Kokaji and Goto
Journal of Economic Structures (2022) 11:34
https://doi.org/10.1186/s40008-022-00286-4

Journal of Economic Structures

RESEARCH Open Access

An analysis of economic losses from cyberattacks: based on input–output model and production function

Akiyoshi Kokaji* and Atsuhiro Goto

*Correspondence:
dgs208101@iisec.ac.jp

Institute of Information Security, 2-14-1 Tsuruya-Cho, Kanagawa-Ku, Yokohama, Kanagawa 221-0835, Japan

Abstract

There has recently been a global increase in economic losses due to cyberattacks. However, research on the economic damage caused by cyberattacks has mainly focused on attacked companies, and spillover damage to other sectors has not been sufficiently investigated. This study analyzed the economic losses from cyberattacks in Japan using the production function and input–output model to improve the accuracy of damage prediction and various national measures. First, we provide an estimation method for the annual direct damage by industry using a production function. The mainstream input dataset is lost working hours owing to cyber incidents. Second, we devised a model to estimate the amount of spillover damage to the entire country using the input–output model. Third, although the cyber damage data were limited to only interview data by the JNSA and IPA, we showed the process of estimating direct and spillover damage in all sectors in Japan. As a result, we consider that our estimation method is feasible and effective at the national level. This study contributes to future research on cyber resilience by analyzing the damage caused by cyberattacks from a macroeconomic perspective using a production function and input–output model.

Keywords: Cyber security, Input–output model, Production function, Spillover damage of cyberattacks

1 Introduction

Several studies have examined the extent of the damage caused by natural and manufactured disasters. These studies determined the amount of damage caused in Japan and its various regions. A report by the Cabinet Office (2013) estimated direct damage from natural disasters to be between 97.6 and 169.5 trillion yen, and the full amount of damage has been estimated to be between 35.1 and 50.8 trillion yen in the Nankai Trough earthquake. Concerning the economic damage caused by cyberattacks, CSIS (2021) indicated that the damage exceeded USD 1 trillion and accounted for 1% of the global gross domestic product. Despite this huge loss, studies on the economic damage caused by cyberattacks have been restricted to micro-analyses. Few studies have performed comprehensive and quantitative damage analyses, including an analysis of spillover damage. Although the government of Japan has adopted several cyber security policies, such as

supply chain security for critical infrastructures in CS (2021), it must be understood that an objective and quantitative analysis of results is the key to effective policymaking.

This study devised a method for quantitatively estimating the economic damage caused by cyberattacks in Japan and contributed to improving the accuracy of damage prediction and the formulation of various national measures. Specifically, we devised a method to analyze Japan's economic damage caused by cyberattacks using production functions and input–output analysis.

The remainder of this paper is organized as follows. Section 2 reviews research analyzing the economic damage caused by natural disasters and cyberattacks. Section 3 presents a method for estimating the direct and spillover damage. Section 4 presents our estimation results and provides a discussion of our findings. Section 5 presents the conclusions of the findings and plans for future research.

2 Previous research

2.1 Analysis in Japan

Most estimation studies on economic loss due to cyberattacks in Japan are restricted to microeconomics analysis and lack quantitative analysis of the economic damage from cyberattacks. Tanaka et al. reported an estimation of economic loss due to information security incidents in Japan of about 4.6 to 9.4 billion yen from 2009 to 2011, respectively, in Tanaka (2014), but their study lacks established methods of analysis. For example, no analysis of spillover damage has been conducted yet.

In the case of natural disasters, studies have shown that the amount of damage is estimated using a production function and input–output table. For example, Shimoda and Fujikawa (2012) used an input–output model to measure the damage caused by the Great East Japan Earthquake on the demand side (backward-relation effect) of production, which experienced a decline, as well as on the supply side. A supply type model is used to measure spillover damage (forward output effect) at the initial stage of the disaster, and a demand-type model is used thereafter.

In Japan, the Information Technology Promotion Agency (IPA) and the Japan Network Security Association (JNSA) have published the results of their analyses of cyberattack damage. The amount of damage was calculated based on their self-developed model. However, the amount of damage from each incident is limited to that of the victim company, and there is no model for calculating the amount for the entire country. Tanaka (2013) suggest using the Cobb–Douglas production function to estimate cyber damage in the entire country, but none showed its feasibility and effectiveness.

2.2 Analysis overseas

Japan's Ministry of Internal Affairs and Communications has analyzed several cases of cyberattacks in the MIC (2019). Emphasizing the model and data related to estimating the amount of damage, Appendix 2 summarizes the analyses.

In terms of the model for estimating the amount of damage, only two studies[1] used the existing economic analysis model. The other models are original, unpublished models.

[1] RAND Cooperation uses the input–output table by the Organization for Economic Co-operation and Development to calculate the spillover damage of cyberattacks. The Mitsubishi Research Institute, Inc. analyzes the reputational damage of cyberattacks from the stock price effect before and after a certain event (e.g., mergers and acquisitions), by analyzing the cumulative abnormal returns. A method for analyzing changes in corporate value is used.

Lloyd and the University of Cambridge's Center for Risk Studies have used the input–output model to calculate spillover damage (disruption of the power supply) from cyberattacks on a power grid on the east coast of the United States.

2.3 Brief summary

We found a limited number of models to calculate the amount of damage. The few existing models are unpublished, self-made models, and most damage amount calculations are based on subjective estimation, which is a general economic effect. Few quantitative estimates have been based on the objective methods used in the analysis. Appropriate analysis cannot be performed using a subjective analysis alone.

In summary, there is no established model for analyzing/estimating the damage and target data and range, among others, of the damage from cyberattacks. The most targeted damage is direct. There is only one overseas document on spillover damage. Reports on the scope of the target damage often differ depending on the literature, and the data are not unified.

Therefore, it is meaningful to estimate the direct and spillover damages using the production and input–output models, respectively. In addition, this study collected mainstream data through interviews and hearings, considering that incident data from cyberattacks are often not disclosed.

3 Methods for estimating direct and spillover damage

3.1 Overview

In this study, we constructed a production function and measured the decrease in production value due to a decrease in the labor force of the IT department caused by cyberattacks. In addition, we measured the negative production-inducing effect caused by this decrease in production using input–output analysis and estimated spillover damage.

The production function expresses the relationship between the production factor and the output (production value/gross value-added amount) using mathematical formulas. Capital stock and labor, considered the most universal factors of production, are usually used as explanatory variables for output. We recognized that analysis by the production function is a suitable approach for calculating the economic damage (from the viewpoint of production) in the event of a cybersecurity incident involving labor damage, as in this study.

Spillover damage (decrease in production) due to damage involving production factors leads to a further decrease in production through dependency between industries. For example, if production were stopped because of a disaster, it would also stop the production of industrial parts. The industrial suspension of industrial parts further causes the production suspension of other parts and raw materials. Input–output analysis is a powerful tool for measuring the magnitude of such spillover damage.

3.2 Direct damage estimation method using the production function

3.2.1 Model

We estimated the direct damage from cyberattacks (including viral infections) to the entire country based on the system and data recovery times. Our estimation model agrees with that of Tanaka (2014).

We estimated the production function by assuming that "the net value added ($\boldsymbol{Y}$)" can be realized by the labor force ($\boldsymbol{L}$-$\boldsymbol{Lr}$) after deducting the system recovery time and data recovery working times ($\boldsymbol{Lr}$) associated with a cyberattack (Eq. (1)). Then, based on the coefficient of the production function, using the labor force ($\boldsymbol{L}$), we were able to determine when the system recovery time and working time ($\boldsymbol{Lr}$) could be used for the original production activity ($\boldsymbol{Y}^{+}$). The difference between ($\boldsymbol{Y}^{+}$) and ($\boldsymbol{Y}$) was used as the direct damage amount ($\boldsymbol{LS}$) (Eq. (2)). We assumed that $\boldsymbol{K}$ is capital stock and constant, regardless of cybersecurity incidents, systems, or data recovery. In addition, Eq. (1) is established when the relationship $\alpha+\beta=1$ (constant returns to scale) holds for capital allocation ratio α and labor allocation ratio β:

$$\boldsymbol{Y} = \boldsymbol{A}\boldsymbol{K}^{\alpha}(\boldsymbol{L}-\boldsymbol{Lr})^{1-\alpha}. \tag{1}$$

Dividing both sides of Eq. (1) by $\boldsymbol{L}-\boldsymbol{Lr}$ gives Eq. (2):

$$\boldsymbol{Y}/(\boldsymbol{L}-\boldsymbol{Lr}) = \boldsymbol{A}\boldsymbol{K}^{\alpha}(\boldsymbol{L}-\boldsymbol{Lr})^{-\alpha} = \boldsymbol{A}(\boldsymbol{K}/(\boldsymbol{L}-\boldsymbol{Lr}))^{\alpha}. \tag{2}$$

To calculate the amount of damage directly based on Eq. (2), we estimated the production function of Eq. (1); however, A, α, and β were calculated based on the logarithmic transformation in Eq. (3):

$$\ln\boldsymbol{Y}/(\boldsymbol{L}-\boldsymbol{Lr}) = \ln\boldsymbol{A} + \alpha\ln\boldsymbol{K}/(\boldsymbol{L}-\boldsymbol{Lr}). \tag{3}$$

Because the relationship between $\boldsymbol{Y}^{+}$ and $\boldsymbol{Y}$ in Eq. (2) is $\boldsymbol{Y}^{+}/\boldsymbol{Y}=(\boldsymbol{L}/(\boldsymbol{L}-\boldsymbol{Lr}))^{\boldsymbol{1-\alpha}}$, the amount of damage can be calculated directly using Eq. (4):

$$\boldsymbol{LS} = ((\boldsymbol{L}/\boldsymbol{L}-\boldsymbol{Lr})^{1-\alpha}-\boldsymbol{1})\boldsymbol{Y} = ((\boldsymbol{L}/\boldsymbol{L}-\boldsymbol{Lr})^{\beta}-\boldsymbol{1})Y. \tag{4}$$

3.2.2 Dataset

We collected economic statistical data published by IPA, JNSA, and unpublished JNSA data. We classified the industrial sector based on 108 industries' data from the Japan Industrial Productivity (JIP) database of the Institute of Economic and Industrial Research.

We describe the following components: (1) output ($\boldsymbol{Y}$), capital stock ($\boldsymbol{K}$), and labor force ($\boldsymbol{L}$); (2) number of working hours ($\boldsymbol{Lr}$) allocated to the system or data recovery times; and (3) estimation method of A, α, and β.

1) Output ($\boldsymbol{Y}$), capital stock ($\boldsymbol{K}$), and labor ($\boldsymbol{L}$)

The net value added ($\boldsymbol{Y}$) is calculated by subtracting the intermediate input from the output using the sectoral output/intermediate input reported in the 2015 JIP data input–output table. Capital stock ($\boldsymbol{K}$) denotes the real net capital stock of the capital sector and investment data. We used data on man-hours, given that the total number of working hours of ($\boldsymbol{L}$) is critical to reflect the system data recovery time after cyberattacks.

2) Number of working hours (***Lr***) allocated for system recovery or data recovery after a cyberattack

Because there are no data on the number of working hours, we estimated (***Lr***) allocated for the system or data recovery by each industry using the following procedure. In addition, ***Lr*** is the time spent on system and data recovery only for the IT department:

A) National-level estimation of the number of working hours allocated to the system or data recovery after a cyberattack

The IPA report (2014) outlined the time the IT department took to recover the system after a cyberattack, the additional data processing time (time spent other than recovery), and the time required to resolve other incidents. For this survey, 13,000 companies with more than 21 employees were randomly selected by industry, whose number of employees was from a private company database (Teikoku Databank). The responses to this questionnaire were 1913, with a valid response rate of 14.7%.

An analysis of the valid responses shows in the case of "large companies with more than 300 employees", the IT personnel spent 18.5 h, 5.6 h, and 23.1 h (total 47.2 hours) on recovery, additional data processing, and other incidents. In the case of "companies of between 21 and 300 employees", they are 13.1 h, 3.8 h, and 23.1 h (40.0 h total), respectively.

The 2014 economic census reported that the number of large companies with 300+ employees is 15,526, and that of employees between 300 and 20 is 320,085. We estimated the lost time for IT department employees to be 728,205 h and 12,795,816 h, respectively, for a total of 13,524,021 h. For reference, this means that the average lost time of the IT department per company is 40.3 h in each cyberattack incident.

It should be noted that this time is only the time lost in the "IT department" and does not include the time lost in other departments such as sales and administration departments.

B) Estimation of the number of working hours by industry

The industries and number of employees are stratified sampling (proportional allocation method) based on the distribution of companies by the number of employees and by industry in the Japan Standard Industrial Classification of the 2012 Economic Census to ensure statistical validity.

Using the number of IT department working hours for the entire country estimated in (A), we estimated the number of working hours by industry based on the 2017 JNSA information security incident data (380 data).

The JNSA data were generated by collecting and analyzing the results of analyses of personal information leakage incidents reported in newspapers and the Internet in

Table 1 The amount of damage by 108 industries calculated by JNSA

JIP data (108 industries)		Damage calculated by JNSA (ten thousand yen)	Proportion (%)
Code	JIP industry name		
9	Seafood products	36,761	0.2
28	Miscellaneous chemical products	7653	0.0
29	Pharmaceutical products	39	0.0
59	Miscellaneous manufacturing industries	718,731	4.1
62	Electricity	1296	0.0
63	Gas, heat supply	97	0.0
67	Wholesale	107,287	0.6
68	Retail	1,273,817	7.3
69	Finance	750,424	4.3
71	Real estate	296	0.0
79	Mail	18,132	0.1
80	Education (private and non-profit)	12,93	0.1
81	Research (private)	8	0.0
84	Other public services	11,566,30	66.0
88	Other services for businesses	13	0.0
90	Broadcasting	296,16	1.7
91	Information services and internet-based services	1,141,597	6.5
92	Publishing	1,449,170	8.3
95	Accommodation	54,421	0.3
97	Other services for individuals	80,500	0.5
Total		17,516,211	100.0

Source: Created by the authors based on JNSA

the relevant fiscal year; these data originally included cases unrelated to cyberattacks. Therefore, we sorted the contents of each incident data and identified cases of cyberattacks[2] (75 of 380 cases were cyberattacks).

Subsequently, we identified the industry (108 industries) from industry category information in the 75-incident data. Next, the amount of damage for each incident calculated independently by the JNSA was tabulated by country and industry (108 industries). Table 1 shows the amount of damage calculated by the JNSA for each incident using self-made method aggregated for each of the 108 industries.

Then, we calculated the ratio of the whole country and each industry regarding damage calculated by the JSNA and apportioned the direct damage amount of the whole country calculated in (A) to each industry using this ratio. Table 2 shows the results. In this study, we used 2017 JNSA data. In the JNSA data, only the 2017 data show the industry category; therefore, we directly used the industry category of the FY2017 JNSA data.

[2] Incident data leakage identified cause categories; such as worm viruses, bug security holes, and unauthorized access during cyberattacks. The cause categories excluded from the target include: internal fraud, loss/misplacement, distress, and erroneous operation.

Table 2 *Lr* of 108 industries

				(1000 h)	
JIP data (108 industries)		**Lr (recovery working time)**	**JIP data (108 industries)**		**Lr (recovery working time)**
Code	**JIP industry name**		**Code**	**JIP industry name**	
1	Rice, wheat production	0	55	Motor vehicle parts and accessories	0
2	Miscellaneous crop farming	0	56	Other transportation equipment	0
3	Livestock and sericulture farming	0	57	Precision machinery & equipment	0
4	Agricultural services	0	58	Plastic products	0
5	Forestry	0	59	Miscellaneous manufacturing industries	555
6	Fisheries	0	60	Construction	0
7	Mining	0	61	Civil engineering	0
8	Livestock products	0	62	Electricity	1
9	Seafood products	28	63	Gas, heat supply	0
10	Flour and grain mill products	0	64	Waterworks	0
11	Miscellaneous foods and related products	0	65	Water supply for industrial use	0
12	Prepared animal foods and organic fertilizers	0	66	Waste disposal	0
13	Beverages	0	67	Wholesale	83
14	Tobacco	0	68	Retail	983
15	Textile products	0	69	Finance	579
16	Lumber and wood products	0	70	Insurance	0
17	Furniture and fixtures	0	71	Real estate	0
18	Pulp, paper, and coated and glazed paper	0	72	Housing	0
19	Paper products	0	73	Railway	0
20	Printing, plate making for printing and bookbinding	0	74	Road transportation	0
21	Leather and leather products	0	75	Water transportation	0
22	Rubber products	0	76	Air transportation	0
23	Chemical fertilizers	0	77	Other transportation and packing	0
24	Basic inorganic chemicals	0	78	Telegraph and telephone	0
25	Basic organic chemicals	0	79	Mail	14
26	Organic chemicals	0	80	Education (private and non-profit)	10
27	Chemical fibers	0	81	Research (private)	0
28	Miscellaneous chemical products	6	82	Medical (private)	0
29	Pharmaceutical products	0	83	Hygiene (private and non-profit)	0
30	Petroleum products	0	84	Other public services	8,931
31	Coal products	0	85	Advertising	0
32	Glass and its products	0	86	Rental of office equipment and goods	0
33	Cement and its products	0	87	Automobile maintenance services	0
34	Pottery	0	88	Other services for businesses	0
35	Miscellaneous ceramic, stone and clay products	0	89	Entertainment	0

Table 2 (continued)

				(1000 h)	
JIP data (108 industries)		**Lr (recovery working time)**	**JIP data (108 industries)**		**Lr (recovery working time)**
Code	**JIP industry name**		**Code**	**JIP industry name**	
36	Pig iron and crude steel	0	90	Broadcasting	229
37	Miscellaneous iron and steel	0	91	Information services and internet-based services	881
38	Smelting and refining of non-ferrous metals	0	92	Publishing	1119
39	Non-ferrous metal products	0	93	Video picture, sound information, character information production and distribution	0
40	Fabricated constructional and architectural metal products	0	94	Eating and drinking places	0
41	Miscellaneous fabricated metal products	0	95	Accommodation	42
42	General industry machinery	0	96	Laundry, beauty and bath services	0
43	Special industry machinery	0	97	Other services for individuals	62
44	Miscellaneous machinery	0	98	Education (public)	0
45	Office and service industry machines	0	99	Research (public)	0
46	Electrical generating, transmission, distribution and industrial apparatus	0	100	Medical (public)	0
47	Household electric appliances	0	101	Hygiene (public)	0
48	Electronic data processing machines, digital and analog computer equipment and accessories	0	102	Social insurance and social welfare (public)	0
49	Communication equipment	0	103	Public administration	0
50	Electronic equipment and electric measuring instruments	0	104	Medical (non-profit)	0
51	Semiconductor devices and integrated circuits	0	105	Social insurance and social welfare (non-profit)	0
52	Electronic parts	0	106	Research (non-profit)	0
53	Miscellaneous electrical machinery equipment	0	107	Other (non-profit)	0
54	Motor vehicles	0	108	Activities not elsewhere classified	0
			Total		13,524

Source: Created by the authors

3) A, α, and β (scale coefficient (A), capital share (α), and labor share (β) in the production function)

We calculated A, α, and β based on Eq. (3), which is a logarithmic transformation of Y, K, L, and Lr for the 108 sectors from 2013 to 2015. Following the method highlighted in the study by Tanaka (2014), in the JIP data, the industrial sections codes 72 (housing) and 108 (activities not elsewhere classified) for three years from 2013 to 2015, and 36 (pig iron and crude steel) for 2013 were excluded. This is because the added value, capital stock, and labor man-hours were zero, owing to a lack of data.

The results of the estimation were as follows: $A = 0.23370315$, $\alpha = 0.53480907$, $\beta = 0.46519093$. The coefficient of determination R2 of $Y/(L-Lr)$ on the left-hand side and $K/(L-Lr)$ on the right-hand side of Eq. (3) was 0.5214027.

3.3 Estimating method of spillover damage by input–output model

3.3.1 Model

We estimated the spillover damage by industry based on the amount of direct damage by industry, as calculated in 3–2, and using the following input–output model: specifically, the amount of damage is calculated using a competitive import model. We define input coefficient matrix $\boldsymbol{A}$, final demand column vector $\boldsymbol{F}$, output vector $\boldsymbol{Y}$, $n \times n$ unit matrix $\boldsymbol{I}$, export column vector $\boldsymbol{E}$, and import column vector $\boldsymbol{M}$. If $\widehat{M}$ is a matrix with the import coefficients on the diagonal and zeros for the off-diagonal, then we can express the formula as follows:

$$\begin{aligned} &\boldsymbol{Y} = \boldsymbol{AY} + \boldsymbol{F} + \boldsymbol{E} - \boldsymbol{M} = \boldsymbol{AY} + \boldsymbol{F} + \boldsymbol{E} - \widehat{\boldsymbol{M}}(\boldsymbol{AY} + \boldsymbol{F}) \\ &\quad \Leftrightarrow \boldsymbol{Y} = (\boldsymbol{I} - (\boldsymbol{I} - \widehat{\boldsymbol{M}})\boldsymbol{A})^{-1}((\boldsymbol{I} - \widehat{\boldsymbol{M}})\boldsymbol{F} + \boldsymbol{E}). \end{aligned} \tag{5}$$

Here, $\boldsymbol{F}$ in Eq. (5) corresponds to the direct damage calculated in Eq. (4), and the direct damage in Eq. (4) is estimated based on the value-added production function. In the input–output table, estimates are made on a production value basis. Therefore, when $\boldsymbol{F}$ is inserted into Eq. (5), it is necessary to revise it to a production value basis. This revision was calculated using the ratio of the value-added amount and the production amount in the input–output table, and the amount excluding non-household consumption expenditure (accommodation, daily allowance, entertainment expenses, welfare expenses) was estimated as the value-added amount. In addition, because this research focuses on the domestic damage caused by cyberattacks in Japan, we calculated $\boldsymbol{F}$ as the product of the amount of added value by the self-sufficiency rate of each industry, where the self-sufficiency rate is obtained by subtracting the import coefficient from 1. The import coefficient is calculated by dividing the absolute value of "(less) Total imports" by "Total domestic demand" in the input–output table.

Because $\boldsymbol{Y}$ calculated using Eq. (5) includes direct damage, it is necessary to exclude direct damage from spillover damage. Therefore, spillover damage is estimated using Eq. (6):

$$\begin{aligned} &\boldsymbol{Y}\left(\text{spillover damage only}\right) \\ &= \boldsymbol{Y}\left(\text{spillover damage including direct damage}\right) - \boldsymbol{F}\left(\text{direct damage}\right). \end{aligned} \tag{6}$$

3.3.2 Dataset

We used the direct input damage by industry calculated in the 2015 input–output table (37 I/O sections). Based on the integrated major sections in the input–output table for Japan, we divided the industrial sections into 37 I/O sections.

4 Results and discussion

In this study, we showed that it is possible to estimate not only the direct damage caused by cyberattacks, but also spillover damage at the national level using the production function and I/O model.

4.1 Estimated damage for each industrial sector

The estimation results are shown in Tables 3, 4, and 5.

Table 3 shows the direct damage, spillover damage in each of the 37 I/O sectors, and total damage (Japan, FY2015) based on the model in 3-2-1 and 3-3-1, and Table 4 shows the proportion of each industry to the total damage of the whole country.

Table 3 Direct, spillover, and total damages in 37 I/O industrial sectors (Japan)

Aggregated sector classification (37 I/O sectors)		Direct damage				(million yen)	
Code	I/O sector name	[*a*] Direct damage based on value-added	[*b*] Output/value added ratio	[*c*] Direct damage based on production value	[*d*] Direct damage based on domestic products	Spillover Damage [*e*] excluding direct damage	Total damage [*d*] + [*e*]
01	Agriculture, forestry, and fishery	0	2.126503	0	**0**	**53**	**53**
06	Mining	0	2.099589	0	**0**	**10**	**10**
11	Beverages and Foods	32	2.756982	90	**74**	**82**	**156**
15	Textile products	0	2.561870	0	**0**	**23**	**23**
16	Pulp, paper, and wooden products	0	2.944163	0	**0**	**341**	**341**
20	Chemical products	22	3.109826	67	**50**	**177**	**227**
21	Petroleum and coal products	0	3.359303	0	**0**	**166**	**166**
22	Plastic products and rubber products	0	2.739282	0	**0**	**254**	**254**
25	Ceramic, stone, and clay products	0	2.133693	0	**0**	**58**	**58**
26	Iron and steel	0	3.913770	0	**0**	**189**	**189**
27	Non-ferrous metals	0	4.257120	0	**0**	**93**	**93**
28	Metal products	0	2.308869	0	**0**	**125**	**125**
29	General-purpose machinery	0	2.349833	0	**0**	**53**	**53**
30	Production machinery	0	2.240863	0	**0**	**38**	**38**
31	Business oriented machinery	944	2.523802	2382	**1663**	**123**	**1786**
32	Electronic components	0	2.767972	0	**0**	**234**	**234**
33	Electrical machinery	0	2.882688	0	**0**	**54**	**54**
34	Information and communication electronics equipment	0	2.990018	0	**0**	**5**	**5**
35	Transportation equipment	0	4.270088	0	**0**	**154**	**154**
39	Miscellaneous manufacturing products	0	2.241849	0	**0**	**354**	**354**
41	Construction	0	2.231711	0	**0**	**103**	**103**
46	Electricity, gas, and heat supply	18	2.873856	51	**51**	**353**	**403**
47	Water supply	0	2.062349	0	**0**	**60**	**60**
48	Waste management service	0	1.569432	0	**0**	**112**	**112**
51	Commerce	1559	1.481588	2310	**2305**	**589**	**2894**
53	Finance and insurance	2279	1.550069	3532	**3392**	**451**	**3842**
55	Real estate	1	1.194597	1	**1**	**516**	**517**
57	Transport and postal services	12	2.004639	25	**23**	**975**	**998**
59	Information and communications	5137	2.009158	10,322	**9857**	**2700**	**12,556**

Table 3 (continued)

Aggregated sector classification (37 I/O sectors)		Direct damage				(million yen)	
Code	I/O sector name	[*a*] Direct damage based on value-added	[*b*] Output/value added ratio	[*c*] Direct damage based on production value	[*d*] Direct damage based on domestic products	Spillover Damage [*e*] excluding direct damage	Total damage [*d*] + [*e*]
61	Public administration	728	1.433960	1045	**1045**	**27**	**1072**
63	Education and research	13	1.385286	18	**17**	**55**	**73**
64	Medical, health care, and welfare	0	1.641402	0	**0**	**10**	**10**
65	Membership-based associations, n.e.c	0	1.775624	0	**0**	**45**	**45**
66	Business services	0	1.639199	0	**0**	**3492**	**3492**
67	Personal services	161	1.957895	315	**308**	**146**	**454**
68	Office supplies	0	0.000000	0	**0**	**58**	**58**
69	Activities not elsewhere classified	0	2.453457	0	**0**	**110**	**110**
Total		10,907	–	20,158	**18,785**	**12,385**	**31,170**

Source: Created by the authors

The direct damage in Eq. (4) in [*a*] of Table 3 was estimated based on the value-added production function. Then, direct damage based on production value ([*c*] in Table 3) is calculated by using the ratio ([*b*] in Table 3) of the value-added amount and the production amount. Next, because this study focuses on the domestic impact of cyberattacks, $\boldsymbol{F}$ in Eq. (5) is calculated by multiplying the direct damage based on the production value ([*c*] in Table 3) by the self-sufficiency rate of each industry so that $\boldsymbol{F}$ in Eq. (5) is shown as [*d*] of Table 3. Finally, we calculate the spillover damage ([*e*] in Table 3) based on Eqs. (5) and (6).

Table 5 shows the top 5 industries with the highest total losses and that the JIP industry code 59 (Information and communications) suffered damages of approximately 12,556 million yen, accounting for 40.3% of the total damage. The damages caused by industry codes 31 (business-oriented machinery), 51 (semiconductor devices and integrated circuits), 53 (finance and insurance), and 66 (business services) accounted for 5.7%, 9.3%, 12.3%, and 11.2% of the total damage, respectively. The top five industries accounted for 78.8% of the total damage.

4.2 Discussion of estimated damage for all sectors

As shown in Table 3, we estimated damages for all sectors based on the IPA dataset in 3-2-2 A). The direct damage (based on domestic production value), spillover damage, and total amount were approximately JPY 18,785 million, JPY 12,385 million, and JPY 31,170 million, respectively.

Here, we should note that the IPA dataset only showed the lost working hours in IT departments caused by cyberattacks and does not include the lost working hours in other business sections during IT department work for IT system recovery. If the cyberattack incident survey includes lost working hours in other business sections, our model

Table 4 Estimated damages and proportion of damages by 37 I/O sectors

Aggregated sector classification (37 I/O sectors)		Estimated value < Repost > (million yen)			Proportion to total (%)		
		direct damage	Spillover damage	Total	Direct damage	Spillover damage	Total
Code	I/O sector name						
01	Agriculture, forestry, and fishery	0	53	53	0.0	0.4	0.2
06	Mining	0	10	10	0.0	0.1	0.0
11	Beverages and Foods	74	82	156	0.4	0.7	0.5
15	Textile products	0	23	23	0.0	0.2	0.1
16	Pulp, paper, and wooden products	0	341	341	0.0	2.8	1.1
20	Chemical products	50	177	227	0.3	1.4	0.7
21	Petroleum and coal products	0	166	166	0.0	1.3	0.5
22	Plastic products and rubber products	0	254	254	0.0	2.1	0.8
25	Ceramic, stone, and clay products	0	58	58	0.0	0.5	0.2
26	Iron and steel	0	189	189	0.0	1.5	0.6
27	Non-ferrous metals	0	93	93	0.0	0.7	0.3
28	Metal products	0	125	125	0.0	1.0	0.4
29	General-purpose machinery	0	53	53	0.0	0.4	0.2
30	Production machinery	0	38	38	0.0	0.3	0.1
31	Business oriented machinery	1663	123	1786	8.9	1.0	5.7
32	Electronic components	0	234	234	0.0	1.9	0.7
33	Electrical machinery	0	54	54	0.0	0.4	0.2
34	Information and communication electronics equipment	0	5	5	0.0	0.0	0.0
35	Transportation equipment	0	154	154	0.0	1.2	0.5
39	Miscellaneous manufacturing products	0	354	354	0.0	2.9	1.1
41	Construction	0	103	103	0.0	0.8	0.3
46	Electricity, gas, and heat supply	51	353	403	0.3	2.8	1.3
47	Water supply	0	60	60	0.0	0.5	0.2
48	Waste management service	0	112	112	0.0	0.9	0.4
51	Commerce	2305	589	2894	12.3	4.8	9.3
53	Finance and insurance	3392	451	3842	18.1	3.6	12.3
55	Real estate	1	516	517	0.0	4.2	1.7
57	Transport and postal services	23	975	998	0.1	7.9	3.2
59	Information and communications	9857	2700	12,556	52.5	21.8	40.3

Table 4 (continued)

Aggregated sector classification (37 I/O sectors)		Estimated value < Repost > (million yen)			Proportion to total (%)		
		direct damage	Spillover damage	Total	Direct damage	Spillover damage	Total
Code	I/O sector name						
61	Public administration	1045	27	1072	5.6	0.2	3.4
63	Education and research	17	55	73	0.1	0.4	0.2
64	Medical, health care, and welfare	0	10	10	0.0	0.1	0.0
65	Membership-based associations, n.e.c	0	45	45	0.0	0.4	0.1
66	Business services	0	3492	3492	0.0	28.2	11.2
67	Personal services	308	146	454	1.6	1.2	1.5
68	Office supplies	0	58	58	0.0	0.5	0.2
69	Activities not elsewhere classified	0	110	110	0.0	0.9	0.4
Total		18,785	12,385	31,170	100.0	100.0	100.0

Source: Created by the authors

Table 5 Summary of the top 5 I/O sectors

Aggregated sector classification (37 I/O sectors)		Estimated value (million yen)					
		Direct damage		Spillover damage		Total	
Code	Sector name						
31	Business oriented machinery	1663	8.9%	123	1.0%	1786	5.7%
51	commerce	2305	12.3%	589	4.8%	2894	9.3%
53	Finance and Insurance	3392	18.1%	451	3.6%	3842	12.3%
59	Information and communications	9857	52.5%	2,700	21.8%	12,556	40.3%
66	Business services	0	0.0%	3492	28.2%	3492	11.2%
Top 5 total		17,217	91.7%	7355	59.4%	24,570	78.8%
Other than the top 5		1568	8.3%	5030	40.6%	6600	21.2%
Total		18,785	100.0%	12,385	100.0%	31,170	100.0%

Source: Created by the authors

will show a larger ***Lr***, therefore the total damage will be huge. In addition, immeasurable losses, such as the loss of business opportunities and brand damage, may occur in cyber-attack victim companies.

4.3 Other discussion

Table 5 shows that JIP industry code 59 (Information and communications) suffered damages of approximately 12,256 million yen, accounting for 40.3. % of the total damages. While these analyses by industry are useful for cybersecurity and economic policy discussions, it is important to improve the input dataset's quantity and quality for our estimation model. Therefore, we expect to establish a framework for collecting

information on cyber incidents at the national level and for data standardization in Japan, as in the case of the United States.[3]

5 Conclusion

5.1 Conclusion

By presenting a method for analyzing the damage caused by cyberattacks from a macroeconomic perspective and using production functions and input–output tables, this study contributes to future studies on cyber resilience.

This study takes a macroeconomic viewpoint to directly estimate the economic losses from cyberattacks in Japan—the amount of direct and spillover damage. Cyberattack recovery consumed at least IT department working hours in Japan and caused damage worth approximately 31,170 million yen for the financial year 2015.

5.2 Future research

Future studies can improve the accuracy of the aforementioned estimation using data on the working hours required for recovery in each industry. As mentioned above, it is also expected to establish a framework for collecting information on cyber incidents at the national level and standardizing data in Japan.

We plan to study and analyze industrial characteristics in future research more precisely. First, we analyze a specific industry's characteristics by utilizing the information and communications input–output table published by the Ministry of Internal Affairs and Communications. Next, we analyze the forward linkage of the spillover effect in addition to the backward linkage, as in this study.

Appendix 1: Definition of term

The terms used in this study are defined as follows:

For "Cyber attack", Information-technology Promotion Agency, Japan revealed in IPA (2021) that the major organizational threats include damage from ransomware, theft of confidential information by targeted attacks, and telework. The new normal ways of working have exposed organizations to supply chain attacks, financial damage from fraudulent emails, information leakage due to internal fraud and negligence, business suspension due to IT infrastructure failure, unauthorized logins for Internet services, and increased misuse after the renewal of vulnerability countermeasure information.

Regarding the characteristics of cyberattacks, the Ministry of Defense and the Self-Defense Forces presented a list of the characteristics of cyberattacks in a report titled (2012). These characteristics include "attacker superiority", "diversity", "anonymity", "top secret (confidentiality)", and "deterrence difficulty. Therefore, it is difficult to analyze the economic damage caused by these characteristics.

This study excluded indirect damage (damage effects due to rumors on brand value). This study focuses on the following direct and spillover damages caused by cyberattacks on the economy:

[3] The US Department of Land Security (DHS) provides insurance companies with a data collection and analysis platform (Cyber Incident Data and Analysis Repository). This platform helps private modeling companies assess cyber risk and cyber accumulation for modeling. In one of the cases, a data standard format was integrated to the management system (CAMS: Cyber Accumulation Management System) (some public institutions (e.g., FBI) also play a role).

Direct damage (damage to the attacked company/industry) includes a general investigation of the cause, system recovery, data corruption, leakage, damage compensation, system outage, business interruption, and opportunity loss.

Spillover damage (damage to companies/industries directly affected by direct damage) includes general damage to other companies and industries doing business with the directly affected companies and damage from the attacked companies to other companies, industries, and society. Damage to social infrastructure may affect social and economic activities and cause significant losses.

Appendix 2: Previous research: analysis of damage caused by cyberattacks

No.	Source/year of publication/title, etc.	Target countries and regions	Target year	Overview of damage calculation	Damage calculation model	Reference data
1	CSIS (Center for Strategic and International Studies, USA), McAfee (2020) *The Hidden Cost of Cybercrime*	Worldwide	2020	$1 trillion (equivalent to 1% GDP)	Unknown	1500 companies in The Overview
2	RAND Cooperation (2018) *Estimating the Global Cost of Cyber Risk: Methodology and Examples*	63 countries	2017	$800 billion (equivalent to 1.1% GDP)	I/O model	OECD data, financial data, incident data, etc.
3	Cyber Security Ventures (2020) *Cybercrime To Cost The World $10.5 Trillion Annually*	Worldwide	2021	$6 trillion	Undisclosed	Undisclosed
4	Microsoft, et al. (2018) *Cybersecurity Threats to Cost Organizations in Asia Pacific US$1.75 Trillion in Economic Losses*	Asia Pacific	2017	$1.745 trillion (equivalent to 7% GDP)	Self-made model	Overview, economic data
5	Accenture (2019) *The Cost of Cybercrime*	11 countries	2018	$13 million per company on average	Self-made model	2600 people from 355 companies from interviews
6	JNSA (NPO Japan Network Security Association) (2019) *Report on Information Security Incidents*	Japan	2018	640 million yen per company and 268.4 billion yen for Japan as a whole	JO model (Self-made model)	Public information
7	Trend Micro (2020) *Corporate Security Trends in 2020*	Japan	2018	Average 210 million yen per company	Unknown	1086 companies from the interview
8	RISI (Repository of Industrial Security Incidents: operated by Security Incidents Organization, a U.S. non-profit organization)	United States	28 years	6% of cases exceed $10 million	Unknown	Unknown
9	Ponemon Institute (2015) *2015Cost of Cyber Crime Study: United States(Cyber Crime)*	8 countries	2015	$15 million per company	Unknown	58 U.S. companies, 553 companies in 7 other countries

No.	Source/year of publication/title, etc.	Target countries and regions	Target year	Overview of damage calculation	Damage calculation model	Reference data
10	Ponemon Institute (2015)*2015 Cost of Data Breach Study: Global Analysis(Cyber Impact)*	11 countries	2015	$3.79 million per company ($154 per record)	Self-made model	1500 companies in the overview
11	McAfee(2013)*The Economic Impact of Cybercrime and cyber-Espionage*	Worldwide, USA	2013	Worldwide: $0.3 trillion to $1, U.S. $0.024-$0.12 trillion	Unknown	Unknown
12	AFCEA (armed forces communications and electronic association military communications and electronics association)	–	–	(Unpublished)	(Unpublished)	(Unpublished)
13	Mitsubishi Research Institute, and Ministry of Economy, Trade, and Industry, (2007) *Evaluation of damage to corporate value due to cybersecurity accident (MRI/ The University of Tokyo)*	Japan	2007	(Mitsubishi Research institute's expected amount of damage is 1.1 billion yen, etc.)	CAR (Cumulative. Abnormal Return) analysis model	Stock market information

Created by the authors based on published materials of the Ministry of Internal Affairs and Communications

Abbreviations

CSIS The Center for Strategic and International Studies (USA)
IPA Information-technology Promotion Agency (Japan)
JNSA The Japan Network Security Association (Japan)
JIP The Japan Industrial Productivity

Acknowledgements
Not applicable.

Author contributions
AG designed the study, and AK performed the calculations. AK interpreted the results and drafted the manuscript. AK revised the manuscript and created the figures. Both authors read and approved the final manuscript.

Funding
Not applicable.

Availability of data and materials
The data for output (***Y***), capital stock (***K***), and labor (***L***) are available from the JIP database: [hyperlink to dataset(s)/data source, e.g., "https://www.rieti.go.jp/jp/database/JIP2015/index.html"]. The data for number of working hours (***Lr***) allocated for system recovery or data recovery after a cyberattack are available from IPA: [hyperlink to dataset(s)/data source, e.g., "https://www.ipa.go.jp/security/fy26/reports/isec-survey/index.html"], and JSNA. Although the JNSA data are not open to the public, they were individually requested and obtained for this research and are available if requested individually. The data for the number of companies are available from the 2015 Economic Census: [hyperlink to dataset(s)/data source, e.g., "https://www.stat.go.jp/data/e-census/2016/kekka/gaiyo.html"]. The Japanese benchmark input–output table is available from the Ministry of Internal Affairs and Communication: [hyperlink to dataset(s)/data source, e.g., "https://www.e-stat.go.jp/stat-search/files?page=1&layout=datalist&toukei=00200603&tstat=000001130583&cycle=0&year=20150&month=0"].

Declarations

Ethics approval and consent to participate
This research does not involve human subjects, human material, or human data.

Competing interests
The authors declare that they have no competing interests.

Received: 6 May 2022 Revised: 4 November 2022 Accepted: 5 November 2022
Published online: 28 December 2022

References

CO (Cabinet Office) (2013) Assumption of damage from the Nankai Trough earthquake (Points of the second report—Damage and economic damage of facilities, 2013.https://www.bousai.go.jp/jishin/nankai/taisaku_wg/pdf/20130318_kisha.pdf. Accessed 20 Mar 2022.

CS (Cybersecurity Strategy,The Government of Japan) (2021) Cybersecurity for All, Sept 2021. https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-en-booklet.pdf. Accessed 18 Sept 2022.

CSIS (Center for Strategic and International Studies) (2021) The hidden costs of cybercrime, 2021. https://www.csis.org/analysis/hidden-costs-cybercrime. Accessed 20 Mar 2022.

IPA (Information Technology Promotion Agency) (2014) Investigation of damage caused by information security events, 2014 (in Japanese). https://www.ipa.go.jp/security/fy26/reports/isec-survey/index.html. Accessed 20 Mar 2022.

IPA(Information Technology Promotion Agency) (2021) Information Security 10 major Threats 2021. (in Japanese) https://www.ipa.go.jp/security/vuln/10threats2021.html. Accessed 20 Mar 2022.

JNSA (Japan Network Security Association) (2018) Survey results on information security incidents—Leakage of personal information, 2018, Available via JNSA (in Japanese) .https://www.jnsa.org/result/incident/2018.html. Accessed 20 Mar 2022.

MIC (Ministry of Internal Affairs and Communications) (2019) White paper on information and communications, section 3 Economic losses such as cyberattacks, 2019 (in Japanese). https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r01/html/nd113320.html. Accessed 20 Mar 2022

Shimoda M, Fujikawa K (2012) Industrial relation analysis model and supply constraints caused by the great East Japan Earthquake. Input–output Anal 20:133–146. https://doi.org/10.11107/papaios.20.133 (**in Japanese**)

Tanaka H (2013) *Report of the Committee on Information Security Damage and Countermeasures—Construction of a new model of threats and damage in companies,* Research Group on Information Security Damage and Countermeasures, IPA, 2013 (in Japanese). (This material is old and not currently available, but we have owned this manuscript.)

Tanaka H, Takemura T, Iitaka Y, Hanamura K, Komatsu A (2014) Research on estimation of economic loss due to information security incidents. J Econ Policy Stud 11:59–62 (**in Japanese**)

Publisher's Note