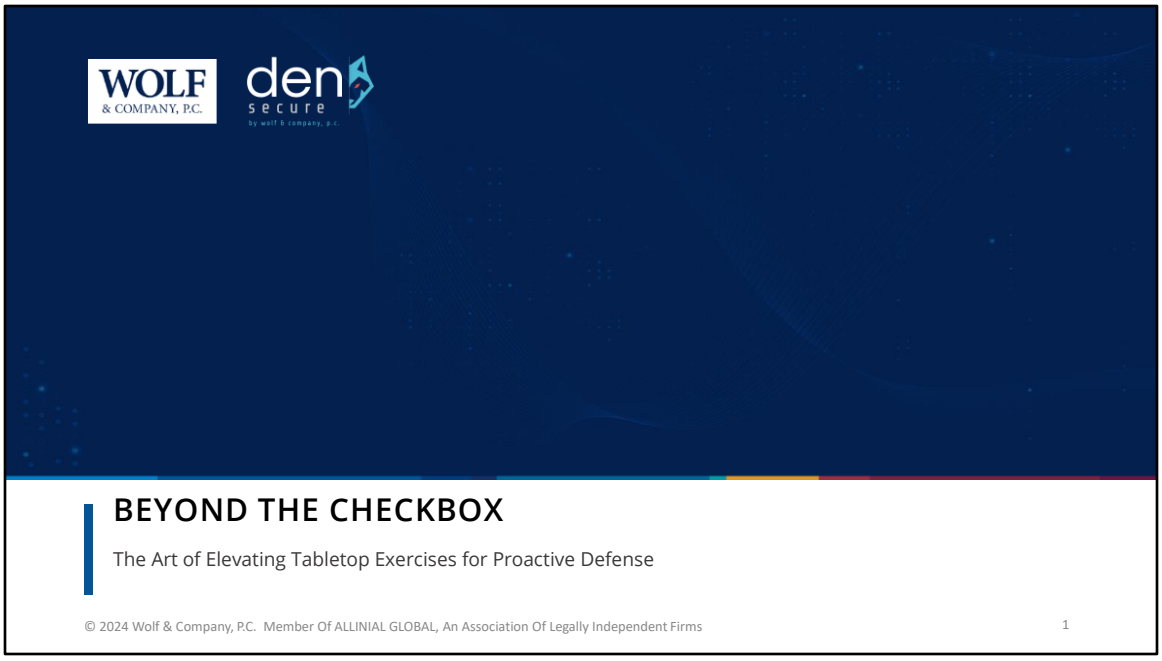


SEAN D. GOODWIN, GSE
SDGoodwin@wolfandco.com
617.261.8139
https://www.linkedin.com/in/0xseang/
https://twitter.com/0xSeanG
https://www.wolfandco.com/services/densecure/

AGENDA

- Why do we run Tabletop Exercises (TTX)?
- Where the typical TTX falls short
- Making the TTX worthwhile

RAISE YOUR HAND IF:

- You run a TTX on an annual basis
- Cover the same few scenarios each time
- Check the box for the auditor and move on until next year

WHY DO WE RUN TTXs?

BECAUSE THE LAWYERS SAY SO

- SEC Form 8-K disclosures
  - https://www.securemetrics.io/sec
- PCI DSS
- FFIEC
- HIPAA Security Rule 164.08(a)(6) – *Security Incident Procedures – Response and Reporting*
  - Requires formal documentation
- HHS "Wall of Shame"
  - Encourages a functional response plan
  - https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html

https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html

https://www.securemetrics.io/sec

IT REALLY IS A BEST PRACTICE

CISA Cybersecurity Tabletop Exercise Tips

https://www.cisa.gov/sites/default/files/publications/Cybersecurity-Tabletop-Exercise-Tips_508c.pdf

2023 Verizon DBIR

"When responding to social engineering attacks (and the same could be said of most attacks), **rapid detection and response is key**."

2023 IBM Cost of a Data Breach

Avg. Cost: **$4.45MM**

Avg. savings with high levels of IR planning and testing: **$1.49MM**

Avg. cost difference between breaches that took more than 200 days to find and resolve, and those that took less than 200 days: **$1.02MM**

WOLF & COMPANY, P.C. denSecure

https://www.cisa.gov/sites/default/files/publications/Cybersecurity-Tabletop-Exercise-Tips_508c.pdf

https://verizon.com/dbir

https://www.ibm.com/reports/data-breach

WHERE THE TYPICAL TTX FALLS SHORT

CLASSIC TTX FAILURES

- Same old song and dance
  - Ransomware
  - Phishing
  - BEC
- Key Personnel don't participate
  - If you are running the TTX, you aren't participating
- RTFM
  - If you complete the TTX without going to the documents, are they any good?

MAKING THE TTX WORTHWHILE

GO BEYOND THE CHECKBOX

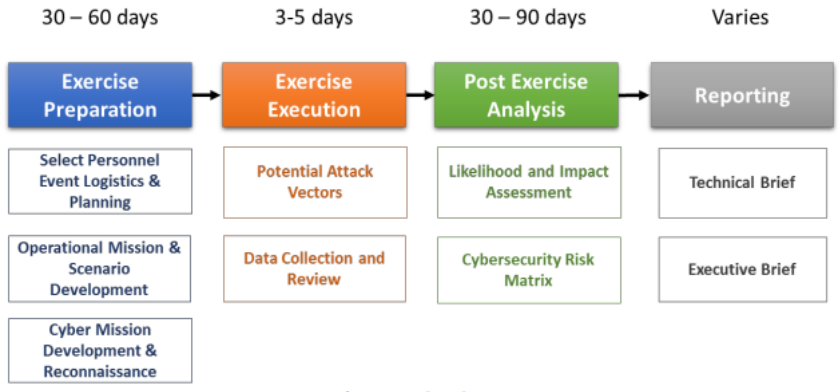
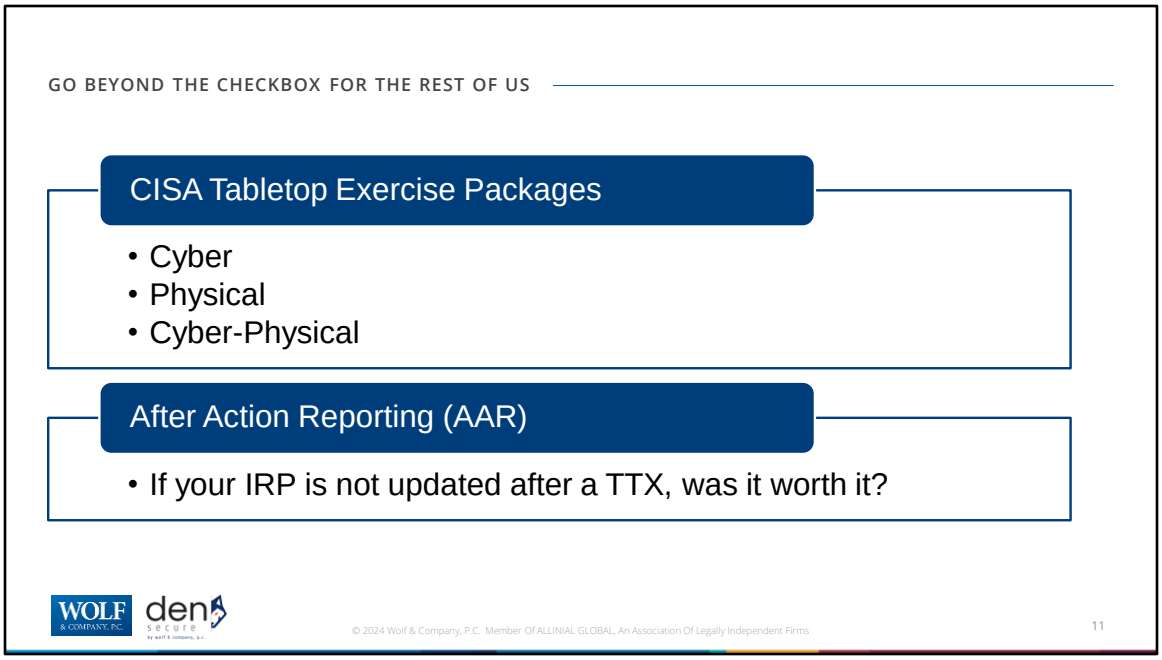


Figure 4. CTT Steps

https://ac.cto.mil/wp-content/uploads/2021/09/DoD-Cyber-Table-Top-Guide-v2.pdf



https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages

CISA sample TTX exercises: https://www.cisecurity.org/insights/white-papers/six-tabletop-exercisesprepare-cybersecurity-team

MAKE IT VALUABLE TO ALL

- Every single participant should learn **<u>something</u>**
- The progression should not be predictable

MAKE IT REALISTIC

- “Our SIEM would flag that”
- “Our E/X/MDR would stop that”
- “We could quarantine that within minutes”

PUT ALL THAT TOGETHER

- Go beyond the checkbox
- Make it valuable
- Make it realistic
- …. Make it fun?

https://play.backdoorsandbreaches.com/

Play for FREE: https://play.backdoorsandbreaches.com/

Play.backdoorsandbreaches.com to play online FREE

More information about the DenSecure expansion deck: https://www.wolfandco.com/resources/alerts/densecure-expands-backdoors-breaches/

HOUSEKEEPING

- These sessions will typically last 30-60 minutes (if the d20 allows) – we'll get through what we can today.
- Nominate One person as the Incident Captain and the rest in at your table as Defenders.
- Play.BackdoorsAndBreaches.com to play at home
- https://spearphish-general-store.myshopify.com/collections/backdoors-breaches-incident-response-card-game to buy physical cards

https://play.backdoorsandbreaches.com/

https://spearphish-general-store.myshopify.com/collections/backdoors-breaches-incident-response-card-game

RULES IN BRIEF

- Incident Captain knows all – they will guide the Defenders through the incident
- Defenders get 10 turns to reveal all 4 attack cards – d20 rolled each turn to determine outcome
  - INITIAL ACCESS
  - PIVOT & ESCALATE
  - C2 & EXFIL
  - PERSISTENCE
- Defenders are randomly given 4 procedures that have a +3 modifier, all others are +0
- 1-10 = FAIL, 11-20 = SUCCESS
- 1, 20, or 3 FAIL rolls in a row = INJECT (can be good, bad, or simply chaos)
- After a procedure is called, it can't be used again for 3 turns

WOLF & COMPANY, P.C. den secure by wolf & company, p.c.

Full rules and guidelines: https://www.blackhillsinfosec.com/wp-content/uploads/2024/03/BnB_VisualGuide_v2_03052024.pdf

Also check out backdoorsandbreaches.com && https://play.backdoorsandbreaches.com/

LET'S PLAY

Play for FREE: https://play.backdoorsandbreaches.com/

[redacted]

[redacted]

[redacted]

[redacted]

Full scenario details will be released after the session for bankers to use at their institution.

- SDGoodwin@wolfandco.com
- https://www.linkedin.com/in/0xseang/
- https://twitter.com/0xSeanG
- https://www.wolfandco.com/services/densecure/

ABOUT WOLF & COMPANY, P.C.

111
YEARS IN BUSINESS

- Established in 1911
- Built on quality and integrity
- Succession strategy to remain independent allows us to be with you throughout your business lifecycle

300+
EXPERIENCED, HIGHLY TRAINED PROFESSIONALS

- Lower-than-industry-average staff turnover means a consistent team structure year after year
- Niche team dedicated to your industry

RESOURCES TO LEARN MORE

- Cultures & Values
- Inclusion & Diversity
- Our History
- Social Responsibility
- Thought Leadership
- Wolf Global

Wolf & Company ranked
#2 BEST LARGE FIRM TO WORK FOR
nationwide
accountingTODAY

WOLF & COMPANY, P.C. den secure

22

https://www.wolfandco.com/

ABOUT WOLF & COMPANY, P.C.

SERVICES WE OFFER

We combine industry expertise with service specialization to provide your organization with insight, opportunities, and solutions allowing you to address your unique business needs.

ADVISORY

- Business Continuity Planning
- Cybersecurity
- Enterprise Risk Management
- Environment, Social & Governance
- Internal Audit
- IT Audit
- Model Risk Management
- Outsourced Accounting Solutions
- Penetration Testing
- Regulatory Compliance
- Strategic Planning

ASSURANCE

- Employee Benefit Plan Audits
- Financial Statements Audits
- HITRUST
- PCI DSS
- SOC Reporting

TAX

- Business Tax
- Federal
- International
- State & Local
- Private Client Group

vSUITE

- Virtual Consulting Services
  - Business Continuity Planning (BCP)
  - Virtual Chief Information Security Officer (vCISO)
  - Virtual Chief Privacy Officer (vCPO)
  - Virtual Chief Risk Officer (vCRO)
  - Virtual Vendor Management

WOLFPAC

- Integrated risk management SaaS suite

WOLF & COMPANY, P.C. den secure by wolf & company, p.c.

https://www.wolfandco.com/

WOLF ACCOLADES

Wolf is pleased to have received recognition from a variety of sources for our efforts at providing responsive client service and development of our professionals. Examples of this recognition include:

https://www.wolfandco.com/

https://www.wolfandco.com/

PANY, P.C.

O.
HED

ABOUT DENSECURE

Wolf & Company's IT Assurance & Advisory team of cybersecurity experts, DenSecure™, brings together extensive technical knowledge and industry experience with internationally-recognized frameworks to develop strong cybersecurity programs.

DenSecure's core services include:

- Advanced Security Assessment
- Application Penetration Testing
- Network Penetration Testing
- Social Engineering
- Threat Emulation

https://www.wolfandco.com/services/densecure/

Back to Home ⟶