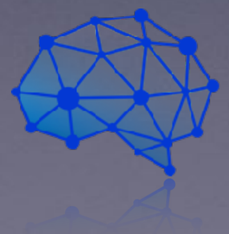
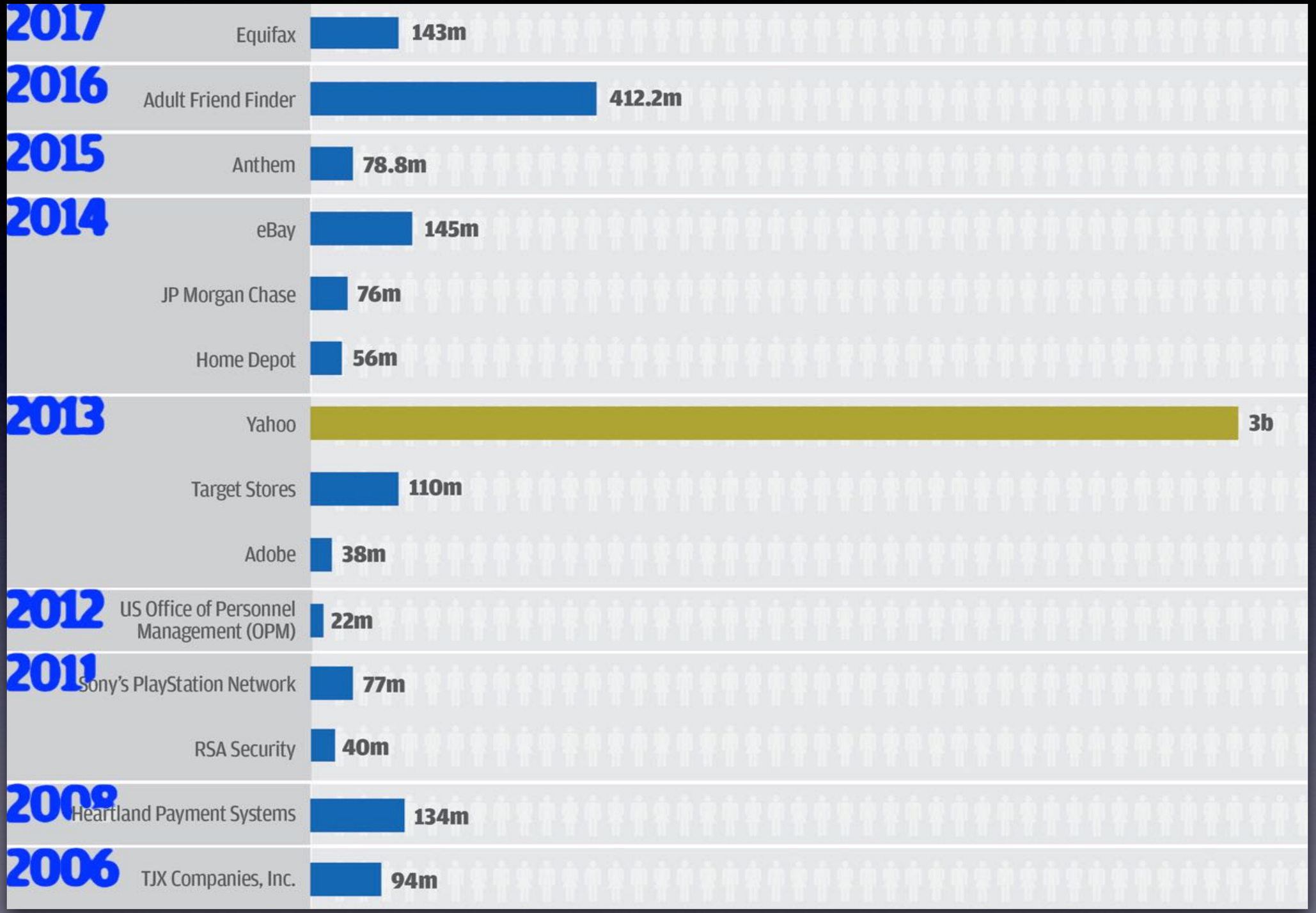
Cyber Hygiene

Hardware, software, wetware



AppliedSense


2017
Equifax
143m
2016
Adult Friend Finder
412.2m
2015
Anthem
78.8m
2014
eBay
145m
JP Morgan Chase
76m
Home Depot
56m
2013
Yahoo
3b
Target Stores
110m
Adobe
38m
2012
US Office of Personnel Management (OPM)
22m
2011
Sony's PlayStation Network
77m
RSA Security
40m
2008
Heartland Payment Systems
134m
2006
TJX Companies, Inc.
94m

Stats to know for 2017

- In Q3 2016 alone, 18 million new malware samples were captured. (*source: Panda Labs*)
- More than 4,000 ransomware attacks have occurred every day since the beginning of 2016.
  - That's a 300% increase over 2015, where 1,000 ransomware attacks were seen per day. (*source: Computer Crime and Intellectual Property Section (CCIPS)*
- The amount of phishing emails containing a form of ransomware grew to 97.25% during Q3 2016, up from 92% in Q1 2016 (s*ource: PhishMe 2016 Q3 Malware Review*)

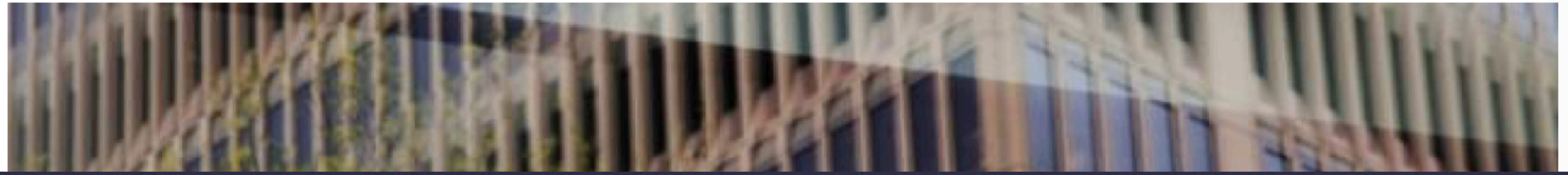
Cyber attack could spark lawsuits but not against Microsoft | Reuters

REUTERS

TOP NEWS

Mon May 15, 2017 | 7:50 PM EDT

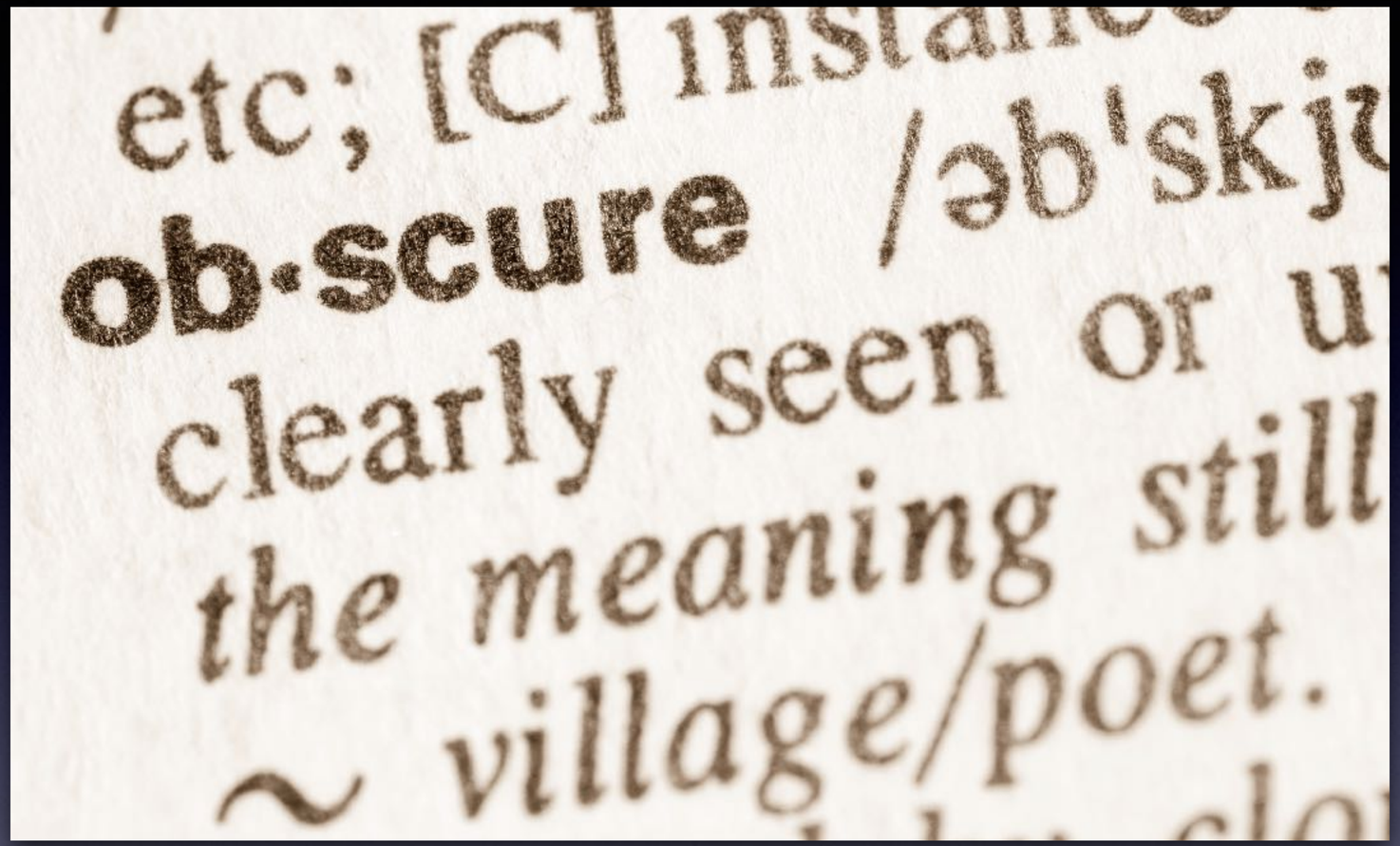
Cyber attack could spark lawsuits but not against Microsoft



"Using outdated versions of Windows that are no longer supported raises a lot of questions," said Christopher Dore, a lawyer specializing in digital privacy law at Edelson PC. "It would arguably be knowingly negligent to let those systems stay in place."

Businesses could face legal claims if they failed to deliver services because of the attack, said Edward McAndrew, a data privacy lawyer at Ballard Spahr. "There is this stream of liability that flows from the ransomware attack," he said. "That's liability to individuals, consumers and patients."

Businesses could face legal claims if they **failed to deliver services** because of the attack, said Edward McAndrew, a data privacy lawyer at Ballard Spahr. “There is this stream of liability that flows from the ransomware attack,” he said. “That’s liability to individuals, consumers and patients.”



Security through obscurity is no security at all!

https://technet.microsoft.com/en-us/library/2008.06.obscurity.aspx

July 29, 2017

https://www.usatoday.com/story/tech/news/2017/09/07/what-do-if-youre-one-44-americans-hit-equifax-breach/644406001/

More stats (sorry)

- 43% of cyber attacks target small business.
- 48% of data security breaches are caused by acts of malicious intent. Human error or system failure account for the rest
- 60% of small companies go out of business within six months of a cyber attack.

https://smallbiztrends.com/2017/01/cyber-security-statistics-small-business.html

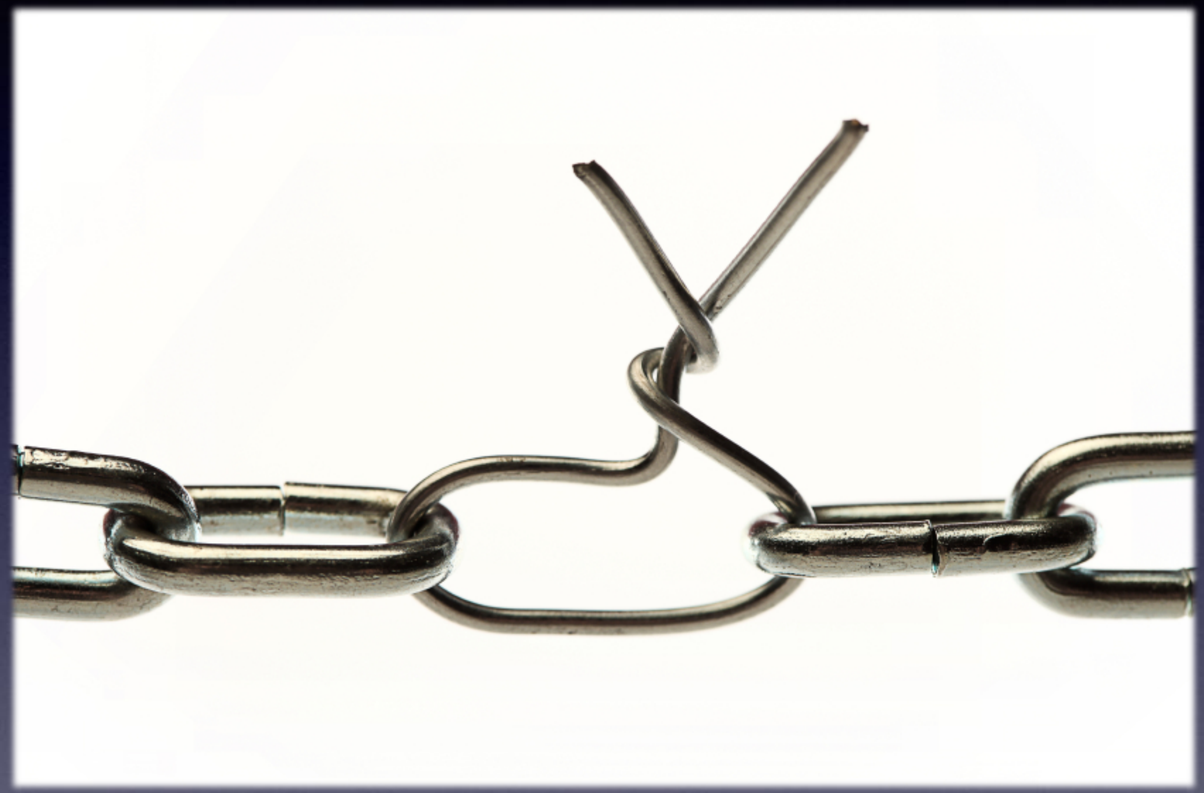
"Cybersecurity is clearly a concern that the entire business community shares, but it represents an especially pernicious threat to smaller businesses. The reason is simple: **Small and midsize businesses are not just targets of cybercrime; they are its principal target."**

- Securities and Exchange Commission (2015)

https://www.cnbc.com/2017/04/05/congress-addresses-cyberwar-on-small-business-14-million-hacked.html

Why?

Where’s the weak link?



Why?

Where’s the weak link?

Why?

Where’s the weak link?

Guess who?

Guess who (cont’d)?

What can ***your*** business do?

Cyber Hygiene 101

- “Harden” the hardware & software
- Implement Secure Communication Methods (email and VPN)
- Mandate a password strategy (mobile, too)
- Have (and use) a secure backup plan
- Be extremely mindful of internal threats
- Have a 24/7 point person
- Education of employees

What can ***you*** do?

Cyber Hygiene 201

1. A new kind of password
2. Verify: firewall, anti-malware (no freeware)
3. Run your own full security scan
4. No personal, unencrypted files in your cloud storage
5. Two browser policy
6. Install updates
7. Encrypt your sensitive files
8. VPNs
9. Look for HTTPS
10. No credit cards stored in the browser
11. Have “fixer” on speed dial
12. Never trust emails
13. Ignore pops-ups ALWAYS


500M likes

1. A new kind of password
2. Verify: firewall, anti-malware (no freeware)
3. Run your own full security scan
4. No personal, unencrypted files in your cloud storage
5. Two browser policy
6. Install updates
7. Encrypt your sensitive files
8. VPNs
9. Look for HTTPS
10. No credit cards stored in the browser
11. Have fixer on file
12. Never trust emails
13. Ignore pops-ups ALWAYS
14. Webcams
15. Two-Step Verification
16. USB ports =/= travel

Thank you!

More info…?

AppliedSenseOnline.com/talk

AppliedSenseOnline.com/quiz