

# ICT Security Across Enterprises: What Factors Matter?

**Electronic  
Communications  
Research Programme  
Conference**  
October 2024

Iulia Siedschlag,  
Seraphim Dempsey &  
Gretta Mohan



Research results are based on analysis of strictly controlled Research Microdata Files provided by the Central Statistics Office (CSO) of Ireland. The CSO does not take any responsibility for the views expressed or the outputs generated from this research.

# Policy Background - Ireland

## 1. Cyber Security (CS) Strategy, 2019 (2015)

*'To ↑ awareness of responsibilities of businesses around securing networks, devices & info'*

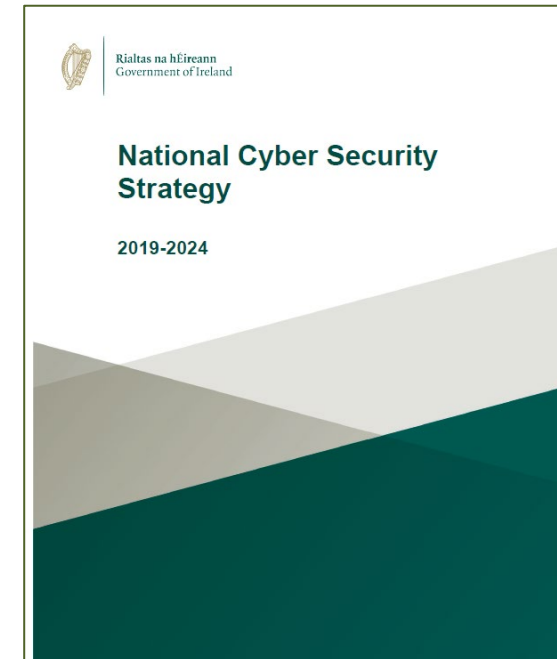
- *Rise malicious online activity - attacks on businesses for financial gain*
  - *61% reported cybercrime e.g. fraud, previous 2 yrs*
  - *Estimated average loss: €3.1m*

## 2. Digital Strategy, 2022

- *Prioritise CS capacity, expertise & infrastructure*
- *CS - barrier to digitalisation*

## 3. Mid-Term Review CS, 2023

- Exponential ↑ CS incidents
- NCSC: expand services to support SMEs
  - Grant funding for CS investment
    - Certification scheme



**Evidence = key to inform policies on digital transition**

# Legislation - Ireland & EU

## Aug 2024: General Scheme for **National Cyber Security Bill**

- Transpose NIS-2 (**Network & Information Security Directive EU 2022/2555**) into Irish law
- Regulation for ‘Essential’/‘Important’ orgs in sectors considered critical to EU’s security & functioning of economy & society:
  - Energy
  - Transportation
  - Banking
  - Digital infrastructure e.g. data centres & electronic communications networks & services
  - Digital providers e.g. social networks & online marketplaces
  - Medical devices
  - Wholesale food production & distribution



# Research questions

1. Which Irish-based firms are > or < likely to experience ICT security incidents?
2. Is the level of digital intensity of firms linked to likelihood of experiencing ICT security incidents?
3. Is adoption of ICT security mitigation measures associated with the likelihood of an ICT security incident?
4. What other factors influence likelihood of ICT security incidents?

## Micro-data sets available from Central Statistics Office (CSO)

### 1. E-commerce and ICT Survey, 2019 & 2022 (10+ employees)

- Business sectors: manufacturing, utilities, construction & services (*financial & insurance services not included*)
- Data on ICT security incidents, digitalisation, ICT security measures
- Firm size (no. employees: small (0-49), medium (50-249), large (250+))
- Firm sector - NACE code

### 2. Business Register 2019 & 2021

- NUTS3 Region
- Weights for national representativeness

### • Data coverage of linked data sets

- 2019: 2,904 firms
- 2022: 1,991 firms

(Around 500 (18%) of firms in 2019 survey captured in 2022)

# Conceptual Framework

Firm reported cyber incident

As a function of:

## Exposure to cyber incidents

- **Digital intensity** of the firm (/sector)
- *Size (number of employees)*

## Firm-level ICT security measures

## External factors



- Sector-specific
- Region-specific

Source: Authors' own elaboration.

# Outcome of interest: ICT security incident

- Had ICT security incident in previous year:
  - =1 where report any incident any of the listed types of ICT security incidents;  
0 otherwise

**E6** During 2018, did your enterprise experience, at least once, any of the following problems due to ICT related security incidents?

- (a) Unavailability of ICT services   
*(e.g. Denial of Service attacks, ransomware attacks, hardware or software failures excluding mechanical failure, theft etc.)* Yes  No
- (b) Destruction or corruption of data  
*(e.g. due to infection of malicious software or unauthorised intrusion, hardware or software failures)* Yes  No
- (c) Disclosure of confidential data   
*(e.g. due to intrusion, pharming, phishing attack, actions by own employees (intentionally or unintentionally))* Yes  No

# Exposure of interest I: Digital intensity

- **Firm Digital Intensity Index (DII) 2019 (based on Eurostat)**
  1. 50% + persons employed used COMPUTERS with access to the internet for business purposes
  2. Max download speed 30Mb/s +
  3. Provide 20%+ of employees with portable internet connected device for business purposes
  4. Received electronic \*orders (web/EDI) from customers from other EU countries
  5. Use any social media
  6. Have ERP software package to share information b/t different functional areas
  7. Have CRM
  8. Use social media for at least 2 purposes
  9. Used any computer networks for sales (at least 1%)
  10. Web sales >1% of total turnover & B2C web sales >10% of web sales

<b>Firm Digital Intensity</b>	<b>Category</b>
0-1	Very Low Digital Intensity
2-4	Low
5-7	Medium
8-10	High



# Exposure of interest II: ICT security

- **Firm level ICT security index, 2019**

1. Has at least 3 security measures
2. Enterprise makes people aware of their obligations in ICT security related issues
3. Documents on ICT security
4. Has insurance against ICT security incidents
5. Has internal/external people carrying out ICT security

---

<b>ICT security</b>	<b>Category</b>
0-2	Low
3-4	Medium
5	High

## Summary Statistics

	<b>2019</b>	<b>2022</b>
Sample size (N)	2904	1991
Had ICT security incident (%)	20.8	17.7

## Statistics by firm size groups

**2019** (*similar pattern for 2022*)

N=2904	<b>Small</b>	<b>Medium</b>	<b>Large</b>
Sample size (%)	50.3	39.2	10.4
Had ICT security incident (%)	17.8	22.1	30.5

## Statistics by sector

**2019** (similar pattern for 2022)

N=2904	Manufacturing	Utilities	Construction	Trade/repair	Transport/ Storage	Accom/Food	ICT	Real Estate	Technical activities	Administrative activities
Sample size (%)	15.7	1.5	6.7	27.8	4.9	14.0	7.8	1.3	11.7	8.8
Had ICT security incident (%)	21.9	9.3	20.0	22.0	21.9	15.8	24.0	24.3	22.3	19.6

## Statistics by region

**2019** (similar pattern for 2022)

N=2904	Border	West	Mid-West	South-East	South-West	Dublin	Mid-East	Midlands
Sample size (%)	6.4	7.8	8.1	7.0	12.9	42.9	11.2	3.7
Had ICT security incident (%)	16.0	18.5	23.5	19.1	19.5	22.4	21.0	15.9

# Model estimation results

# Probability of reporting ICT security incident in previous year - 2019

	(1)
Digital Intensity Index (DII) (continuous)	0.027*
DII category	
- Very low ( <i>Ref</i> )	
- Low	
- Medium	
- High	
ICT security (continuous)	
ICT security (category)	
- Low ( <i>Ref</i> )	
- Medium	
- High	
Number of employees (log)	0.040***
Sector controls	Y
<i>Ref: Manufacturing</i>	
-Utilities	-0.114*
-Accommodation /Food	-0.499
Region controls	Y
<i>Ref: Border – no significant regional dii</i>	
Mean	0.208
Pseudo R-squared	0.044
n	2904

Notes: Estimates reported as average marginal effects. t statistics in parentheses  
 Statistical significance denoted as: \* p<0.05, \*\* p<0.01, \*\*\* p<0.001

## Likelihood of reporting ICT security incident in previous year - 2022

	(1)	(2)	(3)	(4)	(5)
DII (continuous)	0.035***		0.028***	0.030***	
DII category					
- Very low ( <i>Ref</i> )					
- Low		0.095***			0.087***
- Medium		0.152***			0.136***
- High		0.194***			0.173***
ICT security (continuous)			0.028***		
ICT security (category)					
- Low ( <i>Ref</i> )					
- Medium				0.046*	0.043
- High				0.070*	0.070*
Number of employees (log)	0.008	0.010	0.001	0.003	0.005
Sector controls	Y	Y	Y	Y	Y
<i>Ref: Manufacturing – no significant sectoral differences</i>					
Region controls	Y	Y	Y	Y	Y
<i>Ref: Border – no significant regional differences</i>					
Mean	0.178	0.178	0.178	0.178	0.178
Pseudo R-squared	0.043	0.043	0.049	0.046	0.046
n	1990	1990	1990	1990	1990

Notes: Estimates reported as average marginal effects. t statistics in parentheses  
 Statistical significance denoted as: \* p<0.05, \*\* p<0.01, \*\*\* p<0.001



# Key findings - Descriptives

- Between 2019 & 2022
  - ↓ average no. reported ICT security incidents
  - ↑ average DI scale
  - ↓ average ICT security scale
    - > share reporting 'low' ICT security, < share with 'medium' / 'high'
- **Larger firms:** more likely to have had ICT security incident, > DI & > ICT security
- **Sectors:**
  - **ICT, real estate & technical activities** > security incidents & > DI & > ICT security
  - Opposite for **construction**  
[Utilities in 2019 – high investment in ICT security – low incidents]
- **Regions:**
  - **Dublin & west/mid-west** most ICT security incidents
  - Dublin most DI & ICT security
  - **Border** areas lowest DI & ICT security

# 'Take-aways': Estimation results

- Econometric modelling which controls for firm size, sector region finds:
  - >DI & progressively higher levels of DI associated with a > likelihood of reporting ICT security incident
  - Similarly, > ICT security associated with > likelihood of reporting ICT security incident
  - 2019 models – sectors 'utilities' & 'accommodation & food' (*relative to manufacturing*) -ve ass. w/ ICT security incidents (no sectoral differences for 2022 models)
  - No statistically significant differences for regions

# Questions/feedback



# Additional slides

# Limitations & Further Research

## Data Limitations

1. **Once-off questions & cross-section data** allowing to uncover structural relationships - questions around causality could be further investigated where longitudinal data is made available
2. The linked dataset characterised by firms with 10+ persons engaged in the business sector - **findings may not generalise to very small/micro enterprises**
3. Data from the *E-commerce and ICT survey*: **self-reported information** from firms may be subject to **measurement error** and thus could lead to **bias** in estimations

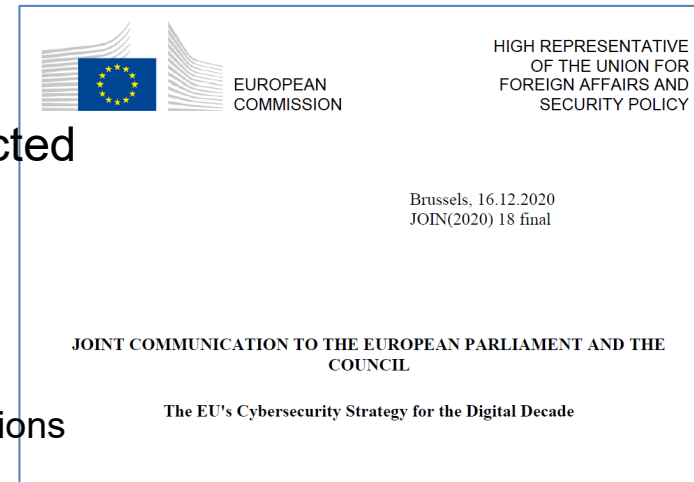
## Further Research

- Merge the 2 datasets
- Examine non-linear effects
- Continued monitoring of cyber incidents in Irish firms – and trends in levels of protection
- Examine the impact of cyber security incidents on firm performance **outcomes**: output growth, productivity

# Policy Background - Europe

## 1. EU's Cybersecurity Strategy, 2020

- 1-in-8 businesses affected by cyberattacks
- > ½ business & consumer personal computers infected w/ malware = re-infected
- 100s of millions of records lost in data breaches
  - Average cost of breach €3.5m
- Impact of cyberattack cannot be isolated -
  - chain reactions through economy & society, affecting millions



## 2. EU's Digital Strategy, 2020

- Digital transformation - citizens & businesses trust applications & products secure
- Need:
  - Consistent rules for companies & mechanisms for proactive information-sharing
  - Operational cooperation b/t Member States, EU + MS's
  - Synergies b/t civilian cyber resilience, law enforcement & defence
  - Ensure law & judicial authorities develop new tools to use against cybercriminals
  - Raise awareness among EU citizens

## Related literature

- **Cyber incidents** associated w/ **increased digitalisation of firms** (Greenberg, 2018) – firms with ↑ digital intensity = more exposed to cyber incidents
- **Perception of cyber security risks & implementation of ICT security measures** vary across firms & industries (Franke & Wernberg, 2020)
- **Cyber incidence probability & maturity of ICT security measures**
  - negative relationship (Gandal et al., 2022)
  - inverted U-shaped relationship (“n”) (Dinkova et al., 2023)
    1. Basic ICT security measures – better detection of cyber incidents
    2. More security measures - ↑ cyber incidents
    3. Most sophisticated ICT measures – ↑ prevention of cyber incidents
- **Increased awareness & training** ↓ incidence of cyber incidents (Kweon et al., 2021)

# Exposure of interest I: Digital intensity 2022

- **Firm Digital Intensity Index 2022**

1. 50%+ persons employed have access to the internet for business purposes
2. Employ ICT specialists
3. Download speed 30mbs+
4. Enterprise which conducted remote meetings
5. Any type of training provided to develop ICT related skills of the persons employed during 2021
6. Any of the persons employed has remote access to any of email, documents, business apps
7. Use industrial or service robots
8. Used any computer networks for sales (1%+)
9. Web sales 1%+ of the total turnover & B2Cweb sales 10%+ web sales

- Scale which runs from 0-9:

<b>Firm Digital Intensity</b>	<b>2022 Category</b>
-------------------------------	----------------------

0-2	Very Low Digital Intensity
-----	----------------------------

3-4	Low
-----	-----

5-6	High
-----	------

7-9	Very High
-----	-----------



# Exposure of interest II: ICT security mitigation 2022

## Firm level Mitigation Index, 2022

1. Enterprise makes people aware of their obligations in ICT security related issues
2. Has at least 3 security measures
3. Enterprise with documents on ICT Security
4. Has insurance against ICT security Incidents
5. Has internal/external people carrying out ICT security

*(Scale & category thresholds same 2019 & 2022)*

- Continuous scale (0-5):

<b>ICT Protection</b>	<b>2022 Category</b>
0-2	Low protection
3-4	Medium protection
5	High protection

# Empirical Methodology

## Econometric Model

$$\text{Prob}(Y_{it} = 1 | \alpha_1 DII_{it}, \alpha_2 P_{it}, \beta X_{it}, \sigma_k, \rho_j, \varepsilon_{it}) = F(\alpha_1 DII_{it} + \alpha_2 P_{it} + \beta X_{it} + \sigma_k + \rho_j + \varepsilon_{it})$$

$Y_{it}$ : 1 if firm  $i$  reported ICT security incident in year  $t$ , 0 otherwise

$DII_{it}$ : DI Index of firm, in year  $t$

$\alpha_2 P_{it}$ : Level of ICT security of firm, in year  $t$

$X_{it-2}$ : vector of control variables in year  $t$

$\alpha, \beta$  are parameters to be estimated

$\sigma_k$  controls for unobserved sector-specific fixed effects

$\rho_j$  controls for unobserved region-specific fixed effects

$\varepsilon_{it}$ : error term capturing unobserved omitted variables associated with ICT security incidents, digitalisation, ICT security e.g., managerial quality

## ICT security incidents across sector

2022

N=1991	Manufacturing	Utilities	Construction	Trade/repair	Transport/ Storage	Accom/Food	ICT	Real Estate	Technical activities	Administrative activities
Sample size (%)	33.9	3.1	4.4	14.3	4.7	6.5	10.9	3.2	11.7	7.1
Had ICT security incident (%)	16.7	11.3	16.1	19.6	15.8	16.0	18.9	15.6	21.6	19.1

# ICT security incidents across regions

**2022**

N=1991	Border	West	Mid-West	South-East	South-West	Dublin	Mid-East	Midlands
Sample size	7.6	7.1	8.4	8.0	13.5	39.0	12.0	4.2
Had ICT security incident (%)	13.2	21.7	16.7	10.6	17.1	20.7	18.0	9.5