

TRAIN FOR THE NEXT THREAT: NOT THE LAST ONE:

A Cyber Intelligence
Primer for Security
Awareness Professionals to
Wage Culture Change





TABLE OF CONTENTS

1.0 What is Intelligence.....	4
1.1 What is Intelligence Analysis	4
1.2 What is Cyber Threat Intelligence	5
2.0 What is Human Risk.....	6
3.0 Security Awareness.....	7
3.1 Intelligence-Driven Security Awareness	8
4.0 Intelligence Research for Security Awareness	11
5.0 Intelligence Writing for Security Awareness.....	12
5.1 Sense of Style.....	13
5.2 Examples	14
5.2.1 Content Marketing (Brand, Voice, Tone)	14
5.2.2 Learning Management System (LMS)	15
5.2.3 Intelligence Alerts	16
5.3 Tips on Writing Well.....	17
6.0 Conclusion	18
References.....	19



BOTTOM LINE UP FRONT (BLUF):

The term security awareness literally means having a knowledge or perception about security threats past, present and future. The problem is that people aren't often aware of the very things that can harm them, their families and their organizations on the internet, especially the things that are relatively new. And for all the comfort that comes when users comply with a security policy, a lack of *awareness* means they are **training for the last threat, not the next one**.

Intelligence analysis, on the other hand, is a discipline made famous by the Central Intelligence Agency and other agencies across the globe to reduce uncertainty in decision-making by increasing awareness of potential threats. Intelligence analysts thrive upon new and relevant information by becoming observant storytellers, writing clearly and recommending action for politicians, military leaders and decision-makers to prepare for **the next threat, not the last one**. Bottom line: understanding the science behind intelligence and the mechanics of good writing can transform a lagging security awareness program into a leading one. It comes when security awareness program owners apply the hard-won innovations from the Intelligence Community (IC) to wage culture change at the highest level.

Key Findings for Security Awareness Professionals

- Intelligence Analysis in Context
- Cyber threat intelligence in context
- Human risk and bad design
- Intelligence-driven security awareness
- Intelligence research for security awareness
- Writing for security awareness

We hope you enjoy reading and welcome your feedback...

WRITTEN BY:

Graham J. Westbrook, Dir. of Intelligence & Content, Living Security

Graham (C|EH, Sec+) manages Living Security's threat intelligence program and content strategy for the Living Security (SaaS) platform. A writer with bylines at top cybersecurity firms, Graham holds a B.A. in Intelligence studies and Russian from Mercyhurst University and an M.S. in Criminal Justice and Forensic Psychology from Liberty University. Speaker at FIRST CTI 2020, ISF 2020 InfoSecWorld 2019, RMISC 2019, Toronto RiskSec 2017 & SANS Security Awareness Summit 2017.

Peter Chuzie, Cyber Intelligence Analyst, Living Security

Peter is a Cyber Intelligence Analyst at Living Security and OSCP candidate. A recent graduate of Mercyhurst University with a B.A. in Intelligence Studies and a B.S. in Cybersecurity, Peter has been published in the Journal of Intelligence and Cybersecurity, after a semester abroad at the University of Cambridge ("The Internet of Things Disruptive Evolution for Intelligence Collection.")



1.0 WHAT IS INTELLIGENCE

Throughout history, people in power have struggled to make sense of the world around them. The most obvious examples come from military disasters. On an expedition to Syracuse in 415 B.C., an entire Athenian army was slaughtered because leadership failed to secure the high ground. In 1857, General Custer sacrificed his entire platoon at the Battle of Little Bighorn by underestimating the opposition.

Good decisions, it seems, are hard to come by in a complex world; so leaders have always resorted to some form of information gathering to understand the enemy, weigh their options and make better decisions.

Modern examples come from the World Wars and into the Cold War, during which national security policymakers determined that an umbrella agency must be formed to combat what they considered the fog of war¹: the Office of Strategic Services (OSS). Here, modern intelligence analysis was born as a discipline to help people reduce uncertainty in decision-making².

To cut through this fog, intelligence analysts began to ask questions like, are our enemies playing chess or checkers? Are cultural differences significantly influencing their decision-making? Are the actions of governments practical and self-interested (*realpolitik*) or simply knee-jerk reactions to triggers? Their assessments became vital to the success of their leaders. After all, forewarned has always been forearmed.

Since then, intelligence analysts have influenced policy and strategy, from the overthrow of despotic leaders to the rise of the Arab Spring. The goal behind all goals has been this: to reduce uncertainty in decision-making³. After that, to mitigate bias, become an observant storyteller and make sense of a complicated world.

1.1 WHAT IS INTELLIGENCE ANALYSIS

Intelligence is a process and a product. Naturally, there's a lifecycle to boot which helps analysts think in the right direction. The gist is that analysts must collect raw data, isolate important pieces of information, analyze and enrich that information, produce intelligent insights and deliver the final product to a decision-maker. Simple, right?

Think of it like a funnel:

By collecting large amounts of data and using different analytical tools to narrow the body of actionable information, an analyst can produce insight. In the funnel, data processed becomes information, information analyzed becomes intelligence and intelligence applied becomes insight. Yes, there is a difference between data, information and intelligence. No, they are not the same.

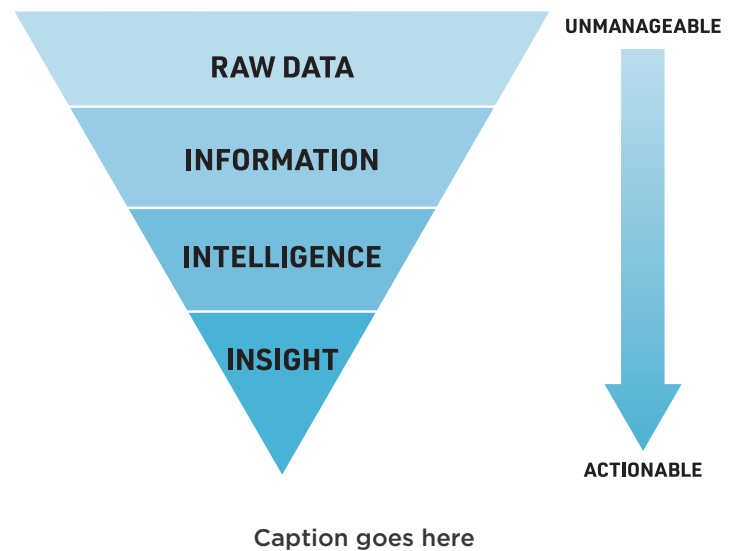
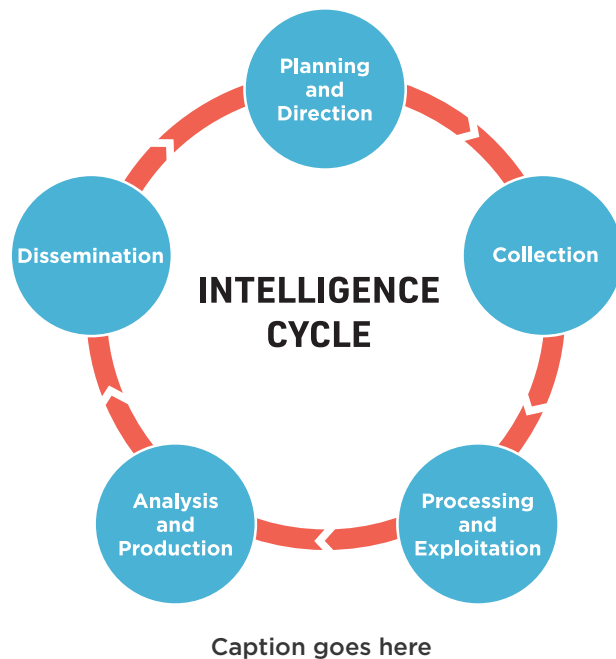
¹<https://medium.com/@markarenaau/being-a-cyber-threat-intelligence-analyst-and-operating-in-the-fog-of-uncertainty-adc7f397d11xe>

²<https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/PsychofIntelNew.pdf>

³Reducing uncertainty has now become more a discipline of assessing uncertainty in recent years: <https://sites.hks.harvard.edu/fs/rzeckhau/Assessing%20Uncertainty%20in%20Intelligence.pdf>



For help enriching, relating, validating, corroborating or contextualizing information, skip ahead to the “intelligence research for security awareness” section. Discovering new relationships between disparate pieces of information is just intelligence having fun, as Einstein would say. You can see there is a good reason to spin the intelligence cycle: to gain knowledge! to separate wheat from chaff! To separate noise⁴ from clarity!



1.2 WHAT IS CYBER THREAT INTELLIGENCE

Cyber threat intelligence (CTI) is traditional intelligence analysis all dressed up. It’s tactics are different, but it’s mission is the same: to reduce uncertainty for (security) decision-makers, namely the ones with wires sticking out of them. So if intelligence is knowledge, then threat intelligence is knowledge of the adversary and cyber threat intelligence is knowledge of the cyber adversary. See what I mean?

So to mitigate risk and better understand cyber threats against their organizations, Chief Information Security Officers (CISOs) hire cyber threat intelligence analysts to work their magic.

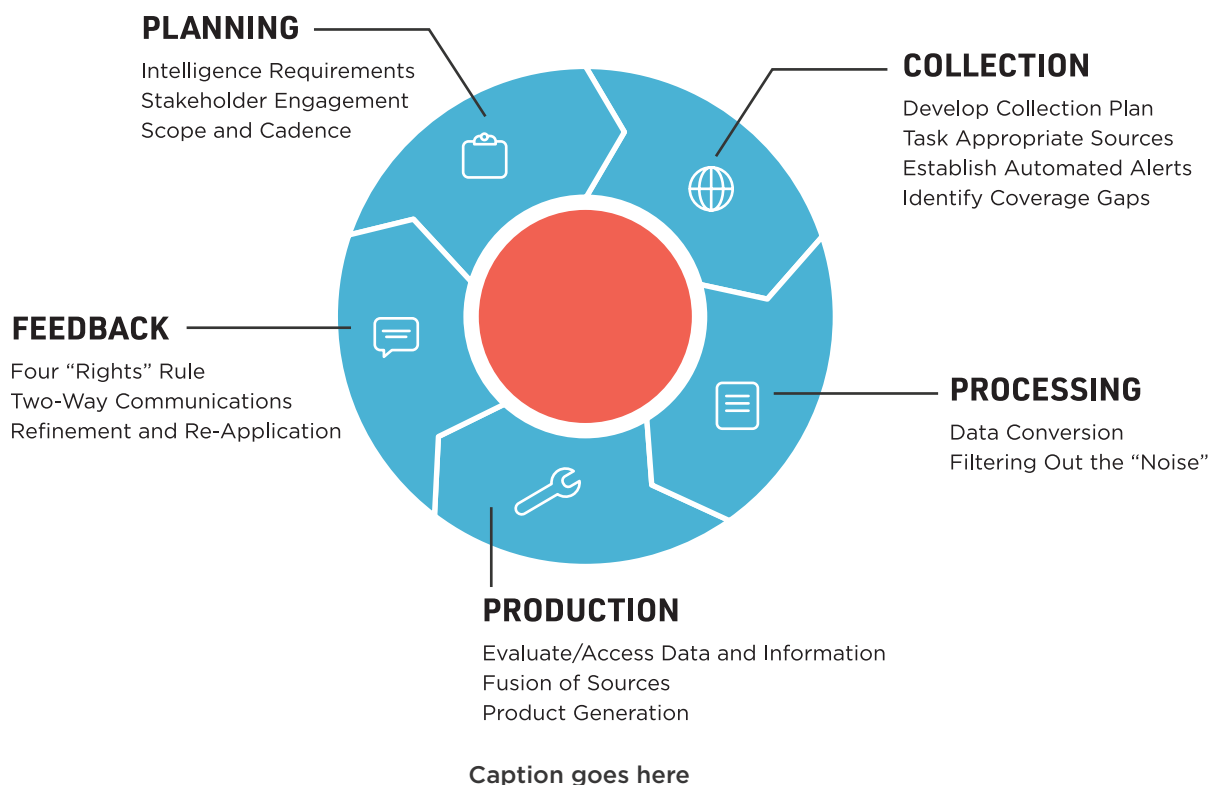
I could tell you about the Diamond model and how it helps analysts understand cyber intrusion from four different perspectives: adversary, capability, victim and infrastructure.⁵ I could tell you about the cyber kill chain, zero trust models and other great CTI resources⁶ that analysts use in their defense against the dark arts⁷. I could even tell you little secrets about an open-source intelligence (OSINT) forum on rocket chat⁸ for CTI professionals or a crowdsourced advanced persistent threat (APT) tracker on google docs⁹.

But you’re not asking. And I have other things to tell you about.

⁴ <https://hbr.org/2016/10/noise>

⁵ <http://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf>

⁶ (e.g. Shodan, PassiveRecon, JustMetadata, Google ‘Hacking,’ Harvester, SocMINT, Hunchly, FOCA, Burp Suite, etc.)



2.0 WHAT IS HUMAN RISK

In cybersecurity, “human risk” describes the danger or liability that humans introduce to an organization when interacting with technology. More broadly, human error is commonly defined as “any deviance from appropriate behavior,” so that’s the definition we’ll stick with.¹⁰

Depending on the report,¹¹ human error accounts for somewhere between 60-90% of security breaches across corporate America and around the world, resulting in huge financial losses.¹² So it is only natural that there is a lot of talk about how to reduce human error. The only problem is that everyone has their own interpretation of human risk. Some call it the ‘human factor.’ Others talk about updating the ‘human operating system.’ Maybe they kick and scream about your ‘people problem’ and all your ‘weakest links.’ A rose by any other name...

⁷ <https://i-sight.com/resources/101-osint-resources-for-investigators/>

⁸ Osint.team

⁹ https://docs.google.com/spreadsheets/d/1H9_xaxQHpwaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/edit#gid=1864660085

¹⁰ (even though what is “appropriate” is often different across organizations).

¹¹ The 2020 Verizon DBIR pointed out that 67% of breaches were caused by credential theft, errors and social attacks... a.k.a. facilitated by the human. We all know how to read between the lines. The only action type that is consistently increasing year-to-year in frequency is Error. People make mistakes, but this is one to watch out for! (“The fact that we now see Error becoming more apparent in other industries could mean we are getting better at admitting our mistakes rather than trying to simply sweep them under the rug.”)

¹² <https://enterprise.verizon.com/resources/reports/dbir/>



Let's just call them end users, as is common practice among security awareness program owners: humans with hands-on-keyboards that require instructional courses and tests to mitigate error.

No one understands end users and their mistakes better than you. But honestly? End users get a bad rap. Sometimes humans really are at fault and even compliant people under certain circumstances will break the rules, drive fast and take chances. Just ask someone late for a meeting.

But just because humans are often involved in enabling cybersecurity attacks does not mean they are always at fault. A "far greater percentage of accidents is the result of bad design."¹³ Technology was not designed with human error in mind nor with security baked-in.

With better design across technology and security awareness programs, people can become some of the best sensors and strongest links in the chain.

People have been criminally underutilized in the fight against cybercrime.

They have been ignored, misunderstood, blamed, shamed and virtually handicapped. This is a tragedy resulting from years of fear-based motivation, bad design, checkbox-security training, security theater and behavior management. The same culture you thought neglected security becomes a resilient, intelligent human firewall with well-designed training.

3.0 SECURITY AWARENESS

As many of you know, security awareness is more of an art than a science. It's not as easy as it sounds to just change user behavior or reduce human risk across the enterprise.

BUT HERE'S WHAT WE DO KNOW:

1. The **first step** in security awareness training is to establish a positive security culture designed for real people, not a police force. Making people aware of the risks associated with apathy - while coming alongside them, listening to their problems and encouraging them like a friend - will help the overall culture catch up with rapid technological advancements.
2. The **second step** is to create safe boundaries, like security awareness policy guidelines, from which to communicate effective training methods. Obviously, this isn't just good advice. It is mandatory, given regulations like NIST, SOX, HIPAA, FISMA, NERC/CIP and others, which require that companies take action to reduce risk among employees.¹⁴
3. The **third step** is rocking the boat! Namely, by immersing people in the challenges they will face in the real world. Instead of waiting for a data breach, you simulate one and see how people react. Rinse, repeat.¹⁵

¹³ <https://www.amazon.com/Design-Everyday-Things-Revised-Expanded/dp/0465050654>

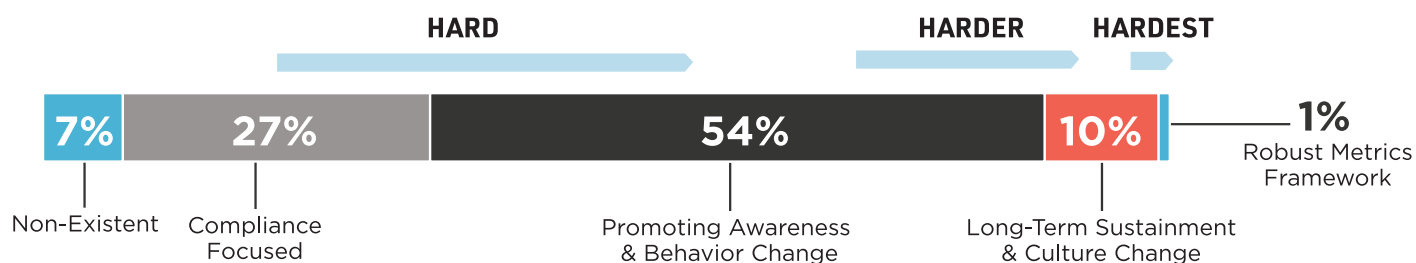
¹⁴ <https://livingsecurity.com/meets-compliance/>

¹⁵ Among the various training methods available on the market, one model has stood out for the numbers of engagement in the employees' learning process: gamification. A Brazilian writer, Renato Alves wrote a book called *Make Your Brain Work for You* in which he argues that the problem with training today is that it is increasingly linked to a significant over-dependence on technology without engaging natural, direct mechanisms for learning, like gamification, story and metaphor. It is in this context that experiences - like escape rooms! - reclaim natural mechanisms for learning in a way that other solutions cannot.



It all depends on the maturity of your security awareness program and what you are trying to accomplish. You can't manage what you can't measure, and you can't measure what you don't understand.

SECURITY AWARENESS PROGRAM MATURITY SCALE



Caption goes here

Security awareness program owners typically implement training every October (also known as Cyber Security Awareness Month (CSAM)) as an opportunity to celebrate security, spread cyber hygiene and energize positive culture change across the enterprise. But to keep pace with threats, and not hope that cyber criminals look the other way until October, you need intelligence-driven security awareness training to be **part of your cultural fabric all year long**.

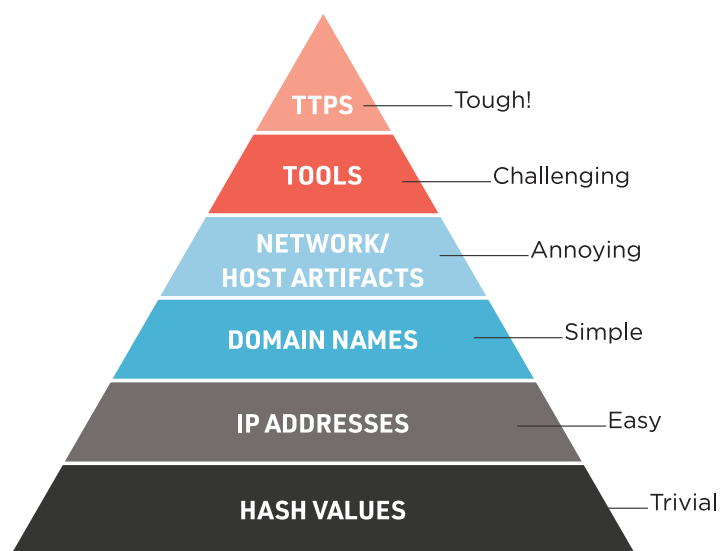
3.1 INTELLIGENCE-DRIVEN SECURITY AWARENESS

“You don’t have a malware problem. You have an adversary problem.”¹⁶ From the perspective of a security awareness program owner, it makes a difference whether you believe ‘malware targets organizations’ or ‘people target people.’ A ‘malware’ view of the world is in bits and bytes, ones and zeroes. Even if that malware is driven by computer machine-learning, it cannot adapt and think like a human being.

But when ‘people target people,’ something else happens. Phishing emails look and feel like they come from your coworker down the hall. Vishing calls sound like they’re really from Microsoft tech support. And ransomware provides better customer service than your bank.

Threat intelligence analysts understand this: they do not stop investigation or analysis at an IP address or a malware signature. In fact, they have a token chart for doing quite the opposite, called the *pyramid of pain...* (right)

Up top you can see that an adversary’s tactics, techniques and procedures (TTPs) are the most challenging to identify, but become the most effective methods of tracking a (human) threat



Caption goes here

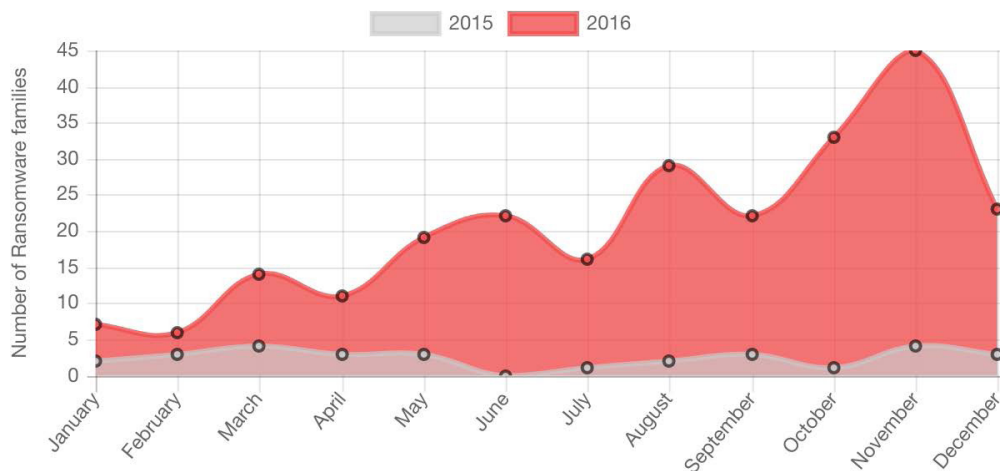
16 CrowdStrike VP of Intelligence, Adam Myers



once found. As the threat landscape shifts and evolves, intelligence traces its grooves and fissures. Not just once a year, but everyday!

Let's rewind back a few years for the sake of example. Without intelligence, you might have believed that 2016 would trend very much like 2015 in terms of the quantity and quality of ransomware families. Evaluating only your assumptions about the previous year, your predictions would project linear growth.

But when ransomware families grew seven-fold the following year, your security team would have been in reaction-mode and your users unprepared for the fight.



Caption goes here

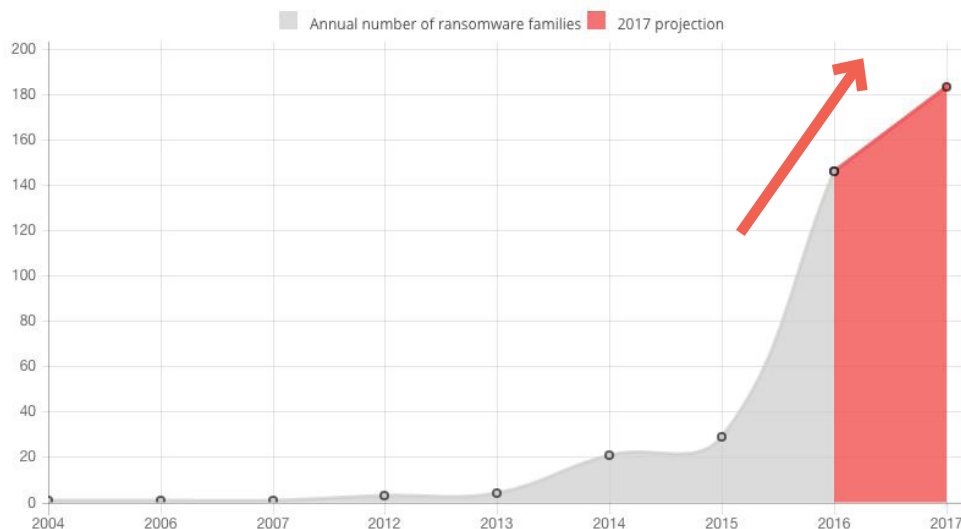
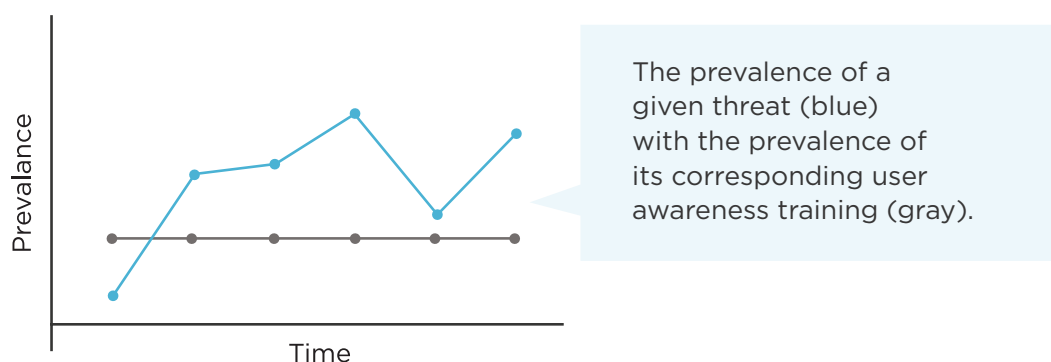


Figure 1: Annual number of ransomware families, including 2017 projection

Caption goes here



Here's the point. In its most basic form, the current disconnect between threats and user awareness feels something like this:



Caption goes here

In blue, you can see the prevalence of a given threat over time; in gray, the frequency of user awareness training for that given threat over the same period of time. This is, of course, an oversimplified model. But in large part, you are likely to have experienced this phenomenon in the form of the same tired security awareness advice you may hear in the workplace...

“Think before you click”

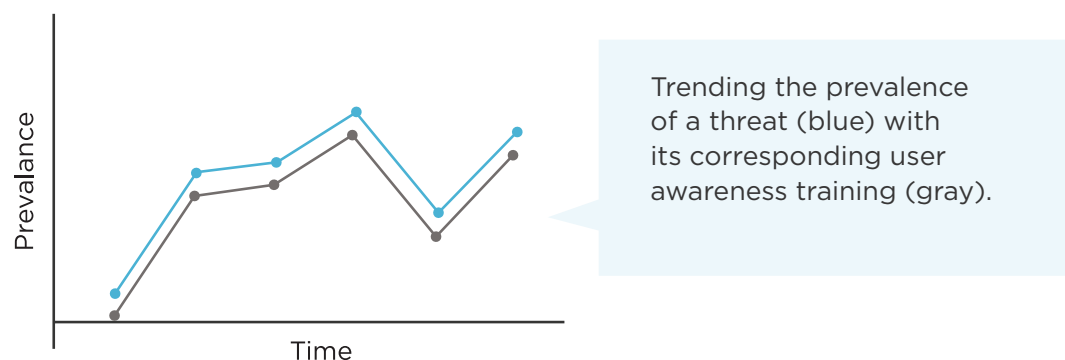
“Make strong passwords”

“Watch out for phishy links”

... when users really need to adapt to current and emerging threats by way of intelligence-driven security content. For example:

- “The Intelligence Team has seen an uptick in CEO-fraud emails against the finance department and the c-suite;”
- “A decrease in Nigerian prince scams means that grammatical errors are less indicative of phishing than things like a suspicious sender address;”
- “COVID-themed donation requests may pique your curiosity, but they are unlikely to be legitimate. If you would like to donate, make sure to browse to the (known-good) website directly.”

The return on investment (ROI) for this training is enormous, and the correlation of this type of threat-to-awareness-training looks something more like this:



Caption goes here



If you take away one thing, it's that

high impact training content sits dead-center at the intersection of threat intelligence and security awareness.

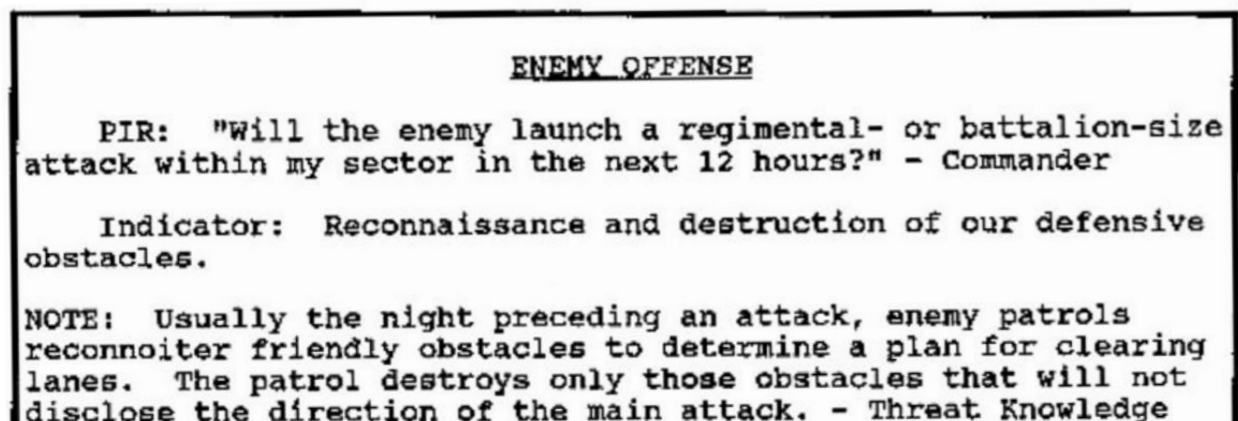
There, intelligence becomes the driver for organizations to keep pace with (trend) – and, at times, outpace (predict) – unique threats to the integrity of their mission.

This is intelligence-driven security awareness.

4.0 INTELLIGENCE RESEARCH FOR SECURITY AWARENESS

OK, now that you're officially up to speed, let's talk about how to level-up your training with intelligence. The most effective way to start is by asking the right questions. Otherwise you'll waste your time barking up the wrong tree.

Classic intelligence practitioners and military intelligence analysts do this by using priority intelligence requirements, or PIRs.



Caption goes here

GOOD AND BAD PIRs:



What emerging threats or vulnerabilities from the last 90 days must general end users understand?



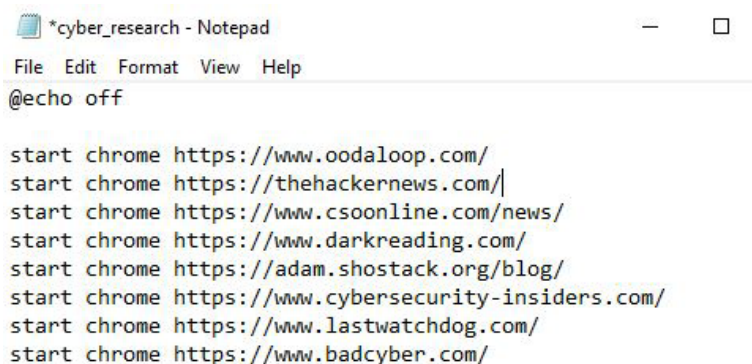
What are some new threats and vulnerabilities?

See how this question alone could help or hinder the overall product depending on how it was asked? Try induction or deduction, whichever you prefer, to start thinking in the right direction.



Once you have a question in mind, you want to identify reliable sources that can start answering it. This will give you clear direction and help you from running around in circles. It also helps you isolate important indicators, events and outcomes. The downside to this step is that it can be very manual. But it doesn't have to be!

For example, once you find reliable sources, you can automate them with a simple batch script file you can click every morning while sipping your coffee.



```
*cyber_research - Notepad
File Edit Format View Help
@echo off

start chrome https://www.oodaloop.com/
start chrome https://thehackernews.com/
start chrome https://www.csoonline.com/news/
start chrome https://www.darkreading.com/
start chrome https://adam.shostack.org/blog/
start chrome https://www.cybersecurity-insiders.com/
start chrome https://www.lastwatchdog.com/
start chrome https://www.badcyber.com/
```

Caption goes here

If you don't even want to click, consider a powershell script that will run the query for you at a set time. Consistency with collection will help you recognize patterns over time and become aware of your gaps.

That said, there are some tasks during the research phase, however, that are too discrete even for a batch file. Like collecting IP addresses, domain names, hashes. Instead of hiring an army of analysts, there are tools out there that will make your life easy. One tool, called Crowdscape, is a free resource that automatically scrapes a web page for such discrete¹⁷ indicators and outputs a file, just like that! At Living Security, we've created a script that utilizes APIs such as DNStwist, GreyNoise, Securitytrails, Quttera and RiskIQ to enrich, relate, validate, corroborate and contextualize the collected information so we can better act on it.

Bottom line: the intelligence community is your friend. With a little nudge, you can build off the shoulders of giants. Good questions and good research lay the groundwork for actionable intelligence that provides real value for training.

¹⁷ <https://chrome.google.com/webstore/detail/crowdscape/jjplaeklnlddpkbbdbnogmppffokemey?hl=en>



5.0 INTELLIGENCE WRITING FOR SECURITY AWARENESS

Now comes the scary part. How do you communicate these newfound insights with Janet from IT? Short answer: empathy.

Think back to when you first got into security. Didn't everything sound so technobabble? That's how users interpret a lot of updates from security. Either that or they're bored numb with the same advice. If you want to change the culture, you have to remember what it felt like.

Let's take fitness for example. You may know the feeling of trying to implement a new diet or begin a new fitness regimen only to fall short of the goal. Like with New Year's resolutions, you are momentarily motivated then repeatedly frustrated. In hindsight, you may ask yourself: "was it really life-changing when my trainer said, 'stop eating junk food?' or 'go run a mile?'" The short answer is of course not.

When you look at the individuals who change their lives to lead more healthy lifestyles, they collectively tell you that when they were inspired to live sustainably well, they started to see a much bigger picture on the pathway to change. Instead of doing one behavior at a time until they were apathetic or regularly frustrated, they were inspired to subscribe to a whole new set of behaviors and plan each day full of small, consistent, repeatable habits. Instead of saying "I just need to run more," they begin to say, "I'm the kind of person that loves to be healthy."

This is a groundbreaking insight when applied to security awareness.

For years, people have been told "think before you click" and "set stronger passwords" without understanding the bigger picture. They ask themselves: Why try when I'm up against a super cyber criminal? How am I even a risk in the grand scheme? Why does this behavior even help anyway? Or they search online for quick answers to cope with security stress without context, background or meaning. Is it any wonder repeated cybersecurity frustration sets in as the cultural norm?

The point is, You must remember what the problem feels like to end users in order to help write in a way that changes their perspective. You must become an observant storyteller to make any impact at all. You must turn tradecraft knowledge into the kind of story your audience will appreciate and understand. Intelligence must drive everything you do.

By writing in a way that helps people train for the next threat, not the last one, people begin to understand risk personally and over time create a new sort of security perimeter (e.g. HUMINT). From a business sense, this reduces behavioral risk, eliminates blind-spots and influences culture change. Intelligence writing for security awareness is a game-changer.

But to change the game, it's important that you have some serious swag.



5.1 SENSE OF STYLE

In the words of Steven Pinker, “what is style, after all, but the effective use of words to engage the human mind?”¹⁸

A sense of style, like a sense of humor, can refer to a way of being; so, how about you puff out your chest, put on your cape and step into a world needing saved from bad writing?!

What if I told you it was possible to write so well that people thanked YOU for not wasting their precious time on earth. To a literate reader, “an arresting metaphor, a witty aside, an elegant turn of phrase are among life’s greatest pleasures.”¹⁹ And they aren’t just eye-candy, either; they are like Claritin for the brain.

This is called classic style, and refers to a way of writing which treats your reader like someone who can think. The catch is that you must be realistic, see the world clearly and present your ideas with disinterested honesty. This doesn’t mean you can’t be playful OR that you need to be abrupt or short with your words. It means that you can be seen, heard and understood right where you are. Remember that! Writing in classic style is not a straight-jacket! It can actually take “whatever form and length you need to present your interesting truth.”²⁰

The early bird gets the worm but the second mouse gets the cheese

... is a classic example of classic style. And according to Pinker, there are at least three reasons why it matters to write this way.

FIRST, that you spare your readers from difficult-to-read, bricks of text.

SECOND, that you earn the readers’ trust.

THIRD, that you add beauty to the world. So let’s give it a try.

5.2 EXAMPLES

5.2.1 CONTENT MARKETING (BRAND, VOICE, TONE)

Let’s imagine we are writing a blog post on phishing that appeals to general end-users — ya know, the common, everyday folk who just happen to be employees.

First, you want to find your ‘voice.’ Your voice is your company’s personality. It’s who you are, what you stand for and how you relate to people. Think of VOICE as your overall strategy/brand for communicating (e.g. empathetic, respectful, human, honest, positive).

Then you want to establish your ‘tone.’ Your tone is the tactics and methodologies you use to actually convey your voice. It’s how you speak, it’s the language you use. TONE is choosing verbiage that embodies your VOICE (e.g. clear, helpful, simple, relevant, consistent).

¹⁸ Pinker, Sense of Style.

¹⁹ Ibid.

²⁰ Ibid.



Figure: SLIDING SCALE - Formality of tone can be adjusted slightly depending upon the channel for which you're writing, but the same basic voice + tone guidelines should apply.

We're humans, writing for humans about human experiences. Always speak to people. Write as if you are talking to that person one-on-one. Your audience is not a faceless entity; they are a group of people who actually care.

Once you start writing, you want to actually start with a statement (never a boring-a\$\$ question!) which draws them in, excites them and piques their interest:

PART 1

"In firearms training, every safety instructor is a curmudgeon for a reason..."

Now, already the brain is automatically asking... 'lol, why is every safety instructor a curmudgeon?' This is called the hook or the lede. And it's almost always a powerful statement that has teeth. It takes some creativity and practice, but it's worth getting right.

Next, we want to add context.

PART 2

"She will tell you a version of this sage piece of advice: keep your finger off the trigger at all times unless you are absolutely intent on firing your weapon. (Oh, and if you are in rural Oklahoma, the advice is simple. Keep your booger hook off the bang switch! - Yes, this is based on a true story)."

I hear you. Setting the stage to talk about phishing and email in the context of a weapon may seem overblown. But the reality is that the criminal tactic of phishing is used to successfully cripple organizations everyday. And in this case, we find that the commentary on gun safety actually works to keep the reader's attention. So we are tactfully drawing the reader into a metaphor, while the (optional) parenthetical provides a plot-thickening anecdote.

Finally, we hit them with the lesson...

PART 3

*All fun aside, this reminds me of the dangerous realities of phishing emails and the need to keep from clicking on links unless you are absolutely intent on launching a URL."*²¹

²¹ The Firearm Metaphor blog - <https://livingsecurity.com/blog/Is-phishing-awareness-training/>



Bam. All of the sudden, this new piece of training content feels significant against the backdrop we created, likely because we've set the stage for a real show. We weren't just chewing the scenery. We captured the reader's mind and emotions and then made space for the reader to learn.

That is good writing. There is no room for fluff. The net economic value of an unread, unshared blog is zero.

5.2.2 LEARNING MANAGEMENT

SYSTEM (LMS)

Let's say now we've switched gears and now we're writing content for your learning management system (LMS) platform, particularly a set of questions, answers and training nudges for a module about ransomware. Here is a fun one:

Q: Ransomware is...

Answer 1: A coupon that redeems for cash value anywhere

Answer 2: A nasty virus that locks computer files and demands payment to unlock them

Answer 3: A nasty sinus illness that happens every tax season

Answer 4: A nasty virus that spams you with money orders when you are unaware

The question is simple, the answers are witty and the knowledge check is useful to a security awareness program owner. So let's hit them with some great training nudges!

Nudge 1 (incorrect): Not so fast! Ransomware is actually a nasty virus that locks computer files and demands payment to unlock them.

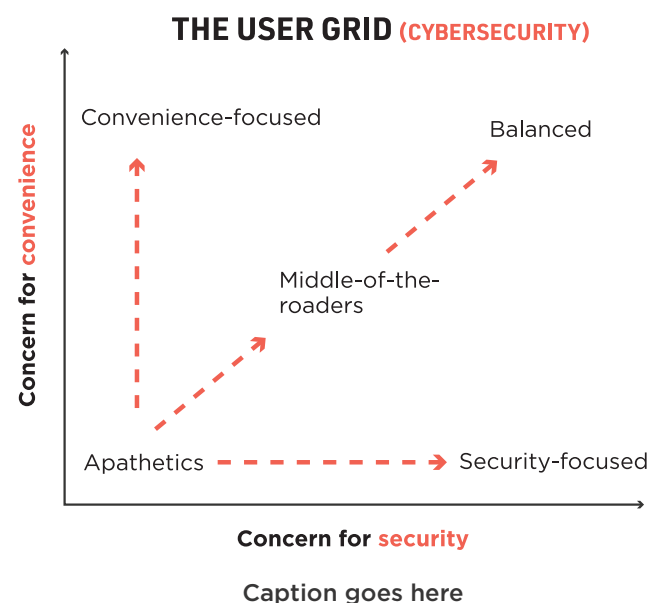
Nudge 2 (correct): Easy, right?! Well, it's just as easy to click on a bad link via email or online and catch this virus. Watch out for unexpected urgency or pressure to interact!

Nudge 3 (incorrect): Hilarious! Ransomware is actually a nasty virus that locks computer files and demands payment to unlock them.

Nudge 4 (incorrect): Sort of! Ransomware is actually a nasty virus that locks computer files and demands payment to unlock them.

All of these are great, specific options that are easy to write, fun for the user to answer and meaningful for the person consuming the results.

Try to be balanced with your training nudges. There is a sweet spot somewhere around the intersection of security and convenience.

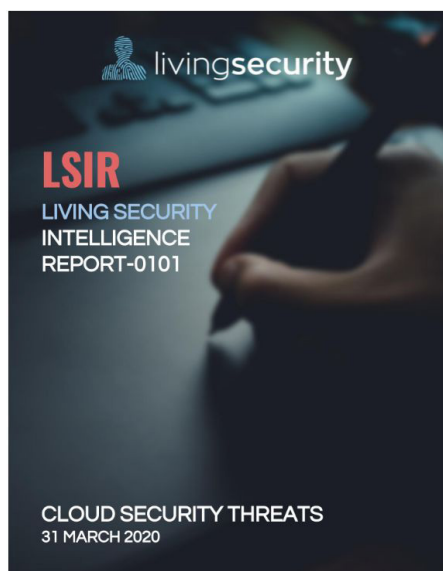




5.2.3 INTELLIGENCE ALERTS

From priority intelligence requirements (PIRs) to final deliverables, you want to be as clear and precise as possible. Don't forget to use the STAAR mnemonic to remember this: you want to produce something Specific, Timely, Accurate, Actionable and Relevant.

Want some homework? Choose a topic, write a measurable PIR, find a news article, write a quick prompt for end users and then give it to a stranger. Do they understand it? Do they need more information? And tweak from there.



<p>LSIR-0101</p> <h3>Cloud Service Introduction</h3> <p>The ability to obtain a seemingly unlimited amount of computer resources and storage can be achieved using cloud services. Cloud services are any service made available to an organization or user on demand over the internet from a cloud computing or storage provider. This allows users to access resources or their information anywhere due to the service being run on the service provider's hardware and accessible over the internet. Also, it greatly reduces the organization or user's responsibility for maintenance and purchasing of hardware because it is all controlled by the service provider. Cloud services increase efficiency and accessibility of work and information, but it also produces security threats that are vital to understand in order to mitigate them.</p> <h3>Cloud Security Threat</h3> <p>As more companies and individuals increase their use of cloud services it inevitably becomes a gold mine for cyber criminals. Organizations often utilize cloud services to store confidential data, personally identifiable information, proprietary products, among other important information. When using public cloud services this information does not always have the same firewalls and security checks a private network or private cloud provides. However, the convenience of not needing to purchase and maintain the hardware that is needed to store massive amounts of information and being able to access it anywhere outweighs the risk involved for most users. Therefore, in order to take advantage of cloud services it is vital to understand the threats and risks in order to better protect from becoming a victim of an attack.</p> <p>Data Breach:</p> <p>A security issue where sensitive information is released, stolen, or accessed by an unauthorized individual. This is a break in the confidentiality of the information which can result in loss of intellectual property, loss of trust or reputation, monetary loss, market value decrease, legal liabilities, as well as incident response costs. It is necessary organizations take precautions such as policies that enforce complex passwords and make users setup multifactor authentication (MFA) so that issues, such as these, are less likely to occur.</p> <p>Misconfiguration and Inadequate Change Control:</p> <p>This occurs when computer systems are set up incorrectly which leaves them vulnerable to malicious activity. These misconfigurations include unsecured data storage, excessive permissions, default credentials, default configuration setting, and the standard security controls being disabled. Misconfiguration is the leading cause of data breaches which leads to confidentiality integrity, and</p>	<p>LSIR-0101</p> <p>potentially the availability of information being compromised.</p> <p>Lack of Cloud Security and Architecture and Strategy:</p> <p>Organizations are moving their Information Technology (IT) infrastructure to public cloud services. The biggest challenge that comes with this is properly implementing security architectures to withstand cyberattacks. Organizations are more inclined to choose speed of the migration over security which leaves the organization vulnerable to attacks during and after the migration process. Therefore, it is necessary for organizations to develop a robust security strategy and implement a security infrastructure in order to build a foundation to conduct themselves securely in the cloud.</p> <p>Insufficient Identity, Credential, Access and Key Management:</p> <p>Cloud services introduce changes to the traditional practices of identity access management (IAM). The cloud service user is required to manage a large portion of their IAM in the attempt to increase security. It is vital to ensure adequate protection of credentials, regular automated rotations of cryptographic keys and certificates, a scalable IAM system for users, use of MFA, and a password policy that ensures strong passwords.</p> <p>Account Hijacking:</p> <p>This is the practice of gaining access to highly privileged accounts by cyber criminals. The accounts at the highest risk are cloud service accounts or subscriptions because they are accessible online to anyone with the correct privileges or credentials. These can fall victim to phishing attacks, exploitation of cloud-based systems, and stolen credentials. The impact of account hijacking can result in a breach in confidentiality, integrity, and availability of information and resources.</p> <p>Insider Threat:</p> <p>Insider negligence or malicious intent is responsible for 50 percent of security breaches. 64 percent of these breaches are due to employee negligence, 23 percent are related to criminal intent, and 13 percent are due to credential theft. This is a threat that is difficult to mitigate but requires educating employees about the prevention systems in place, such as logs of the system, and common scenarios of negligence and credential theft. This will help deter employees from misusing their privileges because they know their actions are recorded as well as inform others on dangerous scenarios where they are putting the company at risk.</p>
--	---

Caption goes here



5.3 TIPS ON WRITING WELL

ALWAYS BLUF

- Meaning, Keep the bottom-line-up-front. Your readers will thank you for not making them dig.

OMIT NEEDLESS WORDS – helps for your sake and the readers'

- E.g. Omit the meaningless... “due to the fact that” when you could just say “because”
- E.g. Omit the obvious... “problematic”
- E.g. Omit unnecessary adjectives... “Very,” “Awesome,” etc.

USE ACTIVE VOICE – Much easier to write and read.

- E.g. “She did this” versus “This was done by her.”

BE SOLUTION-ORIENTED

Everything you write should be directly related to solving end user problems with security and technology. If you're not writing directly about a solving a customer's problem, you probably shouldn't write it. You're in the solutions business and everything you create should reflect that. You should always write with **EMPATHY** towards a customer's pain-points. Use phrases like:

We understand • *It's not always easy* • *We can help*
There is an answer • *Here's a real-world example* • *You're not alone*

GOOD! ON-BRAND

Phishing is a problem we all deal with as employers. And we understand that it's not always easy to implement a program that can really move the needle as far as risk reduction. But there are things you can do. Take Kevin, for example. Kevin ran the Security Awareness program for a medium-sized real estate company. But things got real when his executive assistant accepted a meeting invite...

TAKEAWAYS: This is on-brand because we spoke in a friendly, casual tone; we spoke from a position of understanding the problem and it's difficulties; we gave a human example, not a vague stat; we offered a solution (or the possibility of one later in the text).

NOT-SO- GOOD! OFF-BRAND

Phishing is the number one cause of financial loss through cybercrime. Studies show that phishing costs companies \$300 million a year in damages. In the last year alone, more than 500 small-to-medium sized businesses reported a loss due to cybercrime. Empirical data and peer-reviewed white papers from thought leaders...

TAKEAWAYS: This is off-brand because we never spoke directly to the reader, we spoke at them; we established a problem but never offered a solution or the hope of a solution later (lost them in the first paragraph); we spoke in generalities and not to the human toll; we lumped everyone together and didn't focus on our customer...

BE HUMAN

We're humans, writing for humans, about human experiences. So we should speak like humans. Always speak to people. Write as if you are talking to that person one-on-one. We are not a faceless entity; we are a group of people who actually care.

- Write in ACTIVE voice (you, we, us, do)
- Ask questions
- Create dialogue in your writing
- Write about people having experiences



GOOD! ON-BRAND

You remember that guy that used to hang around the finance cubicle? Didn't you find it odd that he was always asking questions that seemed really precise and irrelevant to his job? I mean, why does someone from social media need the Q4 supply chain forecasts? Your team was right to report those questions as red flags. And Pete from security thought so too. The truth is, insider threats look like everyone else...

TAKEAWAYS: This is on-brand because we talked about a real-world, relatable event; we spoke to the reader; we spoke as if we knew the people involved (Pete, etc.); we created a human example that could apply at any company.

NOT-SO- GOOD! OFF-BRAND

Insider threats are a severe hazard to companies far and wide. While mitigation is a healthy first step, identification and abatement are the ultimate goal. From a risk standpoint, insider threats are the most damaging since the first step of access has already been achieved. Therefore, red-flag behavior warnings are paramount...

TAKEAWAYS: This is off-brand because we spoke of companies as entities, not groups of people; we used a passive voice and never spoke to the reader; we never mentioned any human interaction; we spoke of insider threats as things, not humans with intent.

BE CLEAR AND KEEP IT SIMPLE

I'm smart, you're smart, the reader is smart. Heck, we're all smart. So why do you feel the need to prove it with big words? Or too many words. Never confuse word count with quality. The more cerebral you try to be, the more likely you're alienating 99% of readers.

- Be concise! Shorter is better
- Edit mercilessly. See if you can cut your first draft in half. Or by 75%
- FOCUS! Never try to say everything in one piece of content

GOOD! ON-BRAND

Monday morning in the breakroom and everyone is huddled around the new toy: a coffee machine that talks and remembers your order. And your first thought? Time to release that training on IoT, or Internet-of-Things. IoT security is basically dealing with all these interconnected devices that seem to be everywhere in our daily lives. Alexas, refrigerators, smart doorbells, Roombas...you get the picture.

TAKEAWAYS: This is on-brand because we created a relatable situation; we didn't try to over-explain the concept; we used simple, clean language; we got to the point quickly; we created a scenario and brought up a solution in the 3rd sentence.

NOT-SO- GOOD! OFF-BRAND

IoT, or Internet of Things, is a terminology dictating all manner of everyday devices connected through corporate proxies to the internet. Infant-care monitors, visual security systems, smart home appliances and environmental data collectors are just a few of the mechanisms that exemplify this category of equipment. When delineating use-case risk associated with...

TAKEAWAYS: This is off-brand because we spoke redundantly, simply to squeeze in large words; we never spoke to a situation or solution; could've said the same thing in 80% less copy; we never spoke to the reader.



BE CASUAL + FRIENDLY

Write like you're speaking to a trusted friend. People listen to brands they like and can relate to. Speak the way you want to be spoken to. We're not robots and should never speak that way. Some tips:

- Don't be afraid of contractions. Use *it's*, *you're*, *can't*, *won't* instead of *it is*, *you are*, *cannot*, *will not*
- Try telling your story out loud or to someone else. Use that conversation as the tone for your copy.
- Don't try to create a book or tech manual. Try to create a story or conversation.

GOOD! ON-BRAND

Wow, owning a security awareness program has its days. I mean, I'm not gonna pretend it's all rainbows and butterflies, but sometimes it all just comes together. Maybe you've had the same experience; when you see it all just 'click' in someone's eyes. That high-five session after the training was your first clue. Ditching that Powerpoint and VHS from 1997 was your idea. And now the team is using words like *experience* and *real world*...

TAKEAWAYS: This is on-brand because it feels like a story or conversation; we used conversational language; we turned SA program ownership into a positive thing; we're telling our brand/product story

NOT-SO- GOOD! OFF-BRAND

Outdated and ineffective training materials are a hallmark of almost every security awareness program. And security awareness program owners have the unenviable task of cost vs. risk in introducing new methodologies to their ecosystem. By assessing behavior as it relates to culture, program owners can correlate...

TAKEAWAYS: This is off-brand because we immediately make our clients' job sound miserable; we write in *brochure-speak*, not conversation; we're not speaking to the reader; NOTE: a less formal version of this may be suitable for sales materials or white papers.

STAY POSITIVE + RELEVANT

You shouldn't be the "scare-tactic" organization. You inform users and give good, human advice. It's a tried and true tactic: create a boogeyman, scare the heck out of people, and place the blame in a place where you're the only solution. Might work in politics, but that ain't us.

- Speak from a place of positivity; not fear
- Be honest about emerging threats, but give good advice
- Don't harp on the same issues over and over. Be relevant and timely.



GOOD! ON-BRAND

Maybe you've heard of contact tracing. Or maybe you haven't. Either way, it seems to rile people up on both sides of the argument. And we can definitely see why. First, let's talk about what it is, and then we'll see if we can give you some unbiased advice without planting a flag in either camp. Since we're all in it together, let's figure it out together. Contact tracing is...

TAKEAWAYS: This is on-brand because we're speaking directly to the reader; we're discussing a relevant subject; we're being rational and not reactional; we're offering to give advice from an unbiased viewpoint; we're not immediately screaming that you should be afraid

NOT-SO- GOOD! OFF-BRAND

By now you've heard of contact tracing - governments and corporations placing pseudo-tracking software on your phone to mine data regarding COVID-19 hot spots and transmission. But where is it all heading? Are we destined to become a police state where all of our movements are being watched? Or can we really trust those in power.

TAKEAWAYS: This is off-brand because we are obviously trying to engage them through fear/ we're trying to scare them into our viewpoint; we're ignoring the beneficial side of argument; we're violating trust by practicing subtle, yet obvious manipulation.

6.0 CONCLUSION

If you've read this far, you are likely a change agent who believes in a better security culture and better outcomes in security awareness. Deep in your bones you feel that training lacks relevance and that each new threat is like a gut-punch to the old way of training.

The only way you can fight is to be aware. And that means taking every new lesson you learn from the world of cyber crime and communicating it to real people.

Don't waste your words! Train for the next threat, not the last one. Your actions may change your culture for decades to come...



REFERENCES

<https://www.digitalshadows.com/blog-and-research/5-takeaways-from-the-building-a-strategic-threat-intelligence-program-webinar/>

<https://www.nytimes.com/2018/04/28/opinion/sunday/the-end-of-intelligence.html>

https://www.linkedin.com/pulse/disinformation-changing-way-we-view-world-meredith-wilson/?lipi=urn%3Ali%3Apage%3Ad_flagship3_profile_view_base_post_details%3B3xohlwp0TtuoEwkiWtk84Q%3D%3D

https://www.linkedin.com/pulse/geopolitics-cyber-nexus-meredith-wilson/?lipi=urn%3Ali%3Apage%3Ad_flagship3_profile_view_base_post_details%3B3xohlwp0TtuoEwkiWtk84Q%3D%3D

https://www.linkedin.com/pulse/what-makes-great-intelligence-organization-meredith-wilson/?lipi=urn%3Ali%3Apage%3Ad_flagship3_profile_view_base_post_details%3B3xohlwp0TtuoEwkiWtk84Q%3D%3D

https://www.linkedin.com/pulse/seven-deadly-sins-private-sector-intelligence-meredith-wilson/?lipi=urn%3Ali%3Apage%3Ad_flagship3_profile_view_base_post_details%3B3xohlwp0TtuoEwkiWtk84Q%3D%3D

https://www.linkedin.com/pulse/7-habits-highly-effective-intelligence-teams-meredith-wilson/?lipi=urn%3Ali%3Apage%3Ad_flagship3_profile_view_base_post_details%3B3xohlwp0TtuoEwkiWtk84Q%3D%3D

<https://www.csoonline.com/article/3266610/data-protection/how-to-create-a-gold-standard-intelligence-program.html>

<https://www.recordedfuture.com/smart-threat-intelligence-analysts/>

<https://isc.sans.edu/forums/diary/Defining+Threat+Intelligence+Requirements/21519/>

<https://www.recordedfuture.com/threat-intelligence-challenges/>

<https://swannysec.net/2016/01/14/starting-small-with-threat-intelligence-pt-1.html>

<https://swannysec.net/2016/02/05/starting-small-with-threat-intel-pt-2.html>

<https://sroberts.github.io/2016/03/30/cti-squad-goals-intro-to-requirements/>

<https://www.linkedin.com/pulse/cyber-threat-intelligence-q-n-aka-ctijam-andreas-sfakianakis>

<https://www.digitalshadows.com/blog-and-research/5-takeaways-from-the-building-a-strategic-threat-intelligence-program-webinar/>

<http://www.cyintanalysis.com/an-important-internal-intelligence-source-to-add-to-your-collection-plan/>

<https://www.linkedin.com/pulse/cyber-threat-intelligence-requirements-what-how-do-fit-mark-arena>

<https://isc.sans.edu/diary/Defining%2BThreat%2BIntelligence%2BRequirements/21519>

<https://sroberts.github.io/2016/03/30/cti-squad-goals-intro-to-requirements/>

<https://www.linkedin.com/pulse/cyber-threat-intelligence-requirements-what-how-do-fit-mark-arena>

<https://isc.sans.edu/diary/Defining%2BThreat%2BIntelligence%2BRequirements/21519>

<https://threatintel.eu/2016/12/27/threat-intel-annual-reads-2016/>

<https://securityledger.com/2016/12/bad-neighborhoods-predict-which-computers-turn-to-crime-also/>

https://c.ymcdn.com/sites/www.scip.org/resource/resmgr/White_Papers/Analytic-Thinking-CIA.pdf

<http://sites.dartmouth.edu/friedman/files/2014/07/Friedman-and-Zeckhauser-Assessing-Uncertainty-in-Intelligence.pdf>

<https://medium.com/the-polymath-project/mental-models-dragonfloxes-and-how-to-think-real-good-9c6db8e8fde7f>

<https://putanumonit.com/2018/09/07/the-scent-of-bad-psychology/>

<https://medium.com/@yegg/mental-models-i-find-repeatedly-useful-936f1cc405d>



<https://www.forbes.com/sites/brentdykes/2016/04/26/actionable-insights-the-missing-link-between-data-and-business-value/#4e2dde4451e5>

<https://www.amazon.com/Actionable-Gamification-Beyond-Points-Leaderboards-ebook/dp/B00WAOGY4U>

<https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1501789375.pdf>

<https://sites.hks.harvard.edu/fs/rzeckhau/Assessing%20Uncertainty%20in%20Intelligence.pdf>

<https://www.artofmanliness.com/articles/ooda-loop/>

<https://www.livingsecurity.com/blog/security-personality-types>

<https://www.livingsecurity.com/blog/2019/1/25/using-insight-to-inspire>

<https://www.livingsecurity.com/blog/culture-map>

<https://medium.com/@sroberts/cti-reading-list-a93ccdd7469c>

<https://medium.com/@markarenaau/being-a-cyber-threat-intelligence-analyst-and-operating-in-the-fog-ofuncertainty-adc7f397d11e>

<https://medium.com/disruptive-design/tools-for-systems-thinkers-the-6-fundamental-concepts-of-systemsthinking-379cdac3dc6a>

<https://ryanstutorials.net/problem-solving-skills/>

<https://warontherocks.com/2018/12/what-would-you-say-you-do-here-redefining-the-role-of-intelligence-in-the-information-age/>

<https://inteltechniques.com/book1.html>

Malware reversing threat intelligence - <https://www.youtube.com/watch?v=qpdtOY-7fEc>

RECOMMENDED BOOK LIST

1. Anything by Tversky and Kahneman
2. People-Centric Security by Lance Hayden
3. Creativity Inc. by Ed Catmull
4. Mastermind by Maria Konnikova
5. Actionable Gamification by Yu-Kai Chou
6. Sense of Style by Steven Pinker
7. Effective Threat Intelligence by James Dietle
8. Forensic Psychology by William Harmening
9. Psychology of Intelligence Analysis by Richards Heuer, Jr.
10. Structured Analytic Techniques by Richards Heuer, Jr.
11. Intelligence Analysis (A Target-Centric Approach) by Robert M. Clark
12. Open Source Intelligence Techniques by Michael Bazzell
13. <https://medium.com/@sroberts/cti-reading-list-a93ccdd7469c> (CTI reading list!!!)