10 COMMON ROADBLOCKS TO IMPLEMENTING SE AND POTENTIAL SOLUTIONS

© 2019, Kansas Legislative Division of Post Audit
OVERVIEW / OUTLINE / AGENDA

- Kansas Shout Out
- Social Engineering 101
- Timeline of Kansas' Recent Journey through SE
- 10 Common Roadblocks and Potential Solutions
- Learn from Our Mistakes
- Q & A
KANSAS SHOUT OUT
KANSAS AUDITORS SAY HEY!

- Est. 1971, first audit 1972
- Legislative Agency, performs at direction of LPAC
- Office of ~25 audit staff, who conduct performance audits
- IT Audit Team – 3 (and one manager)
  - Existed since 2010
  - ~ 6-8 IT security audits per year of state agencies, boards, commissions, etc.
  - Project monitoring work
  - Accounted for¹
    - 17 of 37 (46%) of published reports/memos in 2018, including 7 IT security audits
    - 6 of 16 (38%) of published reports in through Sept. 2019 (all IT security audits)

¹. per kslpa.org Archived Audit Library
SOCIAL ENGINEERING 101
SOCIAL ENGINEERING 101 - WHAT IS IT?

- **Def.** - the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.
  - Per [https://www.lexico.com/](https://www.lexico.com/)

- In other words, someone lying to get someone to tell them something they shouldn’t or gain access to something they shouldn’t.
SOCIAL ENGINEERING 101 – COMMON TYPES

- **Quid pro quo** – “Tell us your password and we’ll give you free lunch!”

- **Phishing** – Email with bad link(s) “You’ve won $10,000,000. Click here to enter your info so we can send you the check.”
  - **Spear phishing** – Same as phishing but targeted
  - **Phone phishing (vishing)** – Using SE to get info over the phone
SOCIAL ENGINEERING 101 – COMMON TYPES

- **Baiting** – Stuxnet (2010)
- **Piggybacking** – scene from *Taken*
- **Diversion Theft** – Rerouting info/goods/$$ to somewhere else
  - 2019 – (OH) – St. Ambrose Catholic Parish tricked into changing bank account info for payment of construction ($1.75M)¹
  - 2019 - Cabarrus Co. (NC) – tricked into changing banking info for construction payment – ($2.5M, $1.7M still missing)²
  - 2016 - Barton Co. (KS) - tricked into redirecting funds to different bank account (~$50,000)³

³. [https://www.kwch.com/content/news/Barton-County--380275691.html](https://www.kwch.com/content/news/Barton-County--380275691.html)
NOT QUITE SOCIAL ENGINEERING BUT CLOSE ENOUGH

- Dumpster diving – Digging through people’s trash to find sensitive information or information that can be used in other social engineering attacks

Examples:
- 2019 – (GA) Medical records in dumpster¹
- 2017 – (HI) Medical records in public dumpster²
- 2014 – (TN) Top-secret documents from nuclear facility thrown out with regular trash³

KANSAS’ JOURNEY INTO SE
TIMELINE

- June 2008 audit – Surplus Computer Equipment and Wiping Data
- Spring 2015 – KS Department of Corrections becomes first agency to opt-in to social engineering as part of its IT security audit
- 2018 – Social engineering becomes mandatory EXCEPT phishing, which remains optional
- 2019 – Social engineering becomes mandatory

- Participation rate agencies opting-in to social engineering ~50%
SOCIAL ENGINEERING MENU

- Early menu
  - Email Phishing
  - Phone phishing
  - Trash checks (DD)
  - Piggybacking

- Also included but not strictly SE
  - Door checks
  - Keyboard/work area checks

- Later additions
  - USB drives
MAIN EVENT: 10 COMMON ROADBLOCKS TO IMPLEMENTING SE AND SUGGESTED POTENTIAL SOLUTIONS
OVERVIEW OF ROADBLOCKS

- When altering the audit plan, resistance/skepticism should be expected
- From those implementing (auditors) and those who are being tested (auditees)
- THIS IS NORMAL
- Several suggestions apply both to audit staff conducting the work, and audit supervisors/managers
OVERVIEW OF COMMON ROADBLOCKS

1. Too Green
2. Too Risk-Averse (auditees)
3. Too Risk-Averse (auditors)
4. Too Shady
5. Too Illegal
6. Too Irresponsible
7. Too Time-Consuming
8. Too Time-Consuming II
9. Too Much Auditee Resistance
10. Too Off-Topic (auditors)
ROADBLOCK #1 – TOO GREEN

**Concern:** We are not experienced using social engineering / we will be viewed as not knowing what we’re doing!

Potential Solutions:

- Get some experience! Practice on yourself! Use those as a dry run.
- Start small. Crawl before your walk, walk before you run.
- Acknowledge your inexperience. Don’t hide from it. Use that as a selling point.
Concern: We don’t want to bring down (or be blamed for bringing down) an auditee’s IT environment.

Potential Solutions:
- Many SE tests are not electronic and would not touch an auditee’s IT environment.
- For those that are, testing is super-important.
  - First, test on yourself.
  - Then, test on auditee’s test PC.
- Know your product/test, and anticipate questions.

ROADBLOCK #2 – TOO RISK-AVERSE (THEM)
Concern: We don’t want to cause a panic or false alarm for the auditee.

Potential Solutions:

- So don’t.
- Clue someone(s) from the auditee in on the test. If alarms are raised, the auditee can tell whether it is you testing or an actual security issue.
- You may have others to loop in, depending on your situation.
Concern: If we do this work, we will lose trust or be viewed as untrustworthy by the auditee because SE necessarily involves “abuse” of auditee’s trust.

Potential Solutions:
- Get auditee executive leadership approval.
  - Will talk more about this in Roadblocks 9 & 10
- Be candid with auditee throughout process.
Concern: Social engineering is illegal, isn’t it?

Disclaimer: This is not legal advice, and I am in no way creating an attorney-client relationship with you by discussing this topic with you.

Potential Solutions:

- Can’t speak for all states, and this is not official legal advice
- Generally, audits are viewed as exceptions
- Obtain written authorization from auditee BEFORE conducting tests
- Consult your local legal counsel for additional guidance

ROADBLOCK #5 – TOO ILLEGAL
Concern: What about ethics? Or morals?

- I’m sure we could do a whole presentation (or conference!) about whether social engineering work is ethical or moral.
- For our purposes today, recognize that some people may have personal/professional objections to conducting the work.
  - Possible solution: Allow employees to opt-out of conducting that work.
Concern: We don't want to get anyone fired.

Potential Solutions:

- Tough moral decision.
- Encourage auditees to view tests as an evaluation of the auditee's training program. Employees who are engineered should be retrained to encourage good behaviors / discourage bad behaviors.
Concern: We don’t have time in the audit plan for social engineering work. That takes way too long to conduct.

Potential Solutions:

- SE audit work is adjustable; can take as little or as much time as desired
- Some SE tests take longer than others, require additional set up
- Other tests can be “tacked on” to additional work.
- Regularly yield tangible findings which drive real change

ROADBLOCK #7 – TOO TIME-CONSUMING
Concern: SE work require auditors to be onsite and in person. We don’t have the resources to commit to something like that.

Potential Solutions:
- SE audit work is adjustable
- Some SE tests do not require a physical presence on-site (e.g. phishing, vishing)
#9 – TOO MUCH AUDITEE RESISTANCE
May vary depending on your office's funding model
Make participation optional
  - Those that decline at least had a chance
Make participation mandatory
  - Auditees don’t often get to tell auditors what they can do
  - Can negatively affect your “Get out of Jail Free” card
Regardless of whether you decide to make it optional or mandatory:

- Give auditee shout-out for those who “opt in”
  - More impactful for auditees who want positive

- Create a Rules of Engagement (RoE) document to use that explains what is “in bounds” and what is “out of bounds”
  - Allow auditee to work with you on modifying the RoE if they are uncomfortable with some rules/tests
Additional Selling Points for Auditees

- Tangible results to determine whether entity’s training program works as intended or needs to be tweaked
- Tests will be conducted in safe environment
- Likely to cost less than if auditee was to contract for this to be done by private sector
#10 – TOO OFF-TOPIC / DOESN’T FIT WITH THE REST OF THE AUDIT PLAN.
IT audit / IT Security audit -- Straightforward

Financial audits / other engagements

- SE findings → Direct evidence of security vulnerabilities
- Security vulnerabilities tie to other things auditors look for:
  - Risks of fraud / abuse
  - Segregation of duties
  - Risk to reliability of underlying system data
  - Noncompliance with laws, regulations, contracts

#10 - HOW SE COULD FIT THE AUDIT PLAN
For all types of audits

- Social engineering fieldwork tests actions (practice) rather than words (policies, interviews)
- More likely to get legitimate sense of how auditee operates
- Results = direct evidence
- Direct evidence > indirect

#10 - HOW SE COULD FIT THE AUDIT PLAN (CONT.)
ROE EXAMPLE TEXT ON NEXT SLIDE
LEARN FROM OUR “MISTAKES”
Q & A

Thank you!