[ Albert Carlson, Benjamin Williams et al. (Oct. 17, 2024). Is Everlasting Security Necessary? 2024 IEEE 15th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), IEEE Xplore. Source: https://ieeexplore.ieee.org/document/10754715 ]

# Is Everlasting Security Necessary?

**Albert Carlson**[*], **Benjamin Williams**[†], **Sai Ranganath Mikkilineni**[‡].

[*]Chair for Entropy and Encryption, Quantum Security Alliance &
Computer Science Department, Austin Community College, Austin, TX, USA
[†]Department of Computer Science, University of Idaho, Moscow, ID, USA
[‡]College of Business, Delaware State University, Dover, DE, USA
*Email: [*]albert.carlson@austincc.edu, [†]will9847@vandals.uidaho.edu, [‡]SMikkilineni@desu.edu*

***Abstract*—Security professionals are now part of the risk analysis and business team. Businesses and organizations must protect the valuable information they use in conducting their core functions. Loss or compromise of that information can damage the organization up to and including bankruptcy. A survey and projections report by a cybersecurity firm estimated that 75% of companies based in the US are prone to cyber-attacks. Also, the revenue loss by vulnerable companies due to cyber-attacks may exceed 452 billion dollars in 2024. Most businesspeople are not well versed in cybersecurity and protecting information, but they understand profits, loss, return on investment, loss prevention, and the math behind them. Often, security is seen as a loss center, making it difficult for security personnel to justify taking measures to safeguard information or information-carrying equipment and networks. Encryption is one example of such vital but ethereal costs. Convincing the business side of operations to implement security requires speaking their language. This paper suggests a way to present encryption in a provably cost-effective manner related to return on investment. Simultaneously, an outline of a strategically adaptive approach to security is introduced.**

## I. Introduction

### A. The Question

How long does a message (i.e., information) need to remain secret? In physical security, it is generally well understood that security is a trade-off, almost a form of insurance. It is never necessary to spend more on security than the cost that would be incurred by a breach [1]. Instead, some percentage of the value of the asset being secured should be spent on security. The specific percentage spent depends on risk assessment. A person might not lock up a bike in a very safe neighborhood, while in a more dangerous neighborhood, it might be kept in a closed garage or be attached to a structure with an expensive lock. Likewise, if an asset is at high risk for an attack, more should be spent on security to protect it from attacks. Fewer and less intense measures are acceptable if it is a low risk. A commonly repeated rule of thumb for physical security spending with low to moderate risk is that it should cost 10% of the value of the asset being secured [2]. This number refers to the net liability, not just the market value of the protected equipment. Therefore, if an asset can cause a million dollars worth of harm if compromised, it should be valued at market value plus one million dollars in liability. Calculating the total value for protection is similar to how car insurance plans require liability insurance to be estimated. The owner might care more about insuring their car's replacement value, but the liability is too significant to ignore.

Kiteworks, a cybersecurity company, publishes a yearly survey and projections report regarding cybersecurity vulnerabilities in businesses, cyberattacks, and revenue losses. Their 2024 report stated that 75% of US-based companies are vulnerable to cyber-attacks and estimated that their revenue loss due to cyberattacks will exceed 452 billion dollars in 2024. They also estimated that the global income loss due to cyberattacks would reach 9.22 trillion dollars in 2024 and are projected to soar to 13.82 trillion dollars by 2028 [3]–[5]. The International Monetary Fund (IMF) also stated that cyber threats are a "Near-Term Risk" that could destabilize the Global Economy [6], [7].

Digital security is often handled much less thoughtfully. Instead of mathematically calculated expectations based on risk analysis and time-varying information value, digital security is primarily managed by intuition; it defaults to the advice of various experts in the field. There are very few specialists with deep training in cryptography. Even banks have few or no specialists in charge of digital security. Each transmitted message is unique in content, and the circumstances surrounding a message's data differ. No expert can address these differences in a one-size-fits-all pronouncement. This is why even major companies with extensive liability experience frequent security breaches of high-value private data.

For digital security to mature and live up to its potential, there must be a fundamental change in how providers and clients think about encryption. Changing the perspective from all information must be protected in perpetuity to the view of matching the encryption based on the value of the information in the message will require a different outlook on the encryption process. The foundation for such thinking requires a training period to familiarize users with the math and philosophy of the new practices. The perspective change begins with the premise that no security is perfect. Therefore, the goal should be establishing sufficient rather than ideal security (i.e., everlasting security).

### B. Scope of the Paper

In this paper, we will discuss the real-world security needs of encryption based on the value of the information and its subsequent decline, answering how long an encrypted message

must resist unauthorized decryption to be sufficiently secure. The paper also discusses how to achieve the necessary level of security and includes some of the problems regularly encountered. However, this paper does not address how to quantify the value of information and its subsequent decline.

### C. Composition of the Paper

Section II presents the essential background information, such as the mathematics of passwords and their relationship to encryption keys, everlasting security, return on investment, and engineering efficiency. Section III analyzes this data, with conclusions and future work presented in Section IV.

## II. Background

Understanding how to calculate the time that a message must remain secure means having a basic knowledge of several subjects. Among them are:

- How brute-force attacks [8] work,
- Heuristic reduction of key spaces,
- Risk analysis, and
- Time-varying value of information.

These concepts are crucial to understanding the need to conserve resources while maintaining appropriately strong security.

### A. Passwords

Breaking a cipher is very similar to breaking a password, given that the user knows the user ID associated with it. It is known that there is one attack that always eventually works to break a password - the brute-force attack [8]–[10]. In a brute-force attack, a password is selected randomly and tested for validity when paired with a target user ID; this process is repeated until the valid password for the user ID is found (the password is cracked). When a random selection of a password is made, and that password is tested, the number of passwords that must be attempted on average ($|K_{avg}|$) before finding the valid password is given by

$$|K_{avg}| = \frac{|K|}{2} \tag{1}$$

where the possible number of passwords in the keyspace is $|K|$. Assuming that the time it takes to verify whether or not a password works is $t_t$, then the average time a password is safe ($t_{secret}$) from cracking is

$$t_{secret} \approx \frac{t_t|K|}{2} \tag{2}$$

To ensure that the key space is sufficiently large to maintain secrecy for the desired period, the password space is increased to allow a variable number of characters required in the password, and it does not restrict the largest password size. Assume that the password requires a minimum of $c_l$ characters and has a practical limit of $c_m$ characters where $c_l < c_m$. Also, assume that the size of the alphabet for the password is $|A|$. Then, the number of passwords ($|K|$) can be written in terms of password size as

$$t_{secret} \approx \frac{t_t \sum_{i=c_l}^{c_m} i^{|A|}}{2} \tag{3}$$

The time $t_{secret}$ can be shorter than what is considered safe by administrators, so a safety factor ($s \geq 1$) is introduced to keep the amount of time attackers have to work on the problem longer than the time a password needs to be valid. Therefore, the time a password is valid/safe ($t_{secret}$) is decreased to

$$t_{secret} \approx \frac{t_t \sum_{i=c_l}^{c_m} i^{|A|}}{2s} \tag{4}$$

Here, the safety factor ($s$) is inversely proportional to the time the password is valid/safe ($t_{secret}$) because the attack discussed here is brute in nature (i.e., brute-force attack), where the risk of a password match during the attack increases as the time of the attack increases. Thus, the time of password validity ($t_{secret}$) is inversely proportional to the safety factor ($s$).

Most cybersecurity practitioners are aware of the relationship between passwords and keys. Both passwords and keys allow for access to information and/or resources. Each also depends on keeping the password/key information secret such that they are only known to the user and anyone authorized to view the password-secured/key-encrypted information. Both passwords and keys can be guessed using brute-force attacks, often accelerated by rainbow tables [11]. The primary difference between passwords and encryption keys is that keys are used to encrypt data, and passwords are encrypted using hashes. However, the analysis for passwords can be directly applied to keys.

### B. Risk Analysis and Return on Investment

In the insurance language, a “risk" is an object being protected, or it can be an unforeseen event [12]. Both meanings can be applied in the study of cybersecurity. Risk evaluation can be the evaluation of the state of the target organization. It can also be an evaluation of an event that may occur and the ramifications of that event to the organization. For this study, risk will be applied to an event, specifically, information loss during transmission due to a cyberattack, and that risk will be reduced through encryption.

An organization must always assume that its information is of interest to some attacker. Denying this fact is sometimes used to avoid paying for security because security is often seen as a cost with no return. That reasoning can be shown to be false. Assume that the chance of an attack is $c\%$ per unit of time, a year, for example. Therefore, the chance of keeping something safe over that time is $(1-c)\%$. For $n$ consecutive periods, the chance of avoiding an attack is $c_a$ and is given by

$$c_a = (1-c)^n \tag{5}$$

The answer to this equation will converge on 0% as $n \to \infty$. Conversely, an organization’s chance of being attacked is $(1 - c_a)$, as shown in Figure 1. Eventually, a cyberattack will occur. Therefore, the risk of an attack will reach 100% over time -

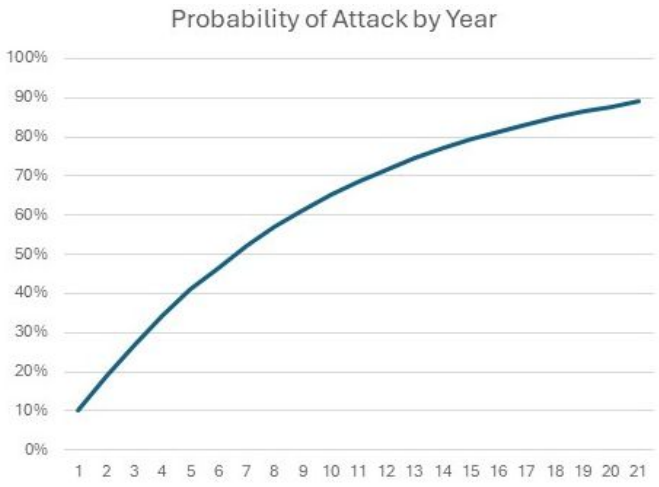


Fig. 1. Probability of an Attack at 10% Chance per Year

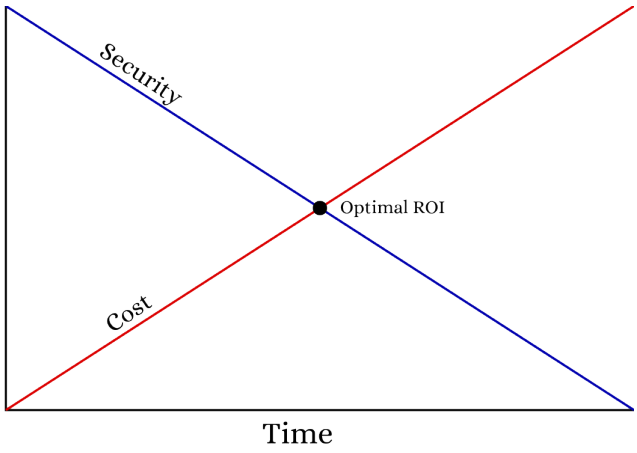


Fig. 2. Optimal ROI

the attack will come, which demonstrates that an organization being of interest to no one is a myth.

In 2017, Cloudflare estimated that from 4% - 10% of all network transmissions are intercepted [13]. This includes encrypted messages. In the intervening seven years, that number has almost certainly increased. Each message intercepted is a cybersecurity attack. Therefore, in Figure 1, the increasing chance of a message being intercepted is entirely plausible.

While this math proves that an attack is inevitable, it is not proof that it will succeed. However, if one attack is inevitable and an attack (irrespective of the success of the attack) does not automatically prevent future attacks, infinite attacks are inevitable over infinite time. Therefore, if it is possible for an attack to succeed, given enough time, that attack will eventually succeed. A successful attack will not necessarily cause damage, though, especially if the information is sufficiently old and no longer holds any of the value or liability it originally had.

Return on Investment (ROI) [14] is the measure of how much is earned for a given amount of money invested in a project. Business leaders often make decisions on whether or not to approve a project based on its profitable return. A deceptively simple formula calculates the ROI ratio:

$$ROI = \frac{Return - Cost}{Cost} \tag{6}$$

The numerator ($Return - Cost$) signifies the Net Return on Investment. For simplicity of the argument in this paper, we will consider ROI to be just about the Net ROI instead of the above ratio. Therefore, for the remainder of this paper, ROI will be considered to be defined by

$$ROI = Return - Cost \tag{7}$$

Returns can be sales or savings in product materials and process costs. For security, the return term depends on how much is spent to avoid the loss related to an attack. This term will encompass both direct costs and opportunity costs associated with the loss of the money needed to pay for the aftermath of the damage done by a successful attack (“loss prevention") [15]. Individual components of the return include but are not limited to damage to equipment, loss of sales/revenue, loss of work, cost of personnel, replacement costs, legal fees, fines, liability costs, and reimbursement costs to suppliers and customers that do not occur because the attack is unsuccessful due to appropriate security in place.

$$R = \sum_{i=1}^{n} r_i \tag{8}$$

In the security model, the cost portion of the formula refers to the amount spent to implement the desired security. These costs include personnel, equipment, licenses, fees, and opportunity costs for channeling resources to prevention programs rather than the organization’s core focus. The cost term resembles the return formula and is given by

$$C = \sum_{i=1}^{n} c_i \tag{9}$$

Resulting in the general formula

$$ROI = R - C = \sum_{i=1}^{n} r_i - \sum_{j=1}^{m} c_j \tag{10}$$

Here, we define the optimal ROI, which is shown at the point where diminishing security over time and increasing net cost of security as required duration increases meet, in Figure 2. The goal is to determine where this crossing point is, based on the value and liability of the data being protected and the risk of attack. ROI is maximized by avoiding paying for security that is stronger than necessary to keep the data safe for as long as it retains value and liability, which makes it easier to justify security. If the boss cannot see a positive ROI, then it is unlikely that security will be implemented appropriately, if implemented at all. As a well-established business axiom says, "We cannot afford to be without adequate protection" [16].

As seen in Figure 1, the probability of an attack happening increases as the time an asset retains value increases. Given enough time, an asset of static value will eventually experience an attack. Figure 2 illustrates how net security at a given price point diminishes over time due to the ever-increasing probability of an attack as time passes. It also describes how the security cost scales with the time it needs to be maintained[1]. For example, security that only needs to keep a particular piece of data safe for a week does not need to be strong and thus can be very inexpensive.

In contrast, security that needs to last tens of years must be robust and will thus be quite expensive. For example, multi-factor authentication codes sent by email are typically only valid for a few to tens of minutes. Given a code that is only valid for 10 minutes, any encryption that takes longer than 10 minutes to break is sufficient because the code no longer has any value once those 10 minutes have passed. Many cryptographic algorithms are considered broken or weak, but they are acceptable for this use case.

Figure 2 is the generic optimization graph for ROI in digital security. It resembles every microeconomics textbook's generic supply and demand optimization graph. The intent of security is loss prevention. Unsecured data that holds significant value (either positive value that an attacker could exploit to divert profits or negative value that an attacker could exploit to cause harm) is a liability to the company or organization. The measure of ROI (see Equation 10) in digital security indicates when the potential loss a successful attack could cause is equal to, or exceeds, the cost of the security to keep an attack from being successful. Because time is a significant factor, it is insufficient to merely pick an acceptable percentage of the liability and spend that on security. The longer the data needs to remain secure, the better the security needs to be, and the more that security will cost. Optimal ROI is a function that is not just about liability and security costs but also about diminishing security over time. Figure 2 illustrates this with a crossing point, similar to the supply and demand crossing point as a function of price in a supply and demand graph. Before the crossing point, strong security can be obtained very cheaply, but the security has high odds of failure before the value and liability of the data have expired. Beyond the crossing point, even the best security will no longer be worth the premium cost. As with supply and demand, this crossing point depends on situation-specific variable factors. This must be assessed on a case-by-case basis. Most data only holds liability for a limited time. Additionally, the liability of any particular piece of data may increase or decrease over time, even before the value is lost completely, and the events that can cause these changes are unpredictable. This means that it is necessary to regularly audit the liability of the data, recalculate ROI, and then adjust security based on the new ROI when necessary.

[1]The value of information is not addressed in this paper; it is assumed that the user knows the value of the information to insert into the indicated formula.

Perhaps the most essential thing this graph reveals is that security is always important when data contains significant liability. There is always a threshold beyond which further improving security will cost more than the data's liability value. Once the ROI boundary thresholds are established, risk analysis should be performed to determine how much security is necessary to keep risk levels acceptable.

An alternative calculation relates to how much must be saved annually to deal with an attack if no security measures are taken. If the probability of an attack per year is known (see Equation 2), the number of years ($n$) can be used to determine how much money must be banked each year to recover from the attack. An attack reaches more than 50% probability in $\frac{n}{2}$ years. In this case, the cost of recovering from the attack ($P$) that must be saved annually ($A$) is then

$$A = \frac{2P}{n} \tag{11}$$

allowing for two approaches to implement protection cost-effectively.

### C. Value of Information

The Law of the Conservation of Information is under scrutiny in the post-quantum environment (PQE) and as related to quantum information [17]. However, this is not the only application of the law. The Law of the Conservation of Information states, "Information cannot be created or destroyed" [18]. In the context of human experience, it can only be forgotten and (re)discovered. While all information exists and can be discovered, a related question is: how much value comes with that information? Such a question is not easily resolved since the value varies with the individual and the time at which the value is evaluated. The time of evaluation shows that information value varies with time and circumstances. For example, consider information about the time an army will attack (such as the place, date, and time of the D-Day invasion). That data held high value for the Germans and Allies before the invasion. Once the date and time of the action arrived, the value of the data was known to all, and the value declined. There is still value from the historical perspective, but it is not the same type of value as before the action.

Information has a value that varies over time. That value increases as needed and falls when it is no longer needed. The exact function for value depends on the person or organization considering the data and the actual time the evaluation occurs. Since information has value, that value can be used to determine how much effort or expense should be expended in protecting that information from attackers. Once the information is identified, it is then given an initial value. After identification, information then tends to decrease in value monotonically. While the information has value, that information may need protection, depending on the nature of the information and the potential damage incurred if the data is prematurely revealed.

### D. Everlasting Security

The maximum time that information might need to be kept secret is until the end of time and is known as “everlasting security" [19]. Everlasting only implies the time remaining until the end of the universe. Beyond that time, no person or object will be left, so there is no reason to keep the secret. The time until the end of the universe can only be estimated. That time varies from 22 billion [20] to 100 trillion years [21]. The former estimate is likely the time humans will be extinct, so that date is the one that will be adopted for the effective expiration date for “everlasting."

A question that is not asked often enough is how long information should be kept secret. The US government, for one organization, does ask this question. Their levels of security typically carry a “declassification time" when information is no longer subject to being kept secret [22]. For US documents, that date is 25 years after the classification date unless the classification is renewed. After this time, the information is considered unimportant to attackers and adversaries and is quietly returned to public access. Government secrets can range in need for secrecy from unclassified (no exceptional value) to Top Secret (can damage national security) [23]. However, operational secrets may require a much shorter secrecy period.

Secrecy does not only apply to government organizations. Commercial entities also produce and attempt to keep secrets to provide a protected edge over their competitors. Patents reveal secrets but protect the data for 20 years [24]. An alternative to the patent is the trade secret [25]. If not revealed, trade secrets can be protected indefinitely [26]. With the evolution of technology, even trade secrets can become obsolete.

Obscuring information is often accomplished by using encryption. The time that information is kept safe using encryption is given by the amount of time it would take using a brute-force attack to break that encryption [8]. This attack is predicated on the time it takes to check if a solution is correct. The same procedure is used to verify passwords and is bounded by the same formula (see Equation 2). Most encryption algorithms use a single key having a known key size. However, if a key size is unknown, then the time to break the encryption, on average, is given by Equation 3.

The maximum bounding time is the brute-force time and resources required for breaking an encryption. However, some encryptions have weaknesses that can be exploited via different attacks to recover plain text data quickly. Known as “heuristic" attacks [27], these attacks reduce the time such that

$$t_h < t_{bf} \tag{12}$$

where $t_h$ is the time taken for a heuristic attack to be successful and $t_{bf}$ is the time required for a successful brute-force attack. Examples of successful heuristic attacks include the language statistic attack, the collision attack [28], and the Venona attack [29].

## III. Analysis

Encryption security requires expending computational resources. Often, the resources expended are proportional to the resulting security. This includes overhead and latency in both the encryption and decryption processes. The cost of security is also proportional to the number of keys that must be created and applied to the message. Therefore, the efficiency of encryption is also proportional to the encryption used. Rather than just choosing the most secure encryption methodology available, the encryption method selection should match the needed level of security and time required for information secrecy. The goal of encryption should be to match the time secrecy needed for the information and not to keep the information secret for as long as possible. Keeping a message secret forever wastes resources, time, and money that could be used elsewhere. While it is impossible to encrypt a message so it can never be decrypted, even if possible, such an action is pointless. Rather than do such encryption, the same result is achieved by never encrypting the information, destroying any recorded instances of the data, or otherwise not transmitting it.

Deciding on the proper selection and application of an encryption algorithm with an appropriate key depends on knowing how long the data should be obscured. This paper does not address how to decide the value of information and its subsequent decline in value. Assume that the time needed to keep the message/information secret is denoted by $t_{secret}$ and the time required to verify a key is $t_t$. Beyond that useful lifetime, the information loses practical value, and little is gained or lost from revealing that data. This is the information theory (IT) [30] equivalent of the $t_{secret}$ in the password case.

Applying Equation 2 as a starting point, it is then possible to appropriately develop the equation and substitute the variables applicable for encryption to estimate the number of keys required to keep the information secret for the appropriate amount of time to minimize the expended resources.

Recognizing that the period a piece of information needs to be safe is likely inaccurate (or, rather, imprecise), a safety factor ($s$) must be included in the calculation. The value of $n$ is a multiplication factor ranging from $1 \leq s < \infty$. This factor comes in a continuous range, does not need to be an integer, and should be much lower than infinity ($s << \infty$). Selecting infinity would mean that the information required everlasting security. Using a multiplier allows the user to overcome an incorrect estimation of the time information needs to be kept secret. A typical value for $s$ is $s = 2$, which doubles the obscuring time.

Other sources of non-linear effects also need to be accounted for. These can be consolidated into a single term ($\epsilon$) that encompasses all the effects that would increase the key size. For example, the computers used to break encryption will continue to become more efficient and faster. This phenomenon was described by Moore in 1965 and is known as “Moore’s Law" [31]. Moore indicated that computers were increasing speed by a factor of two and increasing the number

of transistors by the same figure every two years. Moore's law has remained very accurate for the last six decades. Moore's law is valid for classical computing and should be accounted for when calculating the number of keys needed for security. Speeding up the computer(s) focused on breaking the encryption is dependent on the term $t_{try}$. For each two years in the security time, the speed will double and must be compensated for by doubling the key space size. That adjustment must take place while Moore's Law is applicable. The proper adjustment to the equation is the factor $M$.

$$M = 2^{\left(\frac{y_f - y_s}{2}\right)} \tag{13}$$

This modifies the $\epsilon$ term to be

$$\epsilon = nM \tag{14}$$

When quantum computers develop to the point where they are applied to the encryption problem, the $t_t$ term (the time required to check a possible solution) will have to be re-evaluated, as will the adjustment for Moore's Law, assuming such a law applies to quantum computers.

Other properties can be added to the $\epsilon$ term as they are identified and quantified. The equation for calculating the required key space needed for the desired level of encryption security is

$$|K| \geq \frac{nt_{secret}}{t_t/2} = \frac{2\epsilon t_{secret}}{t_t} \tag{15}$$

In addition to the adjustments in the post-quantum environment for Moore's Law, there will be some adjustments required in response to both Shor's algorithm [32] and Grover's algorithm [33]. Shor's algorithm effectively eliminates asymmetric key algorithms based on the trapdoor functions used by public key encryption (PKE) [34], [35] schemes presently in use. Presently, the National Institute for Standards and Technology (NIST) [36] is attempting to identify "quantum-proof algorithms" (QPAs) to replace the PKE algorithms compromised by Shor's algorithm. Newer asymmetric key algorithms will be developed in the future that will be safe, and when they are created, they can be used to secure information using this approach.

There is very little change in using symmetric key algorithms in the Post Quantum Environment (PQE). Grover's algorithm indicates that to keep security levels constant for symmetric key algorithms, the key space must approximately double. This is a one-time measure but compensates for the effect of moving into the PQE with symmetric ciphers.

To complete the process, the user must match the required key space to one or more ciphers. Therefore, a database of ciphers and their key spaces is required. This database needs to be comprised of the name of the cipher, its maximum key space, its minimum key space if heuristic attacks exist, the cost of running the algorithm, and in which computing environments it is used (classical, quantum, or both). A user can then find all of the listed encryption algorithms such that the minimum key space ($|K_m|$) has the property

$$|K_m| \leq |K| \tag{16}$$

The user can then decide which cipher(s) to use to minimize the cost of security.

Security will only be applied if affordable and can be justified to decision-makers in terms of ROI. The optimal ROI comes when the security price is minimum for the necessary minimum level of security. The system represents engineering efficiency and sound business procedures by minimizing the cost for the necessary return (in this case, protection). Figure 2 also demonstrates that the length of time that data must have security is directly related to its cost. For example, high security for a short time costs very little. Engineering and business efficiency are thus demonstrably related.

## IV. Conclusion and Future Work

Security is insurance against attack(s) and must be considered like any other type of insurance when doing risk analysis. Security professionals must be part of the management team and ensure that economically justifiable security measures are included in a company's business practices. Security is not a loss center or profit drain; instead, it can be shown to be good corporate governance.

Persuading business leaders and decision-makers to implement effective security requires communicating with them using accepted business language and practices. An adversarial approach between management and cybersecurity personnel is not needed or productive. The Chief Information Security Officer (CISO) is responsible for conversing with and using business concepts and language to assist the CEO in understanding the risks and rewards associated with operating in the electronic information environment.

ROI is one of the strongest arguments for implementing security. Quantifying the probability of an attack over time is possible by showing how likely a cyberattack will be on a business. The costs and rate of saving from an eventual attack can easily be calculated and planned, including the costs of surviving and recovering from an attack. Efficient use of resources is also a key concept that business people readily understand and accept. Encryption is a process whose costs depend on the strength of the encryption and algorithm(s) used to affect the encryption. Proper evaluation of information security is critical to the efficient, cost-effective use of encryption.

Not all messages require everlasting security. The goal of encryption is to keep the information/message secure for as long as it can be valuable to an attacker and result in damage to the owner of the information. Protecting it for a longer time than this wastes time, money, and resources. Business and engineering are based on efficiency in using resources to accomplish a particular job and outcome. This approach will enable the user to match the requirements with the proper hard cipher and appropriately protect that data.

Attempting to make all messages safe for all time is based on the belief that information has the same value for all time. Such a viewpoint ignores the fact that information value is a

monotonically decreasing function once the information needs are established. Most information has value and can damage the sender for a much shorter period. Determining the period that a message has that value must be done by the sender. That process is not the point of the work in this paper, but the mathematics is affected by the definition of that period. Information value decay has not been extensively studied. Therefore, estimating time and power loss rates is crucial to deciding when information should be protected. That process of determining information value and its decay function and rate should be addressed in detail in a future research effort.

Breaking the encryption in a message is related to the problem of cracking a password. The password problem demonstrates the equivalence of time and the size of an encryption key space. Therefore, once the time that a message should be kept secret is established, the message's data can be translated into the necessary key space for the encryption that protects the message. An appropriate cipher can be selected if the needed key space is compared to the known key space of available ciphers. The key space for each cipher needs to be adequate, given known heuristic attacks. Such a database needs to be made publicly available for researchers and practitioners. The construction and maintenance of that database are projects that require constant attention.

The technology change to include quantum computing resources necessitates future research into how quantum computers will evolve in the PQE. Specifically, Moore's Law, when applied to quantum computing, is a method of estimating the rate of change in quantum speed. No precise study of Moore's Law in this environment has been made, so this is an important area for future work.

## REFERENCES


[1] National Geographic. 4 hidden causes of dam failures, https://http://news.nationalgeographic.com/2015/10/151007-dam-failures-south-carolina-engineering-science/, 2017.

[2] Krypyonite Support. How much should i spend on my bike lock? https://support.kryptonitelock.com/hc/en-us/articles/231014107-How-much-should-I-spend-on-my-bike-lock.

[3] Noel Sales Barcelona. 75% of us companies prone to cyberattack – report.

[4] Kiteworks. *2024 Kiteworks Sensitive Content Communications Security and Compliance Report*. 2024.

[5] Kiteworks. *2024 Forecast for Managing Private Content Exposure Risk*. 2024.

[6] Fabio Natalucci, Mahvash S. Qureshi, and Felix Suntheim. Rising cyber threats pose serious concerns for financial stability, Apr 2024.

[7] *Global Financial Stability Report*. International Monetary Fund, April 2024.

[8] Bruce Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. John Wiley and Sons Inc., New York, 2nd edition, 1996.

[9] Matthew Bishop. *Computer Security: Art and Science*. Addison-Wesley Professional, Boston, 2003.

[10] Electronic Frontier Foundation. *Cracking DES, Secrets of Encryption Research, Wiretap Politics & Chip Design*. O'Reilly & Associates.

[11] Philippe Oechslin. Making a faster cryptanalytical time-memory trade-off. In *Lecture Notes in Computer ScienceAdvances in Cryptology: Proceedings of CRYPTO 2003, 23rd Annual International Cryptology Conference*, 2003.

[12] James F. Broder and Eugene Tucker. *Risk Analysis and the Security Survey*. Elsevier, $4^{th}$ edition.

[13] Elie Bursztein. Understanding the prevalence of web traffic interception.

[14] Patricia Pulliam Phillips and Jack J. Phillips. *ROI Fundamentals: Why and When to Measure Return on Investment 1st Edition*. Pfeiffer and Company.

[15] Lawrence J. Fennelly. *Handbook of Loss Prevention and Crime Prevention*. Butterworth-Heinemann, $6^{th}$ edition.

[16] George S. Clason. *The Richest Man in Babylon*. Createspace Independent Publishers, 3 December 2014.

[17] Marco Roncaglia. On the conservation of information in quantum physics. *Foundations of Physics*, 49:1–9, 11 2019.

[18] Steven W. Hawking. The information paradox for black holes. In *17th International Conference on General Relativity and Gravitation*, Dublin, Ireland, July 2004. see http://math.ucr.edu/home/baez/week207.html for a transcript.

[19] Uli Maurer. A universal test for random bit generators. *Journal of Cryptography*, 5(2):89–105, 1992.

[20] Ethan Siegel. Ask ethan: Could the universe be torn apart in a big rip?, https://www.forbes.com/sites/startswithabang/2018/06/30/ask-ethan-could-the-universe-be-torn-apart-in-a-big-rip/?sh=762b6d023bd8. Internet, June 2018.

[21] Fred C. Adams and Gregory Laughlin. A dying universe: the long-term fate and evolution of astrophysical objects. *Reviews of Modern Physics*, 69(2):337–372, April 1997.

[22] Barak Obama. Classified national security information, executive order 13526, https://www.govinfo.gov/content/pkg/cfr-2010-title3-vol1/pdf/cfr-2010-title3-vol1-eo13526.pdf, 2009-12-29.

[23] D. Elliott Bell and Leonard J. La Padula. Securecomputer systems: Unified exposition and multicsinterpretation. Technical Report MTR–2997 (ESD–TR–75–306), M.I.T.R.E. Corporation.

[24] USPTO.gov. 2701-patent term, https://www.uspto.gov/web/offices/pac/mpep/s2701.html, 2010-11-19.

[25] World trade organization, agreement on trade-related aspects of intellectual property rights (trips), part ii, section 7, https://www.wto.org/english/docs_e/legal_e/27-trips_04d_e.htm#7.

[26] The Coca-Cola Company. Is the coca-cola formula kept secret because the company has something to hide?, https://www.coca-cola.com/ke/en/about-us/faq/is-the-coca-cola-formula-kept-secret-because-the-company-has-som#:~:text=the formula for making coca,experience time and time again.

[27] Ho Li, A. Samsudin, and Bahari Belaton. Heuristic cryptanalysis of classical and modern ciphers. volume 2, page 6 pp., 12 2005.

[28] David McGrew. Impossible plaintext cryptanalysis and probable-plaintext collision attacks of 64-bit block cipher modes. In *Proceedings of the Fast Software Encryption Workshop*, 2013.

[29] John Earl Haynes and Harvey Klehr. *Venona: Decoding Soviet Espionage in the United States (Yale Nota Bene)*. Yale University Press, 1999.

[30] Thomas Cover and Joy Thomas. *Elements of Information Theory*. John Wiley & Sons, Inc, New York, 2nd edition, 2005.

[31] Gordon E. Moore. Cramming more components onto integrated circuits. *Electronics*, 38(8).

[32] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, 1994.

[33] Lov K. Grover. Quantum computing: How the weird logic of the subatomic world could make it possible for machines to calculate millions of times faster than they do today. *The Sciences*, pages 24 – 30, 1999.

[34] Vasileios Mavroeidis, Kamer Vishi, Mateusz D. Zych, and Audun Jøsang. The impact of quantum computing on present cryptography. *CoRR*, abs/1804.00200, 2018.

[35] Johannes A. Buchmann, Evangelos Karatsiolis, and Alexander Wiesmaier. *Introduction to Public Key Infrastructures*. Springer-Verlag, Berlin, Germany, 2013.

[36] NIST. Nist announces first four quantum-resistant cryptographic algorithms, https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistantcryptographic-algorithms.


## ACKNOWLEDGEMENT


We acknowledge Mr. Bob Weiss, an Oklahoma-based businessman, for his invaluable review and feedback on our paper. Thank you, Mr. Weiss.