

# Information Security Officer (CISO)

**Confidentiality Notice:**

This document is confidential and contains proprietary information and intellectual property of Nitzan Levi. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission. Please be aware that disclosure, copying, distribution or use of this document and the information contained therein is strictly prohibited and may be cause for legal action.

# Nitzan Levi

Cyber Security and Privacy Expert



Cyber Security Expert



Certified Information  
Systems Security Professional



Certified Information  
Security Manager<sup>®</sup>  
An ISACA<sup>®</sup> Certification



Privacy Expert

אוניברסיטת  
בר-אילן  
Bar-Ilan University



Certified Data Privacy  
Solutions Engineer<sup>®</sup>  
An ISACA<sup>®</sup> Certification



Application and Operations Security



CSA  
Certified System  
Analyst

הלשכה לטכנולוגיות המידע בישראל



Certificate of  
Cloud Security Knowledge

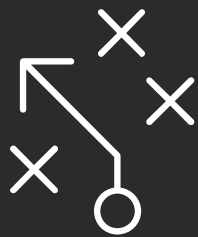


CISCO  
CERTIFIED  
CCNA  
CYBER OPS



PROFESSIONAL SCRUM MASTER I





## Why Security Incidents Happen?



## Why Security Incidents Happen?

Technology is all around us...

how many of you  
have home alarm  
installed?

How many of you  
have cameras at  
home?

Do you keep your  
payment details  
on your phone?

Do you manage  
your bank from  
your mobile?



## Why Security Incidents Happen?

Technology is all around us...

how many of you  
have ho  
inst

How many of you  
as at

Do you  
payme  
on you



**Don't  
Share!**

manage  
from  
ile?



# WHY DOES IT MATTER?



## Digital Transformation

THE WORLD IS  
GETTING MORE  
DIGITAL

Business, banking, healthcare, etc. is all  
online



## Crime is Rising

CRIME IS FOLLOWING  
THE SAME TREND

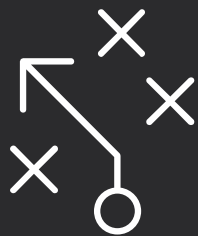
Worldwide ransomware attacks. High-  
profile hacks in the news  
and phishing emails are more  
sophisticated each day



## Regulations

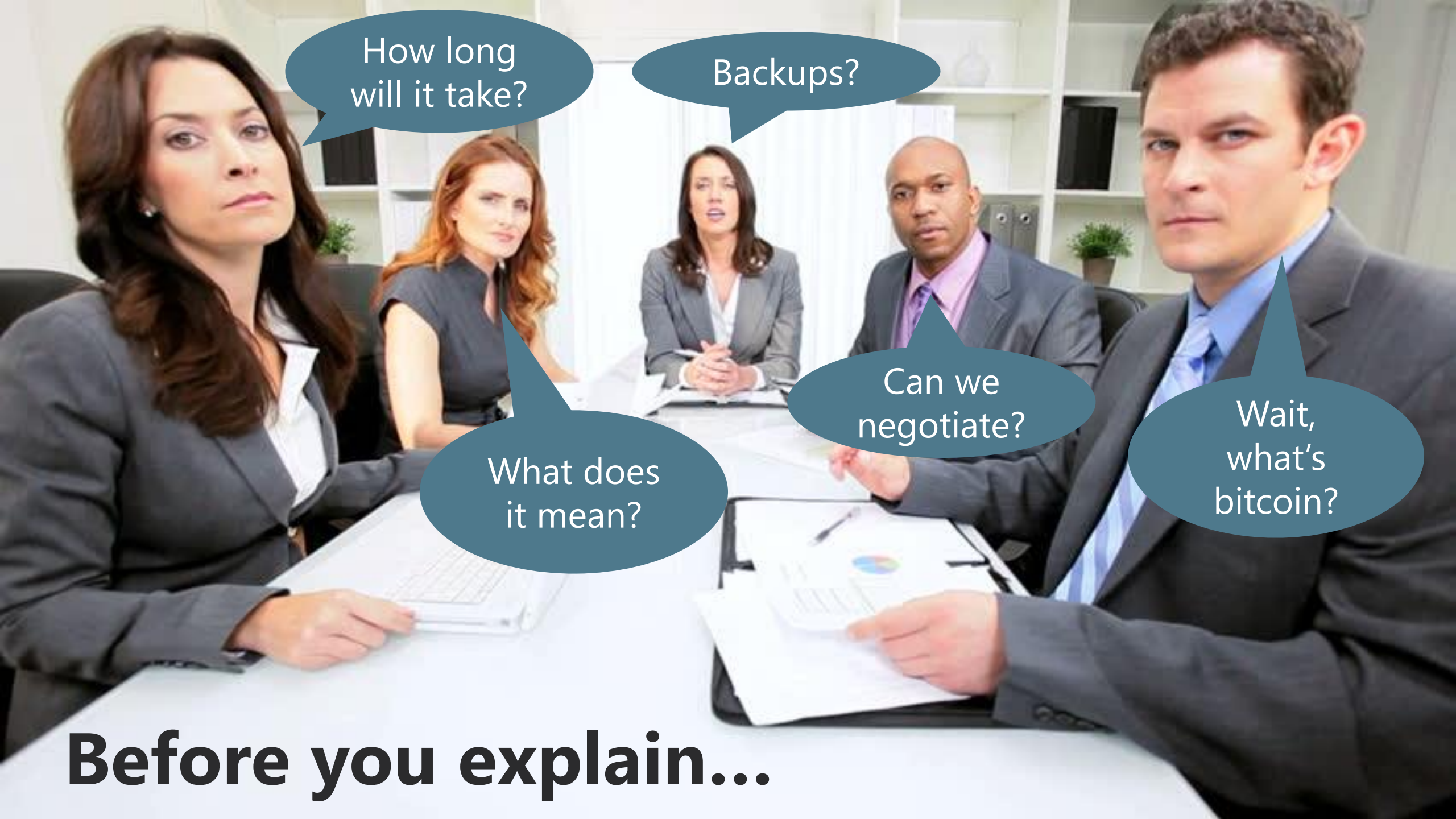
NEW PRIVACY LAWS  
AND REGULATIONS

New laws and regulations require training  
for compliance



# Information Security Incident Management





How long  
will it take?

Backups?

What does  
it mean?

Can we  
negotiate?

Wait,  
what's  
bitcoin?

**Before you explain...**



**After you explain...**



# Discussion Time

What is the difference between "event" and "incident"?





# Common Incident Types

Malicious code attacks

Unauthorized access to IT or information sources



Unauthorized use of services

Unauthorized changes to systems, network devices or information



DoS/DDoS attacks

Surveillance and espionage



Hoaxes/social engineering

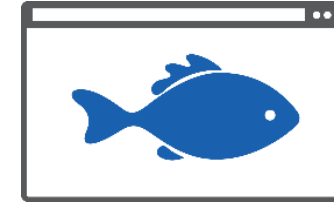
Physical disruption



# It's not that dangerous online, though, right?



1 in 50 URLs is malicious



Nearly 1 in 3 phishing sites uses  
HTTPS to appear legitimate



90% of the malware businesses  
encounter is delivered via email



Most breaches involve phishing  
and using stolen credentials



# But people know better, right?



**Joe Biden**  @JoeBiden · 2m

I am giving back to the community.

All Bitcoin sent to the address below will be sent back doubled! If you send \$1,000, I will send back \$2,000. Only doing this for 30 minutes.

bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh

Enjoy!

 544

 1K

 922

BREAKING | Jul 15, 2020, 05:34pm EDT | 18,690 views

## Twitter Hacked In Massive Bitcoin Scam: Joe Biden, Elon Musk Accounts Among Dozens Breached

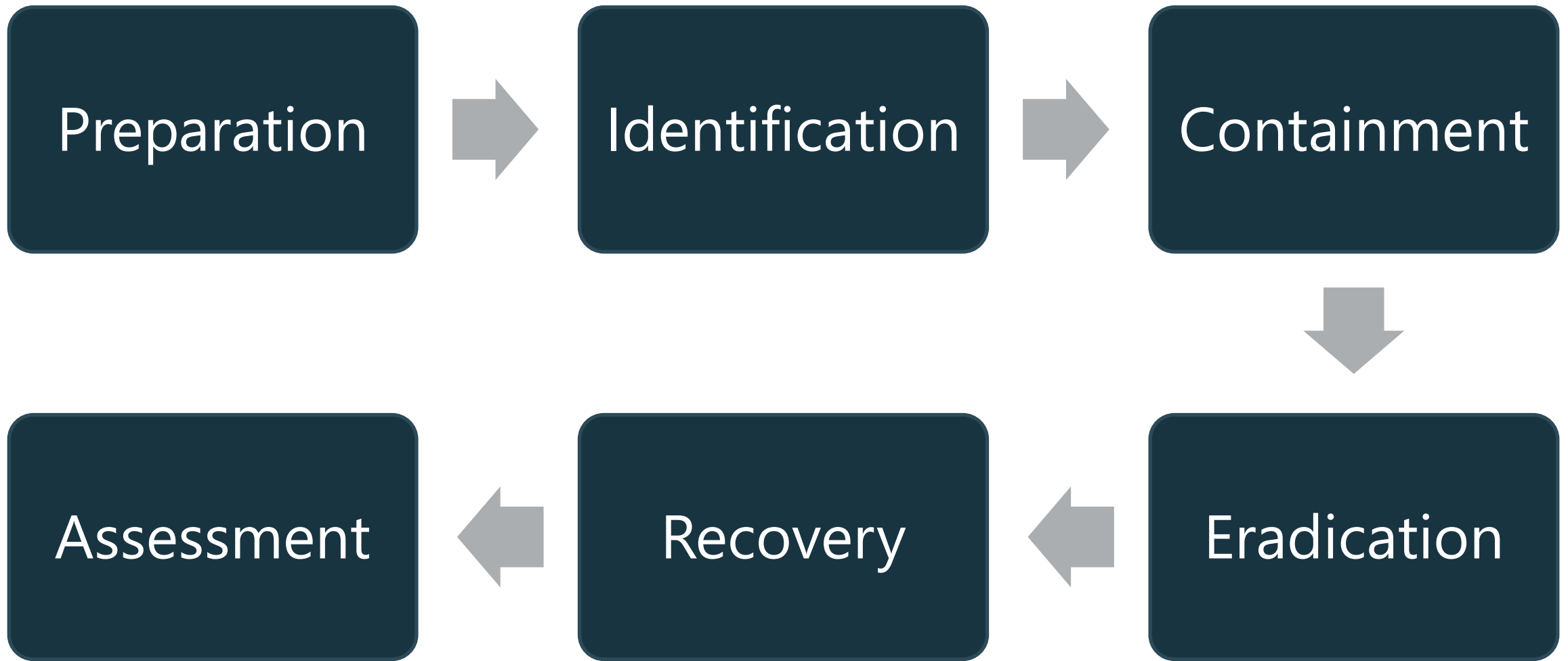


**Rachel Sandler** Forbes Staff 

Business

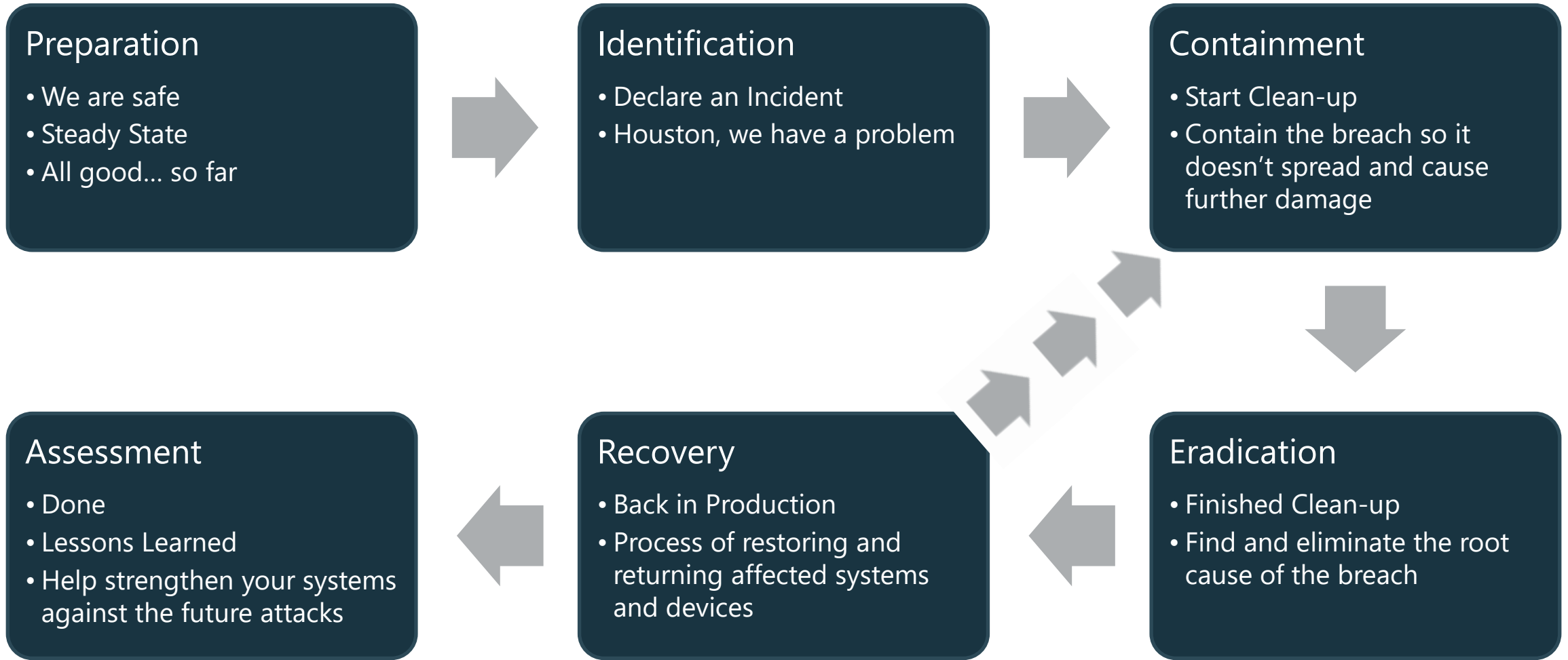
*I cover breaking news.*

# The Incident Response Plan – The Big Picture





# The Incident Response Plan – The Smaller Picture



# The Planning Process

Knowing the organization's risk appetite and goals is the first step:

Determine how your organization defines "acceptable" incident response.

Analyze gap between current and desired capabilities.

Build a plan to close the gap using good practices.

Be sure to take needed resources into account.

Use clear language to avoid confusion.





# Incident Response Teams



## Personal Skills

- Communication
- Writing skills
- Leadership
- Presentation skills
- Team building
- Problem solving
- Time management
- Can handle the pressure...



## Technical Skills

- Technical foundation skills
- Incident-handling skills

**if you can't  
stand the  
heat stay  
out of the  
kitchen !**



# Response and Recovery

Recovery is **specific** to the **affected** systems or data.

Disaster recovery documents the **strategy** and specific activities needed to **recover** overall capabilities in the case of a **major** loss.

**Response, continuity and recovery** often leverage the same resources and staff.

Recovery often **waits** until **eradication** is complete, but it may be **possible** to **restore** IT capabilities at an alternate site.

**Integrating** the incident response plan with the **BCP** and **DRP** can help to identify overlap.

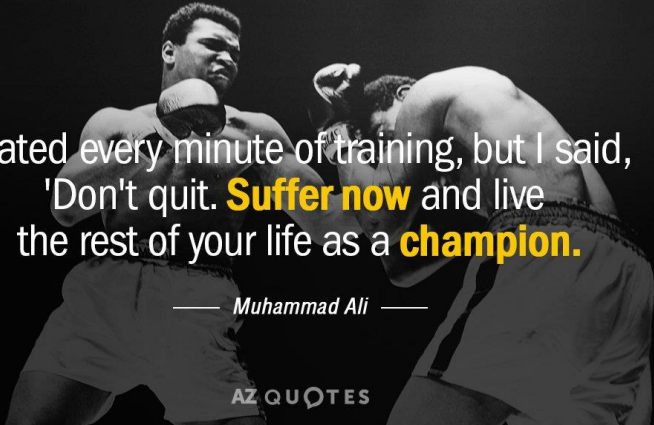


# Training

Incident response needs to be **practiced** in order to be **executed** quickly.

Focus training on criteria and standards to **promote creative thinking** within the **framework**.

Use **skills assessments** to ensure that the IRT includes all **necessary skillsets**.

A black and white photograph of Muhammad Ali in a boxing stance, wearing boxing gloves and trunks. He is looking forward with a determined expression.

I hated every minute of training, but I said, 'Don't quit. **Suffer now** and live the rest of your life as a **champion**.

— Muhammad Ali —

AZ QUOTES



# The Role of Testing



Testing increases the likelihood that a plan will work by:

- Assessing the **technical soundness** of the plan
- Increasing each **participant's familiarity** with the plan



Testing uses:

- **time**
- **resources**
- objectives and criteria should be clear.

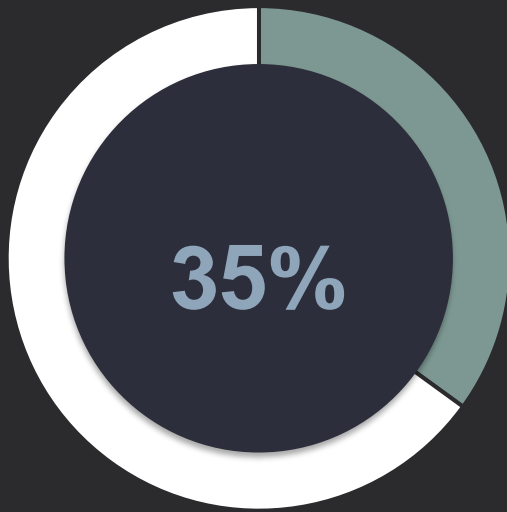


Focus on:

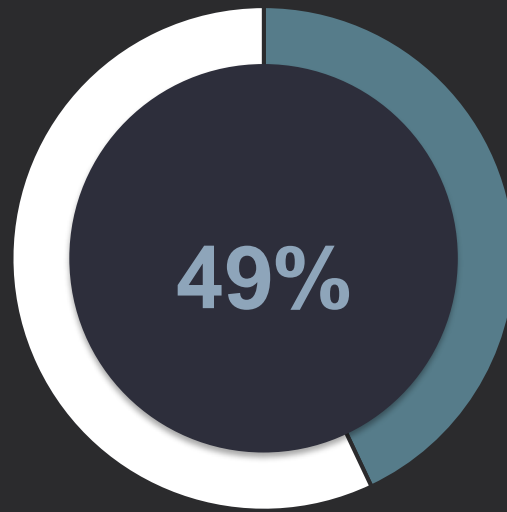
- Identifying **gaps**
- Verifying **assumptions**
- Validating **timelines**
- Determining the **effectiveness** of strategies
- Evaluating the **performance** of personnel
- Determining the **accuracy** of the plan

# But people know better, right?

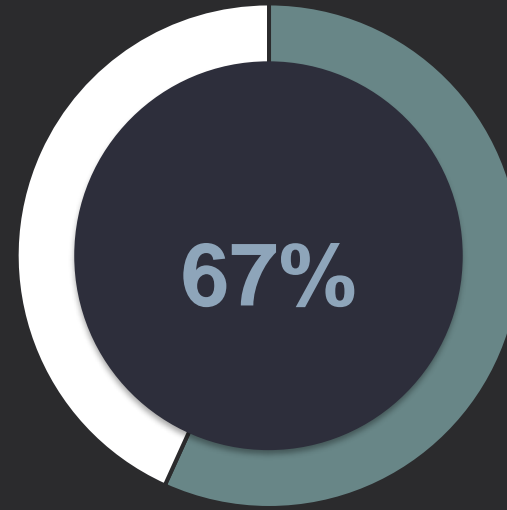
---



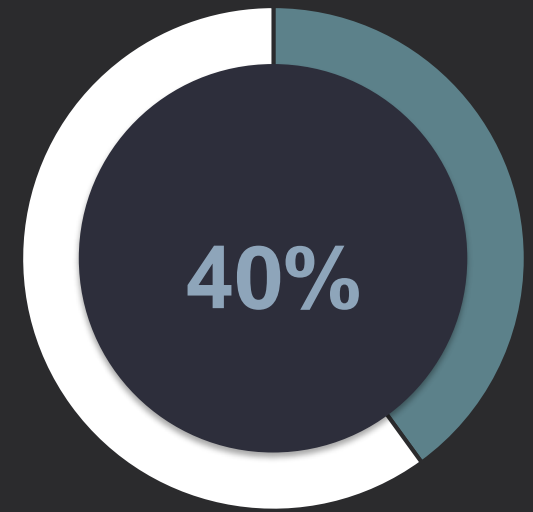
of workers who know  
they've been hacked  
don't bother to change  
their passwords  
afterward



of employees admit  
they click links in messages  
from unknown senders  
during work



of workers are sure  
they've received at  
least one phishing  
email at work



Of those who received  
a phishing email, ~40%  
didn't report it

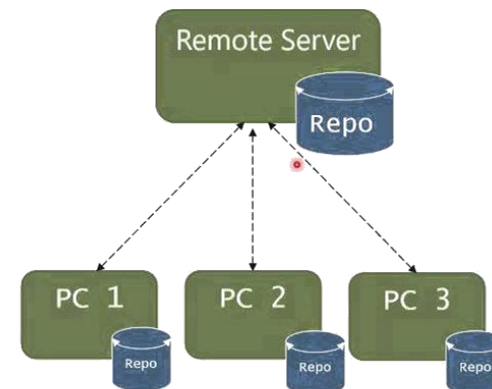
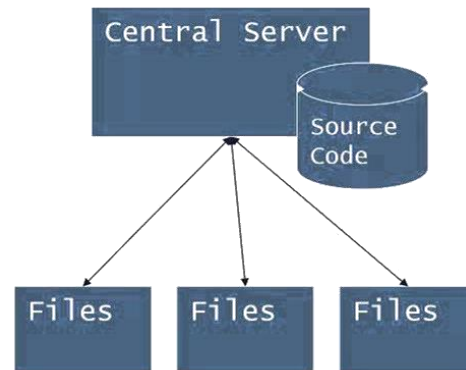
# Incident Management Systems

## Centralized incident management systems

- Pull together data from distinct capabilities for common analysis
- Example: SIEM

## Distributed incident management systems

- Consist of multiple specific incident detection capabilities
- Example: IDS





# Triage

A process of sorting, categorizing, prioritizing and assigning incoming reports/events.

Use BIAs and recovery plans to guide this process.



Problems that cannot be easily resolved



Problems that can wait



Problems that can be efficiently address with available resources





Team  
Work





You are the first line of defense when it comes to protecting the organization from cyber threats.

Stay safe, and we will have a wonderful year!

# 2021

CURR JONES



