

A	90% - 100%
B	80% - 89%
C	70% - 79%
D	60% - 69%
F	0% - 59%

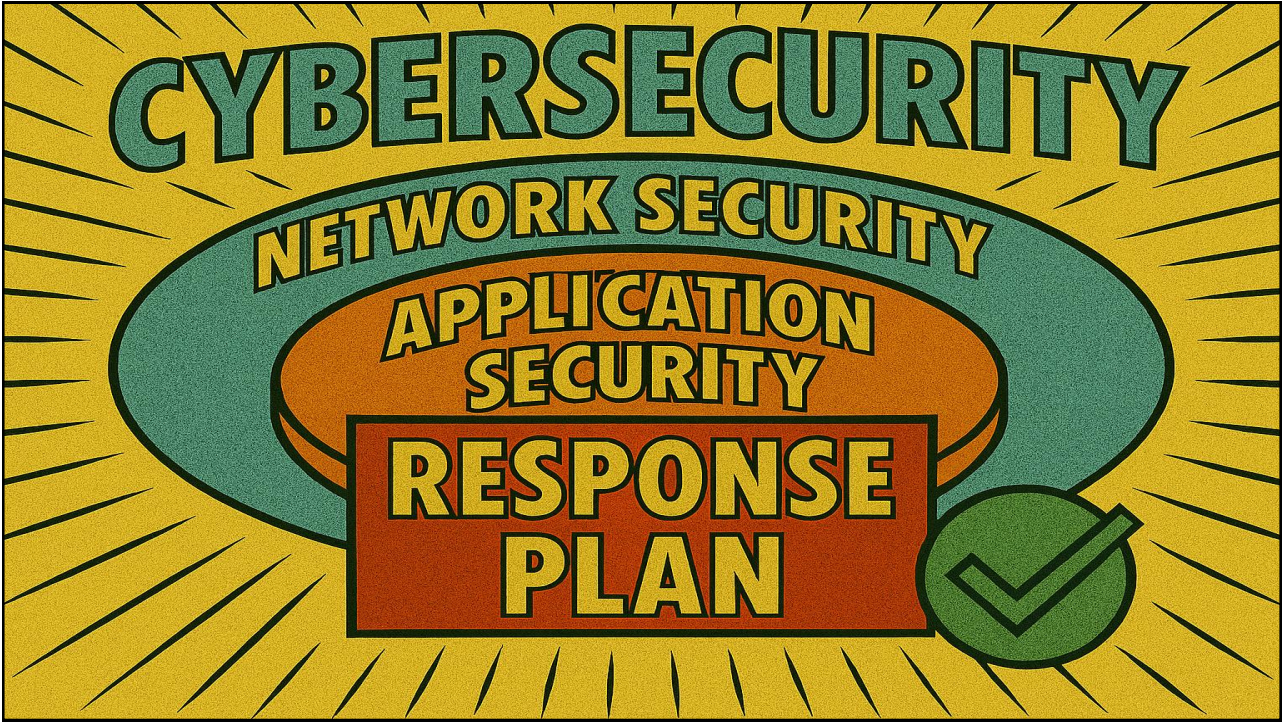
50% of all cyber attacks are successful

1



What protections are in place already?

2



3



4

Does your agency
have a Cyber Incident
Response Plan?

5

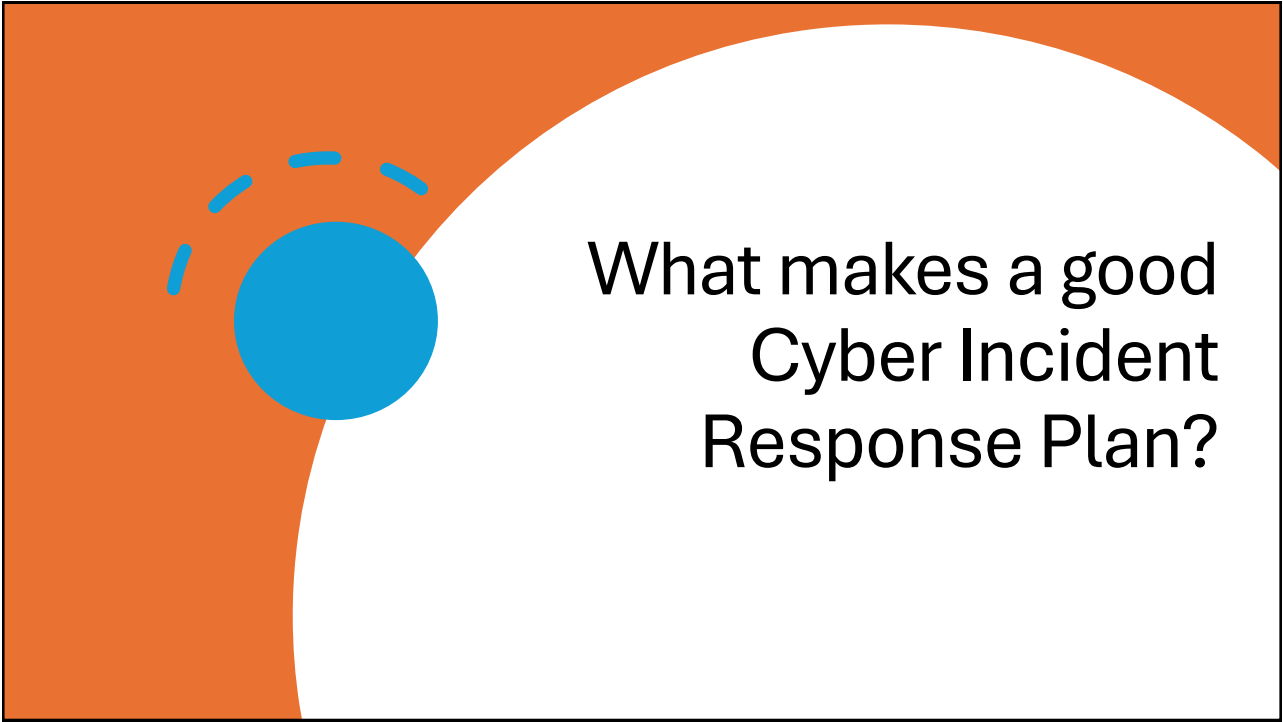


6



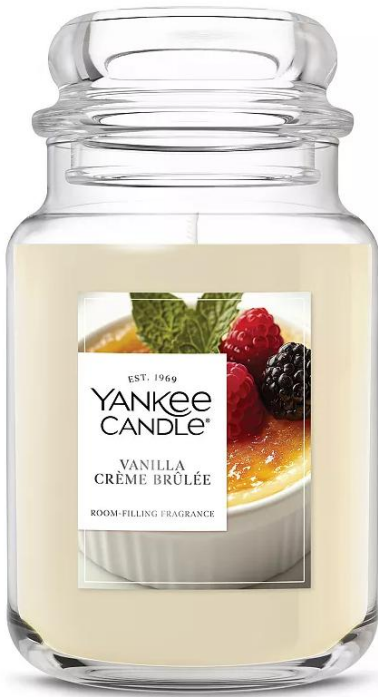
How can we
learn from this?

7



What makes a good
Cyber Incident
Response Plan?

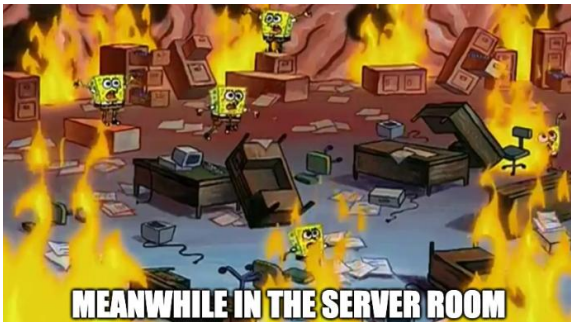
8



Let's Build a Plan:

1.) Identifying Critical Assets and Threats

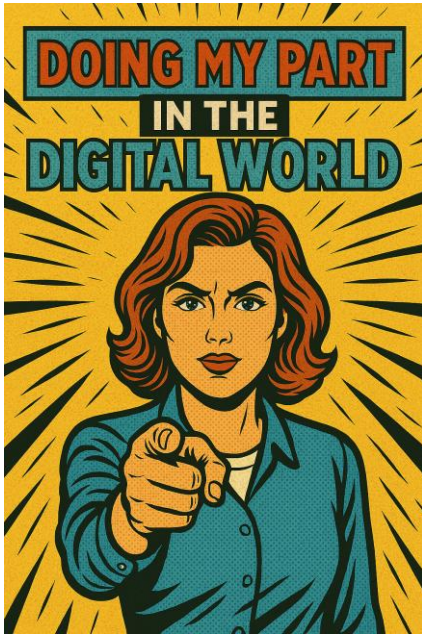
9



Let's Build a Plan:

- 1.) Identifying Critical Assets and Threats
- 2.) Define Incident Types and Severity

10



Let's Build a Plan:

- 1.) Identifying Critical Assets and Threats
- 2.) Define Incident Types and Severity
- 3.) **Assign Roles and Responsibility**

11

**IN CASE OF FIRE
ELEVATORS ARE
OUT OF SERVICE**



USE EXIT

Let's Build a Plan:

- 1.) Identifying Critical Assets and Threats
- 2.) Define Incident Types and Severity
- 3.) Assign Roles and Responsibility
- 4.) **Create Playbooks for Common Scenarios**

12



Let's Build a Plan:

- 1.) Identifying Critical Assets and Threats
- 2.) Define Incident Types and Severity
- 3.) Assign Roles and Responsibility
- 4.) Create Playbooks for Common Scenarios
- **5.) Establish Communication Protocols**

13

Let's Build a Plan:

1.) Identifying Critical Assets and Threats

2.) Define Incident Types and Severity

3.) Assign Roles and Responsibility

4.) Create Playbooks for Common Scenarios

5.) Establish Communication Protocols

6.) **Document, Test, and Update**

14

Practice Makes Perfect
let's start now.

15

1.) Identifying Critical Assets and Threats	1.) What resource is being affected?
2.) Define Incident Types and Severity	2.) What type of incident is this?
3.) Assign Roles and Responsibility	3.) What is mine/others role in responding to this?
4.) Create Playbooks for Common Scenarios	4.) What should I do right now?
5.) Establish Communication Protocols	5.) Who do I notify? What do I say?
6.) Document, Test, and Update	6.) Have we practiced this response?

16



visionIT
by tripleview



Book a Meeting

Dalton Lundgren

509-315-3215

Dlundgren@tripleview.com



Contact Info

17

Morgan Zantua
Associate Professor and Director - Center
for Cybersecurity Innovation at the City U...



Office: 206-239-4865

Cell: 253-677-5649

Zantuamorgan@cityu.edu

18