2021

University of North Carolina Wilmington

Master of Science in

Computer Science and Information Systems

Proceedings

https://csbapp.uncw.edu/mscsis

A LOOK AT SECURITY AWARENESS TRAINING, ENGAGEMENT, AND EMPLOYEE MOTIVATION

Jennifer Wescott

A Capstone Project Submitted to the
University of North Carolina Wilmington in Partial Fulfillment
of the Requirements for the Degree of
Master of Science

Department of Computer Science
Department of Information Systems and Operations Management

University of North Carolina Wilmington

2021

Approved by

Advisory Committee

Dr. Ron Vetter	Dr. Geoff Stoker	William Wetherill
_____	_____	_____

_____
Dr. Ulku Clark, Chair

Accepted By

_____
Dean, Graduate School

TABLE OF CONTENTS

Page

ABSTRACT

A Look At Security Awareness Training, Engagement, And Employee Motivation.
Wescott, Jennifer, 2021. Capstone Paper, University of North Carolina Wilmington.

The motivation for this paper comes from experience working on the security team and taking opportunities to engage with employees to build the partnership between the security team and employees. While conducting in-person presentations, giving public acknowledgements, and other, more personalized, security awareness experiences – the organization saw an increase in willingness to openly discuss security as well as self-report certain incidents. There was an interest in getting more data around the effects of these initiatives. A survey with knowledge-based and attitude-based questions was first conducted to check competency of those who had the more personalized experience versus those that did not. The competency scores from that survey did not show much of a difference when provided these more personal communications versus just the typical video presentations to cover security training compliance requirements. But on the attitude-based questions, there was data that showed that most individuals preferred that personal experience. This majority response led the company to review employee reporting over the course of three years - where these, seemingly more personal, engagement activities fluctuated and so did employee response - which shows that although personal touches may not lead to higher competency scores, they will lead to higher motivation to communicate and partner with the security team in general. And after all, what an organization should really be after is not only high competency scores but rather instilling employees with the confidence and motivation to act during what could seem like or be a potential crisis or security incident.

LIST OF FIGURES

Figure Page

CHAPTER 1: INTRODUCTION

How does an organization encourage action and collaboration regarding security amongst employees? In this paper, the different aspects that may impact security awareness and communication with the security team will be discussed. The motivation of this paper and capstone project is to show the importance of a continued conversation with employees about security in general. It does not necessarily have to be a formal presentation to keep it top-of-mind, but it does need to be continuous and engaging to see an increase in collaboration with employees and the security team. Often, security awareness training is provided to maintain compliance with certain regulatory and/or standard requirements to pass security audits. The company wanted to challenge that baseline goal by going further in engagement opportunities to see if these would increase the communication and collaboration between employees and the security team. This is especially important because of the role that employees themselves play in security as they are often deemed the weakest link. There are many ways to engage employees, but the seemingly most impactful moments to make an impression are at the start of an employee's tenure within an organization and it should continue through various avenues such as newsletters, informal posts/messaging, public "kudos" or acknowledgements, casual conversation, and being responsive and transparent where possible.

Because reaching and maintaining compliance is the typical baseline when it comes to security training and awareness, this paper will discuss those requirements that an organization/institution may be audited against, as well as the more recently trending audit certification within the US.

While communication, engagement, and compliance are important aspects, other variables come into play that have been researched such as capability maturity models and how those are important in building and maintaining the relationship amongst different departments for increased cohesiveness throughout the entire company. This plays a big part in how Information Technology (IT) and Security is seen and collaborated with as well and that can make a big difference in the overall impact of an organization's security posture and awareness.

This paper will first review capability maturity models, which will segue into a security-focused maturity model that is ultimately compliance-related, and then discuss influence and self-efficacy around security awareness. To end, there are the activities the company performed pertaining to training, awareness, and engagement, which is believed to have increased employee responsiveness and collaboration with the security team.

CHAPTER 2: REVIEW OF LITERATURE REVIEW AND ANALYSIS

2.1 Capability Maturity Model(s)

When considering the cohesiveness amongst varying departments within an organization, a great place to start is to look at and even measure, where possible, the relationship between the business and the IT department. There are differing frameworks for maturity models that can be utilized to help measure this cohesiveness. One of the models, known as the Capability Maturity Model, is intended to outline how business and IT (including security) can better align for more effective organizational performance.

2.1.1 Why is it so difficult to align business with IT?

In the article by Luftman and Kempaiah (2007), there are a few reasons. The first being that not only should IT align with the business, but the business also needs to align with IT because IT can "both enable and drive business change." (Luftman & Kempaiah, 2007, p. 2). Often, IT can struggle to keep up with the business growth and requirements, and this can cause the business to almost feel constrained by IT. The difficulties for IT can come from anything such as departments or employees wanting to add new systems for productivity within their own department to hiring at a rapid rate. When adding a new system or ripping/replacing systems, IT is the department that will most likely need to not only implement but also administer those systems which could place ownership and cost on the IT department. This can leave the IT budget disproportionately inflated and cause the IT department to not have the budget to hire more employees to administer those new systems. Therefore, the current employees must take on that administration and ownership responsibility which can come with a learning curve. This can strain both IT and the business departments. Hiring at a rapid pace can place strain on the IT department

as well because they are constantly setting up devices and training new employees either in onboarding or taking in an increased amount of helpdesk tickets because new employees typically need more technological assistance at first. These are just two examples, of many, that could be related to the issue at hand.

The second reason it has been difficult to align business and IT is "that organizations have often looked for a silver bullet." (Luftman & Kempaiah, 2007, p. 2) While having the right technology such as infrastructure and applications in place, it is not necessarily the answer to alignment. When technology is solely relied upon to build that alignment between business and IT, it will not work. All six components are needed to attain alignment. (Luftman & Kempaiah, 2007) Technology and automation is often the go-to for trying to get people in different departments on the same page and working together in an efficient, streamlined manner. The keyword in the previous sentence though is "people". To help people in different departments get on the same page, we need other people who are willing to reach out and build bridges of communication and collaboration, maybe *using* the technology and automation, but the most important piece is people actually talking and understanding one another.

The third reason that it is difficult for business and IT to align is that "there has not been an effective tool to gauge the maturity of IT-business alignment – a tool that can provide both a descriptive assessment and a prescriptive roadmap on how to improve." (Luftman & Kempaiah, 2007, p. 2) Getting on the same page and understanding the different departments' use of certain terminology and verbiage would be a great start. Once employees within each department can speak each other's language, or at least begin to, and have empathy for each other's roles and the importance of those roles, there is a start to a roadmap of understanding and maturity of the relationship.

The six proposed components layered into a capability maturity model that can ultimately be measured and assist in alignment are as follows: Communications, Value, Governance, Partnership, Scope and Architecture, and Skills. (Luftman & Kempaiah, 2007) Many of these translate into assisting the relationships related to security as well. The next section discusses pertinent components in more detail.

2.1.2 Capability Maturity Model Components

As mentioned, the model's six components are Communications, Value, Governance, Partnership, Scope and Architecture, and Skills and all six are needed for alignment. The effort discussed in this paper was to strengthen and mature the Communications and Partnership components, and these are focused on in more detail within this section.

Communications: Used to "measure effectiveness of the exchange of ideas, knowledge, and information between IT and business organizations, enabling both to clearly understand the company's strategies, plans, business and IT environments, risks, priorities, and how to achieve them." (Luftman & Kempaiah, 2007, p. 2) Within the organization, there have been many domain exploration meetings, and this helps everyone in the meeting understand the language of the domain. In fact, there is a great deal of focus on using and defining "ubiquitous language" in these meetings to ensure what one word means to someone in one role (ex: product manager) means the same exact thing and is understood in the same way to someone in a different role (ex: software engineer). Or perhaps what one person calls something; there is an understanding that another role may call it something else. When more people can understand and empathize with other roles or departments, they are more open to discussion and flexibility. They

tend to be more willing to help in times where help or response is needed. This is especially true when considering the relationship with security and the communications with that team.

Partnership: “Gauges the relationship between a business and IT organization, including IT’s role in defining the business’s strategies, the degree of trust between the two organizations, and how each perceives the other’s contribution.” (Luftman & Kempaiah, 2007, p. 2). Partnership is huge in a business when thinking of overall teamwork, otherwise the different departments tend to start working in silos and guessing or reacting to each other’s requests or requirements. Without a solid partnership, there can be many gaps or misunderstood processes in seemingly simple structures such as onboarding and how new employees gain access to necessary systems for their role. A great way to build and maintain a good partnership is to continually communicate and show empathy for others’ roles.

When the departments are aligned, they are stronger together and that goes for stronger in security as well. This alignment can further be evaluated based on varying maturity levels within each component ranging from initial/ad-hoc processes to those processes being optimized or matured over time as described in the following section.

2.1.3 Five Levels of Alignment Maturity

Level 1: Initial or ad-hoc processes: According to Luftman and Kempaiah (2007), at this level there is poor communication and understanding of value between the IT and business organizations. There is more of a formal relationship and metrics tend to be technical instead of business oriented. There is ad-hoc planning on both sides and IT is viewed as a cost center. There is minimal trust and/or partnership. IT projects rarely have

business sponsors/champions and there is little to no career crossovers. Applications tend to focus on the typical support functions like email, accounting, and HR. There is no IT-business alignment strategy. (Luftman & Kempaiah, 2007) At this point, there may not even be a security team or anyone focused on providing security training unless there is a requirement by customers to have it. Therefore, there may be little to no discussion about security or how to handle incidents.

Level 2: Committed processes / Repeatable: Luftman & Kempaiah (2007) state the following concerning Level 2:

> Organizations at Level 2 have begun enhancing their IT-business relationship. Alignment tends to focus on functions or departments (e.g., finance, R&D, manufacturing, marketing) or geographical locations (e.g., U.S., Europe, Asia). The business and IT have limited understanding of each other's responsibilities and roles. IT metrics and service levels are technical and cost-oriented, and they are not linked to business metrics. Few continuous improvement programs exist. Management interactions between IT and the business tend to be transaction-based rather than partnership-based, and IT spending relates to basic operations. Business sponsorship of IT projects is limited. At the function level, there is some career crossover between the business and IT. IT management considers technical skills the most important for IT. (p. 3)

There may now be some security training conducted to be able to provide this evidence to customers requiring it. There may even be policies to be signed, verifying the employees of the organization understand they must take regular security training.

Level 3: Established, focused processes / Defined: Luftman & Kempaiah find the

following concerning Level 3:

> In Level 3 organizations, IT assets become more integrated enterprise-wide. Senior and mid-level IT management understand the business, and the business's understanding of IT is emerging. Service level agreements (SLAs) begin to emerge across the enterprise; although the results are not always shared or acted upon. Strategic planning tends to be done at the business unit level, although some inter-organizational planning has begun. IT is increasingly viewed by the business as an asset, but project prioritization still usually responds to "the loudest voice." Formal IT steering committees emerge and meet regularly. IT spending tends to be controlled by budgets, and IT is still seen as a cost center. But awareness of IT's "investment potential" is emerging. The business is more tolerant of risk and is willing to share some risk with IT. At the function level, the business sponsors IT projects and career crossovers between business and IT occur. Both business and technical skills are important to business and IT managers. Technology standards and architecture have emerged at both the enterprise level and with key external partners. (p. 3-4)

At this level, the organization may have begun to be externally audited to prove compliance and security due diligence to current and prospective customers. To pass an audit at this level, the organization as a whole would understand the importance of having security awareness training conducted at the regular cadence required and set forth within the security compliance audit(s). This cadence is typically upon employee onboarding and annually thereafter.

Level 4: Improved, Managed Processes: Luftman & Kempaiah (2007) state the

following:

> Organizations at Level 4 manage the processes they need for strategic alignment within the enterprise. One of the important attributes of this level is that the gap has closed between IT understanding the business and the business understanding IT. As a result, Level 4 organizations have effective decision making and IT provides services that reinforce the concept of IT as a value center. Level 4 organizations leverage their IT assets enterprise-wide, and they focus applications on enhancing business processes for sustainable competitive advantage. SLAs are also enterprise-wide, and benchmarking is a routine practice. Strategic business and IT planning processes are managed across the enterprise. Formal IT steering committees meet regularly and are effective at the strategic, tactical, and operational levels. The business views IT as a valued service provider and as an enabler (or driver) of change. In fact, the business shares risks and rewards with IT by providing effective sponsorship and championing all IT projects. Overall, change management is highly effective. Career crossovers between business and IT occur across functions, with business and technical skills recognized as very important to the business and IT. (p. 4)

Reaching this level was an aim for the organization and an effort made within this project. By starting to meet with new employees at onboarding [and bootcamp] to personally describe the importance of their role in security as well as the benefit of communicating with and how the security/compliance team could assist them in their role, the goal here was to establish a mutual understanding of each other's role as well as

ensure the employees understood the company took security seriously.

Level 5: Optimized Processes: Luftman & Kempaiah (2007) state the following concerning Level 5:

> Organizations at Level 5 have optimized strategic IT-business alignment through rigorous governance processes that integrate strategic business planning and IT planning. Alignment goes beyond the enterprise by leveraging IT with the company's business partners, customers, and clients, as well. IT has extended its reach to encompass the value chains of external customers and suppliers. Relationships between the business and IT are informal, and knowledge is shared with external partners. Business metrics, IT metrics, and SLAs also extend to external partners, and benchmarking is routinely performed with these partners. Strategic business and IT planning are integrated across the organization, as well as outside the organization. (p. 5-6)

At this level, the organization is most likely going through multiple audits annually and constantly providing evidence regarding not only awareness training but some other type of communications being done on a consistent basis (such as a regular newsletter). This project has aimed to increase the level of not only awareness communications but also engagement to build on the previous levels and mature communications and partnership with all employees.

As mentioned previously, there are compliance requirements regarding security, including awareness/training activities. Because security can be scrutinized from regulators and/or customers, there are more security-specific maturity models to strengthen that area of IT. The next section discusses the more recently trending

Cybersecurity Maturity Model Certification and how that can relate to being compliant.

2.2 Cybersecurity Maturity Model Certification (CMMC) and Other Standards/Frameworks

In addition to the typical maturity models that help align different departments within an organization, there are maturity model frameworks being utilized to measure the maturity of an organization's security posture. One of the more recent frameworks that is gaining popularity is the Cybersecurity Maturity Model created for government and the government's vast supply chain.

Similar to the previously described capability maturity model, the CMMC model "measures cybersecurity maturity with five levels and aligns a set of processes and practices with the type and sensitivity of information to be protected and the associated range of threats." The model encompasses different requirements specified in certain regulations and/or standards (such as National Institute of Standards and Technology (NIST) 800-171. (CMMC, 2020) The organization discussed in this paper has more experience with attaining the security-related certification standardized by the International Organization for Standardization (ISO). This certification is ISO 27001:2013, but the requirements are like those in the CMMC model. The main difference seems to be that ISO is an independent, non-governmental international agency which helps organizations with a global footprint meet different countries' security standards.

The certification consists of maturity levels and best practices that stem from various cybersecurity standards, frameworks, and other references such as NIST and/or ISO. It has organized processes and practices in domains that can be seen in the figure

below. (CMMC, 2020)

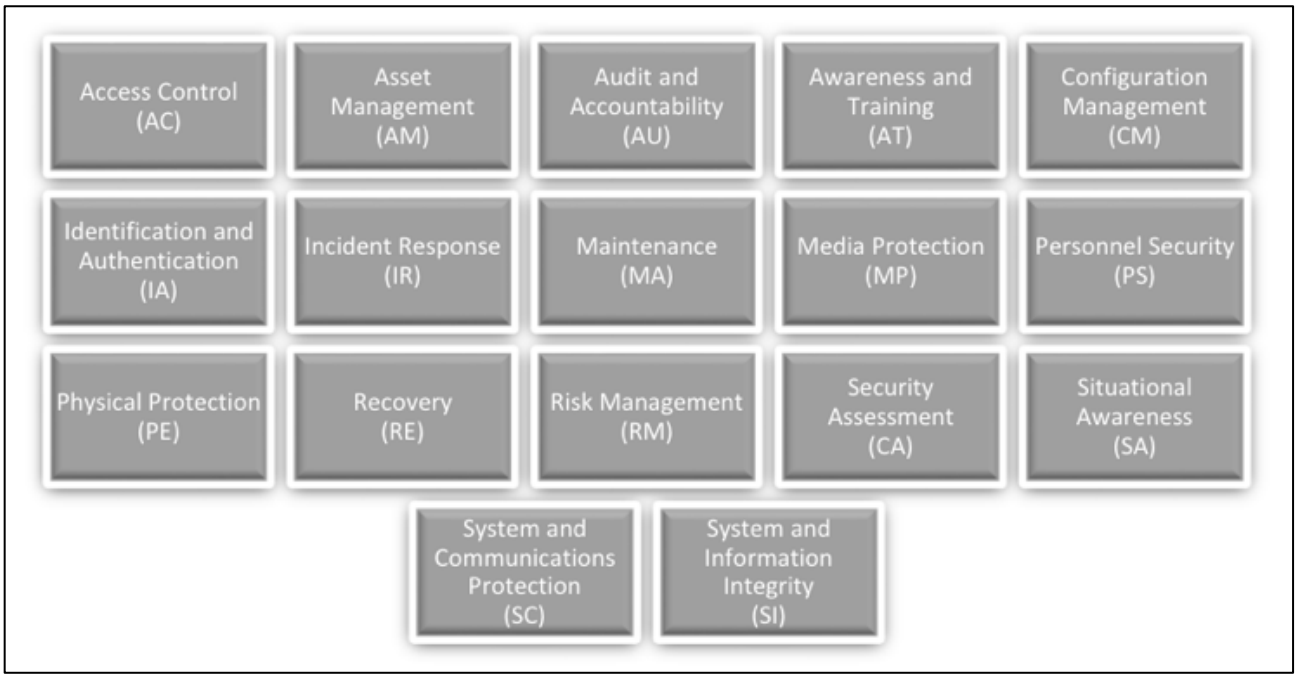


Figure 1 - CMMC model consists of 17 domains (CMMC, 2020)

Because this paper's focus is on security awareness and training, let us review this particular domain a bit further. One can see in the figure below that Awareness and Training (AT) consist of 5 practices that span over different maturity levels:

AWARENESS AND TRAINING (AT)

Level 2

AT.2.056	Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.
AT.2.057	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.

Level 3

AT.3.058	Provide security awareness training on recognizing and reporting potential indicators of insider threat.

Level 4

AT.4.059	Provide awareness training focused on recognizing and responding to threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors; update the training at least annually or when there are significant changes to the threat.
AT.4.060	Include practical exercises in awareness training that are aligned with current threat scenarios and provide feedback to individuals involved in the training.

Figure 2 - Awareness and Training Practices by Level (CMMC, 2020)

The CMMC includes 125 NIST requirements within its model. Because NIST is so engrained in the CMMC Model, the following guidance will be briefly reviewed and can be found in the NIST Special Publication 800-171's document. This guidance is mapping requirements over to the different controls. Often, these types of documents will also map (or do a "cross-walk") to other related standards such as ISO 27001, which can be seen here as well.

SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.2 AWARENESS AND TRAINING				
Basic Security Requirements				
3.2.1 Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	AT-2	Security Awareness Training	A.7.2.2	Information security awareness, education, and training
			A.12.2.1	Controls against malware
	AT-3	Role-Based Security Training	A.7.2.2*	Information security awareness, education, and training
3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.				
Derived Security Requirements				
3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat.	AT-2(2)	Security Awareness Training *Insider Threat*	*No direct mapping.*	

Figure 3 - Awareness/Training Requirements Mapped to Controls. (Ross et al., 2020)

The spirit of compliance regarding frameworks/standards, audits, and certification is very similar across various testing activities but may vary slightly during differing external audits such as SOC 2, ISO 27001, PCI, or CMMC for example. There is a control. There are one or more suggested requirements to meet that control. The organization must map policy, procedure/process, and/or other evidence (sometimes via observation) to those requirements to prove compliance in that area being tested. And even security awareness and training are included in this proof of compliance.

The fact that there is a domain and practices within CMMC, NIST, and ISO that are dedicated to Awareness and Training reflects the importance of this activity. And the CMMC document discusses the term institutionalization and how “the more deeply

ingrained an activity, the more likely it is that an organization will continue to perform the activity – including under times of stress." (CMMC, 2020). The argument could be made that creating a culture of awareness through effective training, practices, communication, positive engagement, building partnerships with employees/departments, and giving in-person presentations affects and assists in the institutionalization of security best practices throughout a company, regardless of an employee's position.

To better understand how to create a culture of awareness, it is relevant to review how psychology and influence can help in this area. The following section will review literature and thoughts on how these factors play a role in overall awareness and confidence regarding security self-efficacy.

2.3 Self-Efficacy and Employee Confidence within Security Awareness

"The ultimate success of information security depends on appropriate information security practice behaviors by the end users." Rhee, et al. (2009) In a study done by Rhee, et al. (2009), "The results suggest that simply listing what not to do and penalties associated with a wrongdoing in the users' information security policy alone will have a limited impact on effective implementation of security measures." People tend to be more motivated by what they are told *to do* [and how that action can help their teammates on the security team] instead of telling them what *not* to do. What not to do seems to put more fear rather than confidence into people and that is the last thing an organization wants to do to its employees when they want them to be able to act appropriately in certain, potential, incident scenarios.

As also discussed with the capability maturity model, organizations tend to devote significant resources and budget geared toward using more technical layers of defense. But these technical layers can, sometimes too easily, "succumb to human failure". Rhee,

et al. (2009) Even with significant tools to control, monitor, prevent, and/or detect threats, the tools can be outdated losing effectiveness or there could be a zero-day, or more recently discovered vulnerability, that the tool itself is not yet aware of within its detection database and even a day behind, would be outdated.

So how can an organization work to solve the people-problem of security? One way is to build more confidence and understanding in the employee base. Rhee, et al. (2009) contends that "individuals' beliefs regarding their ability to protect their information and information systems may help explain current security practices and their intention to persist in the current efforts."

Self-efficacy, or the belief in oneself to execute actions or behaviors to produce certain performance levels, "also determines the level of motivation, which is reflected in how much effort people exert and how long they persevere. Those with moderate to high self-efficacy tend to engage more frequently in task-related activities and persist longer in coping efforts. This leads to more mastery experience, which in turn enhances self-efficacy (Bandura, 1986)". (Rhee et al. 2009) The more experience one gets with a concept, the more confident and motivated they are with that concept. In this case, that concept is coping with security-related incidents. When an employee receives a phishing email, are they confident enough to know that it is phishing or, rather, are they confident enough [that they will not be judged by their co-workers] if they do ask for confirmation before clicking or even deleting?

"According to social cognitive theory, enactive mastery experience is a primary influencing source of efficacy belief. In general, successful experience increases self-efficacy and failure decreases it (Bandura, 1986)." (Rhee et al., 2009) Although Bandura and Rhee, ultimately, state that experience failing decreases self-efficacy, there can still

be what could be considered a successful experience after conducting potential, unintentional, harmful behavior such as clicking a phishing link. If the person who clicked the link is too scared to let anyone know about it (such as the security operations team) because they are ashamed because of how security is presented to them and what *not* to do, then yes – this experience would cause that individual's self-efficacy to decrease. BUT, if the individual was taught at the beginning of their employment that mistakes happen and it is not the mistake that matters, but how we respond to it that matters the most, they are more likely to respond in a more appropriate manner because they feel comfortable knowing that there is a team that has their back and does not think any less of them for making a simple mistake. The reactions of others in certain circumstances and situations can greatly influence future communications with that individual or team and if they react in a demeaning manner, the likelihood of building a partnership of high response, increasing communications and that individual's self-efficacy is unlikely.

But how are those partnerships built? How do people *really* know how to respond in certain situations? Is it through video trainings when they first start and once a year per compliance requirements? While these required activities can help, an advocate needs to constantly be spreading the word and presenting positively to new employees upon hire. They are more likely to be engaged and excited in the beginning of their employment, and then it is important to keep the conversation and topic going throughout the year(s) with the new employees that eventually reach "current employee" status. That is, if an organization really wants a population of employees that *care* enough to respond and communicate. Because training and engaging employees is so important, the next section will focus on these aspects.

2.4 Training And Engagement

Typical security training efforts are videos given to employees upon “new hire onboarding” and then at least once a year. This cadence satisfies certain compliance requirements for training outlined in different regulatory or compliance frameworks previously discussed, but is it effective in having the employee population be more responsive in a security incident situation?

“According to Pineda (2010), there are six elements of training evaluation: ‘participant satisfaction with the training; learning achieved by the participants; pedagogical coherence of the training process; transfer of training to the workplace; impact of training on organizational goals; [and] profitability of training for the organization.’ Kirkpatrick and Kirkpatrick (2007) outlined four levels of training evaluation: reaction to the training, learning from the training, the change in behavior after the training, and demonstrating results in relation to the training. This study focused on the first element, the participants' satisfaction and reaction to the training in terms of how effectively it prepared them to deliver the required instruction in the workplace.” (Hedderly & Scott, 2015) The results from the survey conducted for this paper can show, in the case of security awareness training, that participants/respondents were more satisfied with in-person training and consider security more often after those presentations (see “Review of Data” within the Data Analysis and Results).

“Research has shown that video training can be an effective means of learning as long as the video meets certain criteria. According to Cullen (2011), who studied the effectiveness of a safety training video for the mining industry, videos need a trainer who can relate to the trainees, not a ‘talking head,’ who uses appropriate language for the culture, and whose appearance looks the part.” (Hedderly & Scott, 2015)

"Videos can be developed to appeal to any learning style (Addison, 2013; Lohan, 2013) '... in a way that not only engages and entertains people, but is also easy to remember' (Addison, 2013). Video can now replace the live instructor and engage the learner with interactive activities designed to increase retention (Lohan, 2013)." (Hedderly & Scott, 2015)

While videos can be created in a way that does pique the learner's interest and can be effective in training scenarios, it is obvious that the videos must be curated and created in such a way that they are interactive, relatable, uses certain language, etc. to meet the criteria that does in fact pique the learner and motivate them to take care during certain situations shown in those videos. When it comes to the typical security videos that are required for an organization to maintain compliance year after year, those videos are not typically geared toward each audience member. Security training is a blanket concept that goes out to every employee regardless of position and even though "security is everyone's responsibility", these videos are not always the most motivating to get the end user to take action in the scenarios that may be laid out in the videos [at onboarding and at least once a year]. They are typically the "talking head" type video which, as mentioned by Hedderly & Scott, is not relatable. While these videos may not be the most motivating for employees, they do meet compliance requirements and that "low hanging fruit" within an auditing scenario and that requirement is checked off as completed.

So, if the typical video that organizations provide to their employees is not as relatable as it could be, what else can companies do to keep security top-of-mind in case of actions needed after that training is provided and potentially not remembered? By conducting in-person training and/or presentations in addition to more relatable videos, an organization can make people feel more confident, and help increase employee self-

efficacy, with relation to actions needed in certain incident situations. Creating a population that not only has a higher awareness level when it comes to security incidents, but one that cares enough to respond and communicate with the security team takes more than videos. It takes the team that curates these videos to also care enough to provide well-delivered instructional, interactive, relatable presentations and communications to supplement the videos that are mainly meant to meet compliance requirements.

In a study completed by Schreiber et al. (2010), 100 students attended two different teaching styles on two topics. Half of the students attended a live lecture on arthritis and then a video podcast on vasculitis. The other fifty students attended a live lecture on vasculitis and then a video podcast on arthritis. 66 of the students completed a qualitative and quantitative questionnaire (33 from each group). The students were asked their preferred method of learning/teaching and 92% stated they preferred lectures/tutorials over computer based or self-directed learning. (Schreiber et al., 2010) On the knowledge-based questions, the two groups performed similarly so there was no real difference, other than preference, as far as knowledge/competency was concerned. (Schreiber et al., 2010)

The data from that study aligns somewhat similarly to the data collected in this paper around security awareness training videos and in-person presentations on their first day of employment. Of the respondents (63 people, see in the Data Analysis section) that said they did, in fact, receive some sort of security presentation on their first day of employment, 58.73% stated they believed they considered security more often because it was discussed on their first day while 4.76% stated they did not believe they consider security more often because of that presentation. The respondents were asked if they would have preferred a video rather than an “in-person” meeting concerning security.

57.14% stated they would *not* prefer a video over "in-person" discussions around security and 6.35% stated they would prefer a video.

When reviewing the knowledge-based scores the overall average was in the 87th percentile. Also reviewed, was how might the scores compare depending on one's attitude and how often they consider security and type of data when they are working. The answer options were 'never', 'rarely', 'often' and 'always'. While the individuals who stated they 'always' considered the data they work with did, in fact, receive a higher average score – it was not especially significant as the average of each response type ranged from the 81st-89th percentile.

The conclusion that an in-person presentation is not necessarily superior to any video training when it comes to knowledge/competency based on the survey results provided in the next section, pushed the organization to look at other numbers and reporting as there still "felt" as if there was an increase in reporting, communication and collaboration with the security team while conducting various engagement activities more often. Chapter 4 discusses the types of engagement being conducted, and the employee response results gathered.

CHAPTER 3: SURVEY METHODOLOGY

"Surveys provide evidence on practice, attitudes, and knowledge." (Story, 2019, p. 192). For these reasons, the survey conducted for this capstone paper was aimed to find that very evidence of knowledge toward security [knowledge] in practice and attitude toward not only training but presentations and whether the employee(s) believes that having an actual person on their first day made an impression to the point they care more and/or think more about security within the company.

Kalton et al (2007) state that evaluation studies are around cause-effect, starting from the cause (or intervention) and then investigating the possible effects of that intervention. Surveys conducted for the evaluation studies collect data needed for assessing the effect of the program or intervention (Kalton et al, 2007). In the case of this capstone, the survey helps to identify if the in-person security presentations make a difference in the not only the understanding of the training information, but the response to potential security threats such as potential phishing emails, voicemails, and/or texts.

The intent of the survey was to gather data from those that may or may not have received a security discussion on their first day with the company. The purpose was to see their knowledge of certain aspects but also their feelings and/or attitudes around that day one security presentation, or the lack thereof. I also wanted to see if they thought the security presentation was worth their time and if they thought more about security because of it. What I realized was the question(s) I asked should have been more specific

The survey questions came directly from topics discussed either in the security presentation on their first day or the security training required before gaining access to certain systems. Because the training videos had an obvious topic, I made sure to pull out

the important topics such as Data Classification, Phishing Emails, Incident Response, etc. as these were reiterated during the presentations. See Appendix D. Training Topics Mapped to Survey Questions.

The survey was created using Smartsheet Forms. Smartsheet is a cloud application that allows users to collaborate, manage projects and processes, as well as create forms for feedback. The survey was posted in an informal group web messaging application within the company requesting people to take the survey when they get a moment and letting them know that about twenty-five questions were on the survey as it would take about 5-10 minutes of their time. There were about 500 people who could have possibly seen the request for response and of those 500, there were 78 responses total (or about 15% of the population of those channels). The makeup of the channels consisted of Software Engineers and Managers, QA Engineers and Managers, Product Managers, IT professionals, and Product Designers.

3.1 Data Analysis and Results

The survey consisted of 27-28 questions depending on how the respondent answered question #25. 22 questions were focused on knowledge, 2 questions were intended as benchmarks, and 4 questions focused more on attitude and/or behavior.

3.1.1 Results of the 22 knowledge-based questions:

Mean: 87.59%

Median: 86.36%

Mode: 86.36% & 90.91%

Lowest Score: 63.64% (1 instance)

Highest Score: 100.00% (1 instance)

Scoreable Questions:

How many questions were answered at 90% or above? 13

How many questions were answered between 80%-90%? 2

How many questions were answered below 80%? 6

How can this information help a security training program?

By evaluating the responses to the scoreable questions, the program can adjust the questions that respondents receive greater than 90% to become more layered or difficult in the future as this knowledge seems to be more inherent and does not cause much cognitive load.

All the questions receiving a score of less than 90% should continue to be taught but the way in which these topics are presented may need to be changed/updated to lessen cognitive load or they should be presented more often.

This insight is invaluable in getting an understanding of which topic areas need to be addressed more often.

Which questions/topics received less than 90% accuracy?

Question #3: Data Classification

Question #4: Confidentiality, Integrity, and Availability (CIA)

Question #6: Information Security Principles

Question #8: Protecting Against Malware

Question #9: Protecting Against Malware, Identifying and Reporting

Question #12: Identifying and Reporting

Question #13: Insider Threats, Identifying and Reporting

Questions #21: Keep Data Backed Up Via Appropriate Resources

Key Takeaways:

One can see that the topics that were missed most often were 'Identifying and Reporting' and 'Protecting Against Malware'. While there were other topics that were missed, it is easy to see that these topics need to be addressed and presented more often to increase knowledge on those topics.

What were the 5 most missed questions (in order of most missed to least missed)?

#12: You receive a suspicious email and want to report it, what's the best way to do this?

Q12 - possible answers:	How many times was each response given?
A. Forward to the security team.	20
B. Post in phish-tank	18
C. Send via the Report Message button in Outlook.	40
D. Let your manager know.	0

Figure 4 - Question 12 responses and number of times each response was provided by survey participants. The correct response for this question is highlighted.

A little more than half of the respondents answered the question correctly. The other two options (A. and B.) were conveyed as viable reporting options during the day-1 security onboarding presentation, but C. is the "best" way to report a message to the security team.

Takeaway:

Let the security operations team decide if it makes their job easier and if it is more efficient to actually report phishing via the Report Message button as this not only allows more automation around phishing emails and there is less communication back and forth therefor less focus time taken from the security operations team. Based on that decision, perhaps the presentation no longer includes discussing *forwarding to the security team* or *posting in phish-tank* and instead focuses on using the Report Message button in Outlook.

Cautions to not presenting the other two options: There are potentially more clicks for the end-user and if they do not use Outlook that often or if they use a different version, will they remember how to find that button? The automation also takes away from interacting with the security team and if the intent of creating a security culture, I believe it is important for employees to have experiences interacting with someone from the security team.

#3: Company financial statements, employee salary information, proprietary code, and internal system processes would be classified as what type of data?

Q3 - possible answers:	
A. Public	0
B. Internal	42
C. Confidential	36
D. None of the above.	0

Figure 5 - Question 3 responses and number of times each response was provided by survey participants. The correct response for this question is highlighted.

We can see that more than half of the respondents have correctly answered the question, while 36 actually considered the data classification to be a more stringent one. I believe this thought is a good one but the question for the business, security, and perhaps even legal teams, how important is it that employees truly understand the data types in which they may run in to while conducting daily business?

Because so many answers were answered to be a stricter classification, I wondered how the responses turned out for the question where the answer was, in fact, "Confidential" even though this question was answered correctly at a rate of 92.31%.

#2: Social security numbers, driver's licenses, and account numbers would be classified as what type of data?

Q2 - possible answers:	
A. Public	0
B. Internal	2
C. Confidential	72
D. None of the above.	4

Figure 6 - Question 2 responses and number of times each response was provided by survey participants. The correct response for this question is highlighted.

It's interesting that there were 4 responses that answered, "D. None of the above.". Does this indicate a need for more training or presentations around Data Classification as those 4 individuals may not take care of this type of data in the appropriate way? Or does the majority count as "good enough"? Or perhaps those individuals took this question personal and thought about their own social security number, driver's license, and account number and thought it was not applicable in this survey. There is also the case that a majority of the individuals receiving the survey do not actually work with these types of data on a regular basis but instead mock data types.

Takeaway: People seemed to lean toward a stricter data classification when considering obvious, work-related type data such as company financial statements, employee salary information, proprietary code, and internal system processes. And while a majority of the respondents answered question #2 accurately, I may have received a better response had I opened this survey to a different department that works directly with customers and could potentially work with this type of data in their day-to-day job.

Data classification is still a good topic to continue to present to remind people of these different data categories but maybe just place it in a as a reminder in a follow-up type of presentation rather than the main content.

#6: Which of the four security principles requires that employees shall have no more authority than necessary for their role?

Q6 - possible answers:	
A. Need to Know.	26
B. Least Privilege	49
C. Clean Desk	1
D. Data Protection	2

Figure 7 - Question 6 responses and number of times each response was provided by survey participants. The correct response for this question is highlighted.

A majority of respondents answered correctly but following that are the many "Need to Know" answers. I feel as though this verbiage is not necessarily translated well for typical employment unless the employee is in a compliance or security type of position. While these concepts are taught via online training and Clean Desk was briefly discussed in the day-1 security onboarding presentation, I think it would be helpful to discuss the formal verbiage in an informal way, so it is consumed and understood easily. I think these concepts are especially important for managers to understand as they would be the ones to request access to systems for their employees and they have day-to-day contact with those employees and can reinforce the importance of not unnecessarily providing certain information outside of their team if they are working with potentially sensitive data, systems, and/or proprietary creations, ideas, or information.

Takeaways: Finding a ubiquitous language around the formal, policy-like terminology would be a good start in helping these concepts be more easily differentiated. Present on these topics not only in follow-up departmental presentations but in manager training as well and provide examples of how employees can easily decide what information they work with is Need to Know versus Least Privilege since these can get easily confused.

In the online, video training Least Privilege is defined as "The idea that no employee shall have more privilege or authority than needed for their role." But what does that really mean? It means if someone does not need a certain level of access to a

system to do their job, then they will not get that access. Employees will only gain access to systems and physical locations that they need to conduct their job. A good question to ask yourself to make the distinction is, “Do I need to be an administrator of this system to use it for my job?”. Unless the employee works in the IT department, the likelihood of that answer being a yes is slim depending on the system and the employee’s position. Least privilege though is more of a control that can be restricted by the IT department, so I believe the Need-to-Know concept is one that is almost more important for employees to understand.

In the online, video training Need to Know is defined as “Information that is only provided on a Need-to-Know basis.” But what does that mean? It is not just information from employee to employee, but this also goes for employee to customer or friend, manager to employee, etc. We have many relationships in our lives, and we tend to want to provide help to those asking us questions, but we need to ask ourselves, “Does this individual or business really need this information?”. A great example is when I would receive a request for information (RFI) from a third-party that works for a customer. If that third-party company is not on our files and/or that contact is not on file, I would require multiple steps prior to providing that information and/or documentation. First, I requested a Letter of Authorization (LOA) from the third-party that was signed within the last twelve months. Second, I would read over and check that the signature on the LOA came from the actual customer. Third, I would verify that the individual that signed the LOA is still employed at the organization. While this may seem to be overkill, I would not provide any information until I had all of this documented. And this is more of a compliance function so it is important to present this in a way that would make sense to different employees. The one above may also make sense to Sales as they complete many

Requests for Proposals (RFPs) and they, too, receive RFIs. But what about other functions or scenarios? Thinking of proprietary information or code, not talking about what we are working on or company financials with people outside of the organization are great examples.

#13: You notice an employee gave their computer password to another employee. You bring it to their attention that this is bad practice and could result in a breach, but the employee dismisses your concerns and says they have done it before, and nothing happened. At this point, this employee could be considered an insider threat even if their intent is not malicious. What should you do? Choose the best answer.

Q13 - possible answers:	
A. You have already said something to them so you should not do anything else.	0
B. Report the incident to the security team.	54
C. Contact your manager to make them aware.	13
D. Repeat your concerns to the employee and show them security policy/training to prove your point.	11

Figure 8 - Question 13 responses and number of times each response was provided by survey participants. The correct response for this question is highlighted.

This question comes directly from online training rather than any in-person presentation, and I would consider this one a tricky one because it is a question of culture and wanting to "keep the peace". Nobody wants to be seen as a "tattletale", but technically the correct answer is to "report the incident to the security team". I believe the other two options that respondents chose would be good courses of action as the individual in this situation would be having to make a difficult decision and since this person already brought their concerns to the potential insider threat employee, and that employee would suspect their colleague of telling the security team on them.

Takeaway: Because of the dilemma this question and very real scenario brings to light, I believe it would be good to discuss the options with the security team to see what the actual expectations would be in this circumstance. "Do the right thing" is part of the

culture and while reporting the incident to the security team is technically the "right thing", it could feel wrong to the person having to make this decision. Based on the responses, I believe this exact scenario could be presented at a departmental follow-up presentation and have an open discussion on how it is understandable for someone to not want to tell on their co-workers and perhaps together come up with a better solution to this problem. There could even be security-based training around conflict management, so the employees have better knowledge and skills when it comes to confronting this type of situation.

#4: According to the annual information security training, what are the three pillars that make up good security?

Q4 - possible answers:	
A. Confidentiality, Integrity, Applicability	13
B. Confidentiality, Identity, Applicability	4
C. Confidentiality, Identity, Availability	4
D. Confidentiality, Integrity, Availability	57

Training states: "*the secure handling and storage of sensitive data is mission critical. The CIA triad is composed of Confidential with infosec these are the three pillars that make up good security.*" If there is a desire for these concepts to be understood on a large scale, there should perhaps be more emphasis on this topic within training and/or presentations but should also be wary of over-complicating the thoughts of security as some of this can related to some other topics. The presentation needs to present these in a way that is easy to understand to the typical employee, especially those that may deal with certain aspects such as the product, infrastructure, and/or data (customer or mock).

3.1.2 Results of the 4 attitude-focused questions/answers:

Q #1. To what extent do you think about the data/information you have access to and its classification?

Responses:

Never: 2 – 2.56%

Rarely: 28 – 35.90%

Often: 39 – 50%

Always: 9 – 11.54%

Benchmark – Q#25 Did someone discuss security on your first day?

Responses:

Yes: 63 – 80.77%

No: 15 – 19.23%

Based on the response to question #25, the respondents answered the following:

If yes to #25:

Q #26. Do you believe you consider security more often since it was discussed on your first day?

Responses:

Yes: 37 – 58.73%

No: 3 – 4.76%

Neutral: 23 – 36.51%

Q #27. Would you have preferred a video rather than "in-person" meeting concerning security on your day 1?

Responses:

Yes: 4 – 6.35%

No: 36 – 57.14%

Neutral: 23 – 36.51%

If no to #25:

Q #26.2. Do you believe you would consider security more often had it been discussed on your first day?

Responses:

Yes: 4 – 26.67%

No: 5 – 33.33%

Neutral: 6 – 40.00%

Knowledge-based data compared with attitude-based data:

When reviewing the average knowledge-focused scores, I noticed the following:

Average Score of those who stated they consider the data they work with:		
	Never	81.82%
	Rarely	85.88%
	Often	88.69%
	Always	89.39%

Figure 9 - The average knowledge-based score depending on the response of how much the employee considers the data they work with.

Even though these scores are close, those employees that consider the data they work with more often, received higher scores on the knowledge-based questions.

3.1.3 Review of data:

- Of the 63 respondents or 80.77% of those that responded "yes" to someone discussing security on their first day stated the following:
    - 58.73% or 37 respondents stated they believed they considered security more often because it was discussed on their first day.
    - While only 4.76% (or 3 responders) stated they did not believe that they consider security more often because it was discussed on their first day.
    - With 36.51% being neutral.

- When asked if these individuals would prefer a video rather than an “in-person” meeting concerning security, the respondents answered:
    - Only 4 respondents, or 6.35%, stated they would prefer a video.
    - 36 respondents, or 57.14%, stated they would not prefer a video over “in-person” discussions around security.
    - With 23, or 36.51%, being neutral.

Takeaways: When looking at the attitude-focused questions, it seems that having in-person security presentations on an employee’s first day does make a difference in that person’s experience with security and how they think about security considerations because of that presentation/discussion. A majority of these individuals also prefer people over videos. This tells me that presentations from the security team do, in fact, make a difference and it would be of the company’s and the security team’s best interest to continue doing a mix of not only online training, but in-person presentations and discussions as well. I believe that manager training would make a huge difference as well, so there are security advocates that are in charge of other employees and can understand the importance of a security culture and mindset while conducting day-to-day work activities.

CHAPTER 4: PRESENTATIONS, ENGAGEMENT, AND EMPLOYEE RESPONSE RESULTS

4.1 Engagement and Communications

4.1.1 The New Employee Experience

When thinking of making an impact, if an organization is growing rapidly and is constantly onboarding new employees – the company should consider starting awareness efforts at an employee's first day to make the most impact and then go from there to reach more employees who are currently with the company. In this particular pilot project, this is what this company did. In August 2019, they started to meet every employee on their first day for new hire onboarding. At first, it was to help implement a new security training system to ensure the individuals using the system were doing so accurately. After the new system was fully implemented, the organization wanted to continue to utilize the thirty minutes they had already set aside for the weekly new hire onboarding. A good way to make a bigger impact with new hires was to do a quick presentation on a few different, but important topics, as well as be one of the first contacts the new employees meet to be more memorable and helpful in the start of their tenure. The slide deck for the new hire security onboarding can be seen in Appendix A. The goal of that thirty minutes with the new hire was to do a few things including but not limited to the following:

- Make a helpful and welcoming impression while ensuring the new employee understood the company took security seriously.
- Empower the employee with information and understanding so security did not seem like an overwhelming subject.

- Let the employee know how they could help their fellow teammates on the security team and what the typical threats were and how to respond to those threats.
- Ensure the new employee understood there was zero judgment for any mistakes that happen, and that mistakes happen all the time and the way the company and teammates respond to it is what really matters…not the mistake itself.
- The best ways to report potential phishing or other incidents.
- How and when to complete their required, standard security training videos.

Once several days passed, the company would follow up with the new hires to motivate anyone that may have not already completed the required training videos, give them any necessary follow up information, and – once again – make them feel welcome. This communication typically came in the form of an informal message as seen in the figure below. The response back to this follow-up would typically be positive as seen in Figure 5 below.

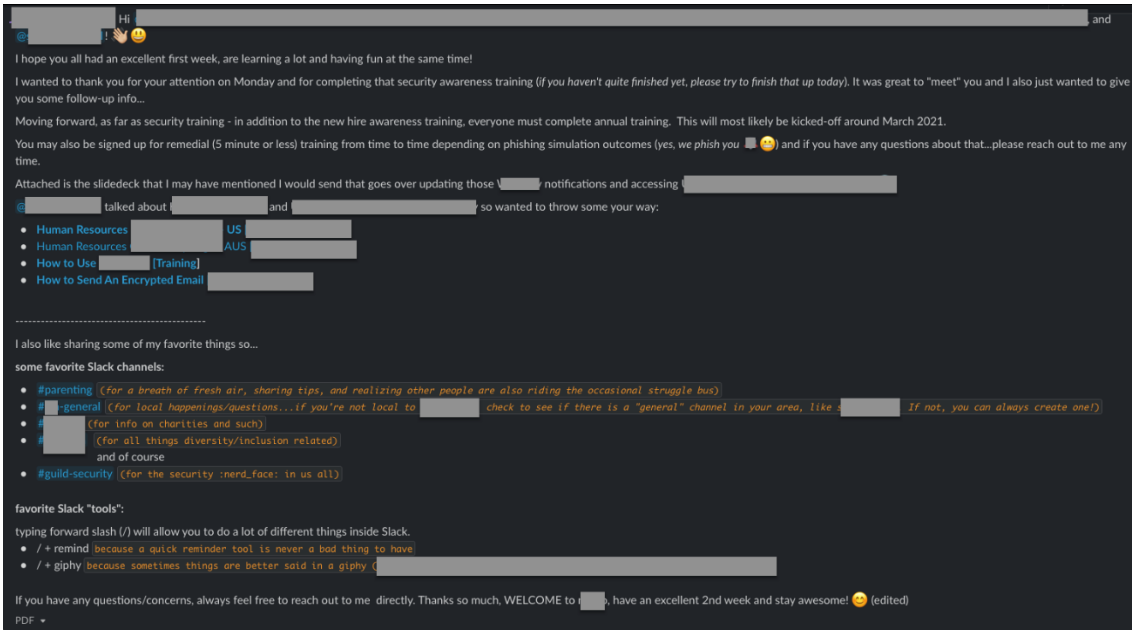


Figure 10 - New Hire Follow-Up Example

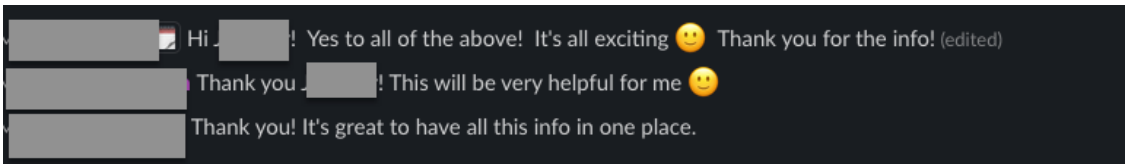


Figure 11 - Typical Follow-Up Response From New Hires

That is not where it ends for new employees though as all newly hired individuals also attend a company "bootcamp" where different departments come speak to present on their department and how that department contributes to the organization. Security also presents at this bootcamp. As a precursor to the presentation, the security team sends out a test phishing email to all the new hires attending bootcamp to see if they could recall the different avenues to report or warn others on the potential phishing email – of which they were told on their first day. During the presentation, anyone who reported the test phishing message would get a public acknowledgement as well as an entry into a raffle for a small reward for their efforts.

It was important to the security team to use the limited bootcamp time (fifteen minutes) to build on what they had started on the employees first day, with the same compassion, empathy, appreciation for the company, and their passion for their job in IT/security. This presentation was not the typical security presentation discussing topics such as passwords and phishing (as that was covered – either in the first day or was already required policy on company tools). This presentation was personal. The individual giving the presentation wanted it to be relatable, so they quickly told a story about something "cool" when they - too - first started, why they love working at the company, and why they love security/awareness. The next important piece of the presentation was to get the employees to really think how a breach or incident would affect them in their day-to-day job, so rather than telling them – the presenter asked the

audience to think about it themselves while giving potential scenarios for people to think about (ex: “As someone in sales, do you - in your sales role, think having a breach/incident would make the next sale more difficult or time consuming?”). The presenter then reiterated to the new employees what the biggest threat is – which is something that was covered explicitly on their first day at onboarding and this topic led into the final point – phishing emails. As mentioned previously, the test phishing email that was sent out prior to bootcamp was presented, and indicators pointed out that could help for any future simulated (or real) phishing emails. This is also where the individuals would get acknowledged if they did report that message (regardless of whether or not they clicked on it). Please see Appendix B for the presentation slide deck.

The team that coordinated the various bootcamp sessions surveyed the new employees bootcamp experience. This helped the presenters in all departments to improve over time. There were three criteria for the audience to provide scoring [on a scale to 100] regarding the different presentations. The three criteria were as follows:

1. My attendance in this session was a valuable use of my time.
2. The presenter delivered the content in a clear and engaging manner.
3. This session provided me with a clear overview of each department’s role and how the departments contribute to the company’s mission.

Data that was also provided with the survey results was the class size, the number of responses, and overall average score. Below are a few of the survey results and comments related to the IT/security sessions:

February 2020:

New Hire Bootcamp Survey Results

Class: February
Class Size: 51
Survey Responses: 20
Overage Average Score: 94

Session: Security/IT	Average Score
My attendance in this session was a valuable use of my time.	92
The presenter delivered the content in a clear and engaging manner.	97
This session provided me with a clear overview of each department's role and how the departments contribute to [redacted] mission.	97

Additional Feedback: Security/IT

Good session to learn from IT what to watch out and to be aware of.
Great idea to include the gift cards
I don't think it was a good use of time, in that I knew about cyber-security etc. but [redacted] kept it entertaining.
Session was very similar to the IT session we had on our first day of work. Very valuable information, but some information we have already gone over. Really enjoyed how they used the phishing email as a game to keep us engaged.

April 2020:

New Hire Bootcamp Survey Results

Class: April
Class Size: 32
Survey Responses: 17
Overall Average Score: 95

Session: Security/IT	Average Score
My attendance in this session was a valuable use of my time.	92
The presenter delivered the content in a clear and engaging manner.	94
This session provided me with a clear overview of each department's role and how the departments contribute to [redacted] mission.	94

Additional Feedback: Security/IT

[redacted] are Rock Stars!
It was nice to have the low down on security - we don't talk about it enough as a whole.
[redacted] were great. Thank you.

May 2020:

New Hire Bootcamp Survey Results

Class: May
Class Size: 15
Survey Responses: 9
Overall Average Score: 94

Session: Security/IT	Average Score
My attendance in this session was a valuable use of my time.	98
The presenter delivered the content in a clear and engaging manner.	98
This session provided me with a clear overview of each department's role and how the departments contribute to [redacted] mission.	98

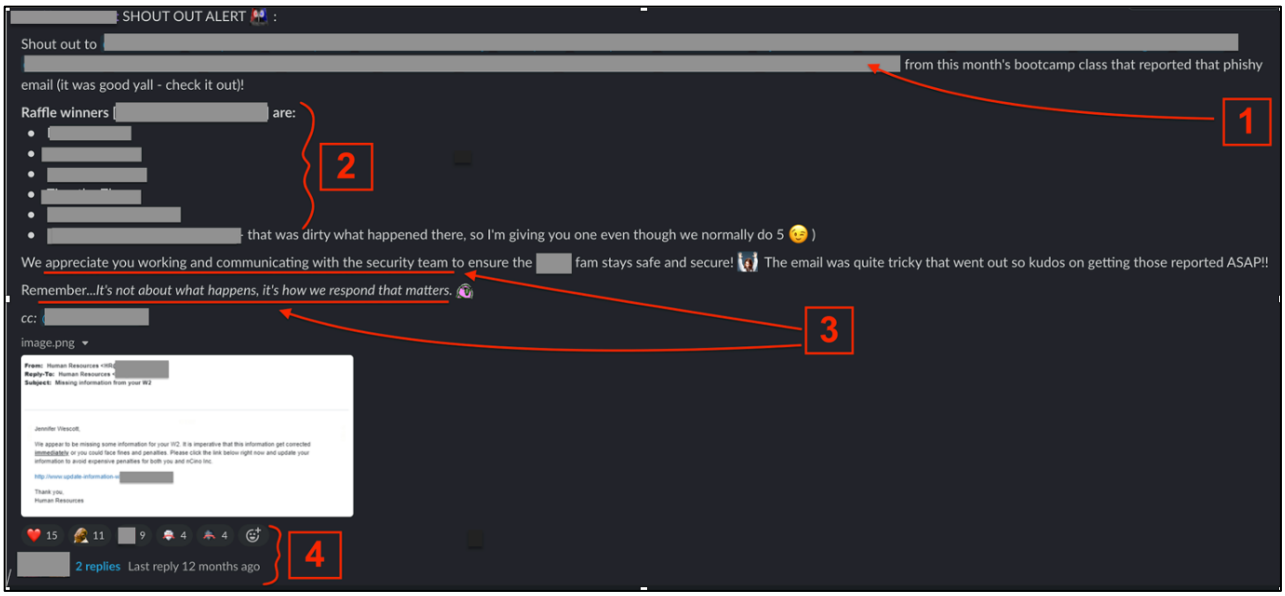
Additional Feedback: Security/IT
I was relieved i passed the phishing test!
[redacted] story gave a genuine feel to why security is so important. I think that will stick with the other new hires too. Sometimes IT security can feel dry so hearing her correlate that to a story with her mom made it personal and engaging.
[redacted] were great and delivered their material in a easy to grasp and fun (with enough seriousness) manner.
Great way to test new employees with the "test email" prior to this session

As mentioned, all new hires that reported the phishing email would be entered into a raffle. After bootcamp, the individual who presented the bootcamp session would invite the new hires who reported the email message to watch the raffle unfold to see if they won. After the raffle commenced and the lucky individuals to receive the gift cards were chosen, there would also be an announcement to publicly acknowledge the new employees' good efforts and to show current employees these efforts as well. One such example can be seen in the figure below.

This public acknowledgement was intended to do the following:

1. Give recognition to each person who took the time out to do the right thing and report that message.
2. Announce the raffle winners.

3. Show appreciation for working and communicating with the security team and remind people that "it's not about what happens, it's how we respond that matters."
4. And finally, to let others give support or "kudos" through emojis and/or comments.



4.1.2 The Continued or Current Employee Experience

While the company wanted to continue to make a great first impression with all the new employees, they knew they needed to also communicate and engage with the current employees. After all "new employees" do end up reaching "current employee" status at some point and the following assists in continuing that original engagement.

A great and relatively easy way to continue to get the word out and keep security "top-of-mind" is through newsletters. And newsletters with varying content that could either be watched or read by the employee gave the employee options on how they prefer to consume that information. The organization thought if someone would prefer to watch

a short yet entertaining security-related video – they could do that, or if the audience preferred to read the newsletter that was attached to the email, they could do that, Either way, the employee is getting some sort of awareness content delivered to them through their inbox and other announcement channels. In addition, a survey was included for increased engagement and employee feedback. For those that completed the survey/questions, the company would often put those individuals in a raffle for a small gift card reward to incentivize more future participation. The questions and survey response results can be seen in Appendix C, but some comments that employees left for this particular newsletter were as follows:

- “Definitely helps to ensure that "Security" is always top-of-mind. I appreciate the effort and message. Thank you.”
- “I enjoy reading and gathering information that pertains to our work family. It's always fun to learn and grow!”
- “Visually interesting. Information is very timely and relevant, and the language is accessible. Also Inside Man vids are weirdly entertaining.”
- “I like that there is a chance to win a gift card. The graphics and design of the letters are good, too.”

Figure 12 - Newsletter Email example

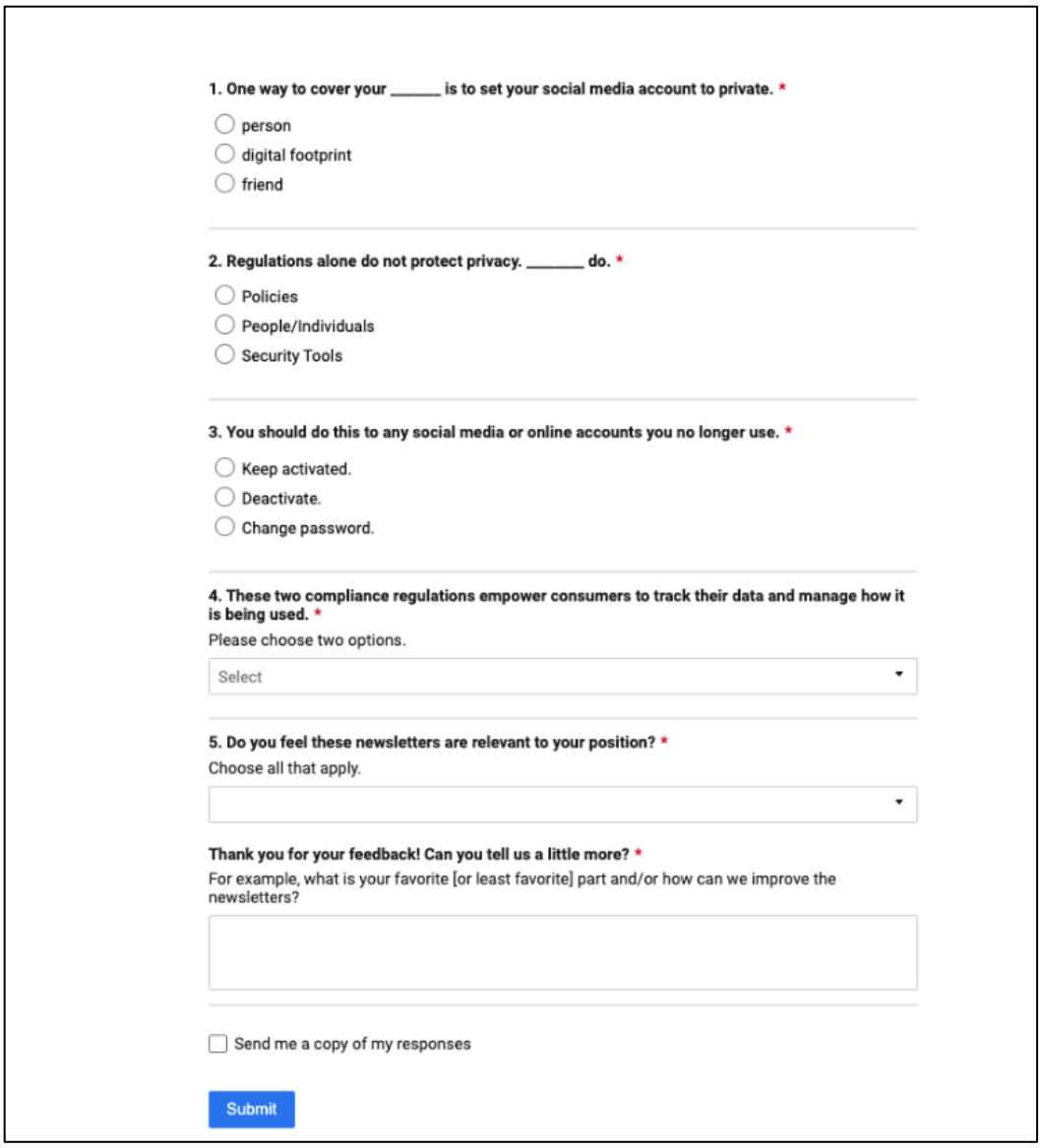


Figure 13 - May-July 2020 Survey Example

4.1.3 Reporting Results Over Time

Over the course of three years (2019-2021), the company reviewed the average number of employees the organization had from May to July. They wanted to see if the percentage of reported messages over the course of that time changed, as in August of 2019 was when a team member started presenting security on every employee's first day with the company. This was continued until February 2021. The newsletters have continued but in December 2020 - the surveys and incentives stopped, and in January

2021 – the videos/episodes were no longer included within the newsletter. Below is the data that shows the fluctuations of reported messages over the course of the three years where the efforts ramped up as well as went down:

Timeframe (Months):	May - July				
Year:	Average Population during the Timeframe	Population Change Over the Years	# of Reported Message during the Timeframe	Percentage	Percentage Change Over the Years
2019	625		57	9.12%	
2020	960	335	135	14.06%	4.94%
2021	1192	232	114	9.56%	-4.50%

As one can see from the numbers above, the engagement efforts made a difference in the reporting of messages to the security team. From 2019 to 2020, there was an increase in the population and naturally, one would think, that there would be an increase in reporting messages and of course there was a 4.94% increase. But from 2020 to 2021, even though there was an increase in population, once the day-1, onboarding presentations stopped and there was less engagement with employees, there was a 4.5% drop in the reporting of messages to the security team.

CHAPTER 5: DISCUSSION, CONCLUSION, AND FUTURE WORKS

5.1 Discussion

As can be seen in this paper/project, there were several data points gathered over time. The first efforts were gathering data via the main survey for knowledge/competency and attitude towards security awareness. The results showed that while more in-person presentations/training may not improve competency scores to the point of mattering for compliance, the in-person training/presentations did increase the employees' consideration of security more often. It was also seen in the survey results that a majority of employees preferred in-person presentations/training over videos.

These survey results led to reviewing employee reporting of phishing emails (which was deemed one of the biggest threats) over the course of three years as within that three years the organization began to provide more of an experience with security starting at the employees first day at onboarding and continuing from there through regular follow-ups via informal channels and/or more formal emails/announcements such as the newsletters. While the experience continued, there was an increase in employee reporting and subsequently, once that engagement and experience dissipated – the employee reporting decreased even though there was an increase in the employee population.

The results can be interpreted to show that increased employee engagement and communication can have a positive effect on partnership and communication between the typical business employees and IT/Security employees which could potentially lead to quicker response times in the case of an incident/breach event.

What the results are not able to show is the monetary and resource consumption cost of the increased communication. While it is great to have more communication with the security team, security teams are typically smaller in size and are not always equipped to handle the potential influx of questions/concerns/suggestions that a more responsive or communicative employee-base may bring to them. But in order to keep that partnership going, a team being asked questions must be responsive to ensure that relationship remains intact as communication and partnership are key components in the capability maturity model, according to Luftman and Kempaiah (2007).

The recommendation to continue increasing employee responsiveness would be to take a look at what really worked over the course of time and see if any of that could potentially be automated or made into a video for consumption as to keep costs down. Keeping in mind what Hedderly & Scott (2015) state - that the effectiveness of videos must be created in a way that is relatable, does not include the typical 'talking head,' making sure the language used in the video is appropriate for the topic and the company culture, and ensuring the person(s) in the video look the part. In addition to automating and/or turning in-person training into relatable videos, it would be recommended to continue to include some sort of in-person presentation to different departments and/or to managers in manager training. This way there is still that personal touch but not so often as to drain resources in the security department. Creating foundational management training would help align the different departments to be on the same page when it comes to what is expected regarding security and responsiveness in certain scenarios, as well as create more knowledgeable resources on what is expected regarding security throughout the organization and potentially help increase responsiveness amongst employees but without overloading the security team themselves.

5.2 Conclusion

Security awareness training, communications, and employee engagement are often too far and few between, but the typical cadence implemented does meet compliance standards. If an organization truly wants to create a culture of not only awareness but response and communication with the security team, the organization needs to focus on the employees, who are often deemed the weakest link in the organizational security posture. The survey conducted during this capstone project shows that even though typical training videos are good enough for competency/knowledge, individuals tend to prefer in-person presentations over videos. And while competency may not be much different with in-person discussions/presentations versus video training, the efforts made by the company to provide awareness from the start of an employee's tenure and then rolling information into an engaging newsletter and providing incentive opportunities for new hires and current employees seems to have led to an increase in communications and reporting to the security team. The company decided to ultimately decrease the efforts as there is a resource cost to meeting with new employees weekly and additional communications. This would be a great point to look into for future work to see how a company can continue to increase employee engagement without increasing cost/time.

5.3 Future Works

As mentioned, the reason the increased efforts were halted was because of the time it took out from the security team's day/week and there is a cost to those team members time and efforts. While it is important to increase employee engagement, is it

worth that cost? Conduct a cost/benefit analysis to quantify a more personalized security awareness program as well as having a highly communicative security team.

Instead of always meeting on the employee's day-1 onboarding for a security session, are there better alternatives. Could an organization create a video that gives more of that personal, welcoming feeling but also keeps security top-of-mind for the employee? Could automation take over some of the interaction?

REFERENCES

Kalton, G., & Piesse, A. (2007). Survey Research Methods in Evaluation and Case-Control Studies. *Statistics in Medicine, (2007), 1675-1687, 26(8)*

Luftman, J., & Kempaiah, R. (2007). An Update on Business-IT Alignment: "A-Line" Has Been Drawn. In *MIS Quarterly Executive* (Vol. 6, Issue 3). John Wiley and Sons.

Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers and Security*, *28*(8), 816–826. https://doi.org/10.1016/j.cose.2009.05.008

Hedderly, D. J., & Scott, H. (2015). Measuring the Effectiveness of Video Training through Technology-Based Education: *Quarterly Journal. S.A.M. Advanced Management Journal, 80(1), 41-50,3.* , 41–50. Retrieved from https://goldcoast.idm.oclc.org:9443/login?url=https://www.proquest.com/scholarly-journals/measuring-effectiveness-video-training-through/docview/1689625506/se-2?accountid=5603

Schreiber, B. E., Fukuta, J., & Gordon, F. (2010). *Live lecture versus video podcast in undergraduate medical education: A randomised controlled trial*. http://www.biomedcentral.com/1472-6920/10/68

Ross, R., Pillitteri, V., Dempsey, K., Riddle, M., & Guissanie, G. (2020). *Protecting controlled unclassified information in nonfederal systems and organizations*. https://doi.org/10.6028/NIST.SP.800-171r2

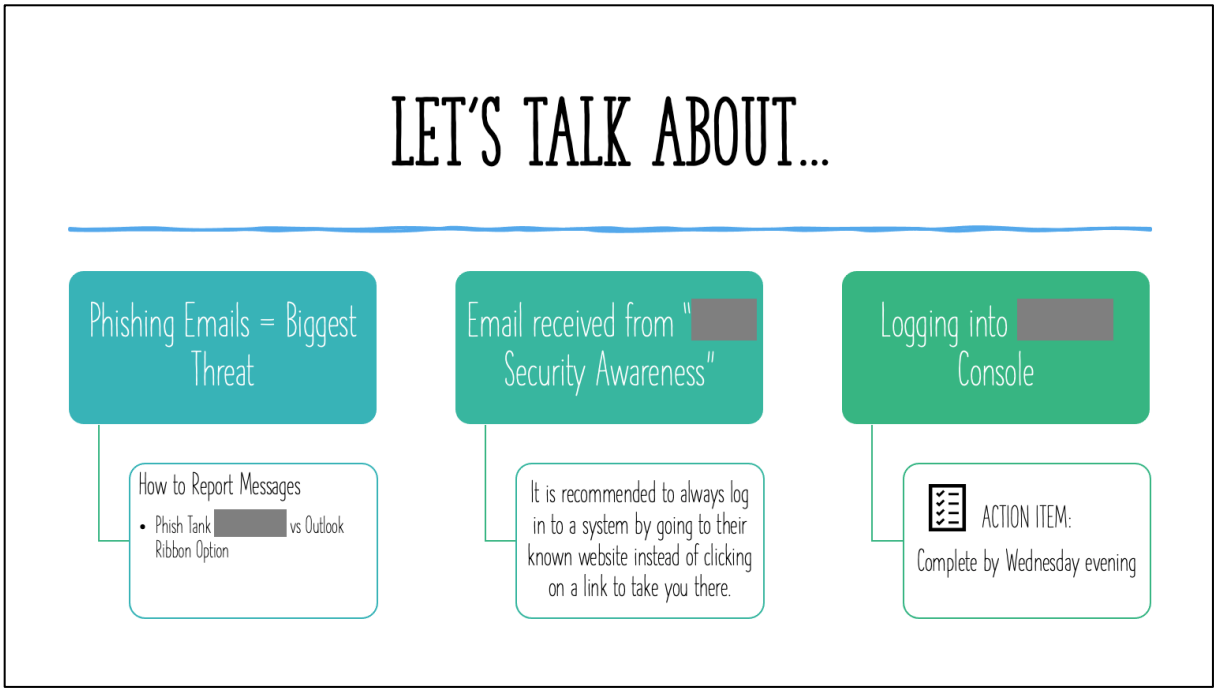
NIST. (2020). Program Review for Info Sec Assistance. In *https://csrc.nist.gov/projects/program-review-for-information-security-assistance/security-maturity-levels*. NIST (National Institute of Standards and Technology). https://csrc.nist.gov/projects/program-review-for-information-security-assistance/security-maturity-levels

Carnegie Mellon University and The John Hopkins University Applied Physics Laboratory LLC. (2020). *CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)*.

Story, D. A., & Tait, A. R. (2019). Survey Research. *Anesthesiology*, *130*(2), 192–202. https://doi.org/10.1097/ALN.0000000000002436

APPENDIX

A. New Hire Security Onboarding Slide Deck:



LET'S KEEP TALKING...

Security is HERE FOR YOU - no judgment
([redacted]@[redacted])

- Email/website mishaps - stuff happens - WE ARE ALL HUMAN (but if you're not - can we meet up later, I have questions?)
- Physical security situations.
  - [redacted]
  - Stranger in building scenario.
  - Lost/Stolen device.

IT/Security Newsletters and other random cool things...

- IT
  - Projects in the pipeline that could affect your access or device(s)
- Security
  - Tips/Tricks/Surveys/Videos
- Your B.O.B.

Third Party Risk Management
([redacted]@[redacted])

- Due Diligence from Customers
- Requests for application installations

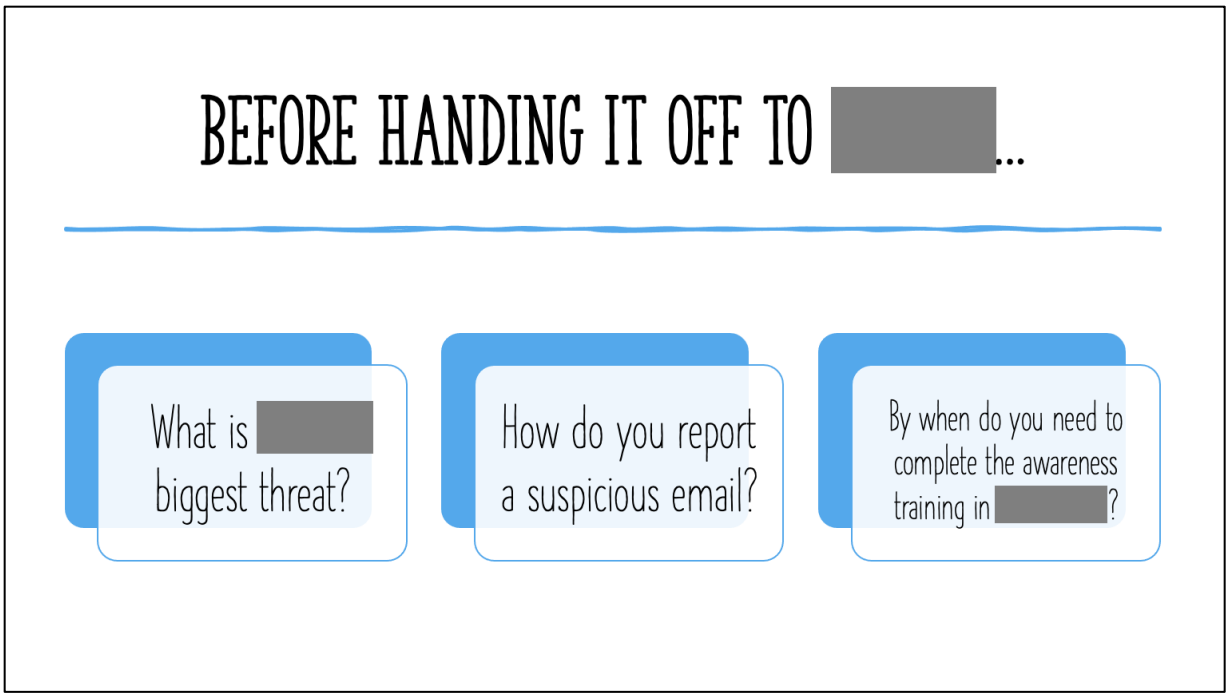
LET'S CHANGE GEARS JUST A BIT...

[redacted]

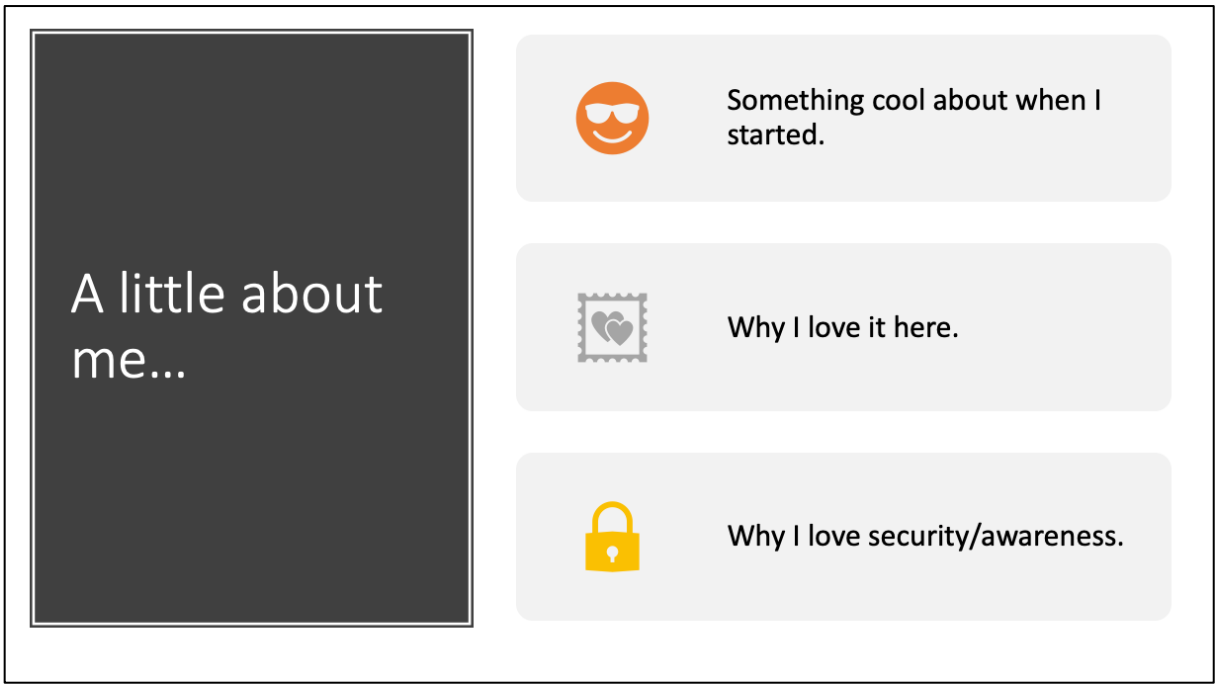
- Update notification preferences
- Action items / Inbox
  - [redacted] profile getting fully provisioned.

WHY update notifications?

- So you know when you have action items, birthdays, benefits like open enrollment, annual attestations, etc.


BEFORE HANDING IT OFF TO [redacted]...
What is [redacted] biggest threat?
How do you report a suspicious email?
By when do you need to complete the awareness training in [redacted]?

B. Security Bootcamp Presentation Slide Deck



Switching modes…

Do you remember what [redacted] biggest threat is?

People who reported:

[redacted]

From: Google <security@mailsender-google.com>
Reply-To: Google <security@mailsender-google.com>
Subject: [redacted] connected to your Google Account

Template ID:191569-1466208
Send me a test email
Toggle red flags

Google

[redacted] connected to your Google Account

You received this message because [redacted] is listed as a recovery email for your Google account. If this is not your Google Account, click here to disconnect from that account and stop receiving emails.

Hi Jennifer,

[redacted] now has access to your Google Account.

[redacted] can:

- Read, send, delete, and manage your email
- Manage your contacts
- View and manage the files in your Google Drive

You should only give this access to apps you trust. Review or remove apps connected to your account any time at My Account.

Learn more about what it means to connect an app to your account.

The Google Accounts team

This email can't receive replies. For more information, visit the Google Accounts Help Center.

C. Newsletter Survey Example Results

1. One way to cover your ____ is to set your socia	2. Regulations alone do not protect privacy. __ do	3. You should do this to any social media accts yo	4. These two compliance regulations empower consum	5. Do you feel like this email/newsletter is info	5a - Yes >> What is your favorite part and how can
digital footprint	Security Tools	Deactivate.	CCPAHIPPA	Yes	I love them. I feel like my company keeps employees and customers' data protected. I enjoy learning about security issues in a broken-down way/using language I can easily follow. Thank you for all you do!
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	Break down the info a little more if possible to help those understand and make it more applicable to them!
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	They're helpful!
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	I am always learning something new!
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	.
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	I find the newsletters helpful but I am not a big fan of the Inside Man clips. Sorry!
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	Great newsletter! I liked the section that had examples of the types of scams related to COVID-19. I also found the resources to learn more about compliance regulations very useful. Thanks!
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	videos are entertaining
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	n/a
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	I like the graphics and short informative points that I can take away. Relevant topics are always interesting and it is nice to be reminded about ways to keep your information secure!!
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	Not bad...short and to the point...
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	Very informative especially in these trying times. It helps us to be aware of what is happening around us. Great job!
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	Keep them coming. They're really great.
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	Nice work!
digital footprint	People/Individuals	Deactivate.	GDPRHIPPA	Yes	I enjoy them as they are!
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	Very well designed newsletter. I appreciated that the information was applicable to both work and home life.
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	It's all good
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	Definitely helps to ensure that "Security" is always top-of-mind. I appreciate the effort and message. Thank you.
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	I like learning more about the digital footprint and what scammers can steal from our identity
digital footprint	Security Tools	Deactivate.	CCPAGDPR	Yes	I very much enjoy the newsletters - they're quite informative!
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	I love following Mark's story! Can't wait to see how it turns out!
digital footprint	People/Individuals	Deactivate.	FMLAHIPPA	Yes	Favorite: Keeping up to date on new issues/features/policies
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	I like to see example of the scams. It was interesting to find out about the new app for finding out who was tested positive. Also it was helpful to know that we could be more proactive about how the data collected by the companies could be used or shared. Thank you.
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	No areas in need of improvements can be seen at this time
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	N/A
person	People/Individuals	Deactivate.	CCPAGDPR	Yes	I enjoy reading and gathering information that pertains to our work family. It's always fun to learn and grow!
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	Sometimes security can be forgotten, especially when business gets busy. These periodic news letters help me keep security in mind.
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	Keep The Inside Man episodes coming!
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	I like the length! It's a quick read and I learn something.
digital footprint	People/Individuals	Deactivate.	GDPRHIPPA	Yes	I like the newsletter and videos. Keep em coming!
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	They're clear, easy to understand, and don't take long to review.
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	.
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	Visually interesting. Information is very timely and relevant, and the language is accessible. Also Inside Man vids are weirdly entertaining.
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	I love that the newsletter was timely, appropriate and short n sweet!
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	Videos are great
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	The Covid Challenges Privacy and scam alerts were good to know

digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	(New employee, first newsletter I'm seeing) I like how you incorporated color/pictures/examples and changed up each page's layout. Visually, the eye is stimulated and it takes what could be dry, boring material and makes it interesting. Very relevant material that can be applied in my personal life as well as business. Side note - I like the Inside Man videos
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	I think it is very helpful as is...
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	I like the addition of current events to make it relatable.
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	I want to be seen as a professional on media, and want to make sure my accounts are properly secured.
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	Favourite part was reading how covid19 challenges privacy and learning about the different scams. That's super relevant to us at the moment and it's good to know what to look out for.
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	No specific feedback
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	The most value i get from the newsletter is the how applicable the content is to my business as well as the current scams our employees are seeing.
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	You are totally crushing it, great newsletter!
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	Nice reminder to reassess what I'm doing security and privacy-wise.
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	Just keep 'em coming. Just like everyone is in sales, everyone is in security!!
digital footprint	Security Tools	Deactivate.	CCPAGDPR	Yes	I like that their short, sweet and to the point.
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	Being new to the company, this is a great way to gain further knowledge of policies/procedures/overall company information.
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	It was good to call out compromised websites around Covid
digital footprint	People/Individuals	Deactivate.	FMLAHIPPA	Yes	I think I was supposed to watch the video first. I skimmed the email. I understand my mistake now
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	n/a
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	Nice reminders
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	It would be great to highlight a real world example of a security threat the security team intercepted and stopped!
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	Great job team ... I like the videos!!
digital footprint	People/Individuals	Deactivate.	FMLAGDPR	Yes	Security awareness is important to the entire company.
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	These newsletters provide great information relevant to my position as an Information Security Professional. But even if I were just an average person out there, these newsletter provide information that is still useful to all!
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	The Inside Man is quite amusing!
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	Like you said, security is on all of us, so I like getting an update on security issues that are relevant to the time at hand.
digital footprint	People/Individuals	Deactivate.	GDPR	Yes	Coming from a company where you had emails full of information all the time coming at you this is quick and easy! Thanks for making it enjoyable to read and the quick videos relatable.
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	Short, sweet, and to the point! Great job!
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	Enjoying the Inside Man videos!
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	Keep up the awesome work!
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	I like that there is a chance to win a gift card. The graphics and design of the letters are good, too.
digital footprint	Security Tools	Deactivate.	CCPAGDPR	Yes	From time to time being made aware of the security practices are a must for everyone and in every role!
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	Some times the newsletters come off a little campy. I think a fairly serious approach to security is not necessarily a bad thing.
digital footprint	Security Tools	Deactivate.	GDPRHIPPA	Yes	The interval of newsletter could be increased.
digital footprint	People/Individuals	Deactivate.	FMLAHIPPA	Yes	Not going to lie. I totally thought the link was a Phishing test.
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	I love how engaging the newsletter is through both the contents and design.
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	Surveys like this are fun, if you have time to do them
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	I like that the newsletters are specific and brief. I can quickly read through best practices without having to get caught up in too many technical details. The real world examples are nice because they are relatable.
digital footprint	Security Tools	Deactivate.	CCPAGDPR	Yes	Very good structured and like it was very interactive
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	Thank you for getting entertaining videos instead of a droning on talking head.
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	I appreciate the info and I like the level of detail shared.

digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	Include content that covers all countries- it is very US focused.
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	Great info! I like how all of this is broken into realistic examples!
digital footprint	Security Tools	Deactivate.	CCPAGDPR	Yes	Always helpful and beneficial to remind folks about protecting each other from any danger
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	I'd like more highlight bullets.
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	layout and graphics are nice and make it fun to read - also very relevant material to what is going on right now. Good job!
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	Relatively quick and easy to read, especially with all of the graphics and organized sections.
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	Thanks for all you do!
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	animation helps my understanding, thanks!
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	It is a good reminder to for things we should already be aware of!
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	I love this security stuff. I've had bank accounts opened without my consent, credit card numbers stolen, money withdrawn from an ATM in Los Angeles while I was physically in Jersey, all kinds of stuff. I dread the day this happens in my professional life and not my personal.
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	I like the reminders to stay secure and vigilant, and I especially appreciated the information about Covid and privacy in this one.
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	Really like the approach to talk about privacy concerns by way of relevant current topics. In particular, I really enjoyed the piece on the proposed COVID app - great explanation!
digital footprint	People/Individuals	Deactivate.	CCPAGDPR	Yes	Anything that informs me of regulations / things to think about in the context of how we interact with our customers during implementation is helpful and interesting to me.
digital footprint	People/Individuals	Deactivate.	GDPRHIPPA	Yes	make the content available in ***** so we can earn badges and points for it.

D. Training Topics Mapped to Survey Questions

Covered	TRAINING VIDEO TOPICS:	QUESTIONS:	RELATED TOPICS:	NOTES:
	1.0 Information Security Overview			
x	1.1 Data Classification (Confidential, Internal, and	**1. To what extent do you think about the data/information you have access to and it's classification?**		
x	1.2 Information Security Principles: Need to Know, Least Privilege, Clean Desk, Data Protection	A. Never	n/a	Behavior/Attitude
x	1.3 Confidentiality, Integrity, Availability (CIA)	B. Rarely		
x	1.4 Everyone is critical to the organizations security	C. Often		
		D. Always		
		2. Social security numbers, drivers licenses, and account numbers would be classified as what type of data?		
		A. Public		
		B. Internal	Data Classification	Training Modules
		C. Confidential		
		D. None of the above.		
		3. Company financial statements, employee salary information, proprietary code, and internal system processes would be classified as what type of data?		
		A. Public		
		B. Internal	Data Classification	Training Modules
		C. Confidential		
		D. None of the above.		
		4. According to the annual information security training, what are the three pillars that make up good security?		
		A. Confidentiality, Integrity, Applicability		
		B. Confidentiality, Identity, Applicability	CIA	Training Modules
		C. Confidentiality, Identity, Availability		
		D. Confidentiality, Integrity, Availability		
		5. Which employee(s) have a responsibility in ensuring security within the company?		
		A. Information Security Specialists		
		B. Security Solution Architects	Everyone is critical to the organziation's security.	Training Modules, Bootcamp
		C. All Employees		
		Implementation Consultants		
		6. Which of the four security principles requires that employees shall have no more authority than necessary for their role?		
		A. Need to Know.		
		B. Least Privilege	Information Security Principles	Training Modules
		C. Clean Desk		
		D. Data Protection		

Covered	TRAINING VIDEO TOPICS:	QUESTIONS:	RELATED TOPICS:	NOTES:
	2.0 Potential Threats			
x	2.1 Malicious software (viruses, worms, trojan horses,	**7. Malware is malicious software that can harm your systems and is a serious security threat. What are some signs that your device may be infected with malware?**	Malicous software and signs of malware.	Training Modules
x	2.2 Signs of malware	A. Changed settings that cannot be changed back to their original settings.		
x	2.3 Protecting against malware	B. Web/Internet Browser has additional components you do not recall downloading		
x	2.4 Password attacks	C. Programs taking longer than usual to start or not starting at all.		
x	2.5 Protecting against password attacks	D. All of the above.		
x	2.6 Wireless threats	**8. Employees can help protect against malware by doing each of the following *except*:**	Protecting against malware.	Training Modules
x	2.7 Physical security threats	A. By only using company-managed device(s) for company-related work.		
x	2.8 Social engineering	B. By having anti-virus installed.		
x	2.9 Internal threats	C. By not working with confidential data.		
		D. By not opening email attachments from unknown senders.		
		9. You are working diligently and open an internet browser to search for something related to your work. All of a sudden, you start getting adverstisements popping up on your screen. What	Protecting against Malware. Identifying and Reporting	Training Modules
		A. Close the adverstisements and continue working.		
		B. Close the advertisments and all other files and restart your device.		
		C. Close the adverstisements and all other files/programs, disconnect from the internet, document what happened, and contact Help Desk.		
		D. Close the adverstisements and all other files/programs, disconnect from the internet, and contact Help Desk.		
		10. What are some ways we can protect ourselves against password attacks?	Password Attacks and Protecting against Password Attacks.	Training Modules
		A. Include uppercase, lowercase, special characters, and numbers in your password(s).		
		B. Use different passwords for your personal and work accounts.		
		C. Use SSO (Single Sign On) and/or password manager.		
		D. All of the above.		
		11. Email mistakes such as clicking on a link happen, but mistakes are inevitable because we are all _____. Please remember it's not about the mistake, but how we respond that matters.	Part of a schpill about Incident Response/ Identifying Reporting	Day 1 onboarding
		A. human		
		B. blind		
		C. ignorant		
		D. nice		
		12. You receive a suspicious email and want to report it, what's the best way to do this?	Social Engineering Identifying and Reporting Email Safety	Day 1 onboarding
		A. Forward to the security team.		
		B. Post in phish-tank		
		C. Send via the Report Message button in Outlook.		
		D. Let your manager know.		
		13. You notice an employee gave their computer password to another employee. You bring it to their attention that this is bad practice and could result in a breach, but the employee dismisses your concerns and says they have done it before and nothing happened. At this point, this employee could be considered an insider threat even if their intent is not malicious. What should you do? Choose the best answer.	Insider Threats Identify and Reporting	Training Modules
		A. You have already said something to them so you should not do anything else.		
		B. Report the incident to the security team.		
		C. Contact your manager to make them aware.		
		D. Repeat your concerns to the employee and show them security policy/training to prove your point.		
		14. You are traveling and have some time in the airport before your flight. You need to send a few emails concerning customers and have not yet been given access to the company VPN. What is the most secure way to access the internet?	Wireless Threats	Training Modules
		A. Use the airport's free, public wifi for internet access.		
		B. Use your phone/hotspot for internet access.		
		C. Use the airport's provided password to access the internet.		
		D. All of the above.		
		15. Your laptop gets stolen or lost. What do you do?	Physical Security Incident Response	Day 1 onboarding and Training Modules
		A. Contact your manager immediately.		
		B. Contact the helpdesk immediately.		
		C. Contact the authorities immediately.		
		D. All of the above.		

Covered	TRAINING VIDEO TOPICS:	QUESTIONS:	RELATED TOPICS:	NOTES:
	3.0 Incident Response			
x	3.1 Identifying and Reporting	Several of the above cover this topic.		
	4.0 Protecting Data			
x	4.1 Password hygiene	**16. Because it makes it easier to remember, basing passwords on a family member's or pet's name is good practice:**	Protecting Data	Training Modules
x	4.2 Email safety	A. True		
x	4.3 Proper media disposal	B. False		
x	4.4 Securing devices physically and logically (locking device,	**17. What are some ways you can protect [company] data?**		
x	4.5 Reinforcing data classification and handling	A. Properly dispose of media such as sensitive data written or printed on paper.		
x	4.6 Using internet responsibly	B. Always lock your device before leaving your desk/workstation.		
		C. Do not open unsolicited links/attachments or post sensitive [company] data/comments on forums or social media.		
		D. All of the above.		
		18. Your Lastpass password has expired and you need to create a new one. Which option is the best for your new password?	Password Hygiene	Training Modules
		A. 14mAmazing123		
		B. qwerty_123		
		C. respect3ach0ther		
		D. haveFun_b3Br4ve		
Covered	**TRAINING VIDEO TOPICS:**	**QUESTIONS:**	**RELATED TOPICS:**	**NOTES:**
	5.0 Mobile Security			
x	5.1 Guard and lock devices	**19. You are staying out of town and decide go to the nearest coffee shop to get some work done. What are some ways you can work securely in a public environment?**	Guard & Lock Devices Using devices in public places Shoulder surfing	Training Modules
x	5.2 Keep data backed up via appropriate resources	A. Be aware of others who may be able to see your screen.		
x	5.3 Don't 'root' devices	B. Do not discuss confidential topics while in public.		
x	5.4 Sensitive info on mobile devices	C. Lock and guard your device at all times.		
x	5.5 Shoulder surfing	D. All of the above.		
x	5.6 Using devices in public places	**20. The use of personal removable media, such as a USB, is allowed.**		
		A. True	Keep data backed up via appropriate resources.	Training Modules
		B. False		
		21. By saving confidential data in an approved storage location, data is protected even if your laptop is stolen.	Keep data backed up via appropriate resources.	Training Modules
		A. True		
		B. False		
		22. It is safe to store sensitive, work-related data on your mobile device.	Keep data backed up via appropriate resources.	Training Modules
		A. True		
		B. False		
		23. "Rooting" or "Jailbreaking" your mobile device opens up the device to vulnerabilities.	Don't root devices	Training Modules
		A. True		
		B. False		

Covered	TRAINING VIDEO TOPICS:	QUESTIONS:	RELATED TOPICS:	NOTES:
	Other Questions for Information Gathering			
		24. How long have you been with the company?		This helps to see the difference (if any) between the individuals who received day 1 onboarding and those who did not.
		>1 year		
		<1 year		
		25. Did someone discuss security on your first day?		
		Yes		
		No		
		25b. If yes, do you believe you consider security more often since it was discussed on your first day?		
		Yes		
		No		
		Neutral		This set of conditional/logical questions help provide insight into end-users personal view/attitude of the day 1 onboarding training.
		25b2. Would you have preferred a video rather than "in-person" meeting concerning security on your day 1?		
		Yes		
		No		
		25c. If no, do you believe you would consider security more often had it been discussed on your first day?		
		Yes		
		No		
		Neutral		