State of Awareness and Training – Then vs. Now

Lessons from Cracking the Enigma

John G. O'Leary, CISSP

O'Leary Management Education

Abstract

- Way back in the late 1930's and early 1940's the British (and a few Americans) at Bletchley Park, an old mansion about 50 miles outside London, broke multiple supposedly unbreakable German encryption codes, primarily those created for the also "uncrackable" Enigma machines. A highly dedicated group of unconventional warriors worked ungodly hours to unravel the codes and kept their efforts secret from even their closest friends and relatives. They succeeded, and their work is thought to have shortened the War by up to two years and saved countless lives.

Abstract

- In March 2010, we're trying to break what sometimes seem to be unbreakable behavior patterns by designing and implementing role-based awareness and training programs for people at all levels of our organizations. Are there things we can learn from the efforts at Bletchley that can carry over to our mission today? We'll examine what they did and how they did it to find out. Sure, it's going on 70 years later, but there are possibly surprising parallels and some real lessons for us as we develop and implement role-based awareness.

Speaker Bio

John G. O'Leary, CISSP, is President of O'Leary Management Education. A computer security practitioner since the 1970's, he has designed, implemented, maintained and managed security for networks ranging from single-site to multi-national, LAN to WAN; including client-server environments connected to the Internet, Intranets, Extranets, Websites, each other, and who knows what else. His background spans programming, systems analysis, auditing, project management, operations and quality assurance, with requisite doses of harmonious, rewarding teamwork and savage corporate infighting. John built and taught one of the USA's first graduate-level university courses in Computer Security at the University of Texas at Dallas in 1976. He has trained tens of thousands of computer security practitioners worldwide in multiple aspects of the field. He is the winner of the 2004 COSAC Award and the 2006 EuroSec Prix de Fidelite.

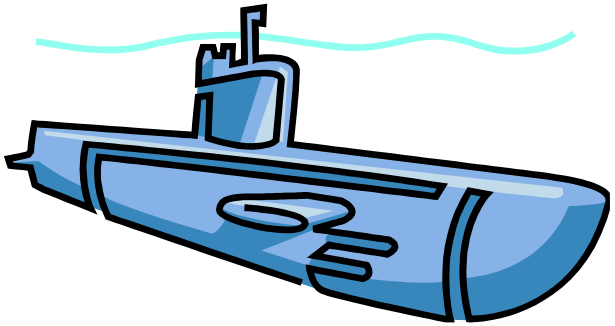
He has even set up and installed encryption hardware in a working US nationwide production network without bringing it *completely* down.

Agenda

- Threats
- Agencies
- Organizations
- Acts
- Documents
- Practices
- Countermeasures
- Lessons from Breaking the Enigma

Threats

- ***For Cracking the Enigma***



- Invasion of Britain
  - Appeared imminent,
  - Germans were right across the channel
- U-Boat wolfpacks sinking supply convoys
  - In WWII, sank 60% of British shipping
  - Killed 50,000 British merchant seamen
- Axis domination of Europe
- Losing the War

Threats

- ***For Role-based Awareness Now***
- Not quite as dire, but getting more serious every day
- Cyber attacks against government and infrastructure sites (possibly by governments)
- Rapidly changing threat profiles and roles
- Economic, political, media realities
- Role complexity

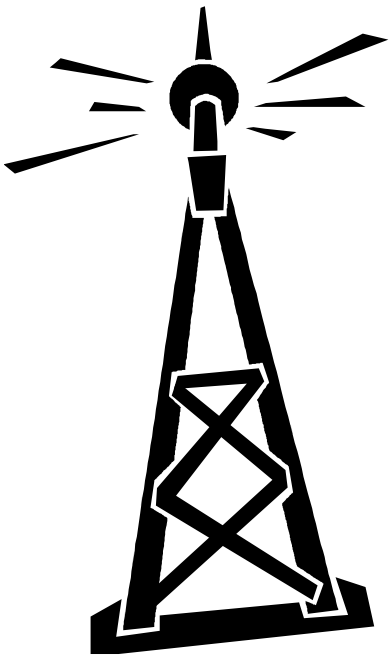
Agencies

- ***For Cracking the Enigma***
  - GC&CS – Gov't. Codes and Cipher School
    - name to hide real mission (Golf, Cheese and Chess Soc.)
    - Cherry-picked from Universities, foreign service, etc
    - Good old boy network, lawyers, math geeks, idle rich
    - Army, Navy, RAF; active and retired
    - Aussies, Canadians, Kiwis, etc. (British Empire)
  - American "Cousins" from Arlington Hall
    - Precursor to NSA, Yanks there part of first nucleus
  - Assorted (but carefully vetted) anti-Nazis

Agencies

- ***For Role-based Awareness Now***
  - NIST, DoD, DHS, NSA, OIG
  - OMB, Treasury, Interior
  - GSA
  - All the agencies represented at this conference
  - Any agency giving guidance and/or doing things similar to our mission and activities
  - Helping each other is key

Organizations



- ***For Cracking the Enigma***
  - Wireless receiving stations all over Britain
  - “Y” Stations in Britain and abroad
  - Polish codebreakers who gave crucial (but simple) rotor letter arrangement data just before the Nazi invasion
  - British military infrastructure around Bletchley Park (secret was kept all through the war, though over 12,000 people worked at Bletchley)

Organizations

- ***For Role-based Awareness Now***
  - FISSEA (of course)
  - ISACA
  - ISSA
  - ISC2
  - ISO
  - And vendors of Awareness and Training items

Acts: Breaking the Enigma

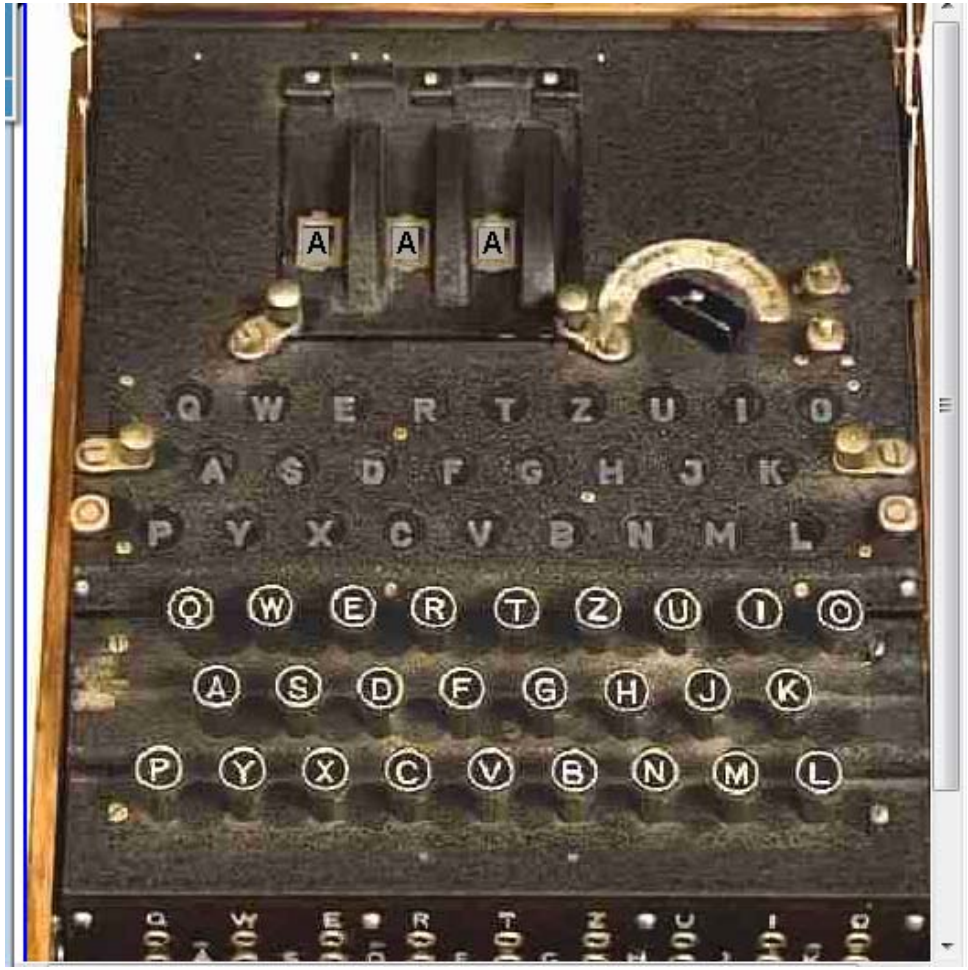
- The Enigma
- Bletchley
- Unconventional Warriors
- Breaking the boxes
- Breaking the codes

The Enigma

- 1918 original vintage
- First used for railroad communications
- Wiring, rotors, lights, setting wheels gave mathematical complexity
- Germans later added “steckers” – plug-in cables to map one letter to another
  - Order of magnitude increases in complexity
  - But also a critical flaw
    - No letter can map to itself

Enigma Box

3-Rotor Enigma



Bletchley Park

- About 50 miles North of London
- Not too close to be accidentally bombed
- Rickety old mansion and grounds
- Stables and garages and huts for the grunt work of deciphering

Bletchley Park

Bletchley – Turing's Hut

Very British

Working Huts at Bletchley

Huts at Bletchley

Bletchley

- Germans never knew what was going on there
- Never got targeted by German bombers
- Almost hit once accidentally, in area where raw messages were bicycled in

Bletchley Park

- Different Huts for different functions
  - Luftwaffe
  - Army
  - Navy

Unconventional Warriors

- Alan Turing
  - Painfully shy, homosexual
  - Recognized mathematical genius
  - Monumental contributions to electronic computing
  - World class distance runner
  - Bicycling around Bletchley in a gas mask
  - Later took his own life via a poisoned apple (a la Snow White)

Alan Turing in 1946.

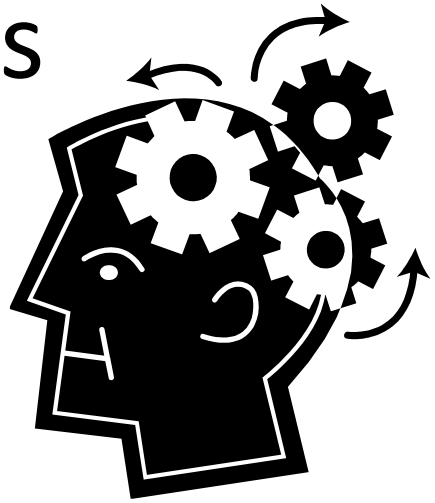
Unconventional Warriors

- Alfred Dillwyn “Dilly” Knox
  - Classics scholar at Kings College Cambridge
  - WWI cryptanalyst (Room 40)
  - Responsible for the early British attempts to break Enigma
  - Created “rodding” – a linguistic, not mathematical technique to break non-steckered Enigma early in the War (good description in Wikipedia)
  - Died in Feb 1943

Unconventional Warriors

- Female Cryptanalysts
  - To their credit, the codebreakers at Bletchley cared more about brainpower than gender
- Puzzle enthusiasts, Oxford Dons, linguists, musicians, Olivia Newton-John's father (Australian AF), …
- Americans from "Arlington Hall" – later some of the base group for NSA
- Remarkably, all kept the secret

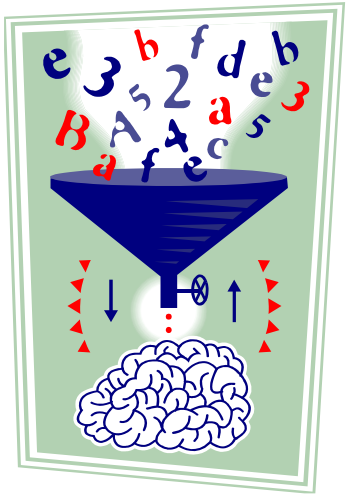
Breaking the Boxes



- Great help from the Poles
- Initial wiring of the rotor wheels
- A, B, C, D, E, F,…..
- But even with that, the Germans changed the settings each day and for each message (usually)

Breaking the Boxes

- British found ways to turn some of Enigma's strengths into weaknesses
- Stecker system
- Vastly increased number of possible mappings, paths, solutions
- But a letter could not map to itself
- So the cryptanalysts had one leg up on figuring out the machine



Breaking the Codes

- Used whatever was available
- Weather reports
- Daily status reports
- Look for patterns in seemingly random data
- Hours upon hours upon hours
- “Your brain felt raw” said one codebreaker

Breaking the Codes

- New settings every day, week, month
- So codebreakers had to start over
- Race to get “into” the code
- Incredible stamina and concentration

- Gardening – false messages on location of naval mines, etc., to get a transmission that could be decoded

Captured German Navy Codebook

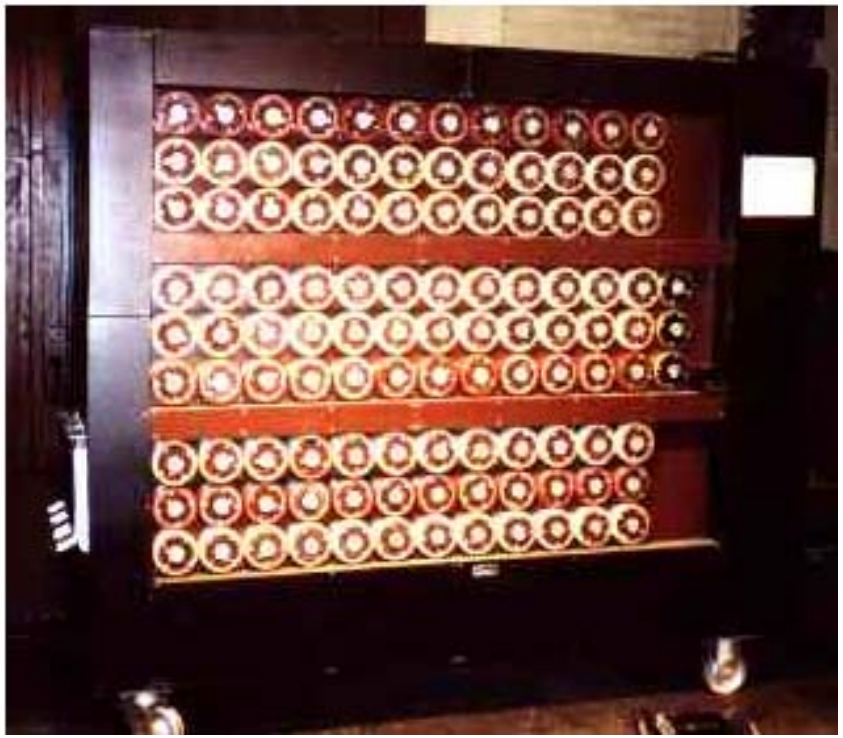
Despite the movies, it was really the British who captured this German U-boat codebook, not Matthew McConaughey

Captured Luftwaffe Codebook

- Mentioned by one of the lady codebreakers
- Burn marks and ashes around the edges of pages
- She was somewhat disturbed because there was a large bloodstain on the codebook
- And it was still wet

A Bombe

This one being rebuilt at Bletchley by Tony Sale and his colleagues. Original built by Tommy Flowers, an engineer with the British Postal System.



Workings of the Bombe

- Similar to what cryptanalysts do today
- Analyze to find what you know or strongly suspect is true
- Reduce the solution space by eliminating those entries that couldn’t possibly be correct (usually via multiple resets and runs of the bombe)
- Brute force and experiential insight through remaining possible solutions

Acts

- ***For Role-based Awareness***

- That's why we're all here
- Will be covered throughout this conference

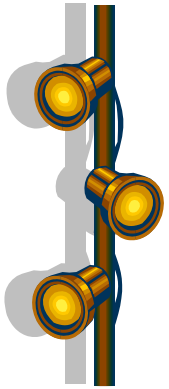
Documents

- ***For cracking the Enigma***

- Might be unbelievable to us in 2010, but …
- All were burned at the end of the War
- Schematics for the bombes also hit the fire
- And the machines were dismantled
- Bletchley's role stayed secret for years

Documents

- ***For Role-based Awareness***



- FISSEA shines a spotlight on the latest information and guidance
- Will be covered throughout the conference

- And I hope you won't have to decrypt them

Practices, Countermeasures

- Again, stay tuned for the next three days
- Focus area for this FISSEA conference

Lessons Learned

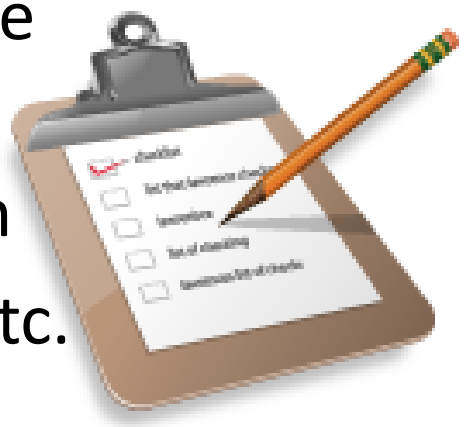
- ***Support from the Top is crucial, but must be used sparingly***
  - Winston Churchill made it clear that Bletchley could have whatever they wanted whenever they wanted it as quickly as it could be provided
  - Dilly Knox and other leaders there were wise enough to not overplay that card

Lessons Learned

- ***Support from the Top is crucial, but must be used sparingly***
  - *What support do you expect from your hierarchy regarding role-based awareness and training?*
  - *How will it be rationed?*
  - *How can you avoid overdoing support requests?*

Lessons Learned

- ***Must produce clear deliverables***
  - Atlantic convoys saved
  - Rommel's supply lines cut through the Mediterranean
  - Monty beating Rommel at El-Alamein
  - Italian Navy destroyed at Matopan, etc.



  - were attributable to GC&CS

Lessons Learned

- ***Must produce clear deliverables***
  - *What specific role-based awareness and training results do you expect to produce?*
  - *Are they measurable?*
  - *Does management agree that these are the correct deliverables?*
  - *What are the fallback positions if these are unattainable?*

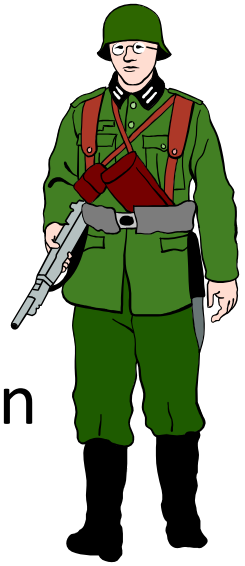
Lessons Learned

- ***Get help wherever you can***
  - Denizens of Bletchley included some decidedly unmilitary types
  - But math geeks, crossword puzzle aficionados, musicians, diplomatic corps officers, etc., were well-suited for the job of monitoring, rationalizing, decrypting and understanding enemy communications

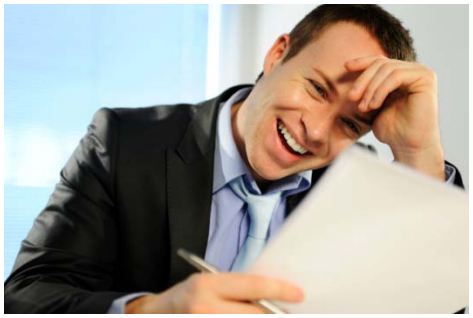
Lessons Learned

- ***Get help wherever you can***
  - *What areas do you perceive to be problematic?*
  - *Who can you ask for help in those areas?*
  - *Any non-standard sources for information and guidance?*
  - *How far ahead of time do you need to let them know you might be seeking help?*

Lessons Learned



- ***Understand the Specifics of the Roles***
  - German Enigma operators were enlisted men
  - Very well-trained in their specific tasks
  - Initiative and creative thought were not called for, expected or even appreciated
  - They followed orders, precisely as prescribed … most of the time
  - This made them very predictable



Lessons Learned

- ***Understand the Specifics of the Roles***
  - *Which roles in your agency require the most training and awareness activity?*
  - *How well do you understand the specific actions required for those roles?*
  - *How will the security changes you'll recommend affect the employee's ability to perform the role up to required standards?*
  - *Will the expected role output standards change with the implementation of your new security measures?*

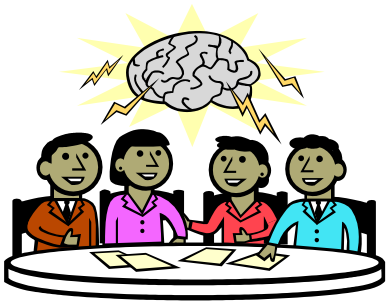
Lessons Learned

- ***Understand the Characteristics of the People Filling the Role***
  - Walter and Klara (initial settings – WAL KLA)
  - "Didn't get that" "OK, I'll send it again" with no change in rotor positions for a massive message
  - Every message starts and ends with "Heil Hitler!"
  - Status report at 1702, weather at 0714 promptly each day in the same format
  - Bletchley codebreakers got to recognize the "fist" of individual operators

Lessons Learned

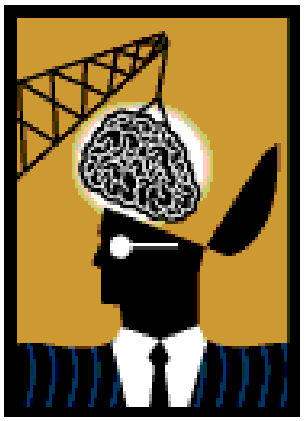
- ***Understand the Characteristics of the People Filling the Role***
  - *Is there a dominant profession in the specific role?*
  - *Is there a way of thinking and problem solving associated with that profession?*
  - *Do any of your role-based security awareness and training activities violate profession norms or challenge profession thought patterns?*
  - *… Same questions for organizational culture*

Lessons Learned



- ***Perseverance and Focus Can Overcome Formidable Obstacles***
  - Enigma and the German procedures accompanying it formed the most complex encryption system derived at that time
  - Even with hints and clues and small breakthroughs, it was a massive effort to make sense out of the transmissions
  - Sinking convoy ships and nightly bombings of English towns focused attention very effectively

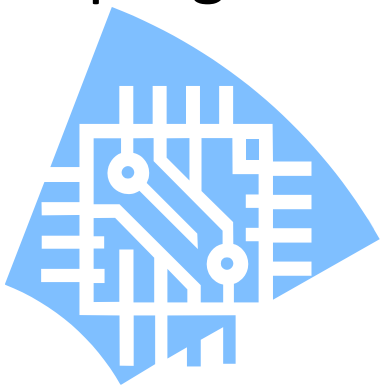
Lessons Learned



- ***Perseverance and Focus Can Overcome Formidable Obstacles***
  - *What roadblocks or potholes do you foresee in your role-based awareness and training efforts?*
  - *What strategies have you used to overcome similar obstacles in the past?*
  - *In what areas must you persevere, no matter how hard the road?*

Lessons Learned

- ***Use All Available Technology; If None Available, Invent Some***
  - Sheets with holes punched into them (Jeffrey's)
  - Sliding matrices of potential solution letters
  - No computers available, hadn't been invented yet
  - So build some, and in so doing move progress significantly ahead for computing



Lessons Learned

- ***Use All Available Technology; If None Available, Invent Some***
  - *What measurement software is available?*
  - *What role-based training technologies are you able to bring to bear?*
  - *What new techniques, hardware, software, gadgets, etc., can you ask contractors and vendors for?*

Final Words

Smile

The role-based security controls you are proposing really will help our Agencies and people

Persevere

Even brick walls crumble over time, particularly when some incident speeds the process

Be enthusiastic

Your own enthusiasm and positive attitude are highly contagious

Final Final Words

- Role-based awareness and training is not an enigma
- Your
  - Sense
  - Smarts
  - Creativity

  Will get the job done

Thanks for listening … now, go get ‘em