# Increasing Industry Profitability and Cyber Hygiene Utilizing Awareness Progression Methods

**John Thebarge, Mark Reith and Wayne Henry**
**Air Force Institute of Technology, Wright-Patterson AFB, USA**
John.thebarge@afit.edu
Mark.Reith@afit.edu
Wayne.Henry@afit.edu

## Author Note

The views expressed are those of the authors and do not reflect the official policy or position of the US Air Force, Department of Defense, or the US Government.

**Abstract:** Securing critical networks and systems through proper cyber hygiene is a constant battle. Businesses spend a significant amount of time and money implementing cybersecurity mechanisms. However, businesses do not always see the cost-benefit from paying for proper cyber hygiene mechanisms, given the inevitability and persistence of cyber threats. This research explores potential financial incentives for businesses to improve their cyber hygiene awareness. Past anti-smoking and climate change awareness campaigns are compared to support a new cyber hygiene awareness campaign. By investigating the effectiveness of the incentive methods used by these awareness campaigns, this work proposes adopting similar incentive methods to improve cyber hygiene awareness.

**Keywords:** Cyber Hygiene, Profitability, Awareness Campaigns, Climate Change, Anti-Smoking

## 1. Introduction

As the Internet and the interconnection of systems grows, the likeliness for cyber incidents to occur grows with it. Cyber incidents frequently exploit the poor cyber hygiene of the Internet's users. Cyber hygiene refers to best practices of users to ensure security of computers, cyber-physical systems, and data (Brook, 2020). The processes and mechanisms required to obtain proper cyber hygiene have always been expensive. The extent of these costs is shown in the global spending on cybersecurity, which was $123 billion USD in 2020 and is projected to be $133 billion in 2022 (Shackleton, 2021). The remediation costs associated with cyberattacks can also be significant. In 2020, global cyber-attacks cost government and industry $1 trillion, averaging $3.9 million per incident. Deloitte and the Financial Services Information Sharing and Analysis Center (FSISAC) performed a study that surveyed 97 major institutions that had annual revenues between $500 million and $2 billion. This report discovered that the companies had increased their cybersecurity budget from 0.34% of their total revenue in 2019 to 0.48% in 2020 (Bernard, 2020). This shift in funding is a reactionary effort from industry to combat the growing number of total breaches between 2018 and 2019. In 2018, approximately 1.257 billion data breaches occurred with 472 million individual records exposed, compared to 2019 with 1.473 billion data breaches and 164 million individual records. (Johnson, 2021). In 2020, the total data breaches dropped to 1 billion, with nearly 156 million individual records exposed. Despite the reduced number of breaches in 2020, a reactionary force is still a losing force in the cyber domain. Allowing companies to remain in a reactionary position in the cyber domain allows a higher level of risk acceptance.

This is not the first-time companies were required to adapt to other major hygiene awareness campaigns. When smoking became a global health concern, companies had to incentivize their employees not to smoke, as it was costing them more due to their employees' decreasing health (Baker et al, 2017; Sammer, 2019). A similar outcome occurred with climate change when companies had to reduce their total emissions. Companies were able to reduce their emissions by utilizing incentives that helped offset the cost of changing to reduced emission processes (EDF, 2018).

This paper investigates the similarities that exist between the anti-smoking, climate change, and cyber hygiene awareness campaigns. We then discuss the financial incentives used to progress the anti-smoking and climate change awareness campaigns. This paper concludes by proposing the adoption of similar financial incentive methods to progress cyber hygiene awareness and reduce the cost of safeguarding assets from persistent cyber threats.

## 2. Comparing Anti-Smoking and the Cyber Hygiene Awareness Campaigns

Smoking kills more than 480,000 people per year in the United States alone, which includes more than 41,000 deaths from second-hand smoking (CDC, 2021). The general population was unaware of the negative health effects cigarettes had when they gained in popularity in the 20th century (Lorgat, 2020). The trend of smoking grew rapidly. It was not unusual to see characters smoking in children's books or famous actors smoking on television. In the 1960s, the Surgeon General publicly recognized the overwhelming evidence that displayed the negative impacts of smoking, such as lung cancer and bronchitis. This recognition came after 45% of Americans were already smoking. The percentage of Americans that smoked has gradually dropped since then. In 2015, 15.2% of Americans smoked (Blakemore, 2015). Despite the 30% decrease of total American smokers since the 1960s, the damage of cigarettes continues to cost over $255 billion in direct medical care for adults and $156 billion in lost productivity each year (CDC, 2021). These costs are associated with smokers and their employers having to pay higher health insurance rates due to their higher risk of illness (Baker et al, 2017; Sammer, 2019). The popularity of cigarettes demonstrates the tendency for society to adopt the latest trends based on its general acceptance without concern for the negative long-term impacts it could have on their individual health and the health of those around them.

The Internet became popular in a similar fashion as smoking did. Unfortunately, the popularity of the Internet has led to poor cyber hygiene of its users. In 1967, the concept of ARPANET (The Advanced Research Projects Agency Network) was created by the Department of Defense (DoD) as the first packet-switched network that allowed for the rapid dissemination of information from one network node to another (Leiner et al, 1997). In 1972, ARPANET was successfully demonstrated, sparking the rapid adoption and creation of communication applications around the world. In 1983, this rapid growth of networks and the seemingly endless capabilities they would provide soon evolved into the Internet. Today, the Internet now has 4.88 billion active users (Johnson, 2021; Leiner et al, 1997).

Very few cared to recognize the threats that would develop with the mass adoption of the Internet. Due to this lack of recognition, malicious actors were able to make these threats a reality early on. In 1986, a German hacker by the name of Marcus Hess used an Internet gateway in Berkeley, CA, to gain access to the ARPANET and MILNET (Chadd, 2020). Hess was able to hack into 400 military computers. Hess had intentions to sell the information to the KGB, who were the main security agency for the Soviet Union. In the 1990s, polymorphic viruses made their first appearance. Polymorphic viruses avoided detection by mutating as it traversed systems. These types of attacks avoided commonly used signature-based antivirus software, leaving no proper methods of detecting and preventing these types of attacks. In 1999, the Internet saw the aggressive propagation of the Melissa virus. The virus propagated via email utilizing the users' email address book of the infected machine.

As the Internet developed, computers became more interconnected. It was near impossible to stop or even deter malicious actors as the threat space was growing exponentially worldwide. As a result, there was a rapid decline of cyber hygiene across companies and those who had adopted the Internet. The capabilities the Internet provided led to its increase in popularity. The Internet's popularity pushed the concern for its lack of security into the background (Timberg, 2015). Today, we continue to see the lack of emphasis on cyber hygiene, considering the number of security breaches that are still occurring. In 2005, there were 157 million data breaches in the United States and 66.9 million individual records were exposed (Johnson, 2021). In 2020, these incidents increased by over 537%, with 1 billion data breaches in the United States, exposing approximately 156 million individual records.

Both the Internet and smoking rapidly grew through popularity without concern for the long-term negative effects they would have. Poor cyber hygiene causes hardship to companies and individuals through expensive remediation costs for cyber incidents and stolen individual records. Stolen identities through the exposure of these records cause direct hardship to individuals and their families. This hardship is caused through impacted credit scores, credit card fraud, and other financial burdens. Similarly, smoking causes hardship to the smoker's employer through increased health coverage costs and reduced productivity. Smokers also see financial burdens and health issues for themselves and their families. The increased likeliness of illness leads to higher health premiums and an increase in medical costs. Second-hand smoke can also impact families and their health. Given the similarities between smoking and poor cyber hygiene, we will examine the incentives used in anti-smoking awareness and how they could be utilized to progress cyber hygiene.

## 3. Comparing Climate Change and the Cyber Hygiene Awareness Campaigns

During the 18th and 19th centuries, the world saw the Industrial Revolution. The Industrial Revolution led to the rise of global production and new manufacturing processes around the world (CPW, 2021). This rise in global production and manufacturing led to the development of emissions. The pursuit of manufacturing led to the industrialization of once-rural areas into factory-filled cities. With industrialization came the dependency on fossil fuels such as coal, natural gas, and oil. The use of these fossil fuels resulted in about 65% of the world's greenhouse emissions through the powering of transportation, heating, and electricity generation. The movement for climate change came after recognizing the negative impacts that the emission processes were having on the planet. The climate change awareness campaign has made several major leaps forward in governance and policy. In 1997, the Kyoto Protocol was introduced as one of the first international policies for reducing emissions around the world. In 2008, it was accepted by 181 countries (Zhou et al, 2018). The Kyoto Protocol outlined the obligations developed countries needed to follow to reduce greenhouse gas emissions and outlined the means for the countries to accomplish this. This included emissions trading and carbon credits. The Kyoto protocol also introduced "Clean Development Mechanisms," which provided carbon or tax credits for investing in technology and infrastructure that reduced emissions. The Paris Agreement was another major international agreement created to ensure the world is progressing the climate change campaign. Activated in 2016, it introduced the idea of international carbon trading markets through its article 6 (EDF, 2021). Additionally, it outlined the objective of reducing the rise in mean global temperature to below 2-degrees Celsius (UNFCCC, 2021).

When comparing climate change and cyber hygiene, we recognize that cyber hygiene was not at the forefront through the rapid adoption and popularity of the Internet. Similarly, the negative impact of emissions on our climate was also not at the forefront through the adoption and popularity of industrialization. In the climate change awareness campaign, we saw the implementation of international policies due to the high level of emissions worldwide. In the same vein, cyber hygiene is also an international concern. We saw the acknowledgment of cyber being an international concern in the United States International Strategy for Cyberspace (USISC) under the Obama administration (Congress, 2011). This cyber strategy addressed the need for a stable cyberspace and the critical role it plays in the success of the global economy. The strategy also outlined the need to develop international norms of behavior in cyberspace, and international cybersecurity capacity building. The policy also mentioned the necessary frameworks to stabilize cyberspace. These frameworks emphasized the protection of critical infrastructure. Like the efforts of the Kyoto Protocol and the Paris Agreement combatting carbon emissions worldwide, the USISC stresses the need for a global effort on cyber hygiene by recognizing worldwide cyber threats and risks. Like climate change, cyber hygiene is a global issue. Both efforts require key world players to work together to combat the diminishing health of our planet and the cyber hygiene of Internet users.

## 4. Incentives in Climate Change and Anti-Smoking Awareness Campaigns

Some of the incentive methods currently being used to progress the climate change and anti-smoking awareness campaigns are as follows:

### 4.1 Climate Change Emissions Trading

Emissions trading, commonly referred to as "cap-and-trade" programs, provides economic incentives to companies to reduce their greenhouse gas emissions. One of the major US-based programs is the Regional Greenhouse Gas Initiative (RGGI). This program was the first market-based initiative that involved companies in Connecticut, Delaware, Maine, Maryland, Massachusetts, New Hampshire, New York, Rhode Island, Vermont, and Virginia (Ceres, 2020; RGGI, 2021). The program operates by having an authority provide a maximum cap of greenhouse gas pollution per region. The cap is then split into individual limits and issued to companies. The limit indicates the total greenhouse gas pollution the company can produce in a three-year timeframe. If a company is below their maximum emission limit, they can sell their unused portion to a buyer company, turning their reduced emission expenses into profit. Alternatively, if a company knows they will exceed their limit, they can negotiate to buy another company's unused portion. This prevents the company from paying steep fines for going over their allotted limit. If companies refuse to implement the necessary processes and procedures, they will be forced to continue buying other companies' unused limit portions or go over their allowed limit. This will ultimately cost them more in the long term, given the cap for the region is lowered over time.

The cap-and-trade program forces companies to reduce their overall emissions and has yielded positive results. The decrease of emissions due to the lowering of the authorized cap over the years within the RGGI program can be seen in Figure 1. This graph shows the gradual decrease in emissions (per million tons) as the cap is lowered annually (Climatenexus, 2019; RGGI, 2021). This program has not only led to the reduction of greenhouse gas emissions but provided over $416 million in revenue in 2020 alone. Since 2005, RGGI has collected $3.8 billion in total revenue (ICAP, 2021). This revenue is returned to the states involved in the RGGI program, where it has been primarily invested in consumer benefit programs.

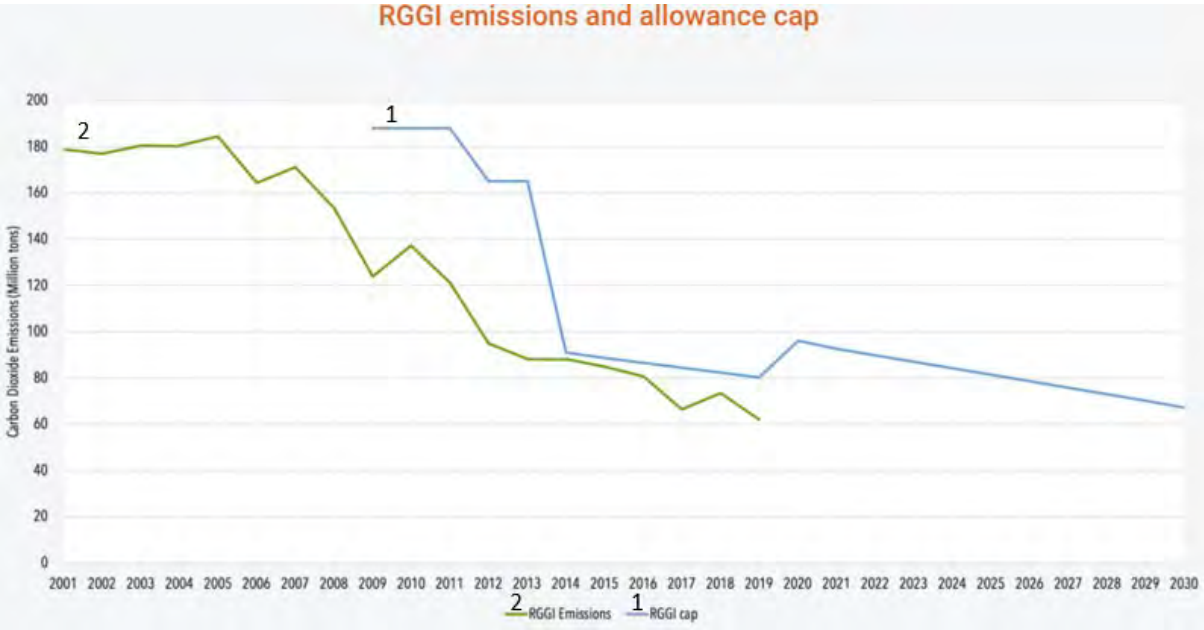


**Figure 1:** Total emissions against the lowered cap in RGGI (C2ES, 2020).

In the United States, California has implemented a similar cap-and-trade program called the "AB 32 Scoping Plan." The AB 32 Plan has seen a 10% decrease in total emissions between 2013 and 2018 and aims at achieving 40% below 1990 emission levels by 2030 (EDF, 2016; 2018). Emissions trading has also proven to be successful outside of the United States. Europe has seen success with the European Union's Emissions Trading System (EUETS), as well as China. China produces the largest emissions of greenhouse gases and implements cap-and-trade elements into their new emissions trading system. In 2018, they saw a 29% decrease in stationary structure emissions when compared to 2005 emission levels (EDF, 2018). Emissions trading has not proven its success internationally between countries. The Paris Agreement Article 6 introduced the concept of international emissions trading, but it becomes a more difficult incentive to implement across different countries given the international rules that must be in place and agreed upon by all parties. Recently approved in mid-November 2021, its international effectiveness has not been determined (Hedley, 2021).

### 4.2 Climate Change and Carbon Capture Credits

Carbon capture and sequestration is the process of injecting carbon oxides underground after they have been captured from the original emission source, such as a powerplant (Hasan et al, 2015). The power of carbon capture is immense. In an optimal nationwide design of carbon capture, utilization, and sequestration (CCUS), it is possible to capture over 1.5 Gt (gigatons) per year of carbon emissions. This requires the capture of 50% of stationary structure emissions. Figure 2 presents the total carbon emissions captured from stationary structures. As the reduction level increases from 60% to 80%, it yields a total of over 1.8 Gt/year and over 2.4 Gt/year, respectively.

Nationwide CCUS costs.

| | $CO_2$ reduction level | | |
|---|---|---|---|
| | 50% | 60% | 80% |
| Total stationary $CO_2$ emission (Gt/year) | 3.068 | 3.068 | 3.068 |
| Total $CO_2$ captured (Gt/year) | 1.534 | 1.841 | 2.454 |
| Total flue gas dehydration cost (billion dollars/year) | 15.677 | 18.815 | 25.080 |
| Total capture &compression cost (billion dollars/year) | 38.238 | 46.823 | 70.906 |
| Total transportation cost (billion dollars/year) | 2.551 | 3.870 | 7.636 |
| Total injection cost (billion dollars/year) | 1.627 | 2.001 | 2.994 |
| Total CCUS cost (billion dollars/year) | 58.093 | 71.509 | 106.616 |
| Total CCUS revenue (billion dollars/year) | 3.43 | 3.52 | 3.60 |
| Overall CCUS cost (billion dollars/year) | 54.663 | 67.989 | 103.016 |
| Overall CCUS cost (dollars/ton $CO_2$ captured) | 35.634 | 36.930 | 43.445 |

**Figure 2:** Total costs for an optimal CCSU supply chain network in the United States (Hasan et al, 2015).

The total carbon captured demonstrates the strength of this technology, while the cost shows the extreme prices associated with using it. To successfully capture 50% of stationary structure emissions, it would cost over $54 billion per year (Hasan et al, 2015). This is where carbon or tax credits are used. Companies and individuals who invest in carbon capture projects or technology can receive tax or carbon credits per ton of carbon successfully captured and sequestered. These tax credits can range from $35 to $50 per ton of carbon. To receive this benefit, the total carbon captured must range between 25,000 and 500,000 metric tons. This could yield anywhere between $875 thousand to $25 million worth of credits. The range specified is dependent on how much the carbon emission facility produces annually (CRS, 2021). A limiting factor of the effectiveness of carbon-capturing is the immense cost that is associated with it. The technology is expensive to develop, and the cost is preventing an ideal supply chain network in the United States from coming to fruition (Baylin-Stern, 2021).

### 4.3 Anti-Smoking Incentives

As previously highlighted, the damage of cigarettes continues to cost $255 billion in direct medical care for adults and $156 billion in lost productivity (CDC, 2021). The loss of productivity is an indirect cost to a company because it is caused by the increased risk of illness from smoking, leading to absenteeism. In 2017, Pfizer surveyed 75,000 individuals across the United States, EU, and China. They found that active smokers had 28% more absenteeism over a seven-day span than those who had never smoked or had quit (Baker et al, 2017). Companies recognized smokers were costing them more annually to provide adequate healthcare coverage than a non-smoker. To encourage smokers to quit, surcharges and incentives were introduced. In 2004, a study involving General Electric found that offering a cash incentive of $750 yielded almost three-times as many people quitting as those without the incentive. This increased the quit rate from 5.0% to 14.7%. This ultimately led General Electric to provide an incentive program for all United States employees. This study was later published by the New England Journal of Medicine and became a widely adopted approach by governments, employers, and insurers to progress the anti-smoking campaign further (Halpern et al, 2015).

A similar study with CVS employees and their families tested the effectiveness of different variations of incentive programs. This study which had 2,538 participants focused on two main approaches. The first approach focused on an individual-oriented incentive program that offered either a reward for the individual or a reward with an initial deposit by the participant. The second approach was identical to the first, except it was group-oriented with 6 participants per group (Halpern et al, 2015). The reward offered was $800 for smoking cessation past six months. The deposit study entailed a refundable deposit of $150 and $650 in a reward payment. The study results showed that 90% of participants accepted the reward-based program. Only 13.7% of participants accepted the deposit-based program. Overall, the reward-based programs had a higher cessation rate of 15.7% compared to 10.2% from the deposit-based program. The difference in success rates between individual-oriented and group-oriented incentive programs was considered negligible, with success rates of 12.1% and 13.7%, respectively. Additionally, the individual reward-based program saw a 9.7% higher smoking cessation rate compared to those under usual care at 6%. Figure 3 represents the outcomes of the CVS study. The difference in the success of both individual and group-based rewards can be seen compared to the deposit-based incentive. One of the major highlights from Figure 3 is the cessation rate through 12 months, where both reward programs maintained the highest percentage of smoking cessation.

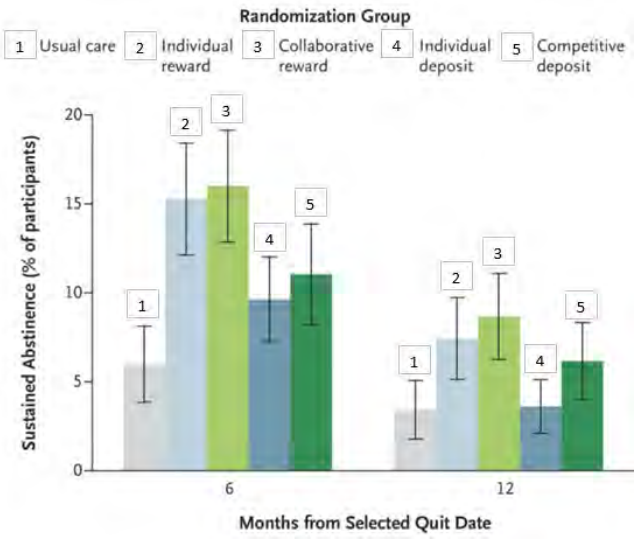


**Figure 3:** Smoking cessation success rates for reward-based and deposit-based incentive programs (Halpern et al, 2015).

These incentive-based programs may cost companies more in the short term due to the upfront costs of the rewards. Although, it is estimated that having these types of programs will save an employer anywhere between $150 and $540 per additional non-smoking employee (Ekpu & Brown, 2015). This has been a widely adopted incentive program because of its success and has ultimately turned a profit for companies over a multi-year timeframe. It is important to note that the cessation rate into 12 months dropped by about 8% compared to the six-month interval at 15.7%. Although the six-month timeframe is relatively impressive, the effectiveness of the program does not seem as impressive over the longer 12-month period (Halpern et al, 2015).

## 5. Proposal

The anti-smoking and climate change awareness campaigns used multiple methods to incentivize companies to progress their overall awareness. Again, these incentive methods included cash rewards, tax and carbon credits, and trading. Utilizing the incentive methods introduced in climate change, we have a foundation of a cyber risk trading concept. Instead of an emissions limit for climate change over three years, we have an allowable cyber risk limit for a company over a similar timeframe. Cyber risk in a company is measured through identifying critical infrastructure and assets, the impact of losing those assets, and identifying cyber threats and their applicability to the respective company (Dumont, 2020). This allows cyber risk to be a quantifiable metric. This measurement of risk can be used by a government-based authority to determine the maximum limit of cyber risk per a given region. Regions would consist of different companies with different lines of business. For example, the cyber risk of health institutions will be different from the risks pertaining to financial institutions; therefore, it would be unfair to categorize these types of companies under the same cyber risk allowance. Additionally, the authority will lower the risk cap annually, forcing companies to reduce their cyber risk, ultimately improving their cyber hygiene over time. Companies can trade their unused risk limits to other companies who need them. This would assist in offsetting the cost of implementing adequate cyber hygiene processes and mechanisms. This concept also introduces the potential of utilizing an existing framework, the Cybersecurity Maturity Model Certification (CMMC). The CMMC is a framework that assesses an organization's implementation of cybersecurity practices (Dumont, 2020). These assessments are done by a certified 3rd party organization. The CMMC framework is expected to be implemented across the DoD over the next five years, and its use of certified 3rd party assessment organizations could be leveraged to assess the cyber risk of the companies in the risk trading concept (Dumont, 2020). Forcing companies to reduce their risk over time while financially incentivizing them through the trading concept would progress the cyber hygiene of the companies involved.

Continuing with climate change incentives, we have carbon capture with investment benefits. The extreme costs associated with carbon-capturing technology are akin to the extreme costs in implementing proper cyber hygiene. The use of outside investors could prove beneficial to the progression of cyber hygiene, just like it has with carbon capturing. Instead of carbon capture, we have a concept of cyber risk capturing. The concept of cyber risk capturing is to provide an investor company with risk credits or tax credits that choose to invest in the progression of cyber hygiene in other companies. The investing companies can use the risk credits they receive

to offset their own cyber risk limit. Risk capturing and its usability can be seen with an example of an increase in ransomware attacks towards health institutions. The authority overseeing the health institutions would lower their risk limits to combat the increase in ransomware. In this scenario, an outside company not directly targeted by the increase in ransomware attacks can choose to invest in the progression of cyber hygiene in the health institution. Not only will the outside investment aid in increasing the cyber hygiene of the health institution and lower their risk limit, but the investing company can use the credits they would receive to offset their own cyber risk limit as well.

Moving to anti-smoking awareness incentives, we have a concept for positive cyber hygiene incentives. Companies will provide incentive funds to their employees who collectively increase their cyber hygiene on an annual basis. Companies would gauge an increase in cyber hygiene across their employees through the application of cyber hygiene best practices. The use of these best practices would reduce the number of incidents that occur through the end-user. The funds will be restricted to being spent solely on employee improvement programs. The goal is to incentivize the employees to apply what they learn in their cyber hygiene training. Doing so will directly increase the company's cyber hygiene and ultimately save them money from the reduced number of cyber incidents.

## 6. Conclusion

This paper recognizes similarities between the anti-smoking, climate change, and cyber hygiene awareness efforts. Through these similarities, we identified that cyber hygiene, personal hygiene, and the health of our planet rapidly declined through the popularity of the Internet, cigarettes, and industrialization, respectively. Society has shown a tendency to adopt the latest trends based on its public acceptance and not think twice about the negative long-term impacts these trends could have. It is important to recognize that the previous awareness campaigns are just as much a social issue as they are a technical issue. This enables the possibility of adopting progression methods other awareness efforts have used to progress other seemingly unrelated awareness campaigns.

The smoking and climate change awareness campaigns recognized that incentives were needed to get companies to progress their awareness, which ultimately yielded positive results in their respective efforts. Cyber hygiene is in a similar position. Companies need to be incentivized to properly safeguard their assets and personnel due to the increasing costs of proper cyber hygiene mechanisms and the persistence of cyber threats. Adopting a cap-and-trade program for cyber risk would reduce the cyber risk companies are accepting. This would increase their overall cyber hygiene and would prove to be financially beneficial. Similarly, the adoption of carbon or tax credits for cyber risk could reduce a company's overall risk, which would increase their cyber hygiene as well.

## References

Baker, C. L. et al., 2017. Benefits of quitting smoking on work productivity and activity impairment in the United States, the European Union and China. *International Journal of Clinical Practice,* 1.71(1).

Baylin-Stern, A., 2021. Is carbon capture too expensive?. *https://www.iea.org/commentaries/is-carbon-capture-too-expensive.*

Bernard, J., 2020. *Reshaping the cybersecurity landscape.,* s.l.: s.n.

Blakemore, E., 2015. In 1965, 45 percent of Americans smoked, today it's only 15 percent.. *https://www.smithsonianmag.com/smart-news/only-15-percent-americans-smoke-180956504.*

Brook, C., 2020. What is Cyber Hygiene? A definition of cyber hygiene, benefits, best practices, and more. *https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more.*

C2ES, 2020. *Regional Greenhouse Gas Initiative (RGGI).* [Online] Available at: https://www.c2es.org/content/regional-greenhouse-gas-initiative-rggi/

CDC, 2021. Tobacco Fast facts. Centers for Disease Control and Prevention. *https://www.cdc.gov/tobacco/data_statistics/fact_sheets/fast_facts/index.htm.*

Ceres, 2020. Ceres Report. *https://www.ceres.org/sites/default/files/Fact%20Sheets%20or%20misc%20files/March%2015%20S177%20Letter%201.pdf.*

Chadd, K., 2020. The history of Cybersecurity. *https://blog.avast.com/history-of-cybersecurity-avast..*

Climatenexus, 2019. Emissions trading. *https://climatenexus.org/climate-change-us/politics-and-policy/emissions-trading/..*

Congress, U. S., 2011. International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World..

CPW, 2021. The warming effects of the Industrial Revolution - global temperatures. *https://www.climate-policy-watcher.org/global-temperatures/the-warming-effects-of-the-industrial-revolution.html..*

CRS, 2021. The tax credit for carbon sequestration (section 45Q).. *https://sgp.fas.org/crs/misc/IF11455.pdf.*

Dumont, C., 2020. CMMC - risk assessment. *https://www.tenable.com/sc-dashboards/cmmc-risk-assessment.*

EDF, 2016. California leads fight to curb climate change.. *https://www.edf.org/climate/california-leads-fight-curb-climate-change.*

EDF, 2018. How cap and trade works.. *https://www.edf.org/climate/how-cap-and-trade-works.*

EDF, 2021. Cop 26: Implementing Article 6 of the Paris Agreement.. *https://www.edf.org/climate/implementing-paris-climate-agreement.*

Ekpu, V. U. & Brown, A. K., 2015. The Economic Impact of Smoking and of Reducing Smoking Prevalence: Review of Evidence. *Tobacco Use Insights,* 1.Volume 8.

Greig, J., 2020. 66% of companies say it would take 5 or more days to fully recover from a ransomware attack ransom not paid.. *from https://www.techrepublic.com/article/66-of-companies-say-it-would-take-5-or-more-days-to-fully-recover-from-a-ransomware-attack-ransom-not-paid.*

Halpern, S. D. et al., 2015. Randomized Trial of Four Financial-Incentive Programs for Smoking Cessation. *New England Journal of Medicine,* 5.372(22).

Hasan, M. F., First, E. L., Boukouvala, F. & Floudas, C. A., 2015. A multi-scale framework for CO2 capture, utilization, and sequestration: CCUS and CCU. *Computers & Chemical Engineering,* 10.Volume 81.

Hedley, A., 2021. Paris agreement article 6 success - A long time coming. *https://www.lexology.com/library/detail.aspx?g=75d8c877-c351-494d-a14b-44ebe0f899e4..*

ICAP, 2021. USA - Regional Greenhouse Gas Initiative (RGGI). *https://icapcarbonaction.com/en/?option=com_etsmap&task=export&format=pdf&layout=list&systems%5B%5D=50.*

Johnson, J., 2021. Internet users in the world 2021. *from https://www.statista.com/statistics/617136/digital-population-worldwide..*

Johnson, J., 2021. U.S. data breaches and exposed records 2020.. *https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/..*

Leiner, B. M. et al., 1997. The past and future history of the Internet. *Communications of the ACM,* 2.40(2).

Lorgat, I., 2020. Smoking: A 100-year story that doesn't end here. Smoking: a 100-Year Story That Doesn't End Here.. *https://www.rgare.com/knowledge-center/media/articles/smoking-a-100-year-story-that-doesn-t-end-here.*

Murphy, P., 2020. To defend forward, US cyber strategy demands a cohesive vision for information operations.. *https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/2420176/to-defend-forward-us-cyber-strategy-demands-a-cohesive-vision-for-information-o/.*

Pearlson, K., 2021. Cyberattacks are inevitable. is your company prepared?. *https://hbr.org/2021/03/cyberattacks-are-inevitable-is-your-company-prepared.*

RGGI, 2021. About the Regional Greenhouse Gas Initiative. *https://www.rggi.org/sites/default/files/Uploads/Fact%20Sheets/RGGI_101_Factsheet.pdf.*

Sammer, J., 2019. Employer incentives encourage employees to quit smoking. *https://www.shrm.org/hr-today/news/hr-magazine/1118/pages/employer-incentives-encourage-employees-to-quit-smoking.aspx.*

Shackleton, T., 2021. A cost-benefit analysis approach to cyber security. *https://www.6dg.co.uk/blog/cost-benefit-approach-to-cyber-security/.*

Timberg, C., 2015. The real story of how the internet became so vulnerable. *https://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/.*

UNFCCC, 2021. Key aspects of the Paris Agreement. *https://unfccc.int/process-and-meetings/the-paris-agreement/the-paris-agreement/key-aspects-of-the-paris-agreement.*

Zhou, Y., Hu, F. & Zhou, Z., 2018. Pricing decisions and social welfare in a supply chain with multiple competing retailers and carbon tax policy. *Journal of Cleaner Production,* 7.Volume 190.