The Cyber Attack Tabletop Exercise: The Best Defense is Preparation

08.22.24

Mark Magruder, C|CISO, CISSP, CISM

ClearBalance Healthcare

Thank you

to our session Sponsors

John Lloyd

National Account Manager

ClearBalance HEALTHCARE®

rJLloyd@ClearBalance.org

Elkin Pinamonti

Assistant Director, Patient Access

NOVANT HEALTH

epinamonti@novanthealth

Allison White

Assistant Director, Revenue Integrity

CONE HEALTH

Allison.white@conehealth

ClearBalance Healthcare

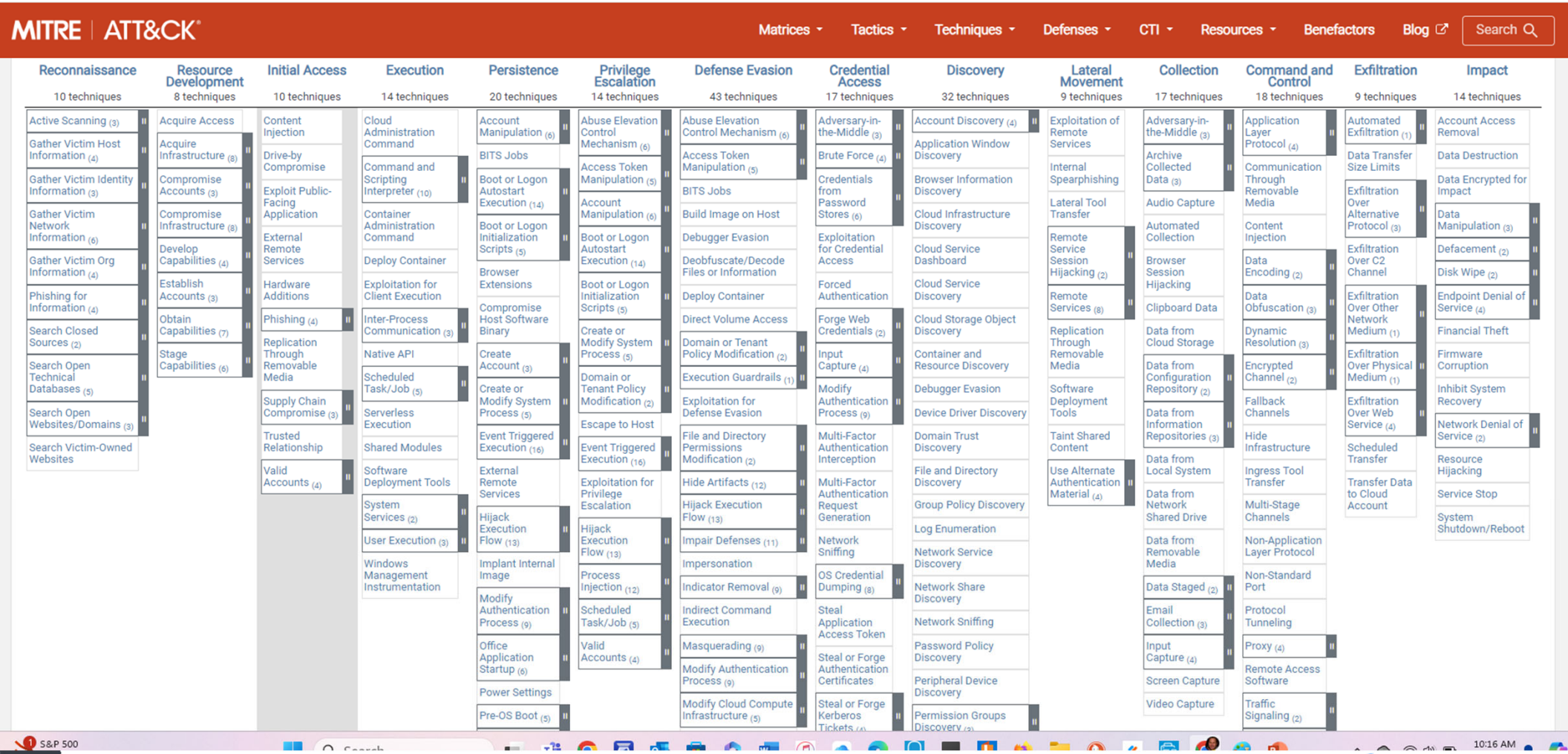
Audience

- IT
- Finance/Rev Cycle
- Cybersecurity Team

- If you think because you don't work in IT or Cybersecurity that this doesn't apply to you, you are wrong.

ClearBalance Healthcare

The Cyber Attack Kill Chain



ClearBalance Healthcare

Your CEO: *"I know a cyber attack is a matter of when, not if, so please, do all that you can to minimize its impact!"*

Impact:

- Unplanned Costs/down time
- Loss or delayed Revenue
- Reputation/Brand Value
- Regulatory Penalties
- Patient Lawsuits

Mary Barra, CEO General Motors

ClearBalance Healthcare

2. Tabletop Participants

- -1D#ë 1´o#ffio/o†É#jo••o†#,/mo†‡•b/m#w‡¡‡É#£ fibk•‡É#kƒ‡•‡
- -9D ë -ƒò¢obmo†É#-ƒ£ £ ,/wkb•wƒ/‡
- -9PD ë Oo‡fiƒ/‡o#¢obmo†‡vwiÉ#o‡ƒ,‡kw/uÉ#kƒ£ £ ,/wkb•wƒ/‡
- Po†‰wko#@w/o#@obmo†ÄXL#ëj,‡w/o‡‡#£ fibk•É#•ob£ #/ƒ•wwkb•wƒ/É#,,‡w/o‡‡# -ƒ/•w/,w•´#L¢b/#obmw/o‡‡
- Po†‰wko#@w/o#,,‡w/o‡‡#$/b¢´‡•#ë vo¢i#•ƒ#mo‡k‡wjo#¿ vb•#vbfifio/om
- Pok,‡w•´#Dfio†b•wƒ/‡#-o/•o†#ÉPD-™#b/b¢´‡•‡ë $¢b†£ ‡É#b‰o/•#b/b¢´‡w‡É# w‡ƒ¢b•wƒ/É#kƒ/•bw/£ o/•É#okƒ‰o†´
- 9/t†b‡•†,k•,to Ä/o•¿ƒ†¡#ë kƒ/•bw/£ o/•É#okƒ‰o†´
- Pok,‡w•´#L/uw/oo‡w/u#b
- D•vo†Ò#-ƒ£ fi¢b/koÉ#@oub¢É#kw/b/ko

ClearBalance Healthcare

Cyber Attack Tabletop Exercise: The best defense is preparation

Agenda:

1. What are we preparing for? Goals Objectives
   - How to respond to a Ransomware Attack – threat modeling, test scenario
   - Test effectiveness of our Cyber Incident Response Plan
2. Tabletop Participants
3. Involve Top Level Management
4. Plan realistic attack scenario
5. Conduct the exercise: walk through the simulated crisis
6. Lessons Learned

1. **Why simulate a cyber attack with a Tabletop exercise?**
   - What are our Goals Objectives in Tabletop exercise
   - How to respond to a Ransomware Attack – threat modeling, test scenario
   - Test effectiveness of our Cyber Incident Response Plan

Let's make it realistic:

- Ransomware Attack
- Test the steps in your Incident Response (IR) Plan Document

Steps in an IR Plan	Details
Preparation	The IR Team, Participants resolving a cyber attack, Notifications, Communications,
Detection & Analysis	Security Ops Center (SOC) Who, what, where, when, (how, why); Spreading? Prioritization, Notifications
Containment, Eradication, Recovery	System isolation, account reset, invoke DR plan to restore data
Post Incident Activity	Evidence collection/retention, Lessons Learned

ClearBalance Healthcare

2. Tabletop Participants

- -1D#ë 1´o#ffio/o†É#jo••o†#,/mo†‡•b/m#w‡¡‡É#£ fibk•‡É#kƒ‡•‡
- -9D ë -ƒò¢obmo†É#-ƒ£ £ ,/wkb•wƒ/‡
- -9PD ë Oo‡fiƒ/‡o#¢obmo†‡vwfiÉ#o‡ƒ,‡kw/uÉ#kƒ£ £ ,/wkb•wƒ/‡
- Po‡‰wko#@w/o#@obmo†‡#ëj,‡w/o‡‡#£ fibk•É#•ob£ #/ƒ•wwkb•wƒ/É#,,‡w/o‡‡# -ƒ/•w/,w•´#L¢b/#obmw/o‡‡
- ,,‡w/o‡‡#$/b¢´‡•#ë vo¢fi#•ƒ#mo‡k‡wjo#¿ vb•#vbfifio/om
- Pok,‡w•´#Dfio‡b•wƒ/‡#-o/•o†#ÝPD-™#b/b¢´‡•‡ë $¢b†£ ‡É#b‰o/•#b/b¢´‡w‡É# w‡ƒ¢b•wƒ/É#kƒ/•bw/£ o/•É#okƒ‰o†´
- 9/t‡b‡•†,k•,‡oÄ/o•¿ƒ†¡#ë kƒ/•bw/£ o/•É#okƒ‰o†´
- Pok,‡w•´#L/uw/oo‡w/u#b
- D•vo‡Ò#-ƒ£ fi¢b/koÉ#@oub¢É#kw/b/ko

ClearBalance Healthcare

Cyber Attack Tabletop Exercise: The best defense is preparation

3. Involve Top Management

- A simulated cyber attack tabletop exercise is **an eye opener** for top management.
- Leaders instantly start adding up the **costs** of an outage for a day, a week, a month …
- Often Service Line leaders re-prioritize their **DR testing** and dust off their Business Continuity **Plan** documents

  (#1 weakness/gap – missing or incomplete BC plans).
- They become acutely aware of their software and infrastructure **vulnerabilities** and query the CIO/CISO about VM program and monthly patching. Less Risk exceptions, prioritize application upgrades.
- They place a very high priority with **security awareness and phishing testing**
- Increased awareness of **documentation quality** and **IT footprint** and interconnectedness/dependencies

4. Cybersecurity needs to plan a realistic cyber attack scenario

- Ob/ŧƒ£ ¿btо#$••bk¡
- $kkƒ,/•#-ƒ£ fiŧƒ£ wŧo
- P´ŧ•o£ #-ƒ£ fiŧƒ£ wŧo#ÉmƒÂ£ bw/#kƒ/•ŧƒ¢¢oŧÉ#LPZ#vƒŧ•É#ok,ŧw•´#w/tŧbŧ•ŧ,k•,ŧo#ÉPƒ¢oŧY w/mŧ™
- P,fifi¢woŧ#ƒ,•buoÄw£ fibk•

ClearBalance Healthcare

5. Conduct the Simulated Tabletop exercise

Łÿ $¢#ibt•wkwib/•t#bto#ito+o/•#

The Attack Begins (Detection)

Øÿ PD-#Ab/buotÒ#$•#bfifit+`w£ b•o¢´#ØÒŒª#w/#•vo#£ +t/w/uÉ#•vo#PD-#•bt•t##okow‰w/u#o‰otb¢#vwuv# t+o‰otw´#b¢bt£ t#•vb•##o‰otb¢#k¢wo/•#´t•o£ t#bto#w/tok•om#¿ w•v#b#Ob/t+f£ ¿ bto#´fio#‰wt,t÷ÿ

Œÿ Po‰wko#/o+¡#Ab/buotÒ#Pw£ ,¢#b/of,t¢É#•vo#Bo¢i#/o+¡#vbt##¿ f#tofift•t#+ft#¢fk¡om#Ł-t#¿ w•v#b# #b/t+f£ ¿ bto#£ o+#buo#mwfi¢b´omÿ##Rvo#kb¢‰o+t#b`fi¢bw/om#•vb•#•vo´#¿ oto#w/#•vo#£ wmm¢o#ft# #ouwt•otw/u#tf##vb#bt+#£ o/•#•bw/w/u#¿ vo/#b¢#ft#b##,mmo/#•vo´#uf•#b#Ob/t+f£ ¿ bto#£ o+#buo#f/# •vow#Ł-ÿ##

°ÿ PD-#Ab/buotÒ#Ś/b¢´tw+#b/m#-f/•bw/£ o/•™°##´t•o£ t#vb‰o#b¢tobm´#joo/##w/tok•om#b/m#w+f¢b•om# j´#•vo#PD-É#j,•#•b•o#£ f to#w/tok•wf/t#bto#w¡o¢ÿ#Rvow#Ob/t+f£ ¿ bto#Ł¢b´jff¡#w+#w/‰f¡omÿ##

The Severity 1 Incident Response Process Starts

æÿ -9PDÒ#Rvo#-9PD#kb¢t#•vo#-9D#o-,o+•w/u#•vo´#mok¢bto#b#Po‰otw´#Ł#w/kwmo/•#b/m#w/‰f¡o#•vo#9O# Ł¢b/ÿ#Rvo#Po‰Ł#Rob£ t#kf/tobto/ko#kb¢#w+#ffio/om#j´#•vo#-´jot+ok,tw•´#/wtok•ft#b/m#•vo#9O#Ł¢b/# t•ofi+#bto#jow/u#w/w•b•omÿ

ıÿ PD-#Ab/buotÒ#Rvo#PD-#•ob£ ##ofift•t#f/#•vo#ŁŁ#$¢bt£ t#b/m#•vo#fitob,•vftw¡om#Ob/t+f£ ¿ bto# Ł¢b´jff¡#•ofi+#b¢tobm´#b¡o/#f#w+f¢b•o#¡/f¿ /#bttok•om#´t•o£ t#vb‰o#joo/#b`ok,•omÿ

łÿ ,,tw/ot+#KLÒ#Rvo#w/o#ft#j,tw/ot+#KL#ofift•t#b•#ob+•#¿ f#,to+t#bto#m¢o#¿ w•v#b/t+f£ #/f•wko+# mw+fi¢b´om#f/#•vow#Ł-ÿ

øÿ -9DÒ#Rvo#-9D#o/m+#b#kf£ £ ,/wkb•wf/#f#BO#b/m#b¢#@D,#KL+#f#ofift•t##wu/+#ft#b/´#k´jo+#b••bk¡ÿ

ClearBalance Healthcare

5. Conduct the Simulated Tabletop exercise cont.

9. SOC Manager: Reports additional alarms from their NGFW and OpenDNS are reporting attempted connections to a suspicious website. The website is unknown and the connections are not blocked.
10. Cybersecurity: (Analysis) Engineering reports affected users opened emails from a “Spoofed” sender, meaning the display name is fake and hovering over the name shows an obscure email and domain.
11. SOC Manager: Reports the urgent harassment training email is not from the VP and the email sent users to a malicious website that downloaded virus payloads that started the ransomware attack.
12. Help Desk Manager: reports users are unable to access Teams folders containing excel lists of patient insurance records. The file names are long cryptic random numbers and letters.
13. Infrastructure: Reports Teams folders permissions included the affected users who reported the Ransomware notices.
14. CIO: Upon hearing this news, the CIO orders access to Azure cloud services be severed. This has only minimal protections to office users because remote users can still access Azure using outlook.live.com.
15. Infra/Email Security: Reports they have blocked new emails from the malicious domain and are in the process of revoking emails already sent to users who haven’t opened them yet.

5. Conduct the Simulated Tabletop exercise cont.

16. CISO: Sends an enterprise email to all employees that a malicious email claiming to be Urgent and required Harassment training made past security defenses and please do NOT open it but report it to the Help Desk. (containment)
17. Infra/email security: Reports all malicious emails have been revoked and there are no new encrypted files.
18. CIO, CISO, VP: It is now 3PM. Affected and some non affected business units taking precautions have been idle all day. The team discusses turning access back on, resuming business activity and initiating recovery activities. (recovery)
19. CIO, CISO, VPs: No new infections have occurred since the morning events. Eradication and recovery plans are still being discussed. The CIO orders access to the Azure cloud services restored. (eradication, recovery)
20. Infrastructure, SOC teams: continue to scan related systems and for any evidence of unauthorized elevated user privileges. Restoring the encrypted files has been slow and better backups with immutable storage have been raised. Everyone goes home (lessons learned)
21. Bobby in Accounting: returning from a business trip boards his plane at 8:45AM. While in the air Bobby checks his emails and opens the malicious email that IT could not revoke. He didn't buy in-flight internet services so the malware is sitting there waiting to connect to the malicious site once Bobby's system reconnects to the internet. Bobby gets home, he's exhausted from flying coach and his laptop connects to his home internet …

5. Conduct the Simulated Tabletop exercise cont.

22. Bobby: Because the company's architecture allows open access to the internet from home, Bobby's laptop connects to the internet and his laptop becomes infected. The malware attempts to connect to shared folders but can't because Bobby hadn't authenticated to Azure yet.
23. Bobby, SOC Team, Infra Team: Bobby shows up to work the next morning and when his laptop connects to the company network, the Ransomware starts encrypting files and Alarms in the SOC go off like a Christmas Tree. The SOC and IT react quickly to contain the attack but the fact that there was a recurrence does not sit well with the CEO.

6. Lessons Learned

25. All Participants: the team begins to address challenges that allowed the infection in the first place, causes of delays in containment and eradication, and challenges with Recovery.

Recommendations:

a. upgrade to storage with immutable backup features

b. Retire vulnerable VPN remote access for improved security for remote workers and their devices.

Conclusion

Preparation is absolutely critical to uncovering weakness in tools or processes.

Thank you for participating