Cybersecurity Best Practices for Journalists

Peter Marsh, VP Marketing, Newscycle Solutions
@pgm

2016 ACES national conference, Portland, OR
What is the problem?

What you can do about it right now?

Q&A

@Newscycle_News
@pgm
THE PROBLEM IS REAL, IT’S GLOBAL, AND IT’S URGENT
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.
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.
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).
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
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.
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
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.
38 percent of media companies surveyed do not have a security awareness program in place today.

**Percentage of News Media Companies with a Security Awareness Program**

- Do not have a security awareness program: 45%
- Have a security awareness program: 38%
- Planning to implement a program: 17%

© 2016 Newscycle Solutions
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.

How Likely News Media Companies Think it is That They Will Experience a Cyber-attack in 2016

- Very likely: 27%
- Likely: 33%
- Not very likely: 29%
- Uncertain: 10%
- Not likely at all: 1%

Over the past six months, has your company increased its focus on cybersecurity?

- Yes: 65%
- Not certain: 13%
- No: 22%
https://www.youtube.com/watch?v=bjYhmX_OUQQ
WHAT CAN YOU DO ABOUT IT?

› Here are four quick wins ...
WHAT CAN YOU DO ABOUT IT?

1. Strengthen your passwords
WHAT CAN YOU DO ABOUT IT?

1. Strengthen your passwords

DUH!

OBVIOUSLY.

GAWD.
1. Strengthen your passwords

Who’s Got the Toughest Password?

A password study at Carnegie Mellon University (CMU) discovered a disturbing trend for companies looking to hire business school graduates — they consistently create the weakest passwords. Not surprisingly, people associated with CMU’s computer science and technology school chose the strongest passwords. In short, given the same number of attempts, an experienced offline hacker could gain 124 business school passwords for every 68 computer science school passwords.

FACTS:
Password Weakness at CMU (From Weakest to Strongest)

Source: http://grahamclayton.com/2013/08/get-name-pass-words/
WHAT CAN YOU DO ABOUT IT?

1. Strengthen your passwords

<table>
<thead>
<tr>
<th></th>
<th>Password</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>123456</td>
<td>4.1%</td>
</tr>
<tr>
<td>2</td>
<td>password</td>
<td>1.3%</td>
</tr>
<tr>
<td>3</td>
<td>12345</td>
<td>0.8%</td>
</tr>
<tr>
<td>4</td>
<td>1234</td>
<td>0.6%</td>
</tr>
<tr>
<td>5</td>
<td>football</td>
<td>0.3%</td>
</tr>
<tr>
<td>6</td>
<td>qwerty</td>
<td>0.3%</td>
</tr>
<tr>
<td>7</td>
<td>1234567890</td>
<td>0.3%</td>
</tr>
<tr>
<td>8</td>
<td>1234567</td>
<td>0.3%</td>
</tr>
<tr>
<td>9</td>
<td>princess</td>
<td>0.3%</td>
</tr>
<tr>
<td>10</td>
<td>solo</td>
<td>0.2%</td>
</tr>
<tr>
<td>11</td>
<td>login</td>
<td>0.2%</td>
</tr>
<tr>
<td>12</td>
<td>welcome</td>
<td>0.2%</td>
</tr>
<tr>
<td>13</td>
<td>loveme</td>
<td>0.2%</td>
</tr>
<tr>
<td>14</td>
<td>hottie</td>
<td>0.2%</td>
</tr>
<tr>
<td>15</td>
<td>abc123</td>
<td>0.2%</td>
</tr>
<tr>
<td>16</td>
<td>121212</td>
<td>0.2%</td>
</tr>
<tr>
<td>17</td>
<td>123654789</td>
<td>0.2%</td>
</tr>
<tr>
<td>18</td>
<td>flower</td>
<td>0.2%</td>
</tr>
<tr>
<td>19</td>
<td>passwd</td>
<td>0.2%</td>
</tr>
<tr>
<td>20</td>
<td>dragon</td>
<td>0.1%</td>
</tr>
</tbody>
</table>

Source: Skyhigh 2016 analysis of 11 million passwords for cloud services users
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’
WHAT CAN YOU DO ABOUT IT?

1. Strengthen your passwords

1Forrest1
WHAT CAN YOU DO ABOUT IT?

2. Encrypt your USB drives
WHAT CAN YOU DO ABOUT IT?

2. Encrypt your USB drives
WHAT CAN YOU DO ABOUT IT?

2. Encrypt your USB drives
WHAT CAN YOU DO ABOUT IT?

2. Encrypt your USB drives

CompTIA USB Drop Social Experiment – October 2015

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.
3. Consider a new web browser
WHAT CAN YOU DO ABOUT IT?

3. Or, get an app that monitors network activity

Little Snitch 3
Protect your privacy.
WHAT CAN YOU DO ABOUT IT?

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