

TRANSFORMATIONAL SECURITY AWARENESS

**WHAT NEUROSCIENTISTS, STORYTELLERS,
AND MARKETERS CAN TEACH US ABOUT
DRIVING SECURE BEHAVIORS**

BY PERRY CARPENTER

Contents

Figure 1.1	4
Figure 1.2	4
Table 1.1	5
Table 1.2	8
Figure 2.1	8
Figure 2.2	9
Table 2.1	10
Figure 3.1	11
Figure 3.2	12
Table 3.1	13
Figure 3.3	15
Table 3.2	16
Table 3.3	17
Figure 3.4	17
Figure 3.5	18
Figure 3.6	18
Figure 4.1	19
Figure 4.2	19
Figure 4.3	19
Table 4.1	20
Table 4.2	21
Figure 4.4	23
Figure 4.5	23
Figure 4.6	24
Figure 4.7	24
Figure 4.8	25
Figure 4.9	26
Table 4.3	27
Table 4.4	27
Table 4.5	28
Figure 4.10	30
Figure 5.1	30
Figure 5.2	31
Figure 5.3	32
Figure 5.4	33
Figure 6.1	34

Figure 8.1	35
Figure 8.2	36
Table 8.1	37
Table 8.2	38
Figure 9.1	40
Figure 9.2	41
Table 9.1	42
Figure 9.3	45
Figure 9.4	45
Figure 9.5	46

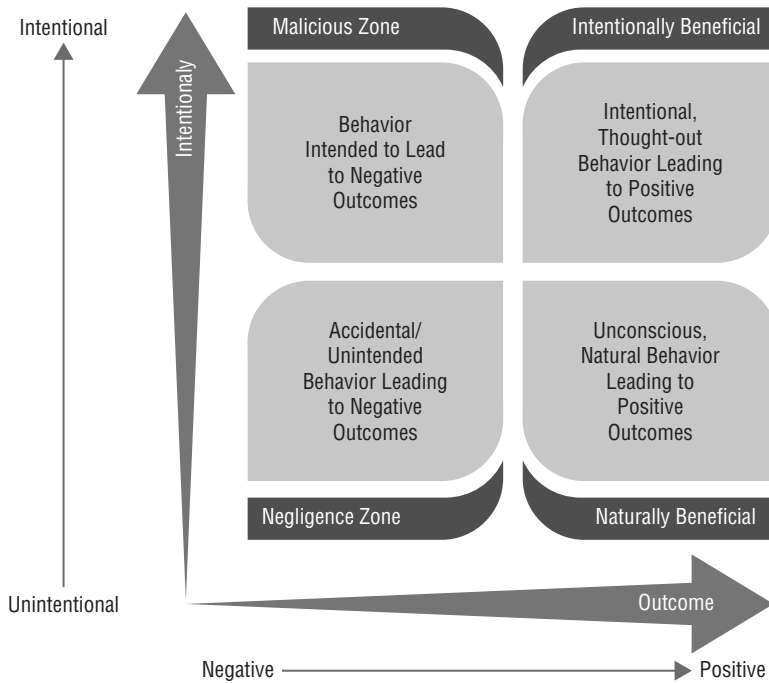


Figure 1.1: Continuum of behavior from unintentional to intentional with malicious/harmful to beneficial outcomes.

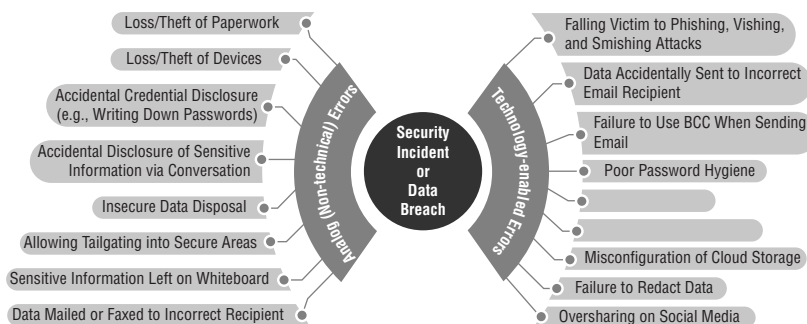


Figure 1.2: Examples of both analog and technology-enabled human errors that lead to security incidents and breaches.

Table 1.1: Example data breaches and their human factor causes

Year	Organization	Impact	Human Factor Cause
2008	Bank of New York Mellon	<p>Multiple issues contributed to a data breach impacting up to 12.5 million BNY Mellon customers. The first issue was that sensitive data on the tape was not encrypted. Then the tape went missing.</p> <p>The incident was caused by the loss of a backup tape that was handed off to a third party for storage with nine other tapes. When the tapes arrived at the off-site storage building, one was missing; the other nine were accounted for.</p>	Loss of unencrypted backup tape
2009	Heartland Payment Systems	Heartland Payment Systems was breached by hackers using a common SQL injection vulnerability. The result was the loss of 130 million credit and debit card numbers and more than \$140 million in breach-related expenses.	Poor coding (SQL injection)
2010	CitiGroup	Approximately 600,000 CitiGroup customers received year-end tax statements with their Social Security numbers printed on the outside of the mailing envelope delivered by the U.S. Postal Service.	Formatting error oversight
2011	RSA Security	Attackers were able to breach RSA Security's network by sending two different phishing emails over a two-day period. The two emails were sent to two small groups of employees; you wouldn't consider these users particularly high-profile or high-value targets. The email subject line read "2011 Recruitment Plan." Seeds for RSA SecureID two-factor authentication token were exfiltrated. In addition to dealing with the public outcry and loss of face in the security community, RSA Security spent approximately \$66 Million reissuing physical tokens to SecureID customers.	Spear-phishing attack with malware payload

Table 1.1: Example data breaches and their human factor causes (continued)

Year	Organization	Impact	Human Factor Cause
2012	Yahoo!	Attackers embarrassed Yahoo! and shocked the security community by posting the usernames and passwords of 450,000 users associated with the Yahoo! Contributor Network. The attackers used a common SQL injection vulnerability. Adding insult to injury, the passwords that the attackers accessed were in plaintext.	Poor coding (SQL injection vulnerability) and user passwords stored in plaintext
2013	Target	Credentials from one of Target's HVAC contractors were stolen via a phishing attack that downloaded and launched malware. These credentials were used to gain access into Target's networks and move laterally across systems. The effects resulted in the loss of data from approximately 40 million credit and debit cards as well as personal information associated with 70 million Target shoppers.	Phishing attack with malware payload
2014	eBay	Credentials from a number of (up to 100) eBay employees were compromised to gain network access. The attackers were able to exfiltrate data from 145 million customers.	Phishing attack leading to credential theft
2015	Anthem	The records of approximately 78.8 million current and former customers were exposed as the result of a successful phishing attack potentially carried out by a foreign government. An investigation found that the phishing email was opened by a single employee at an Anthem subsidiary in February 2014, nearly a year before the breach was discovered and reported.	Phishing attack with malware attachment

Table 1.1: Example data breaches and their human factor causes *(continued)*

Year	Organization	Impact	Human Factor Cause
2016	Democratic National Committee (DNC)	It's hard to overestimate the impact that the DNC hack had. As the result of a credential harvesting attack, hackers were able to access the email account of John Podesta, campaign manager for Hillary Clinton. The emails were leaked and were the source of a number of embarrassing media stories that may have influenced the results of the 2016 U.S. Presidential Election.	Phishing attack leading to credential theft
2017	Equifax	The Equifax breach of 2017 exposed the personal information (including Social Security numbers) of approximately 145 million people. In addition to the data breach, Equifax's incident response and public reporting was extremely unorganized and caused great confusion to consumers wanting to know if their data was exposed.	Hack enabled by internal miscommunication and failure to apply patches in a timely manner
2018	Exactis	Exactis is a large data broker located in Florida. Security researchers found a fully exposed database containing personal information of nearly every U.S. citizen and millions of businesses. It contained data such as phone numbers, email addresses, personal habits, and information on the children (including age and gender) for each of the named individuals.	Unintended disclosure/misconfiguration of cloud storage

Table 1.2 : The reality of human nature and security awareness programs

Statement	Implication
"Just because I'm aware doesn't mean that I care."	Awareness doesn't lead to caring. And, if I don't care about something, I'm unlikely to go out of my way to engage with it or perform related tasks.
"If you try to work against human nature, you will fail."	Humans are wired in specific ways. We don't like to do things that are difficult, awkward, or require change.



Figure 2.1: The four main reasons why organizations create security awareness training programs.

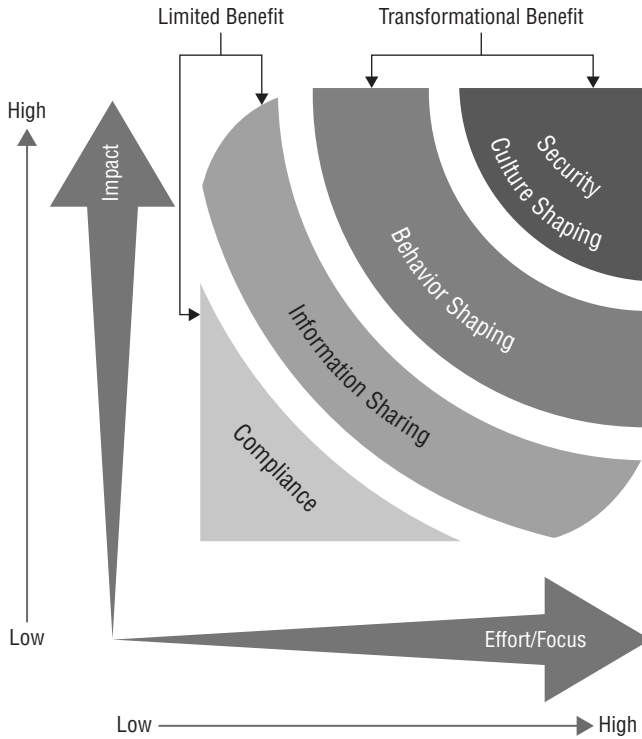


Figure 2.2: Your program's goal either will produce limited benefit or can be transformational for your organization.

Table 2.1: Human nature and security awareness programs: statement, implication, and resolution

Statement	Implication	Resolution
“Just because I’m aware doesn’t mean that I care.”	Awareness doesn’t lead to caring. And, if I don’t care about something, I’m unlikely to go out of my way to engage with it.	Connect security awareness messaging to topics, situations, and outcomes that your audience will naturally find relevant and meaningful. In cases where the connection is less intuitive, you will need to help them “connect the dots.” Don’t neglect the power of emotion and story. The more human the ideas become, the better. Move away from abstract, security-centric information and connect the information to human-centric outcomes, purposes, and compelling visuals. I’ll be discussing the nuts and bolts of how to do this in Chapter 3.”
“If you try to work against human nature, you will fail.”	Humans are wired in specific ways. We don’t like to do things that are difficult, awkward, or require change.	When human nature makes performing secure behaviors difficult, you will need to either increase their motivation to perform the behavior (help them remember or understand why it is important), or you will need to find ways to make it easier for them by helping to facilitate the correct behavior. This can be accomplished with technology-based help or by “prompting” the correct behavior at the appropriate time. Even more difficult behaviors can begin to become easy and intuitive when repeated enough times. The goal is to create healthy security habits so that the behavior no longer becomes an exercise in logic but instead becomes engrained, effectively second nature. I’ll be discussing how this is achievable in Chapters 4 and 5.

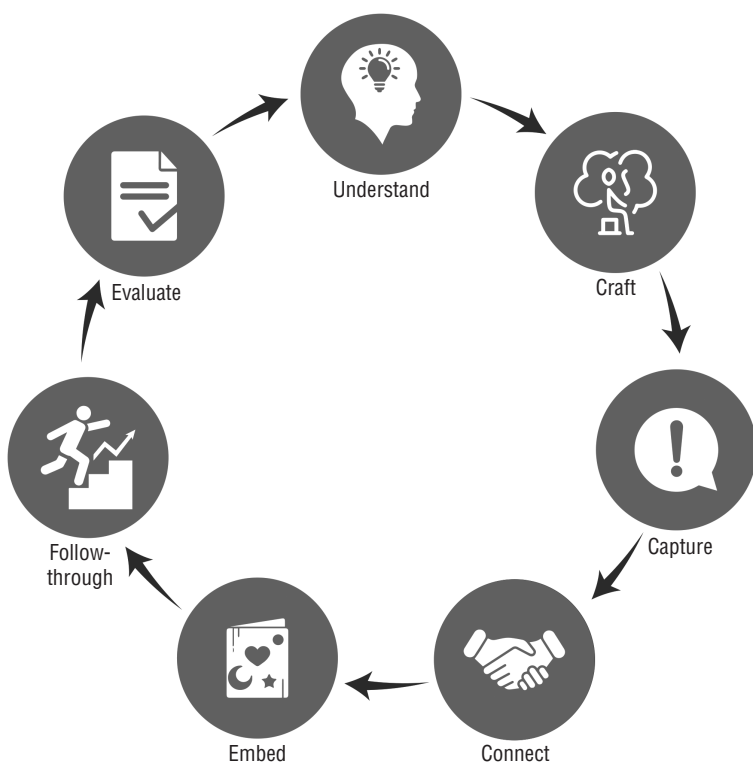


Figure 3.1: Seven key takeaways from the communications disciplines

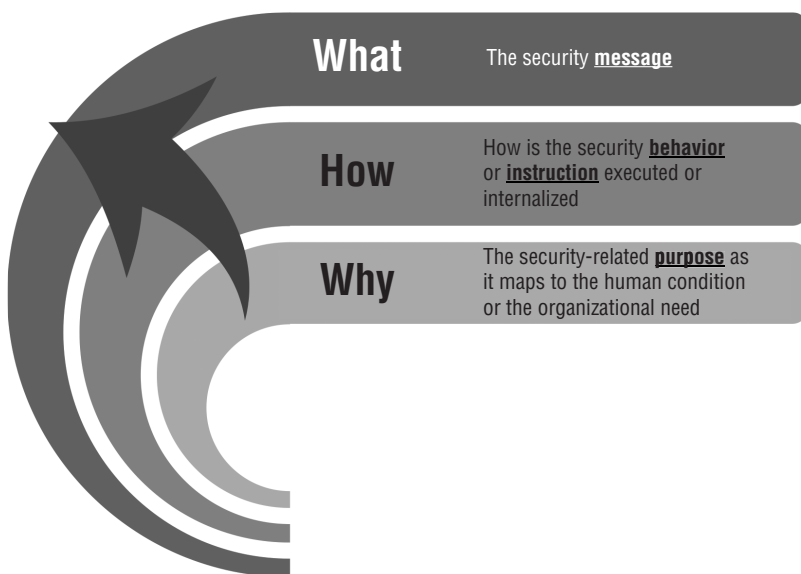


Figure 3.2: Security awareness leaders should start with “why.”

Table 3.1: Connecting the 8Ps of Marketing to Security Awareness

8Ps That Comprise the Marketing Mix		Marketing Context	Awareness Context
Product/service		The thing being sold or charged for.	The security-related message or behavior that you are hoping to train.
Price		The fee and associated pricing model.	The time, effort, or sacrifice that the end user must put in as part of the training.
Place		Where the customer can find the product. This is the store, website, or other distribution channel.	Where does the training take place? How do end users receive the training? Examples include computer-based training (CBT) modules, videos, posters, in-person events, simulated phishing campaigns, and so on. How do your people encounter training within the context of their lives?
Promotion		How and where is the product or service being “talked” about? Advertising, word-of-mouth, press releases, endorsements, etc.?	Similar to Place. But, the distinction here is that there are certain activities, forums, or people used to support or advance the object of your training. Examples here would be events such as National Cybersecurity Awareness Month or an executive video talking about the importance of security to the organization.
Physical evidence		Proof of quality, design elements, packaging, online presence, company stability/relevance, etc.	These are the subtle and not so subtle cues that you provide (both intentionally and unintentionally) about the value and traits of your security message or the behavior that you are promoting. How do they encounter the artifacts of your messaging naturally throughout the day? And what is the experience they receive when they intentionally seek out security-related information or advice in your organization?

8Ps That Comprise the Marketing Mix	
Marketing Context	Awareness Context
<p>People</p> <p>Your internal people (such as your employees, management, culture, and customer messaging) and your external people (such as your customers, social influencers, and media).</p>	<p>These are the people involved in creating your program, advocating your program, and who are on the receiving end of the training. It's important to think in terms of roles. For instance, how does your executive team support (or work against) your security messaging? What is the overall tone and direction of your organization's security culture? What is the overall tone that your security team takes when engaging with the broader organization? And, how are others outside of your security team supporting or working against your security-related messaging?</p>
<p>Process</p> <p>Your operational processes. The things you do to create, market, and support the product. Your processes help ensure consistency and predictability.</p>	<p>This is your formal security awareness training plan and the methodologies (both intentional and unintentional) that you use to promote security-related messaging and behaviors. Understanding your process and being intentional about your plan, methodologies, and metrics is vitally important. Process is what helps you drive continual improvement so that you learn from your successes and challenges. Process is the key that unlocks consistency and sustainability.</p>
<p>Partners</p> <p>Other people or organizations that can become new channels for promoting and selling the product or services.</p>	<p>The other methods that you've put in place that will work to propagate your message and reinforce behavior. Security liaison/champion/ambassador/advocate programs are a prime example. Used well, these groups can be a force multiplier for your program.</p>

(continued)

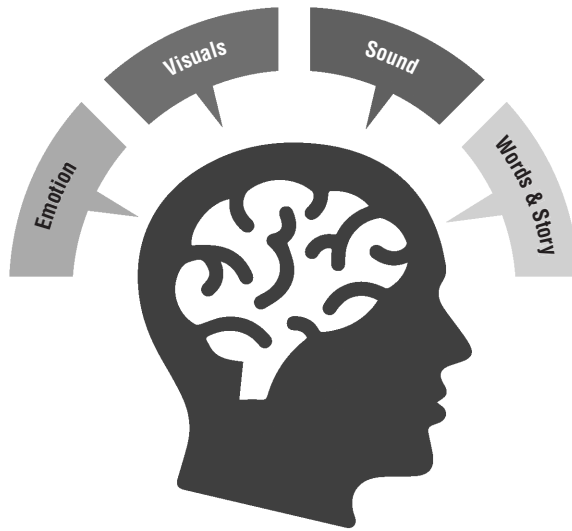


Figure 3.3: Trojan Horses for the mind

Table 3.2: Power of Visual Branding

Brand Name as Text		Brand Representation as Logo
Facebook	or	
YouTube	or	
CocaCola	or	
Amazon	or	
Taco Bell	or	

Table 3.3: Even Simplified Versions of Brand Logos Are Effective

Facebook Icon	YouTube Icon	CocaCola Icon	Amazon Icon	Taco Bell Icon
				

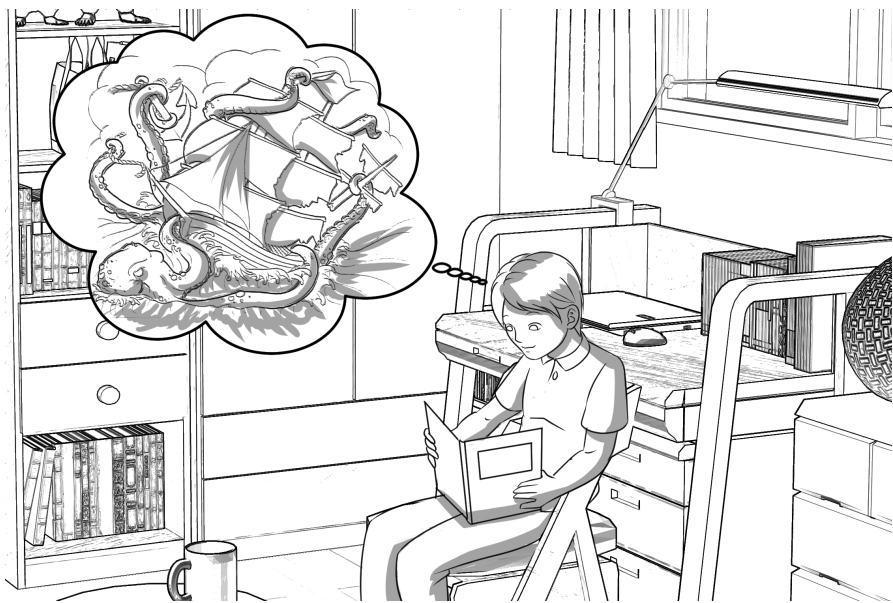


Figure 3.4: Images are the language of the mind.



Figure 3.5: Marketing-based thinking helped drive awareness for the Heartbleed bug.

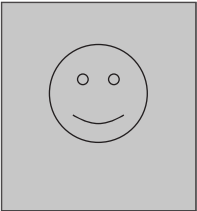
	Name		
	Job Title		
	Job details: quick description		
Demographic Info:	Drivers:	Challenges:	
<ul style="list-style-type: none">• Age• Gender• Location• Salary• Education	What motivates them or is something they need to accomplish?	What issues and frustrations do they deal with? What do they need to overcome?	
Values & Fears: List any strong values or fear that they have.			
How we can help: What do we offer that can help this person accomplish their goals and/or avoid pain and fear?			
Our message to _ (insert persona name) _: A quick customer-centric message about our product that is tailored to this persona, addressing their needs, fears, and goals.			

Figure 3.6: Personas transform “targets” into people.

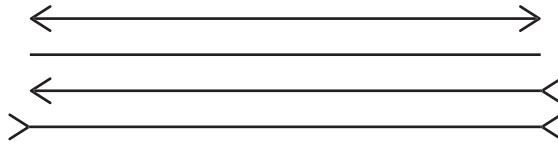


Figure 4.1 System 1 thinking example, part A

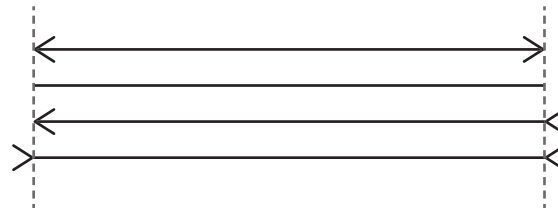


Figure 4.2: System 1 thinking example, part B

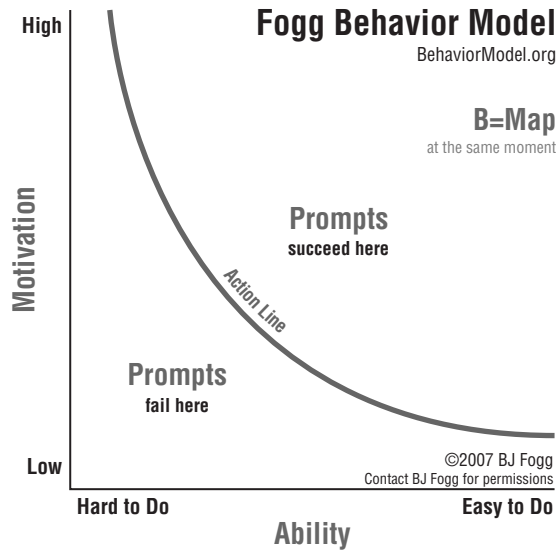


Figure 4.3: Fogg Behavior Model

Table 4.1: Understanding the components of the Fogg Behavior Model (nonsecurity example)

Fogg Behavior Model Component	Description
Behavior (B): What is the specific behavior you're designing for?	Drink a glass of water.
Motivation (M): What types of things might motivate someone to perform the B ?	<ul style="list-style-type: none">■ They could be thirsty or have just eaten a spicy meal.■ They might want social acceptance (everyone else is doing it).■ They might want to avoid offending the person, offering them water.■ They believe that there are positive health benefits associated with staying hydrated.■ Etc.
Ability (A): What types of things must someone already be able to do or know to successfully perform the B ?	<ul style="list-style-type: none">■ A glass of water is available to the person or can be obtained with little effort.■ The person's mouth is not taped shut.■ The person is not asleep or otherwise incapacitated.■ Etc.
Prompt (P): What types of things can cue the B ?	<ul style="list-style-type: none">■ The person notices that they are thirsty or is reacting to the spicy meal.■ Someone offers the person a glass of water.■ The person receives a prompt from a health app reminding them to drink.■ Etc.

Table 4.2: Understanding the components of the Fogg Behavior Model (security example)

Fogg Behavior Model Component	Description
Behavior (B): What is the specific behavior you’re designing for?	Choose a good password.
Motivation (M): What types of things might motivate someone to perform the B ?	<ul style="list-style-type: none">■ They understand and appreciate the value of choosing a good password.■ They feel empowered by choosing a good password.■ They feel more secure by choosing a good password.■ They are afraid that their current password has been (or might be) compromised due to its simplicity.■ They feel pressure to create a better password because the organization is monitoring password strength.■ Etc.
Ability (A): What types of things must someone already be able to do or know to successfully perform the B ?	<ul style="list-style-type: none">■ The person has the required knowledge of how to construct a password that is both strong and memorable.■ The person has tools that will help them construct a password that is both strong and memorable.■ The person has tools that will choose a strong password and remember that password for them.■ Etc.

Fogg Behavior Model Component	Description
Prompt (P): What types of things can cue the B?	<ul style="list-style-type: none">■ The person just feels like changing their password.■ The person receives notification that it is time to change their password.■ The person is locked out of their account because they forgot their current password.■ The organization issues a forced password reset.■ The person receives a security tip that has advice on how to create and remember a good password.■ The person forgot their current password and is about to perform a password reset.■ The person receives a notification that their account was breached and hackers may have accessed the password.■ Etc.

(continued)



Figure 4.4: Example of nudge theory: improving bathroom sanitation
https://commons.wikimedia.org/wiki/File:Nudge_Toilet_1.jpg



Figure 4.5 Example of nudge theory: encouraging recycling

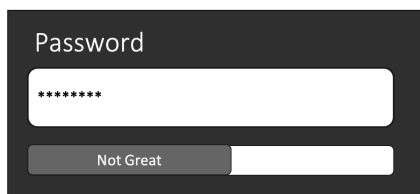


Figure 4.6: Password strength meters are a great security example of nudge theory in action.

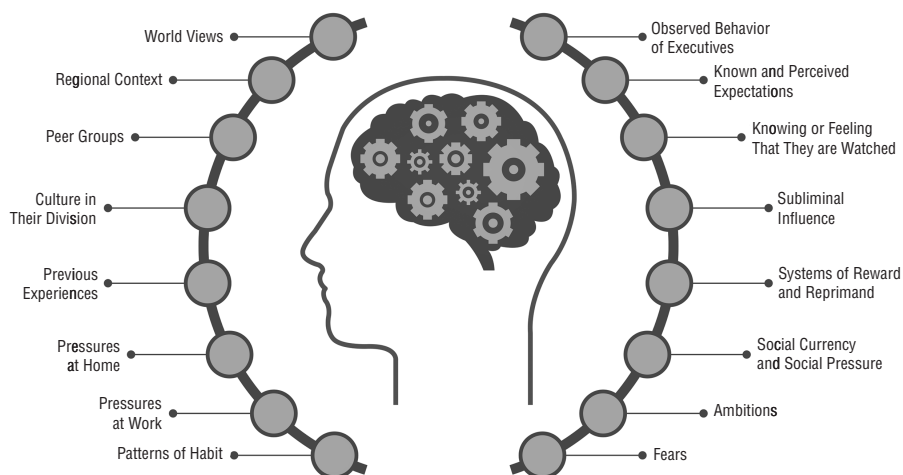


Figure 4.7: Everything is interpreted through context.

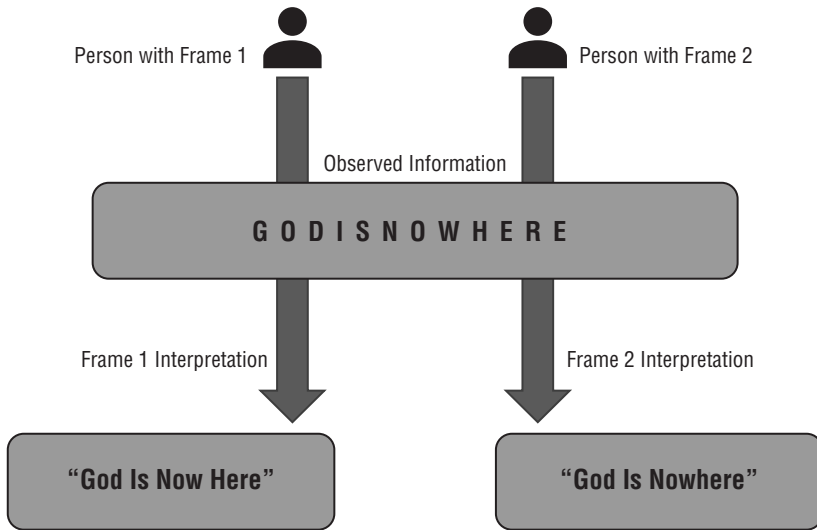


Figure 4.8: Example of frames as interpretive filters

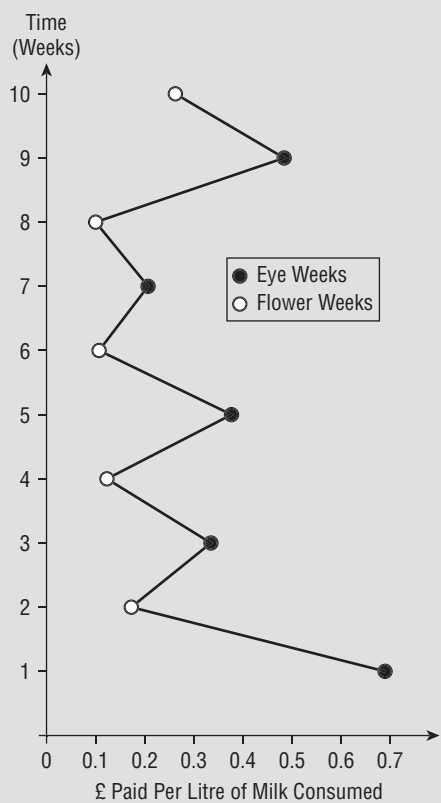


Figure 4.9: The Newcastle University experiment

Table 4.3 : Outcomes arising from different combinations of motivation and ability within the Fogg Behavior Model

Conditions Existing at the Time of Prompt	Outcome
The person has sufficient <i>motivation</i> and sufficient <i>ability</i> .	When prompted, the person will perform the behavior.
The person has sufficient <i>motivation</i> but lacks sufficient <i>ability</i> .	When prompted, the person will want to perform the behavior but will be <i>unable to do so</i> . This can lead to feelings of frustration, incompetence, disillusionment with the task, etc.
The person lacks <i>motivation</i> but has sufficient <i>ability</i> .	When prompted, the person has the ability to do the behavior <i>but doesn't feel like it at the time (doesn't care)</i> . Repeated prompting will likely lead to aggravation and agitation.
The person <i>lacks</i> both motivation and <i>ability</i> .	When prompted, the person isn't <i>able</i> to perform the behavior and is <i>apathetic</i> about it.

Table 4.4 : Different combinations of motivation and ability within the Fogg Behavior Model from a target person's perspective

Conditions Existing at the Time of Prompt	Target Person's Perspective
Motivated and able	"Yes, I'll do that now."
Motivated but lacking ability	"I'd be willing to do that, but I can't. Help me."
Unmotivated but able	"I can do that, but I don't feel like it right now."
Unmotivated and lacking ability	"Huh? Oh . . . nope. I can't, and I don't want to."

Table 4.5: Example of the Fogg Behavior Model applied to password management

Fogg Behavior Model Component	Description
Behavior (B): What is the specific behavior you’re designing for?	Choose a good password.
Motivation (M): What types of things might motivate someone to perform the B ?	<ul style="list-style-type: none">■ They understand and appreciate the value of choosing a good password.■ They feel empowered by choosing a good password.■ They feel more secure by choosing a good password.■ They are afraid that their current password has been (or might be) compromised due to its simplicity.■ They feel pressure to create a better password because the organization is monitoring password strength.■ Etc.
Ability (A): What types of things must someone already be able to do or know to successfully perform the B ?	<ul style="list-style-type: none">■ The person has the required knowledge of how to construct a password that is both strong and memorable.■ The person has tools that will help them construct a password that is both strong and memorable.■ The person has tools that will choose a strong password and remember that password for them.■ Etc.

Fogg Behavior Model Component	Description
Prompt (P): What types of things can cue the B?	<ul style="list-style-type: none"> ■ The person just feels like changing their password. ■ The person receives notification that it is time to change their password. ■ The person is locked-out of his/her account because they forgot their current password. ■ The organization issues a forced password reset. ■ The person receives a security tip that has advice on how to create and remember a good password. ■ The person forgot their current password and is about to perform a password reset. ■ The person receives a notification that their account was breached and hackers may have accessed the password. ■ Etc.

(continued)

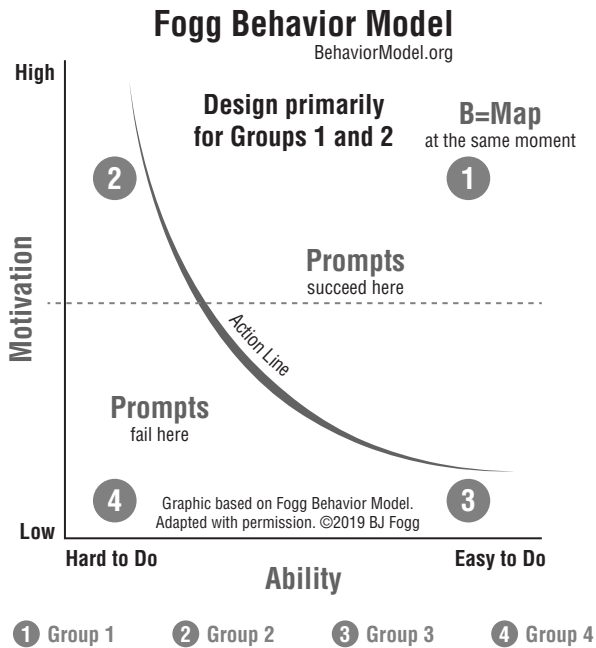


Figure 4.10: Thinking through behavior groups with the Fogg Behavior Model

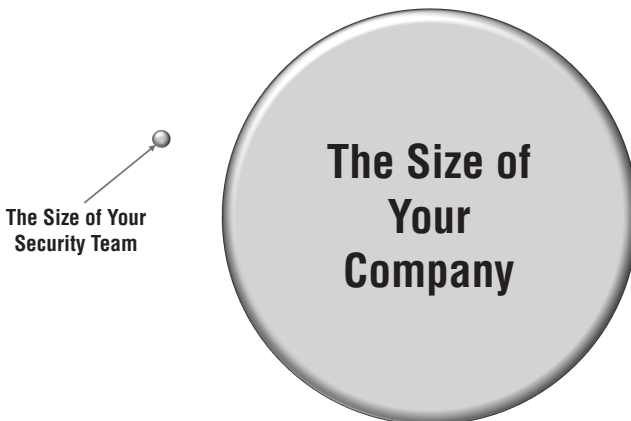


Figure 5.1: Security teams face issues of scale and gravitational influence.

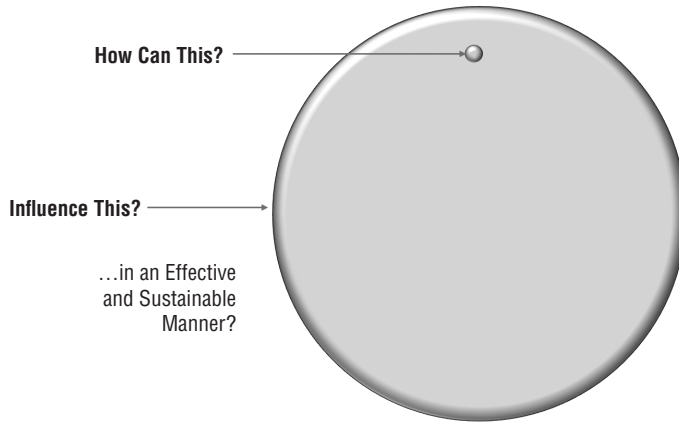


Figure 5.2: Security teams need a force multiplier.

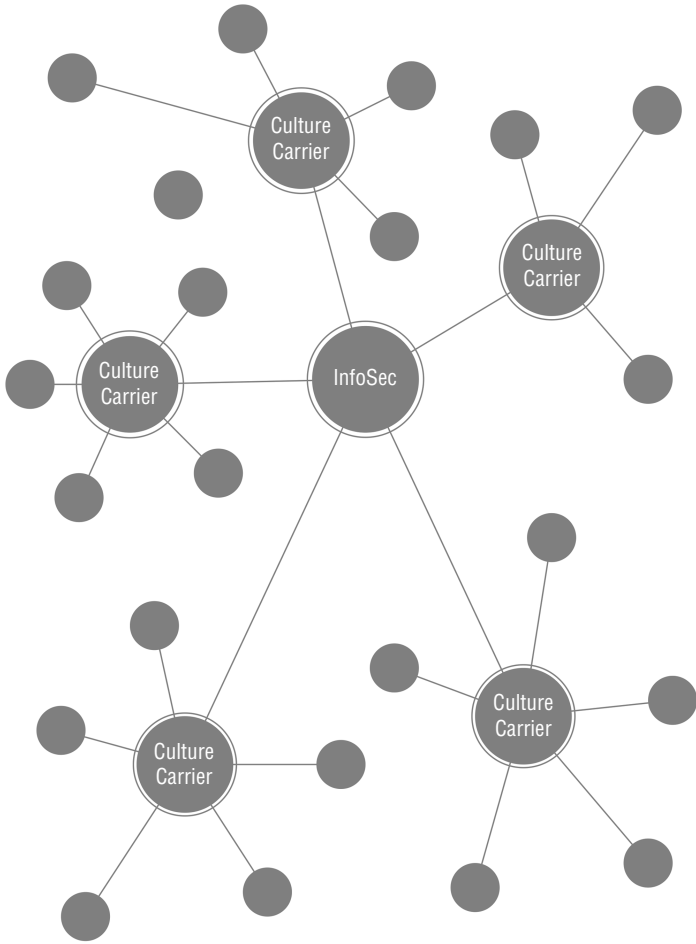


Figure 5.3: Visualization of how culture carriers are viral in nature

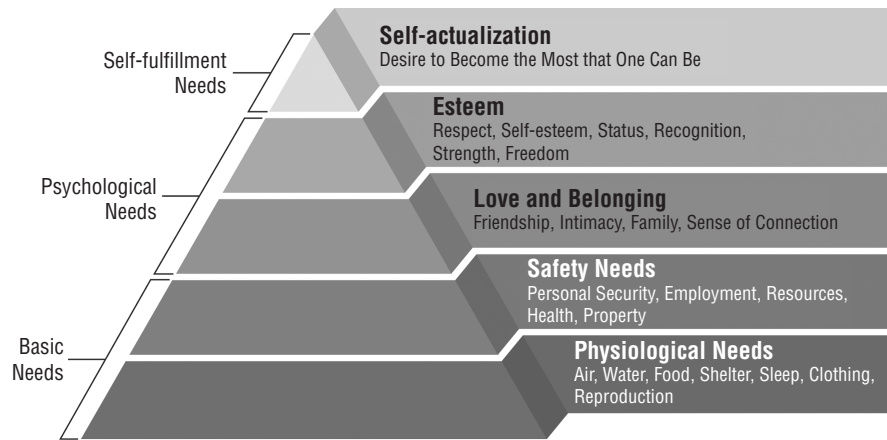


Figure 5.4: Considering Maslow's hierarchy of needs as it relates to security culture

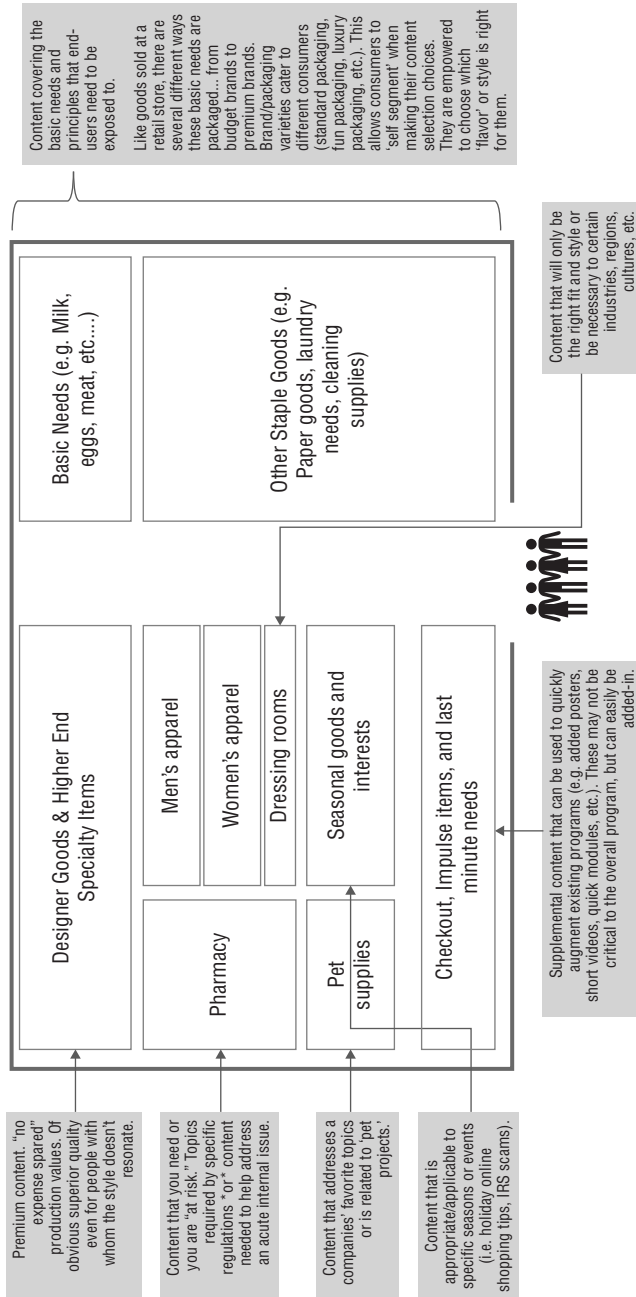


Figure 6.1: Content variety: big-box shopping example

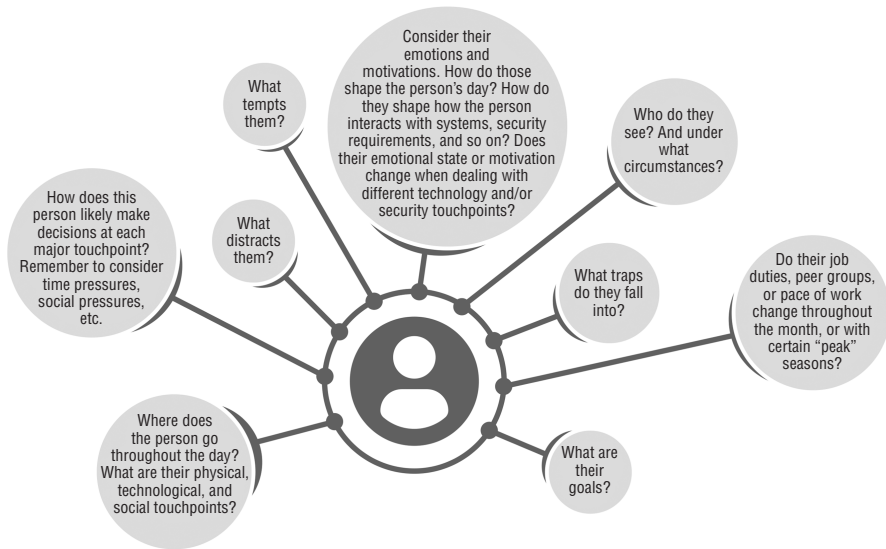


Figure 8.1: Live your awareness program through the eyes and lives of your people.

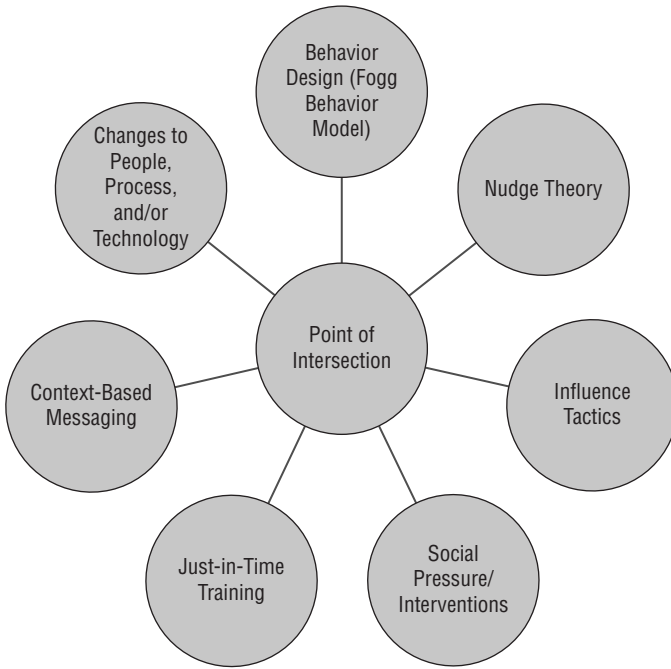


Figure 8.2: Example tactics to use at points of behavioral intersection

Table 8.1: Security Behavior Journey Map Brainstorming Sheet

Function	Answers	Additional Notes/ Comments/ Observations
Who are they?		
When is it? (time of day)		
Where are they? (location)		
What are they doing or about to do? (event/behavior)		
What is their goal?		
What are they feeling? (emotions)		
Who else is around? (social)		
Are there any other interesting or important aspects of the context they are in?		
How might they make mistakes or deliberately make insecure choices?		
Thoughts on Fogg Behavior Model (B=MAP) elements for encouraging secure behaviors?		
What program elements can we use to encourage and reinforce the behavior we want?		
How can we reward people who are doing the right thing or people who accept intervention?		

Table 8.2: Security Behavior Journey Map Brainstorming Sheet
(Completed Example)

Function	Answers	Additional Notes/ Comments/ Observations
Who are they?	General employees/everyone.	This is for everyone, regardless of role.
When is it? (time of day)	Early morning, beginning of the workday.	
Where are they (location)?	Building entrance.	
What are they doing or about to do? (event/behavior)	Enter the building.	
What is their goal?	Get to work on time.	
What are they feeling? (emotions)	Hurried and potentially distracted thinking about home issues or distracted thinking about what they need to get done today.	
Who else is around? (social)	Others entering; more traffic than at other times during the day.	
Other notes about the context they are in	General business, lots of other conversations, people bringing breakfast, coffee, work bags, etc.	
How might they make mistakes or deliberately make insecure choices?	This is a prime time when someone might tailgate or allow someone to tailgate.	Business, hurriedness, distractedness, and social graces (holding the door for someone) conspire against an anti-tailgating policy.

Function	Answers	Additional Notes/ Comments/ Observations
Thoughts on Fogg Behavior Model (B=MAP) elements for encouraging secure behaviors?	<p>The behavior we want is for everyone to badge in.</p> <p>How are we <i>prompting</i>?</p> <p>Do they have the <i>ability</i>?</p> <p>Do they have the <i>motivation</i>?</p>	<p>If we aren't prompting, then add a prompt (see the next row).</p> <p>If the employee doesn't have the ability, then problem solve for the ability. Are their hands full? Find a way to solve for that.</p> <p>Are they not motivated? Staff and culture carriers may give the added social push merely by their presence.</p>
What program elements can we use to encourage and reinforce the behavior we want?	<p>We can add a <i>prompt</i> in the form of a sign at the door. Something like:</p> <p>"For the safety of our associates, we require that everyone badge in. One badge = One entry."</p>	<p>We may also be able to station security staff and culture carriers at the doors to encourage the right behavior in a non-threatening way. For instance, if someone's hands are full, staff can offer to hold the associate's bag so that they can fish out their badge and enter properly.</p>
How can we reward people who are doing the right thing or people who accept intervention?	<p>A warm, genuine "thank you" from staff at the door.</p> <p>Randomly awarding gift cards for helping encourage a safe work environment.</p>	<p>Positive social feedback.</p> <p>Variability of reward.</p>

(continued)

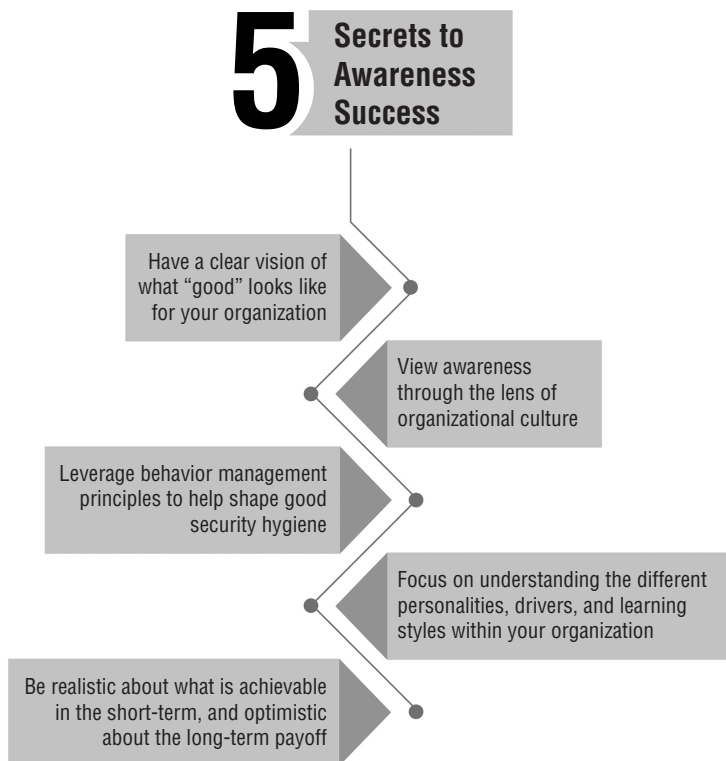


Figure 9.1: The five secrets to security awareness success

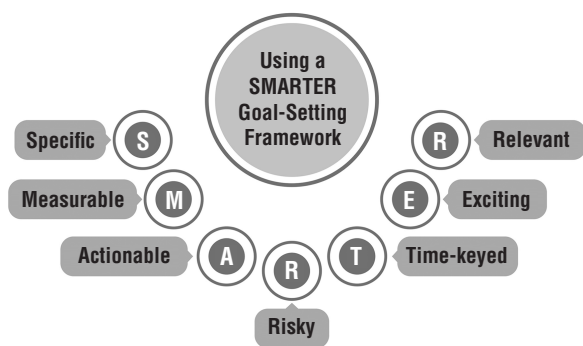


Figure 9.2: The SMARTER goal setting framework

Table 9.1: Brainstorming worksheet for obtaining stakeholder support

Stakeholder Name	Title and Department	Stakeholder's Primary Business Drivers and Needs	Potential Stakeholder Concerns, Questions, etc.	Departmental Benefits If the Program Is Successful	Benefits to Stakeholder If the Program Is Successful	Other Notes and Comments
Jane Doe	Head of _____	What is Jane's core business?	How might elements of your program feel like they work against Jane's core mission and values?	How might elements of your program make Jane's department look good?	How might elements of your program increase Jane's social currency?	Additional pre- or post-meeting thoughts go here.
		How is Jane's success measured?	Might elements of your program feel like they take focus from areas that Jane is measured against?	How might elements of your program help Jane's program perform better?	How might elements of your program help Jane's career?	
				How might elements of your program help Jane's department link to a greater organizational mission or support a broader goal?	Can this help Jane feel connected with a greater cause?	

Stakeholder Name	Title and Department	Stakeholder's Primary Business Drivers and Needs	Potential Stakeholder Concerns, Questions, etc.	Departmental Benefits If the Program Is Successful	Benefits to Stakeholder If the Program Is Successful	Other Notes and Comments
Mary H.	Head of Application Development	Needs developers to create solid code. On budget. On time.	May fear that training initiatives will take focus and time away from production activities and timelines.	Application developers will be more aware of the ways that attackers find and exploit vulnerabilities. They will be more conscientious as they develop applications and peer review code. As a result, there may be fewer security-related issues flagged during the Q&A cycle. There will also be fewer issues found during vulnerability scans. Fewer exploitable bugs make it into production.	The stakeholder will ultimately run a department filled with security-conscious coders who are known for developing reliable, secure code. Coders also see the stakeholder as someone who is enabling them to learn new skills and enhance their careers.	During meetings with Mary, we noticed that she feels like this is the "right thing to do"; but has a number of production timeline commitments. She wants to wait until Q3. Can we potentially help evangelize this training and the benefits to the CIO so that she feels greater executive support?

(continued)

Stakeholder Name	Title and Department	Stakeholder's Primary Business Drivers and Needs	Potential Stakeholder Concerns, Questions, etc.	Departmental Benefits If the Program Is Successful	Benefits to Stakeholder If the Program Is Successful	Other Notes and Comments
Aliana R.	EVP of Legal					
Mark J.	VP of Marketing					
Name	<u>Title of Department</u>					
Name	<u>Title of Department</u>					
Etc.						

(continued)

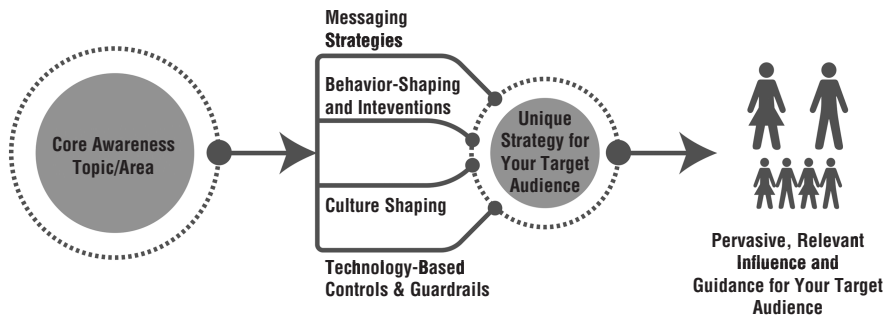


Figure 9.3: Security awareness topics should be planned and targeted in ways most relevant to each target segment.

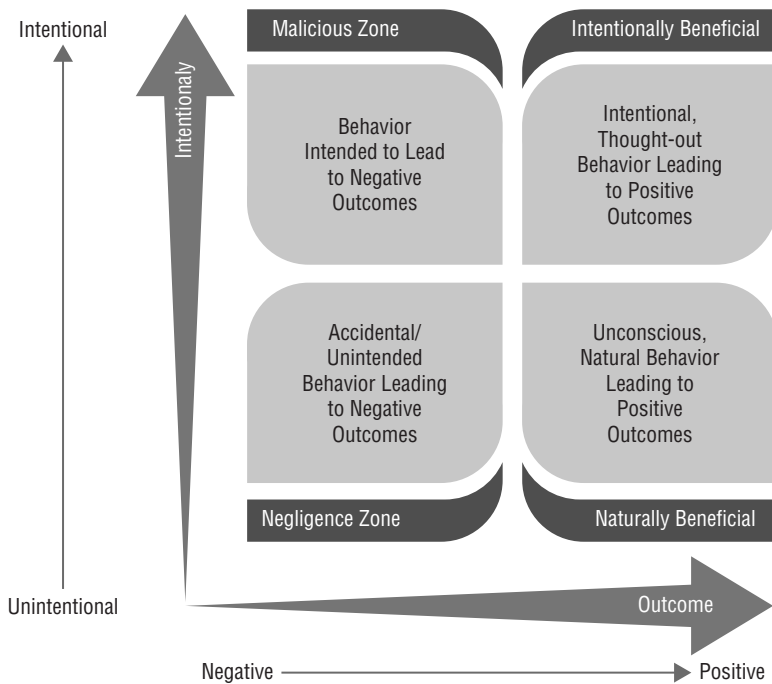


Figure 9.4: Security behavioral outcomes (reprise)

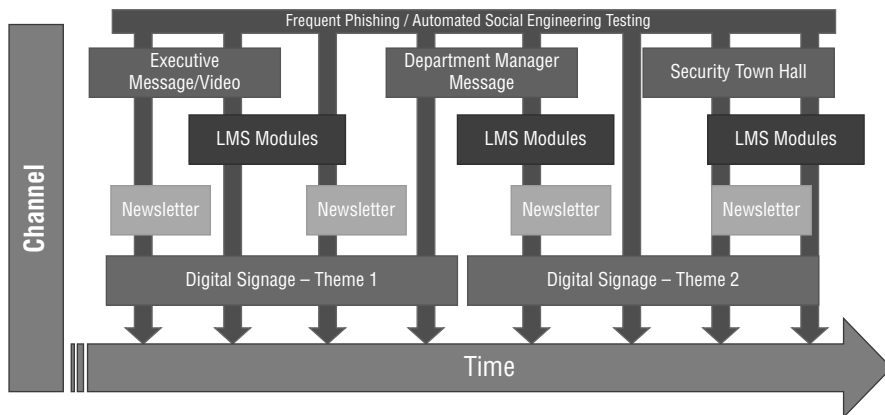


Figure 9.5: A robust security awareness program is a combination of multichannel marketing and attack simulation.