Effective Cybersecurity Training Using Microlearning and the Drip Concept: A Case Study of a Large Regional Hospital

Daisy Le
Gonzaga University

Cassidy Matsuda
Bank of Hawaii

Sebastian Pena
Gonzaga University

Ian Platou
University of Florida

Timothy Olsen
Gonzaga University

ABSTRACT

Cybersecurity is a critical aspect of any business, with organizations investing in sophisticated software to protect sensitive data from potential hacks or breaches. However, human error remains the leading cause of security breaches. Most employees access the internet and email, exposing businesses to various risks. Businesses and organizations within all industries take action to mitigate this risk by providing cybersecurity training. For most, cybersecurity training takes the form of an annual 60-minute-long video training with a short quiz or acknowledgement for completion. This traditional format has been proven ineffective. In contrast, the drip concept employs a constant steam of information to educate and persuade. The concept comes from the practice of and 'drip irrigation' and 'drip marketing' whereby small drops of water provide constant nourishment to plants, or automated emails capture viewers attention. We propose that the use of microlearning and the drip concept will allow employees to become better educated on the topic of IT security. The microlearning technique, which involves repeating small bits of information over an extended period, has been proven effective through programs like Duolingo and Fitbit. In our paper, we explore the implementation of cybersecurity microlearning in the healthcare industry. We utilized two group interviews followed by a member check where our findings were confirmed with the informants. We found that microlearning was effective when combined with effective incentives, however several professional groups required specialized training and different engagement methods.

Subject Areas: Information Systems, HRM and Organizational Behavior
Article Type: Editorially Reviewed Journal Article

Introduction

Problem

Cyber Security Defined

Cyber Security is the practice and measures organizations take to protect their systems, data, networks, etc, from cyber-attacks (Guerra & Kim, 2020). Cyber security has a few layers that need to be taken into consideration for it to be effective. Some of those layers are software, hardware, procedures, and most importantly employee training. A lot of cyberattacks start through human error, a great example of this would be an employee falling for a phishing email or social engineering. Those errors can completely compromise an organization and its sensitive information, even if there are some other cyber security barriers in place to protect the organization. Phishing and social engineering are some of the biggest threats when it comes to cyber security and that is why it is so important to make sure appropriate cyber security training is in place (Guerra & Kim, 2020). Cyber security is an area that cannot be overlooked in today's world and needs to be constantly improved in order to make sure that an organization's sensitive information is being kept safe.

Cyber Attacks

A cyber-attack is the act of trying to maliciously breach a person's or organization's privacy, steal data and benefit from it (Kadivar, 2014). Nowadays, the most common types of cyber-attacks seen across industries are ransomware, malware, Denial of Service (DoS), and SQL injections (Wollman, 2023). Cyber-attacks are a big concern for companies that handle sensitive data, as those organizations might be seen as a bigger target for hackers. It is important for companies to implement security measures that stop hackers from gaining access to the company's sensitive information. The biggest action an organization can take to prevent these attacks is to implement cyber security procedures and training that allow systems to be in place to protect information, and people to know what to look out for. Human error is one of the main points of entry when it comes to cyberattacks, mainly through phishing emails (Ulrich et al., 2021). Due to this, it is very important for organizations to implement Information System Security Training, as it helps employees and other members of the organizations detect threats at an early stage and avoid attacks.

Cybercrime targets and occurs in all industries and businesses of all sizes. Cybercrime has been up 600% since the 2020 COVID-19 pandemic (Halouzka et al., 2023). In 2022, the healthcare sector is the most targeted by cyber-attacks, followed by the financial industry, retail, and education (Exhibit B - Appendix). Healthcare institutions contain patient information, health records, clinical research data, and an abundance of sensitive information. The financial industry and banking institutions contain personal customer data, credit card information, and bank account information. Retail corporations include intellectual property, strategy data, employee and client data, and research and development information. Higher education holds personal information, enrollment data, and financial records. This sensitive information makes these industries most vulnerable to cyber-attacks (Verma & Bharot, 2023).

Human Error in IT Security

Cyber defenses and supporting technologies can only do so much to protect companies from viruses and breaches. In the chain of data security, humans are the most vulnerable element and are becoming increasingly targeted in data hacking. All sophisticated organizations utilize technology, software systems, and emails for operation. In corporations, employees tend to have daily access to two things: computers and emails. Research has shown that 88-95% of breach incidents in companies are caused by human error (CISOMAG, 2020).

Phishing is the most frequent and successful attack on companies. An average of $4.9 million is lost to phishing attacks (Smartlockr, 2023). Even large corporations with sophisticated technologies can be subject to breach through phishing. One of the costliest phishing attacks happened to Facebook and Google between 2013 and 2015. The companies were attacked over the course of two years by an attacker who impersonated Quanta and extracted over $100 million from both companies. One of the most common phishing techniques practiced by hackers across the world is impersonation of high-level executives and instructing employees to transfer money or buy gift-cards. Crelan Bank, in Belgium, fell victim to this business email compromise scam that cost the company around $76 million (Al-Haija & Al Badawi, 2021).

Cybersecurity Compliance Training

It has been a challenge in the IT world to mitigate human error. One of the most common actions organizations take to combat cyber breaches is by educating users. This is commonly taken in the form of annual online cybersecurity training with a short quiz or acknowledgement for completion. Organizations have also adapted “phishing” email ploys to test employees and educate those who failed. Data shows that investing in security awareness training can result in 70% fewer security breach incidents. In addition, password security improves by 30-50%, phishing awareness improves by 40%, and costs of breaches are reduced by 50% (Ponemon Institute LLC, 2022). Environmental, social, and governance (ESG) trends are being increasingly adapted by corporations due to pressure from stakeholders. ESG, also known as the practices, to be socially responsible, includes security awareness training to reduce organizational vulnerability. Security awareness doesn’t only impact businesses, but also affects its customers, suppliers, distributors, and everyone else involved in the business operations.

This study investigates the a novel form of cybersecurity compliance training at a large regional hospital in the United States. In the following section we describe the novel form of cybersecurity training. Next, in the Case Study and Analysis section we describe the Hospital and their training program. We conclude the paper with a discussion of our findings including the successes and challenges experienced by the hospital.

Framing & Literature Review

Microlearning in Professional Development

Training has traditionally been a time-consuming and monotonous process. The ability to educate employees swiftly and efficiently is vital for businesses to maintain their competitive edge in today's rapidly evolving market (Dolasinski & Reynolds, 2020). Microlearning has emerged as a promising solution to these challenges, offering a more engaging and efficient approach to skills development. According to a study by Cognitive Design and Statistical Consulting LLC, microlearning is particularly effective for hard skills training due to its alignment with the cognitive skills learning system, which encompasses the prefrontal cortex and hippocampus (Maddox, 2018). By leveraging the inherent processing characteristics of these brain regions, microlearning techniques facilitate better retention and application of new knowledge in real-world situations.

In today's fast-paced business environment, learners face an ever-increasing amount of information to process and comprehend. Microlearning offers a practical solution by breaking down complex content into smaller, more manageable units, making it easier for learners to understand and apply. This method encourages critical thinking and problem-solving, which is essential in industries that are constantly evolving due to advancements in technology and systems (De Gagne et al., 2019).

The effectiveness of microlearning has been demonstrated in various professional contexts, including mobile apps for on-the-job training, interactive case-based teaching sessions, mobile gaming devices for skill development, and streaming video systems for real-time learning (Hayes Lane et al., 2016). Consequently, microlearning has garnered widespread support from business educators, training programs, and organizations as a valuable tool for promoting employee learning, professional development, and ongoing education.

Microlearning Applications

Fitbit and Duolingo both utilize microlearning strategies to deliver content and foster a sense of progress and achievement among users (Ringeval et al., 2020). Fitbit, for instance, breaks down fitness goals into small, manageable steps, allowing users to track their progress throughout the day. The platform also provides personalized feedback and insights on users' activity levels, sleep patterns, and nutrition, facilitating an incremental approach to improving health and wellness. This microlearning approach not only makes it easier for users to engage with the content but also encourages long-term commitment to their fitness goals.

Similarly, Duolingo utilizes microlearning principles by dividing language lessons into small, focused segments that teach vocabulary, grammar, and pronunciation. These bite-sized lessons are designed to be completed in just a few minutes, making it easy for users to fit language learning into their busy schedules. Duolingo's gamified approach, which includes elements such as streaks, points, and levels, further enhances engagement and motivation by rewarding users for their consistency and progress.

Proposition

The current paper proposes that microlearning is the most effective way to teach content, as it leads to increased retention and engagement among learners. Microlearning is an educational strategy that focuses on delivering information in small, easily digestible units, with a strong emphasis on the practical application of the content.

Solution

Microlearning

Microlearning can play a pivotal role in minimizing human error in IT security and cyber-attacks. It involves breaking down complex information into smaller, easily digestible modules that can be quickly absorbed and retained (Busse, Lange, Hobert, et al., 2020). The objective is to provide just-in-time training that is relevant, effective, and easily accessible. One way to implement microlearning is through micro-lessons. These short lessons can be delivered through a mobile app or desktop software and can be completed in just a few minutes. This allows employees to learn at their own pace and in their own time, making the learning process more accessible and convenient. Additionally, micro-assessments can be used to test and reinforce employees' understanding of key concepts (Busse, Lange, Briesemeister, et al., 2020). This can be done through regular quizzes or simulations that mimic real-world scenarios. This way, employees can practice applying the information they've learned in a safe environment, reducing the risk of human error.

Gamification

Gamification is a powerful tool for implementing microlearning in technology. It integrates game-like elements into the learning process, making it more engaging and enjoyable (Schöbel et al., 2021). This approach has proven to increase motivation, engagement, and information retention. By transforming the learning process into a game, employees are more inclined to participate in training and retain the information. Utilizing points, badges, and leaderboards fosters a sense of competition and motivation for employees to excel. With the interactive and hands-on learning experiences, users are more likely to retain information and apply it in real-world situations (Jia et al., 2023). One of the benefits of this approach is the in-time training. For example, short games or challenges can be delivered through a mobile app or desktop software, allowing employees to learn at their own pace and in their own time. This makes the learning process more accessible and convenient for employees.

Drip

Drip is a newly researched concept and communication strategy that sends "drips" of information continuously over time to engrain information into the viewer's mind. Drip stands for differentiate, reinforce, inform, and persuade (Rubin, 2022). It is a strategy used to achieve education and persuasion tactics. Drip was originally very popular in marketing, making the term 'drip marketing' well known in the sales industry. Drip marketing would involve sending automated emails, repetitive ads to capture viewers' attention, and other visualization and persuasion tactics to be top-of-mind for potential customers (Kalpana, 2013). Over time, the

concept has spread throughout other industries and began utilized for education, rather than persuasion. The drip method now capitalizes on engagement, repetition, and testing and teaching to make information stick. The brain is optimized to learn, process, and recall information through small quantities over time. Short bursts of targeted learning results in more knowledge retention and higher confidence in applying the mastered concepts into real life. Drip learning has been used in organizations to train and educate employees on information through small, digestible, and intentional bursts of information (Wright, 2021).

Case Study and Analysis

MultiCare

MultiCare is a not-for-profit health care organization located in Washington state that consists of a network of 12 hospitals, over 230 clinics, and over 23,000 members. MultiCare generates over $4 billion in revenue. Brant Borchert serves as the Assistant Vice President and Chief Operating Officer for Information Services and Technology in the Inland Northwest and Central Washington regions for MultiCare Health System. Borchert acts as the regional IT executive leader with an aim to deliver the highest value technology enabled healthcare.

Borchert identified that employees at MultiCare need access to the internet and email to conduct their jobs effectively. In the information security world security risks often arise through these two avenues. MultiCare requires its employees to participate in yearly security awareness education training under the name “Annual Mandatory Education” which was provided by a third-party standardized IT education platform. The annual training takes about 45 minutes to complete, so Borchert thought about taking a different and unique approach to change this critical area of information technology. The idea of providing an alternative and engaging microlearning approach for employees to satisfy their information security and other training requirements led to the partnership between MultiCare and drip7.

One of Borchert’s goals is for the MultiCare employees to exhibit solid security behavior as the MultiCare hospital system holds personal client data, which the hospital system has a duty to protect. Data breaches are very costly, so Borchert had posed the question “how do you measure a non-event happening?” as it is easy to say an initiative would have been worth the investment in hindsight. Properly teaching and equipping employees with practical info security information in a way that motivates them is a smart approach to combat costly information security risks. Borchert realized a partnership with Drip7 to develop a microlearning platform could result in significant learning outcomes among MultiCare employees. Due to the consistent employee engagement with bite-sized practical info security information and a gamification reward plan in place to incentivize employees, Borchert concluded the initiative with drip7 would be worth the investment.

Drip7

MultiCare was Drip7's first customer. The partnership began when Drip7 was founded by Heather Stratford in early 2020, during the start of the COVID-19 pandemic. Drip7 is a full training platform designed to educate users on cyber-security knowledge. Drip7 is available on all platforms and provides a mobile and convenient source for IT education. The consistent training and ongoing skill development allows users to gain and retain knowledge. Drip7 utilizes microlearning to provide a fun, engaging, skill-learning experience for its users. Through videos, short articles, and quizzes, users learn core cybersecurity content. The app asks one simple question a day, called "drips", 7 days a week. Users can spend as much time on the app as they would like to learn the content before answering a single question. Users are rewarded through points, which are kept on an organization leaderboard. Therefore, users are encouraged to engage in competition with themselves and others by completing tasks and quizzes that increase their ranking on the leaderboard. The rewards-based learning system incentivizes Drip7 users to continuously engage with the app and its content. MultiCare saw Drip7 as the opportunity to deliver cyber education to their workforce in a fun, engaging way. The two companies worked together to create a customizable platform with educational content presented in a fun and easy way. MultiCare helped Drip7 administer the rollout of their platform as its first customer and provided feedback on the content and ease of use. The official rollout of Drip7 at MultiCare began on August 1, 2021. Drip7's platform allows the MultiCare administrators to see who is logging on, the amount of time that is spent on the app, consecutive user streaks, and player rank.

Drip7 is currently operating a blue ocean strategy and has little competition in their niche offering. Drip7's core competency is the microlearning and customization aspect of their cybersecurity educational platform. There are currently no other competitors in the market using drip education to teach cybersecurity content. However, there are competitors with standardized training programs for teaching cybersecurity to workforces. Many of their IT education competitors, like Living Security, Ninjio, and Wiser Training are traditional, off the shelf platforms with no customization or flexibility. Drip7 operates on all devices, with their main distribution being mobile phones. This makes the platform easily accessible and available for users to play at their convenience. In contrast, competitors commonly used CDs or downloadable computer apps to deliver their content.

Drip7 Platform

Drip7's platform has three layers that change depending on company contracts. The base of Drip7's platform education is the cyber-core (See Figure 1). The cyber-core contains the 7 core topics universally needed for all companies. These topics include the cyber security bases and best practices for acting on the internet. The second layer of the platform education is compliance. This varies based on different industries and institutions. For example, hospitals need to provide compliance information on HIPPA while construction and manufacturing will require OSHA. The third layer of Drip7's informational platform is human resource and

leadership focused. This is becoming a more common implementation onto the platform's educational agenda, with topics including DEI and ESG based information.

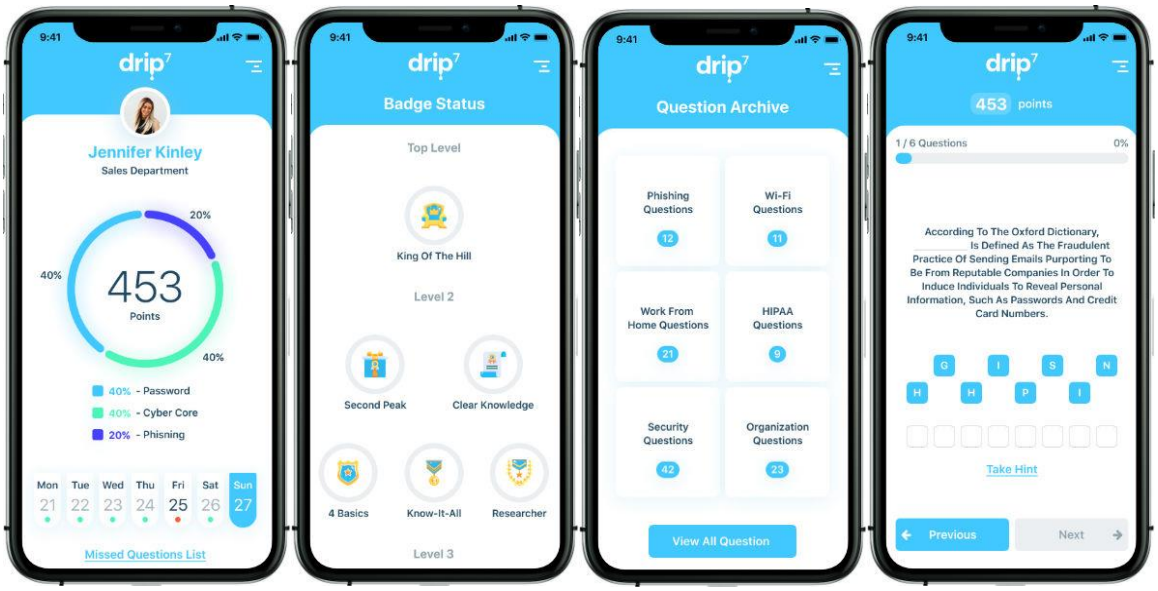

Figure 1. Drip7 App Screenshots (provided by Drip7)

Implementation

Drip7's introduction into MultiCare involved a lot of testing for trials and errors. MultiCare assisted Drip7 through feedback on the ease of use, downloading and operating on different phones, and enjoyment of users. The official rollout of Drip7 at MultiCare was on August 1, 2021. MultiCare's goal was to get 1,000 employees on the app within the first 3 months. They worked to reach this goal by marketing the app through emails, flyers, and monthly IT newsletters. In addition, Borchert highlighted Drip7 in leadership and department meetings in effort to get the word spread hospital wide.

Findings

Overcoming Challenges

1. *IT education delivered through an app in healthcare industry.*

One of Borchert's biggest requests for Drip7's microlearning technique was to have it be delivered through a mobile app. Prior to Drip7, information security training at MultiCare was delivered annually through video training with onsite computers. The MultiCare IT department identified that people carry around and utilize their mobile phones all day, every day. Therefore,

delivering the microlearning experience through a mobile app was crucial for the Drip7 implementation.

This challenge of creating the platform in the form of a mobile app was overcome by the partnership with Drip7. Stratford and her innovative team met Borchert's request by delivering the IT security educational platform in the form of an app. The mobile app delivery allows users to access Drip7 easily from their mobile devices. Individuals value being able to access everything they need at the tip of their fingers through mobile devices. Therefore, access to Drip7 on smartphones was a crucial part of implementing this microlearning platform to the MultiCare workforce. The current environment also values hybrid environments, and the Drip7 app allows users to access it at any time, from any place. This plays into the ease of use and convenience for users, which is a motivating factor for many individuals. As a drip microlearning platform, bursts of small, repetitive information are key to the learning environment. Therefore, a mobile app accessed on smartphones was the simplest way to execute this concept. The mobile app increases the use frequency, therefore making the knowledge learning experience more effective.

MultiCare's healthcare training for employees is required to be completed once a year. Healthcare information security is very important because it trains employees in the best practices to protect client information. However, only completing the training once a year does not lead to the strongest retention of information. Using an app that employees can interact with more frequently provides consistent interaction and learning. Therefore, the ease of having the training on an app and the frequency of the learning drips make for a desirable approach to information security training in the healthcare industry.

2. *Incentivizing the MultiCare workforce to utilize Drip7.*

One of MultiCare's greatest challenges was motivating people to utilize the voluntary Drip7 app. MultiCare and Drip7 worked tirelessly together to bring the Drip7 microlearning platform to market. MultiCare's workforce consists of over 20,000 team members, which includes full-time employees, providers, and contractors. Drip7 is not mandatory for employees because MultiCare is prohibited from mandating this for unionized workers. For example, the nurses' union requires that if MultiCare were to mandate participation in the app, they would need to provide the technology and overtime pay to do so. This is not feasible for MultiCare because they don't have the ability to provide all unionized workers with mobile phones just for the Drip7 app and would have difficulty keeping track of the time spent on the app. Drip7's app is designed for frequent, daily knowledge reinforcement that is easily accessible on smart devices. If MultiCare wanted to mandate participation, they could set aside time and technology for nurses to participate daily. However, this would be a faulty use of resources as the thousands of nurses would be taking time away from caring for patients every day in the hospitals.

MultiCare decided that making app participation voluntary and providing incentives would be the best route in getting workers on the app. MultiCare heavily marketed Drip7 among their workforce and encouraging employees to opt in. For months leading up to the start of the

program, MultiCare posted flyers around the hospital campuses, spread the word to departments and employees, and geared up to provide incentives for winners. MultiCare decided that the best incentive for getting employees on the Drip7 platform was with cash rewards. Drip7 contains data on individual streaks, success rates, and rankings, so MultiCare names monthly winners with the highest rankings. In the first month, MultiCare created lottery style checks for the winners and included the pictures in websites, social media, and monthly newsletters. The cash rewards are now a line item in the IT budget, which creates goodwill with the company and IT department.

Drip7 Ranking

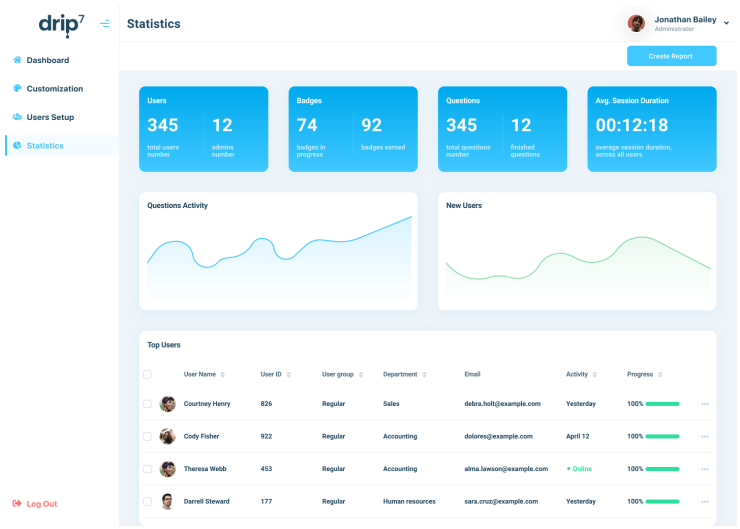

Figure 2. Drip7 Ranking Feature Example (Provided by Drip7)

MultiCare rewards employees based on monthly ranking. They will take the top three highest ranked users each month and give them cash rewards based on performance (Figure 2). The KPI that determines ranking combines a variety of statistical data to respectively rank users. These metrics include highest answer streaks, session time spent in the app, and percentage of correct questions. It is the most accurate and comprehensive way to rank employees. Thus, the user should focus on improving all aspects including increased time spent learning, consecutive daily logins, and correctly answering questions, to increase their ranking and opportunity for rewards.

Takeaways & Successes

1. *Microlearning is an effective way of learning.*

Drip and microlearning education are becoming increasingly utilized in many different industries to educate diverse workforces. Microlearning is the most effective way of educating employees on important content. It ensures reinforcement of knowledge through 'bite-sized learning nuggets' that are repeated through tiny chunks of information. Learning activities can include small pieces of information, small quizzes, and/or short videos. Microlearning is preferred by many organizations because programs are easy to create and implement, it is easy to track progress, and it's a budget-friendly implementation. Microlearning can also be supportive in hybrid business models, as employees can do training in various locations because time constraints are not a factor. Microlearning is a continuous process, rather than a one-time training, which maximizes the user's learning time and allows people to learn and practice at their own pace. Data has shown that microlearning improves engagement by 50% and supports long-term retention by 80% (Kumar, 2022). Microlearning has the advantage of providing employees who are going through cyber security training with an engaging platform. One of the main ways that cybersecurity training is done nowadays is through a yearly training session where employees go through a presentation that has dozens of slides. This type of training has proven to be ineffective when compared to microlearning. Microlearning can provide an engaging training experience that reinforces key cyber security concepts in a more efficient way.

2. *Optional educational programs with incentives can increase employee goodwill and retention.*

Employee recruiting, motivation, and retention is one of the most important aspects in all organizations. Turnover is very costly for businesses and most organizations cannot afford to lose their top employees. For MultiCare, retention of nurses is crucial, as turnover costs the hospital around $11,000 per nurse. Therefore, businesses are finding it increasingly important to motivate, train, and retain their workforce. This includes onboarding and continuously training employees in an effective and engaging way. Employee education is beneficial for both the company and individual employee motivation. Data shows that 70% of employees would leave their current organizations for a job in a company that invests in employee development and training. Retention rates can rise 30-50% when companies implement strong learning cultures (Lorman Team, 2021). Therefore, educational platforms like Drip7 can motivate and engage employees through their offerings and education. The cash reward incentives provide employees with the opportunity to engage in fun, learning activities. The Drip7 program can provide the means for company culture and motivation to increase.

MultiCare was unable to give us data that could quantify increased goodwill and reduction of turnover. However, providing incentives for employees and giving monthly cash rewards is an additional benefit of the job. It shows that MultiCare cares about the education of employees and rewards them for their efforts. Drip7 has seen that all generations are excited in the microlearning app, and they have seen buy-in from the most diverse groups of people. The platform is also rewarding on an individual level and makes users feel confident and successful.

Apps like Wordle and Candy Crush have been popular with users of all ages and capitalize on self-satisfaction from success and streaks. Drip7 operates in the same way, thus when MultiCare provides the app to their workers it creates a multitude of beneficial factors. MultiCare and Drip7 have heard tremendous positive feedback about the platform (Exhibit C, Appendix), showing it increases employee satisfaction and thus may be linked to lower employee turnover. However, MultiCare will still need to evaluate data and quantify a connection or causal relationship between app implementation and employee turnover.

Current Challenges

1. *Some divisions or departments need more targeted training.*

Another challenge for MultiCare is preferably having differentiated training for different departments. Currently, the Drip7 platform provides standardized training to all MultiCare's employees. It includes the core cybersecurity education and HIPPA regulations required for the healthcare industry. However, some employees may benefit from more targeted training. For example, system administration in IT would need different training than the general hospital nurses. In addition, departments are very differentiated at MultiCare; some may be more subject to auditing than others and some may have access to more sensitive information than others. These factors pose the challenge of different departments needing differentiated and targeted training.

2. *Employee Engagement and Retention*

One of the significant challenges faced by organizations in implementing effective cybersecurity training is maintaining employee engagement and retention of the learned material. Traditional training formats, such as annual video sessions, often fail to capture the interest of the employees and lack the reinforcement needed for long-term retention. Employees may view these sessions as a mundane obligation rather than a valuable learning opportunity. This challenge emphasizes the need for innovative solutions that not only educate employees on cybersecurity best practices but also maintain their interest and encourage active participation in the learning process. By addressing employee engagement and retention, organizations can create a culture of continuous learning and improvement in their IT security practices, ultimately reducing the risk of human error-related breaches.

Discussion

Next Steps

As a 3-year-old startup company, Drip7 is still continuously revising, updating, and tweaking their platform. Their company and app platform has gained worldwide success, but the founder and company are still focusing on learning, growing, and improving. There are a lot of missing pieces to Drip7's platform, which they are investing research and development into improving. Two of their main focuses moving forward are integrating into other platforms and measuring success of the IT education within organizations.

Integrating into Other Platforms

Drip7 has expanded across the world into multiple industries and thousands of companies. Drip7 recently started to gain great traction in banks and financial institutions. Currently, the company is working on integrating digital banking and financial accounts for use by customers and clientele.

Measuring Success

Drip7 and MultiCare's biggest challenge is measuring the success of security training. Some of the questions that have yet to be researched and answered are:

- Is increased security training directly correlated with decreased security breaches?
- Is the Drip7 method more effective than traditional 45-minute annual training?
- Does implementation of the Drip7 app and ongoing rewards increase employee goodwill and decrease turnover?

Conclusion

Cybersecurity is a big issue in today's world, it is important for all organizations to implement information system security training as it helps them stop hackers from obtaining their sensitive information. With most of cyberattacks occurring due to human error, it is key for organizations to make sure that the training their employees go through, truly helps them retain enough cyber security information to protect the organization, its customers, and its sensitive information. Using Multicare and Drip7 as an example, we are confident to say that microlearning is a better platform when it comes to cyber security training. It helps employees retain more information while being more engaged in the training process, which eventually can lead to employees being more aware of cyberattacks and threats, strengthening the organization's barriers against these attacks.

References

Al-Haija, Q. A., & Al Badawi, A. (2021). URL-based phishing websites detection via machine learning. *2021 International Conference on Data Analytics for Business and Industry (ICDABI)*, 644–649. https://ieeexplore.ieee.org/abstract/document/9655851/

Busse, J., Lange, A., Briesemeister, M., & Schumann, M. (2020). BECOME COMPETENT IN 15 MINUTES? - THE SUITABILITY OF MICRO LEARNING FOR COMPETENCE DEVELOPMENT. *ECIS 2020 Research Papers*. https://aisel.aisnet.org/ecis2020_rp/12

Busse, J., Lange, A., Hobert, S., & Schumann, M. (2020). How to Design Learning Applications that Support Learners in their Moment of Need – Didactic Requirements of Micro Learning. *AMCIS 2020 Proceedings*. https://aisel.aisnet.org/amcis2020/is_education/is_education/15

CISOMAG. (2020, September 12). "Psychology of Human Error" Could Help Businesses Prevent Security Breaches. *CISO MAG | Cyber Security Magazine*. https://cisomag.com/psychology-of-human-error-could-help-businesses-prevent-security-breaches/

De Gagne, J. C., Park, H. K., Hall, K., Woodward, A., Yamane, S., & Kim, S. S. (2019). Microlearning in Health Professions Education: Scoping Review. *JMIR Medical Education*, *5*(2), e13997. https://doi.org/10.2196/13997

Dolasinski, M. J., & Reynolds, J. (2020). Microlearning: A New Learning Model. *Journal of Hospitality & Tourism Research*, *44*(3), 551–561. https://doi.org/10.1177/1096348020901579

Guerra, K., & Kim, D. (2020). Cybersecurity: A Definition across Europe and North America. *AMCIS 2020 Proceedings*. https://aisel.aisnet.org/amcis2020/info_security_privacy/info_security_privacy/16

Halouzka, K., Coufalíková, A., Buřita, L., & Kozak, P. (2023). The impact of the Covid-19 pandemic on the evolution of cyber threats. *2023 International Conference on Military Technologies (ICMT)*, 1–8. https://ieeexplore.ieee.org/abstract/document/10171277/

Hayes Lane, S., Serafica, R., Huffman, C., & Cuddy, A. (2016). Making Research Delicious: An Evaluation of Nurses' Knowledge, Attitudes, and Practice Using the Great American Cookie Experiment With Mobile Device Gaming. *Journal for Nurses in Professional Development*, *32*(5), 256–261. https://doi.org/10.1097/NND.0000000000000292

Jia, F., Bao, X., & Yu, J. (Joseph). (2023). Gamification of Digital Platform: A Meta-analysis. *PACIS 2023 Proceedings*. https://aisel.aisnet.org/pacis2023/103

Kadivar, M. (2014). Cyber-Attack Attributes. *Technology Innovation Management Review*, *4*(11), 22–27.

Kalpana, S. (2013). DRIP MARKETING: SLOW AND STEADY WINS THE CUSTOMERS. *CLEAR International Journal of Research in Commerce & Management*, *4*(6). https://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=22494561&asa=Y&AN=119727960&h=MrNlUhiTtpF8J4lIhPA2clA0GYNiKR2fralZtvATXdXuFb02oSUEij601ZyTUqrySeGq72bZeNAnyUbRVYxrZw%3D%3D&crl=c

Kessem, L. (2021). Threat Actors' Most Targeted Industries in 2020: Finance, Manufacturing, and Energy. *Security Intelligence*. https://securityintelligence.com/posts/threat-actors-targeted-industries-2020-finance-manufacturing-energy/

Kumar, S. (2022, August 16). *Microlearning In 2022*. eLearning Industry. https://elearningindustry.com/microlearning-in-2022

Lorman Team. (2021). *39 Statistics that Prove the Value of Employee Training*. https://www.lorman.com/blog/post/39-statistics-that-prove-the-value-of-employee-training

Maddox, T. (2018, November 28). Microlearning and the Brain. *Chief Learning Officer - CLO Media*. https://www.chieflearningofficer.com/2018/11/28/microlearning-and-the-brain/

Ponemon Institute LLC. (2022). *Cost of a data breach report 2022*. IBM. https://www.ibm.com/downloads/cas/3R8N1DZJ

Ringeval, M., Wagner, G., Denford, J., Paré, G., & Kitsiou, S. (2020). Fitbit-Based Interventions for Healthy Lifestyle Outcomes: Systematic Review and Meta-Analysis. *Journal of Medical Internet Research*, *22*(10), e23954. https://doi.org/10.2196/23954

Rubin, V. L. (2022). Manipulation in Marketing, Advertising, Propaganda, and Public Relations. In V. L. Rubin (Ed.), *Misinformation and Disinformation: Detecting Fakes with the Eye and AI* (pp. 157–205). Springer International Publishing. https://doi.org/10.1007/978-3-030-95656-1_6

Schöbel, S., Schmidt-Kraepelin, M., Janson, A., & Sunyaev, A. (2021). Adaptive and Personalized Gamification Designs: Call for Action and Future Research. *AIS Transactions on Human-Computer Interaction*, *13*(4), 479–494. https://doi.org/10.17705/1thci.00158

Smartlockr. (2023). *Biggest cause of data leaks: Human errors*. http://www.smartlockr.io/en/blog/biggest-cause-data-leaks-human-errors

Statista. (2023). *Industries most targeted by web application attacks 2022*. Statista. https://www.statista.com/statistics/221293/cyber-crime-target-industries/

Ulrich, P., Frank, V., & Buettner, R. (2021). One Single Click is enough – an Empirical Study on Human Threats in Family Firm Cyber Security. *Hawaii International Conference on System Sciences 2021 (HICSS-54)*. https://aisel.aisnet.org/hicss-54/in/behavioral_is_security/5

Wollman, Y. (2023, June 1). How to Keep Cyberattacks from Tanking Your Balance Sheet. *Harvard Business Review*. https://hbr.org/2023/06/how-to-keep-cyberattacks-from-tanking-your-balance-sheet

Wright, K. (2021, September 16). *The Ultimate Guide to Drip Content*. Restrict Content Pro. https://restrictcontentpro.com/blog/drip-content-ultimate-guide/

Appendices

Exhibit A: Types of Cyber Attacks (Kessem, 2021)

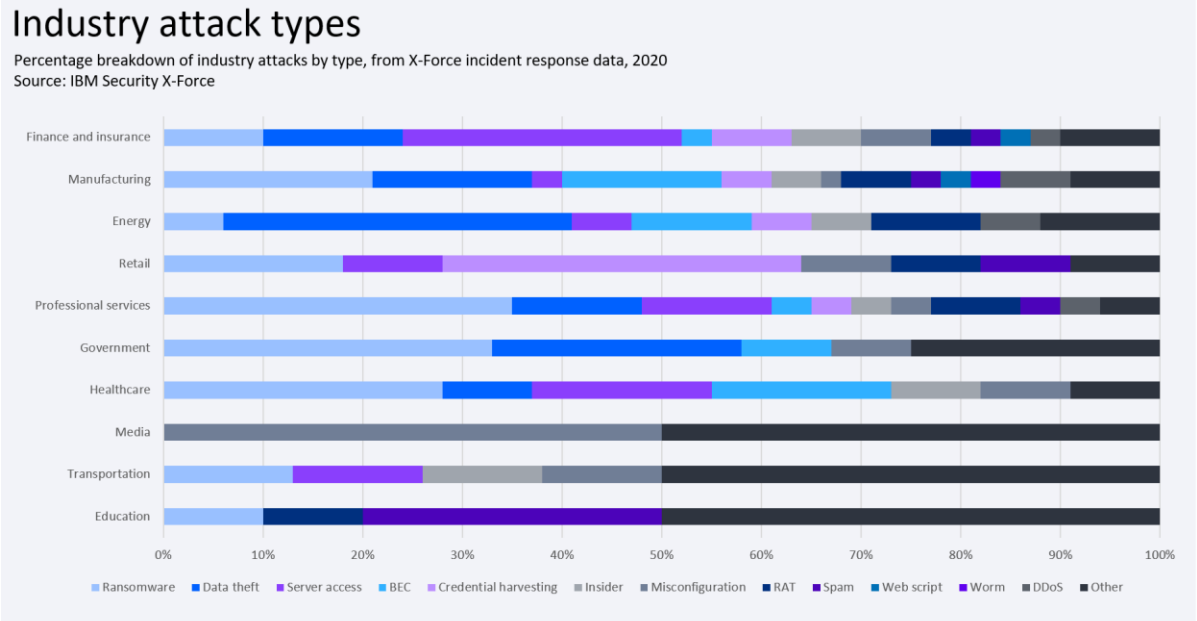

Exhibit B: Cyber Attacks by Industry (Statista, 2023)

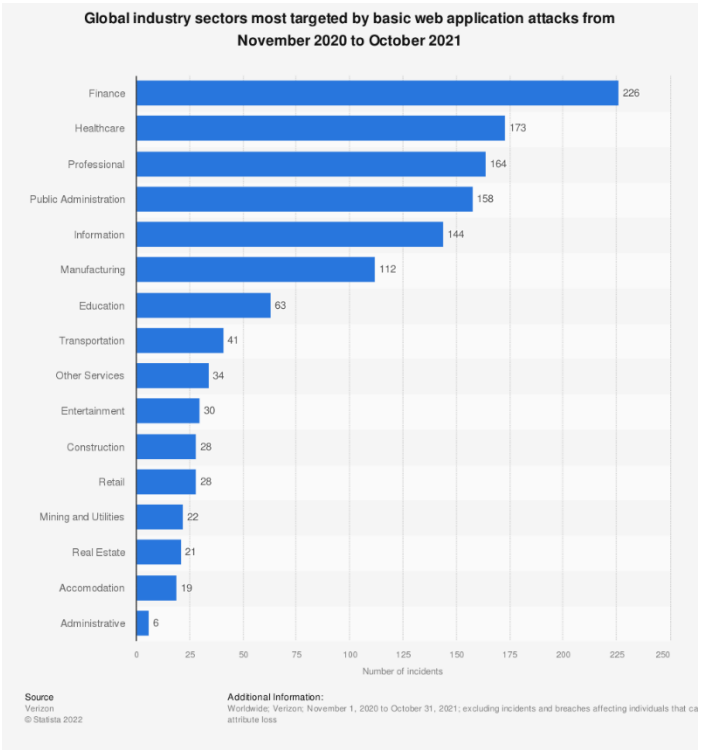

Exhibit C: Drip7 Testimonies (Provided by Drip7)

What People Say about Drip7

*"I really like trivia quizzes, so when I saw this ... **I was excited to give it a try**. It's been a **part of my daily routine** to check in and answer a question. I think answering my daily questions has kept IS&T security much more on the front of my mind for a much longer period of time than an annual module. I've been intrigued by the tidbits about social engineering and the various ways others might be trying to get into various systems."*

*"Who doesn't love a fun contest, with prizes ... Once I began playing, I stayed engaged as I discovered **the content is applicable in both my work and personal life** ... I downloaded the app on my personal phone which makes it easy access for answering the daily question even when I'm at home. **This takes only a few seconds of my time and worth it**!"*

*"I found Drip7 to be an excellent source for challenging myself and learning about information security. **I learned a lot** about how information security works, I learned a lot of new terminology, and finally— I acquired an understanding of how to protect company and my personal assets from being compromised by hackers."*

drip7

What People Say about Drip7

*"I played Drip 7 because I use and transfer a lot of data in my work, so I'm concerned about security and thought this might offer some relevant learning. **I was pretty surprised by how much I learned**, and because of Drip7 **I have changed my practices around passwords** in my work and personal realms."*

***"I enjoy playing Drip7 because it challenges my knowledge** on internet safety, data protection and even HIPAA. Drip7 has helped me identify gaps in my understanding of how to protect data — personal and otherwise."*

*"I'm always up for something new and this little game is a **fun change** from the usual newsletter or quiz that can be sent out that no one really pays much attention to. Competition can be fun and watching where you are on the leaderboard is great...It's been interesting to me to see the questions that I get wrong and **find areas I need to improve upon**."*

drip7