DREAM TEAM ASSEMBLE: COMBAT CONSTRAINT WITH COLLABORATION



Erin Reese TPRA 2023 Fall Conference



AGENDA

Same Villains, New Targets Assemble the Team Battle Constraint

Erin Reese

Erin Reese has spent more than (*choke*) 20 years in IT, focused on Incident Response for the last 10. She prefers to spend her time outside running, biking, gardening and hiking, or just spending time with family and friends. You can connect with her on LinkedIn.





Same Villains, New Targets

IBM CODB 2023

USD 4.45M

Global average total cost of a data breach

82% Share of breaches that

involved data stored in cloud environments public cloud, private cloud or across multiple environments Percentage of organizations increasing security investments after a breach

51%



Share of data breaches originated from a software

supply chain attack

Cost of a data breach by country or region

Figure 3. Measured in USD millions

Just keeps getting worse

#1 United States 2023 \$9.48 ↑ 2022 \$9.44

Impact of key factors on total cost of a data breach

The Bane of My Existence

Constraints!

- Information about incident
- Knowledge about environment
- Ability to validate resolution
- Meets requirements?

2023 IBM Cost of a Data Breach, p 28

DevSecOps approach	-\$249,278	
Employee training	-\$232,867	
IR plan and testing	-\$232,008	
AI, machine learning–driven insights	-\$225,627	
IR team	-\$221,794	
Encryption	-\$221,593	
rity information and event management (SIEM)	-\$202,347	
SOAR tools	-\$202,232	
Proactive threat hunting	-\$201,111	
Threat intelligence	-\$196,936	🗕 \succ Constraint
Insurance protection	-\$196,452	
Offensive security testing	-\$187,703	
Identity and access management (IAM)	-\$180,358	
EDR tools	-\$174,267	
Data security and protection software	-\$170,412	
Board-level oversight	-\$167,818	
ASM tools	-\$162,278	
CISO appointed	-\$130,086	
MSSP	-\$73,082	
Remote workforce		\$173,074
Supply chain breach		\$192,485
IoT or OT environment impacted		\$195,428
Third-party involvement		\$216,441
Migration to the cloud		\$218,362
Noncompliance with regulations		\$218,915
Security skills shortage		\$238,637
Security system complexity		\$240,889

Figure 16. Measured in USD



Figure 26. Measured in USD millions

Time to identify and contain a data breach based on occurrence of a business partner supply chain compromise



More Costly; Longer to Identify

They are our trusted partners!

Cost of a data breach based on occurrence of a software supply chain compromise



Figure 28. Measured in USD millions

Time to identify and contain a data breach based on occurrence of a software supply chain compromise



NOT THE SOFTWARE!!!

What's paper?

Figure 29. Measured in days

YOU CAN'T JUST HAVE A BATMAN.

You need a whole Justice League.



0

9/27/2023

LAW

PROCUREMENT

🙆 🖸 🗐 🔍



Assemble the Team



ASSEMBLE THE TEAM

Your power is being prepared



Clean Up the Streets

Collaborate on Contracting

- Legal, Procurement & TPS create and implement a strong security policy
- Review & renegotiate key contracts if necessary
- Identify Security staff at third parties

Educate the League on Risks

- Threat Intel and Incident Response educate team on org-specific threats
- Share information frequently, even rumors
- Road goes all ways—everyone should have access to the Bat Signal

Find Your Commissioner Gordon

 Leadership support is essential

+

0

- Escalate issues, translate the messages
- Champion changes, especially when they're hard



Battle Constraint



ACTION!

- Go to the Bat Cave War Room
- What do we think we know?
- What do we need to know?
- Course of Action & Assignments
- Follow Legal's lead, listen to everyone's input
- Ask for validation when appropriate
- Reevaluate relationships when necessary
- Do Better



THANK YOU