

The Cyber Attack Tabletop Exercise: The Best Defense is Preparation

08.22.24

Mark Magruder, C|CISO, CISSP, CISM

Thank you

to our session Sponsors

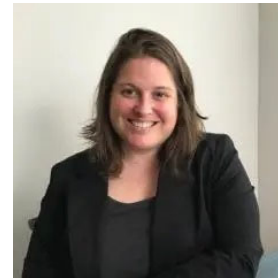


John Lloyd

National Account Manager



rjLloyd@ClearBalance.org

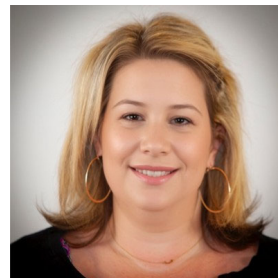


Elkin Pinamonti

Assistant Director, Patient Access



epinamonti@novanthealth



Allison White

Assistant Director, Revenue Integrity



Allison.white@conehealth



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.



The Cyber Attack Kill Chain

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques	17 techniques	32 techniques	9 techniques	17 techniques	18 techniques	9 techniques	14 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (10)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Debugger Evasion	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Host Software Binary	Create or Modify System Process (5)	Deploy Container	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Native API	Create Account (3)	Domain or Tenant Policy Modification (2)	Direct Volume Access	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2)	Exfiltration Over Web Service (4)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (5)	Event Triggered Execution (16)	Domain and Resource Discovery	Modify Authentication Process (9)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	Exfiltration Over Physical Medium (1)	Financial Theft
Search Open Websites/Domains (3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (16)	Event Triggered Execution (16)	Debugger Evasion	Multi-Factor Authentication Process (9)	Device Driver Discovery	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Hide Infrastructure	Inhibit System Recovery	Firmware Corruption
Search Victim-Owned Websites		Valid Accounts (4)	Shared Modules	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation	File and Directory Permissions Modification (2)	Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Local System	Ingress Tool Transfer	Network Denial of Service (2)	Resource Hijacking
			Software Deployment Tools	Hijack Execution Flow (13)	Hijack Execution Flow (13)	Hide Artifacts (12)	Network Authentication Request Generation	File and Directory Discovery		Data from Network Shared Drive	Multi-Stage Channels	Scheduled Transfer	Service Stop
			System Services (2)	Implant Internal Image	Process Injection (12)	Hijack Execution Flow (13)	Network Sniffing	Group Policy Discovery		Data from Removable Media	Non-Application Layer Protocol	Transfer Data to Cloud Account	System Shutdown/Reboot
			User Execution (3)	Modify Authentication Process (9)	Scheduled Task/Job (5)	Impair Defenses (11)	OS Credential Dumping (8)	Log Enumeration		Data Staged (2)	Non-Standard Port		
			Windows Management Instrumentation	Office Application Startup (6)	Valid Accounts (4)	Impersonation	Steal Application Access Token	Network Service Discovery		Email Collection (3)	Protocol Tunneling		
				Power Settings		Indicator Removal (9)	Steal or Forge Authentication Certificates	Network Share Discovery		Input Capture (4)	Proxy (4)		
				Pre-OS Boot (5)		Indirect Command Execution	Steal or Forge Kerberos Tickets (4)	Password Policy Discovery		Screen Capture	Remote Access Software		
						Masquerading (9)		Peripheral Device Discovery		Video Capture	Traffic Signaling (2)		
						Modify Authentication Process (9)		Permission Groups Discovery (2)					
						Modify Cloud Compute Infrastructure (5)							

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

2. Tabletop Participants

- - 1D #ë 1´ o#ffio/oÉ#j o••o# , /mot#b/m#w# ; #ÉwÉ fibk•#Ékf#•#
- - 9D ë - fòc obmoÉ# fÉ É , /wkb•wf / #
- - 9PD ë Oo#fif / #o# obmot#vfiÉ#to#f , tkw/uÉkfÉ É , /wkb•wf / #
- Po f%wko#w/o# obmotÄXL#ë j , #w/o#t#É fibk•É#obÉ # / f•wkb•wf / É# , #w/o#t##
- f / •w , w´ #L• / #obmw/o#t#
- Po f%wko#w/o# , #w/o#t# \$ / bç #•#ë voçif#f#no#ktwj o#ë vb•#vbfifio/om
- Pok , tw´ #Dfiotb•wf / # o / o#t# PD -™# / bç #•#ë \$ ç b tÉ #É#%o / •# / bç #wÉ#
wfç•wf / Ékf / •bwÉ o / •É#okf%ot´
- 9/tb#•t , k• , toÄ/o•; fti#ë kf / •bwÉ o / •É#okf%ot´
- Pok , tw´ #L / uw/ootw/u#
- D•vo#É# fÉ fivb/koÉ#oubÉ#wb/ko

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

2. Tabletop Participants

- - 1D #ë 1´ o#ffio/oÉ#j o••o# , /mot#b/m#w# ; #ÉwÉ fibk•#Ékf#•#
- - 9D ë - fòobmoÉ# f£ £ , /wkb•wf/†
- - 9PD ë Oo#fif/†o#obmot†vfiÉ#to†f , tkw/uÉkf£ £ , /wkb•wf/†
- Po#wko#ow/o#obmot†#ë j , †w/o††#É fibk•É#ob£ #/f•wkb•wf/É# , †w/o††# - f/•w , w´#L•b/#obmw/o††
- , , †w/o††#\$/bç†•#ë voçif#f#mo#k#wj o#ë vb•#vbfifio/om
- Pok, tw´#Dfio#b•wf/†# o/•o†#PD -™#b/bç†•#ë \$çb†£ †É#%o/•#b/bç†wÉ# wfç•wf/Ékf/•bw/£ o/•É#okf%ot´
- 9/t#b†•t, k•, toÄ/••; f†i#ë kf/•bw/£ o/•É#okf%ot´
- Pok, tw´#L/uw/ootw/u#b
- D•vo†G# f£ fiw/koÉ#@oubÉ#w/b/ko

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/†f£ ç b to# \$ ••bkj
- \$kkf, /•# f£ fitf£ wto
- P´†•o£ # f£ fitf£ wto#m f£ bw #k f/•†f ç to #LPZ #v f†•#ok, tw´ #
w/tb†•†, k•, to#P f ç tY w/m†™
- P, fifi ç to #f, •buoÄw fibk•

5. Conduct the Simulated Tabletop exercise

Ly \$ #fib t w fib / # b to fi to to / #

The Attack Begins (Detection)

Øy PD - #A b / buo t \$ # of if it f ` w e b o c # o e a w / # vo e f t / w u e # vo e PD - # b t # tok o w / u # o o b c # w u v # t o o t w # b b t e # v b # # o o b c # k o / # # ' t o e # b t o w / t o k o m # w v # b b / t f e ; b t o # f i o # w t , t y

Ey Po % k o / o t ; # A b / buo t P w e , o b / o f , t c e # vo # o c i # / o t ; # v b # # ; f # o f i t # t f t y k ; o m # L - # e w v # b # b / t f e ; b t o # e o t # buo # m w f i o ' o m y # R v o # k b c t # b ` f i o w / o m # v b # # v o ' # e o t o w / # vo e w m m o # t # t # t o u w # o t w / u # f # v b b t # e o / # b o w w u e v o / # c # t # # , m m o / # v o ' # u f # b b / t f e ; b t o # e o t # buo # / # o v o w # L - y #

°y PD - #A b / buo t # S / b c # w # / m # f / o w / e o / # # # ' t o e # v b % o # b c t o b m # j o o / # w / t o k o m # b / m # f o o m # j # v o e PD - # # , # b o e f t o w / t o k o w / # b t o # w o c # y R v o w # b b / t f e ; b t o # L o ' j f f i # # w % f i o m y #

The Severity 1 Incident Response Process Starts

æy - PD R v o # PD # b c # # v o # D # o - , o t w u # v o ' # n o k o t o # # P o o t w # L w / k m o / # b / m # w % f i o # v o # D # L o / y R v o # P o # L # R o b e # k f / t o t o / k o k b c # w # f i o / o m # j # v o # ' j o t o k , t w # / w o k o f # b / m # v o # D # L o / # t o o f i # b t o # j o w u # w / w b o m y

ly PD - #A b / buo t R v o # PD - # o b e # # o f i t # t # / # v o # L # # o t e # b / m # v o # i t o b , o v f t w o m # b b / t f e ; b t o # L o ' j f f i # # o f i # b c t o b m # # b i o / # f # # f o o # # / f ; / # t t o k o m # # ' t o e # v b % o # j o o / # b ` o k , o m y

ly , , # w o t # # K L R v o # w / # t # j , # w o t # # K L # o f i t # t # # o b t # # ; f # , t o t # b t o # m o e w v # b b / t f e # / f o k o # # m w f i o ' o m # / # v o w # L - y

øy - D R v o # D # o / m # b # k f e e , / w k o w / # f # B O # b / m # c # @ D , # K L # # f # o f i t # # w a / # # t # b / ' # k ' j o # b o o k i y

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

