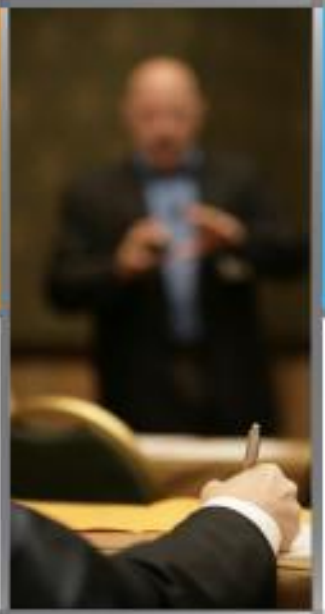
@CSOevents
#CSO50

CSO50 CONFERENCE+AWARDS

Aligning Proactive Security with Modern Threats



May 1-3, 2017

The Scottsdale Resort
Scottsdale, Arizona

PRODUCED BY
CSO
FROM IDG

CSO 50 CONFERENCE +AWARDS

Improving Safety and Security Through Improved Awareness

Bob Eichler

Director of Information Security

Cancer Treatment Centers of America

Cancer Treatment Centers of America®

Making Information Security Important to Your Users

Bob Eichler – Director, Information Security

"In an age of cyber threats, we must ensure that a patient's information is treated with as much care as our clinicians give their bodies."

- Bob Eichler

About me…

Bob Eichler

- Director of Information Security at Cancer Treatment Centers of America since 2009
- Charged with protecting some of the most sensitive information people possess
- Previously Enterprise Security Architect at one of the world's largest airlines
- 20+ years' experience in IT Security space
- Smart enough to surround myself with really good security professionals!

$1,000,000,000

A report by cybersecurity company, Herjavec Group, asserts that $209M was paid in cyber-ransoms in 1Q 2016.

Ransomware is worth a cyber criminal's investment

Cancer Treatment Centers of America
Winning the fight against cancer, every day.®

2016 numbers from the Internet*:

- Number of new ransomware modifications in Q1: 2,900
- Number of new modifications in Q3: 32,091 (11x as many!)
- Q1 – Individuals attacked every 20 seconds
- Q3 – Individuals attacked every 10 seconds (2x as fast!)
- Q1 – Business attacked every 2 minutes
- Q3 – Business attacked every 40 seconds (3x as fast!)

*Source: Kaspersky Lab

The power of a mouse click…

- Encrypt every file on your computer
- Encrypt every file on a departmental shared drive
- Encrypt every file on every mapped drive that can be reached on the network
  - (Thanks a lot, Locky!)

What is the "We ARE Safe" Program?

Industry Standard Anti-Malware Program

- AV + Anti-malware solutions
- Anti-spam / content filtering
- Backup / recovery procedures
- Alerting / notification procedures
- Awareness training program
  - Newsletters
  - Computer based training
  - Handouts
  - Phishing exercises

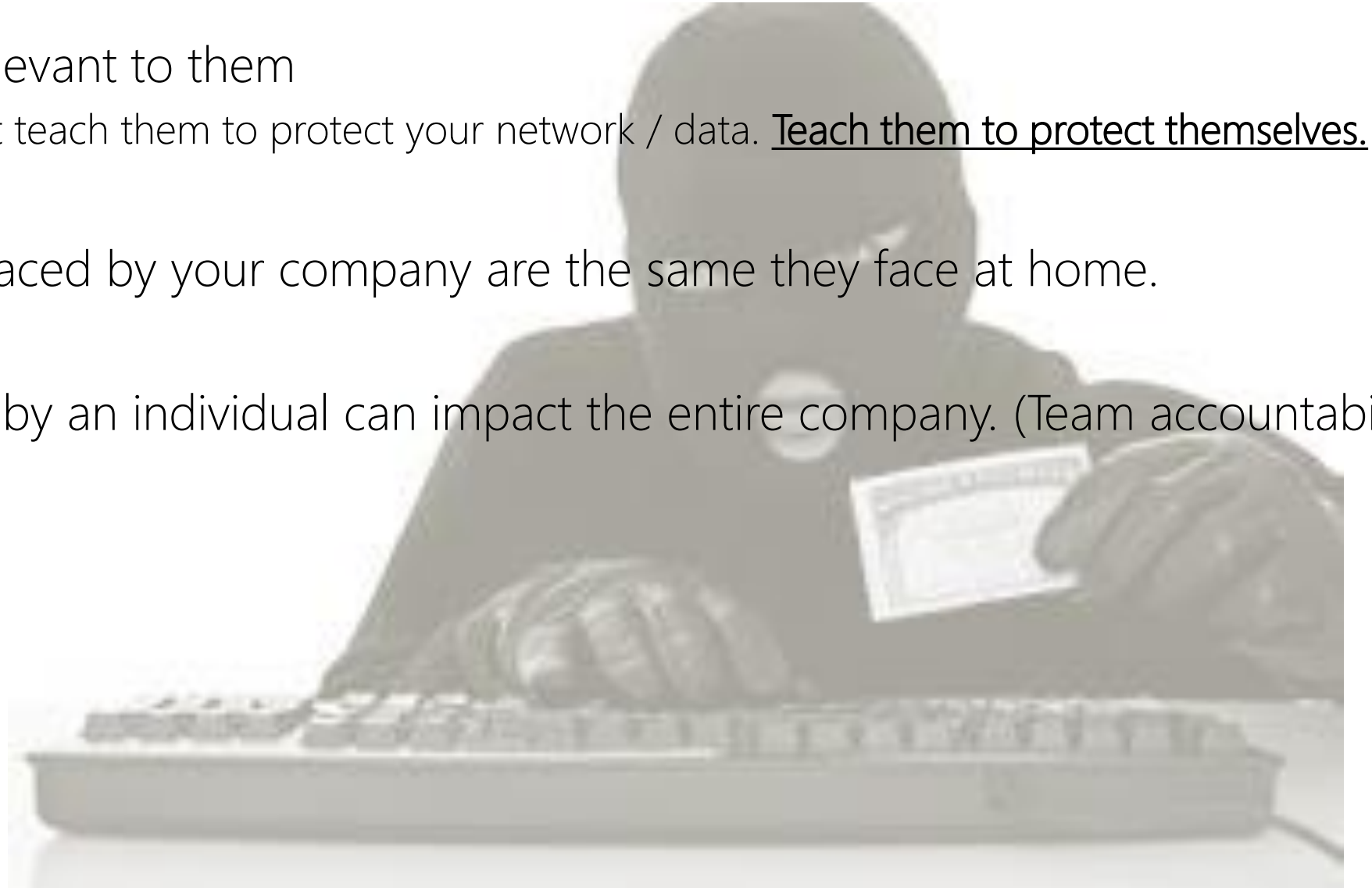
How do you engage your users?

Make it relevant to them

- Don't teach them to protect your network / data. Teach them to protect themselves.

The risks faced by your company are the same they face at home.

A mistake by an individual can impact the entire company. (Team accountability)



The Talk…

…about Passwords!

How many passwords do you need to manage?

Average is 20-30

How do you manage all these?

Most try to make them all the same

Who has a Yahoo email account?

Compromised for 2-3 years

The password you have been using for everything has been floating around the Internet for years

When's the last time you changed you personal email password?

The Talk…

…about Malware!

From compromised websites:

When you're on MSN.com or Facebook, and click on the link to see the child stars of the '80's and '90's, you're no longer where you started.

From Email / Phishing:

You've successfully avoided the Nigerian Oil Minister

What about the message from "FedEx"?

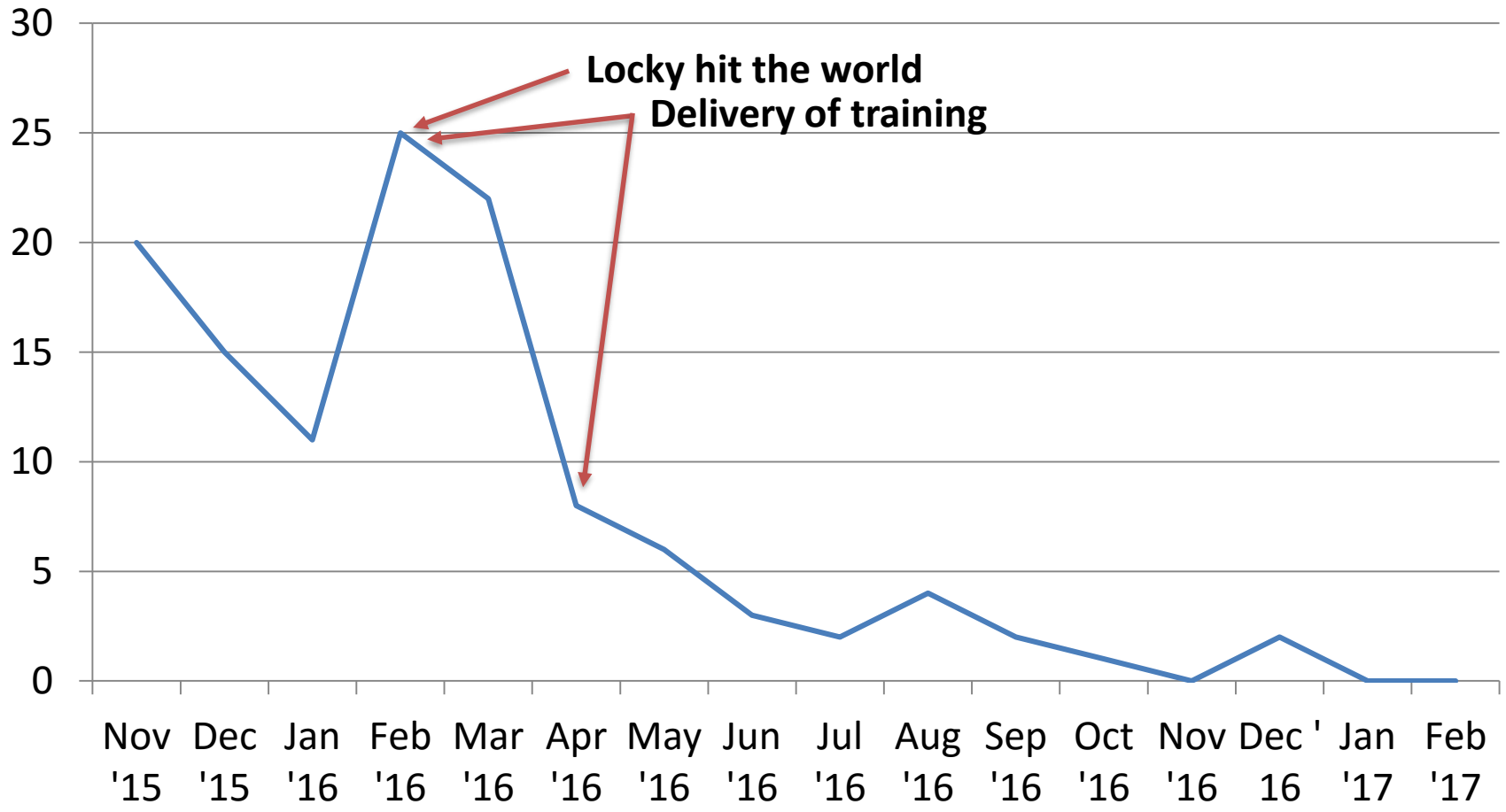
What about the message with the receipt / invoice / resume?

What about the message from your boss?

What was the impact?

- We know there are no silver bullets…
- Standard tools had positive impact
- General awareness helped reduce impact
- How many people did your training really reach?

Security events



Lessons learned and takeaways:

- Emails and Posters are of limited value
- Mandatory online training courses are slightly better
- Large, generic, meetings are avoided because users are “too busy” or they “forgot”
- People react best when spoken to in smaller groups, in their local work area
- Make the risk relatable. Provide real examples. Try to make it humorous. Tie it to something personal. Allow for Q/A.

Perspective

Examine entire information security budget:

2015 CIO magazine article: 11-15% of your IT budget

Does the investment of a few thousand dollars in resource time and travel provide an adequate return?

I assert "YES!"