NEWSCYCLE

Cybersecurity Best Practices for Journalists

Peter Marsh, VP Marketing, Newscycle Solutions
@pgm

2016 ACES national conference, Portland, OR

TODAY'S SIMPLE AGENDA FOR A COMPLEX PROBLEM

- What is the problem?
- What you can do about it right now?
- Q&A

@Newscycle_News
@pgm

NEWSCYCLE

THE PROBLEM IS REAL, IT'S GLOBAL, AND IT'S URGENT

m.washingtonpost.com

Hacked by SEA

The Washington Post

view-source:m.washingtonpost.com

```
<html>
<script type="text/javascript">
alert("You've been hacked by the Syrian Electronic Army!");
alert("US govt is training the terrorists to kill more Syrians");
alert("Saudi Arabia and its allies are killing hundreds of Yemens people everyday!");
alert("The media is always lying");
</script>
Hacked by SEA
</html>
```

The Suburban

Home | Newspaper | Magazine | Sublog | Contest/Events | Contact Us

HackeD By Laakel En Person

-| You GoT HaCKeD By Laakel En Person |-

n Person :Operation Israel has been initiated to help the Gazans currently being annihilated by the sadistic forces of the IDF. It has also been initiated to destroy the Israeli network and preserve the Internet for

the Palestinians facing persecution by the Israeli government.

im Muslim . I don't forgive .I don't forget

embarcadero media

Greetings, This site has been hacked.

Embarcadero Media Group (Alamanac) has failed to remove content that has been harmful to the wellbeing and safety of others.

Failure to honor all requests to remove content will lead to the permanent shutdown of all Embarcadero Media Group Websites.

If you have a request and would like your content removed please inform Bill Johnson - bjohnson@embarcaderomediagroup.com

We do not forgive, we do not forget, we are legion.

ESTADÃO

Política

الاتحاد

www.alittihad.ae

BBC NEWS BUSINESS

28 August 2013 Last updated at 01:22 GMT

New York Times website down after suspected hacking

The New York Times

The newspaper continued to tweet news after going offline

The New York Times website has gone offline for the second time this month after what the company described as a "malicious external attack".

Related Stories

SyrianElectronicArmy
@Official_SEA16

Follow

We have successfully hacked Le Monde and we will never fail to deliver our message of peace and anti-terrorism. #SEA

Le Monde

JE NE SUIS PAS CHARLIE

Je suis la Palestine qui se fait voler ..
Je suis la Syrie qui se fait bombarder ..

www.independent.co.uk/?CMP=ILC-refresh

The page at www.independent.co.uk says:

You've been hacked by the Syrian Electronic Army(SEA)

OK

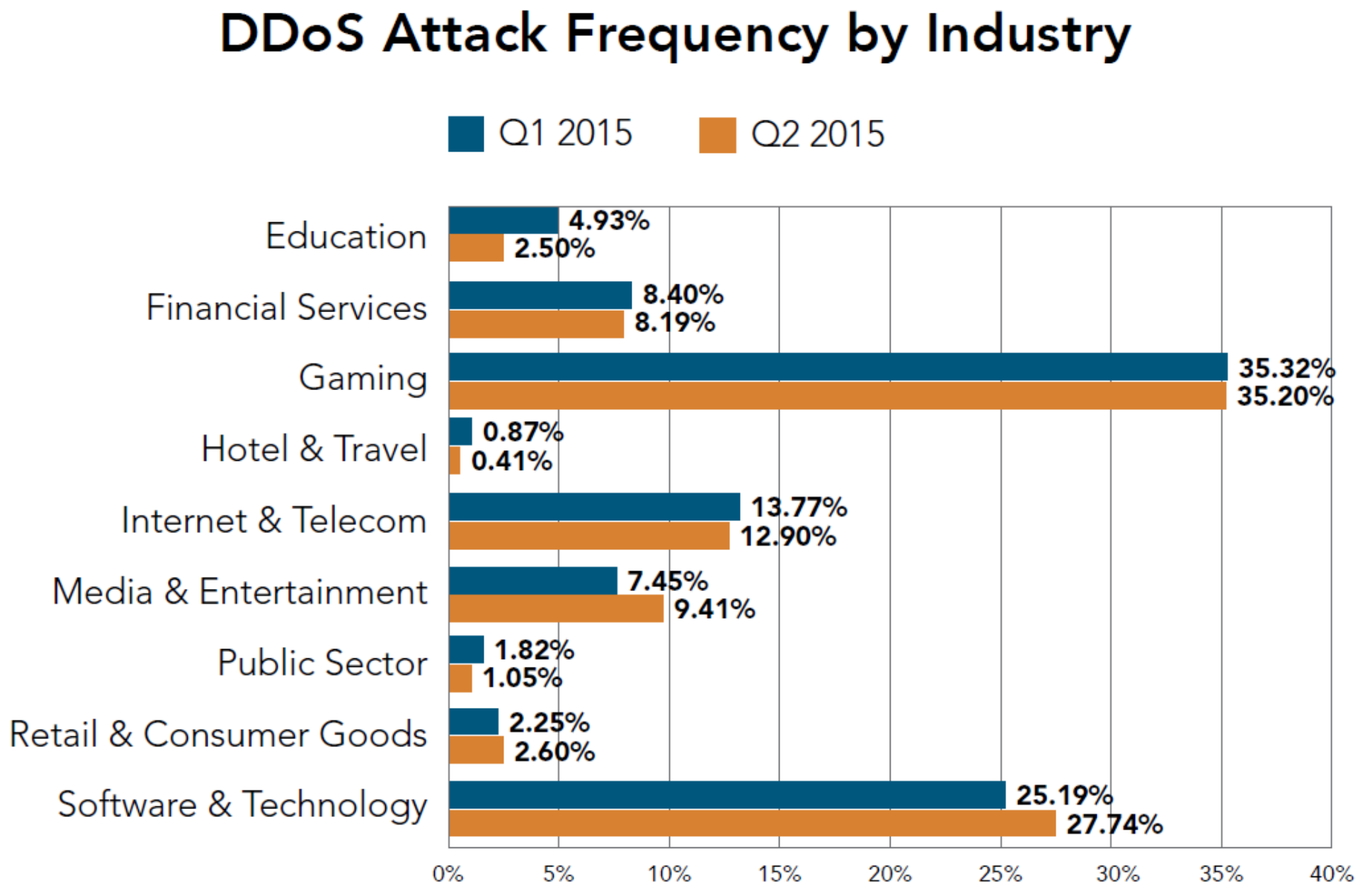
NEWSCYCLE

HOW BAD IS IT?

- A recent *Global IT Security Risks* survey conducted by international software research group Kaspersky Lab found that **42% of media companies around the world experienced some form of DDoS attack in the last 12 months**.
- The same study found that **only 38% of media companies surveyed are actively taking DDoS counter-measures**.

HOW BAD IS IT?

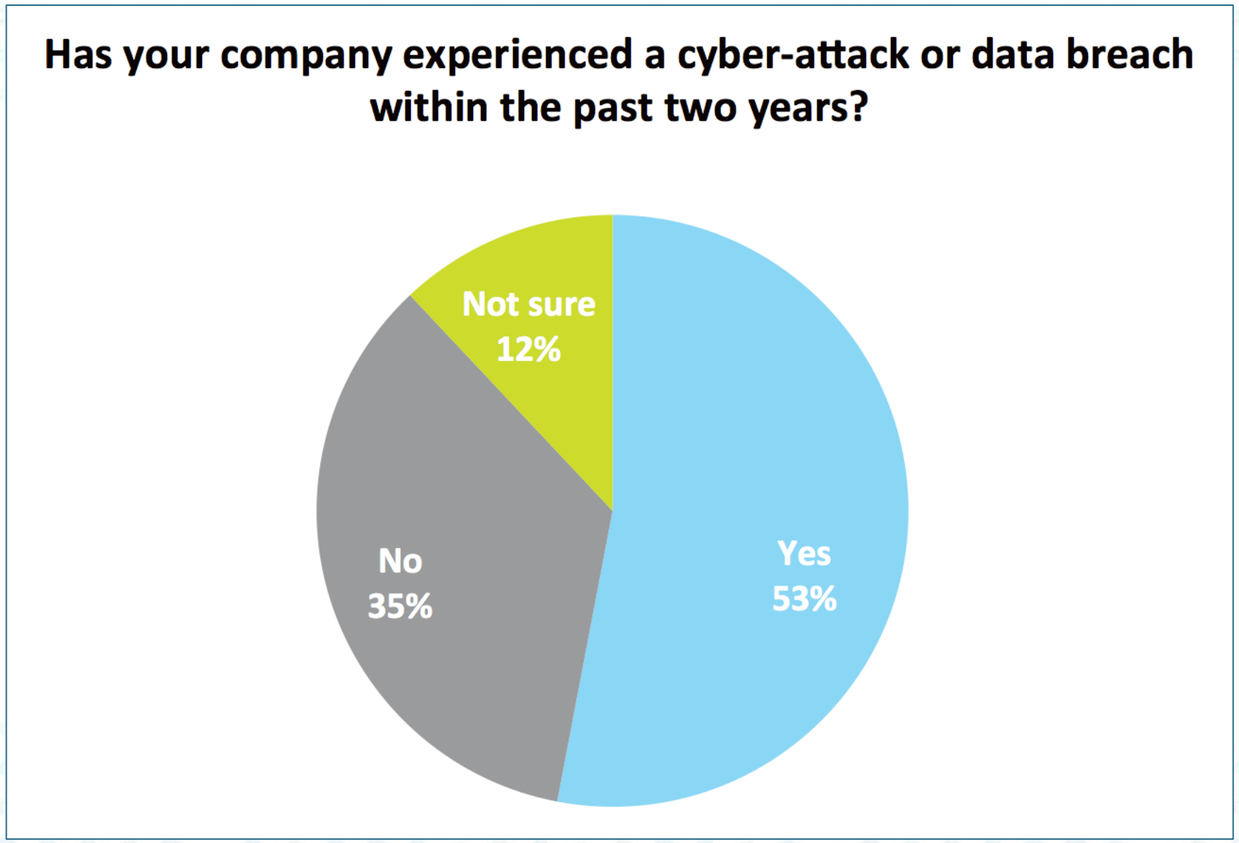
› According to an October 2015 **Akamai survey on internet security,** the media industry saw an increase in the percentage of DDoS attacks, from 7.45 percent in Q1 2015 to **9.41 percent in Q2 2015**.



NEWSCYCLE

PREVALENCE

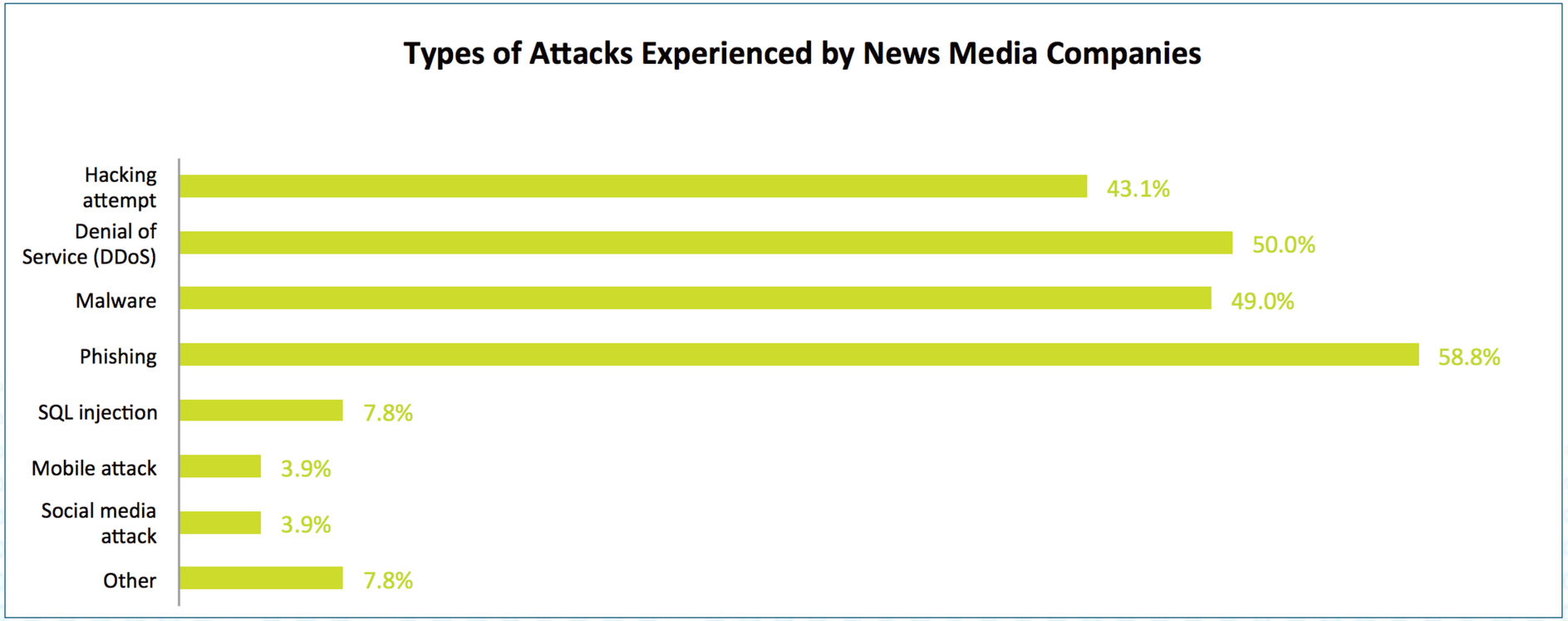
- 53 percent of news media companies were hacked or suffered a data breach since the beginning of 2014. Another 12 percent were not certain if their businesses had been attacked or compromised, while 35 percent reported no attacks.



NEWSCYCLE

ATTACK TYPES

- The most common type of cyberattack reported is phishing (59 percent), followed by Distributed Denial of Service attacks (50 percent), malware (49 percent), and hacking attempts (43 percent).



NEWSCYCLE

PwC REPORT ON SECURITY AND THE MEDIA INDUSTRY

Data is central to digital media industry business models

Digital media companies use data for:

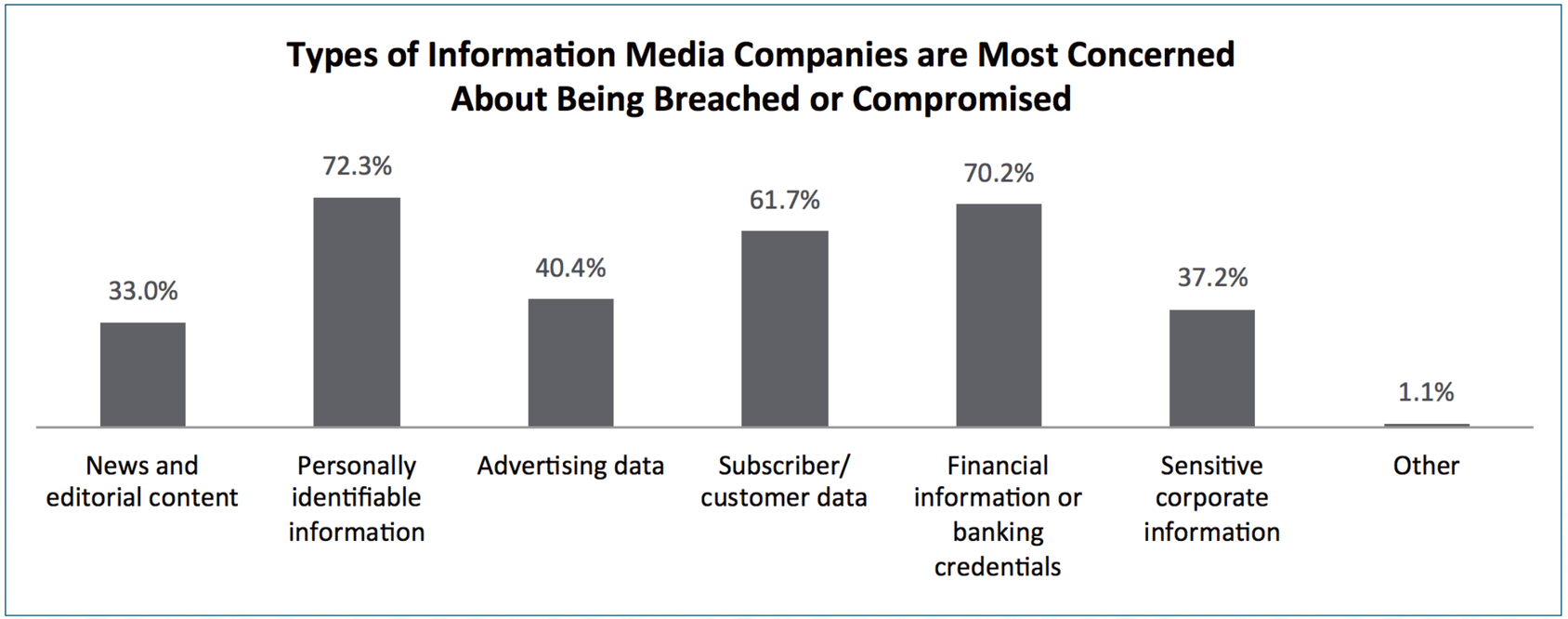
- Collecting user-generated content
- Communicating via social media
- Customer credit card information
- Conducting business operations

Source: ***PricewaterhouseCoopers***

NEWSCYCLE

INFORMATION AT RISK

- Over 72 percent said they are most concerned about personally identifiable information (PII) being breached or compromised. 70 percent are concerned about breaches in financial information or banking credentials. Hacking of subscriber and customer data is cited by 62 percent of respondents.



NEWSCYCLE

PwC REPORT ON SECURITY AND THE MEDIA INDUSTRY

Costs of a data breach

Data breaches can have major consequences for digital media companies

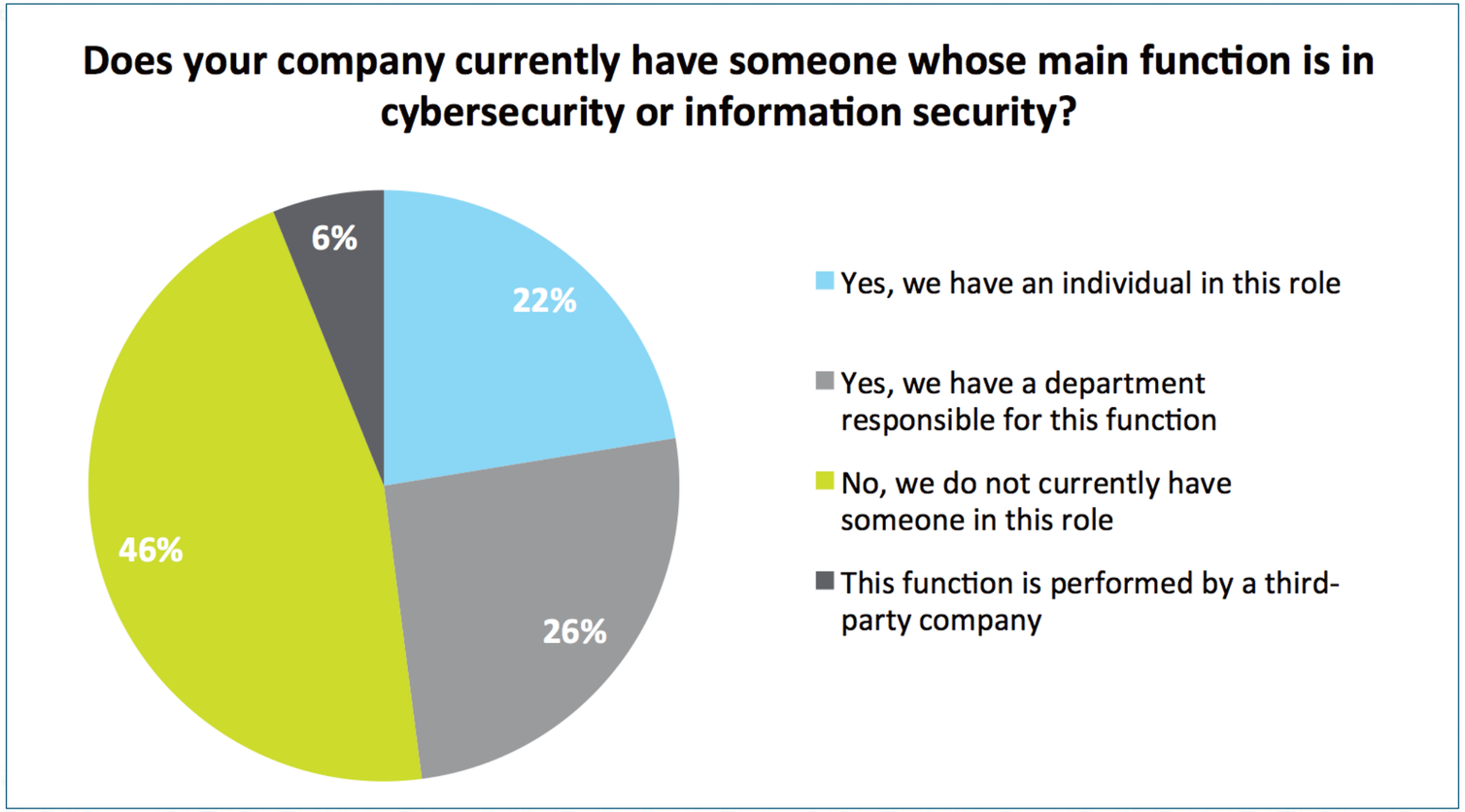
- Negative press reports
- Loss of business
- Penalties
- Class-action lawsuits

Source: ***PricewaterhouseCoopers***

NEWSCYCLE

FOCUS

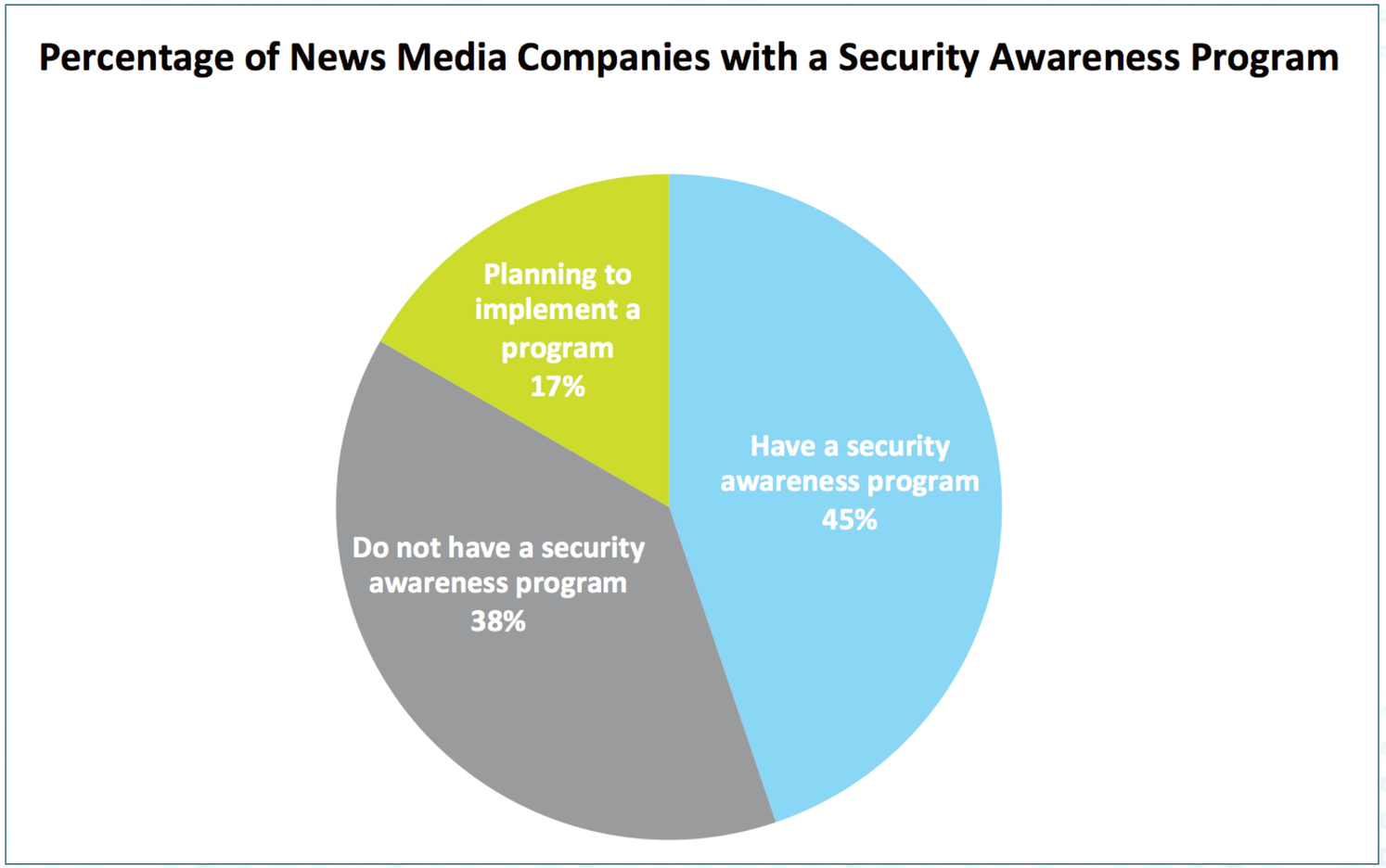
- Almost half of all Newscycle survey respondents indicate that their company does not currently employ someone whose main function is to oversee cybersecurity or information security.



NEWSCYCLE

AWARENESS

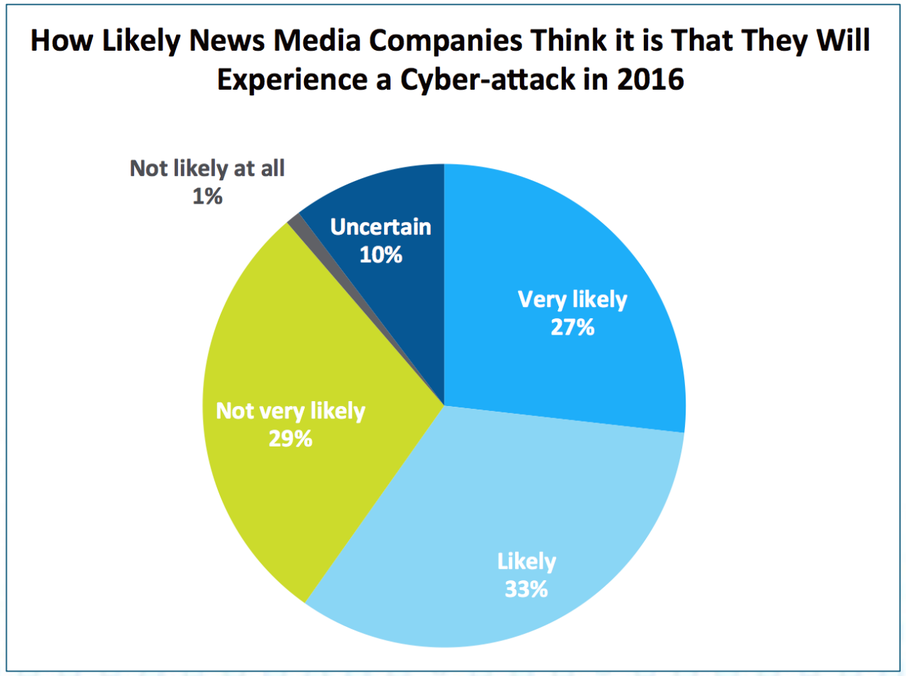
- 38 percent of media companies surveyed do not have a security awareness program in place today.



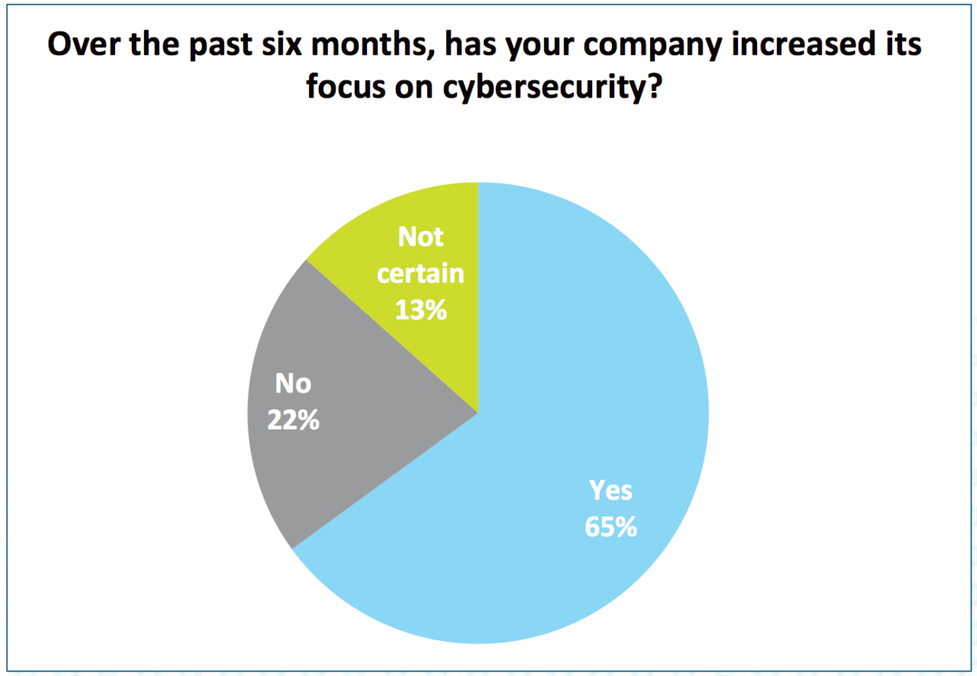
NEWSCYCLE

FORWARD LOOK

› **60 percent** of respondents predict that a cyberattack against their media company is likely or very likely to occur in 2016.



› In the face of the growing threat of cyberattack, **65 percent** have increased the focus on cybersecurity in the past six months.



NEWSCYCLE

Source: Kevin Roose, News Director, Fusion, Feb. 26, 2016

https://www.youtube.com/watch?v=bjYhmX_OUQQ

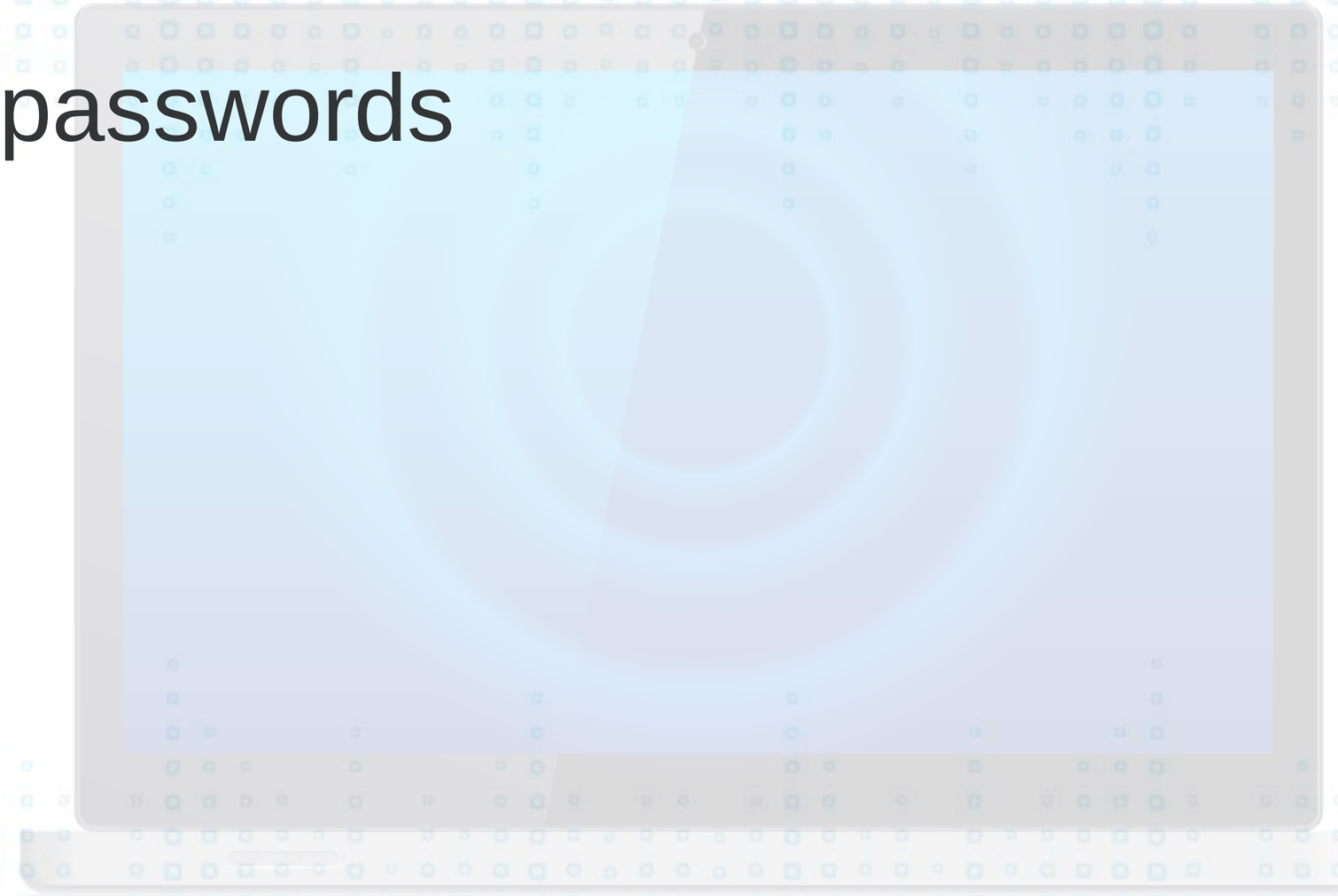
WHAT CAN YOU DO ABOUT IT?

› Here are **four quick wins** …

NEWSCYCLE

WHAT CAN YOU DO ABOUT IT?

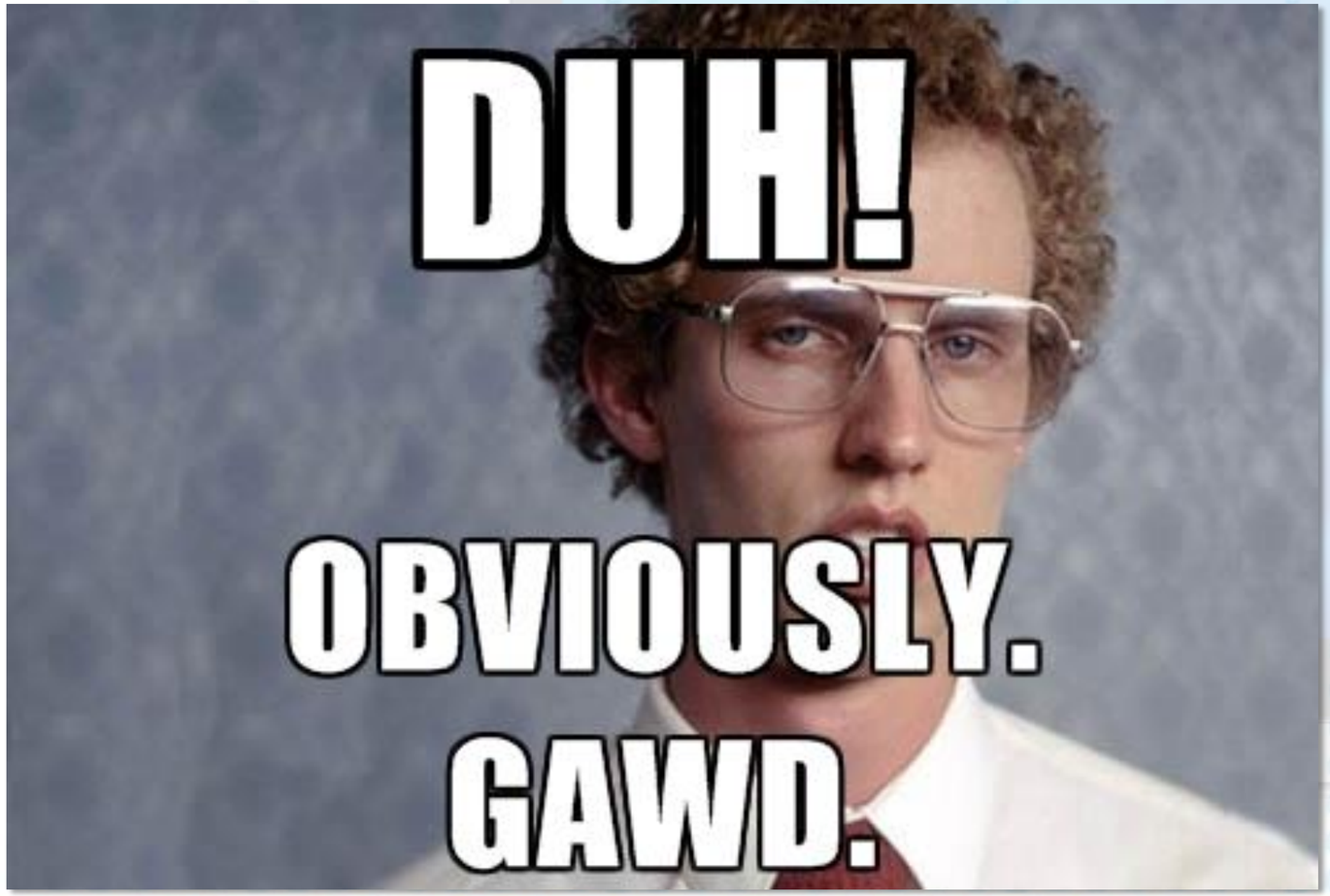
1. Strengthen your passwords



NEWSCYCLE

WHAT CAN YOU DO ABOUT IT?

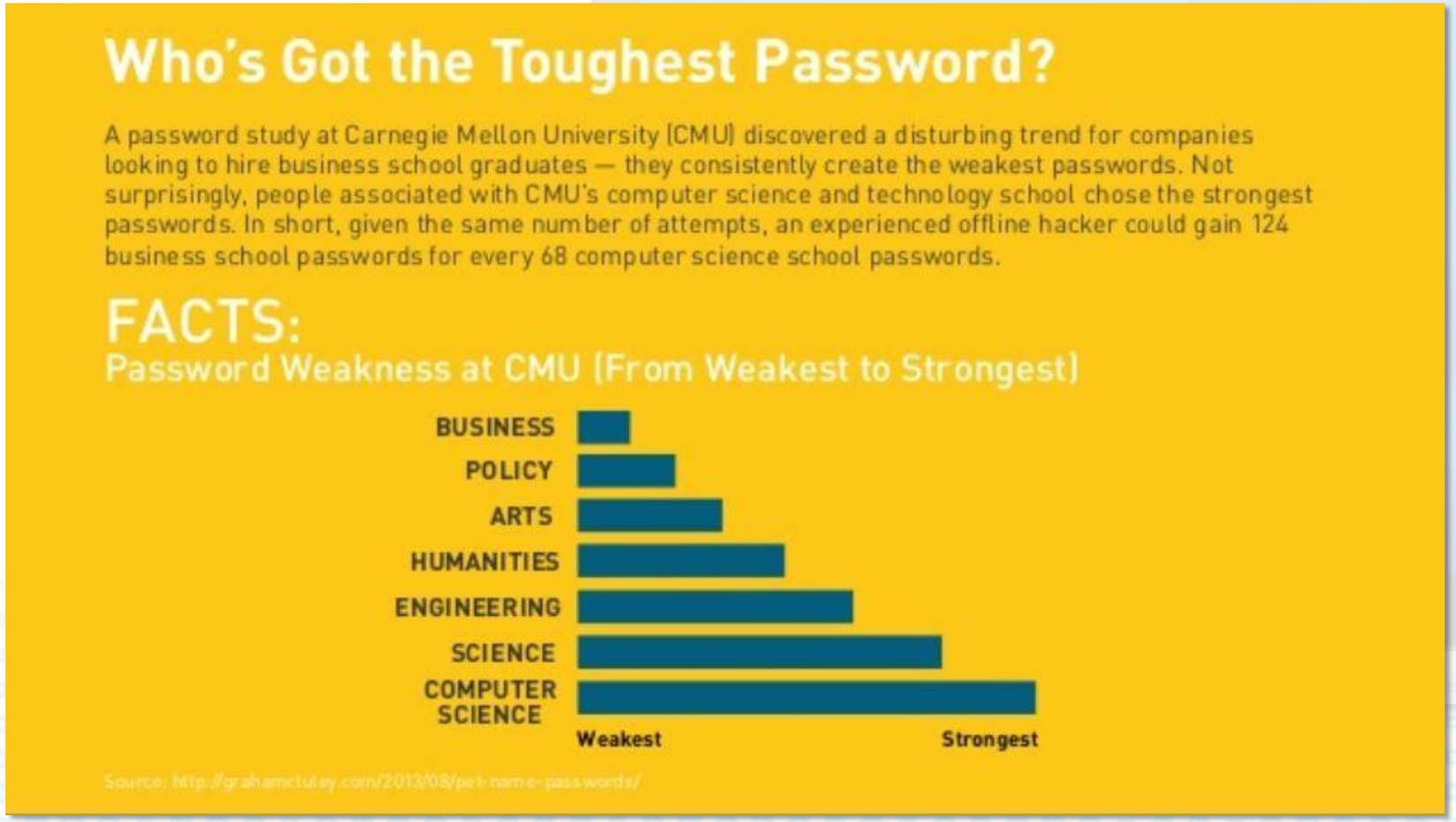
1. Strengthen your passwords



NEWSCYCLE

WHAT CAN YOU DO ABOUT IT?

1. Strengthen your passwords



NEWSCYCLE

WHAT CAN YOU DO ABOUT IT?

1. Strengthen your passwords

TOP 20 MOST COMMON PASSWORDS
(as a percentage of all passwords)

1.	123456	4.1%	11.	login	0.2%
2.	password	1.3%	12.	welcome	0.2%
3.	12345	0.8%	13.	loveme	0.2%
4.	1234	0.6%	14.	hottie	0.2%
5.	football	0.3%	15.	abc123	0.2%
6.	qwerty	0.3%	16.	121212	0.2%
7.	1234567890	0.3%	17.	123654789	0.2%
8.	1234567	0.3%	18.	flower	0.2%
9.	princess	0.3%	19.	passw0rd	0.2%
10.	solo	0.2%	20.	dragon	0.1%

Source: Skyhigh 2016 analysis of 11 million passwords for cloud services users

NEWSCYCLE

WHAT CAN YOU DO ABOUT IT?

1. Strengthen your passwords

Think outside these top-ten most popular password types:

1. Pet's name
2. A significant date (i.e. wedding anniversary)
3. Relative's birthday
4. Child's name
5. Family member's name
6. Birthplace
7. Favorite holiday
8. Favorite football team
9. Current partner's name
10. The word 'password'

NEWSCYCLE

WHAT CAN YOU DO ABOUT IT?

1. Strengthen your passwords

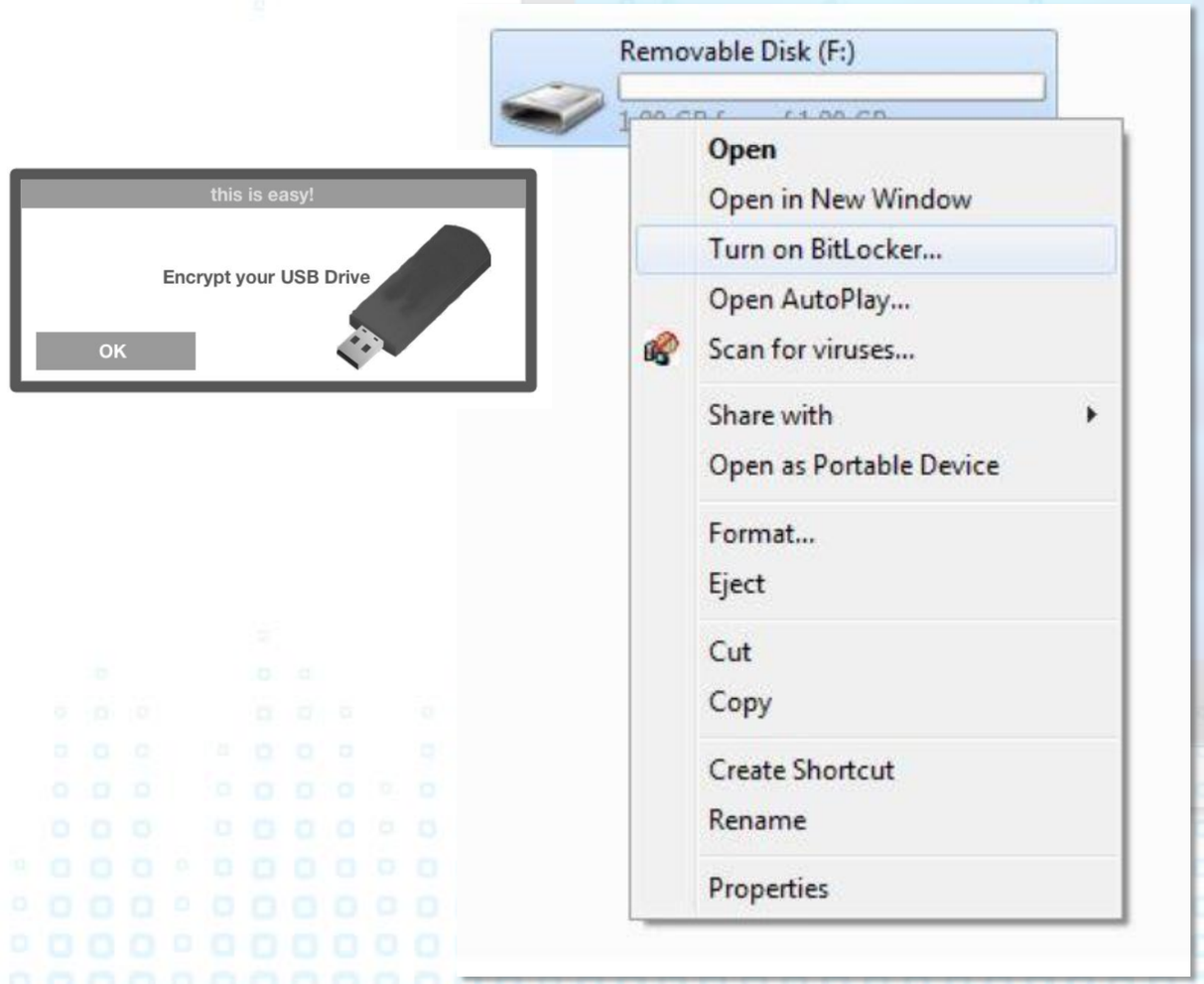
NEWSCYCLE

WHAT CAN YOU DO ABOUT IT?

2. Encrypt your USB drives

WHAT CAN YOU DO ABOUT IT?

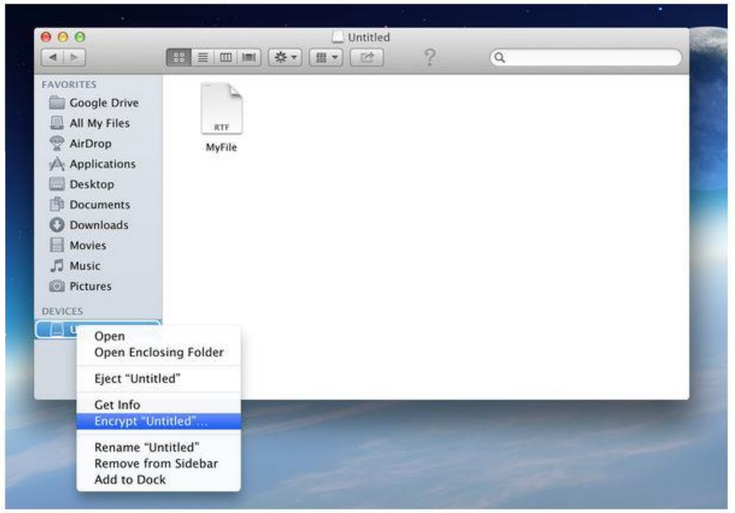
2. Encrypt your USB drives



NEWSCYCLE

WHAT CAN YOU DO ABOUT IT?

2. Encrypt your USB drives



From here select the *Encrypt* option.

NEWSCYCLE

WHAT CAN YOU DO ABOUT IT?

2. Encrypt your USB drives

CompTIA USB Drop Social Experiment – October 2015

17%

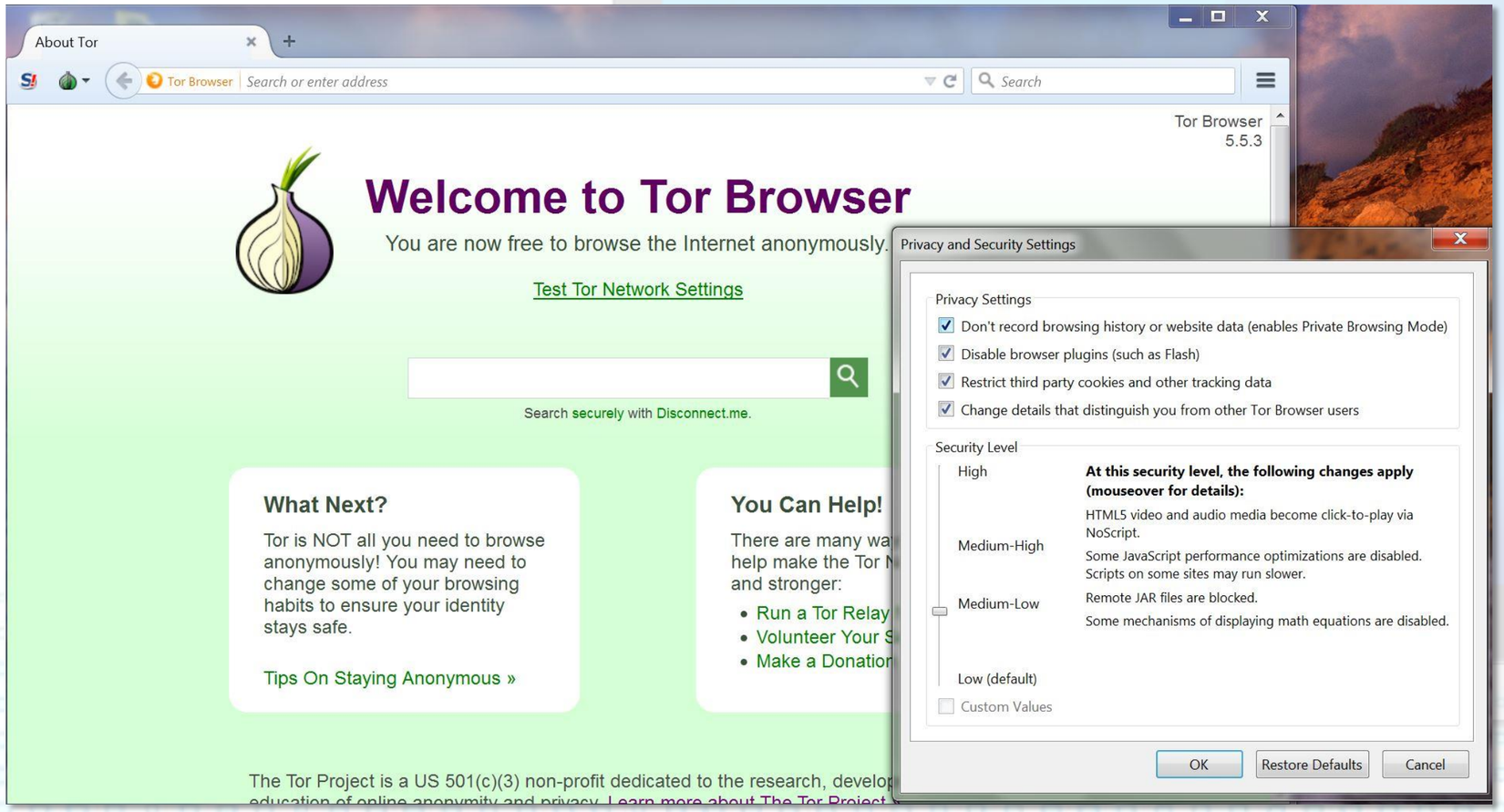
of employees plugged the found USB stick into their device

200 unbranded USB sticks were dropped across high traffic public spaces – such as airports, coffee shops and public squares in business districts – including Chicago, Cleveland, San Francisco and Washington D.C. The sticks were preprogrammed with text files prompting anyone who plugged the found USB sticks in to email a specific address or click through a trackable link.

NEWSCYCLE

WHAT CAN YOU DO ABOUT IT?

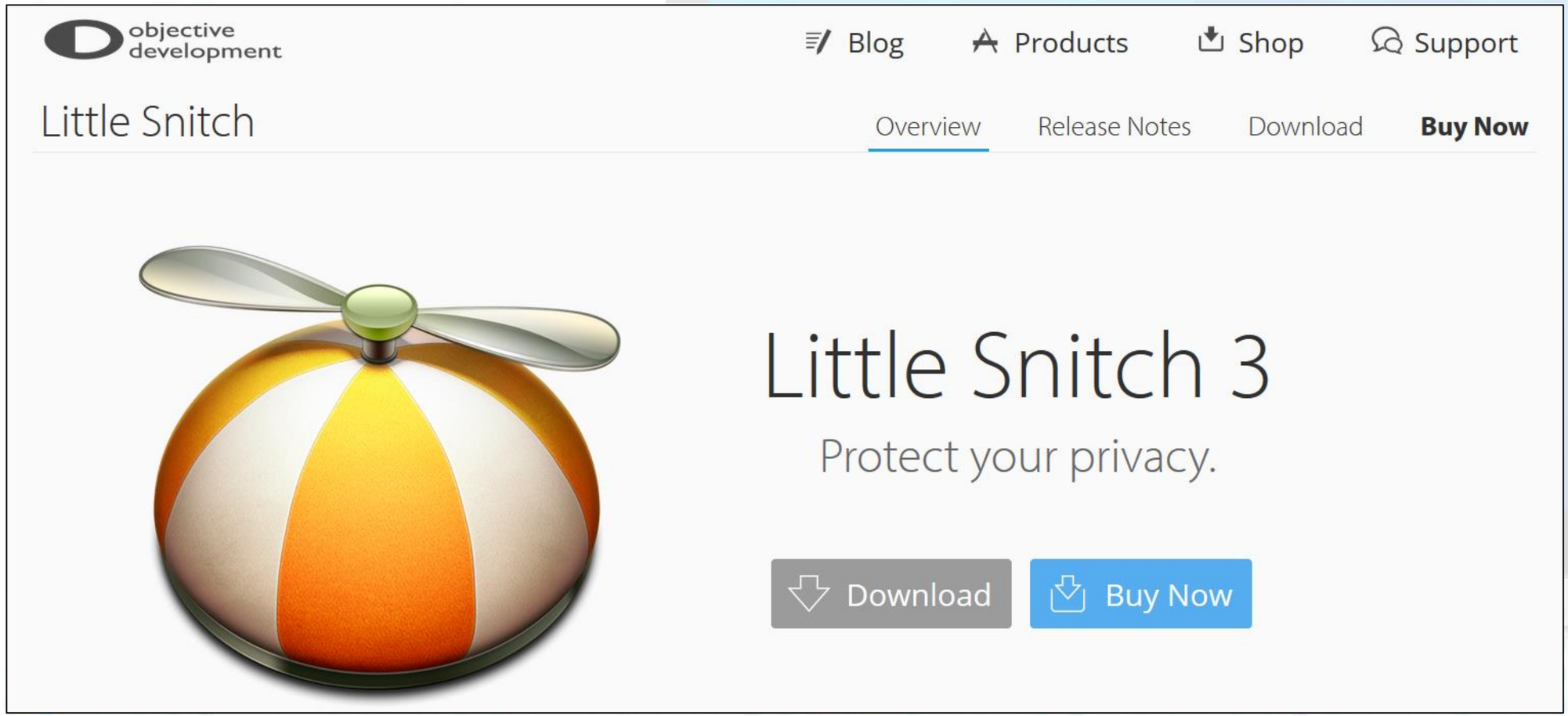
3. Consider a new web browser



NEWSCYCLE

WHAT CAN YOU DO ABOUT IT?

3. Or, get an app that monitors network activity



NEWSCYCLE

WHAT CAN YOU DO ABOUT IT?

4. Stay vigilant against **malware** and **phishing**

NEWSCYCLE

WHAT CAN YOU DO ABOUT IT?

4. Stay vigilant against **malware** and **phishing**

- Dangerous files include those with a **.exe** extension
- If you run Java, the **.jar** extension can be dangerous as it triggers the execution of Java programs
- Other extensions that should set off red flags are **.bat**, **.cmd**, **.com**, and **.sbr.** These programs can be used to steal information off your computer, use your computer as a way to infect others, or delete your data completely.

SUMMARY: FRONT END DEFENSES

1. Strengthen your passwords
2. Encrypt your USB drives
3. Consider a new web browser
4. Stay vigilant against malware and phishing

DON'T FORGET THESE BACK-END PROTECTIONS

› **CSC** quick win controls …

1. **Application whitelisting**
2. **Standard, secure system configurations**
3. **Patch systems and software promptly**
4. **Reduce number of users with administrative privilege**

COUNCIL ON CYBERSECURITY
LE CONSEIL DE LA CYBERSÉCURITÉ

NEWSCYCLE

Q & A

Thank you.

For additional information, please contact us:
Email: info@newscycle.com
Web: www.newscycle.com

Peter G. Marsh
+1 978.590.7400
peter.marsh@newscycle.com
@pgm

NEWSCYCLE