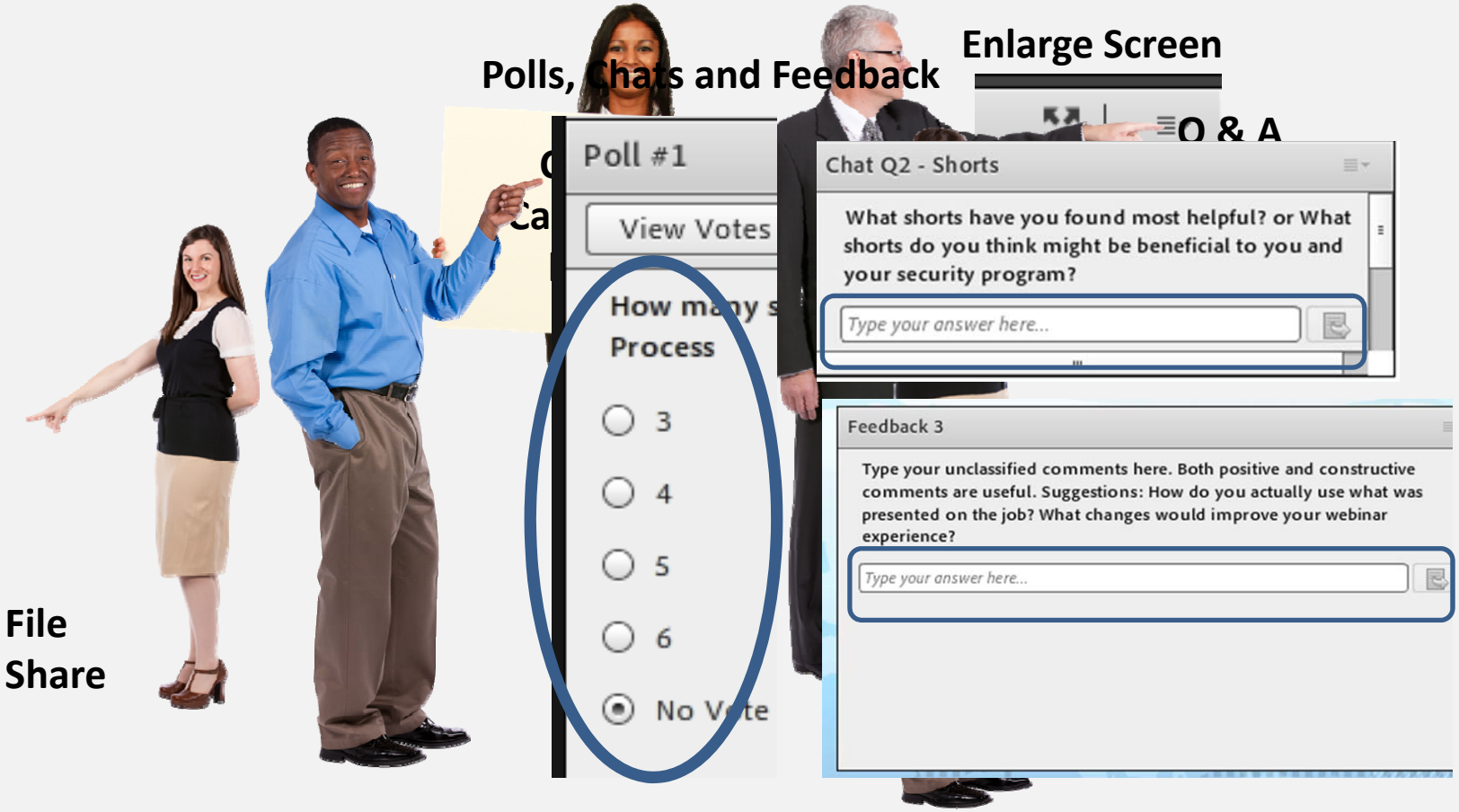
CDSE Center for Development of Security Excellence

The Top 10 Cybersecurity incidents of 2017

LEARN.
PERFORM.
PROTECT.


Polls, Chats and Feedback
Enlarge Screen
Q & A
Poll #1
View Votes
Process
3
4
5
6
No Vote
Chat Q2 - Shorts
What shorts have you found most helpful? or What shorts do you think might be beneficial to you and your security program?
Type your answer here...
Feedback 3
Type your unclassified comments here. Both positive and constructive comments are useful. Suggestions: How do you actually use what was presented on the job? What changes would improve your webinar experience?
Type your answer here...
File Share

Back to 2017…

MILK

FEDERAL RESERVE NOTE
THE UNITED STATES OF AMERICA
B 03542754 F
WASHINGTON, D.C.
ONE DOLLAR

Back to 2017…

51% of the world's population is online

4000 Ransomware attacks every day

$1 billion in ransomware payments

2 Minutes: the time it takes for an IoT device to be attacked

1.4 million phishing websites created every month

197: average number of days to detect a breach

1 in 131 emails contain malware

The

Top Ten

Cybersecurity incidents of 2017

10: Equifax

Credit reporting agency that collects information on more than 800 million individuals and 88 million businesses.

Impact:

145.5 Million (45% of the US population)

Cause:

Outdated / unpatched software

Lessons Learned:

- Patch management is key
- Regularly scan your systems
- Act first

9: Uber

Peer-to-peer ridesharing and food delivery company operating in 633 cities worldwide.

Impact:

57 million records

Cause:

Compromised developer accounts

Lessons Learned:

- Know data breach notification laws
- Protect admin accounts
- Use two-factor authentication (when possible)

8: Verizon

Telecommunications company specializing in wireless products and services.

Impact:

14 million records

Cause:

Unsecured cloud server maintained by third-party vendor

Lessons Learned:

- Ensure partners protect your data as well as you would
- Protect cloud storage accounts

7: Shadow Brokers Leaks

Hacker group tied to several leaks of NSA hacking tools and zero-day exploits.

Impact:

5 major leaks

200,000+ compromised computers

Cause:

Allegedly hacked NSA partner

Lessons Learned:

Install updates and patches

6: New Ransomware Variants

Malicious software designed to deny authorized users access to their files or system until a ransom is paid.

Impact:

$1,077 average

Over $5 billion worldwide

Cause:

User behavior

Misconfigured systems

Shadow Brokers leak

Lessons Learned:

- Install updates and patches
- User awareness training
- Anti-malware software
- BACKUP, BACKUP, BACKUP

5: Voter Record Leak

Voter records include names, birth dates, addresses, and voter registration details.

Impact:

198 million voter records

Cause:

Misconfigured cloud server

Lessons Learned:

Secure cloud storage

4: Emmanuel Macron Campaign Hack

Macron, then a candidate, is now the President of France.

Impact:

9GB of leaked emails from the campaign

Cause:

Phishing emails to obtain user passwords

Lessons Learned:

User awareness and training

Use two-factor authentication

3: Di5s3nSi0N vs ISIL

Self-described "steadfast youth of ahlus-Sunnah wal-Jammah" organized cyber attacks against ISIL.

Impact:

Leaked 2000 email addresses
Compromised Telegraph accounts
Multiple websites hacked

Cause:

Unknown

Lessons Learned:

Rise of hacktivism

2: Crash Override / Triton

Industrial Control Systems are used to support critical infrastructure, including power plants, water and wastewater, transportation, and similar sectors.

Impact:

Unknown
Power outages in Ukraine
Unsuccessful attack in the Middle East

Cause:

Targets specific manufacturer's systems
Payload after initial compromise
Most likely shutdown vs. damage

Lessons Learned:

Continued targeting of ICS

1: Yahoo (2 breaches)

Web services provider that was purchased by Verizon in 2017

Impact:

3 Billion

Cause:

Spear phishing email

Lessons Learned:

- Confirm email senders
- Don't click untrusted attachments
- Use strong encryption

Conclusion

1. Perform regular data backups
2. Update and patch systems
3. Secure cloud accounts
4. Ensure users are trained and aware of the threats