KENDALL SQUARE ASSOCIATION

Future of (how we) Work Task Force

Cybersecurity

Presenter

Neil Jones
Director of CyberSecurity Evangelism
EGNYTE

Kendall Square
The Future Lives Here

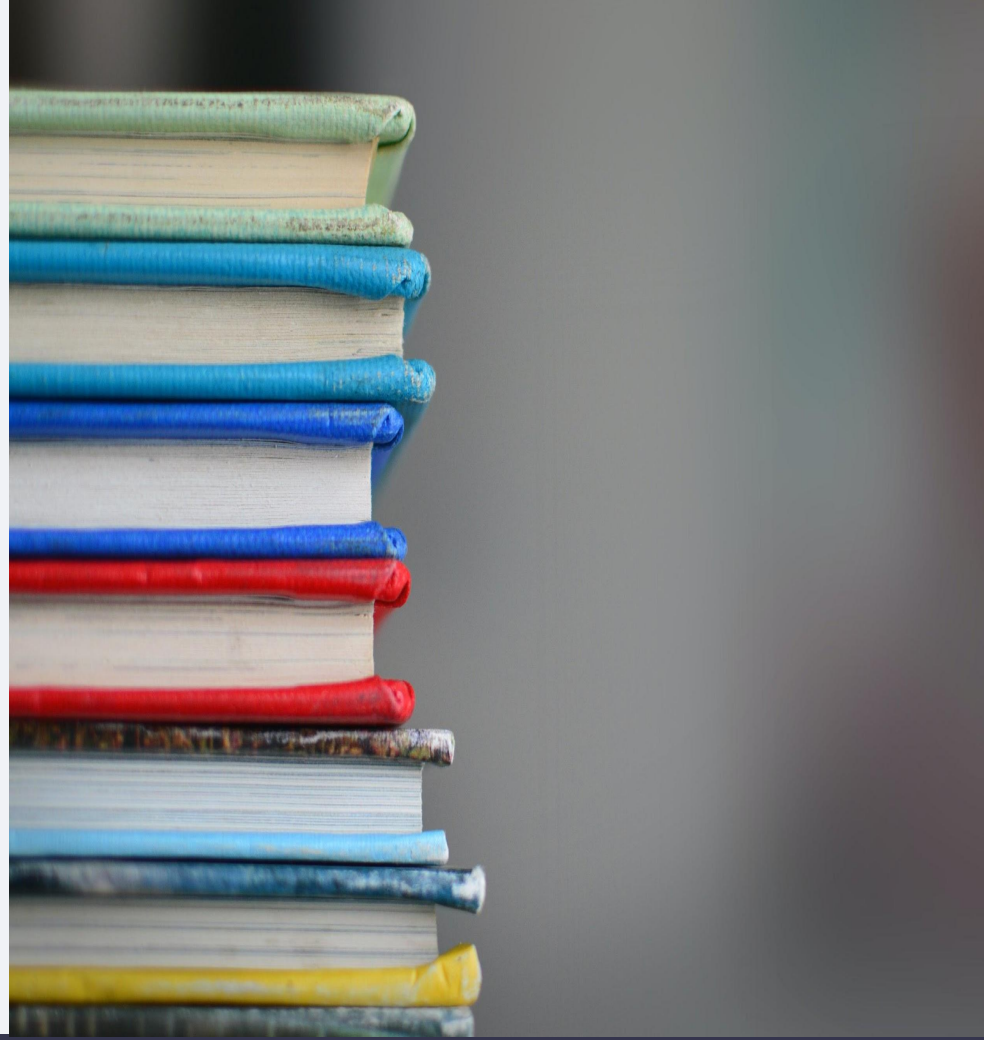
“Cybersecurity Protection & The Future of Work”

Neil Jones, Cybersecurity Evangelist, Egnyte

October 18, 2022

Importance of Cybersecurity Education

- Your company's livelihood- and potentially your job security-could depend on it.
  - Were you aware of Colonial Pipeline before last Spring?
- There are simple steps you can take to protect your company's data and your own data privacy.
- Today's session is interactive, with a series of poll questions based on a recent cybersecurity study.



Study Demographics: Job Titles

Total Survey Questions: 15

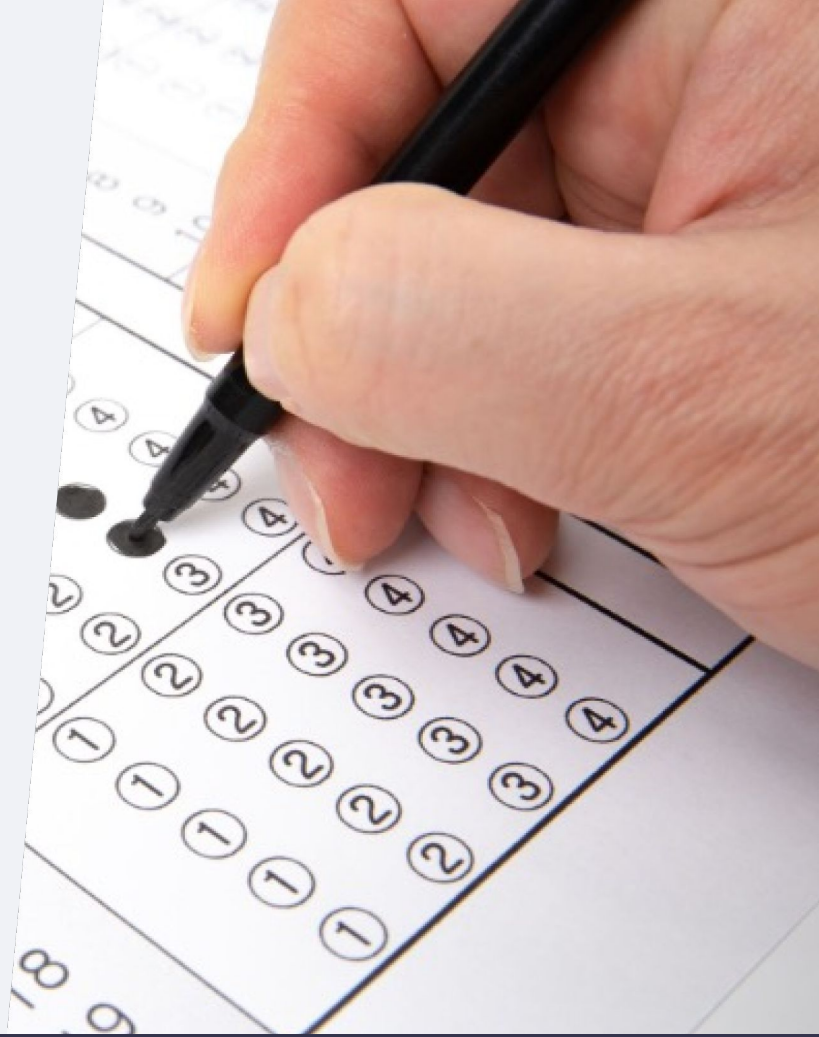
Total Survey Respondents: 400

Job Titles:

- CIO/CTO: 164
- Security: 47
- Data: 72
- Digital: 32
- Other Job Titles: 85

Company Tenure:

- Less than 10 years: 269 respondents
- 10 years or more: 131 respondents



Study Demographics: Company Specifics

Company Size:

- 100-499 Employees: 191 respondents
- 500-1,000 Employees: 209 respondents

Company Revenue:

- Less than $100 million: 230 respondents
- More than $100 million: 170 respondents

Company's Number of Years in Business:

- Fewer than 15 years: 184 respondents
- 15 years or more: 216 respondents

Poll Question #1: Can You Guess?

How many data repositories does the average mid-sized company manage?

Data repository examples include:

Egnyte, Microsoft Sharepoint & Google Drive.

EGNYTE

Survey Question:

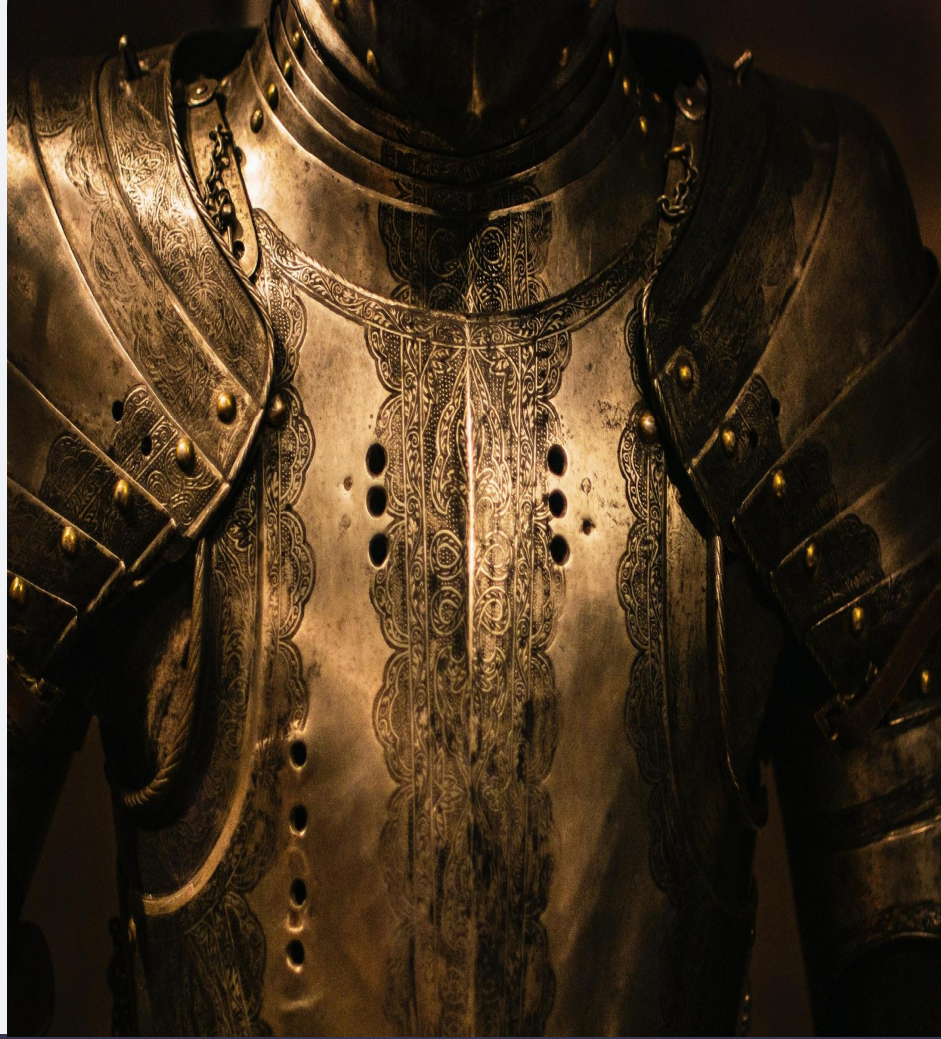
How many data repositories does your company currently manage?

Survey Options	Actual Survey Responses
5 or fewer repositories	6%
6 to 10 repositories	43%
11 to 15 repositories	43%
16 to 20 repositories	7%
More than 20 repositories	1%
QuickFacts	
10 OR FEWER (NET)	49%
MORE THAN 10 (NET)	51%

Findings from: Egnyte Survey
Wakefield Research | May 2022

What can you do to protect your company's data?

- Utilize officially sanctioned data stores at work.
- Listen to your users: "Shadow IT" normally happens when current solutions don't meet users' needs.
- Think long and hard before adopting a brand-new solution.
- Restrict sensitive information based on users' "Need to Know."



Poll Question #2: Can You Guess?

What percentage of companies allow a user to add another user to a sensitive data repository without the IT team's oversight?

Sensitive data repositories contain healthcare, financial, customer confidential information, etc.

EGNYTE

Survey Question:

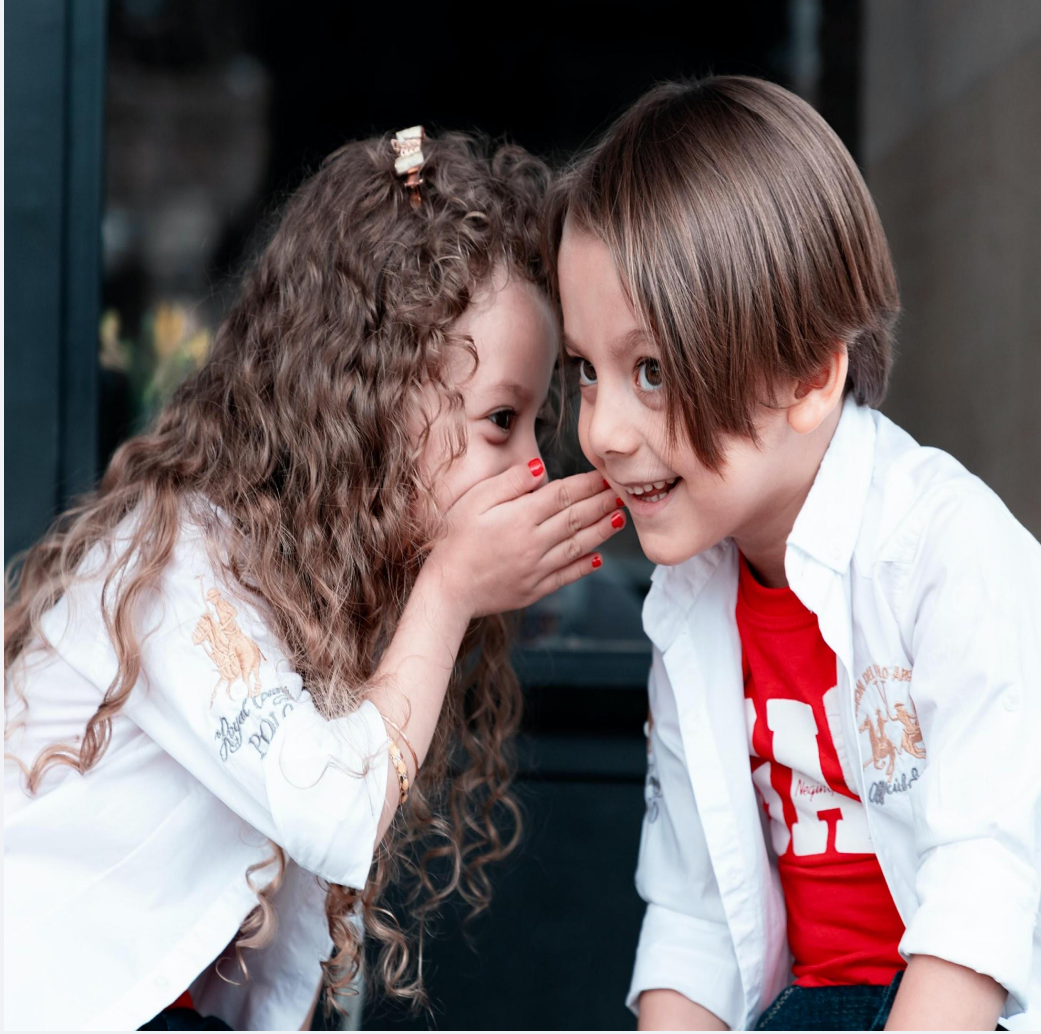
How does your company manage user access for repositories that contain sensitive data?

Response Options	Actual Survey Responses
IT administrator(s) must review user additions to repositories that contain sensitive data	69%
Users can add other users to repositories that contain sensitive data without IT oversight	31%
There is no defined process	0%

Findings from: Egnyte Survey
Wakefield Research | May 2022

How do you share data safely?

- Be mindful about the level of required access when you give someone else access.
- If the information is particularly confidential, consider placing an expiration date on file access.
- When it's a casual request- like they need a single financial figure for a presentation- collaborate on a Web conference.
- Never share confidential information via unencrypted e-mail



Poll Question #3: Can You Guess?

Guess what percentage of companies educate their users about the risk of phishing attacks.

NIST's Definition of Phishing:

"A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email…in which the perpetrator masquerades as a legitimate business or reputable person."

EGNYTE

Survey Question:

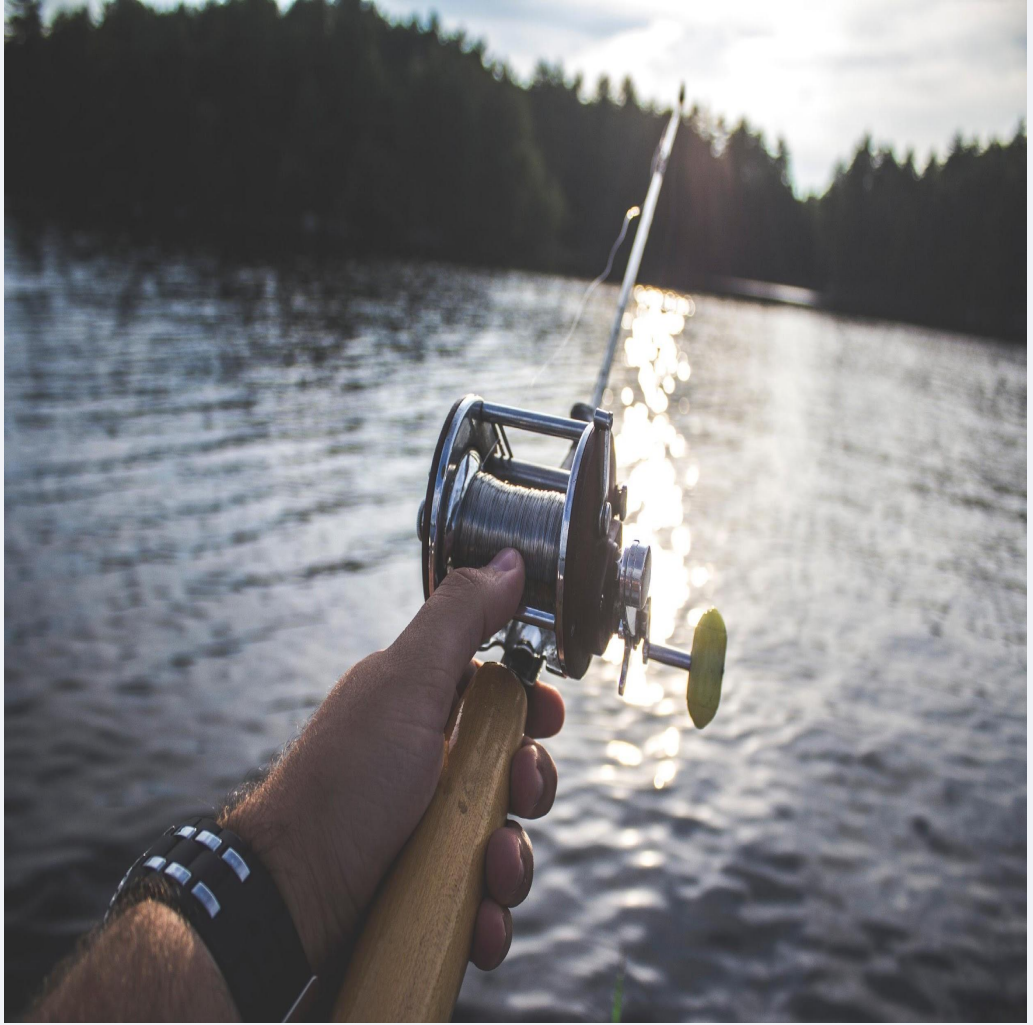
If at all, by which methods does your company engage in educating users about potential dangers of phishing attacks?

Survey Options	Actual Survey Responses
We send out security awareness newsletters / emails	65%
We offer security training or workshops	59%
We engage in white hat phishing programs	58%
Other	-
My company does not educate users about potential dangers of phishing attacks	0%
QuickFacts	
EDUCATES USERS ABOUT POTENTIAL DANGERS OF PHISHING ATTACKS (NET)	100%

Confidential Findings from: Egnyte Survey
Wakefield Research | May 2022

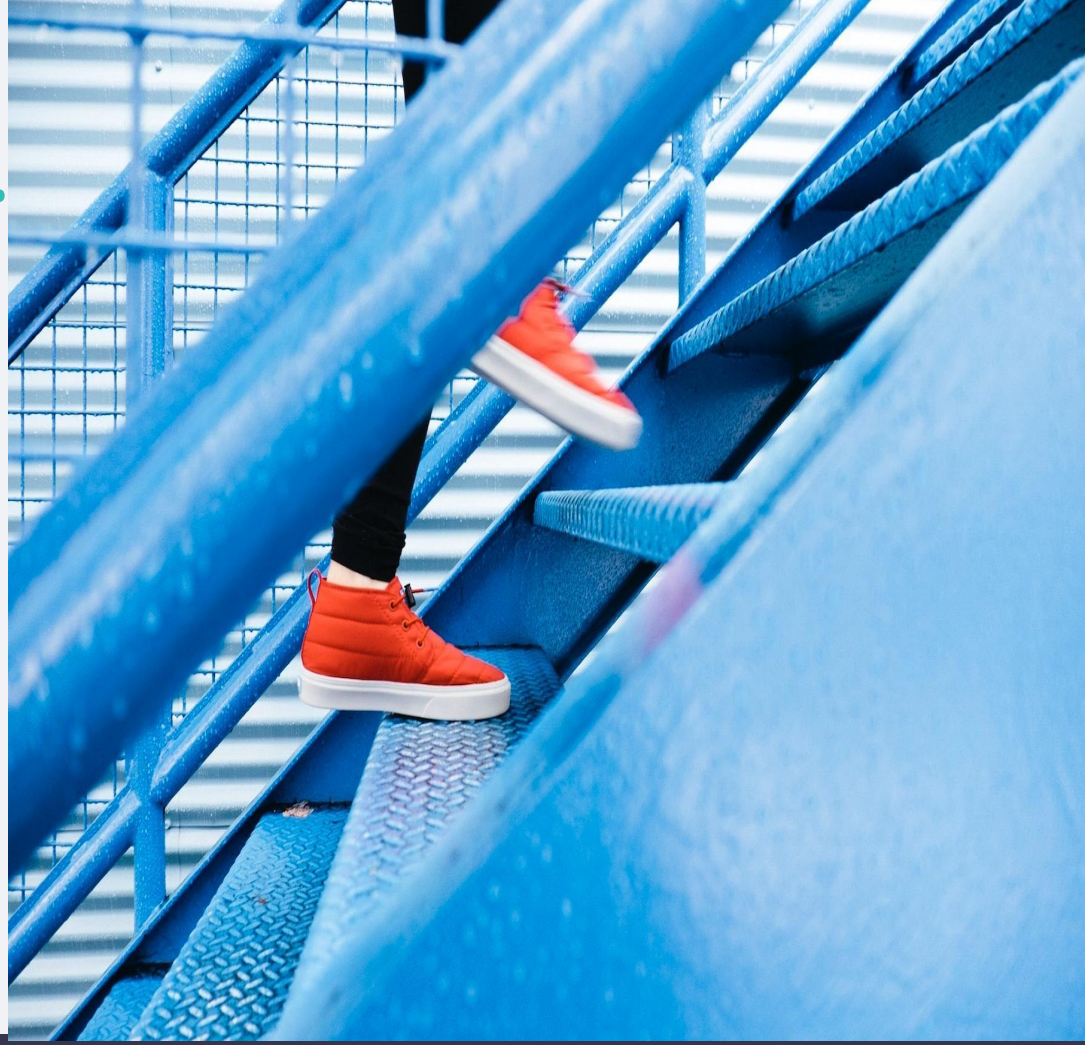
How can you discourage phishing attacks?

- If an e-mail appears unfamiliar to you, never click on links or attachments.
- If the unfamiliar e-mail is from a colleague, utilize a different means of communication to determine if it's legitimate.
- IT teams should reward users who report potential phishing messages.
- Everyone should understand the link between phishing and ransomware.



Take the First Step...

- Change your WiFi password today, especially if you Work from Home.
- Be careful about sharing your phone number or e-mail address in public locations.
- Educate less technologically-savvy family and friends.
- Understand the value of “If you see something, say something.”
- Remember that “IT Security is a team sport.”



Learn More

[Complete Study Findings Available Here]

Follow Me on Twitter:

@NKJ11

Thank You!

Back-Up Slides

EGNYTE

How many data repositories does the average mid-sized company manage:

a) 5 or fewer repositories
b) 6 to 10
c) 11 to 15
d) 15 to 20
e) 20 or more

EGNYTE

What percentage of companies allow a user to add another user to a sensitive data repository without the IT team's oversight:

A) 25%
B) 31%
C) 57%
D) 69%

EGNYTE

Guess what percentage of companies educate their users about the risk of phishing attacks:

A) 22%
B) 41%
C) 77%
D) 100%

EGNYTE