[Albert Carlson, Benjamin Williams et al. (May 28, 2025). Identifying the Factors in Reporting the Cost of a Hack. 2025 IEEE World AI IoT Congress (AIIoT), IEEE Xplore. Source: https://ieeexplore.ieee.org/document/11105291]

Identifying the Factors in Reporting the Cost of a Hack

Albert Carlson*, **Benjamin J Williams**†, **Sai Ranganath Mikkilineni**‡, **1st Lieutenant Mandeep Singh**§, **Ariana Carlson**¶

*Chair for Entropy and Encryption, Quantum Security Alliance
†Department of Computer Science, University of Idaho, Moscow, ID, USA
‡College of Business, Delaware State University, Dover, DE, USA
§Technical & Information Support Company, 1st Special Forces Group (Airborne), US Army
¶Independent Researcher
*Email: *ACarlson2@nu.edu*, †*will9847@vandals.uidaho.edu*, ‡*SMikkilineni@desu.edu*,
§*mandeep.singh35.mil@army.mil*, ¶*MikellanStartoucher@gmail.com*

***Abstract*—Cybersecurity professionals often advise their managers and companies about responding to attacks and/or implementing prevention measures. Managers and companies typically base their actions on the cost to the company and the return on investment. However, there has never been a good summary of the expenses incurred by a company from a hacking attack. Cybersecurity professionals cannot adequately inform their managers if they do not have complete information on these costs. Courses educating technical professionals rarely, if ever, address the full spectrum of business issues on the subject. This paper gives a comprehensive picture with a fundamental template of the costs involved so that a professional can fully counsel management and produce defendable estimates for reimbursement from insurance or testify in legal actions.**

***Keywords*—Hacking, Risk analysis, Return on Investment, Cybersecurity insurance.**

I. Introduction

Cybersecurity professionals are responsible for advocating for their companies to invest in cybersecurity measures. Their arguments must encompass both technological and business perspectives. However, the business side of the argument is not taught extensively and lacks a clear framework.

Companies rely heavily on computers and networks in all phases of their operations. Engineering employs computers for design. Other functions, such as purchasing, and sales, which are done online, and accounting functions store and process business and personal data. Information related to all of these functions makes cybersecurity attacks attractive to hackers. Any financial, industrial, and personnel record repository can be stolen and monetized [1]. Whether a person or an organization recognizes the value of that information, the hacker does and will target the data wherever they find it.

Security professionals are often called upon to help an organization report the specifics of an attack once it has occurred, so that an organization can recover costs and prepare the computing and networking environment to better fend off future attacks. Both reports require that the attack's costs be known to recover losses and enable decision-makers to plan defenses and responses to attacks yet to come. Specifically, these reports are required to prepare annual reports to government, regulators, and stockholders, analyze return on investment (ROI) [2] for management so that they can make decisions about cyber protection, answer legal and government inquiries, make insurance claims, and be used for training both management and workers, among other needs.

Every year, the number of cyber attacks grows. In 2024, more than 6.3 trillion intrusion attacks were attempted [3]. Billions more attacks of various types were reported, with more than 59% of all businesses reporting attacks. These numbers are almost certainly below the actual attack numbers, as most companies do not want to admit attacks that can scare customers, suppliers, and affect their stock price [4].

A. In this paper

The aim of this paper is to present an approach for cybersecurity professionals to evaluate and report the costs of a hack when it is required during execution of their normal duties. In this paper

- We use an analysis inspired by the Birthday Paradox [5] to show that an organization will almost certainly be attacked yearly.
- We also present a list of the usual costs incurred by an organization due to a cyberattack.
- We have also provided a framework and template that can be used by cybersecurity professionals when they're tasked with reporting the costs incurred because of a cyber attack.

B. Organization of the Paper

This paper is organized into five sections. The first section is the introduction to the paper, which explains the problem and proposes a solution. Section II is an essential background for the paper that a reader should understand to contextualize the paper. The third section presents the costs of a hack and explains the reasons at a high level for including them in the

979-8-3315-2508-8/25/$31.00 ©2025 IEEE

price of a hack under the heading of actual and intangible costs. Section IV summarizes applying the various categories of hacking costs. The final section gives the conclusions for the paper and addresses future work. An appendix is provided that gives a general outline of a report giving the costs of an attack.

II. Background

Several subjects generally address and frame the problem to justify the subject matter. A systematic treatment of costs and giving examples of valid expenses will allow the cybersecurity professional to decide whether additional costs fit the spirit of inclusion as costs.

A. Risk Analysis

All persons and organizations face risks in their operations. Identifying and minimizing risks is the aim of a field known as “risk analysis" [6]. In this field, all possible risks to the continuation of operations and the maintenance of quality production (or service) are listed, and plans to minimize the effects and sources of the risks are made. Many risks come from inside the organization, but risks may also come from competitors and events that occur in the world.

Actors from outside the organization pose significant risks. This is the case with hackers. Hackers seek to achieve their goals by attacking and taking something from their victims, the target of their attacks. The motivation for those attacks varies and is typically irrelevant to the damage caused to the targets during and after the hacking attack. What is relevant is the attack vector, the equipment or personnel attacked, and the resulting loss (cost) caused by the attack. Risk analysis seeks to identify the attack vector on critical assets/equipment that causes the most damage, then formulate actions taken in the present to prevent losses from that vector.

The cost of an attack is critical to the risk analysis process. Risk is often evaluated in terms of the probable cost of a successful attack over some period of time, such as a year. The expected cost for an attack for that time period (year) must be planned for in order to ensure continued operation. The amount of money that must be covered for continuity is given by

$$expected\_cost = Pr(event) \times cost\_of\_attack \tag{1}$$

where $Pr(event)$ is the probability of an event occurring during the stated time period.

Both the probability of an attack and its costs must be estimated. This paper will focus on compiling the actual costs of the attack when a hack occurs and estimating the cost of a future attack for planning and implementing preventive measures. For a cybersecurity professional advising management, the more accurately and defensibly the cost of a hack is presented, the better the decision that management can make.

B. Probability of an Attack

Cybersecurity attacks (hacks) are almost inevitable over time. Claims that a person or an organization is not interesting

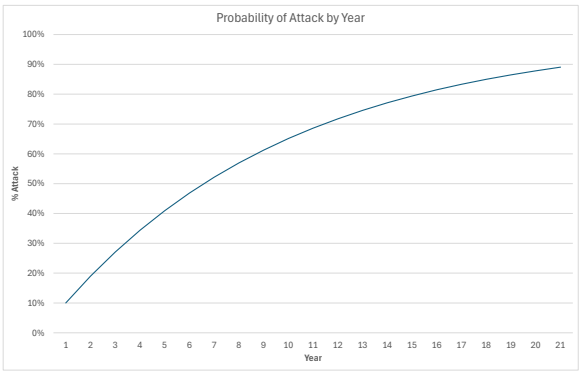

Fig. 1. Chance of Attack, $pr(a) = 10\%$

to hackers can be shown to be wrong [7]–[13]. Consider an attack that occurs once per year, with a probability of attacking a particular target ($pr(a)$) each year. The probability of attack is calculated by

$$Pr(attack) = (1 - Pr_t(a))^y \tag{2}$$

where $Pr_t(a)$ is the probability of that attack over time (year), the chance of being attacked over the years constantly increases and is exponential in shape, with an asymptotic limit of 100%. An organization’s chance of being attacked passes 50% very quickly. Taking the opportunity of an attack at 10% a year, the probability of an attack over time is shown in Figure 1. In year 6, the organization has more than a 50% chance of being attacked using that hack. At $Pr(attack) \geq 50\%$, an attack of that type is likely to occur in the next year. This math characterizes the likelihood of only one kind of attack happening. Unfortunately, organizations face many attacks simultaneously, with the number of attacks increasing annually.

Many attacks can be employed against a person or an organization (target). The mathematics of the probability of attack on an organization changes when the target must defend against more than one attack vector. The likelihood of being hacked at least once is given by $Pr(attack)$ for $n+1$ possible attacks during a period, such as a year, is provided by

$$Pr(attack) = 1 - \left(\overline{Pr(a_0)} \times \overline{Pr(a_1)} \times \ldots \times \overline{Pr(a_n)} \right) \tag{3}$$

$$= 1 - \left(\prod_{i=0}^{n} \overline{Pr(a_i)} \right) \tag{4}$$

$$= 1 - \left(\prod_{i=0}^{n} \left(1 - Pr(a_i) \right) \right) \tag{5}$$

where

$$\overline{Pr(a_i)} = 1 - Pr(a_i) \tag{6}$$

and is defined as the probability of failure to prevent the event a_i. That is, the likelihood of an organization having at least one

cybersecurity attack during a year is one minus the product of not having any attack (an “attack failure") during the same period. This is similar to the analysis used for the well-studied Birthday Paradox problem [5]. As with the birthday problem, considering the possibility of even a small number of possible hacks, the probability of at least one hack in the year is precipitously high. Websites list many types of attacks, often listing the top 12 - 20 software attacks [14], with many versions of these attacks found in the NVD CVSS repository [15]. According to online threat maps, millions of attacks take place daily worldwide [16], [17]. Hacks will happen to any organization, given enough time. That period is constantly constricting.

III. Costs

In assessing the anticipated costs for a period, such as a year, the probable costs relate to the anticipated attacks against a target. A target must be prepared to cover the costs of attacks based on that probability. Costs may be covered by cybersecurity insurance or savings. That amount is calculated by

$$C_{anticipated} = \sum_{i=1}^{n} pr(attack_i) C_a(i) \tag{7}$$

That is the sum of the product of the probability of $attack_i$ and its anticipated cost.

Anticipated costs can be reduced by changing the probability of the attack by employing preventative measures. Those measures reduce the probability of a successful attack from $pr(a_i) \rightarrow pr(a_i)'$ where $pr(a_i) > pr(a_i)'$. The closer $pr(a_i)'$ is to 0 (full prevention), the less money the target can be expected to need to keep on hand to react to a hack.

Costs (losses) are important to quantify because they must be accurately reported for insurance reimbursements (if applicable) and for the organization’s cybersecurity planning. When assembling a report that lists the cost of an attack, a systematic treatment and organization of the losses make it easier to include all relevant costs, ease the auditing and accounting of the incident, and provide a checklist for the person or team assembling the report. A structured and logical approach leads to a defensible treatment of expenses that can be defended under examination. Costs from a hack come from several sources. Costs can be broadly classified into three categories:

1) Direct/Actual Costs (C_a) - These are expenses incurred in responding to and recovering from the hacking attack. Such costs can be directly shown as “out of pocket" costs for the organization. The costs can be calculated to precision and can be anything backed up with a receipt, including but not limited to:
   - The stolen/destroyed money and assets
   - Fines
   - Legal expenses
   - Regulatory expenses
   - Costs for services
   - Personnel costs
2) Indirect/Intangible Costs (C_i) - These are the costs that are not directly attributable to an attack but occur as the result of the attack; they affect the organization, but ledger entries cannot directly prove their amount. Nevertheless, the cost can be estimated/projected, and a monetary loss could be assigned, such as for the loss of goodwill or reputation.
3) Future costs (C_f) - These costs are associated with preventing the same, or similar, attacks from occurring again.

There could be an overlap in the composition of the above costs due to the human factor involved. Based on the above, we can say that the total cost (C_t) incurred from an attack is:

$$C_t = C_a + C_i + C_f \tag{8}$$

A. Actual Costs/Damage (C_a)

One of the significant costs of an intrusive attack (malware in the system) is the actual cost of removal of that software. Removing the code requires that the malware be identified, the location(s) for the code (including copies left by the malware) must be found, the code is removed (or the system is re-imaged), and critical software is reinstalled. This cost is covered in the category of personnel costs (C_p).

During the attack, personnel are often diverted from other tasks to respond to the hack. The personnel diverted from their normal activities do not perform their usual duties. Those duties must then be completed later by the personnel working on the attack, adding the cost of the lost productivity. This cost should be covered under the charged cost of personnel, C_p. If personnel are diverted from producing a product, the loss of the ability to sell that product should also be added to the loss.

Legal costs (C_l) are associated with legal work to protect the organization. These actions include legal measures to prevent attacks and defend against lawsuits for damage incurred by or through the attack. In 2025, these costs typically run from $500 - $1,000 per hour of legal advice and protection.

$$C_a = C_l + C_p \tag{9}$$

1) Stock Cost: One of the critical measures of success for a company is the stock price of the organization and its history. The company’s leaders are also judged by the stock price, which reflects the well-being and performance of the company. Shareholders can replace the management structure and personnel of the company if the stock price falls or if it remains stagnant for a sufficiently long time [18]–[20]. The stock price indicates the confidence of the investor (and the market) in the company, reflecting the well-being and value of the company. Most companies have a value (market capitalization [21]) that is given by the total value of the number of shares multiplied by the price per share. A successful cyber attack can affect the stock value of the target organization [22].

Harvard Business Review [23] reported in 2024 that more than 83% of companies in the US experienced two or more hacking incidents. On average, there was a stock price reduction of 7.5%, with reports of a 5% to 15% loss, depending on the company, circumstances, industry, and whether or not individual customer data was exposed. Stock cost should be calculated as

$$C_{sp} = \Delta_p(n_s) \tag{10}$$

where Δ_p is the loss of price per share and n_s is the number of shares. The drop should be adjusted as needed, but at a minimum,

$$\Delta_p \approx .075(Shareprice) \tag{11}$$

2) Customer Restitution: Data from the Target attack incident of 2014 [24] indicated that up to 70 million credit card accounts were compromised, costing Target $18.5 million, or $3.78 per account. Besides Target, other firms also paid consumer restitution due to failing to prevent cyberattacks from succeeding [25]. This amount should be considered a lower limit for restitution per account number or social security number (C_cr). On average, the price of a successful theft of a customer's identity is $1,170 [26]. Since hackers are willing to pay this amount per identity, this should be assumed to be the minimum return per revealed identity that an organization may have to return if sued for lack of proper security. Many companies offer a year of credit monitoring as the minimal remediation. Annual plans for the service through LifeLock run $12.49 per month, or $149.88 annually [27]. Therefore

$$C_cr \approx n\left(\frac{c}{acct} + C_t\right) \tag{12}$$

where c is the cost per account in settlement, and C_t is the average loss per identity exposed. If no personal identities are exposed, $C_t = 0$.

3) Fines: Some companies are subject to regulatory rules that must be followed to provide sufficient prevention practices to avoid damage from successful cyber attacks [28]. The regulatory agency may be a government or industry governing organization by which the company agrees to be governed under the penalty of fines and prosecution for violations and noncompliance. Those fines (C_{fines}) should be included in the actual cost of loss of the attack, as they can be quantified once imposed by the regulatory agency. Such penalties (for example, HIPAA violation fines [29]) should also be included in future costs if no remediation is taken that would reasonably avoid those fines.

4) Damage to Sales and Advertising: Hacks often cause damage to the customers' view of the company. If that damage is sufficient, the customer may choose to purchase products and/or services from another company to avoid possible problems from downstream use of those products or services. Changing suppliers causes a loss of revenue to the organization until that organization proves its product/services are safe, which can be measured via sales. The way to estimate this actual cost (C_{sl}) is to take the total loss in sales for a period of time (s_l) and subtract the historical loss of sales (s_h) for the same time period. Therefore,

$$C_{sl} = s_l - s_h \tag{13}$$

The loss should be considered to continue until $C_{sl} \approx 0$. Approximating the loss in the future if no measures are taken to stop hacks of the same type should be done for the same period, with the loss adjusted for inflation and expected sales levels.

Compensation for sales loss requires advertising measures to help restore consumer confidence. Properly designed and executed advertising can help minimize sales loss. The advertising costs (C_{ad}) are easily assembled for a hack. The same number can be estimated for the category of future costs.

5) Personnel: C_p comprises the various personnel costs associated with the response to the attack and the costs of responding to the attack in the future. This could include recruiting new talent, and the cost of personnel expended in finding and stopping the attack, including the time and effort.

The cost of responding is the sum of all of the personnel responding to the attack, their rate of pay, and the number of hours spent on the response. Personnel will respond to the attack on all levels. Management must respond to the action, supervisors will direct the response, and individual technicians will work to repulse the attack. Each group of workers can be grouped by their pay rate ($rate_i$) to calculate the actual personnel cost.

$$C_{response} = \sum_{i=1}^{n}(num_i)(rate_i)(hours_i) \tag{14}$$

The same equation can be used to estimate the personnel cost for future prevention operations. If management can project the number of hours needed to plan and set up the environment to prevent future attacks, then that information can be plugged into the proper terms for the cost estimate.

The total cost for response and prevention through personnel (C_{pi}) is also symmetrical in the calculation and is given by,

$$C_{pi} = C_{response} + C_{prevent} \tag{15}$$

Using the above formula allows for separate calculations of response and prevention efforts. While the formulae are generally the same, the data used in the response portion of the calculation will be different than the prevention. If desired, one of the terms can be ignored to create a report that splits the costs for comparing the response and the prevention activities.

6) Product: During attacks, it is sometimes necessary to reallocate personnel and resources away from product manufacturing and shipping to address the attack and its aftermath. Suppose the product is not created and is not available for sale. In that case, revenue may be delayed, creating a loss of actual revenue and the ability to use that money in further

operations. The cost associated with what would have been produced (C_{dp}) is part of the loss. It can be calculated by the difference in actual inventory during normal operations versus what is actually put into inventory during an attack. This amount is given by

$$C_{dp} = (I_n - I_a)P_p \tag{16}$$

Where I_n is the normal inventory, I_a is the inventory during the hacking period, and P_p is the price of the product(s) not manufactured and/or shipped.

7) Actual Cost Summary: The summary of the actual costs for an attack is as follows:

$$C_a = C_l + C_p + C_{sp} + C_{cr} + C_{fines} + C_{pi} + C_{sl} + C_{ad} + C_{dp} \tag{17}$$

B. Intangible Costs (C_i)

1) Damage to Reputation and Name: One of the major intangible costs is the damage to the brand's reputation and name associated with the organization that is/was hacked. Customers and potential customers often give great weight to the brand name and organization behind a product when deciding to buy a service or a product. The higher the confidence shown in the service or product, the more likely that the decision will be to go along with the trends in the market. We can see the following quote as an example of consumers' trust's potency: "No one was ever fired for selecting IBM" [30]. You can replace IBM with any of the popular tech companies like Microsoft and Cisco [31]. Successful hacking attacks and the massive loss of information (corporate or private) undermine that confidence. A sharp drop in confidence due to the attack and the following loss of cash and focus on deliverables to recover from the attack may cause buyers and customers to avoid purchasing from the company, decreasing income to the organization. The organization must estimate the cost of the loss of reputation and name ($C_{r,n}$) and then add it to the cost of intangibles.

2) Loss of Market Share (C_m): As discussed in the reputation section for intangible costs, buyers pay attention to which organizations are preferred by other buyers and might move their business to the most preferred alternative. This move can result in a loss of market share [32]. Market share for the product indicates the highest acceptance and the decisions made by other organizations/competitors. Standards for protocols, data representation, and interoperability come from having the largest market share and acceptance. Loss of market share for a significant period can result in redesigning products as new standards are created to cater to the major players in the technology sector. The redesign means increased design costs and latency for new product introduction. Those costs can only be estimated at the time of an attack.

In addition to the engineering costs, the organization must expend considerable effort to regain its market share. However, those costs are associated with restoring confidence and name recognition. Products and services may have to be discounted to persuade reluctant customers to use those services and products behind, resulting in a loss of income, which is a cost of the attack.

3) Increase in Attacks: A consequence of a successful hack is that the report of that success spurs other hackers to attempt attacks on the target organization. Hackers rate themselves by their credibility, or "cred." The first person who successfully attacks a prime target or executes a new attack gains credibility. Once the attack is made public, other hackers often attempt to repeat it to prove their abilities. It may also be that a successful attack brings monetary return. In either case, one successful attack is often followed by additional attacks until the hack is prevented and the news of its failure is passed around the hacking community. The number of times additional attacks will occur depends on the value of the target to hackers. This cost C_{ia} must be estimated.

4) Summary of Intangible Costs: The amount of intangible costs (C_i) is given by

$$C_i = C_{r,n} + C_m + C_{ia} \tag{18}$$

C. Cost of Future Protection (C_f)

The cost of future protection of an organization and its networks and equipment is a topic of considerable interest and discussion. Once a successful attack has been executed, an attacker is more likely to return to the same target and repeat the attack. The word of the attack and its results is often spread in the hacking community, resulting in additional attacks from those who seek to enhance their credibility and add to their hacking resume. Script kiddies [33] will also take notice and seek to replay the same attack. Therefore, protecting the system against these additional anticipated attacks becomes essential.

The first cost is a personnel cost: research. However, this research is not limited to how long it takes to complete. From the point of the attack, there are two phases of research:

- Phase one is spread across the time from recognizing the attack until a method of breaking the attack is found and implemented. During this phase, a majority of the team of responders is expended in finding the proper response to stop the attack.
- After an effective response has been implemented, phase two is entered. Regular but infrequent research is needed to ensure that proper preventive programs and measures are in place if another attack occurs. The amount of time used in research activities is minimal compared to the original research. Phase II research is often restricted to annual or semi-annual reviews.

Personnel time will also be spent creating and maintaining cybersecurity policies and procedures. Policies and procedures are required by many regulatory agencies, as well as industry groups [34]. Policies are documents created and maintained at the corporate level that say what an organization will do. Procedures give instructions for how the policy will be implemented. If policies and procedures are not already in place, time and effort must be expended in creating them. In addition to that, policies and procedures must be regularly

reviewed and updated. Standard intervals for review and updating typically vary from 1 - 5 years and involve an entire committee of subject matter experts (SMEs), support personnel, and managers.

Future protection also relies on performing the maintenance required to keep the system up to date with preventive measures. One irregular but vital task is patch management when software updates become available. Each time the environment changes, including the operational software, new vulnerabilities and avenues for attack also become available. The user must assume that the same attack is possible if the security updates are not installed. Personnel time and cost are expended in this action.

Similarly, diagnostic and preventive system scans must be run periodically. This activity allows the users to ensure that information remains intact and correct, or find potential threats. These actions can be scheduled, and the impact on costs can be minimized but still accounted for.

Remediation plans may involve the use of new networking and computer equipment. This may be the result of the attack or the result of changes in the network and computers installed on that network. Such equipment should be allocated to future actual costs based on the present price of the anticipated equipment needed. Projections of such expenses should only be near-term because the uncertainty increases quickly with increasing time from the present. Hardware is not the only new equipment that may be required. Software may also be required to respond to an attack and prevent future attacks. Software costs should include the purchase price of the program, as well as the annual fees for program maintenance.

IV. Applying Costs

If the actual and intangible costs are segregated from the future costs, then ROI can be estimated. That is, a comparison will be made between the two. If $C_a + C_i \geq C_f$, then spending the money for the prevention of the attack is indicated by the ROI. That cost can be spread across several years [35] or delegated to escrow (or savings) to recover from an attack.

V. Conclusions and Future work

Cyber attacks are now a fact of life. Even a low-probability hack will be attempted against a company, given enough time. However, there are many different attack vectors. Using an analysis similar to that applied to the Birthday paradox, it can be shown that any organization will almost certainly be attacked every year. Millions of attacks take place every day, worldwide. Fighting, recovering from, and protecting against hacks becomes essential for any organization.

Cybersecurity professionals are often called upon to estimate the costs of a hacking attack on an organization. However, their training does not often show them how to make such an estimate. They must rely on their experience to complete that report to their management. Completing that report requires interaction with other departments and personnel, but the cyber professional must know the information needed to assess the loss accurately. A template of those costs is necessary to standardize reports, include the proper costs for insurance recovery, and determine how to fortify the organization from attack.

Another important task often assigned to cybersecurity personnel is hardening an organization against attacks, if appropriate. Deciding on a course of action depends on accurately forecasting costs and applying risk analysis principles. Without knowledge of what costs, both actual and intangible, are likely to be encountered in an attack, the decision will often be erroneous. It may result in severe damage to the organization.

In response to this need and the lack of generally available templates for calculating the costs of a hacking attack, one has been presented with reasoning for each item. Proofs have also been included to assist the cyber professional in supporting the need for preventive measures. The costs have also been listed using formulae to make them easily calculable.

This paper presents a list of normal costs for a hacking incident. Each attack is unique and may include other costs that the authors did not anticipate. New items that should be included in costs need to be investigated and added to the list under the appropriate category of costs. If necessary, new categories of costs should also be added.

A part of the future actions that need to be taken involves collaborating with accounting, legal, insurance, and business personnel to determine the evidence required to support the costs and to establish an acceptable report format, including worksheets. If possible, these should be standardized and distributed for use. Additionally, we can focus on identifying how the factors we discussed would interact with each other and the impact of these interactions on the cost of a hack. We can also delve deeper than merely citing relevant cybersecurity incidents and examine them in more detail to enrich the model of hack costs.

Appendix

A simple template for the financial data that should be reported on for an attack. This template is really just an outline with guidance for the section, leaving the detail to the person documenting the attack. Either a report of an actual event or the estimation of what an event will cost can be documented in this way.

I. Organization Information
   Name, address, and contact information of the Organization
   Date of report
   Date, time, and detailed description of the event
   Contact information of the insurer

II. Direct Costs - Itemize all direct costs with justification of why each is listed. At the end of the section a subtotal of the section is presented.

III. Indirect Costs - Itemize each indirect cost. Justify why each is listed and show the calculations for arriving at the amount. The section ends with a subtotal of costs.

IV. Regulatory Costs and Details - All regulatory costs, along with justification for the costs are listed. Again, the section ends with a subtotal of costs.

V. Summary - All of the subtotals are added together with a final cost presented. Conclusions about the attack are reported here.

VI. Receipts - A copy of each receipt is presented, along with the source of the receipt as evidence of the material used in the calculations.

REFERENCES

[1] Office of the Attorney General-California Department of Justice. Search data security breaches. https://oag.ca.gov/privacy/databreach/list. [Online; accessed 21-March-2025].

[2] George T. Friedlob and Franklin J. Plewa Jr. *Understanding Return on Investment*. john Wiley and Sons, 1^{st} edition.

[3] James Martin. How many cyber attacks occur each day? (2024). https://explodingtopics.com/blog/cybersecurity-stats.

[4] Josh Breaker-Rolfe. The relation between breaches and stock price drops. https://www.tripwire.com/state-of-security/relation-between-breaches-and-stock-price-drops, 2024. [Online; accessed 6-March-2025].

[5] E. H. McKinney. Generalized birthday problem. *The American Mathematical Monthly*, 73(4):385–387, 1966.

[6] Thomas L. Norman. *Risk Analysis and Security Countermeasure Selection*. CRC Press, 2^{nd} edition.

[7] Bert Kondruss. Cyber attack news today 2025/2024 – cyber attack map, recent attacks, and statistics: Us, canada, uk, australia, new zealand around the world. https://konbriefing.com/en-topics/cyber-attacks.html. [Online; accessed 21-March-2025].

[8] CSIS-Center for Strategic and International Studies. Significant cyber incidents. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents. [Online; accessed 21-March-2025].

[9] Charles Harry and Nancy Gallagher. *The Elgar Companion to Digital Transformation, Artificial Intelligence, and Innovation in the Economy, Society, and Democracy*, chapter Categorizing Cyber Effects, pages 7–32. Edward Elgar Publishing, 2023.

[10] C Harry and N Gallagher. Classifying cyber events: A proposed taxonomy. *Journal of Information Warfare*, 17(3):17–31, 2018.

[11] Cybersecurity Ventures. Cybercrime magazine: Who's hacked? latest data breaches and cyberattacks. https://cybersecurityventures.com/intrusion-daily-cyber-threat-alert/. [Online; accessed 21-March-2025].

[12] Town of Hempstead, Long island, NY. Famous phishing incidents from history. https://www.hempsteadny.gov/635/Famous-Phishing-Incidents-from-History. [Online; accessed 21-March-2025].

[13] Charles Griffiths. The latest 2025 phishing statistics (updated january 2025). https://aag-it.com/the-latest-phishing-statistics/, 2025. [Online; accessed 21-March-2025].

[14] Fortinet. Top 20 most common types of cyber attacks | fortinet. https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks.

[15] National Institute of Standards and Testing (NIST) National Vulnerability Database (NVD). Nvd - search. https://nvd.nist.gov/search.

[16] Check Point. Live cyber threat map | check point. https://threatmap.checkpoint.com/.

[17] ThreatLabZ. Zscaler | threatlabz. https://threatlabz.zscaler.com/cloud-insights/threat-map-dashboard.

[18] Bruce Gill. 23andme is falling apart. https://www.yahoo.com/tech/23andme-falling-apart-204700692.html, 2024. [Online; accessed 6-March-2025].

[19] Noah Barsky. 23andme taps 'founder mode' after 99.9% stock plunge and board exit. https://www.forbes.com/sites/noahbarsky/2024/10/21/23andme-taps-founder-mode-after-999-stock-plunge-and-board-exit/, 2024. [Online; accessed 6-March-2025].

[20] Bhanvi Satija, Anushadevan Shah, and Surbhi Misra. Dna testing firm 23andme files for bankruptcy as demand dries up. https://www.reuters.com/business/healthcare-pharmaceuticals/dna-testing-firm-23andme-files-chapter-11-bankruptcy-sell-itself-2025-03-24/. [Online; accessed 28-March-2025].

[21] John R. Graham, Scott B. Smart, and William J. Megginson. *Corporate Finance*. Cengage Learning, 3^{rd} edition.

[22] Kristin Masuch, Maike Greve, Simon Trang, and Lutz M. Kolbe. Apologize or justify? examining the impact of data breach response actions on stock value of affected companies? *Computers Security*, 112:102 – 502, 2022.

[23] Keman Huang, Xiaoqing Wang, William Wei, and Stuart Madnick. The devastating business impacts of a cyber breach. *Harvard Buisiness Review*. https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach.

[24] Chuck Brooks. The target breach 10 years later. https://www.securityinfowatch.com/retail/article/53098895/the-target-breach-10-years-later.

[25] Michael Hill and Lynn Greiner. What is the cost of a data breach? https://www.csoonline.com/article/567697/what-is-the-cost-of-a-data-breach-3.html, 2024. [Online; accessed 7-March-2025].

[26] John Brandon. Your online identity sells for exactly $1,170 on the dark web – here's how to block the sale, 2018.

[27] LifeLock. Lifelock prices and enrollment | lifelock. https://lifelock.norton.com/offer.

[28] Critical infrastructure protection standards, phase ii, http://www.nerc.com/filez/standards/project_2008-06_cyber_security_phaseii_standards.html, April 2011.

[29] The HIPAA Journal. Hipaa violation fines. https://www.hipaajournal.com/hipaa-violation-fines/. [Online; accessed 7-March-2025].

[30] Guy Melamed. "nobody gets fired for buying ibm". https://www.finextra.com/blogposting/26205/nobody-gets-fired-for-buying-ibm, 2024. [Online; accessed 7-March-2025].

[31] Origina. Nobody ever got fired for buying ibm (and other too-safe thinking). https://www.origina.com/blog/nobody-ever-got-fired-for-buying-ibm, 2023. [Online; accessed 7-March-2025].

[32] Shinichi Kamiya, Jun-Koo Kang, Jungmin Kim, Andreas Milidonis, and René M Stulz. What is the impact of successful cyberattacks on target firms? Working Paper 24409, National Bureau of Economic Research, March 2018.

[33] Saliha Figen Arifgoğlu. Information security, privacy issues and an application. Master's thesis, Middle East Technical University, 1988.

[34] North American Electric Reliability Corporation (NERC). Cip-003 cyber security - security management controls. http://www.nerc.com/files/CIP-0031.pdf.

[35] Albert Carlson, Benjamin Williams, and Sai Ranganath Mikkilineni. Is everlasting security necessary? In *2024 IEEE 15th Annual Ubiquitous Computing, Electronics Mobile Communication Conference (UEMCON)*, pages 0563–0569, 2024.