https://doi.org/10.3311/PPso.22150



Periodica Polytechnica Social and Management Sciences

# The Economic Measurement of Cyber Incidents

Tamás Szádeczky[1,2*], Zsolt Bederna[1]

[1] Department of Management and Business Economics, Faculty of Economic and Social Sciences, Budapest University of Technology and Economics, H-1111 Budapest, Műegyetem rkp. 3., Hungary
[2] Czech CyberCrime Centre of Excellence C4e, Masaryk University, Zerotinovo nam. 9., 601 77 Brno, Czech Republic
[*] Corresponding author, e-mail: szadeczky.tamas@gtk.bme.hu

Received: 05 March 2023, Accepted: 05 July 2023, Published online: 08 September 2023

**Abstract**

In recent decades, Information and Communication Technologies (ICT) have significantly evolved, further establishing the information society. However, ICT systems are subject to security incidents, and most malicious attacks have cascading effects. Decision-makers need to understand the potential financial effects of incidents if they wish to clearly perceive the potential risks and thus make an appropriate allocation of resources to ICT security.

Our research attempts to develop a comprehensive toolset for the analysis of cybersecurity incidents. The toolset is based on conventional methodologies of cash-flow evaluation and balance of payments. We discuss several use cases of real-world examples with incidents affecting essential service providers and manufacturers. The case studies involve incidents affecting energy service providers, banks, water utilities, aircraft manufacturers, car manufacturers, IT software providers, air, rail, and water transport companies, the pharmacy, and the health sector. Analysis of the incidents involves our framework being applied at three levels: organisational, governmental, and international.

**Keywords**

cybersecurity, cash-flow analysis, risk management

## 1 Introduction

The technological advancements of Information and Communication Technologies (ICT) have significantly evolved in recent decades, further establishing an information society, creating cyberspace, which, according to Kuehl (2009:p.28), is "a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interdependent and interconnected networks using information-communication technologies", comprising information technology (IT) and operational technology (OT). IT is widely applied where ICT supports business processes, including processing data. At the same time, OT services are the basis for technological processes, such as manufacturing or streaming. OT highly benefits from the concept of Industry 4.0 (Lydon, 2019), aiming to make ICTs build smart cities, smart factories and manufacturing with intelligent productions based on the Internet of Things (IoT) and traditional manufacturing automation, fostering a paradigm shift from automated manufacturing toward intelligent manufacturing (Roblek et al., 2016). The role of ICT systems in critical infrastructures (CIs) is inevitable. An industrial control system (ICS) can be used in many processes like water treatment plants, management of water, fertilisers and agrochemicals, chemical plants, sewage treatment plants, mines and metals, power plants and boiler controls, automobile manufacture, metallurgical plants, paper and pulp mills, control of quality, refineries and petrochemicals (oil), food processing, and pharmaceutical manufacturing (Kumar et al., 2019). Moreover, other kinds of business services and processes are deeply dependent on traditional IT systems.

However, the higher the dependence on ICT, the higher the information value it processes, and the more serious the cash-flow-related financial and non-financial effects that may be caused by an incident (Na et al., 2019). Successful cyberattacks could paralyse internal processes, cause financial losses, and cause severe impact not only to organisations but also to individuals, alongside which societal-level problems may arise. The extent of their impact on an organisation depends on the business processes and activities and the processed data affected due to the

**Cite this article as:** Szádeczky, T., Bederna, Z. (2023) "The Economic Measurement of Cyber Incidents", Periodica Polytechnica Social and Management Sciences. https://doi.org/10.3311/PPso.22150

targeted system(s). Another problem could arise from the fact that incidents' technical effects and their business-related effects do not have to come about at the same time. For example, an incident that occurs at the time of $t = 1$ is recognised at $t = 2$ having effects on the organisation's operation, causing fiscal impact at $t = 4$.

These various effects need a comprehensive framework for analysing those effects resulting at organisational level and its surroundings. Based on our defined framework, this paper analyses the cases of Airbus, Kojima, and SolarWinds. Furthermore, we analyse the WannaCry ransomware attack on Bristol Airport, Deutsche Bahn, and the National Health Service and the involvement of Maersk and Merck in the NotPetya ransomware attack.

## 2 Methodology development

For businesses, cash flows (CFs) are one of the bases of their financial functions (Oral and CenkAkkaya, 2015), representing an amount of cash or cash equivalent that the company receives or gives out. One calculates cash flows by subtracting the opening balance at the beginning of a period from the closing balance, which can be assessed monthly, quarterly, or yearly. Naturally, the cash flow is positive if the balance is also positive, meaning that the inflow amount is greater than the outflow amount. On the other hand, the cash flow is negative if the outflow amount is higher than the inflow. Cash flow can be determined for the whole business, a business function, a project, or even a change. Contrary, negative cash flows can cause liquidity problems, preventing the organisation from meeting its financial obligations as they become due. Thus, the greater the granularity with which the cash flow is determined, the more precise the liquidity analysis can be.

The net present value (NPV) (Žižlavský, 2014) applies to a series of cash flows occurring at different times, determining the present value of a cash flow that depends on the interval between now and the cash flow and the discount rate. NPV calculation is one of the essential tools in the financial world for investment calculations, evaluating and comparing capital projects or financial products with cash flows spread over time. It is also excellent for the analysis of security investments (Brotby, 2009) and events. NFV is widely applied, on the other hand, it gives the present value of later CFs. Conversely, a later value of a series of future values is determined based on the net future value (NFV). Assuming yearly based cash flows that arise in the end of the given year, we apply the following formula for NFV calculation:

$$\mathrm{NFV} = \sum_{t=1}^{n-1}\left(\mathrm{CF}_t \times \prod_{i=t}^{n-1}\left(1+r_{i+1}\right)\right) + \mathrm{CF}_n. \tag{1}$$

In the following, we denote NFV of an incident as $\mathrm{NFV}_I$.

Within cash flows, corporate ($A$), shareholders' ($E$), and creditors' ($D$) value each make a simultaneous difference, making it necessary to distinguish these aspects when examining financial effects with a view to calculating the interest based on the cost of capital. There are several options whereby one may calculate the shareholders' cost of capital, among which the Capital Asset Pricing Model (CAPM) (Sharpe, 1964) is a widely applied formula which operates as follows: where $r_E$ represents the return on an individual share, $r_f$ is the risk-free interest rate, and $r_M$ is the market interest rate, and lastly, $\beta$ (beta) measures the volatility of an individual stock compared to the systematic risk of the entire market:

$$r_E = r_f + \beta\left(r_M - r_f\right). \tag{2}$$

In Eq. (2), $\beta\,(r_M - r_{f,nom})$ represents the risk premium that investors expect from owning a specific stock or portfolio above the return on risk-free assets. At the same time, a company without being publicly traded poses a higher risk to its owners, which is represented by total beta (Damodaran, 2012) given by the following formula, where $\beta_T$ is the total beta, $\beta_M$ market portfolio beta, $p_{jM}$ is the correlation between the stock and the market portfolio:

$$\beta_T = \beta_M \times p_{jM}. \tag{3}$$

From a financing perspective, an organisation may apply for debt in addition to equity. For an unleveraged company, the corporate interest rate must be calculated without any debt, but if a company is leveraged, the weighted-average cost of capital (WACC) must be considered (Fernández, 2010), where $r_{\mathrm{WACC}}$ is the WACC interest rate, $E(\cdot)$ is the expected value, $E$ is the equity, $D$ is the debt, $r_E$ is the equity interest rate, $r_D$ is the debt interest rate, and $t_c$ is the corporate tax:

$$r_{\mathrm{WACC}} = \frac{E}{E+D} \times E\left(r_E\right) + \left(1-t_c\right) \times \frac{D}{E+D} \times E\left(r_D\right). \tag{4}$$

In the later use cases, we assume leveraged companies and, therefore, apply consequently WACC with total beta provided by (Damodaran, 2022a; 2022b).

However, for financial analysis, cash flows must be properly established, consisting of Eq. (1) direct costs, such as replacement of devices, missed revenues, and extra costs,

and Eq. (2) indirect costs, such as fines and reputational damages, causing a decreased level of orders or left customers. Table 1 illustrates a simple breakdown of multiple years, separating the remaining income and the arising operational costs (operating costs – OPEX) and capital costs (capital expenditure – CAPEX) categories.

The proper determination of incidents' effects requires the application of income and expense categories according to accounting rules, so for example, when evaluating cash flows from insurance income, the accounting may differ based "*on a variety of factors, including the nature of the claim, the amount of proceeds (or anticipated proceeds) and the timing of the loss and corresponding insurance recovery*" (EY, 2017:p.5). In terms of OPEX categories, there may be additional costs of responding to the event, fines, compensation, additional costs for public communication and lobbying. In terms of CAPEX, depreciation of broken equipment, as well as full write-off and reinvestment costs may be incurred.

Moreover, incidents can affect an organisation and indirectly hit its suppliers and customers, potentially influencing even competitors and the government multiple times. Each indirectly affected entity of the chain has an NFV depicted in Table 2.

Taking the multiple NFVs into consideration, theoretically, the overall cash flow, i.e., the aggregated effect denoted as $\mathrm{NFV}_{Sum,I}$, is calculated according to the following equation, taking all $E$ entities that are members of the set of the affected entities:

$$\mathrm{NFV}_{Sum,I} = \sum\nolimits_{E}\left(\mathrm{NFV}_{I} \mid \forall E \in \left(\text{affected entities}\right)\right). \tag{5}$$

## 3 Case study: banking service – Tesco Bank

On 06 November 2016, British newspapers, including BBC reported (BBC, 2016) that Tesco Bank, providing retail banking and insurance services in the United Kingdom as part of Tesco PLC (2017), was hit by a cyberattack in which customers lost different amounts of money from their accounts. The next day, the bank suspended online transactions and made a statement that up to 40,000 customers had been affected. Initially, the bank's shares in the retail group fell 3% on the news but the extent of those losses reduced to around 1.1% by the middle of the day (Botter, 2016).

**Table 1** Incident's NFV calculation

| | $t = 1$ | $t = 2$ | $t = n$ |
|---|---|---|---|
| Income modifying items | | | |
| OPEX increasing items | | | |
| CAPEX increasing items | | | |
| Yearly cash flows of the incident | $\mathrm{CF}_1$ | $\mathrm{CF}_2$ | $\mathrm{CF}_n$ |
| $r$ | $r_1$ | $r_2$ | $r_n$ |
| $\mathrm{NFV}_I$ | | | |

**Table 2** Conceptualised microeconomic incident's effects

| | Organization | Supplier | Customer | Insurer | Government |
|---|---|---|---|---|---|
| Income modifying items | | | | | |
| OPEX increasing items | | | | | |
| CAPEX increasing items | | | | | |
| $\mathrm{NFV}_{Sum,I}$ | $\mathrm{NFV}_I$ | $\mathrm{NFV}_I$ | $\mathrm{NFV}_I$ | $\mathrm{NFV}_I$ | $\mathrm{NFV}_I$ |

In fact, 8,261 personal current accounts at Tesco Bank were compromised. Attackers obtained customers' debit card details and made thousands of unauthorised transactions, stealing £2.26 million ($2.5) from bank accounts. The rest of the customers suffered from the unavailability of the online banking interface as the IT staff shut it down as a measure (Kumar, 2016). Although the Bank subsequently refunded all customers with compromised accounts by the end of Tuesday, 08 November, some customers were heavily affected, e.g., they were unable to pay for food (Kumar, 2016). Hence, there might have been organisations which were indirectly affected by the temporary liquidity problem experienced by the Bank's customers.

The National Crime Agency (NCA), the Information Commissioner's Office (ICO), and the National Cyber Security Centre (NCSC) were working closely with the Bank to investigate the incident. Furthermore, Tesco Bank promised to issue new cards to affected customers within ten days. Two years later, on 01 October 2018, the Financial Conduct Authority (FCA) (2018) fined Tesco Bank £16.4 million (appr. $21.4 million) in connection with the cyberattack.

Table 3 summarises the exact point in time and the possible effects of the incident. Table 4 displays the cash flows and NFV from Tesco Bank's perspective. At the end of 2018, the negative cash flows regarding the incident through the years were worth $\mathrm{NFV}_{I,A}^{2018} = -\$24{,}1011$ million. As for the international account, no transactions were highlighted, although there could in theory have been a few, at least temporarily.

## 4 Case study: IT supplier

In 2020, an ICT-related advanced attack was revealed against SolarWinds (Wolpoff, 2020) that has seriously

**Table 3** Effects of the incident (Tesco Bank)

| | Tesco Bank | 8,261 customers | UK government |
|---|---|---|---|
| OPEX | | | |
| Extra costs for responding the incident | Unknown (includes issuing new cards) | Temporal liquidity problem | |
| Fine | −$21.4 (2018) | | +$21.4 (2018) |
| Extra costs of investigations | Probable | | Unknown amount |
| Indemnities | −$2.5 (2016) | +$2.5 (2016) | |

**Table 4** Calculating NFV for the incident from Tesco Bank's perspective (million)

| | 2016 | 2017 | 2018 |
|---|---|---|---|
| Overall cash flow discounted to the end of year | −$2.5001 | – | −$21.4023 |
| $r^{a}_{WACC}$ | 3.86% | 3.94% | 4.29% |
| $NFV^{2018}_{I,A}$ | −$24,1011 | – | – |

[a] Based on (Damodaran, 2022a, pt. Costs of Capital by Industry Sector, Europe, Banks (Regional))

affected its customers via its so-called Orion IT network management tool. Threat actors gained unauthorised access to the SolarWinds network in September 2019 (Oladimeji and Kerner, 2023). In October 2019, they tested the code injection process into the Orion codebase, and on 20 February 2020, the malicious code, also known as Sunburst, was injected into Orion, which started to be sent to customers on 26 March 2020. The affected versions of SolarWinds Orion versions are April 2019 through 01 February 2020 HF1.

SolarWinds had that time, 33,000 Orion customers around the world, from which around 18,000 SolarWinds customers installed the malicious updates (SolarWinds, 2020).

In the United States, affected entities comprise:

1. public entities such as the Pentagon, the Department of Homeland Security, the State Department, the Department of Energy, the National Nuclear Security Administration, and the Treasury in the United States;
2. private entities that include tech giants as FireEye, Microsoft, Cisco, Intel, Nvidia, and VMware and other entities as Deloitte;
3. other organisations like the California Department of State Hospitals, and Kent State University (Jibilian and Canales, 2021).

Up to 12 January 2021, approximately 40 companies were targeted and compromised. 80% of the identified victims were from the United States, and the remaining 20% were spread over seven other countries, including Canada, Mexico, Belgium, Spain, the United Kingdom, Israel, and the United Arab Emirates, according to BitSight's report (Shah, 2021). However, there could be unidentified other entities worldwide, including OESs, and DSPs in the European Union, who suffered from this attack indirectly. Furthermore, how deeply SolarWinds' customers were affected in what may have been a chain-like effect is not easy to gauge.

According to SolarWinds' financial reports, the company spent $3.5 million in December 2020 alone (SolarWinds, 2021a). In the first nine months of 2021, the Orion breach cost SolarWinds $40 million, the company's quarterly report (SolarWinds, 2021b), which may be recoverable somewhen in the future recovery under cybersecurity insurance coverage of $15 million. In January 2021, some experts (Ratnam, 2021) estimated US businesses and government agencies, i.e., $NPV^{\text{United States}}_{Sum,I}$, spending upward of $100 billion over many months to contain and fix the damage.

Table 5 summarises the yearly costs and conceptualises possible effects of the incident, while Table 6 calculates the NFV of SolarWinds' known costs.

## 5 Case study: Car manufacturing – Kojima

Toyota's operations in Japan encompass a supply chain of 60,000 companies across four tiers (Hope, 2022), out of which Kojima Industries is one of the top-tier suppliers to Toyota with plastics and electronic components and a second-tier supplier of others, including Hino and Daihatsu Motors.

**Table 5** Effects of the incident (SolarWinds)

| | SolarWinds | SolarWinds' customers | US government |
|---|---|---|---|
| OPEX | | | |
| Extra costs for responding and investigation | $3.5 million (2020)<br>$40 million (2021) | No data is available | No data is available |

**Table 6** Calculating NFV for the incident from SolarWinds's perspective (million)

| | 2020 | 2021 |
|---|---|---|
| Overall cash flow discounted to the end of year | −$3.5 | −$40,0062 |
| $r_{WACC}$ | 9.7%[a] | 6.15%[b] |
| $NFV^{2021}_{I,A}$ | −$43,846 | |

[a] Based on the Costs of Capital by Industry Sector, US, Software (System & Application) given by (Damodaran, 2022a)
[b] Based on the Costs of Capital by Industry Sector, US, Software (System & Application) given by (Damodaran, 2022b)

On Saturday, 26 February 2022, the systems of Kojima Industries were attacked with ransomware. Due to the incident, Kojima's production halted, which seriously affected Toyota because of its just-in-time approach. Toyota suspended its operations on all 28 lines at 14 domestic plants in Japan on Tuesday, 01 March 2022, making shares finish flat on that day, underperforming a 1.2% gain in the broader market. Toyota resumed its operations from the first shift on Wednesday, 02 March; however, the supply-chain problem may have reduced production by 5% of its nationwide monthly output or 13,000 units.

Furthermore, at least part of those cars would have been exported, meaning that the Japanese government missed the export tariffs, while other governments also missed the import tariffs. Moreover, the distributors could make fewer deals, and at the end of the chain, the new-car buyers also had to deal with the problems. This incident may therefore have affected exchange rates and several other international accounts. Table 7 summarises the possible effects of the incident from Kijoma's perspective, so the domino effects on Toyota's distributors and would-be car buyers are not shown.

## 6 Case study: WannaCry ransomware attack

### 6.1 Campaign description

In 2017, WannaCry ransomware hit several actors operating in various sectors as it spread (ENISA, 2017), forming a common cause-effect, propagated as a worm that used EternalBlue, an exploit leaked from the National Security Agency (NSA) targeting a zero-day vulnerability (Akbanov et al., 2019). The initial attack happened in May 2017 and is estimated to have hit more than 200,000 devices in as many as 150 countries (Gillis and Rosencrance, 2021), including systems in Bristol airport, Deutsche Bahn, and the National Health Services of England and Scotland, which are shortly discussed in Sections 6.2 to 6.4, and several more entities as FedEx, University of Montreal, and the Spanish Telefónica, etc. WannaCry encrypted files on the hard drives of Windows devices, demanding a ransom payment of between $300 to $600 in bitcoin. However, only a partial set of victims received decryption keys, forcing them to suffer from downtime and recovery processes. At that time, Symantec (which now acts as part of Broadcom) estimated the total costs at $4 billion, while others estimated $8 billion (Barlyn, 2017).

**Table 7** Effects of the incident (Kojima)

| | Kojima | Toyota | Japanese government |
|---|---|---|---|
| OPEX | | | |
| Extra costs for responding to the incident | Probable | | Unknown |
| Extra costs of investigations | Probable | | Unknown |
| Fewer orders | Probable | −5% of the monthly plan | Fewer tax incomes |

### 6.2 Air transport service – Bristol Airport

The Bristol airport should have recovered its information screens. During the two days of downtime, informing passengers about departing flights and gates were done on paper-based notes. Other systems of the airport, including critical ones, were fortunately not halted. Unfortunately, only a little information is available publicly, so we can only infer the possibilities for the extra costs for responding and investigation.

### 6.3 Rail transport service – Deutsche Bahn

The Deutsche Bahn was hit not only on passenger information display systems on approximately four hundred seventy railway stations for several hours in the middle of the weekend traffic, but ticket automats did not work, too. Beyond the supporting systems, the rail transport systems were not affected. In the case of Deutsche Bahn effects, a similar assumption can be made with the extra of fewer orders due to the missed ticket selling.

### 6.4 Health sector service – National Health Service

The National Health Service (NHS) had already officially published the WannaCry infection on the afternoon of 12 May 2017, which made ICT unavailable for days resulting in delayed planned operations and rerouted emergency treatment to unaffected hospitals (National Audit Office, 2018). Five hospitals had to close their emergency departments (EDs); therefore, patients and emergency ambulances had to travel further to other hospitals. Overall, the widespread incident resulted in a 6% decrease in admissions in the infected hospitals. Furthermore, 13,500 appointments, including at least 139 patients with potential cancer seeking urgent clinics, were cancelled at outpatient treatment across the infected hospitals during the infection week. The financial impact of the attack was also calculated, and the value of the reduction in the activity in the infected trusts amounted to £5.9m (Ghafur et al., 2019), which is an intra-year virtual cash flow.

## 7 Case study: NotPetya ransomware attack

### 7.1 Campaign description

The NotPetya campaign started on 27 June 2017, the day before the celebration of the Ukrainian Constitution. The first infections happened via the Intellect Service's MEDoc application software update mechanism, which was an officially approved tax return program serving Ukrainian companies. The malware's characteristics had similarities to the well-known Petya ransomware, but it was intentional camouflage, hence the name NotPetya, belonging to the disruptionware (Brichant and Eftekhari, 2019) malware category. In Ukraine, thousands of companies were hit, including critical infrastructures, such as banks, Kyiv Borispol Airport, and energy companies, such as Kyivenergo and Ukrenergo. However, as collateral damages, several entities were also hit in other countries, including Germany, France, Italy, Poland, and the United States (Krasznay, 2020), from Sections 7.2 and 7.3 discuss the Danish Maersk's and the US Merck's case studies.

Only on 04 July 2017, Ukraine's cybercrime unit seized the Intellect Service's servers, advising MEDoc users to stop using the software. There was evidence of the Russian presence, and the company could be found criminally responsible for enabling the attack because of its negligence in maintaining the security of its IT infrastructure (Hern, 2017).

It was initially estimated that NotPetya caused between $4 billion and $8 billion costs in the global economy (Greenburg, 2018), but it can easily have been $10+ billion. However, there were political-level consequences, too, as "[…] in February 2018, seven governments – Australia, Estonia, Denmark, Lithuania, Ukraine, the United Kingdom, and the United States – each issued respective statements formally attributing the attack to Russia and the Russian military, which was officially supported by New Zealand, Norway, Latvia, Sweden, and Finland" (Krasznay, 2020:p.489).

### 7.2 Transport service – Maersk

Maersk, as the leading shipping company by volume in that time, got NotPetya via its office located in Odesa, Ukraine (Greenburg, 2018). As the result of the infection, which propagated in 7 minutes across the whole company, the effect was devastating as 49,000 laptops, 3,500 out of 6,200 servers, all print capability, file shares, and Enterprise Service Bus were destroyed; furthermore, IT services such as DHCP and Active Directory were badly damaged, vCenter managing cloud services were damaged and unstable, and all the 1,200 applications were inaccessible from which approximately 1,000 were destroyed. Although data was preserved through the backup, applications couldn't be restored from the backup as they would immediately have been re-infected. Deloitte assisted in cyber forensics to understand how the malware worked. After four-nine days, Maersk rebuilt 2,000 laptops and the Active Directory and enabled core business processes and systems. After two weeks, all global applications were restored, and after four weeks, all laptops were rebuilt (Pownall, 2019; van Hees, 2020).

NotPetya reached Maersk when it had decreased profitability and pressure to consolidate its activities. The incidents cost $300–350 million, taking part in a −$1.9 billion operating loss in 2017. Furthermore, as a delayed effect, a −27% change in market capitalisation occurred one year after the incident happened (Pownall, 2019), as several customers bought services from Maersk's competitors, denoted in Table 8.

### 7.3 Pharmacy – Merck

The US-based pharmaceutical giant Merck also suffered from NotPetya as its systems got infected via its office in Ukraine. The incident affected 30,000 computers and caused a disruption in its worldwide operations, including manufacturing, research, and sales operations (Sagonowsky, 2019). However, Merck first said it was confident in being able to maintain a continuous supply of its top-selling and life-saving drugs. Still, it warned of temporary delays in delivering some other products, which it did not identify (Erman and Finkle, 2017). On the other hand, as a vaccine plant went down, making the company borrowed nine doses of Gardasil from the US strategic stockpile to fulfil its orders (Sagonowsky, 2019).

According to Merck's 2018 annual report (Merck, 2019), the company was unable to fulfil orders for certain products in certain markets, which had an unfavourable effect on sales (which amounted to approximately $260 million in 2017). Manufacturing-related expenses, which were primarily unfavourable manufacturing variances relating to cost of sales and expenses related to remediation efforts in selling, general and administrative expenses, and research and development expenses, altogether amounted to

**Table 8** Effects of the incident (Maersk)

| | Maersk | Maersk's customers | Maersk's competitors | Danish government |
|---|---|---|---|---|
| OPEX | −$300–350 million (2017) | Possibly | More orders | Unknown |

$285 million in 2017. Even in 2018, sales were unfavourably affected by approximately $150 million. However, approximately $45 million was recoverable via insurance payments in 2017. Although Merck suffered from the incident with far more financial expenses, insurers said the damages were excluded from policies as the cyberattack was an act of war (Sagonowsky, 2019). In response, Merck has sued the insurer because, at the time, the company had a $1.75 billion insurance policy covering software-related data loss events, too. On 06 December 2021, the New Jersey Superior Court granted partial summary judgment in favour of Merck, declaring that the War or Hostile Acts exclusion was inapplicable to the dispute (Merck & Co. Inc. v. ACE American Ins. Co., 2022), covering $1.4 billion.

Table 9 summarises the discussed financial effects of the incident and makes further assumptions. Table 10 presents (or at least attempts to present) two NFV values of related cash flows as still there are uncertain cash flows.

## 8 Conclusion

We shortly reviewed information and communication technology systems' elements. Those systems, however, are aimed to be compromised by threat actors due to several reasons deriving from human motives, causing confidentiality, integrity, or availability-related security incidents. Depending on an attack's sophistication and objectives, a common cause, cascading, or escalating effects may arise, deepening the problems for non-ICT organizations and companies and, at the end of the chain, for citizens. These problems can also have environmental and economic effects, despite the most direct affect being felt by an organisation. We outlined an appropriate method, analysing financial effects that we tested on a few incidents.

As for IT-related incidents, we reviewed Tesco Bank, SolarWinds, and Airbus incidents. Even if a bank refunds all its customers, it could cause a temporal liquidity problem, at least for a partial set of those customers. As a severe supply-chain attack, the compromised SolarWinds Orion platform resulted in further cyberattacks. However, threat actors probably stole confidential information from the Airbus aircraft manufacturer. On the other hand, the OT-related incidents show that they could easily cause severe hazards and threaten life if the water supplier or air or rail transport providers did not respond appropriately, not to speak about the pharmacy company and the health service provider.

The SolarWinds incident could have affected thousands of customers, but threat actors, with other than financial motives, targeted "only" a few of them as knowing; however, there could be unknown cases. Regarding the financial effects, various operation costs, such as loss of effective and expected sales, and extra costs of response and investigation, can emerge. Sweeping cyberattacks, like WannaCry and NotPetya were, have a devastating aggregated financial effect as several individual effects aggregate.

**Table 9** Effects of the incident (Merck)

| | Merck | Insurer | US government |
|---|---|---|---|
| Income | | | |
| Unfavourable effect on sales | -$260 million (2017)<br>-$150 million (2018) | | Missing tax income |
| OPEX | | | |
| Selling, general and administrative expenses, and research and development expenses | -$285 million (2017) | | Missing tax income |
| Insurance | +$45 million (2017)<br>+$1.4 billion (?) | -$45 million (2017)<br>-$1.4 billion (?) | Court fees |

**Table 10** Calculating NFV for the incident from Merck's perspective (million)

| | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 |
|---|---|---|---|---|---|---|
| Overall cash flow discounted to the end of year | -$500 | -$150 | – | – | – | – |
| $r_{WACC}$ | 9.7%[a] | 6.15%[a] | 8.51%[a] | 4.75%[a] | 5.63%[b] | N/A |
| $NFV_{I,A}^{2018}$ | | | -$690.65 | | | |
| $NFV_{I,A}^{2021}$ | | | -$916.2037 | | | |

[a] Based on Costs of Capital by Industry Sector, US, Drugs (Pharmaceutical) given by Damodaran (2022a)
[b] Based on Costs of Capital by Industry Sector, US, Drugs (Pharmaceutical) given by Damodaran (2022b)

**Acknowledgement**

The article was financed in the cooperation of the National Bank of Hungary and Budapest University of Technology and Economics under the Digital Research Project in the period of 2021-2022 and the Hungarian Academy of Sciences Bolyai János Research Scholarship.

This work was supported by ERDF project "Cyber-Security, CyberCrime and Critical Information Infrastructures Center of Excellence" (No. CZ.02.1.01/0.0/0.0/16_019/0000822).

**References**

Akbanov, M., Vassilakis, V. G., Logothetis, M. D. (2019) "WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms", Journal of Telecommunications and Information Technology, 1, pp. 113–124. https://doi.org/10.26636/jtit.2019.130218

Barlyn, S. (2017) "Global cyber attack could spur $53 billion in losses: Lloyd's of London", Reuters, July 17. [online] Available at: https://www.reuters.com/article/us-cyber-lloyds-report/global-cyber-attack-could-spur-53-billion-in-losses-lloyds-of-london-idUSKBN1A20AB [Accessed: 16 June 2022]

BBC (2016) "Tesco Bank attack: What do we know?", BBC, Nov. 07. [online] Available at: https://www.bbc.com/news/technology-37896273 [Accessed: 08 February 2023]

Botter, L. (2016) "Tesco Shares Fall After Cyber Attack at its Online Banking Group Hits 40,000 Customers: The grocer's banking subsidiary freezes online current accounts after deposits are plundered", The Street, Nov. 07. [online] Available at: https://www.thestreet.com/investing/tesco-shares-drop-on-bank-hack-13882530 [Accessed: 25 April 2022]

Brichant, R., Eftekhari, P. (2019) "The rise of disruptionware", [pdf] Institute for Critical Infrastructure Technology (ICIT). Available at: https://icitech.org/wp-content/uploads/2019/09/ICIT-Brief-The-Rise-of-Disruptionware.pdf [Accessed: 29 September 2019]

Brotby, W. K. (2009) "Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement", Auerbach Publications. ISBN 9781420052855

Damodaran, A. (2012) "Investment Valuation: Tools and Techniques for Determining the Value of Any Asset", John Wiley & Sons. ISBN 978-1-118-01152-2

Damodaran, A. (2022a) "Data:Archives, Discount Rate Estimation", [online] Available at: https://pages.stern.nyu.edu/~adamodar/New_Home_Page/dataarchived.html#discrate [Accessed: 06 December 2022]

Damodaran, A. (2022b) "Data:Current, Discount Rate Estimation", [online] Available at: https://pages.stern.nyu.edu/~adamodar/New_Home_Page/datacurrent.html [Accessed: 06 December 2022]

ENISA (2017) "WannaCry Ransomware Outburst", ENISA, May. [online] Available at: https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst [Accessed: 10 March 2019]

Erman, M., Finkle, J. (2017) "Merck says cyber attack halted production, will hurt profits", Reuters, June 28. [online] Available at: https://www.reuters.com/article/us-merck-co-results/merck-says-cyber-attack-halted-production-will-hurt-profits-idUSKBN1AD1AO [Accessed: 18 June 2022]

EY (2017) "Applying IFRS: Accounting for the financial impact of natural disasters", [pdf] EY: Buliding a better world. Available at: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/ifrs/ey-applying-ifrs-natural-disasters.pdf [Accessed: 17 February 2023]

Fernández, P. (2010) "WACC: Definition, Misconceptions, and Errors", Business Valuation Review, 29(4), pp. 138–144. https://doi.org/10.5791/0897-1781-29.4.138

Financial Conduct Authority (2018) "FCA fines Tesco Bank £16.4m for failures in 2016 cyber attack", Financial Conduct Authority, Oct. 01. [online] Available at: https://www.fca.org.uk/news/press-releases/fca-fines-tesco-bank-failures-2016-cyber-attack [Accessed: 25 April 2022]

Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A., Aylin, P. (2019) "A retrospective impact analysis of the WannaCry cyber-attack on the NHS", npj Digital Medicine, 2(1), 98. https://doi.org/10.1038/s41746-019-0161-6

Gillis, A. S., Rosencrance, L. (2021) "WannaCry ransomware", TechTarget. [online] Available at: https://www.techtarget.com/searchsecurity/definition/WannaCry-ransomware [Accessed: 16 June 2022]

Greenburg, A. (2018) "The Untold Story of NotPetya, the Most Devastating Cyberattack in History", Wired, Aug. 22. [online] Available at: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [Accessed: 17 June 2022]

Hern, A. (2017) "Hackers who targeted Ukraine clean out bitcoin ransom wallet", The Guardian, July 05. [online] Available at: https://www.theguardian.com/technology/2017/jul/05/notpetya-ransomware-hackers-ukraine-bitcoin-ransom-wallet-motives [Accessed: 17 June 2022]

Hope, A. (2022) "Toyota's Supply Chain Cyber Attack Stopped Production, Cutting Down a Third of Its Global Output", CPO magazine, Mar. 09. [online] Available at: https://www.cpomagazine.com/cyber-security/toyotas-supply-chain-cyber-attack-stopped-production-cutting-down-a-third-of-its-global-output/ [Accessed: 30 April 2022]

Jibilian, I., Canales, K. (2021) "The US is readying sanctions against Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal", Insider, Apr. 15. [online] Available at: https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12 [Accessed: 05 February 2022]

Krasznay, C. (2020) "Case Study: The NotPetya Campaign", In: Török, B. (ed.) Információ- és kiberbiztonság, Ludovika Egyetemi Kiadó, Budapest, Hungary, pp. 485–499.

Kuehl, D. T. (2009) "Chapter 2: From Cyberspace to Cyberpower: Defining the Problem", In: Kramer, F. D., Starr, S. H., Wentz, L. K. (eds.) Cyberpower and National Security, University of Nebraska Press, Potomac Books, pp. 24–42. ISBN 978-1-59797-933-7 https://doi.org/10.2307/j.ctt1djmhj1.7

Kumar, M. (2016) "Tesco Bank Hacked – Cyber Fraudsters Stole Money From 20,000 Accounts", The Hacker News, Nov. 07. [online] Available at: https://thehackernews.com/2016/11/tesco-bank-hack.html [Accessed: 25 April 2022]

Kumar, S., Singh, A. K., Kalam, M. A. (2019) "Intelligent electronic device functionality and interfacing: An experimental examination of smart grid", International Journal of Recent Technology and Engineering (IJRTE), 8(2S11), pp. 3922–3926. https://doi.org/10.35940/ijrte.B1523.0982S1119

Lydon, B. (2019) "RAMI 4.0 reference architectural model for Industrie 4.0", International Society of Automation, Research Triangle Park, NC, USA, InTech, 66. [online] Available at: https://www.isa.org/intech-home/2019/march-april/features/rami-4-0-reference-architectural-model-for-industr [Accessed: 04 March2023]

Merck (2019) "Form 10-K", Merck, Kenilworth, NJ, USA, Rep. 1-6571. [online] Available at: https://www.sec.gov/Archives/edgar/data/310158/000031015819000014/mrk1231201810k.htm [Accessed: 18 June 2022]

Merck & Co. Inc. v. ACE American Ins. Co. (2022) N.J. Super. Ct. Law Div., USA, UNN-L-002682-18. [online] Available at: https://www.documentcloud.org/documents/21183337-merck-v-ace-american [Accessed: 04 March 2023]

Na, O., Park, L. W., Yu, H., Kim, Y., Chang, H. (2019) "The rating model of corporate information for economic security activities", Security Journal, 32(4), pp. 435–456. https://doi.org/10.1057/s41284-019-00171-z

National Audit Office (2018) "Investigation: WannaCry cyber attack and the NHS", National Audit Office: Department of Health, London, UK, Rep. HC 414. [online] Available at: https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf [Accessed: 15 March 2019]

Oladimeji, S., Kerner, S. M. (2023) "SolarWinds hack explained: Everything you need to know", TechTarget, June 27. [online] Available at: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know [Accessed: 02 February 2022]

Oral, C., Cenk Akkaya, G. (2015) "Cash Flow at Risk: A Tool for Financial Planning", Procedia Economics and Finance, 23, pp. 262–266. https://doi.org/10.1016/S2212-5671(15)00358-5

Pownall, C. (2019) "The Context and Impact of Maerk's NotPetya cyber attack", [pdf] CPC&ASSOCIATES. Available at: https://www.researchgate.net/publication/346080185_The_Context_and_Impact_of_Maerk's_NotPetya_cyber_attack [Accessed: 17 June 2022]

Ratnam, G. (2021) "Cleaning up SolarWinds hack may cost as much as $100 billion", Roll Call, Jan. 11. [online] Available at: https://rollcall.com/2021/01/11/cleaning-up-solarwinds-hack-may-cost-as-much-as-100-billion/ [Accessed: 06 November 2022]

Roblek, V., Meško, M., Krapež, A. (2016) "A Complex View of Industry 4.0", SAGE Open, 6(2). https://doi.org/10.1177/2158244016653987

Sagonowsky, E. (2019) "Merck, insurers fight over $1.3B in damages from cyberattack: Bloomberg", Fierce Pharma, Dec. 04. [online] Available at: https://www.fiercepharma.com/pharma/merck-insurers-fight-over-1-3-billion-damages-from-cyberattack-bloomberg [Accessed: 18 June 2022]

Shah, S. (2021) "The Financial Impact of SolarWinds Breach", BitSight, Jan. 12. [online] Available at: https://www.bitsight.com/blog/the-financial-impact-of-solarwinds-a-cyber-catastrophe-but-insurance-disaster-avoided [Accessed: 06 November 2022]

Sharpe, W. F. (1964) "Capital Asset Prices: A Theory of Market Equilibrium under Conditions of Risk", The Journal of Finance, 19(3), pp. 425–442. https://doi.org/10.2307/2977928

SolarWinds (2020) "Form 8-K", SolarWinds, Austin, TX, USA, Rep. 001-38711. [online] Available at: https://www.sec.gov/ix?doc=/Archives/edgar/data/1739942/000162828020017451/swi-20201214.htm [Accessed: 05 February 2022]

SolarWinds (2021a) "Form 10-K", SolarWinds, Austin, TX, USA, Rep. 001-34358. [online] Available at: https://www.sec.gov/Archives/edgar/data/1428669/000119312512081986/d270120d10k.htm [Accessed: 08 February 2023]

SolarWinds (2021b) "Form 10-Q", SolarWinds, Austin, TX, USA, Rep. 001-38711. [online] Available at: https://www.sec.gov/Archives/edgar/data/1739942/000173994221000154/swi-20210930.htm [Accessed: 08 February 2023]

Tesco PLC (2017) "Serving shoppers a little better every day: Annual Report and Financial Statements 2017", Tesco PLC, Dundee, Scotland. [online] Available at: https://www.tescoplc.com/media/474467/16-tesco-annual-report-2017.pdf [Accessed: 28 April 2022]

van Hees, M. (2020) "The 2017 MAERSK Cyber Incident: Learning from and applying the Lessons of a Major Cyber Incident", [pdf] Industrial Cyber Security. Available at: https://fhi.nl/app/uploads/sites/75/2020/10/201029-FHI_Maersk.pdf [Accessed: 17 June 2022]

Wolpoff, D. (2020) "After the FireEye and SolarWinds breaches, what's your failsafe?", TechCrunch, Dec. 21 [online] Available at: https://techcrunch.com/2020/12/21/after-the-fireeye-and-solarwinds-breaches-whats-your-failsafe [Accessed: 04 March 2023]

Žižlavský, O. (2014) "Net Present Value Approach: Method for Economic Assessment of Innovation Projects", Procedia – Social and Behavioral Sciences, 156, pp. 506–512. https://doi.org/10.1016/j.sbspro.2014.11.230