PHISHING

in your own pond…

Gary Blackburn
May 2014

WHY?

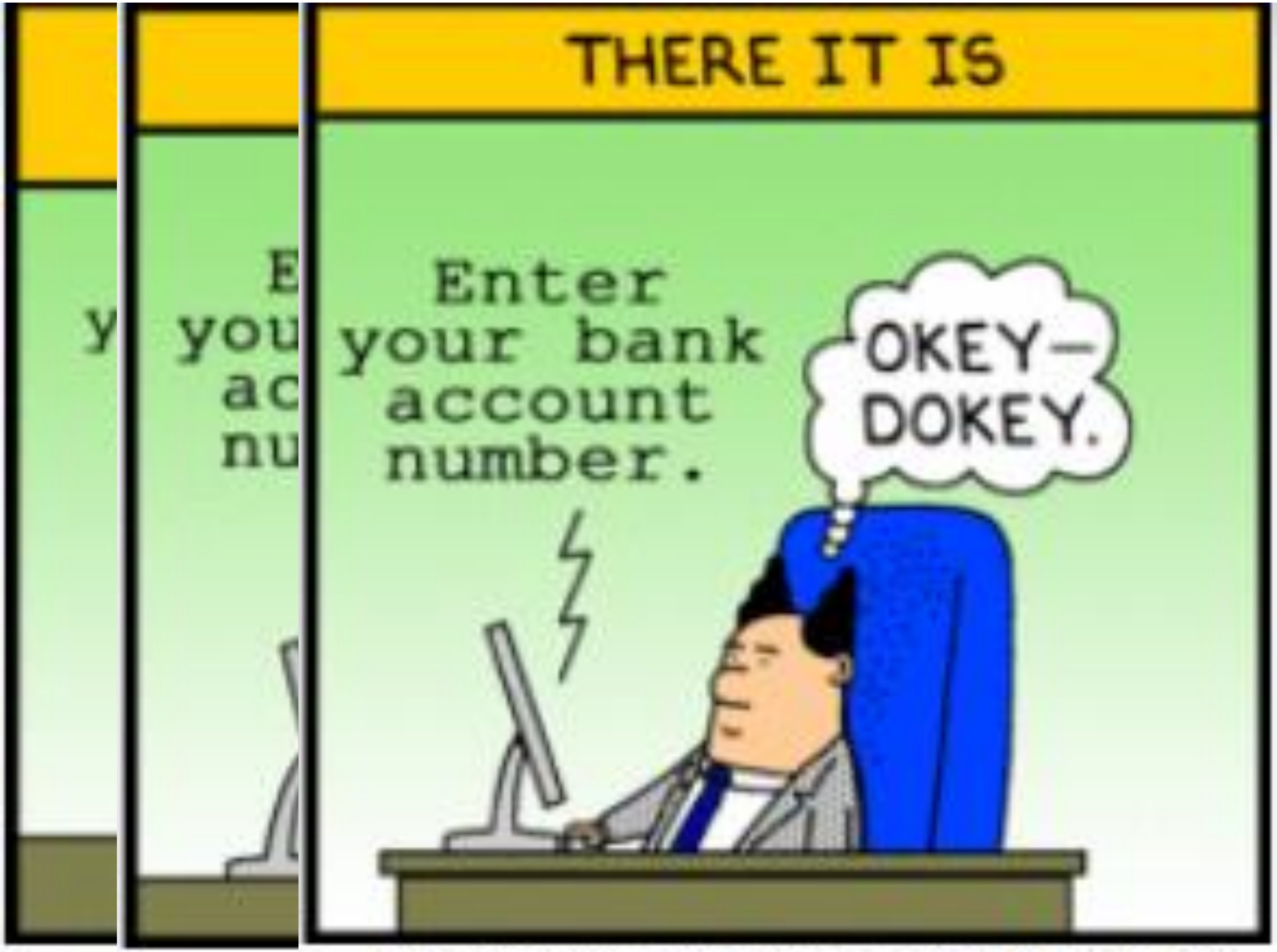
*** Valuable Training,**

*** Common attack vector,**

*** Attacks are successful**

People are social creatures, with predictable behaviors!

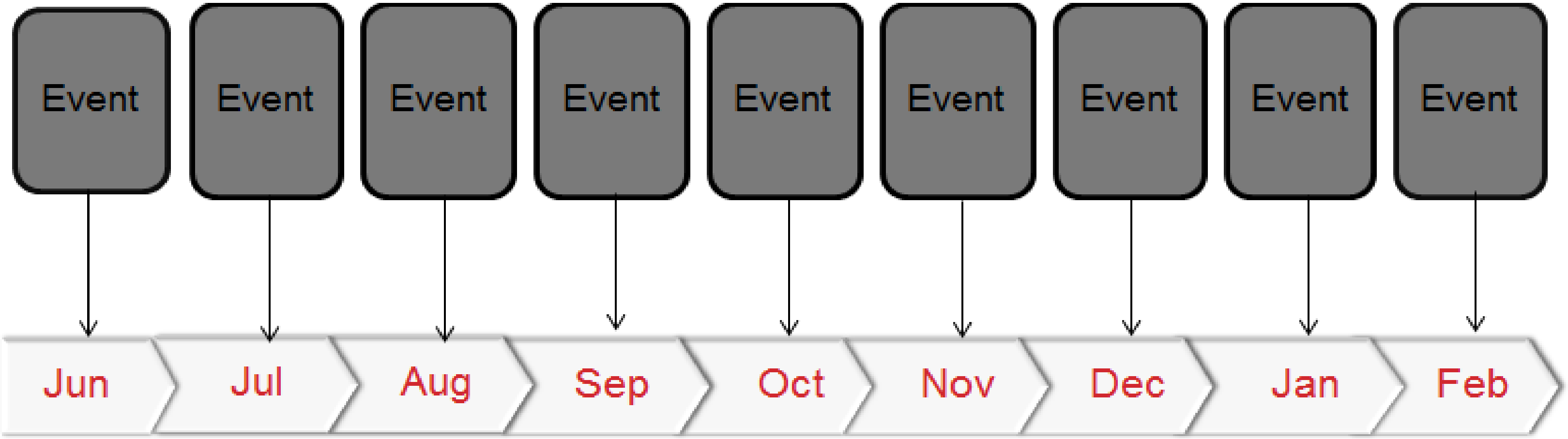
Sophisticated technical controls aren’t enough…



http://www.dilbert.com/2014-05-19/

THE APPROACH

1. Select targets – Random, representative
2. Execute Phish
3. Train victims, immediate feedback
4. Collect and analyze metrics
5. Report and train ALL USERS



MANAGING RISK

- **Minimize operational impact**
  - Small sample of users targeted; less than 15% of organization
- **Contain exercise activity, reduce political risks**
  - “Rogue” web site is hosted internally
  - Email blocking capability
- **Reduce legal risks**
  - No impersonation / only fictitious entities used
  - No Personally Identifiable Information (PII) collected on victims

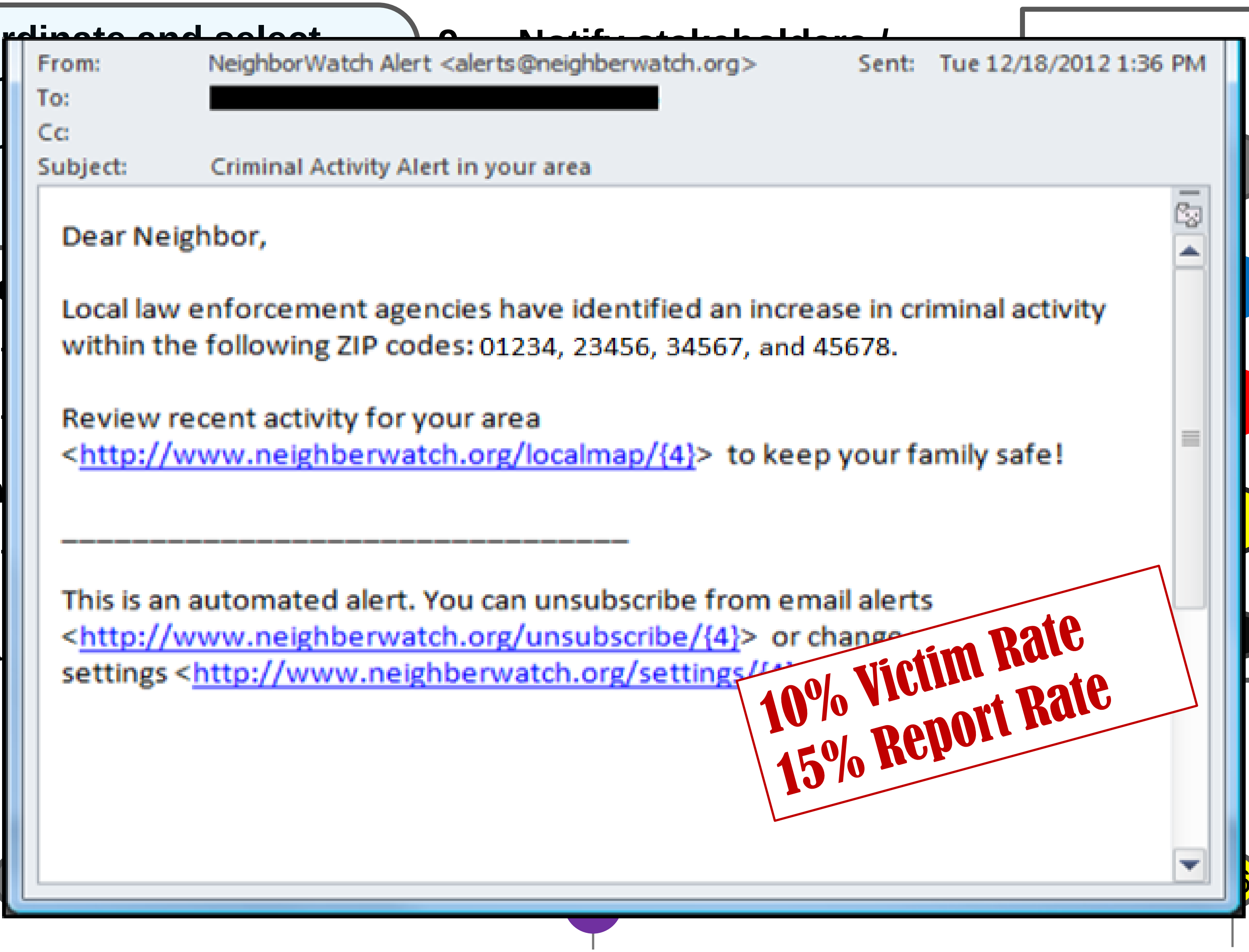
MANAGING RISK

- **De-confliction**
  - Strong event communications plan
- **Coordination**
  - Stakeholders identified, trusted insiders established
- **Event Integrity**
  - A ‘safe
  - training event’, anonymous results
- **Feedback**
  - Victims immediate, users overall summary

EVENT OVERVIEW

1. Coordinate and select
ever
2. Auth
3. Faci
4. Deve
5. Con
6. Con
7. Iden
8. Con
and
ema

9. Notify stakeholders /



From: NeighborWatch Alert <alerts@neighberwatch.org>
Sent: Tue 12/18/2012 1:36 PM
To: [redacted]
Cc:
Subject: Criminal Activity Alert in your area

Dear Neighbor,

Local law enforcement agencies have identified an increase in criminal activity within the following ZIP codes: 01234, 23456, 34567, and 45678.

Review recent activity for your area <http://www.neighberwatch.org/localmap/{4}> to keep your family safe!

____

This is an automated alert. You can unsubscribe from email alerts <http://www.neighberwatch.org/unsubscribe/{4}> or change settings <http://www.neighberwatch.org/settings/{4}

10% Victim Rate
15% Report Rate

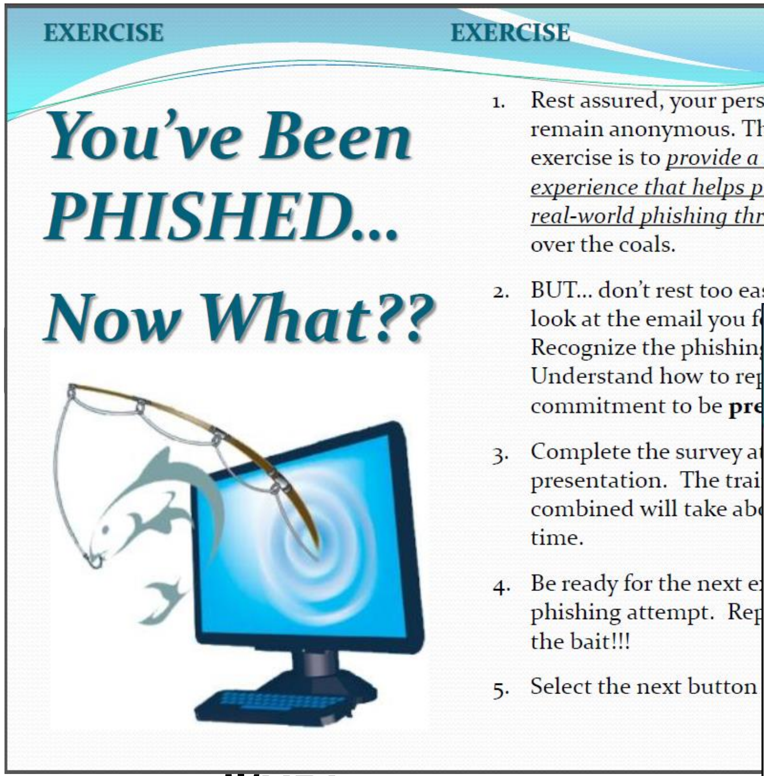
1 2

- 2 weeks

Event Execution

+ 2 weeks

EVENT OVERVIEW



EXERCISE EXERCISE EXERCISE

You've Been PHISHED…

Now What??

1. Rest assured, your personal identity will remain anonymous. The point of the exercise is to *provide a realistic training experience that helps prepare you to face real-world phishing threats*, not to rake you over the coals.
2. BUT… don't rest too easy. Take another look at the email you f
Recognize the phishin
Understand how to rep
commitment to be **pre**
3. Complete the survey at
presentation. The trai
combined will take ab
time.
4. Be ready for the next e
phishing attempt. Rep
the bait!!!
5. Select the next button

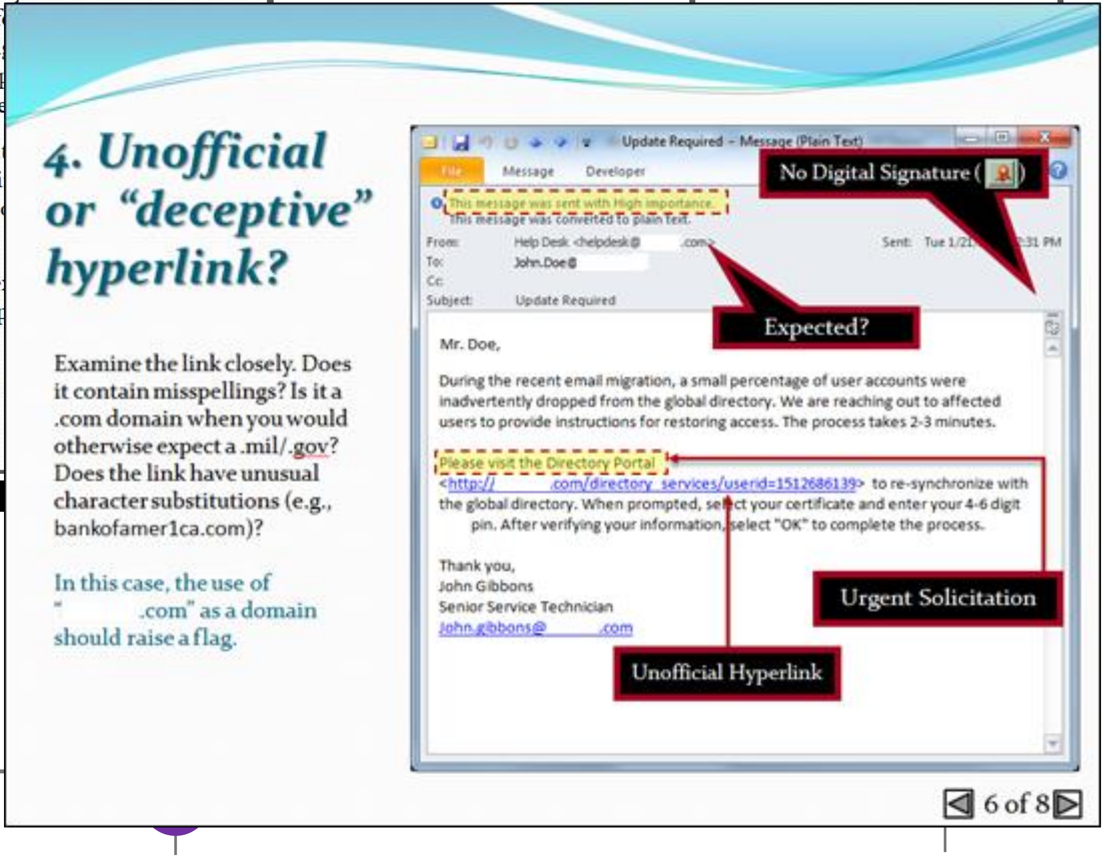
akeholders /
gents of event

attack

metrics

Legend

Event Coordinator



4. Unofficial or "deceptive" hyperlink?

Examine the link closely. Does it contain misspellings? Is it a .com domain when you would otherwise expect a .mil/.gov? Does the link have unusual character substitutions (e.g., bankofamer1ca.com)?

In this case, the use of " .com" as a domain should raise a flag.

This message was sent with High importance.
This message was converted to plain text.

From: Help Desk <helpdesk@ .com>
To: John.Doe@
Cc:
Subject: Update Required
Sent: Tue 1/21 :31 PM

Mr. Doe,

During the recent email migration, a small percentage of user accounts were inadvertently dropped from the global directory. We are reaching out to affected users to provide instructions for restoring access. The process takes 2-3 minutes.

Please visit the Directory Portal
<http:// .com/directory_services/userid=1512686139> to re-synchronize with the global directory. When prompted, select your certificate and enter your 4-6 digit pin. After verifying your information, select "OK" to complete the process.

Thank you,
John Gibbons
Senior Service Technician
John.gibbons@ .com

email/URL

1

1 2 3 4 5 6 7 8

- 2 weeks

Event Execution

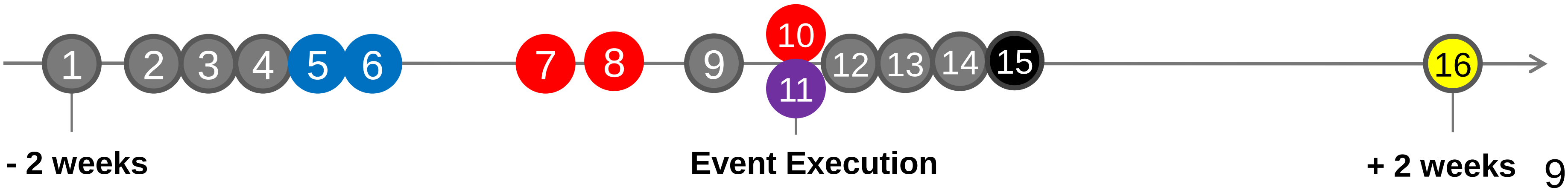
+ 2 weeks

EVENT OVERVIEW

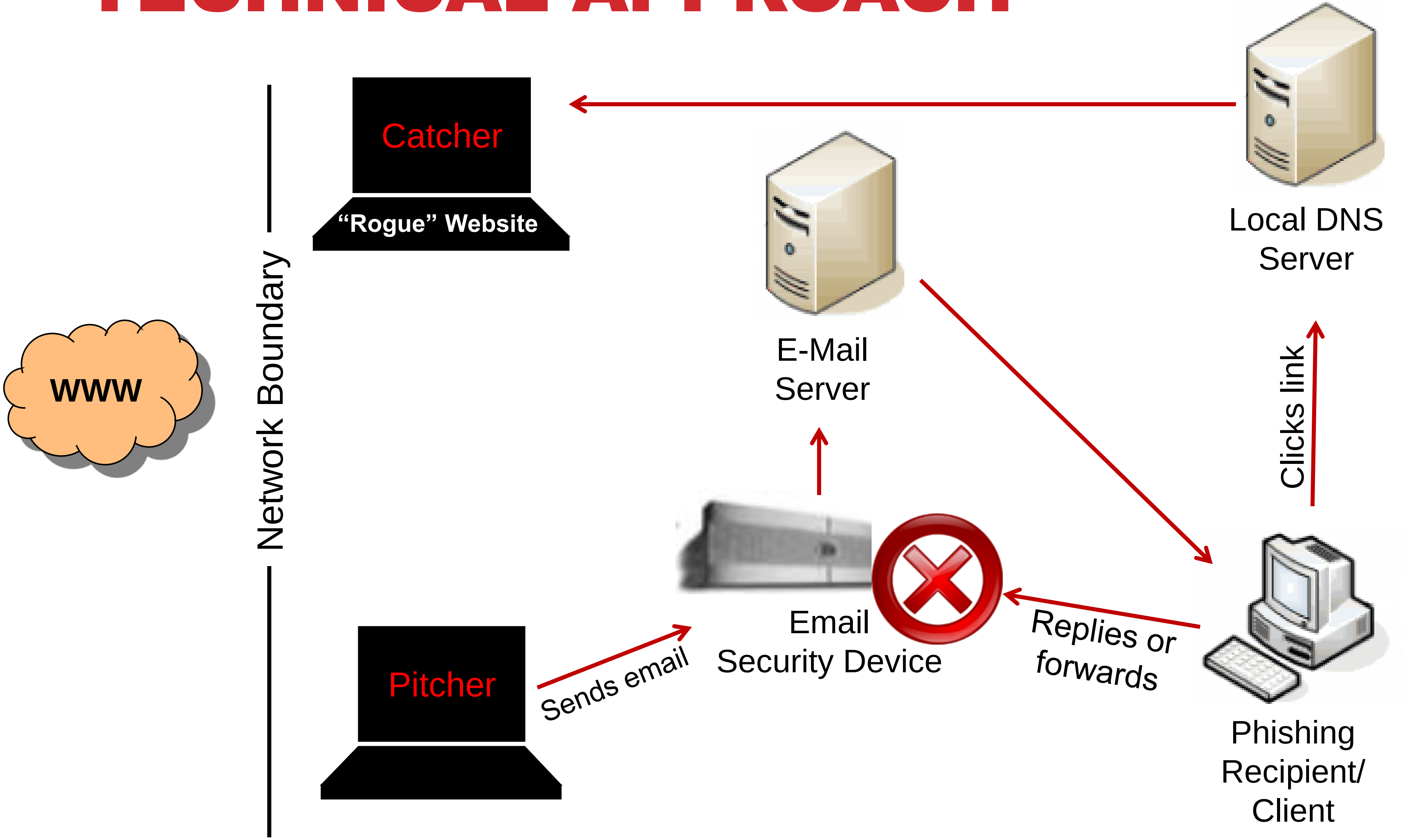
1. Coordinate and select event date
2. Author/select phish email
3. Facilitate legal review
4. Develop landing page
5. Configure local DNS
6. Configure email gateway
7. Identify email recipients
8. Configure attack script and test phishing email/URL
9. Notify stakeholders / trusted agents of event
10. Execute attack
11. Collect metrics
12. Prepare/send executive summary
13. Praise reporters
14. Prepare event recap training
15. Publish event recap
16. Publish final report

Legend

- Event Coordinator
- Network Defenders
- Execution Team
- Analytics Lead
- CIO



TECHNICAL APPROACH

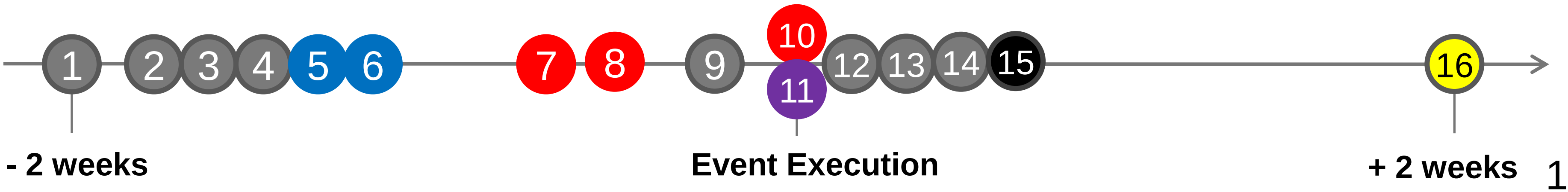


EVENT OVERVIEW

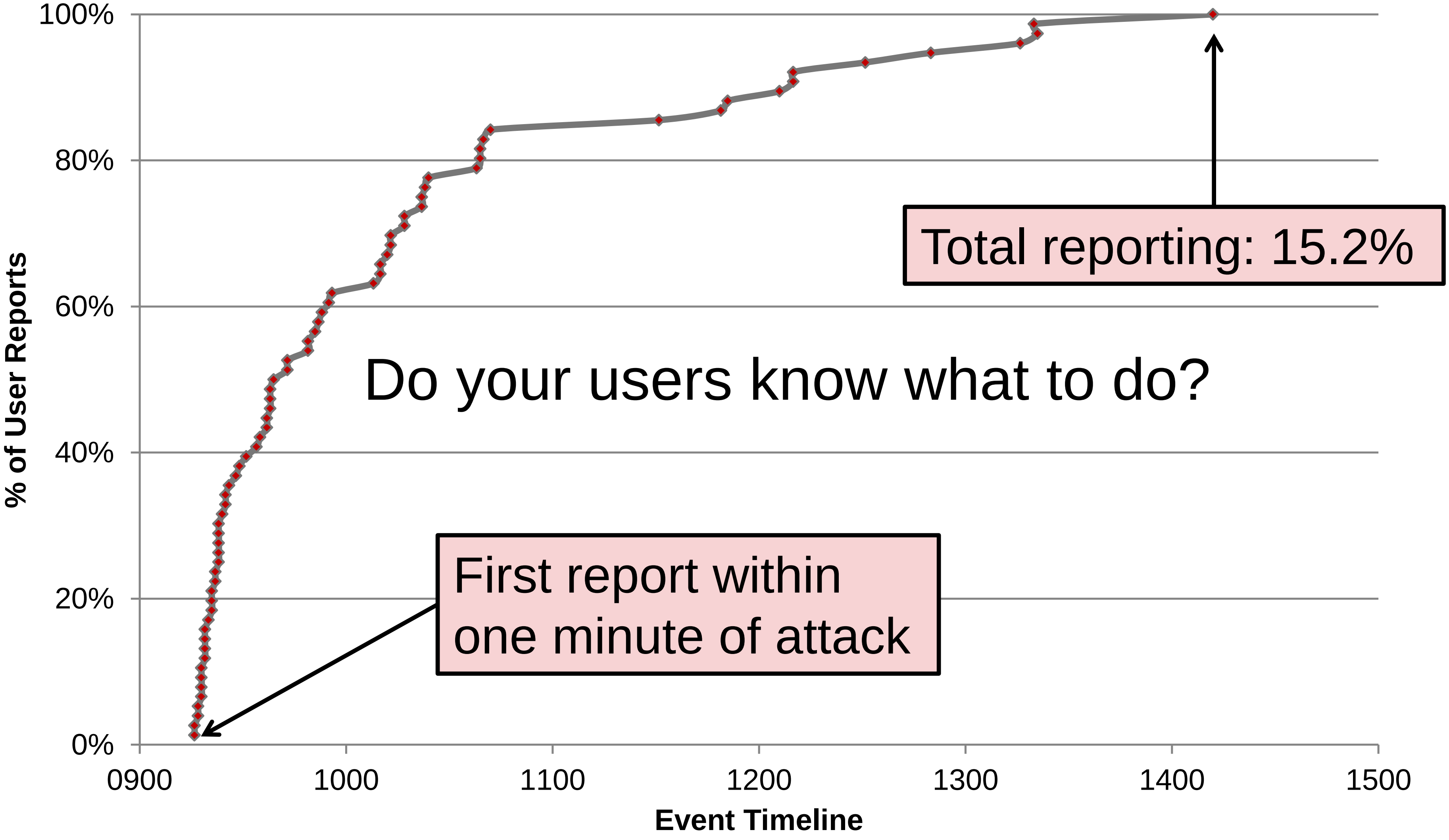
1. Coordinate and select event date
2. Author/select phish email
3. Facilitate legal review
4. Develop landing page
5. Configure local DNS
6. Configure email gateway
7. Identify email recipients
8. Configure attack script and test phishing email/URL
9. Notify stakeholders / trusted agents of event
10. Execute attack
11. Collect metrics
12. Prepare/send executive summary
13. Praise reporters
14. Prepare event recap training
15. Publish event recap
16. Publish final report

Legend

- Event Coordinator
- Network Defenders
- Execution Team
- Analytics Lead
- CIO



USER REPORTING

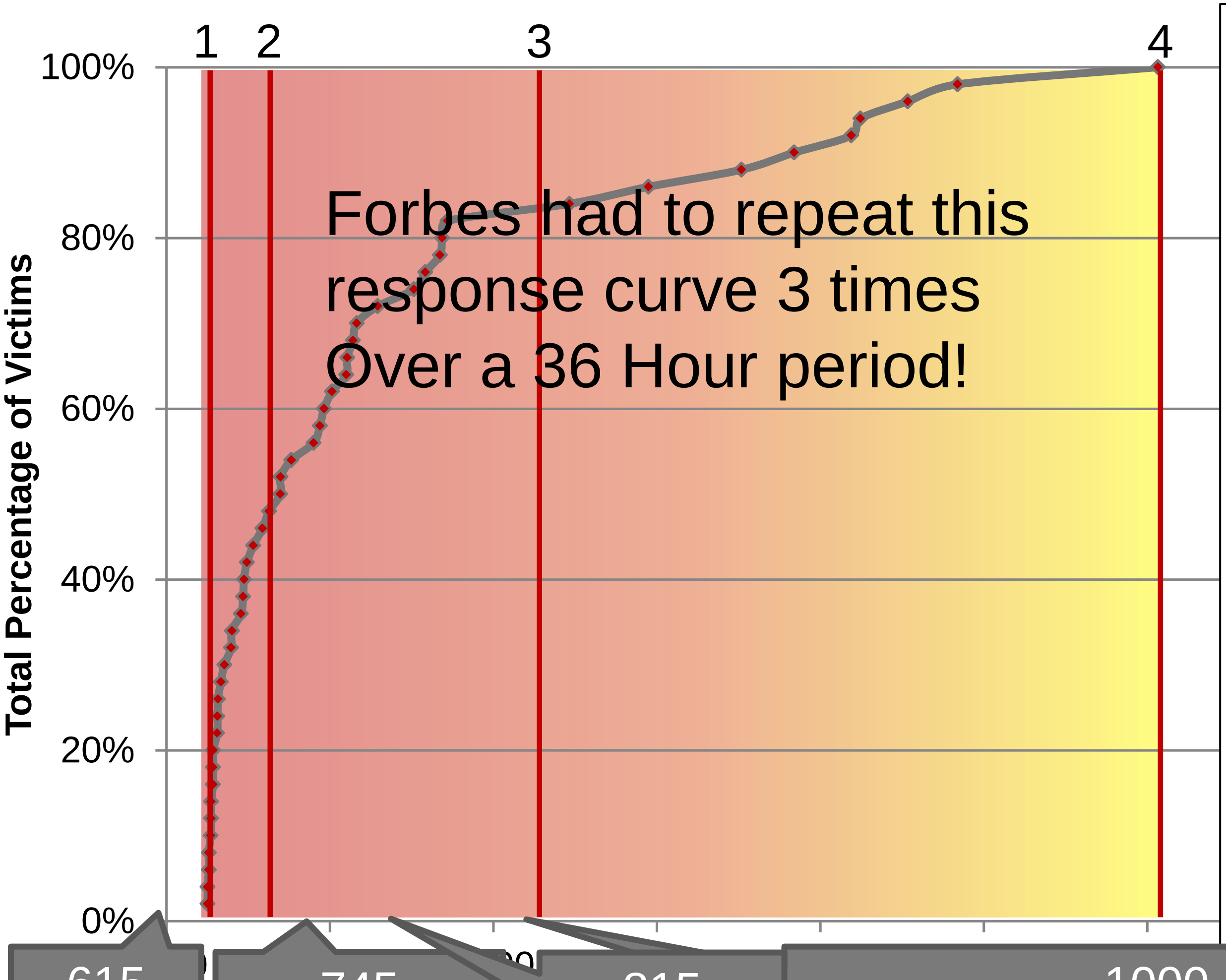


Total reporting: 15.2%

Do your users know what to do?

First report within one minute of attack

TIMING OF VICTIMS VS NOTIONAL NET DEFENSE RESPONSE



Forbes had to repeat this response curve 3 times Over a 36 Hour period!

615 Phish

745 2nd Phish

815 Warning

1000 Administrative shutdown

1. **First report (7 victims)**

   Network defenders receive 1st user report of suspicious activity

2. **Attack + 15 mins (24 victims)**

   Reflects the point at which outbound web traffic to malicious IP(s) *might* be blocked, effectively blocking command and control

3. **Attack + 2 hours (41 victims)**

   Reflects the point at which phishing emails *might* be removed from infected mailboxes, removing the threat footprint and any associated footholds

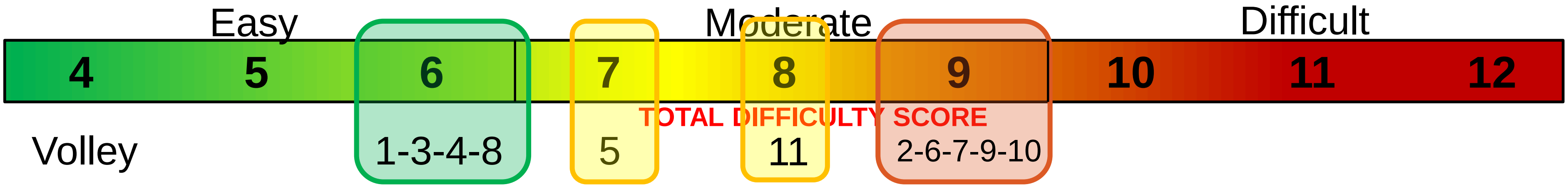
ms)

OTHER METRICS

- **Email Forwarding**
  - On average, 4% of recipients attempt to forward email externally
- **Email Replies**
  - On average, 6% of recipients attempt to reply to fictitious sender
  - Most are the result of “out of office” agents (auto-replies)
  - Use of “out of office” can increase risk to the organization

PREDICTORS AND SCORING MODEL

Personalization	1 Low; no personalized characteristics (more likely to appear as SPAM)	2 Medium; refers to at least one characteristic familiar to the user (e.g., industry, region, company name)	3 High; contains highly personalized elements (spear-phishing by name or department)
Appeal/ Applicability	1 Low; applicable to only a small number of recipients	2 Medium; applicable to a large number of recipients	3 High; potentially applicable to all recipients
Perceived Urgency	1 Low; recipient has a lot of time to respond (unlimited to weeks/days)	2 Medium; recipient has limited time to respond (day/hours)	3 High; recipient has very little time to respond (hour/minutes)
Consequence/ Opportunity Lost	1 Low	2 Medium	3 High



	Easy				Moderate		Difficult		
	4	5	6	7	8	9	10	11	12
Volley			1-3-4-8	5	11	2-6-7-9-10			

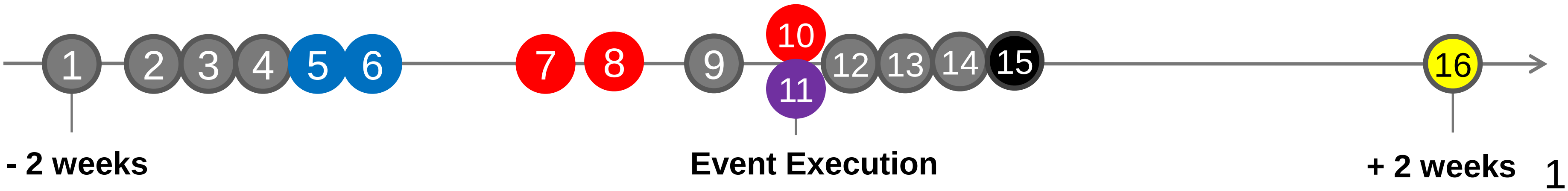
TOTAL DIFFICULTY SCORE

EVENT OVERVIEW

1. **Coordinate and select event date**
2. **Author/select phish email**
3. **Facilitate legal review**
4. **Develop landing page**
5. **Configure local DNS**
6. **Configure email gateway**
7. **Identify email recipients**
8. **Configure attack script and test phishing email/URL**
9. **Notify stakeholders / trusted agents of event**
10. **Execute attack**
11. **Collect metrics**
12. **Prepare/send executive summary**
13. **Praise reporters**
14. **Prepare event recap training**
15. **Publish event recap**
16. **Publish final report**

Legend

- Event Coordinator
- Network Defenders
- Execution Team
- Analytics Lead
- CIO



EVENT REPORTS

Deliverable/ Report	Target Audience	Periodicity/ Timeline	Description
Executive Summary	CIO	Within 2 hours of event end	Executive summary of the event properties and event results (e.g., 37% failure rate).
Event Recap Article	All users	Within 24 hours of event end	Non-attributional summary and result of the phishing event. Identifies indicators of phishing attempt and how users should respond/report.
Detailed Report	CIO	Within two weeks of event end	Detailed report showing event approach, metrics, results and analysis.
Quarterly Progress Report	CIO	Quarterly, within two weeks of event end	Detailed report highlighting successes, challenges, trends, etc. Identifies whether objectives were met/unmet.

“Event training recap” provides an opportunity for all users to learn from each training scenario

SUMMARY

- Steady increase in user reporting in both real-world and exercise phishing scenarios
- Organizational victim rate has remained largely unchanged since the start (Average: 10%)
- Participant survey results overwhelmingly positive: 97% say live phishing scenarios realistic and impactful

Insure your users know how to respond!

DISCUSSION / QUESTIONS