HOW TO MAKE YOUR SECURITY AWARENESS PROGRAM – FAIL!

Winn Schwartau

Founder & Chief Visionary Officer

1.727.393.6600 X 8

winn@thesecurityawarenesscompany.com

What is Security Awareness FAIL?

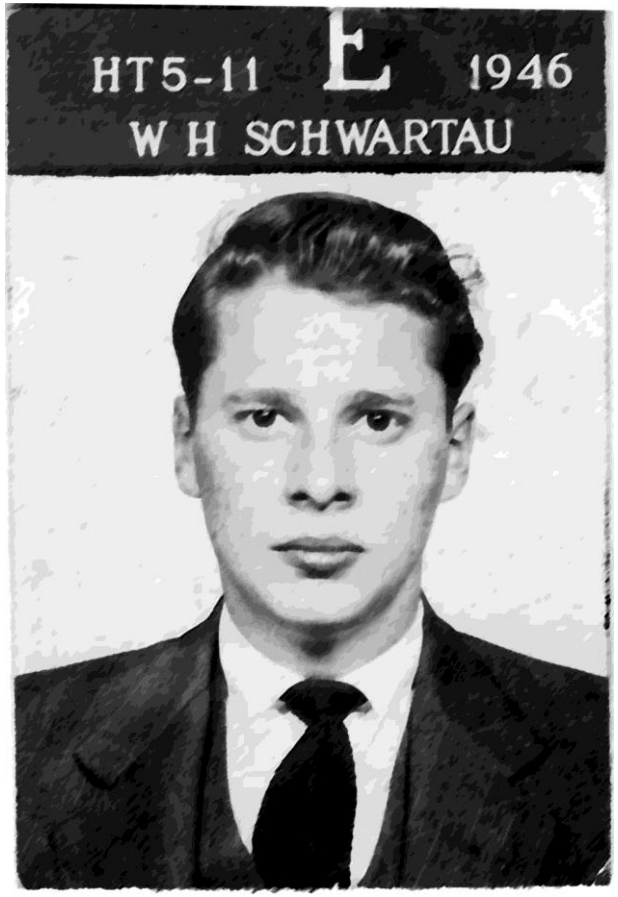
Oh… let me count the ways…but First… All About Me!

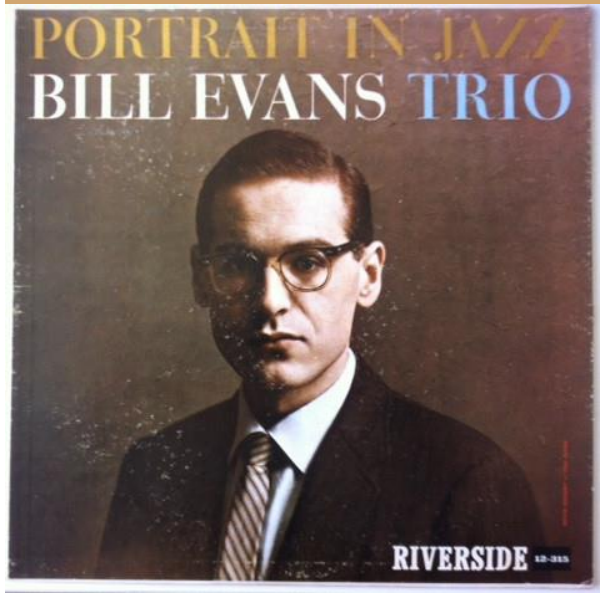
Family of Entertainment-Geeks

My Mom -1943. Actress/
NBC Mastering Engineer

All About Dad!

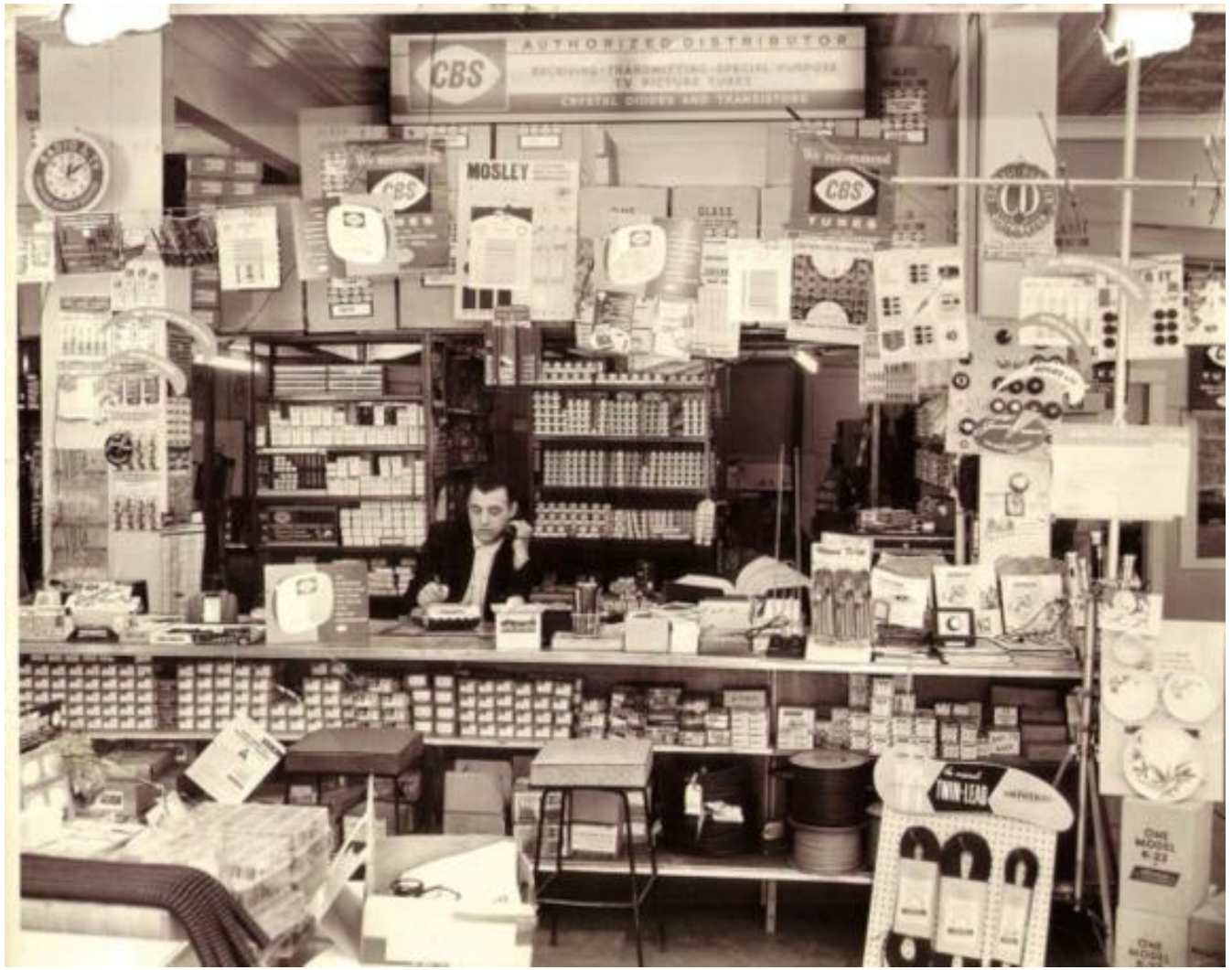
Dad: Dev. Radar WWII
Actor/Producer/Engineer





Winn As TV Repairman: $.50 per Repai

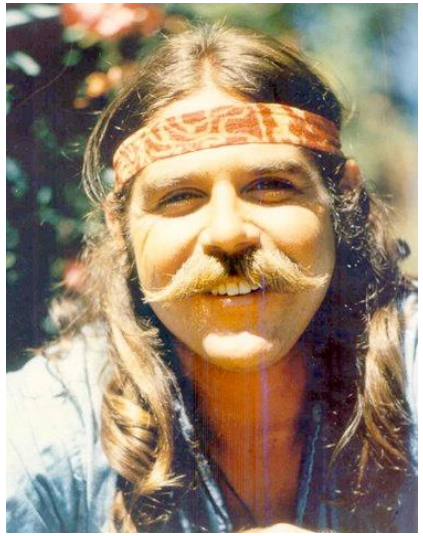
My Electronics Store: Audio Engineering



High School Computer

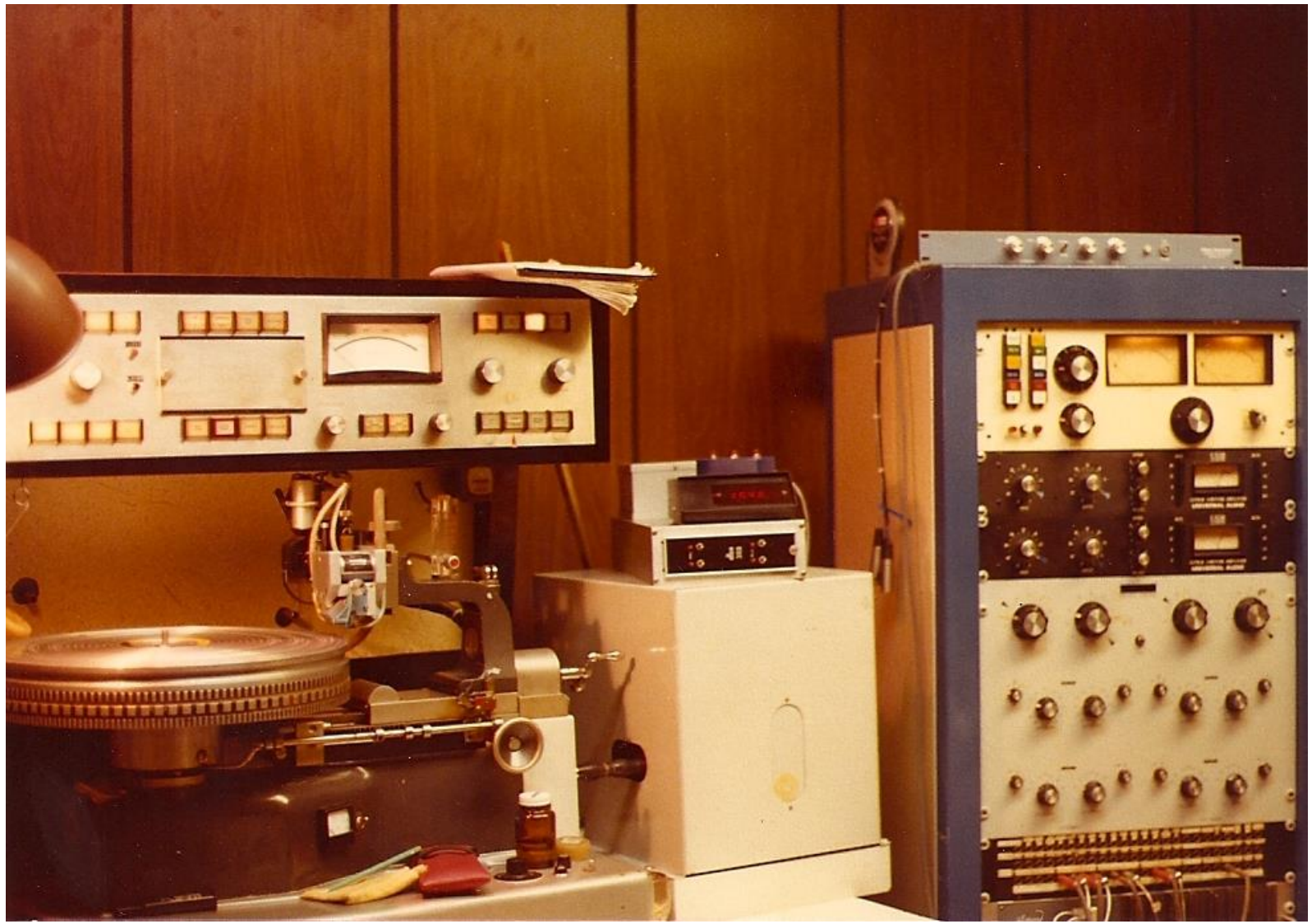
High School Sucked and I Couldn’t Get a Jo

IBM

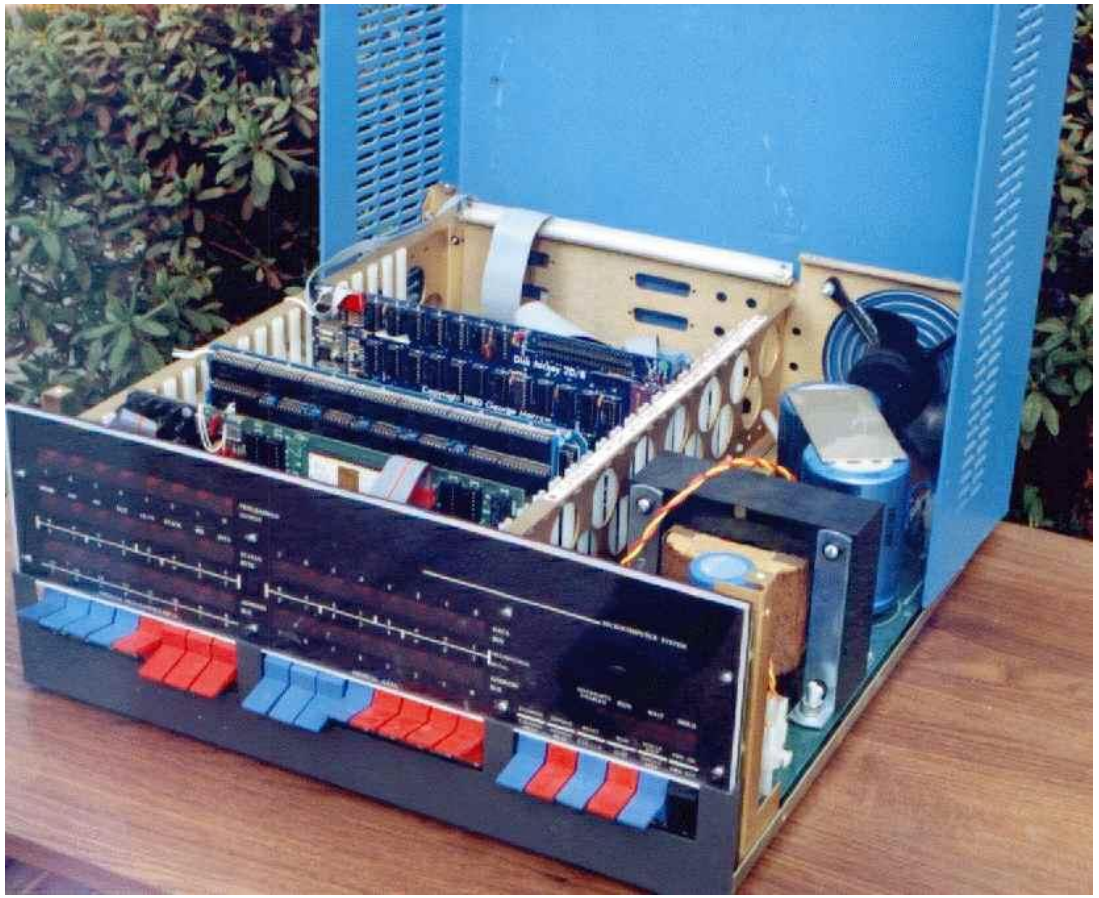


The Family Business:
My First Studio (16 yrs. Old)

My First Cutting Lathe



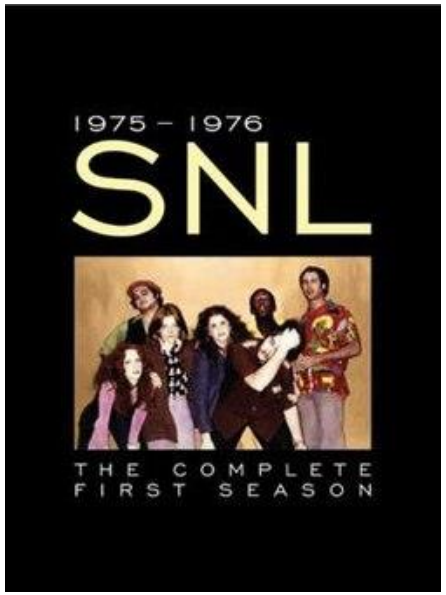
My First Machine Language Compute

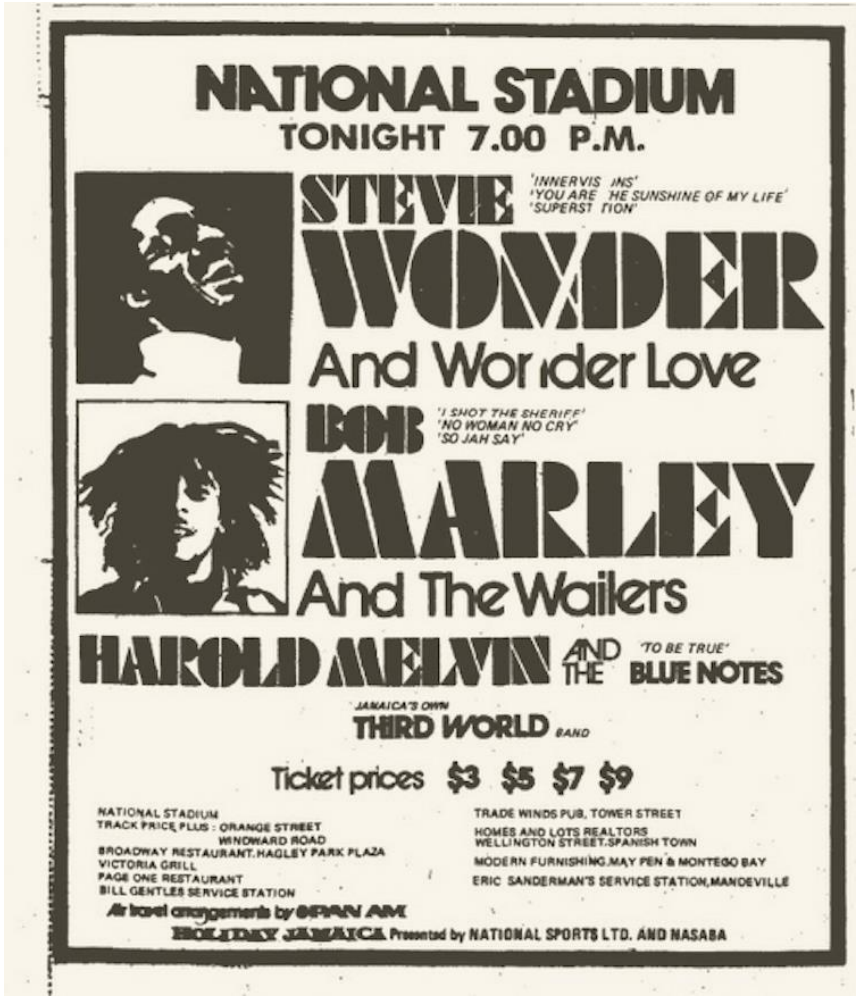


1969-1981: Audio/Video/TV (Computers...sort of...)

- Hit Factory
- Record Plant
- A&R
- MediaSound

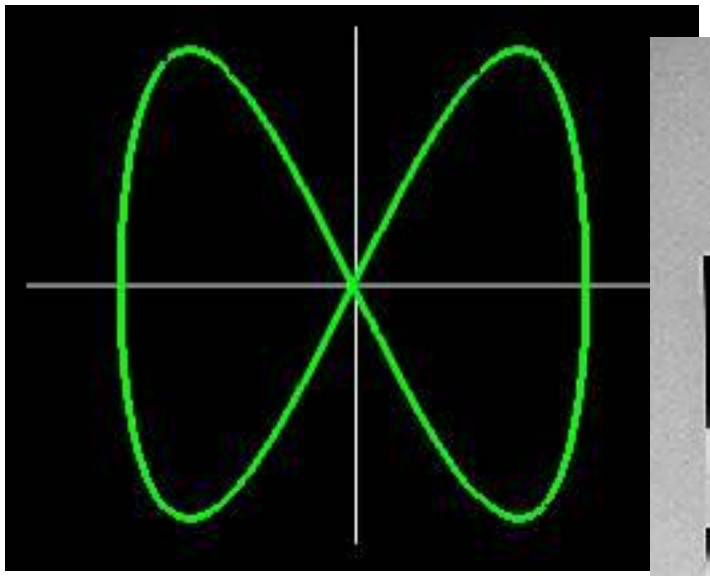
I Loved Going Live: When the Show MUST Go On

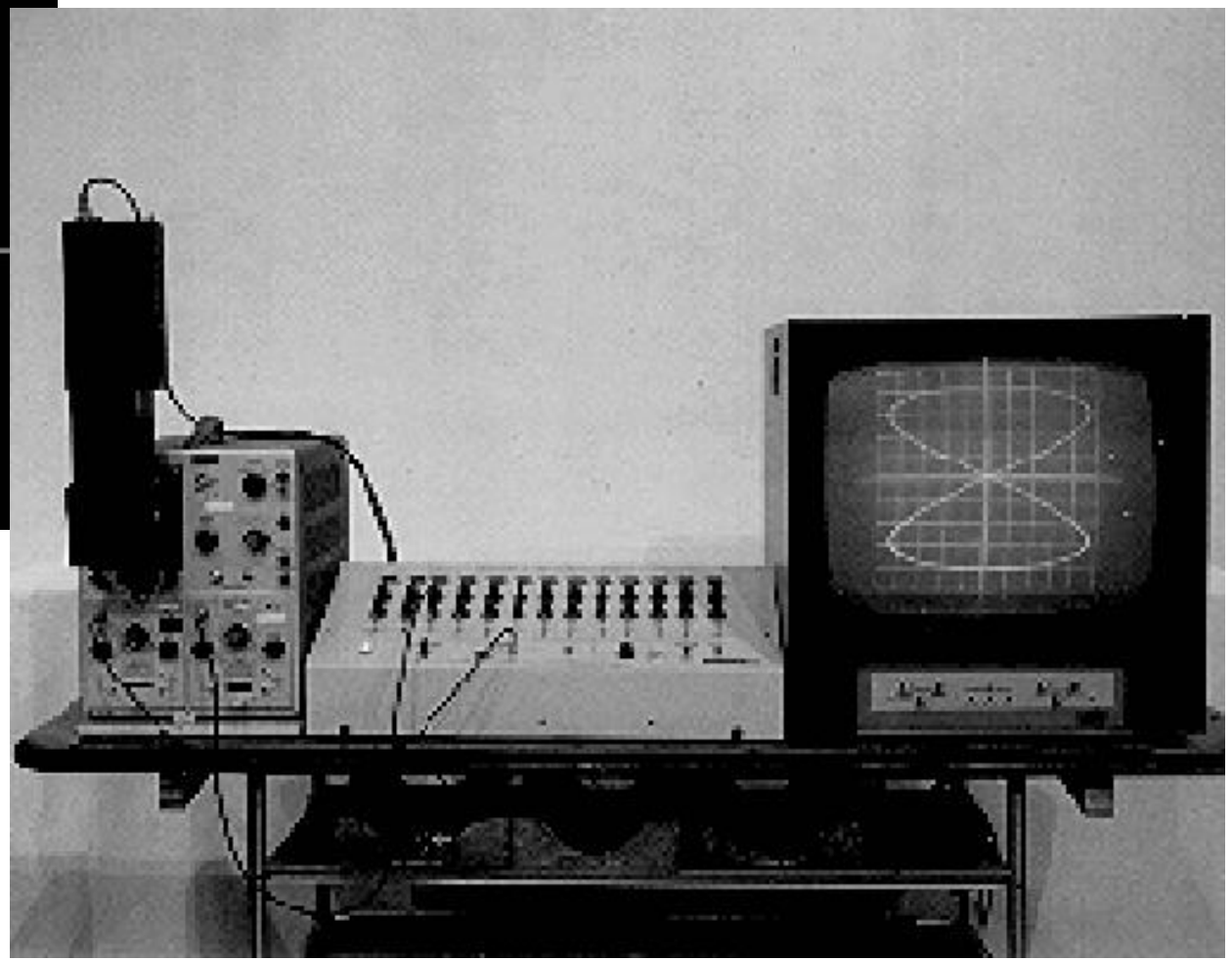




TV:Movies - Auto Sync (Right!)

And When It Fails - The Show Must Still Go



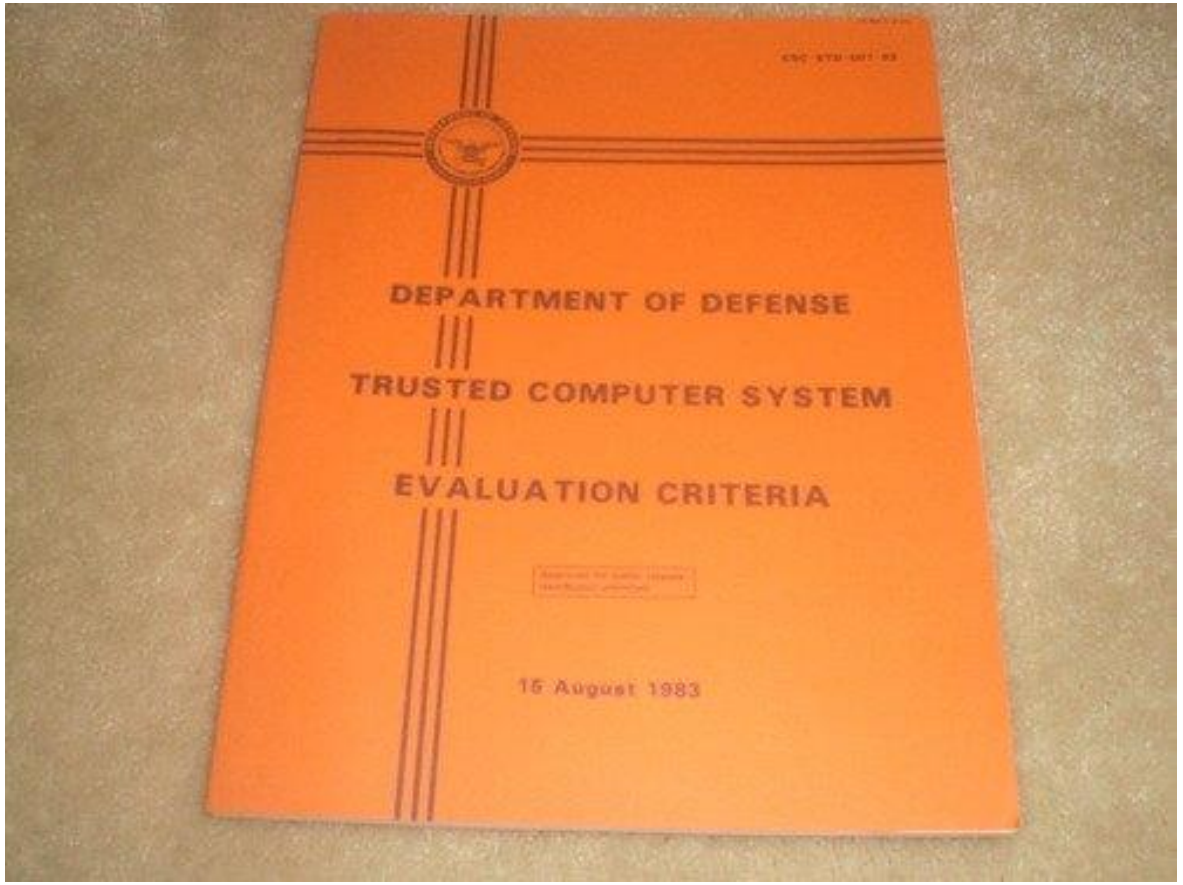


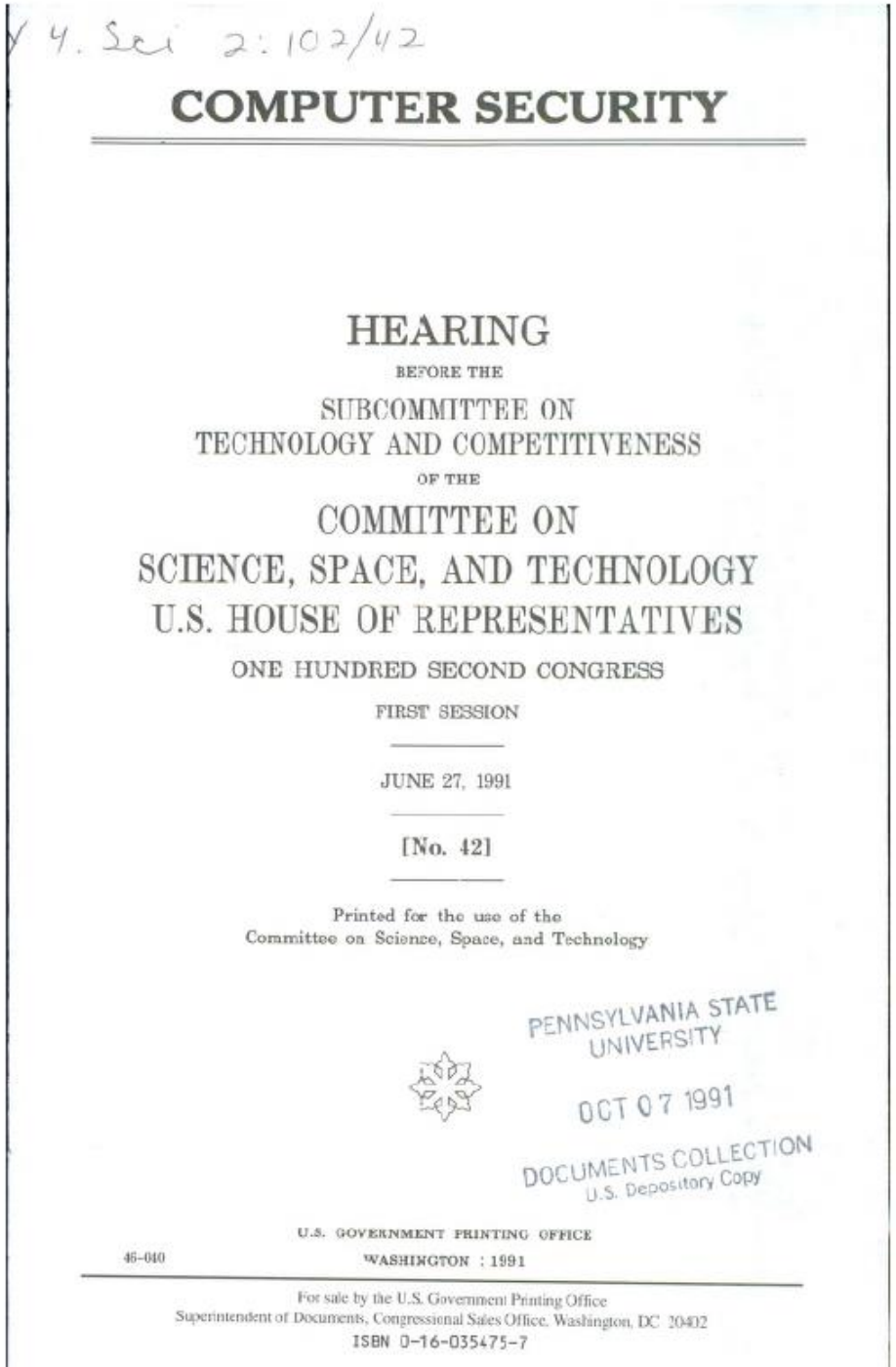
1979: Building Recording/TV/Movie/Remo

My Studio: 1980

Digital Audio/TV/Movie Automation: 19

7 January 1983: Went Into Security





Y 4. Sci 2:102/42

COMPUTER SECURITY

HEARING

BEFORE THE

SUBCOMMITTEE ON
TECHNOLOGY AND COMPETITIVENESS

OF THE

COMMITTEE ON
SCIENCE, SPACE, AND TECHNOLOGY
U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED SECOND CONGRESS

FIRST SESSION

JUNE 27, 1991

[No. 42]

Printed for the use of the
Committee on Science, Space, and Technology

U.S. GOVERNMENT PRINTING OFFICE
46-040 WASHINGTON : 1991

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-035475-7

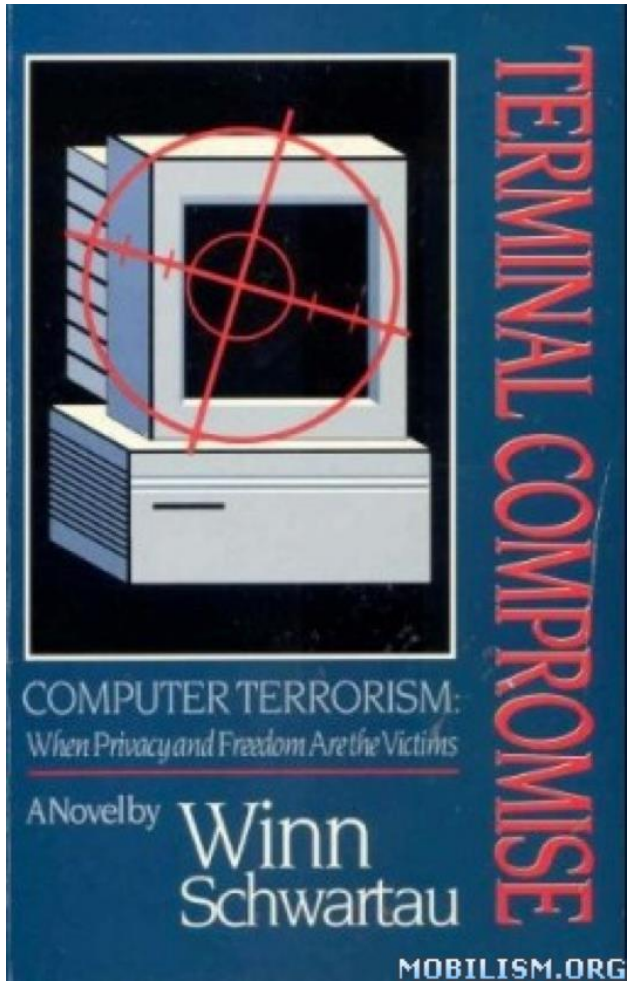
Congressional Testimony June 27, 1991

Our computer systems are so poorly protected, they are *"An electronic Pearl Harbor waiting to happen."*

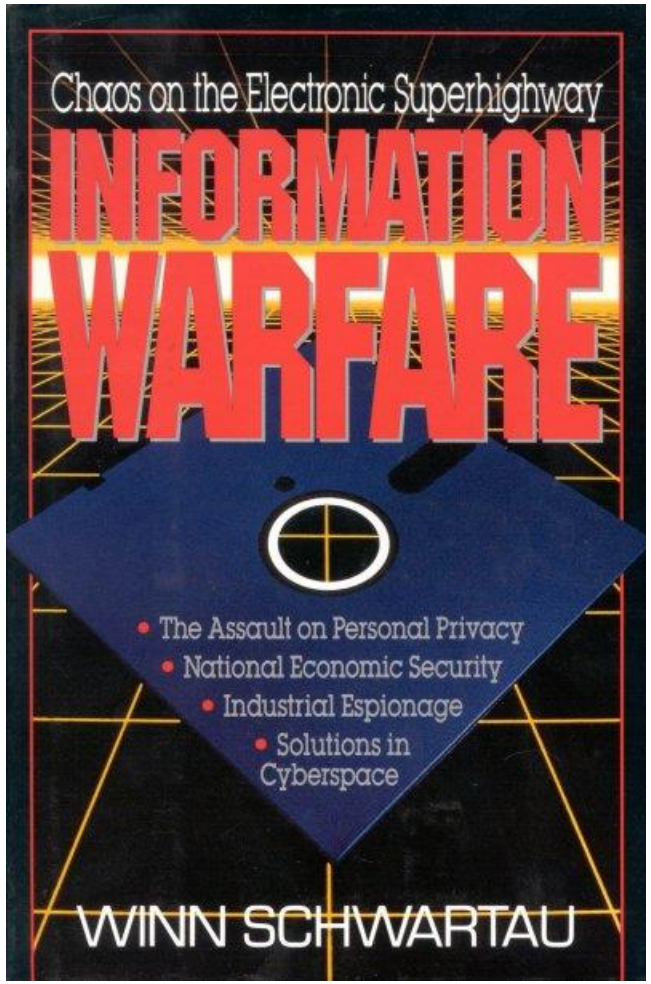
"The Civilian Architect of Information Warfare."

Admiral Tyrrell, UK MoD

The Early Days: Weaponization of the Internet



1990



1993

Teaching Cyberwar/CyberTerrorism Awarenes

Ministry of Defence

SWEDISH DEFENCE LEAGUE
IN HOC SIGNO VINCES

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

Australian Government
Department of Defence

UNITED STATES CENTRAL COMMAND

DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FIDELITY BRAVERY INTEGRITY

MINISTERSTWO OBRONY NARODOWEJ

UNITED STATES NAVY SEALS

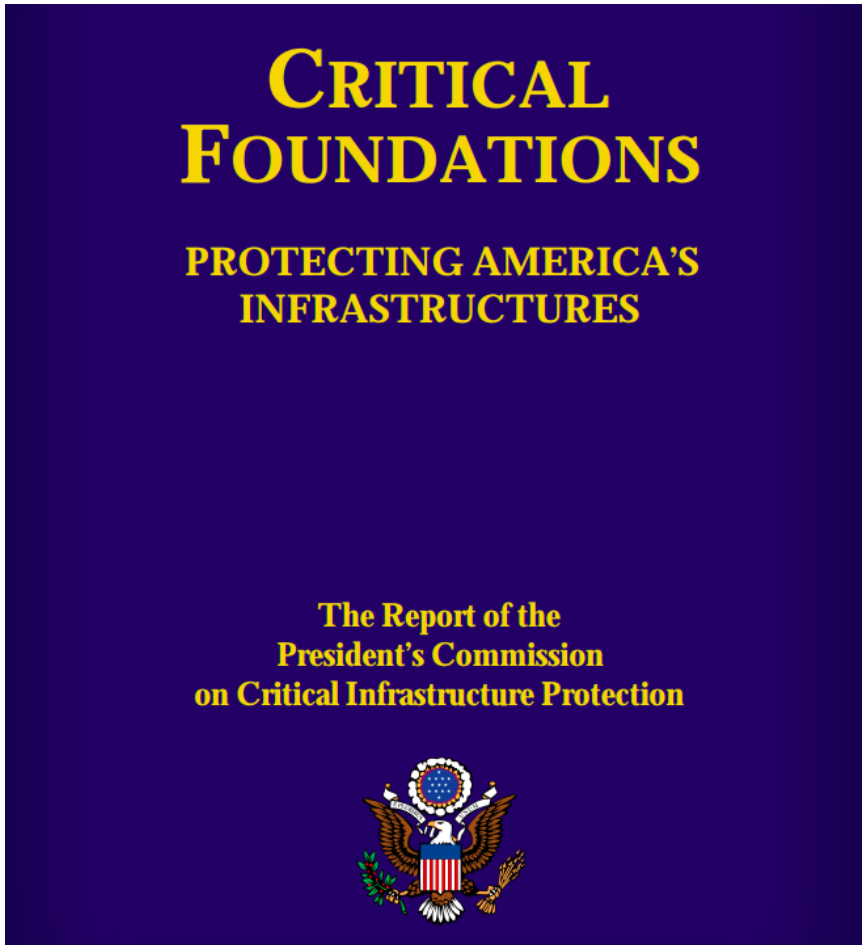
AIRBORNE
UNITED STATES SPECIAL OPERATIONS COMMAND

YANG PERTAMA DAN UTAMA
MINDEF SINGAPORE

ROYAL NAVY

NATO OTAN

Clinton's Marsh Commission on Critical Infrastructure: 1996-97

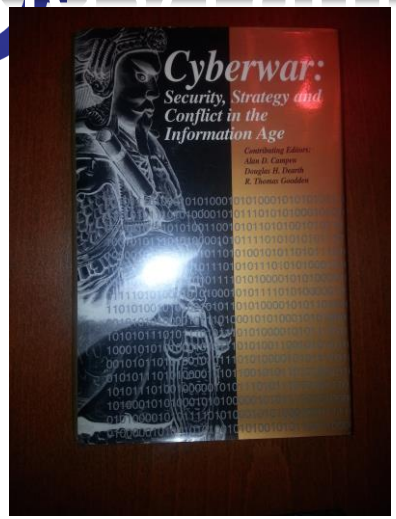


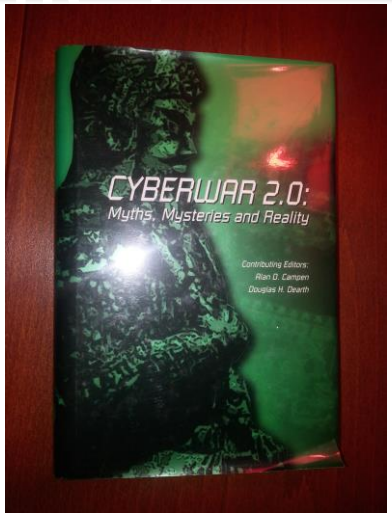
FINANCIAL SERVICES Information Sharing and Analysis Center

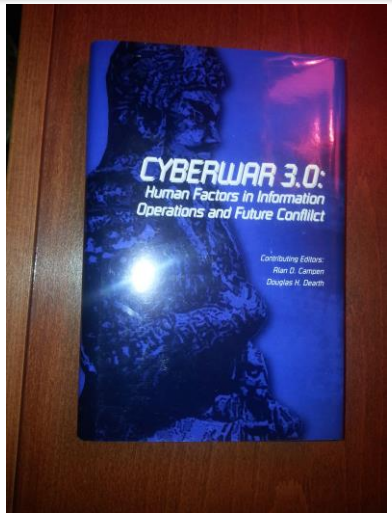
NH-ISAC NATIONAL HEALTH - ISAC

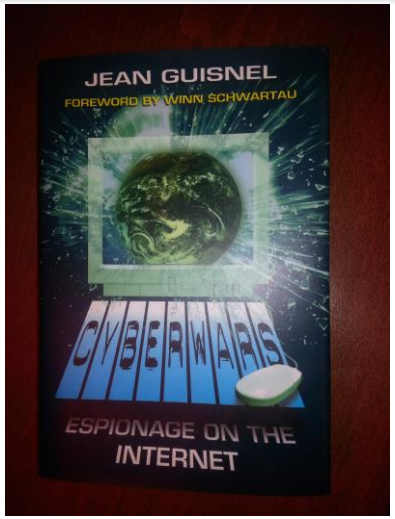
NationalCouncilofISACs

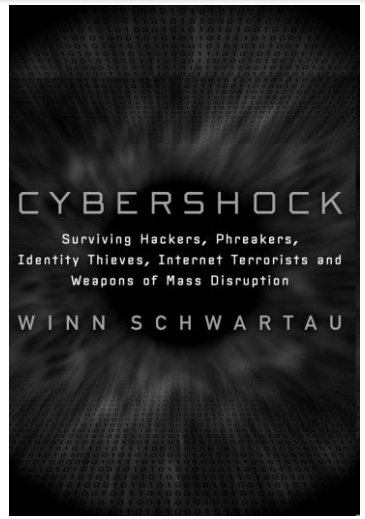
Expanding Awareness: Gov/Mil ➡ Enterprise ➡ EDU ➡ Kids/Families

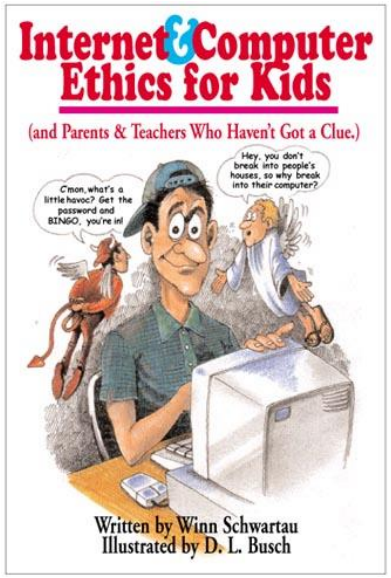


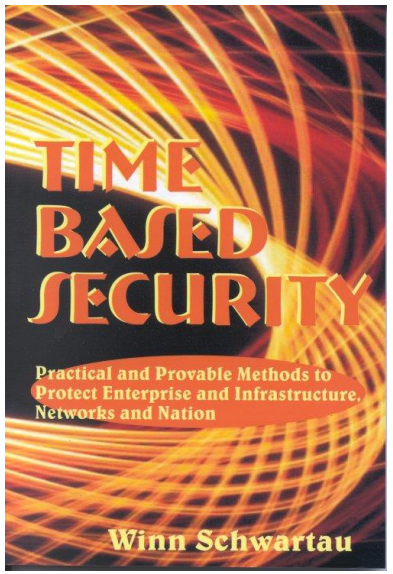


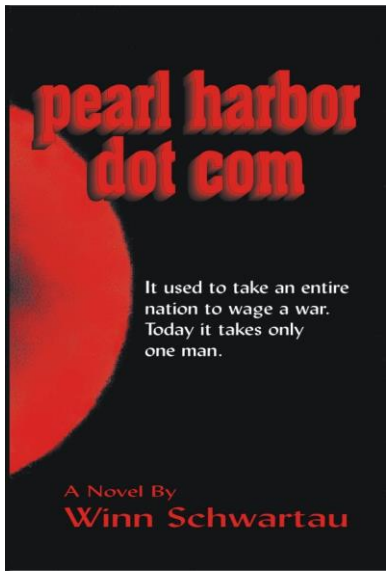


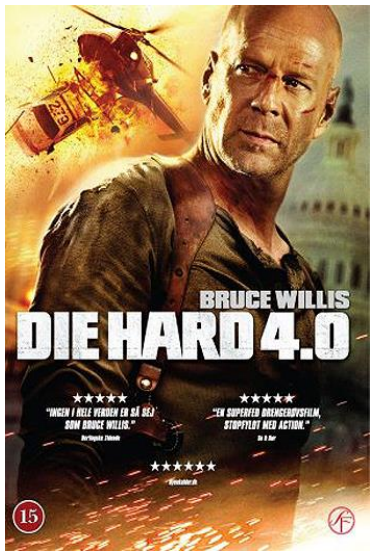




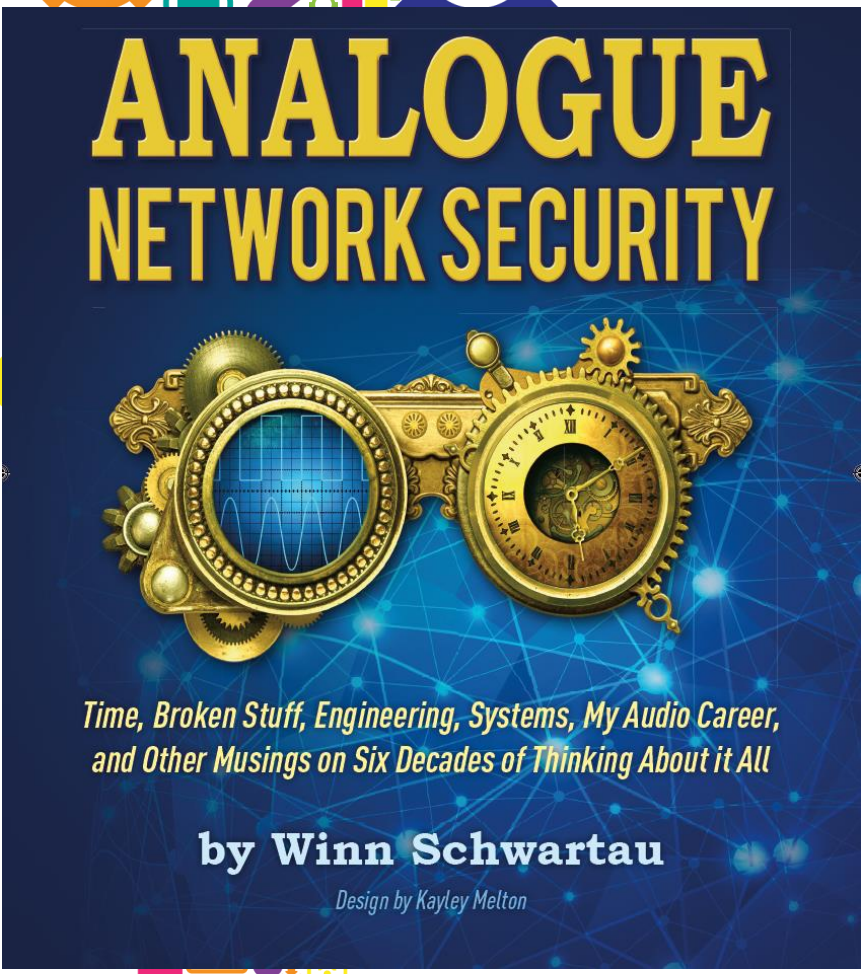


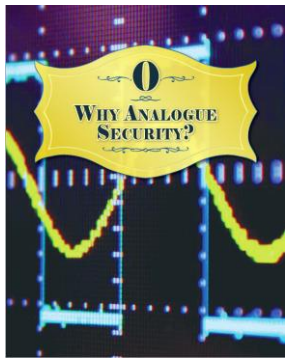


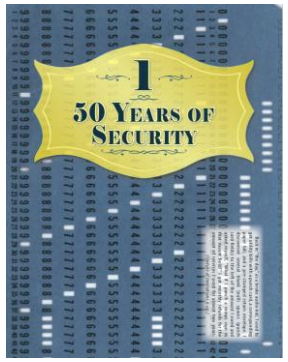


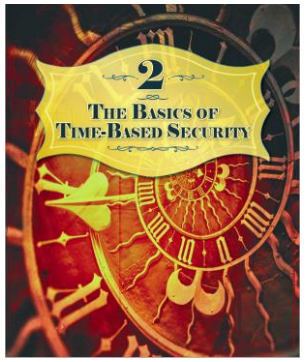


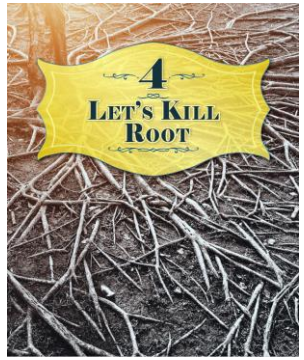
Amazing Good Fortune: Audio, Video, Entertainme

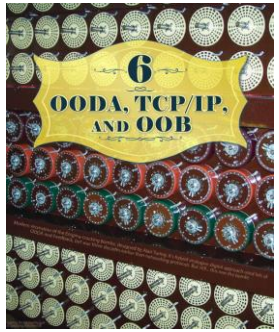


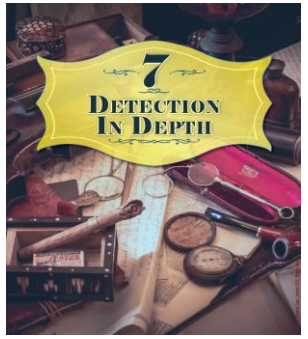


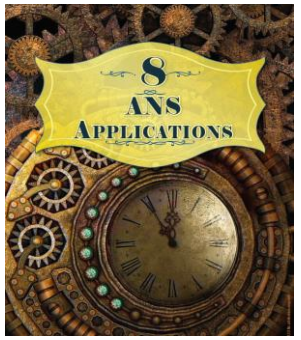


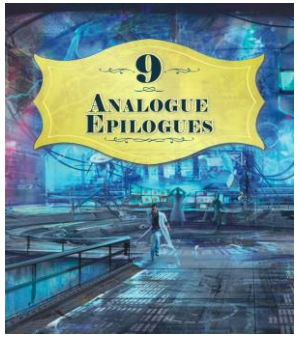












So, Back to How to Make Security Awareness FAIL!

Oh… let me count the ways…and but always remember

Awareness Must Be Boring

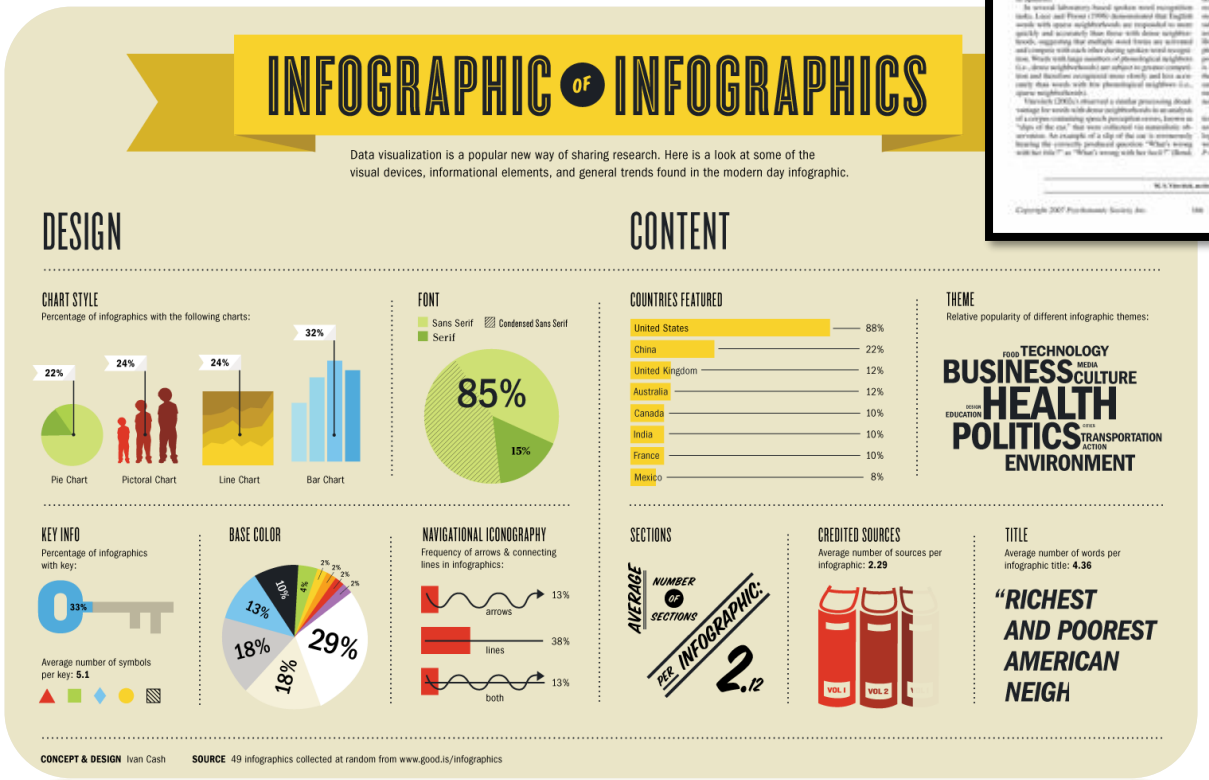
- ✓ Mind numbingly so, if budget permits.
- ✓ Words, words, and more words.
- ✓ Extra dull earns extra points!

Graphics Just Get in the Way

Why waste time organizing information in infographics? Eight pages of agonizingly small 7.5pt font is just as effective, right?


The spread of the phonological neighborhood influences spoken word recognition

If you **DO** break down and use graphics, don't waste time hiring graphic designers: all graphics are created equal.



Never Use Humor

In fact, smiling is discouraged. People should understand the serious nature of security.

Work and security require a business attitude. If people laugh, are they really paying attention?

All You Need to Teach Is Policy & Compliance

Repeat the same dry, boring rules over and over again. People will get it.

Knowing policy means no security breaches.

YOU CAN'T DO THAT

YOU MUST DO THIS

NO

Tell - Don’t Show (Hollywood Style, eh?)

Multi-media is cheesy, silly, and overrated. Videos are pointless.

Tell in lots of words. Never ‘show’ or create visual metaphors.

Videos do not reinforce information in a memorable way. Emailed instructions are just fine, thank you!

Do Not Make Awareness Personal

Don't acknowledge a person's family or personal life. Concern should only lie with whether or not the company is secure. Everything else is expendable.

Remember, when in doubt, just follow policy.

Don’t Go Mobile!

- Employees belong at their desks, working.
- We simply don’t see any value in putting SA content, videos, updates, news, or alerts on a mobile device. What good would that do?
- And, why should we invest in an easy-to-use mobile security reporting tool that works from any platform, anywhere at any time? We don’t see the value.

Don’t Set Vision, Goals or Objectives…

If you have no vision or goals, and are not supported by C-Level and Board… you WILL fail.

You cannot build a house without:
Land
Foundation
Designs & Plans

Start Too Big

Do too much at the beginning.

Turn on the firehose instead of reasonable starting plans…

Make small changes… one at a time… and demand them tomorrow

Let Corp Comm Run All Awareness

Corp Comm can build you the ‘box’ from which creative escape is impossible.

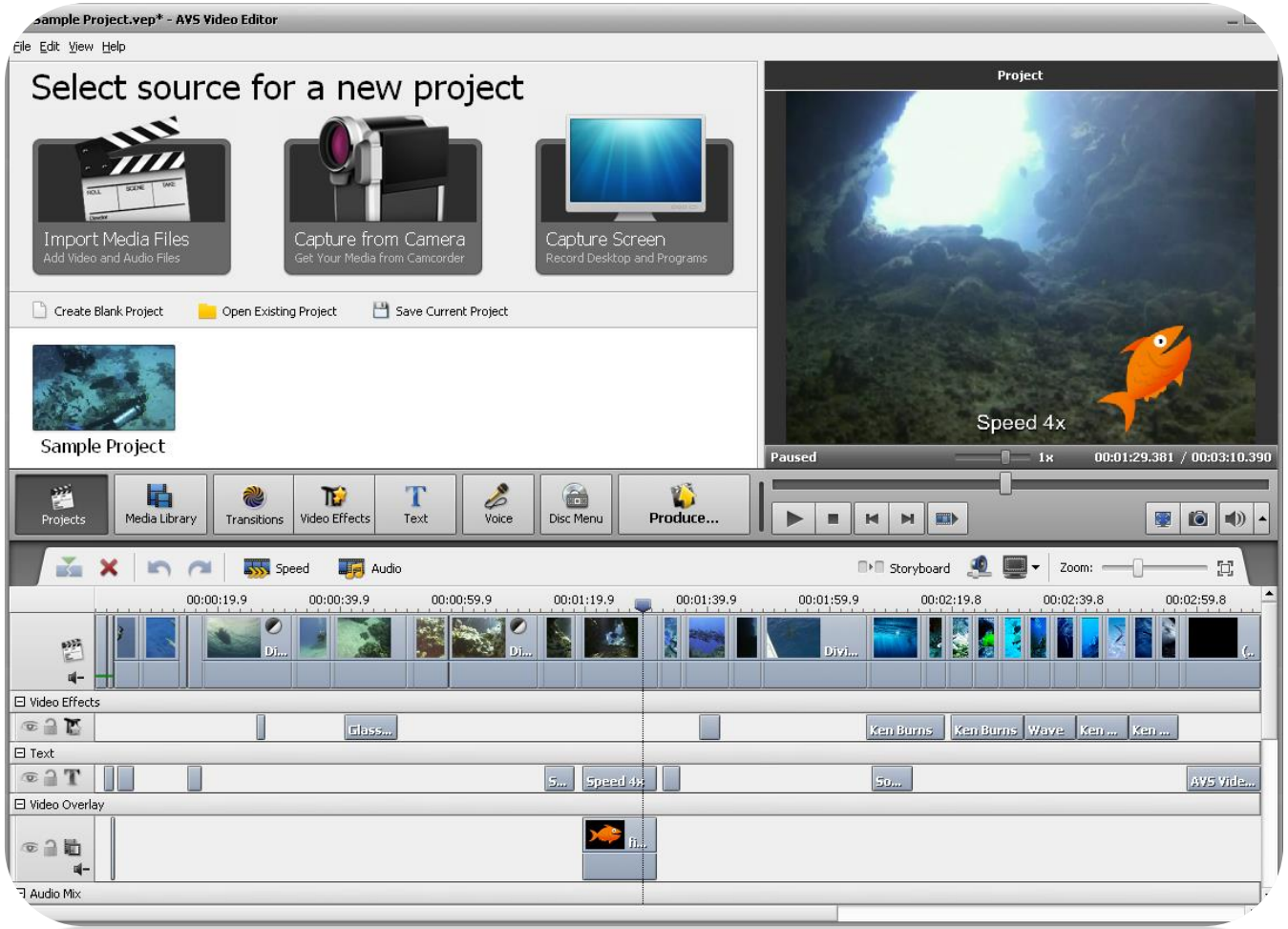
Want to delay a program for months? CorpComm can help you with that.

Let the CISO into the Production Process

The CISO took a film class.

The VP-IT took a semester of creative writing.

Let them set the tone and have the final say in both graphics and editing!



Design by Committee

Who needs leadership or technical knowledge? Add needless complexity & internal inconsistency?

Who needs to waste time with a strong, creative vision? The quality of a product doesn't matter. All that matters is a committee approval.

Never Use Casual Written or Spoken Language

Gonna

Oopsy!
Slangish

Blind Eye

AWARENESS

INS AND OUTS OF SOCIAL ENGINEERING

SPEAK GEEK?

Flim Flam

Scam Man

DNS TCP/IP

IPS DLP TLS

SIEM AES

Casual is unprofessional!

Use academic terms only!

People love words and acronyms they don't understand.

Don’t Follow The Gold Fish Rule

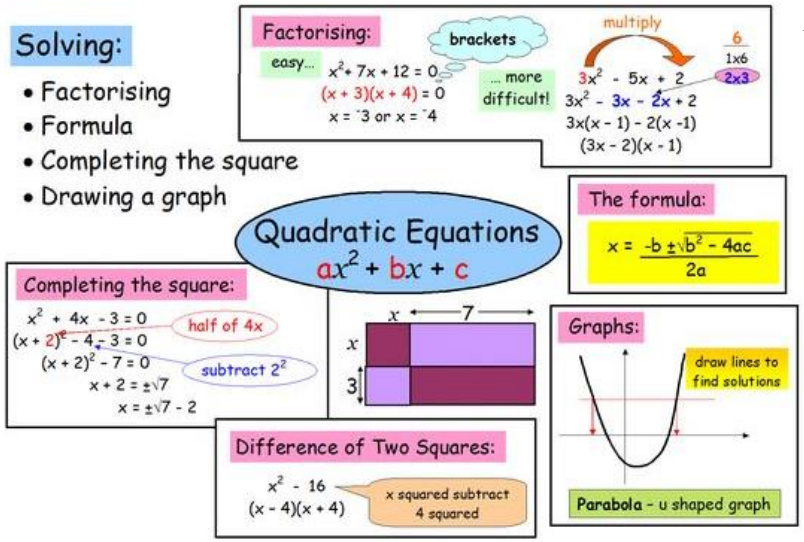
You know that your Security Awareness Messaging is the most important thing ever.

Just refuse to accept that the average human attention span is 8.3 seconds; about that of a gold fish.
People should just focus better.

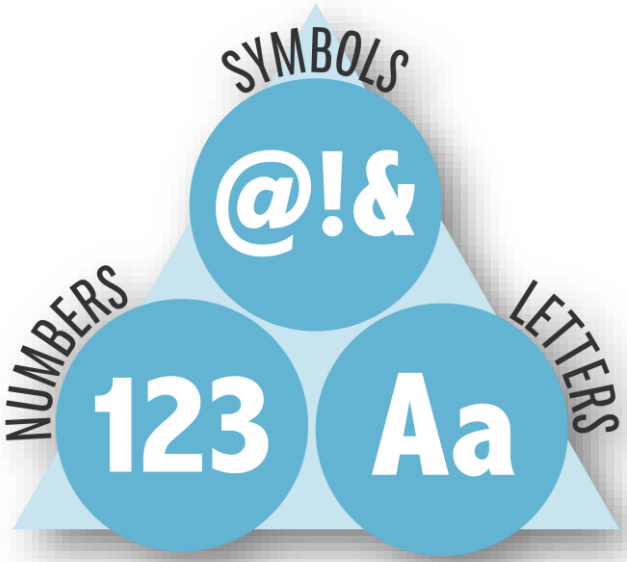
Sex, Drugs, and Rock'n'Roll: Don't Use the Rule of Three.

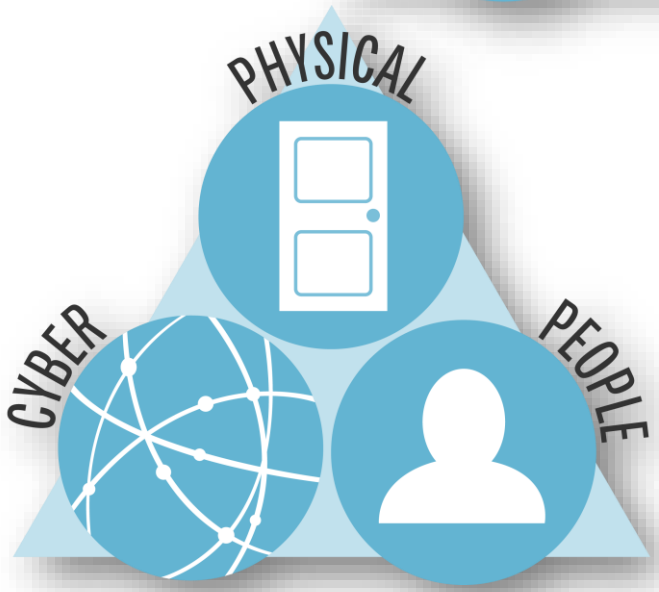
You need users to know 14 different details on 8 disparate, but somewhat related, cyber-security best practices, corporate policies, and the latest compliance regulations.

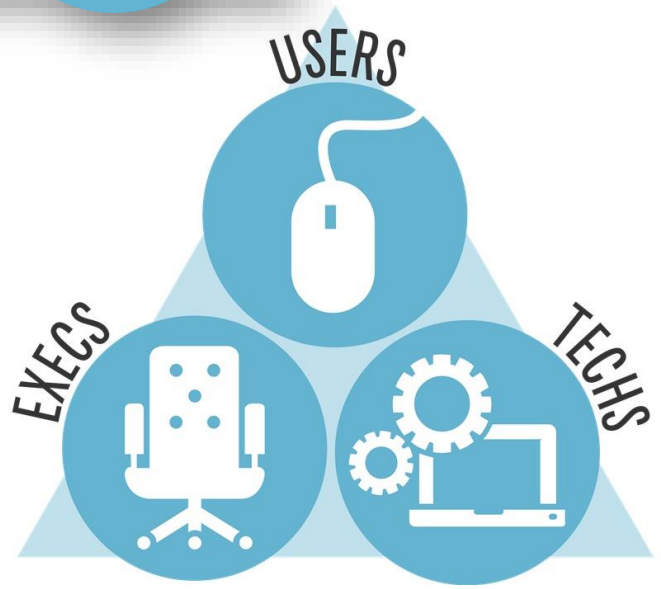
Nothing less will suffice.



Don’t Use Triads





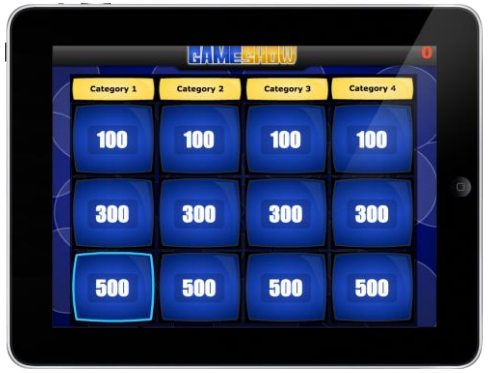


Ignore The Science of Learning

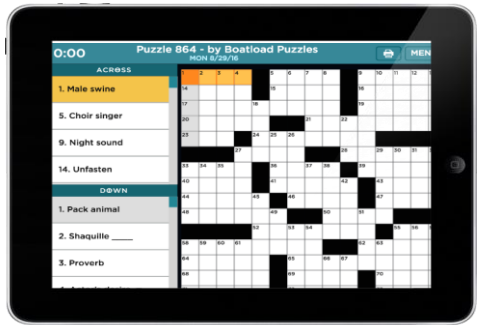
- "When I was a kid …"
- "If it was good enough for me …"
- "Can't teach an old dog …"
- We 'understand' Learning
  - Apply Neuro-Science
  - Employ Addiction Techniques
  - Brain – Best Averaging Machine, Ever!
  - Micro-Learning & Chunkification
  - Interactivity & Gamification stimulate stronger neural pathways, which = Modified Behavior.

Games? We Won't Use Games!

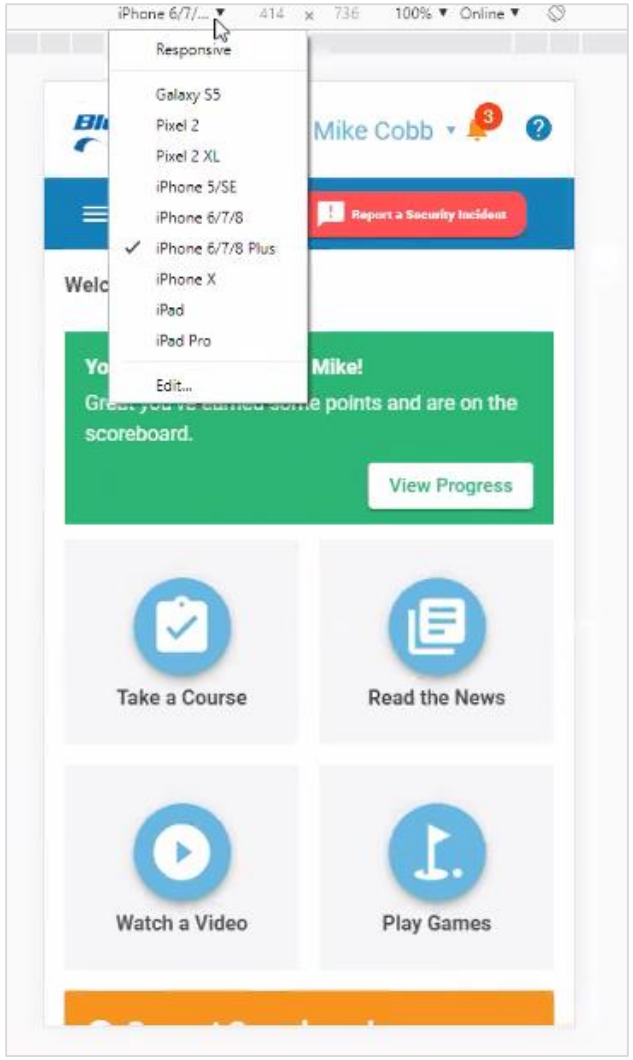
Just because games are addicting, and we can get people's attention, and we can have SA messaging and content built-in, let employees compete for fun or prizes, and develop metrics … so what?

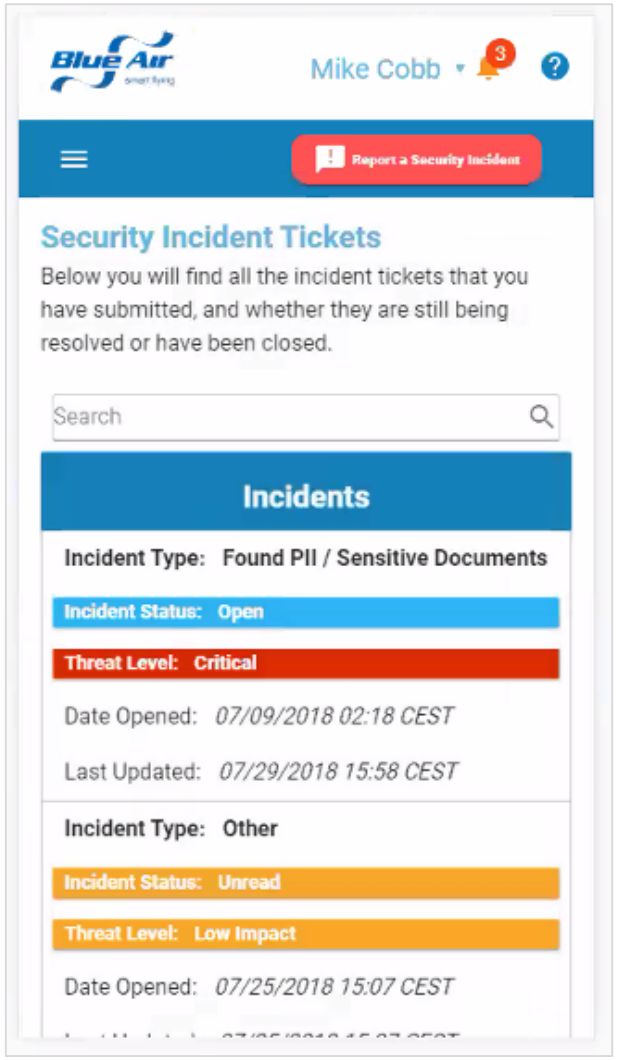


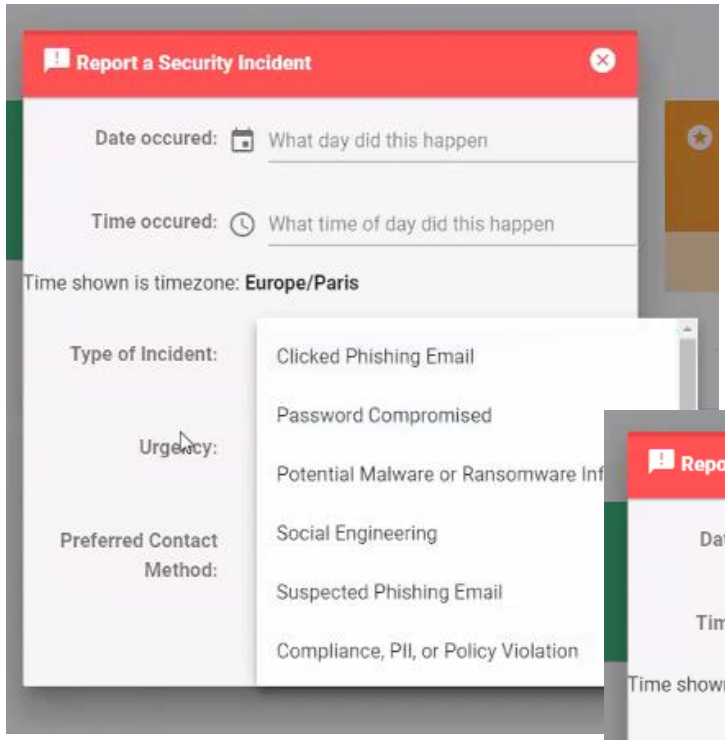
It's still a … Game?!$%!%?

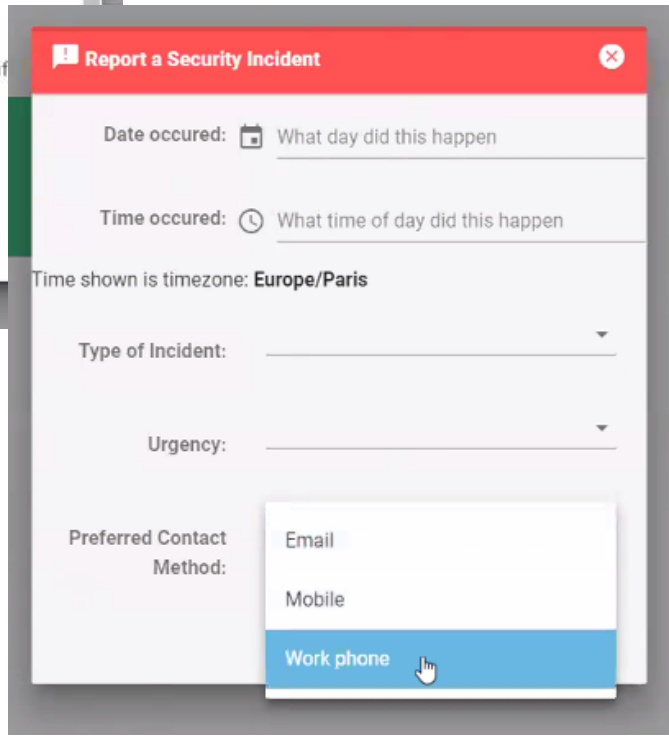


Don’t Use An Awareness & Incident Reporting Portal









No Feedback, Please! Don’t Listen To Your Customer

They don’t know anything, anyway.

They’ll just want it their way.

If they go away, we will know awareness doesn’t work.

Never Test Behavioral Reactions

We know that phishing tests are valuable, but they are so discriminatory. It can hurt people's feeling to know they clicked on stupid s***.

We'd like, to, but HR and Legal are saying it's too hard to do fairly.

Awareness Should Be Super Technical:
More Security Experts is Better!

A helpdesk is just another mindless expense.

Saves $ on Tech Support.

Who says your time is valuable?
Don't go to the experts for help.
Waste a couple of hours and troubleshoot the problem yourself.

Make all of your employees super-geeky security experts.

The Execs Don’t Need Security Awareness

C-Suiters don’t have time to waste on security awareness.

They approved their policies, they obviously know how to avoid security risks.

So save your funds and don’t train them.

Ignore IT & Technical Staff

Save money!
Don't train the geeks.

Geeks design the software and run the networks; why would they need training?

Geeks ***only*** have to stay up-to-date on how to manage firewalls and ensure your security. Save that extra $100 and don't train them.

Use Threats & Give Orders

Want to be a better leader? Use more fear.

Leadership through fear is exceedingly effective in controlling people's behavior.

Everyone Knows, Awareness Is Just A Once A Year Event

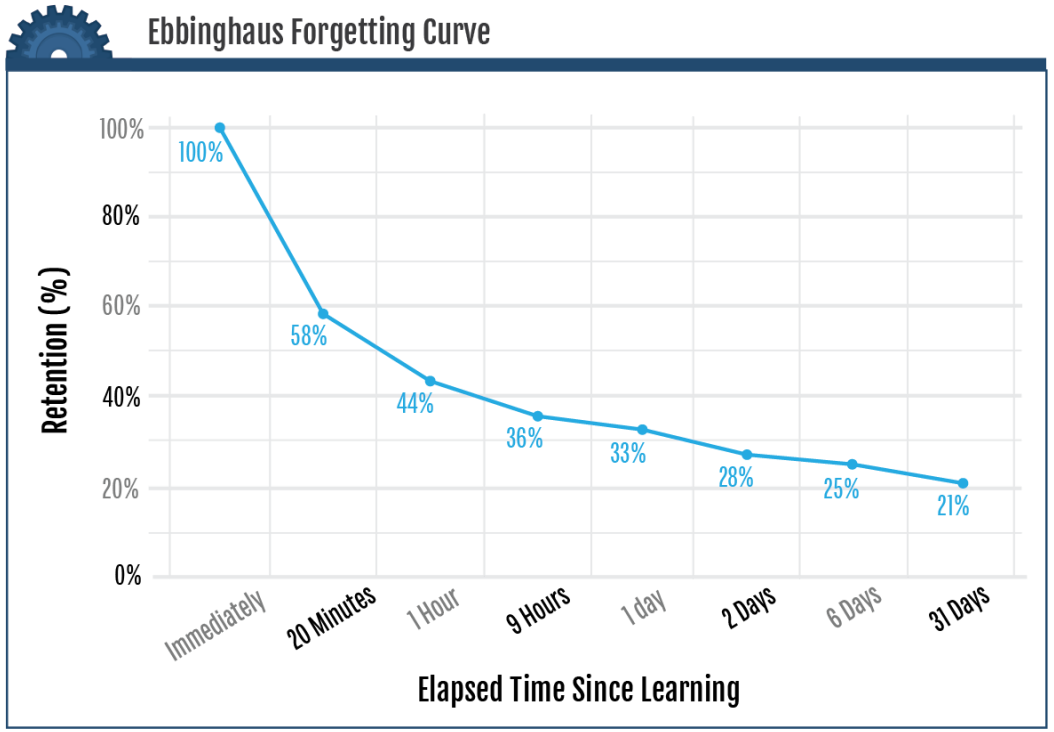
Once is always enough.
Especially for security.

Checked all the right boxes?

Reinforce policy through **one** yearly video or **one** short course.

Make it mandatory! Force every employee to check the **"I will always follow policy"** box under threat of termination.

Yes! Then congrats, you're done! No need to repeat it.
We're done. Right?



The Awareness Answer? What Does Work?

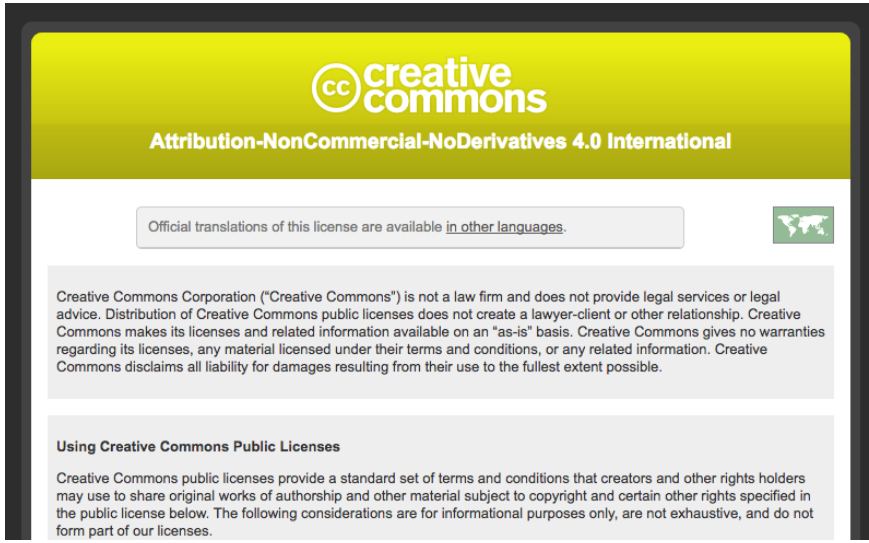
The Exact Opposite of Everything we Discussed!

Security Awareness Program Resources: Free. Really. No Gimmicks.

A huge repository of Free Security Awareness Program Materials.

https://free.thesecurityawarenesscompany.com/

Materials protected under Creative Commons CC BY-NC-ND 4.0.
https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode


creative commons

Attribution-NonCommercial-NoDerivatives 4.0 International

Official translations of this license are available in other languages.

Creative Commons Corporation ("Creative Commons") is not a law firm and does not provide legal services or legal advice. Distribution of Creative Commons public licenses does not create a lawyer-client or other relationship. Creative Commons makes its licenses and related information available on an "as-is" basis. Creative Commons gives no warranties regarding its licenses, any material licensed under their terms and conditions, or any related information. Creative Commons disclaims all liability for damages resulting from their use to the fullest extent possible.

Using Creative Commons Public Licenses

Creative Commons public licenses provide a standard set of terms and conditions that creators and other rights holders may use to share original works of authorship and other material subject to copyright and certain other rights specified in the public license below. The following considerations are for informational purposes only, are not exhaustive, and do not form part of our licenses.

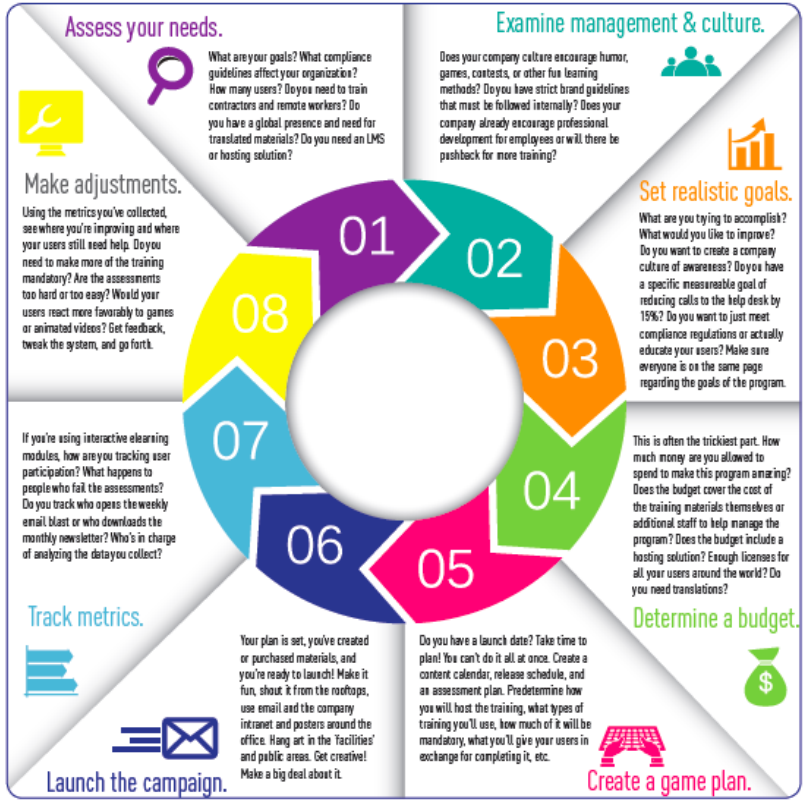
Security Awareness Program Management

The Introductory Guide to

Creating and Managing a Successful Security Awareness Program

Where do I start?

Follow our Circle of Awareness to help you build and manage an awesome security awareness program. These eight steps will help you get on the right track to shifting your users' mindsets and changing behavior. Pretty soon you'll have a whole team of human firewalls!



09 Rinse and repeat.

Treat your awareness campaign like a marketing and advertising campaign. Does Coke run just a few commercials a year? Do movie companies only run one trailer for upcoming releases? Subway ads, billboards and window displays change regularly to send consumers the same messages in different ways. Once you've followed steps 1 - 8, start again. Awareness is a dynamic process, not a thing. Re-assess your needs, update your goals, and make improvements to your campaign.

Security Awareness Case Studies

SECURITY AWARENESS PROGRAM CASE STUDY

Industry: Health Care
Company size: 30,000+
Number of countries: 3+

When did you implement your security awareness program?
January 2016.

Can you describe your launch process? What did you do to bring attention to your efforts?
Our launch process, not to be confused with our progr process, took only a few weeks. With an established relat our Corporate Communications Dept. and the executive announcement communication was drafted from the EV bring attention to our efforts and released on the intran few days later by our first branded magazine.

What sorts of materials and content are y including in your program?
Our program includes a wide variety of SAC products a custom in-house material as well. Most of our released n consists of; LMS courses, Screen Saver, Focus Topic New Magazines, Videos, Monthly Roundup and Incident resp messaging.

What topics are the most important for y program participants?
Our data suggests that material released about Social big hit topic for our program participants

Do you have a central learning portal of s
Our company has an Intranet and we use that as our n repository for all our digital material releases.

How much of your training is mandatory?
Only a small amount of our LMS courses are mandator into the realm of compliance courses. If I had to assign a I would say 90% of what we release to our participants i mandatory to interact with.

What have you done to encourage emplo participation?

Currently we are focused on making the announcemer material more enticing to grab reader's attention but we utilize different participation rewards from contests, gan for rewarding desired behavior like not interacting with a phishing campaign or reporting a REAL social engineerin

How do you maintain momentum and keep people interested?
Interests are unique to each and every employee. By having a wide array of topics or delivery methods that appeal to different individuals you'll increasing your participation.

Any final pieces of advice you can give to other SAP admins or companies launching a new security awareness program?

1. The main piece of advice to those just starting or looking to start a SAP; Slow and steady wins the race!

SECURITY AWARENESS PROGRAM CASE STUDY

Industry: Consulting & Certification
Company size: 12,000+
Number of countries: 44+

When did you implement your security awareness program?
This is still a new program, we launched only a few months ago.

Can you describe your launch process? What did you do to bring attention to your efforts?
It was really important for us to get our president involved, to show that security was important to everyone within the company, from the top down. So the initial launch video was hugely helpful. It included not only an introduction to the key tenants of the program and the materials that users could expect to see in coming months, but also a personal message from the president. We found this to be really helpful in our global offices, especially in Asia where they need to see buy-in from the top down. This video was integral for gaining initial support.

What sorts of materials and content are you including in your program?
We have a monthly newsletter, which includes a global security team update. We've received feedback from our European and North American offices that they find this useful. We haven't gotten much feedback from our Asian offices concerning the newsletter. Also a monthly elearning course. Posters. Videos.
While we have many elearning modules, we still have some instructor-led trainings, especially for workplace violence and active shooter scenarios. A good balance of the two is important to not burn out employees on any one kind of learning.

Do you have a central learning portal of some sort?
Yes, we have a Sharepoint site where we put all of the resources and post relevant news and updates. We have linked all of our security policies in one place so employees can report incidents easily from the intranet to save them time and energy.

Is any of your training mandatory?
No, the entire program is voluntary. Our employees already have plenty of other training they have to take throughout the year, so we didn't want to overwhelm them with more mandatory stuff. This is why wee didn't go with the internal L&D department for developing the awareness content. Last year, they had only a 46% participation rate in the training they produced. This year, with our non-mandatory program, we had an immediate 80% participation rate.

What have you done to encourage employee participation?
We've focused on security issues from a personal perspective. By doing this, instead of focusing on the corporate, it shows employees the benefits of following security practices.
We've offered prizes for the best security tip that our program taught them. So they email us something they've learned from one of our courses or videos, and we pick the best one, and that person gets a prize. The prize isn't something big, but something with company branding on it. A mug, a t-shirt. Something small and inexpensive.
If managers see people doing security aware things -- removing papers from the copy room, not allowing tailgating, locking their workstations, keeping neat desks -- they get called out, praised for it, and are rewarded.
Posters are everywhere, in offices around the world, and we ask employees to send photos of the best poster placement -- just using their phones. Where's the most creative place a security poster is hung? Or the place that will be seen by the most people? It encourages a friendly sort of competition and gets people to pay more attention to the posters.
We only push out one course a month, and as it's not mandatory we just say "this is something you might be interested in, take a look when you have some time." Since we use short, engaging courses, people are generally interested. They can find five or ten minutes a month to spare to take a course. And if they don't do it this month, that's okay, they might do it next month.
The badge and leaderboard system is useful too. People seem to like that -- having a way to see their progress, see where they rank compared to their colleagues, earning little marks of completion along the way.

How do you maintain momentum and keep people interested?
We send out a weekly email from the president -- again, showing interest in security from the top down -- that talks about security and the importance of being security aware at work.
We definitely believe in the carrot method. There's no stick here! We try to remain transparent and inclusive, letting everyone know what's going on, what we hope they will learn, how we want to help them and their families be more secure. We also encourage feedback from our users. This is a safe place for people to share their thoughts. And this helps us make sure we deliver content that they will find engaging and useful, which will continue to drive participation.

SECURITY AWARENESS PROGRAM CASE STUDY

Industry: Insurance
Company size: 5,000 - 10,000
Number of countries: 1

When did you implement your security aw program?
We have had security awareness training and activities of years. In late ate 2014 we brought all of those activities implementing a formal Security Awareness Program.

Can you describe your launch process? Wh you do to bring attention to your efforts?
When we first started our Security Awareness Program, outreach efforts consisted of just a few security related ar month.
In order to draw attention to our security awareness pro garnered the support of several executives to show the ne more involved program. After we received this top level su were able to obtain funding to allow us to purchase conte to help us build our security awareness program.

What sorts of materials and content are yo including in your program?
In 2016, our primary focus has been on educating our pe on email phishing related topics. Although phishing has b effort, we also are trying to utilize all of the SAC- provided that our audiences can learn about anything with a simple button on our internal sites.

What topics are the most important for yo
Currently are most important topic email phishing. Phis currently a hot topic and critical risk based on several high profile companies having data stolen by hackers through attacks. In order to proactively combat this risk, we have b focused on educating our users on how to spot and repor phishing emails.

Do you have a central learning portal of so
Yes we do. Currently we have an internal Learning Mana System that hosts all of our training modules and games, internal SharePoint site that hosts additional content.

How much of your training is mandatory?
Currently we have two mandatory security-related train company. The first is our Annual Security Awareness train required for all employees and contingent workers. The se secure code training, which is required for all developers.

What have you done to encourage employee participation?
The backbone of our program is promoting a fun and interactive program. In order to encourage participation, we routinely host

SECURITY AWARENESS PROGRAM CASE STUDY

Industry: Consulting & Certification
Company size: 12,000+
Number of countries: 44+

When did you implement your security awareness program?
This is still a new program, we launched only a few months ago.

Can you describe your launch process? What did you do to bring attention to your efforts?
It was really important for us to get our president involved, to show that security was important to everyone within the company, from the top down. So the initial launch video was hugely helpful. It included not only an introduction to the key tenants of the program and the materials that users could expect to see in coming months, but also a personal message from the president. We found this to be really helpful in our global offices, especially in Asia where they need to see buy-in from the top down. This video was integral for gaining initial support.

What sorts of materials and content are you including in your program?
We have a monthly newsletter, which includes a global security team update. We've received feedback from our European and North American offices that they find this useful. We haven't gotten much feedback from our Asian offices concerning the newsletter. Also a monthly elearning course. Posters. Videos.
While we have many elearning modules, we still have some instructor-led trainings, especially for workplace violence and active shooter scenarios. A good balance of the two is important to not burn out employees on any one kind of learning.

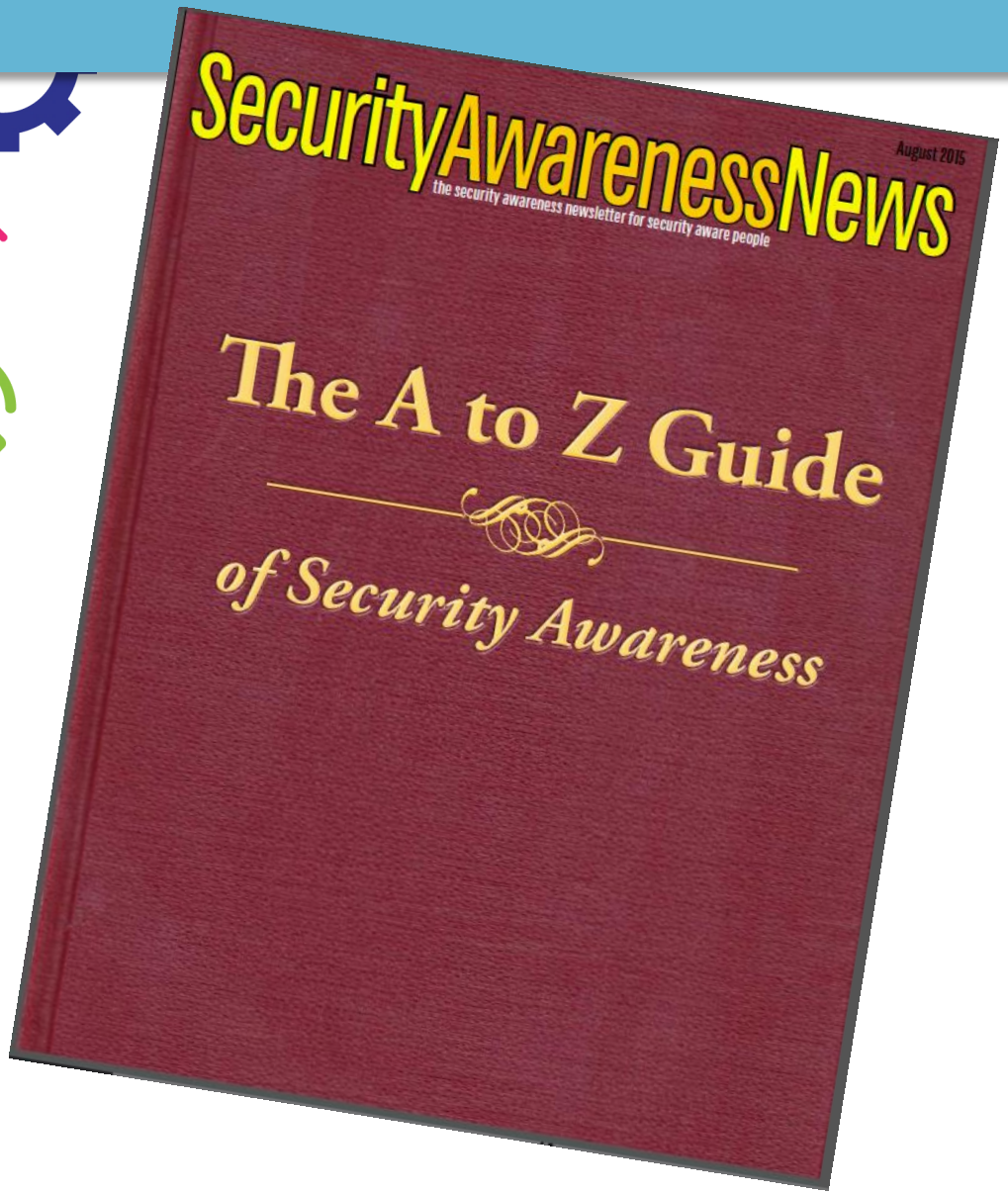
Do you have a central learning portal of some sort?
Yes, we have a Sharepoint site where we put all of the resources and post relevant news and updates. We have linked all of our security policies in one place so employees can report incidents easily from the intranet to save them time and energy.

Is any of your training mandatory?
No, the entire program is voluntary. Our employees already have plenty of other training they have to take throughout the year, so we didn't want to overwhelm them with more mandatory stuff. This is why wee didn't go with the internal L&D department for developing the awareness content. Last year, they had only a 46% participation rate in the training they produced. This year, with our non-mandatory program, we had an immediate 80% participation rate.

What have you done to encourage employee participation?
We've focused on security issues from a personal perspective. By doing this, instead of focusing on the corporate, it shows employees the benefits of following security practices.
We've offered prizes for the best security tip that our program taught them. So they email us something they've learned from one of our courses or videos, and we pick the best one, and that person gets a prize. The prize isn't something big, but something with company branding on it. A mug, a t-shirt. Something small and inexpensive.
If managers see people doing security aware things -- removing papers from the copy room, not allowing tailgating, locking their workstations, keeping neat desks -- they get called out, praised for it, and are rewarded.
Posters are everywhere, in offices around the world, and we ask employees to send photos of the best poster placement -- just using their phones. Where's the most creative place a security poster is hung? Or the place that will be seen by the most people? It encourages a friendly sort of competition and gets people to pay more attention to the posters.
We only push out one course a month, and as it's not mandatory we just say "this is something you might be interested in, take a look when you have some time." Since we use short, engaging courses, people are generally interested. They can find five or ten minutes a month to spare to take a course. And if they don't do it this month, that's okay, they might do it next month.
The badge and leaderboard system is useful too. People seem to like that -- having a way to see their progress, see where they rank compared to their colleagues, earning little marks of completion along the way.

How do you maintain momentum and keep people interested?
We send out a weekly email from the president -- again, showing interest in security from the top down -- that talks about security and the importance of being security aware at work.
We definitely believe in the carrot method. There's no stick here! We try to remain transparent and inclusive, letting everyone know what's going on, what we hope they will learn, how we want to help them and their families be more secure. We also encourage feedback from our users. This is a safe place for people to share their thoughts. And this helps us make sure we deliver content that they will find engaging and useful, which will continue to drive participation.

Security Awareness Newsletters



Security Awareness Cheat Sheets

Small-Medium Company Security Risks on the Rise

The British Home Office and Cabinet Office are appropriately warning small- to medium-sized companies that they are now at an increased risk for attack and that it's time to build their cyber defenses!

What should we learn from this?

- Smaller companies are often easier to successfully attack because of limited security awareness and technical resources.
- Small companies are ideal "stepping stones" to launch larger attacks.
- Penetrations of small companies' networks can go unnoticed for years.
- A database of 100,000 names is just as desirable to cyber criminals as one with 100 million. It's all a numbers game.

CONSIDER: Cyber attacks from outside the business often occur as a result of information gleaned from Social Engineering. An example of this, social engineering can include phishing emails that attempt to trick users to open an attachment that includes some type of exploit or payload. Social engineering techniques include showing up dressed as delivery people, tech support, corporate attorney, salespeople, job applicants—you name it and it probably had been attempted and likely been used successfully somewhere.

The U.K. government's Cyber StreetWise program (https://www.cyberstreetwise.com/) released some disturbing revelations about the mindset of small business owners:

2 out of 3 don't consider their business to be vulnerable.

Only **16%** say that improving their cyber security is a top priority for 2015.

78% of those surveyed believed at least one of these potentially disastrous myths:

- Only companies that take payments online are at risk of cyber crime.
- Small companies aren't a target for hackers.

Last year **one-third** of small businesses suffered a cyber attack from someone outside their business.

They All Look Alike

Detroit Lions linebacker Kyle Van Noy retrieved the wrong laptop from security at the Salt Lake City International Airport last week. He had, in error, picked up an elementary school teacher's identical machine. A lot of computers look alike, so keep this from happening to you by making yours unique! Add stickers, design a colorful sleeve, or try making your mobile devices "ugly" in the eyes of a thief. In the words of one security expert, "*Your technology should not be about bling. It should be about performance and utility. My gorgeous Apple MacBook Air is sinfully ugly so no one would ever steal it, and I can spot it from 100 meters.*"

Outbreak!

Fake discount vouchers are only one of the latest attacks against mobile devices. It's called **Smishing**, or **SMS Phishing**. Users will receive a text that looks like it comes from a retailer with a significant discount or coupon code. *Just click to redeem!* This attack is often well-crafted, but if you click the link, your device will become infected with mobile malware. And different versions are constantly evolving; one version causes your device to become part of a larger network of malware distribution!

You have been randomly selected for a BestBuy gift. Get your $1000 gift card at www.bestbuy.com.youre-a-winner.net/?id=ichfcvlck

Dear Walmart shopper, Congratulations you hav just won a $1000 Walmart Gift Card. Click here to claim your gift. www.WmartClick.com (cancel: reply STOP)

Congratulations, your number has made you Apple's winner of the day! Go to http://www.apple.com.au.txtaprize.com and enter code: 9750 on last page to claim

Security Awareness Posters

Gone With the Wind Posters

What is a Man in the Middle Attack? Poster

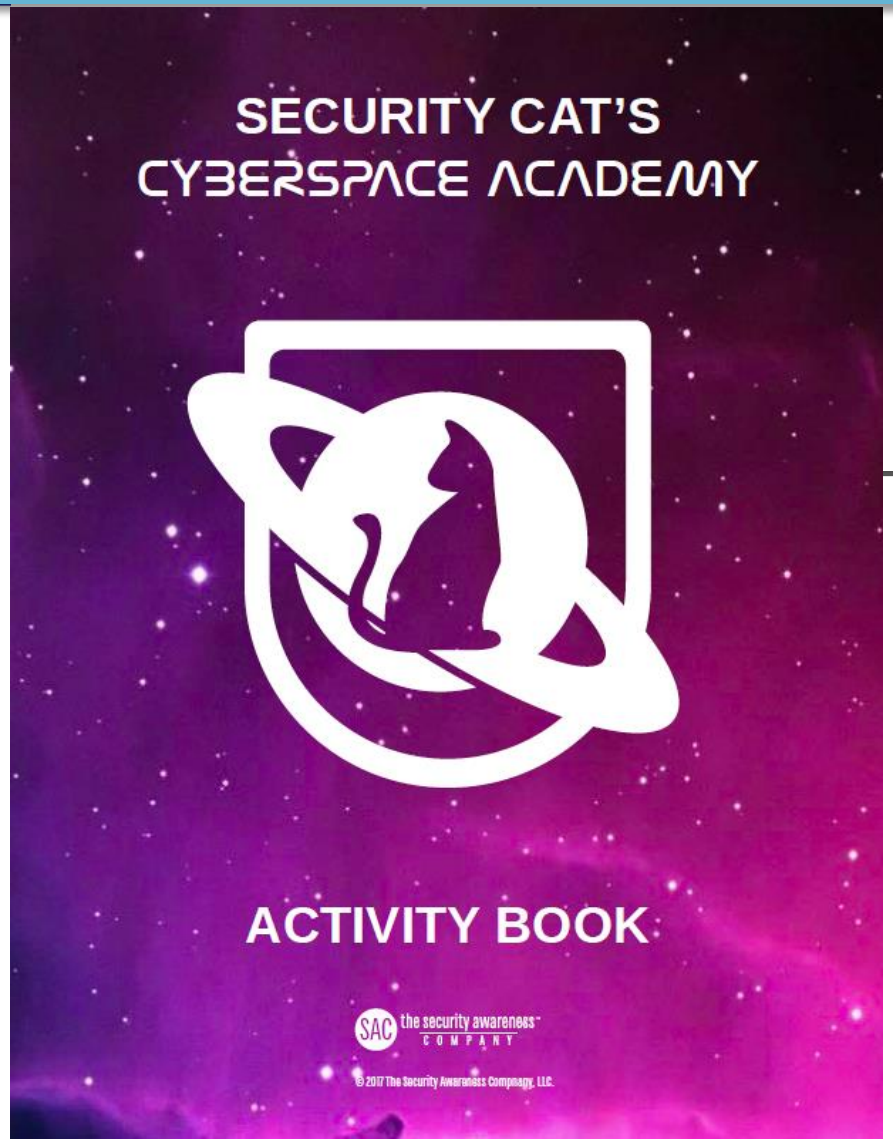
Are You A Reckless Surfer? Poster

Safe Surfing Tips & Tricks Poster

VPN Scene Poster

Hard to Guess Password Poster

Security Awareness Activity Book



CYBER CRYPTOGRAM

You just received your daily motivational message from High Command, but something went ha
and the message is all mixed up. Decode the message below. Record each letter in the box as y
figure out which letter it has replaced. (Solutions are in the back of the book.)

ALIEN PHISH

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
																S							

K J N K U L D C S C I V K U I J V J N C

G V V U F C R Z T Q C K J Q K U J N C

MISSION LOGIC

DATA BREACH ATTACKS

Four space ships have found themselves the victims of data breaches. Each one was attacked in a different method, while travelling through different sectors, and losing an astonishing number of records. Can you match the space ships with the number of lost records, the type of attack and the star date of breach from the following clues? (Solutions are in the back of the book.)

1. The four data breaches were: the one that lost 10 million, the one that took place latest in the star date, the Ransomware attack, and the one that hit the S.S. Tabby.
2. The USB attack happened before the S.S. Bobtail got breached, which was before the 101 million records were lost. The USB drop did not result in the loss of 85 million records.
3. The last data breach did not lose 30 million records nor happen to the S.S. Sphinx.
4. The social engineering attack took place before the S.S. Tabby was breached, and did not result in the loss of 85 million records.

		SPACE SHIP				ATTACK TYPE				RECORDS LOST			
		S.S. Tabby	S.S. Bobtail	S.S. Bengal	S.S. Sphinx	Ransomware	Social Engineering	Spear Phishing	USB Drop	10 Million	30 Million	85 Million	101 Million
STAR DATE	One												
	Two												
	Three												
	Four												
RECORDS LOST	10 Million												
	30 Million												
	85 Million												
	101 Million												
ATTACK TYPE	Ransomware												
	Social Engineering												
	Spear Phishing												
	USB Drop												

SPACE SHIP	RECORDS LOST	ATTACK TYPE	STAR DATE

CYBER SYLLACROSTIC

Fill in the answers to the clues by using all of the syllables below. The number of syllables to be used in each answer is shown in parentheses. The number of letters in each answer is indicated by the dashes. Each syllable will be used once. (Solutions are in the back of the book.)

A AL BA BER CA CAL CI CIAL CON CRIME CRYP CY CY DGES
DEN DENT DENT DIS EN EN ER FAC FI FI FI GI HI I I I I IN
ING LOCK MAL MOUSE NEER NESS NI NON O PAA PO POL PORT
RAN RE RE ROR SAL SCREEN SO SOM TECH TI TI TION TION
TOR TWO TY VER WALL WARE WARE WARE

1. Keeping secrets a secret (7) _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
2. Compliance mandate that regulates protected health information (2) _ _ _ _ _ _
3. Technique to see the real URL under a link (3) _ _ _ _ _ _ _ _ _ _
4. A more secure form of authentication (3) _ _ _ _ _ _ _ _ _ _ _
5. Human attack using non-technical methods (6) _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
6. Not just viruses anymore (2) _ _ _ _ _ _ _ _
7. Crucial to know and follow this at all times (3) _ _ _ _ _ _ _
8. This is one of the most common causes of data breaches (2) _ _ _ _ _ _
9. Passphrase or PIN (2) _ _ _ _ _ _ _ _ _ _ _
10. Physical identification (2) _ _ _ _ _ _ _ _
11. Prevents destructive/hostile data from crossing a cyber barrier (3) _ _ _ _ _ _ _ _ _
12. See something? Say something! (2) _ _ _ _ _ _ _
13. Shredding (3) _ _ _ _ _ _ _ _ _
14. Simplest method for protecting information (3) _ _ _ _ _ _ _ _ _
15. Malware that locks your computer and demands money to open it (3) _ _ _ _ _ _ _ _ _
16. Ransomware, identity theft, data breaches, oh my! (3) _ _ _ _ _ _ _ _ _
17. User login (6) _ _ _ _ _ _ _ _ _ _ _ _
18. Physical (4) _ _ _ _ _ _ _ _ _ _ _ _
19. Report this (3) _ _ _ _ _ _ _ _ _
20. A full-time job that is our collective responsibility (3) _ _ _ _ _ _ _ _ _

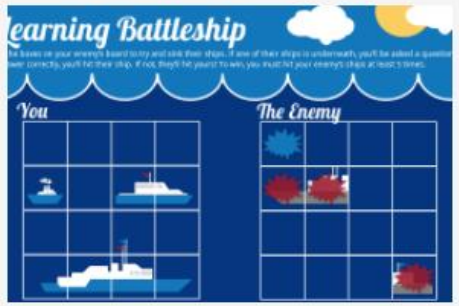
Security Awareness Games

Game: Password Shootout Challenge

Is it a Phish? Secret Mission

Game: Spooktacular Trivia for Kids

Game: Spooktacular Trivia



Game: Internet Security Battleship

Game: Alpine Skiing – Human Firewall

Security Awareness Videos

Mobile Browser Attacks Video

I'll Be Stalking You

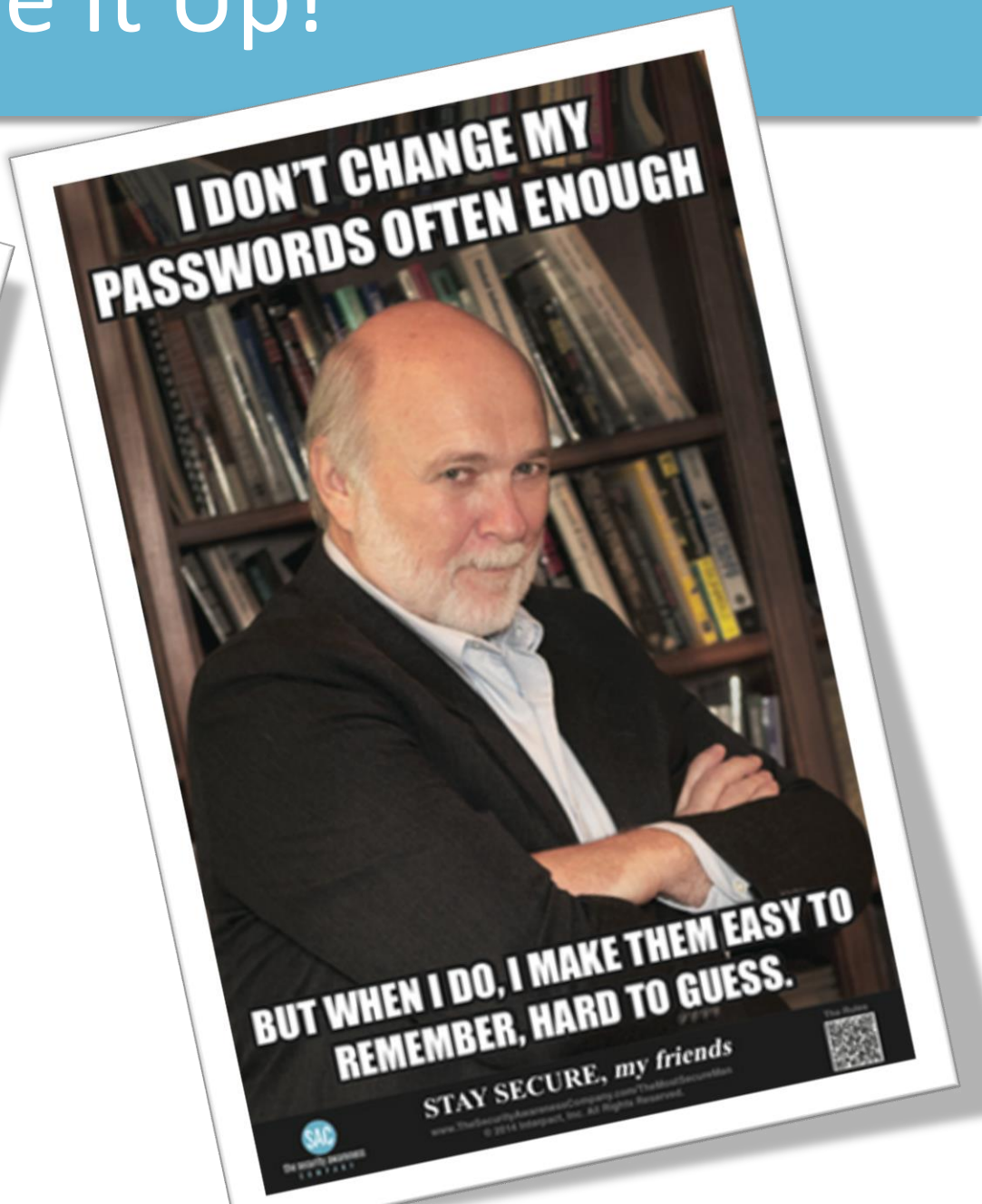
Thinkin' 9 to 5

Hacker's Paradise

Security Cat's™ Guide to Social Media

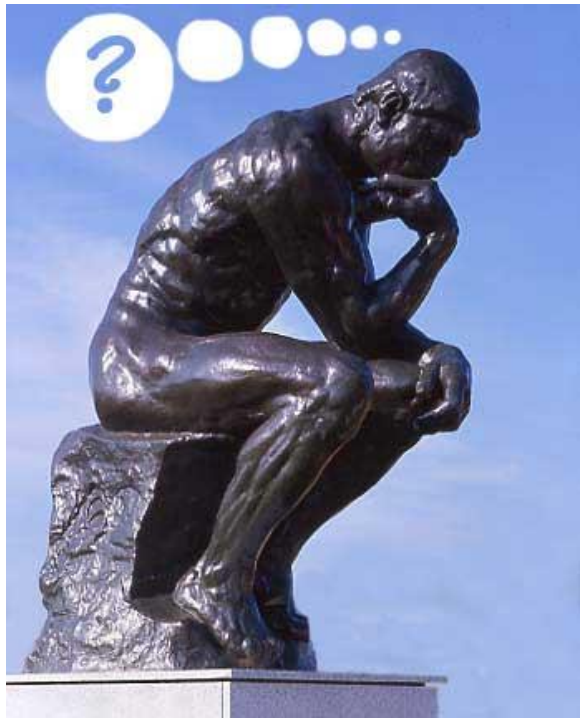
Security Cat's™ Guide to Fighting Cybercrime

Have Fun! Meme It Up!



Say YES! To Security Cat™!

Comments? Questions? Responses?



Winn Schwartau

Founder & Chief Visionary Officer

1.727.393.6600

winn@thesecurityawarenesscompany.com

DO NOT USE FROM HERE ON

Comments? Questions? Responses?

Find my slides on LinkedIn SlideShare!

https://www.slideshare.net/winnschwartau/how-to-make-your-security-awareness-program-fail

Look out for an email from us with a recording of this webinar inside!

Winn Schwartau

Founder & CEO

1.727.393.6600

winn@thesecurityawarenesscompany.com

The Security Awareness Company

www.thesecurityawarenesscompany.com

facebook.com/TheSACo

twitter.com/@SecAwareCo

linkedin.com/company/the-security-awareness-company

Kayley Melton

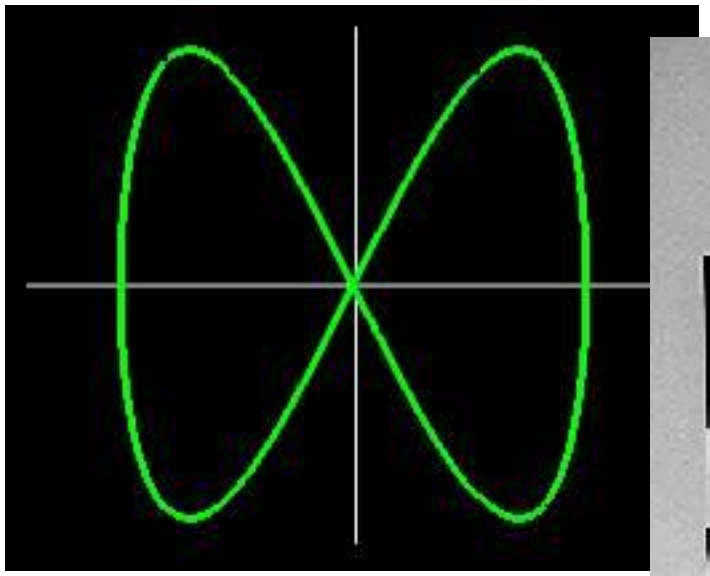
Founder & CEO

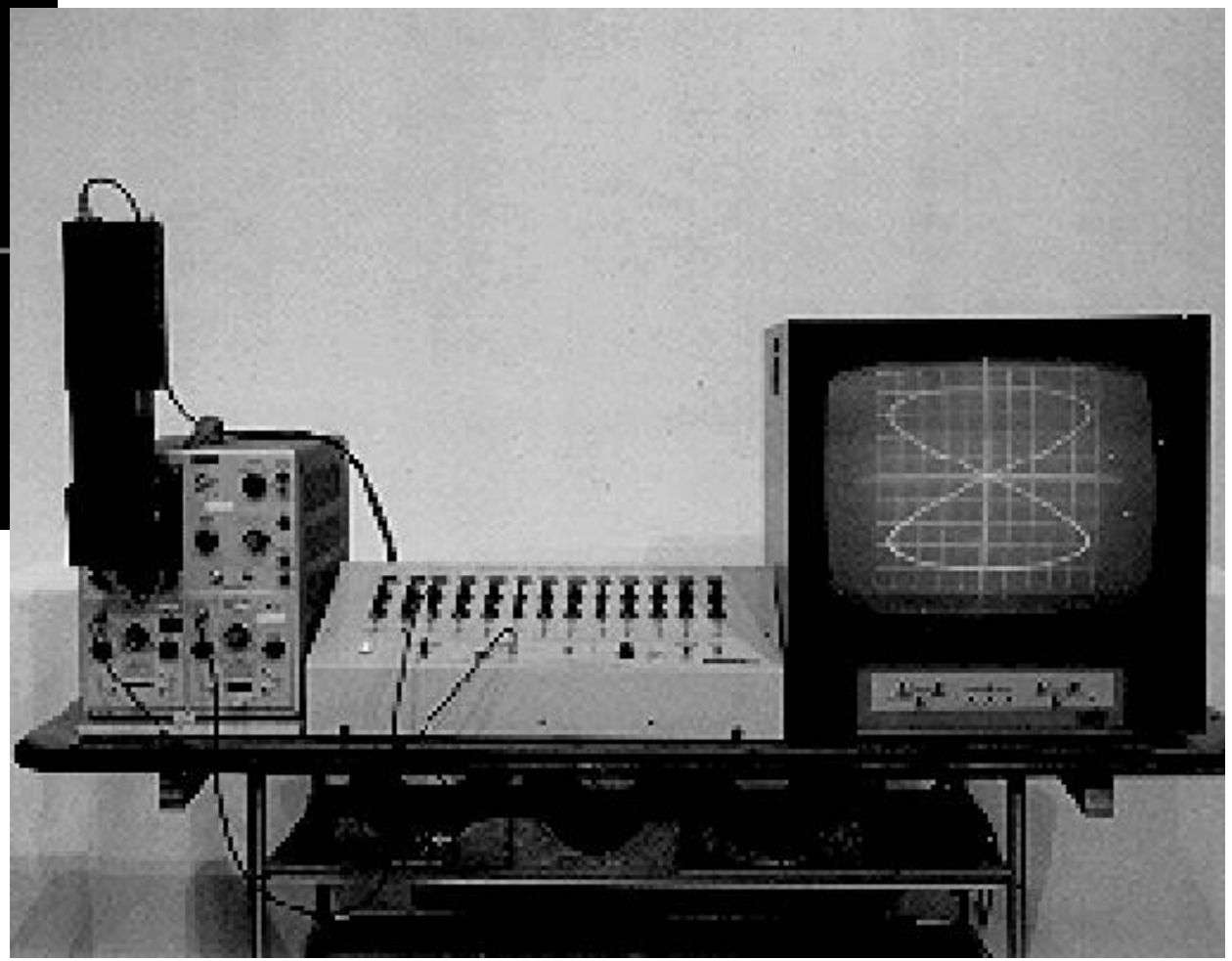
kayley@thesecurityawarenesscompany.com

Reach out to us via email

TV:Movies - Auto Sync (Right!)

And When It Fails - The Show Must Still Go



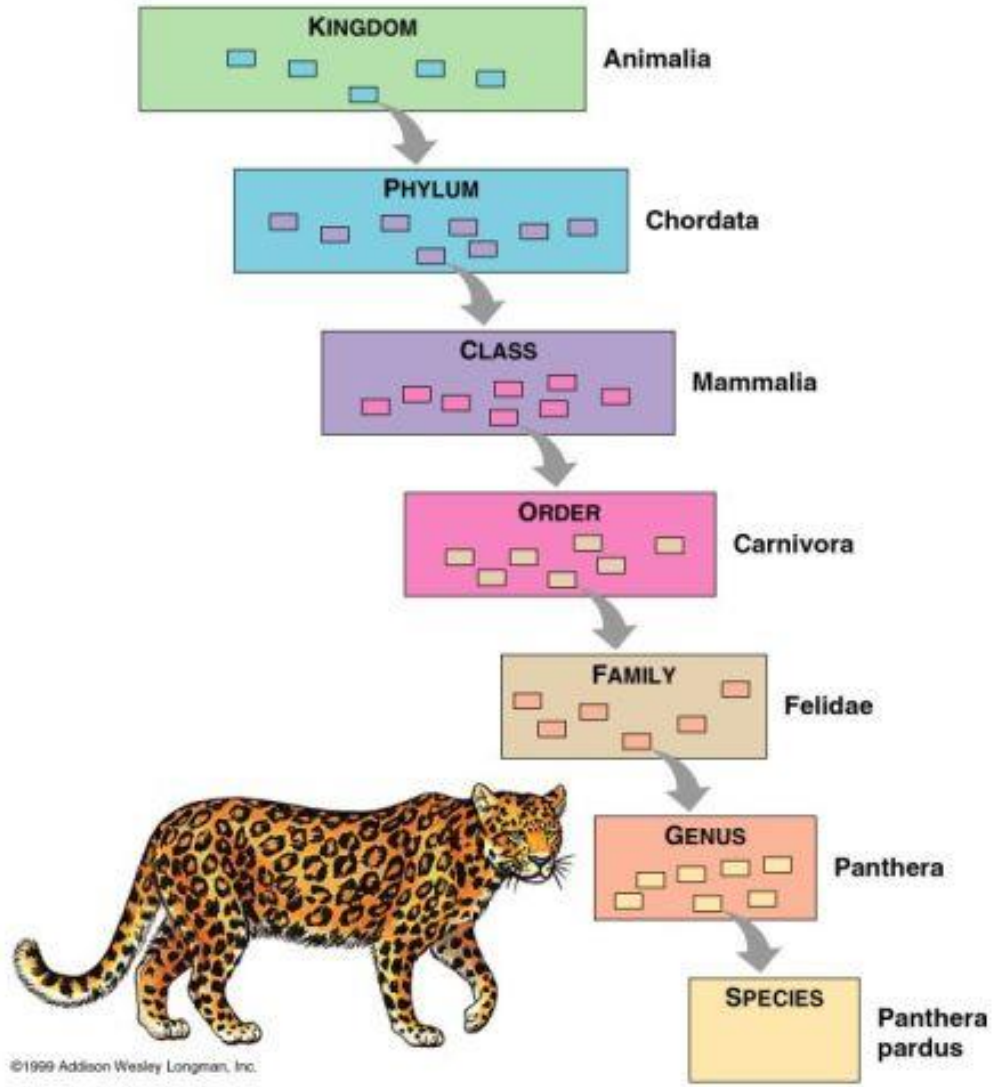


Taxonomy? Huh?

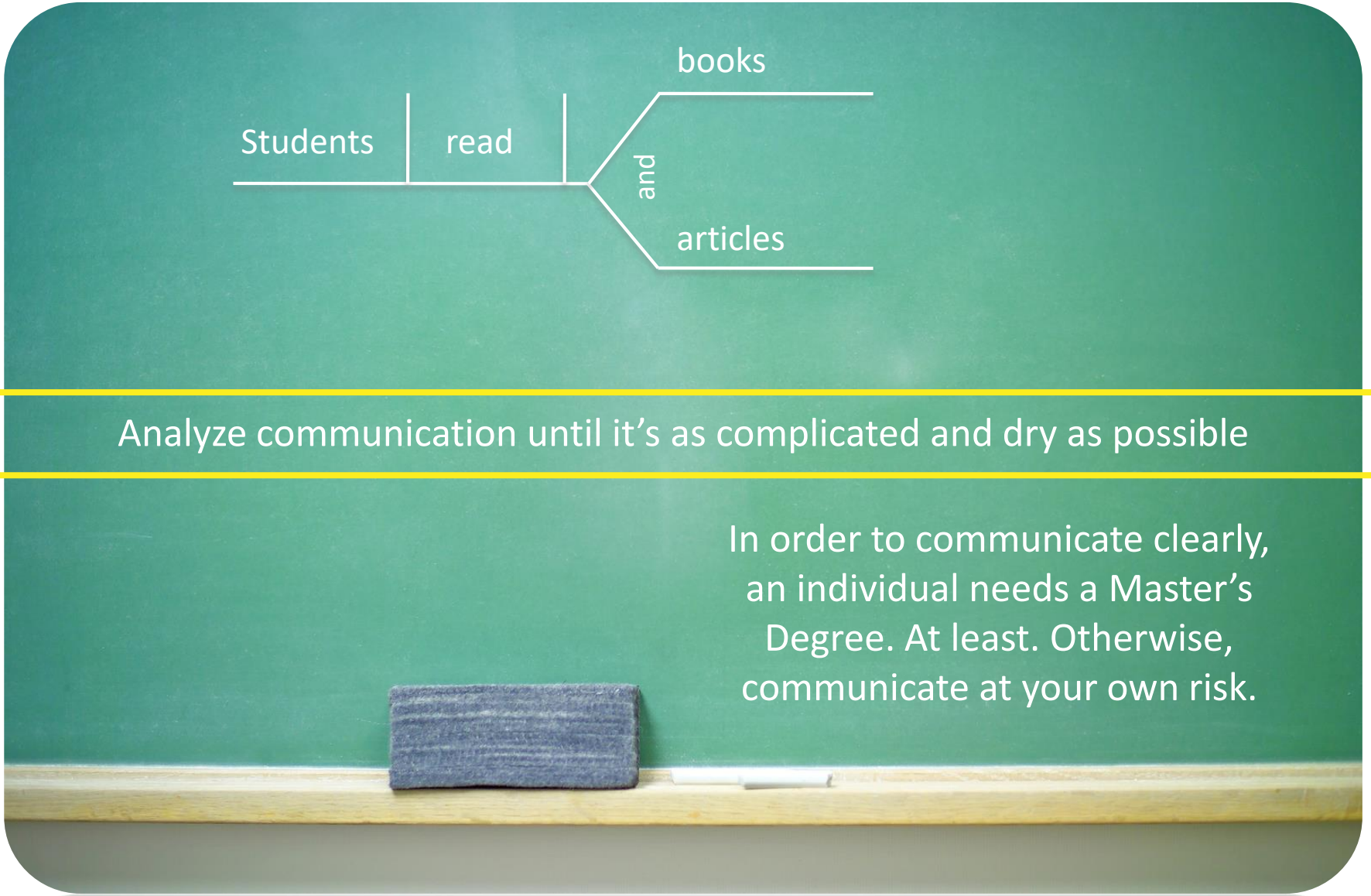
Periodic Table

Learning/Knowledge Maps

Dewey Decimal System



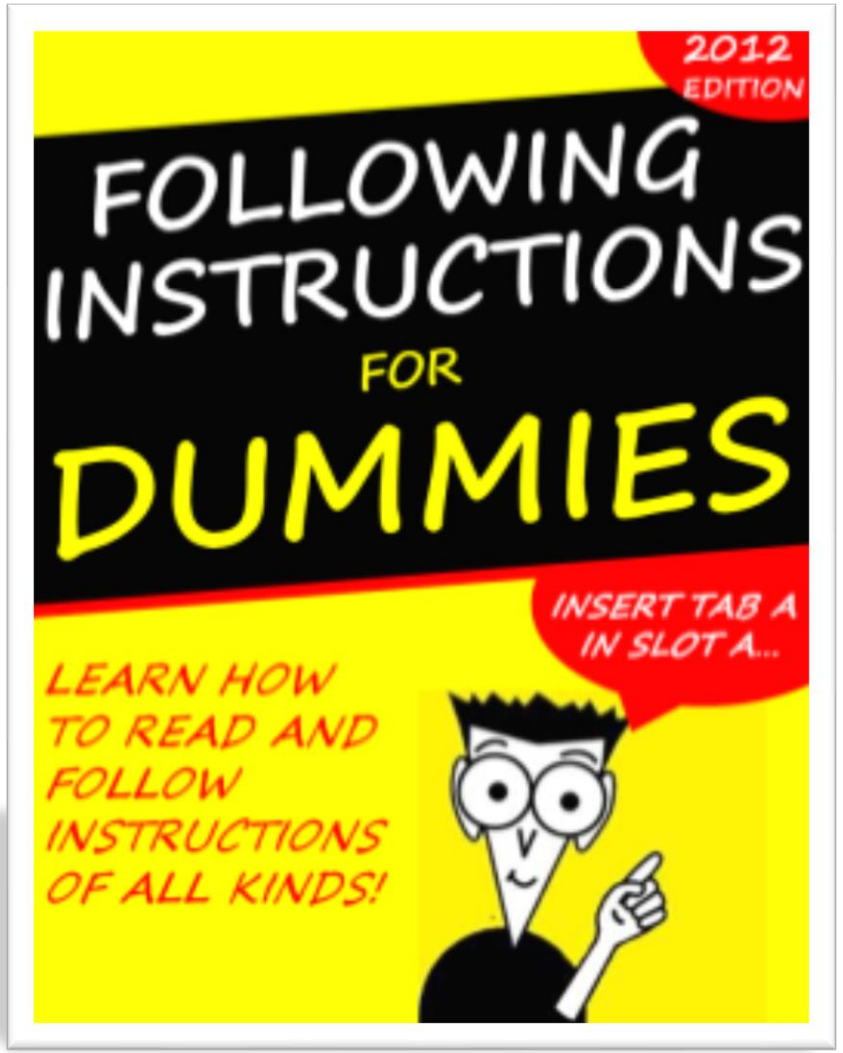
Hire An English Major & Parse



Analyze communication until it's as complicated and dry as possible

In order to communicate clearly, an individual needs a Master's Degree. At least. Otherwise, communicate at your own risk.

Do Not Violate The Formal or Structured Instructional Process



Complicated instructions ensure the most secure programs

Standards should be rigid and require an instructional consultant

Testing Is Absolutely Reliable and Accurate

Everyone who passes the test knows how to behave when a security event occurs.

Make tests super easy so everyone gets an ‘A’ and the auditors are happy.

Security Awareness Program Planning Guide.

Any security issue or event fits into at least one of the open cells.

Some may fit into more than one.

	Confidentiality	Integrity	Availability	Physical	Cyber	People	Professional	Personal	Mobile
Confidentiality									
Integrity									
Availability									
Physical									
Cyber									
People									
Professional									
Personal									
Mobile									

Confuse Awareness With Training

Coke obviously wastes $3B/yr. on global brand awareness

Repetitive multi-media branding is useless. It doesn't change behavior.

Brilliant marketing is a myth. Don't buy into the hype.