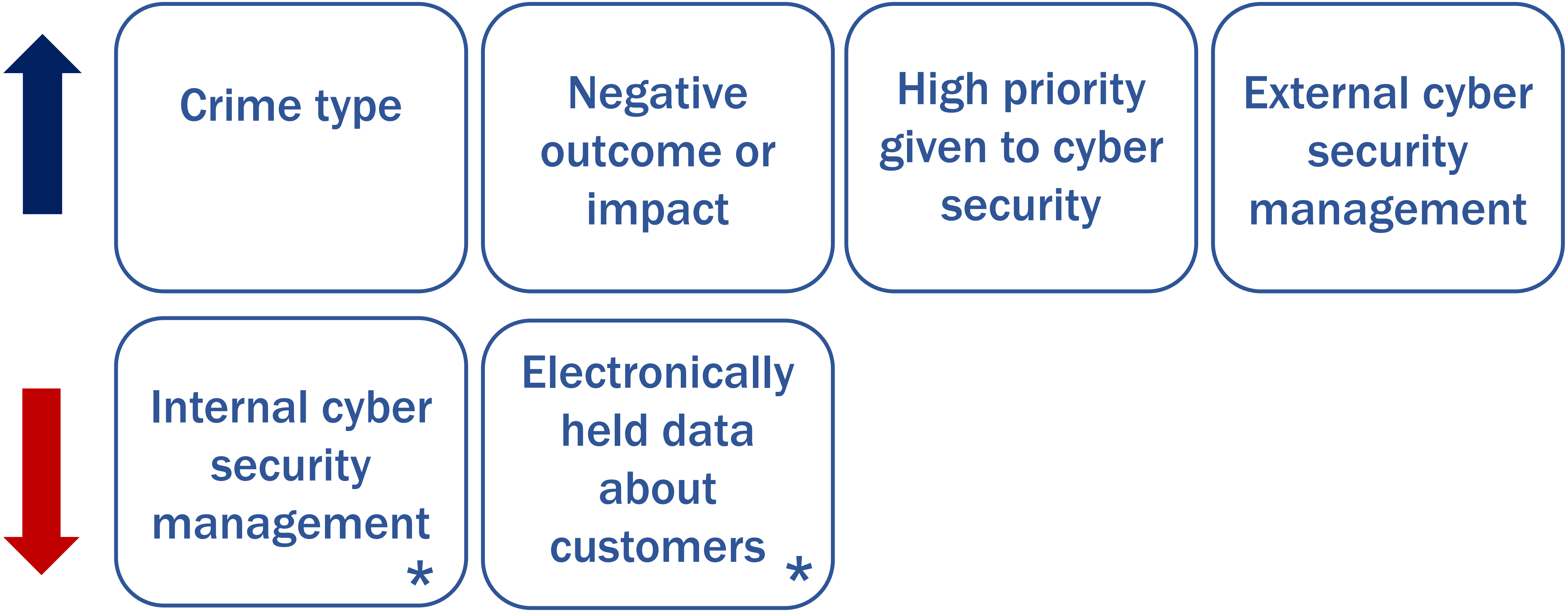
Department for
Digital, Culture,
Media & Sport

Cyber Security
Breaches Survey
2021

Variables and method

- Dependent variables:
  - Report the incident to someone outside the organisation
  - Report the incident to a UK public authority
- Independent variables:
  - Size, sector, online activities (hold personal data electronically, systems to pay or order online, online bank account, employees use personal devices for work, etc.)
  - Cybersecurity (priority, outsourced or internal cybersecurity management, insurance, risk identification, seeking government advice)
  - Crime type and whether there was a negative impact
  - In 2018 & 2019, preparedness and training
- Method: 4 binary logistic regression models to test for correlations

Results: reporting to someone outside the organisation



Crime type

Negative outcome or impact

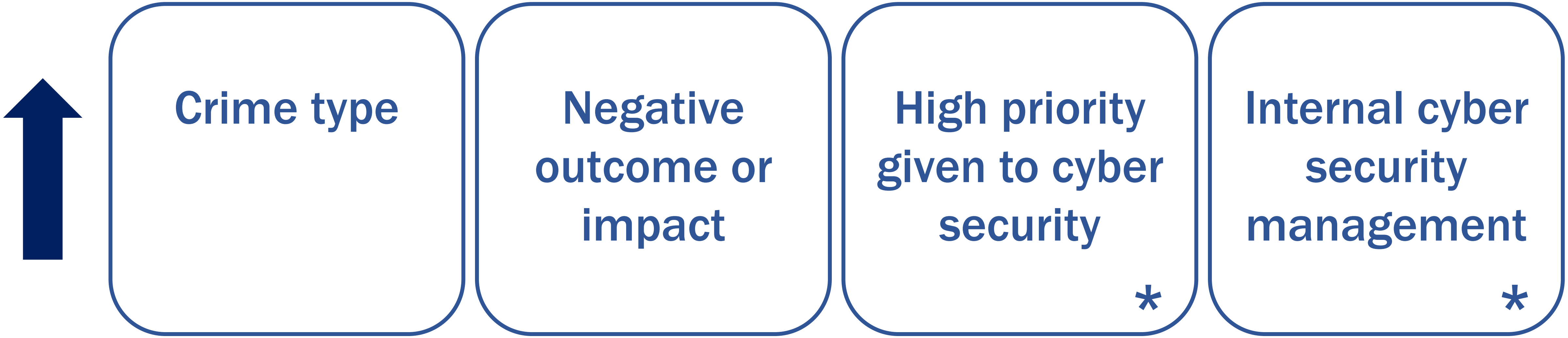
High priority given to cyber security

External cyber security management

Internal cyber security management *

Electronically held data about customers *

Results: reporting to public authorities



↑

Crime type

Negative outcome or impact

High priority given to cyber security *

Internal cyber security management *

In answer to our questions…

- RQ1 Are the characteristics of businesses associated with cybercrime reporting?
  - Limited evidence
- RQ2 Are the attitudes of businesses towards cybersecurity and the cybersecurity practices instituted by businesses associated with cybercrime reporting?
  - High priority = perceived benefits of reporting and rational choice?
  - External or internal cybersecurity management
- RQ3 Are the characteristics of the cybercrime event associated with reporting?
  - Impact: rational choice, insurance, mandatory reporting?
  - Crime type

Key takeaways and discussion

- Much lower reporting to public authorities: role of private security and the criminal justice system in cybercrime prevention?

- Role of outsourced cyber security management in reporting?

- Businesses with outsourced cyber security management report more to other organisations:
  - do cyber security companies, directly or indirectly, discourage reporting to public authorities due to lack of confidence in their ability to deal with the issue?
  - Or is there an economic interest in reducing involvement of public authorities?

- Do in-house cyber security teams trust public authorities more? Are they less driven by direct profit motive and, thus, more inclined to seek external public help?

upf. Universitat Pompeu Fabra Barcelona

MANCHESTER 1824 The University of Manchester

UNIVERSITAS Miguel Hernández

Thanks for listening!

S.Kemp, D. Buil-Gil, F. Miró-Llinares, and N. Lord

Email: steven.kemp@upf.edu

Twitter: @StvnKemp

Limitations

- Cap of 1 crime
- Don’t know or no answer to reporting = 30.8%
- Overlap between categories
- Non-response to self-reported survey because of fears for reputation