SECURITY & DEFENCE QUARTERLY

https://securityanddefence.pl/

Managing the financial impact of cybersecurity incidents

Zsolt Bederna[1], Tamás Szádeczky[2]

[1] https://orcid.org/0000-0003-0444-7275

[1]Doctoral School for Safety and Security Sciences, Obuda University, Bécsi út 96/B, 1034 Budapest, Hungary

[2]szadeczky@mail.muni.cz

[2] https://orcid.org/0000-0001-7191-4924

[2]Department of Management and Business Economics, Budapest University of Technology and Economics,
Muegyetem rkp. 3, 1111 Budapest, Hungary; Czech CyberCrime Centre of Excellence C4e, Masaryk University,
9 Zerotinovo nam., 601 77, Brno, Czech Republic

Abstract

The complex relationships of economic actors and the high dependency on information and communication technologies make it necessary for all relevant entities to develop protection. This protection should include preventive and reactive controls in a risk-proportionate manner in relation to the business value protected. We aimed to develop a solution to support cybersecurity-related business decisions with financial analytics. The risk-based approach helps management find the optimum solution with minimal costs, where protection prevents some incidents from occurring, while the risks associated with other incidents are accepted in an informed way. The security industry developed a number of apparatuses to find the optimum security controls that enforced the fiscal aspects, which typically contain solutions used in planning. However, the actual expenditure often differs from the planned budget for several reasons, one of which is the occurrence of security incidents. We used the common methodology toolset for financial analysis (NPV, NFV, risk assessment). We developed novel metrics based on these that can be used in cybersecurity management. Within the framework thus defined, the article discusses the economic context of the effects of incidents involving Meta (previously Facebook) services from 2016 to 2020. This paper introduces the 'Effect of incidents' metric to measure the impact of unplanned incidents' on actual expenditure compared to the planned budget and the 'Incidence of incident recognition' metric to measure deviations of an incident's impact as perceived by owners relative to the effect on the value of the assets. The paper also proves the applicability of those metrics using the example of Meta.

Keywords:

economic analysis, economic impact, cybersecurity, cybersecurity incidents

Article info
Received: 25 October 2022
Revised: 7 January 2023
Accepted: 22 January 2023
Available online: 24 February 2023

Citation: Bederna, Z. and Szádeczky, T. (2023) 'Managing the financial impact of cybersecurity incidents', Security and Defence Quarterly, 41(1), pp. 15–35.
doi: 10.35467/sdq/159625.

Introduction

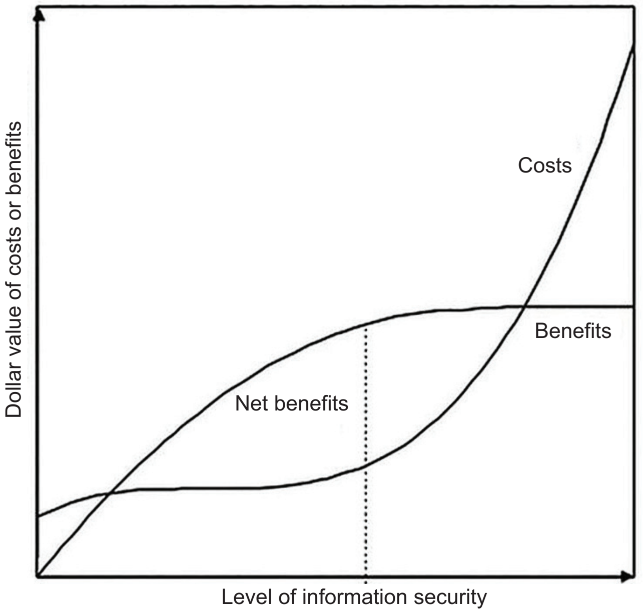
As a result of the dynamically changing operational environment due to the dynamic development of technology, the information society has a dominant and growing dependency on information and communication technologies (ICTs), resulting in an IT service portfolio that considerably affects value for shareholders (Sun *et al.*, 2021). In parallel, this dependency has created an increasing need for working in a secure environment. Therefore, legislation requires all relevant entities to plan and design security controls that include preventive and reactive controls in a risk-proportionate manner in relation to the protected business value.

Selecting the specific security controls from the possible set of control mixes to be implemented is far more complicated than it looks at first. Those that have a negative impact on the given IT system's usability and functionality are unacceptable. Considering this fact, one must choose one of the possible control mixes that comprises the proper preventive, detective, reactive, and compensatory controls, which do not endanger the business operation. On the other hand, the implemented controls must support the preventative or reactive capabilities in the right way to provide the required level of security and ensure the confidentiality, integrity, and availability of the IT services and the processed data and prevent and react to security incidents.

One must select security controls based on risk proportionality from a financial perspective, i.e., the costs remain lower than the benefits. The chosen control mix should help achieve the (pseudo-) optimum from the economic point of view. According to the microeconomic concepts of marginal revenue and marginal cost (Sklavos and Souras, 2006), a security budget is spent optimally when the marginal revenue and marginal cost are equal. This point represents the optimal security level (Gordon and Loeb, 2002, p. 9), denoted by S^* in Figure 1.

However, due to inadequate knowledge or a negative attitude, management may view cybersecurity controls as unnecessarily bound up with legislation. The results of a survey conducted by Ernst & Young between August and October 2019 (Ernst & Young, 2020) supports the existence of this issue. Cybersecurity investment in the non-profit field is much lower, about half of the for-profit investments, according to (de Geest and Stranlund, 2019).

Figure 1. Cost-benefit analysis of information security (based on Gordon and Loeb, 2002, p. 9).



Many organisations consider IT security and other security aspects as a subset of IT management functionally and fiscally despite the apparent difference, goals, and incompatible functions. For example, organisations allocated an average of 8 per cent of their revenue for IT spending in 2019 (Statista, 2020). Nevertheless, finding the optimum where costs can be (pseudo-) minimised is not an easy task. However, the risk-based approach helps achieve this objective while meeting several constraints. For example, according to the balanced operational constraints, security controls that hinder or even prevent the achievement of business goals are unacceptable (Wheeler, 2011).

The following questions arise: What are the effects of the incidents? How do owners perceive the incidents? Furthermore, what are the options for an economic analysis of defence planning? Below, we introduce a framework to analyse our chosen case study comprising security-related events that affected Meta's (previously Facebook's) services, incidents which are not recognised or even disclosed publicly Romanosky (2016).

Methodology development

Cash-flow calculations

The NPV calculation is an essential tool for dynamic investment economics calculations and considers the time value of money. Therefore, the NPV is also excellent for analysing security investments (Brotby, 2009). To calculate the value of the expected expenses and returns before starting the investment, one must apply the following formula, in which CF_t is the annual cash flow, while r is the interest rate:

$$\mathrm{NPV} = \sum_{t=1}^{n} \frac{CF_{tt}}{\prod_{i=1}^{t} (1 + r_i)}$$

Unlike the NPV, the Net Future Value (NFV) calculates the value of a sum of the cash flows at some point in the future, giving the represented value:

$$\mathrm{NFV} = \sum_{t=1}^{n-1} \left(CF_t \times \prod_{i=t}^{n-1} (1 + r_{i+1}) \right) + CF_n$$

In the above equations, it is assumed that cash flows occurred at the end of each year or, at least, they are discounted to the end of a given year by the effective interest rate, e^{ri}, where i is the number of days remaining until the end of the given year.

Although NPV and NFV calculations are essential tools in investment calculation, they are sensitive to determining the proper cash flows and choosing appropriate interest rates unless they represent valid present or future values (Beccarini, 2007).

Determining the interest rates

When examining corporate and shareholder values, the basis for calculating interest is usually the cost of capital, where corporate (*A*), shareholder (*E*), and lending (*D*) capital costs differ. There are several options for calculating the shareholders' cost of capital, from which the Capital Asset Pricing Model (CAPM) (Sharpe, 1964) is a widely applied formula:

$$r_E = r_f + \beta(r_M - r_{f,nom})$$

In the above equation, r_E represents the return on an individual stock, r_f is the risk-free interest rate, and r_m is the market interest rate. β measures the volatility of an individual stock compared to the systematic risk of the entire market, representing a particular stock's returns against those of the whole market. For an unleveraged company, the corporate interest rate (r_A) equals the shareholder interest rate (r_E); however, if a company is leveraged, the weighted-average cost of capital (r_{wacc}) must be taken into account. Furthermore, considering that particular case of r_{wacc} when D = 0, r_{wacc}, equals r_A ($r_A = (r_{wacc}|D=0)$). Therefore, we consequently apply r_{wacc} for the calculations.

Possibilities of ex-ante analysis

When planning security controls, there are uncertainties in valuing expenditures and revenues (benefits) that each organisation must tackle. Over time, incidents may happen intentionally, according to the risk-proprietary approach. In this case, the expected total cost of security comprises the cost of the security-enhancing or reservation mechanism and the expected total cost of violations (Olovsson, 1992; Ruan, 2017), as displayed in Figure 2. This is a cost-based approach finding the optimal security level denoted by *S** in Figure 1.

The base of estimation methods is very often the annualised loss expectancy (ALE) which is the product of the single loss expectancy (SLE) multiplied by the annualised rate of occurrence (ARO):

$$\text{ALE} = \text{SLE} \times \text{ARO}$$

ARO is the estimated frequency of the given risk's occurrence within one year. SLE is the amount of the aggregated expected monetary loss of a security incident's impact on an entity's operations, data, and IT assets. The SLE thus summarises direct, indirect, legal, operational, and human-like damage values which depend on the affected asset's value (AV) and exposure factor (EF), which is the percentage of the damage or loss compared to the AV:

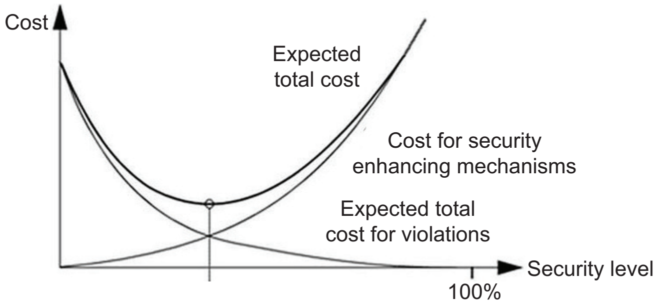
$$\text{SLE} = \text{AV} \times \text{EF}$$

Finally, as the ALE is a multiplication of the AV, EF, and the annualised rate of occurrence (ARO) representing a one-year interval loss value, assuming the loss expectancy is constant for an *n*-year-long time interval, one can calculate it like this:

$$\text{loss expectancy}_n = \sum_{t=1}^{n} \text{ALE} = \sum_{t=1}^{n} \text{AV} \times \text{EF} \times \text{ARO}$$

Several models or metrics use the ALE to analyse risks choosing security controls in the planning phase, and evolving the *S** optimal control mixes, such as the value at risk (VAR)

Figure 2. Information security cost analysis (based on Olovsson, 1992, p. 6).



and the net present value (NPV) methodologies. We should be aware that security incidents might have national or global impacts on the market, such as the Colonial Pipeline shutdown on gasoline prices (Tsvetanov and Slaria, 2021). Due to its special nature, we cannot count on that in the ALE calculation.

Regarding the given security control mix that affects the operation, i.e., the controls can prevent incidents or reduce their impact from its activation with a planned ALE, the aggregated cost of commissioning and maintenance is the solution cost (SC). Therefore, if one needs to calculate the cash flow comprising possible expenditures, then the NPV is calculated as follows:

$$NPV^{\text{expenditures}} = \sum_{t=1}^{n} \frac{-\overbrace{AV * EF * ARO}^{ALE} - SC_t}{\prod_{i=1}^{t}\left(1 + r_i\right)}$$

Possibilities of ex-post analysis

For the periodic reviews of security controls, the substantial economic impacts of incidents serve as a crucial exact input about the nature of the non-compliance with confidentiality, integrity, or availability requirements determined by business needs. In contrast to the design of security controls, one must examine the effects of incidents afterwards, i.e., the NFV of the damage caused by an I incident.

However, an incident's effects may last for years so the value concerned can be strictly determined by the summation of each year's effect, I_t, applying the following formula, in which the subscript A represents that the examination's subject is a company:

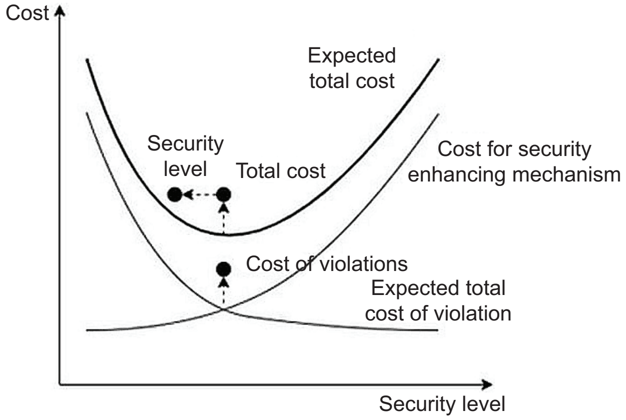
$$NFV^{I_A} = \sum_{t=1}^{n-1}\left(I_{A,t} * \prod_{i=t}^{n-1}\left(1 + r_{wacc,i+1}\right)\right) + I_{A,n}$$

However, in performing an ex-post analysis, it is necessary to avoid confusion between the uncertain planning values and the past factual budgeting and incidents' values. Accordingly, a distinction must be made between the date of design and repeated analysis when discounting values. Therefore, when comparing the planning value to the value modified after the incident, one must analyse the same time interval, and cash flows must, of course, be discounted to the same date.

In the ex-ante analyses, ALE and SC_i are determined from the risk analysis that more or less represents the security budget for the given control mix, assuming an optimal cost-benefit balance. However, in the course of ex-post analysis, one has the exact yearly SC_i values from its yearly planning security budget. Nevertheless, there may be a clear difference between the planning budget at the beginning of the year (BOTY) and the realised budget at the end of that year (EOTY). So, incident types and impacts are maybe different than the planned value. The question is the magnitude and direction of deviation in which the risk-based planning, the planned (BOTY), and the realised (EOTY) budgets may differ. In the following calculation, their NPVs are calculated and displayed; however, NFVs could also be checked in the same way:

$$\overbrace{\sum_{t=1}^{n} \frac{-ALE - SC_t}{\prod_{i=1}^{t}\left(1 + r_{wacc,i}\right)} \overset{?}{=} \sum_{t=1}^{n} \frac{-Budget_t^{BOTY}}{\prod_{i=1}^{t}\left(1 + r_{wacc,i}\right)}}^{ex-ante} \overset{?}{=} \overbrace{\sum_{t=1}^{n} \frac{-Budget_t^{BOTY} + I_{A,t}}{\prod_{i=1}^{t}\left(1 + r_{wacc,i}\right)} = \sum_{t=1}^{n} \frac{-Budget_t^{EOTY}}{\prod_{i=1}^{t}\left(1 + r_{wacc,i}\right)}}^{ex-post}$$

Figure 3. Impact of incidents on costs (modified from source: Olovsson, 1992, p. 6).



Furthermore, the realised interest rate can be applied for a more precise evaluation in an ex-post analysis. However, a negative deviation may result in an increased total cost for violations, having a chain-like effect that can ultimately reduce the security level of the entire system, as depicted in Figure 3.

In the interest of examining the mechanism's on-the-fly effect on the budget, the following formula defines the *Effect of incidents* for an [1,n] examined interval based on NFV values of the security budget and incidents:

$$\text{Effect of incidents} = \frac{\mathrm{NFV}^{I_A}}{\mathrm{NFV}^{\mathrm{Budget}}} = \frac{\sum_{t=1}^{n-1}\left(I_{A,t} * \prod_{i=t}^{n-1}\left(1+r_{\mathrm{wacc},i+1}\right)\right)+I_{A,n}}{\sum_{t=1}^{n-1}\left(\mathrm{Budget}_t^{\mathrm{BOTY}} * \prod_{i=t}^{n-1}\left(1+r_{\mathrm{wacc},i+1}\right)\right)+\mathrm{Budget}_n^{\mathrm{BOTY}}}[\%]$$

However, considering the shareholders' behavioural biases and the differences in the perception of positive and negative events (Tversky and Kahneman, 1981), there may be a deviation between the shareholders' perception and the magnitude of the incidents affecting the organisation. Matthew Rabin (1998) points out that shareholders overwhelmingly dislike losses. With regard to cybersecurity incidents, the following formula compares the change in stock prices (I_P) and the change in shareholders' value (I_E) caused by the examined set of events connected with an incident that must be discounted by the shareholder interest rate (r_E):

$$\text{Incidence of incident recognition} = \frac{\mathrm{NFV}^{I_P}}{\mathrm{NFV}^{I_E}} = \frac{\sum_{t=1}^{n-1}\left(I_{P,t} * \prod_{i=t}^{n-1}\left(1+r_{E,i+1}\right)\right)+I_{P,n}}{\sum_{t=1}^{n-1}\left(I_{E,t} * \prod_{i=t}^{n-1}\left(1+r_{E,i+1}\right)\right)+I_{E,n}}[\%]$$

Analysis of the effect of security on stock prices

We use an event study (Armitage, 1995) to quantify an events' economic impact with abnormal returns (ARs), applying the market model (MM) to calculate the expected return:

$$AR_t = R_t - (\alpha + \beta R_{M,t})$$

The MM builds on the actual returns of a reference market and the correlation of the given firm's stock with the reference market, for which this model uses the ordinary least squares

(OLS). The AR_t signifies the difference between the actual stock return (R_t) on a particular day within the event window and the normal return, depicted by the relationship between the firm's stock and its reference index (expressed by the α and β parameters). The model assumes that the residuals are normally distributed with a zero mean, have constant variance (homoscedasticity), are not serially correlated, and are not correlated with the explanatory variables. To test if heteroscedasticity negatively affects the estimation, we apply the Breusch-Pagan test (Breusch and Pagan, 1979).

To calculate the normal return, we use the S&P500 market's return ($R_{M,t}$). The R_t and $R_{M,t}$ are calculated by the natural log-normalised returns, i.e., in case of stock return, $R_t = \ln\left(\frac{P_t}{P_{t-1}}\right)$ where P_t is the closing price for a given day and P_{t-1} is the closing price of the previous day.

We apply observation windows of [–150,–2] to analyse daily abnormal returns at a [–1,3] time interval as **Figure 4** shows.

To measure the statistical significance of ARs, we apply the t-test (N = 149) for hypothesis testing, where the null hypothesis states that the mean of the ARs within the event window is zero (H_0:μ = 0) and the alternative hypothesis states the opposite (H_1:μ ≠ 0) for which test statistic is the standardised abnormal return given by:

$t_{AR_t} = \frac{AR_t}{S_{AR}}$ S_{AR} is the standard deviation of the abnormal returns in the estimation window based on

$$S_{AR}^2 = \frac{1}{M-2}\sum_{t=T_0}^{T_1}\left(AR_t\right)^2$$

where T_0 is the earliest day of the estimation window and T_1 is the latest day of the estimation window, and M denotes the number of non-missing (i.e., matched) returns.

Identification of the security-incident-related events

Short review of Meta's incidents

In 2014, Cambridge Analytica collected Facebook user profiles in unethical and non-legal ways, affecting about 87 million users in the US (Business Insider, 2019). The publicity regarding the incident caused a drop in the company's share price by approximately 7 per cent, on 19 March 2018 (CNBC, 2018).

According to revenue shortfalls, the share price fell 19 per cent on 26 July 2018 (MarketWatch, 2018). The closing price was $176.26, which means that compared to the previous day's Wednesday market capitalisation, which was $630 billion, it fell to $510

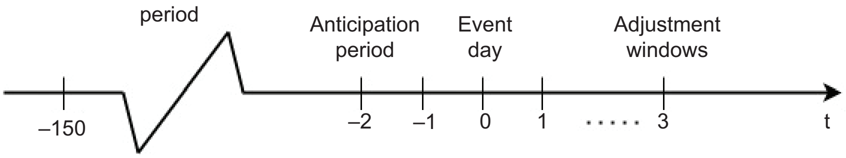


Figure 4. Windows' sizes for the event study.

billion by the end of Thursday's trading day with a trading volume of 170 million. This change meant an impairment loss of approximately $120 billion.

On 28 September 2018, Meta revealed a data theft affecting about 2 million Facebook users' date of birth, phone number, search history, and last login location. Even before the official announcement, on 27 September 2018, the share price fell by 3 per cent due to the publicity around the cyberattack (Business Insider, 2018).

By the end of the trading day on 18 March 2019, the shares were closing at 7.4 per cent lower than when the four-day long decrease began (International Business Times, 2019) due to the departure of product manager Chris Cox and vice president Chris Daniels of WhatsApp and the Needham downgrade. However, on 13 March, several hours of service outages affected all services due to an application error (The Verge, 2019).

On 24 March 2019, a security incident affecting the Instagram service was announced (Facebook, 2019c). On 18 April 2019, new information was revealed. When, on 12 June 2019, CEO Mark Zuckerberg's sent a related email concerning problematic privacy practices, share prices fell 2.9 per cent (Markets Insider, 2019).

On 24 October 2018, the Information Commissioner's Office (ICO) in the UK fined Meta £500,000 (approximately $643,000) for its role in the Cambridge Analytica scandal. However, Meta appealed on 21 November 2018, and on 14 June 2019, the General Court issued an interim decision ordering the ICO to disclose materials related to its decision-making process. On 2 September 2019, the ICO appealed against the interim decision, and finally, on 30 October 2019, the parties agreed, as a result of which Meta paid the penalty (Information Commissioner's Office, 2019).

On 24 July 2019, the Federal Trade Commission (FTC) in the US imposed a $5 billion fine on the company (Federal Trade Commission, 2019). Furthermore, the Securities and Exchange Commission (SEC) charged an additional $100 million penalty (Facebook, 2019b) due to the investigation process.

Despite the fines and additional security incidents (e.g., in September 2019, Techcrunch (2019) reported data leaks due to several unencrypted databases with 419 million records), Meta's 2019 Q3 results exceeded the expectations of analysts and investors (CNBC, 2019).

On 19 May 2020, the competent authority, the Competition Bureau Canada, imposed a CAD 9 million fine for improper data protection practices in Canada. The authority added a procedural fee of CAD 500,000 (approximately USD 13,221,150 in total) (Competition Bureau Canada, 2020).

Although several data protection authorities in the European Union have been active against the company on several issues, Meta was only fined €51,000 in Germany alone in 2019 for non-compliance with Article 37 of the General data protection regulation (GDPR), i.e., the failure to appoint a data protection officer (Hamburgischen Beauftragten für Datenschutz und Informationsfr., 2019).

Identification of events

Five distinguishable incidents affected Meta's services (|I| = 5) – (1) Cambridge Analytica scandal, (2) Instagram vulnerability and possible data breach, (3) the leakage of 419 million data records, (4) data theft affecting 50 million users, and (5) downtime affecting all services. The fine of €51,000 imposed in Germany for non-compliance with Article 37 of the GDPR does not relate to the identified security incidents; therefore, we simply omit it.

Table 1 notes the identified events of the given incidents that modify the event date for which there are essential modifier factors discussed herewith. On 17 March 2018, Meta announced suspension of Cambridge Analytics access due to misuse of user data. The announcement was made on a Saturday. On 25 July 2018, the company announced a 19 per cent decrease based on a market report describing revenue shortfalls in the late afternoon. Unofficial sources revealed data theft affecting 50 million users on 27 Sep 2018; however, the official announcement was made during a call with reporters the following morning. On 13 March 2019, an application downtime for all services lasted for hours, which got publicity among shareholders the next day. However, on 18 March 2019, Facebook notified business and personal changes unrelated to the incidents but shortened the previous event's observation period. Lastly, the FTC imposed a $5 billion penalty for Cambridge Analytica data leaks on 24 June 2019, which got publicity the following day.

In connection with the separate incidents, based on the modifier factors, we identified the first trading days determined by the incident-related events displayed in Table 2. Regarding further incidents, we use numbers in superscript to distinguish them consequently. The events of 12 June 2019 and 19 May 2020 occurred due to Meta's previously conducted security behaviour; therefore, they cannot be clearly categorised as an incident. So, we divide their cash-flows among I^1, I^2, I^3, and I^4 incidents if there are any.

Discussion

Data and methodology

Based on the review we previously provided, we distinguish five security incidents: (1) End users suffered paramount and impactful privacy and information security incident in 2016 from Cambridge Analytica, (2) Instagram vulnerability and possible data breach, (3) leakage of 419 million data records, (4) data theft affecting 50 million users, and (5) downtime affecting all services. Table 3 displays the results of the publicly known corporate costs of the incidents. However, in our opinion, these values serve as the estimated minimum for the extra corporate costs of the incidents as there are potential publicly unknown extra negative cash flows.

The Cambridge Analytica scandal deeply affected Meta in the period following March 2018, resulting in the company's revenue being reduced. For the 2018 Q2 period, revenue was $13.73 billion, which fell short of initial expectations (–$92.44 million). For the Q3 2018 period, the company had $13.23 billion in revenue, which also fell short of analysts' expectations (–$115.24 million). These shortfalls are to be expected as an undesired impact of the incident. However, despite further incidents with high consequences, Meta was profitable in both years as it had annual revenues of $55,838 billion in 2018 and $70,697 billion in 2019, while its total operating expenses were $30,925 billion in 2018 and $46,711 billion in 2019, respectively (Facebook, 2020).

However, although the events displayed in Table 2 relating to the identified incidents started to occur in 2018, the root cause of the Cambridge Analytica scandal originated in 2016. Therefore, it is worth examining the overall company-related effects from 2016 to when the last event occurred in 2020. According to an announcement by the CEO of Meta (Roettgers, 2019), 2019's security budget was worth $3.7 billion. However, to analyse the corporate effects, there is a further need to identify Meta's yearly security budget. There is no additional exact information about budgeting, so we must assume other years.

Table 1. Incident-related events.

Event	Date	Comment
Facebook is suspending Cambridge Analytics due to misuse of user data	17 March 2018	The announcement was on Saturday
A 19 per cent decrease based on a market report describing revenue shortfalls	25 July 2018	The announcement was in the afternoon
Techcrunch reports data leaks affecting 419 million records	04 Sep 2018	
Unofficial sources reveal data theft affecting 50 million users	27 Sep 2018	The breach was discovered
	28 Sep 2018	The announcement was made in a conference call with reporters on Friday morning
The ICO imposes a $643,000 penalty for Cambridge Analytica data leakage	24 Oct 2018	
Realised quarterly revenue does not reach estimated quarterly revenue	30 Oct 2018	
Facebook appealed to the Court of First Instance	21 Nov 2018	
Application downtime for all services	13 March 2019	
	14 March 2019	Got publicity
Notification of business and personal changes	18 March 2019	Does not relate to incidents, but shortened the observation period
Report an Instagram privacy incident	25 March 2019	
The company reports additional information that aggravates the incident	18 April 2019	
Letter from CEO Mark Zuckerberg on concerns about "potentially problematic privacy practices"	12 June 2019	
In an interlocutory judgment, the General Court ordered the ICO to disclose its decision-making material.	14 June 2019	
The FTC imposes a $5 billion penalty for Cambridge Analytica data leaks	24 June 2019	
	25 June 2019	Got publicity
The ICO appealed against the interim decision.	03 Sep 2019	
Facebook pays the penalty	30 Oct 2019	
Competition Bureau Canada imposed a 9 million CAD fine for improper privacy practices	19 May 2020	

Many organisations consider IT security and other security aspects as a subset of IT management functionally and fiscally despite the apparent difference, goals, and incompatible functions. Therefore, it is worth assuming the budget in the same way. According to Gartner (Hall *et al.*, 2016), IT security spending ranged from approximately 1 per cent to 13 per cent of the IT budget in 2016. Meanwhile, in 2021, researchers measured IT spending of the software companies as 15 per cent of revenue on ICT (Flexera, 2021). With regard to the cybersecurity budget, the analysts estimated the cybersecurity budget from 6 to 14 per cent of their information technology budget according to the Deloitte and the Financial Services Information Sharing and Analysis Centre (FS-ISAC) report in 2019. On average, organisations allocated 10.1 per cent of the IT budget and 10.9 per cent for 2020 (Bernard *et al.*, 2020). For the analysis, we assume higher budgeting percentiles. Assuming that the IT budget was 11.4 per cent of the revenue and the cybersecurity or IT security budget was 10.1 per cent of the IT budget, on average, we apply 0.011514 multipliers to the revenue for calculating the cybersecurity or IT security

Table 2. Date of the effective events.

Incidents	Description	Effective events' date
I^1	Cambridge Analytica scandal	19 March 2018; 26 July 2018; 24 October 2018; 30 October 2018;21 November 2018 12 June 2019; 14 June 2019; 24 June 2019; 03 September 2019; 30 October 2019 19 May 2020
I^2	Instagram vulnerability and possible data breach	25 March 2019; 18 April 2019; 12 June 2019 19 May 2020
I^3	Leakage of 419 million data records	04 September 2018 12 June 2019 19 May 2020
I^4	Data theft affecting 50 million users	27 September 2018 12 June 2019 19 May 2020
I^4	Downtime affecting all services	13 March 2019

Table 3. Publicly known extra corporate costs of the incidents.

Date	I^1_A	I^2_A	I^3_A	I^4_A	I^5_A
26 July 2018	–$92,550,000				
30 October 2018	–$115,240,000				
13 March 2019					–$96,845,205.48
24 June 2019	–$5,100,000,000				
30 October 2019	–$643,000				
19 May 2020	–$3,305,288	–$3,305,288	–$3,305,288	–$3,305,288	

budget. Considering this multiplier is a rough estimate, we conduct a risk analysis later in the paper that examines budget changes for the given calculation.

Table 4 displays the NFV of the yearly estimated security budget of Meta and the identified incidents and other input data as revenues, expenses, shares, asset and shareholder value, and liabilities (Facebook, 2017, 2018, 2019a, 2020, 2021). The yearly cost of capital ex-post is based on the CAPM model using exact values for the given years. We applied the annual real returns on T Bond (Damodaran, 2021) as r_f and the MSCI ACWI Index (USD) (MSCI, 2021) for calculating r_M. We determined $r_{f,nom}$ from the US real interest rate (Federal Reserve Bank of St. Louis, 2021) and the US inflation rate (Coin News, 2021), and lastly, we calculated β using Meta stock prices (Financial Content, 2021) and the S&P500 index (Yahoo! Finance, 2021). The publicly known corporate costs of the incidents displayed in Table 3 are discounted to the end of the given year by the effective interest rate (e^{ri}). Lastly, according to the annual reports, the company did not work with long-term debt; however, liabilities exist yearly, so we apply r_{wacc} to discount cash-flows, and we approximate r_D with $r_{f,nom}$ assuming a perfect lending market (Ahn, 2016) without any spread, as Meta did not have any debt rating.

Findings

Table 5 displays the value of corporate changes related to incidents discounted to the end of the given year with the effective rate. Based on the highlighted extra cash-flows and the

Table 4. Corporate financial data.

Annual revenue and operating expenses (millions)					
	2016	**2017**	**2018**	**2019**	**2020**
Revenue	$27,638	$40,653	$55,838	$70,697	$85,96
Total costs	–$15,211	–$20,450	–$30,925	–$46,711	–$53,294
Number of shares (millions)					
Class A	2,354	2,397	2,385	2,407	2,406
Class B	538	509	469	445	443
Sum of shares	2,892	2,906	2,854	2,852	2,849
Equity (E), Asset (A), and Dept (D) value (millions)					
A =	$64,961	$84,524	$97,334	$133,376	$159,316
E =	$59,194	$74,347	$84,127	$101,054	$128,29
D =	$5,767	$10,177	$13,207	$32,322	$31,026
Calculated yearly cost of capital					
$\mathbf{r_E}$ **=**	0.0494	0.2259	–0.2000	0.3520	0.2733
$\mathbf{r_D}$ **=**	0.0316	0.0448	0.0538	0.0398	0.0210
$\mathbf{r_{wacc}}$ **=**	0.0473	0.2029	–0.1665	0.2739	0.2237
Value of corporate changes related to incidents at the end of the given year (million)					
$\mathbf{I_A^1}$ **=**			–$207.67	–$5,107.98	–$3.31
$\mathbf{I_A^2}$ **=**					–$3.31
$\mathbf{I_A^3}$ **=**					–$3.31
$\mathbf{I_A^4}$					–$3.31
$\mathbf{I_A^5}$				–$97.19	

Table 5. Calculation of the incidents' corporate net future values and the *Effect of incidents*.

Value of corporate changes related to incidents at the end of the given year (millions)					
	2016	**2017**	**2018**	**2019**	**2020**
Estimated security budget	–$318.22	–$468.08	–$642.92	–$3,700.00	–$989.80
$\mathbf{I_A^1}$ **=**			–$207.69	–$5,107.92	–$3.31
$\mathbf{I_A^2}$ **=**					–$3.31
$\mathbf{I_A^3}$ **=**					–$3.31
$\mathbf{I_A^4}$ **=**					–$3.31
$\mathbf{I_A^5}$ **=**				–$97.10	
Discounted values of incidents – net future values for 2020 (millions)					
			$\mathbf{NFV_{sec\ budget}}$		–$7,625.22
	=		$\mathbf{NFV_{I_A^1}}$ =		–$6,577.57
	=		$\mathbf{NFV_{I_A^2}}$ =		–$3.309
	=		$\mathbf{NFV_{I_A^3}}$ =		–$3.309
	=		$\mathbf{NFV_{I_A^4}}$ =		–$3.309
	=		$\mathbf{NFV_{I_A^5}}$ =		–$118.77
	=		$\mathbf{NFV_{I_A}}$ =		–$6,706.27
			Effect of incidents = +87.95%		

estimated security budgets, the calculated *Effect of incidents metric* shows that the corporate effects of the incidents increased the overall costs by approximately 87.95 per cent of the estimated security budget.

However, assuming the security budget's estimation was probably inaccurate, we created what-if scenarios to analyse lower and higher yearly security budgets. Figure 4 displays the impact of incidents depending on the NFV of the annual budgets and the NFV of the incidents that altered the security budgets. Unsurprisingly, the higher the yearly budget, the lower the impact of incidents as the incidents' values remain.

On the other hand, we created what-if scenarios regarding the valuation of the incidents' corporate effects representing lower estimates. Figure 6 displays the impact of incidents depending on the NFV of the yearly budgets and the NFV of the incidents that altered the costs. Inevitably, the higher the corporate expenses of incidents (via the cost multiplier), the higher the impact of incidents. The security budget is constant for this time.

Analysing the Incidence of incident recognition

We used significant ARs to calculate the *Incidence of incident recognition* on the stock and asset changes on discounted values up to 2020, the corporate effects (I_A) of which we apply in Table 3, and the cost of capital and shares in Table 4. However, in this case, the corporate effects must be discounted with I_E to get the equity-related changes.

According to Table **6**, there are six events for which significant ARs can be identified. Taking the identified ARs, we calculate the overall values they represent for a given year and their NFVs discounted to 2020. Comparing the calculated NFV of stock changes to the equity-related changes shows that the stock changes were -70.40 per cent of the effects on equity, meaning that the short term abnormal-return-related stock price changes and the equity-related changes had opposite effects. Because the estimation of the security budget creates uncertainty for the *Incidence of incident recognition*, we analyse what-if scenarios on the security budget. As **Figure** 7 depicts, the higher the costs of security incidents, the lower the *Incidence of incident recognition*.

Figure 5. The effect of security budget changes.

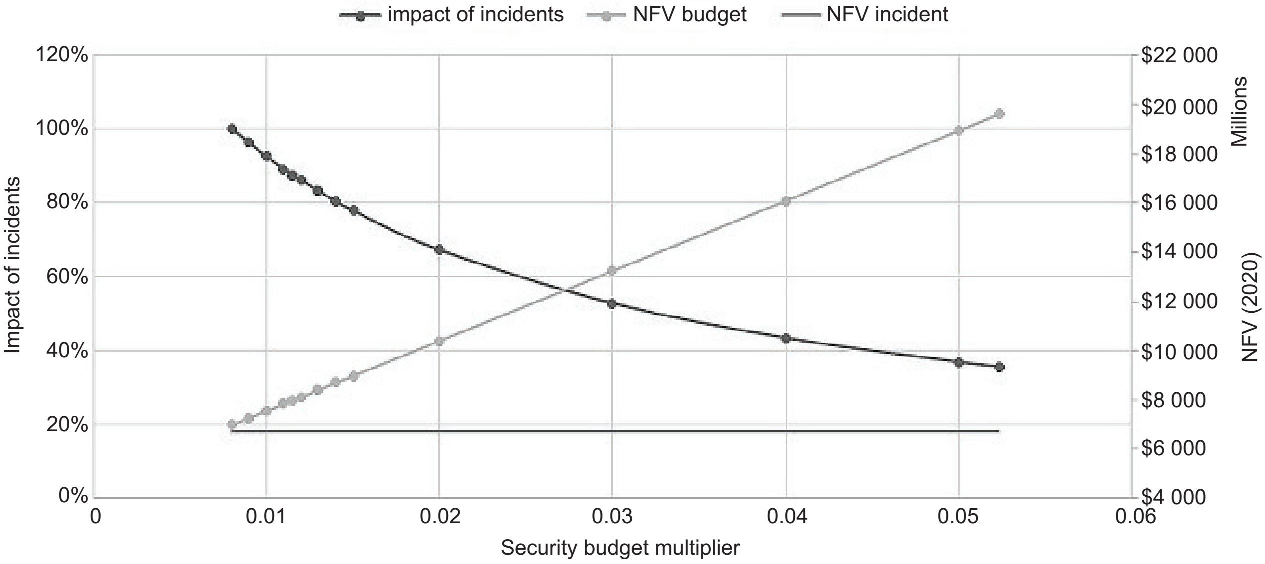
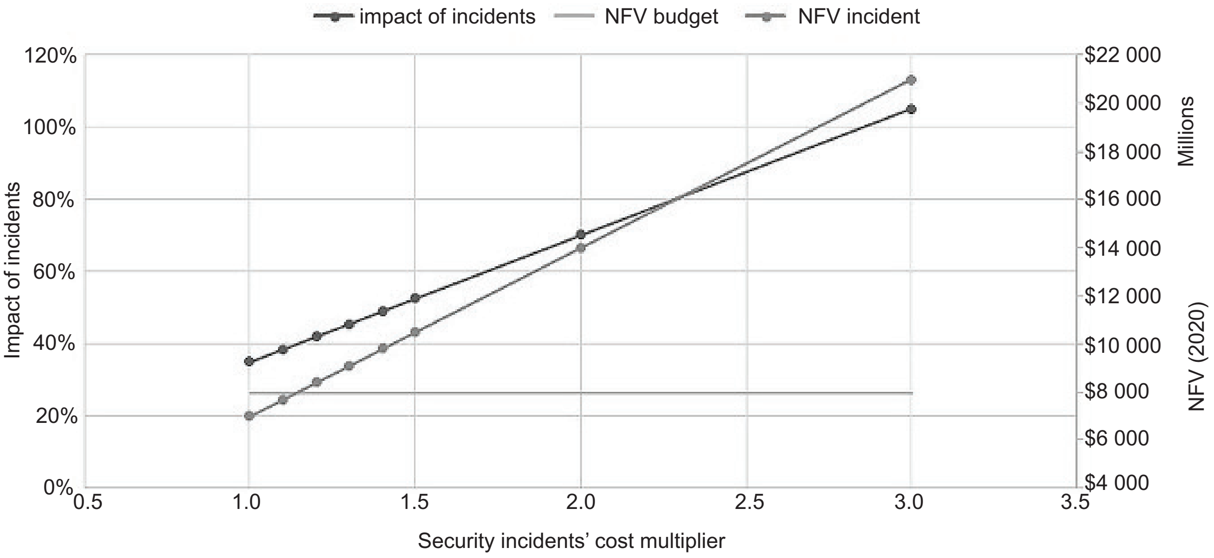


Figure 6. The effect of incidents' costs changes.



Conclusions

Although the development of technology has improved efficiency for individuals, organisations, and hence society, it appears as a risk factor. The complex chain of entities' relationships also creates a complex ecosystem in terms of cybersecurity. Therefore, to reduce risks, each entity's responsibility is to establish and maintain cybersecurity controls for which several control mixes can be selected for creating and maintaining the appropriate preventive and reactive capabilities, i.e., there are several alternatives. Each alternative may differ not only in nature but also in the quality of security controls, but it is necessary to select and optimise security capabilities per risk proportionality and risk appetite for cyber safety, and the absence of such has economic implications. The consequence of taking risks is that it consciously entails incidents. However, some incidents can increase planned costs and decrease security level. The cash flows caused by unplanned incidents with such an impact are generated in addition to the "normal" (planned) operation. However, once the incidents' financial impacts have been identified, it is possible to analyse ex-post and compare the past and planned values, for which we started the methodology development from loss-expectancy-based ex-ante analysis that should serve the basis for the annual security budget using CAPM-based interest rates.

The consequences of the incidents, such as the possibility of imposing a penalty, imposition, loss of revenue, can be huge, significantly increasing the costs related to IT security compared to the assumed budget. The financial consequences for a company may be that the incidents increase the expenditure compared to the pre-defined budget. To analyse these effects, we introduced the *Effect of incidents* and the *Incidence of incident recognition* metrics for measuring business effects and making a deduction related to the behaviour of shareholders. Because shareholders can perceive incidents as a kind of shock effect, we assumed in advance that the share price might differ from the asset value in connection with the examined events.

We took publicly disclosed cybersecurity incidents that affected Meta's (previously Facebook's) services during a time interval from 2016 to 2020 to find answers to the preset questions, applying the introduced metrics. We distinguished five security incidents:

Table 6. Abnormal returns.

Event	Observation	Abnormal return	Params (α, β, Breusch-Pagan p value)	t stat	p value
Facebook suspends Cambridge Analytics due to misuse of user data (19 March 2018)	AR (–1)	0.55%	α = –0.00093	0.4655	0.64246
	AR (0)	–5.15%	β = 1.23583	–4.3639	**0.00003***
	AR (1)	–2.68%	p = 0.25248	–2.2706	**0.02498***
	AR (2)	1.06%		0.8947	0.37279
	AR (3)	0.55%		0.4659	0.64212
A 19% decrease based on a market report describing revenue shortfalls (26 July 2018)	AR (–1)	0.16%	α = –0.00067	0.1105	0.91219
	AR (0)	–20.55%	β = 1.33758	–13.7854	**2.41E–26***
	AR (1)	0.17%	p = 0.04550	0.1122	0.91083
	AR (2)	–1.38%		–0.9226	0.35808
	AR (3)	0.30%		0.2011	0.84095
Techcrunch reports data leaks affecting 419 million records (04 September 2018)	AR (–1)	–0.97%	α = –0.00135	–0.4274	0.66985
	AR (0)	–2.26%	β = 1.45744	–0.9999	0.31943
	AR (1)	–1.81%	p = 0.43168	–0.8006	0.42495
	AR (2)	–2.15%		–0.9529	0.34260
	AR (3)	0.77%		0.3415	0.73335
Unofficial sources reveal data theft affecting 50 million users (28 September 2018)	AR (–1)	0.80%	α = –0.00074	0.3765	0.70723
	AR (0)	–2.55%	β = 1.45349	–1.2042	0.23091
	AR (1)	–1.69%	p = 0.36474	–0.7971	0.42697
	AR (2)	–1.80%		–0.8496	0.39725
	AR (3)	1.90%		0.8947	0.37276
The ICO imposes a $643.000 penalty for Cambridge Analytica data leakage (24 October 2018)	AR (–1)	0.65%	α = –0.00177	0.3060	0.76013
	AR (0)	–1.28%	β = 1.30940	–0.6037	0.54723
	AR (1)	1.07%	p = 0.55097	0.5039	0.61527
	AR (2)	–1.30%		–0.6145	0.54010
	AR (3)	–1.24%		–0.5873	0.55813
Realised quarterly revenue does not reach estimated quarterly revenue (30 October 2018)	AR (–1)**	–1.32%	α = –0.00161	–0.6275	0.53155
	AR (0)	1.14%	β = 1.21653	0.5397	0.59044
	AR (1)	2.59%	p = 0.27570	1.2296	0.22129
	AR (2)	–1.14%		–0.5431	0.58808
	AR (3)	0.01%		0.0026	0.99796
Facebook appealed to the Court of First Instance (21 November 2018)	AR (–1)	3.18%	α = –0.00147	1.5031	0.13549
	AR (0)	1.54%	β = 1.28986	0.7304	0.46657
	AR (1)	–1.32%	p = 0.16738	–0.6263	0.53234
	AR (2)	1.63%		0.7703	0.44264
	AR (3)	–1.29%		–0.6105	0.54269
Application downtime for all services (14 March 2019)	AR (–1)	–0.09%	α = 0.00074	–0.0510	0.95939
	AR (0)	–1.83%	β = 1.23484	–1.0467	0.29736
	AR (1)	–3.18%	p = 0.45731	–1.8198	0.07132
	AR (2)	–3.91%		–2.2350	**0.02730***
	AR (3)	0.63%		0.3578	0.72114

(*continues*)

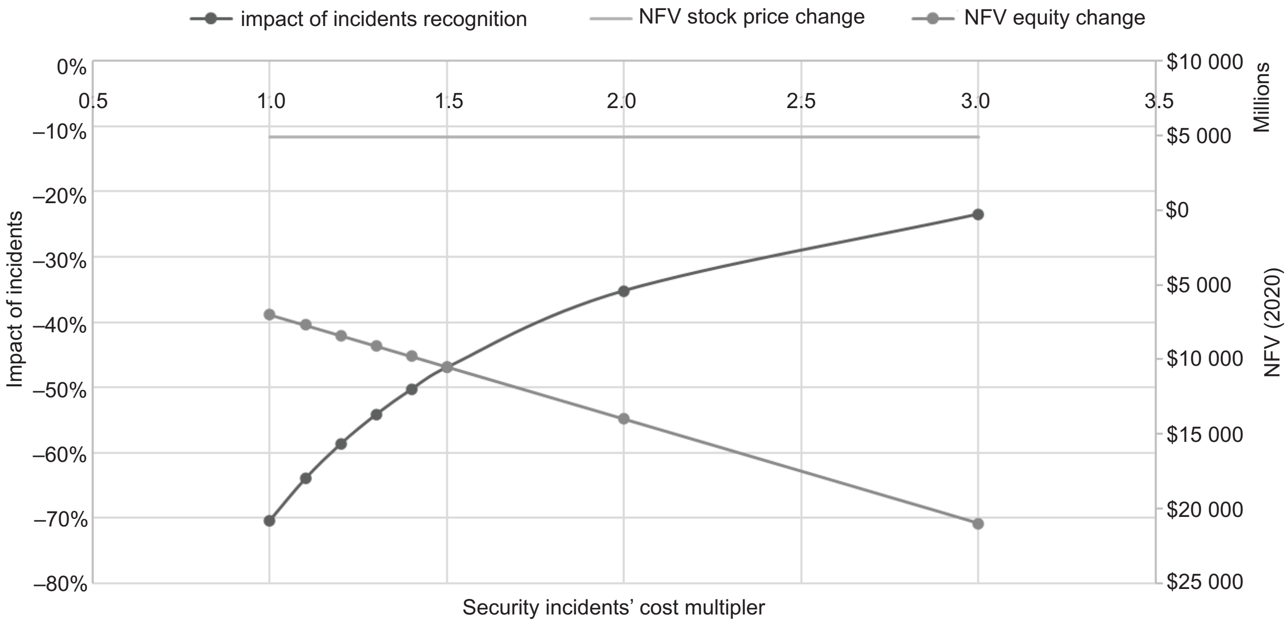
Table 6. Continued

Event	Observation	Abnormal return	Params (α, β, Breusch-Pagan p value)	t stat	p value
Instagram privacy incident reported (25 March 2019)	AR (–1)	1.20%	α = 0.00103 β = 1.22883 p = 0.61060	0.6534	0.51478
	AR (0)	1.18%		0.6435	0.52114
	AR (1)	–0.15%		–0.0821	0.93472
	AR (2)	–0.62%		–0.3365	0.73713
	AR (3)	–0.74%		–0.4020	0.68841
The company reports additional information that aggravates the incident (18 April 2019)	AR (–1)	0.13%	α = 0.00110 β = 1.26832 p = 0.51517	0.0715	0.94315
	AR (0)	–0.59%		–0.3278	0.74362
	AR (1)	1.52%		0.8440	0.40038
	AR (2)	0.06%		0.0307	0.97557
	AR (3)	–0.49%		–0.2704	0.78734
Letter from CEO Mark Zuckerberg on concerns about ”potentially problematic privacy practices” (12 June 2019)	AR (–1)	1.80%	α = 0.00107 β = 1.32723 p = 0.50482	0.9541	0.34200
	AR (0)	–1.57%		–0.8325	0.40679
	AR (1)	0.73%		0.3868	0.69960
	AR (2)**	2.26%		1.1984	0.23317
	AR (3)**	3.92%		2.0784	**0.03984***
In an interlocutory judgment, the General Court ordered the ICO to disclose its decision-making material. (14 June 2019)	AR (–1)**	0.73%	α = 0.00096 β = 1.35376 p = 0.47877	0.3854	0.70067
	AR (0)	2.27%		1.2013	0.23202
	AR (1)	3.93%		2.0739	**0.04026***
	AR (2)	–1.69%		–0.8931	0.37363
	AR (3)	–1.03%		–0.5418	0.58898
The FTC imposes a $5 billion penalty for Cambridge Analytica data leaks (25 June 2019)	AR (–1)	0.87%	α = 0.00100 β = 1.23191 p = 0.37060	0.4581	0.64769
	AR (0)	–0.90%		–0.4692	0.63977
	AR (1)	–0.57%		–0.3009	0.76401
	AR (2)	0.41%		0.2126	0.83203
	AR (3)	1.02%		0.5359	0.59305
The ICO appealed against the interim decision (03 September 2019)	AR (–1)	–0.01%	α = –0.00010 β = 1.18391 p = 0.12823	–0.0074	0.99413
	AR (0)	–0.95%		–0.5810	0.56238
	AR (1)	1.30%		0.7955	0.42793
	AR (2)	0.47%		0.2861	0.77533
	AR (3)	–1.90%		–1.1588	0.24890
Facebook pays the penalty (30 October 2019)	AR (–1)	0.10%	α = –0.00038 β = 1.32352 p = 0.23034	0.0760	0.93957
	AR (0)	–0.95%		–0.7159	0.47549
	AR (1)	2.23%		1.6745	0.09667
	AR (2)	–0.21%		–0.1589	0.87399
	AR (3)	0.12%		0.0869	0.93093
Competition Bureau Canada imposed a 9 million CAD fine for improper privacy practices (19 May 2020)	AR (–1)	–1.90%	α = 0.00124 β = 0.92412 p = 0.81414	–1.1833	0.23908
	AR (0)	2.57%		1.5982	0.11268
	AR (1)	4.21%		2.6221	**0.00989***
	AR (2)	1.21%		0.7555	0.45147
	AR (3)	1.17%		0.7279	0.46809

*The given AR is significant

**The given calculation belongs to another event due to windows’ overlap

Figure 7. The effect of security budget on the *Incidence of incident recognition*.



(1) End users suffering a significant attack on their privacy because of the Cambridge Analytica information security incident in 2016; (2) the Instagram vulnerability and possible data breach; (3) the leakage of 419 million data records; (4) the data theft affecting 50 million users, and (5) downtime affecting all services.

Based on the calculated *Effect of incidents* metric, there were extra cash flows compared to the estimated security budgets that considerably increased the security-related expenditures. In light of this, companies should take extra care to choose the right security control mix and budgeting. However, with regard to the uncertainty around estimating the security budget, we created what-if scenarios in order to analyse lower and higher yearly security budgets, which clearly show that the higher the annual budget, the lower the impact of incidents because the incidents' values remain. On the other hand, with regard to the lower valuation of the incidents' corporate effects, we created what-if scenarios on the incidents' corporate effects which showed that the higher the corporate costs of incidents (in this case via the cost multiplier), the higher the impact of incidents.

The event-study-based analysis of stock prices showed that there were six events with abnormal returns that significantly influenced daily prices. Based on the abnormal returns, comparing the calculated NFVs of stock changes to the equity-related changes showed a deviation between the shareholders' perception and the actual magnitude of the incidents affecting the organisation. The what-if scenarios on the security budget indicated that the higher the security budget, the lower the *Incidence of incident recognition*.

The *Incidence of incident recognition* suggests that investors may have significantly overreacted to the related news. Accordingly, the security incidents apparently affected the company's beta and stock volatility. However, to find out whether these effects are unique for the examined incidents or Meta, it will be necessary to carry out further research. Currently, it is only an assumption that a cyberattack is a considerable non-systematic, diversifiable risk factor for shareholders.

Funding

This work was supported by ERDF project “CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence” (No. CZ.02.1.01 / 0.0 / 0.0 / 16_019 / 0000822); János Bolyai Research Scholarship of the Hungarian Academy of Sciences.

Author Contributions

Conceptualization, Z.B. and T.S.; methodology, Z.B. and T.S.; Formal analysis, Z.B.; Writing-original draft preparation, Z.B.; Writing-review and editing, T.S.; Supervision, T.S.; Project administration, T.S.; Funding acquisition, T.S. All authors read and agreed to the published version of the manuscript.

Data Availability Statement

The data presented in this study is openly available in Open Science Foundation at 10.17605/OSF.IO/ZEM8Y, reference number ZEM8Y.

Disclosure statement

No potential conflict of interest was reported by the authors.

References

Ahn, J.H. (2016) ‘The impact of the banking competition in funding and lending markets on lending technology’, *Revue Economique*, 67(6), pp. 1117–1139. doi: 10.3917/reco.pr2.0069.

Armitage, S. (1995) ‘Event study methods and evidence on their performance’, *Journal of Economic Surveys*, 9(1), pp. 25–52. doi: 10.1111/j.1467-6419.1995.tb00109.x.

Beccarini, A. (2007) ‘Investment sensitivity to interest rates in an uncertain context: is a positive relationship possible?’, *Economic Change and Restructuring*, 40(3), pp. 223–234. doi: 10.1007/s10644-007-9025-1.

Breusch, T.S. and Pagan, A.R. (1979) ‘A simple test for heteroscedasticity and random coefficient variation’, *Econometrica*, 47(5), p. 1287. doi: 10.2307/1911963.

Brotby, W.K. (2009) *Information security management metrics*. New York, NY: Auerbach Publications.

Business Insider (2018) *Facebook just announced it was hacked, and almost 50 million users have been affected.* Available at: https://www.businessinsider.com.au/facebook-security-attack-affecting-50-million-users-2018-9 (Accessed: 2 January 2023).

Business Insider (2019) *Facebook understood how dangerous the Trump-linked data firm Cambridge Analytica could be much earlier than it previously said. Here's everything that's happened up until now.* Available at: https://www.businessinsider.com/cambridge-analytica-a-guide-to-the-trump-linked-data-firm-that-harvested-50-million-facebook-profiles-2018-3 (Accessed: 2 January 2020).

CNBC (2018) *Here are the scandals and other incidents that have sent Facebook's share price tanking in 2018*. Available at: https://www.cnbc.com/2018/11/20/facebooks-scandals-in-2018-effect-on-stock.html (Accessed: 6 March 2021).

CNBC (2019) *Facebook stock rises on better-than-expected revenue and earnings.* Available at: https://www.cnbc.com/2019/10/30/facebook-fb-q3-2019-earnings.html (Accessed: 2 January 2023)

Coin News (2021) *Current US inflation rates: 2000–2021*. Available at: https://www.usinflationcalculator.com/inflation/current-inflation-rates/ (Accessed: 6 March 2021).

Competition Bureau Canada (2020) *Facebook to pay $9 million penalty to settle competition bureau concerns about misleading privacy claims*. Available at: https://www.canada.ca/en/competition-bureau/news/2020/05/facebook-to-pay-9-million-penalty-to-settle-competition-bureau-concerns-about-misleading-privacy-claims.html (Accessed: 8 January 2021).

Damodaran, A. (2021) *Historical returns on stocks, bonds and bills: 1928–2020*. Available at: http://pages.stern.nyu.edu/~adamodar/ (Accessed: 9 July 2021).

Bernard, J., Golden, D. and Nicholson, M. (2020) 'Reshaping the cybersecurity landscape', Deloitte Insights. Deloitte Development LLC. Available at: https://www.fsisac.com/hubfs/DI_2020-FS-ISAC-Cybersecurity.pdf (Accessed 20 March 2021).

Ernst&Young (2020) *How does security evolve from bolted on to built-in?* Available at: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/ey-global-information-security-survey-2020-report-single-pages.pdf (Accessed: 26 September 2020).

Facebook (2017) *Form 10-K 2016*. Available at: https://investor.fb.com/financials/?section=annualreports (Accessed: 6 March 2021).

Facebook (2018) *Form 10-K 2017*. Available at: https://investor.fb.com/financials/?section=annualreports (Accessed: 6 March 2021).

Facebook (2019a) *Form 10-K 2018*. Available at: https://investor.fb.com/financials/?section=annualreports (Accessed: 6 March 2021).

Facebook (2019b) *FTC agreement brings rigorous new standards for protecting your privacy*. Available at: https://about.fb.com/news/2019/07/ftc-agreement/ (Accessed: 8 November 2020).

Facebook (2019c) *Keeping passwords secure*. Available at: https://about.fb.com/news/2019/03/keeping-passwords-secure/ (Accessed: 10 August 2020).

Facebook (2020) *Form 10-K 2019*. Available at: https://investor.fb.com/financials/?section=annualreports (Accessed: 6 March 2021).

Facebook (2021) *Form 10-K 2020*. Available at: https://investor.fb.com/financials/?section=annualreports (Accessed: 6 March 2021).

Federal Reserve Bank of St. Louis (2021) *Interest Rates, Government Securities, Government Bonds for United States*. Available at: https://fred.stlouisfed.org/series/INTGSBUSM193N# (Accessed: 01 February 2023).

Federal Trade Commission (2019) *FTC imposes $5 billion penalty and sweeping new privacy restrictions on Facebook*. Available at: https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions (Accessed: 10 August 2020).

Financial Content (2021) *Yahoo (NQ:)*. Available at: https://markets.financialcontent.com/stocks/quote/historical?Symbol=537%3A453745&Year=2018&Range=432&Month=3%0A (Accessed: 7 January 2021).

Flexera (2021) *State of tech spend report*. Available at: https://info.flexera.com/SLO-REPORT-State-of-Tech-Spend (Accessed: 14 March 2021).

de Geest, L.R. and Stranlund, J.K. (2019) 'Defending public goods and common-pool resources', *Journal of Behavioral and Experimental Economics*, 79, pp. 143–154. doi: 10.1016/J.SOCEC.2019.02.006.

Gordon, L.A. and Loeb, M.P. (2002) 'Economic aspects of information security', *ACM Transactions on Information and System Security*, 5(4), pp. 438–457.

Hall, L., Futela, S. and Gupta, D. (2016) *IT key metrics data 2017: key industry measures*, Gartner Research Report.

Hamburgischen Beauftragten für Datenschutz und Informationsfr (2019) *Tätigkeitsbericht datenschutz 2019*. Available at: https://datenschutz-hamburg.de/assets/pdf/28._Taetigkeitsbericht_Datenschutz_2019_HmbBfDI.pdf (Accessed: 6 March 2021).

Information Commissioner's Office (2019) *Statement on an agreement reached between Facebook and the ICO*. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/10/statement-on-an-agreement-reached-between-facebook-and-the-ico (Accessed: 10 August 2020).

International Business Times (2019) *Facebook stock suffers biggest drop of 2019, loses $37B in 4 trading days*. Available at: https://www.ibtimes.com/facebook-stock-suffers-biggest-drop-2019-loses-37b-4-trading-days-2776826 (Accessed: 6 March 2021).

Markets Insider (2019) *Facebook shares drop sharply after unearthed emails reportedly show Mark Zuckerberg is aware of "problematic privacy practices" (FB)*. Available at: https://markets.businessinsider.com/news/stocks/facebook-stock-price-reaction-to-zuckerberg-reportedly-aware-privacy-issues-2019-6-1028274446 (Accessed: 1 March 2021).

MarketWatch (2018) *Facebook stock drops roughly 20%, loses $120 billion in value after warning that revenue growth will take a hit*. Available at: https://www.marketwatch.com/story/facebook-stock-crushed-after-revenue-user-growth-miss-2018-07-25 (Accessed: 6 March 2021).

MSCI (2021) *MSCI ACWI index (USD)*. Available at: https://www.msci.com/documents/10199/8d97d244-4685-4200-a24c-3e2942e3adeb (Accessed: 7 January 2021).

Olovsson, T. (1992) *A structured approach to computer security, Chalmers University of Technology, Gothenburg*. Gothenburg: Chalmers University of Technology.

Rabin, M. (1998) 'Psychology and economics', *Journal of Economic Literature*, 36(1), pp. 11–46.

Roettgers, J. (2019) 'Mark Zuckerberg says Facebook will spend more than $3.7 billion on safety, security in 2019', *Variety*, 5 February. Available at https://variety.com/2019/digital/news/facebook-2019-safety-speding-1203128797/ (Accessed: 6 March 2021)

Romanosky, S. (2016) 'Examining the costs and causes of cyber incidents', *Journal of Cybersecurity*, 2(2), pp. 121–135. doi: 10.1093/cybsec/tyw001.

Ruan, K. (2017) 'Introducing cybernomics: a unifying economic framework for measuring cyber risk', *Computers and Security*, 65, pp. 77–89. doi: 10.1016/j.cose.2016.10.009.

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. doi: 10.1111/j.1540-6261.1964.tb02865.x.

Sklavos, N. and Souras, P. (2006) 'Economic models and approaches in information security for computer networks', *International Journal of Network Security*, 2(1), pp. 14–20.

Statista (2022) *IT budgets & investments*. Available at: https://www.statista.com/study/71560/it-budgets-and-investments/ (Accessed: 1 February 2023).

Sun, W., Ding, Z. and Xu, X. (2021) 'A new look at returns of information technology: firms' diversification to IT service market and firm value', *Information Technology and Management*, 22(1), pp 13–31. doi: 10.1007/s10799-021-00322-y.

Techcrunch (2019) 'A huge database of Facebook users' phone numbers found online', 4 September.

The Verge (2019) 'Facebook, Instagram, and WhatsApp are still down for some users around the world', 13 March.

Tsvetanov, T. and Slaria, S. (2021) 'The effect of the Colonial Pipeline shutdown on gasoline prices', *Economics Letters*, 209, p. 110122. doi: 10.1016/J.ECONLET.2021.110122.

Tversky, A. and Kahneman, D. (1981) 'The framing of decisions and the psychology of choice', *Science*, 211(4481), pp. 453–458. doi: 10.1126/science.7455683.

Wheeler, E. (2011) *Security risk management*. Syngress. doi: 10.1016/C2010-0-64926-1.

Yahoo! Finance (2021) *S&P 500 (^GSPC)*. Available at: https://finance.yahoo.com/quote/%5EGSPC/history?p=%5EGSPC%0A (Accessed: 7 January 2021).