



Trends in Breach Incident Management

Greg Murray

Vice President, Information Security & CISO

Rogers Communications

How You Might Know Us

Brands we Protect



YOUR BRAND

Something You May Not Know About Us...

Brands we Protect



CYBERWAR TV Series

Ben Makuch travels the world to discuss Cyberwarfare with hackers & dissidents



If this is your reality, then this may be interesting to you...

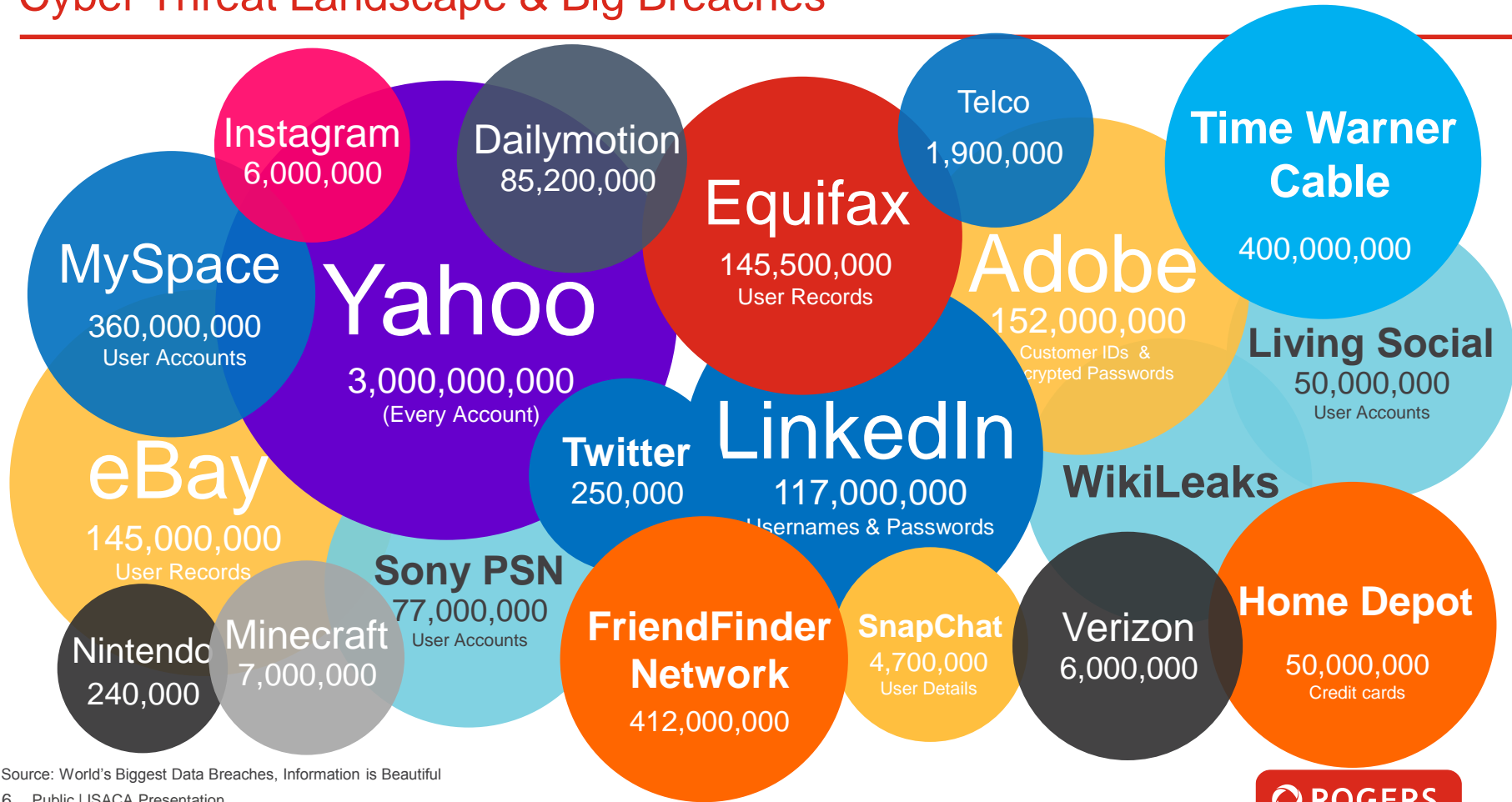
Let's Unpack This... So Who are the Adversaries Targeting?

My Mom



It's not You...**It's your Customers!** Turns out it's just faster to steal from you!

Cyber Threat Landscape & Big Breaches



Source: World's Biggest Data Breaches, Information is Beautiful

Cybercrime Impacting Canadians & Our Organizations



Source: 1. Government of Canada 2. PwC Canada's 2016 Global State of Information Security Survey. 3. Phishing SCAMS - CBC news

Pop Quiz: Your Organization has Sustained a Cyber Breach

Please check all appropriate breach responses per your existing playbook:

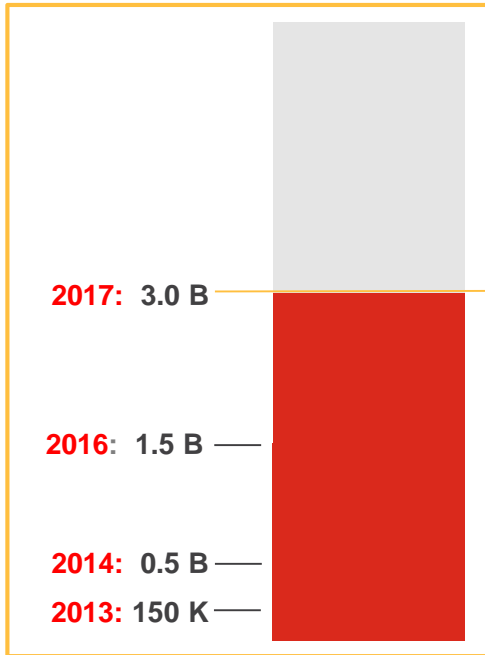
- A. Accept
- B. Mitigate
- C. Remediate
- D. Transfer (Insurance)
- E. Ignore*
- F. Respond extremely poorly / hide / retire (immediately)*

* Please note: Not an ISACA best practice

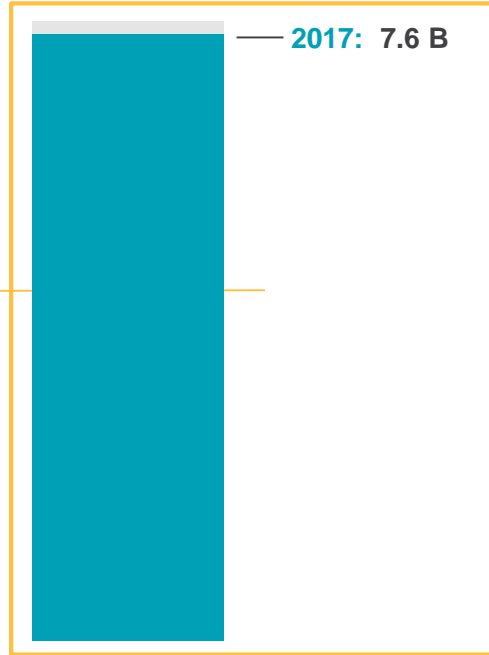
So what happens to those who pick options E and/or F?

Yahoo! A Lesson in Numbers – Let's start with 350...

Yahoo! Breaches



World Population








What Did We Learn?

- Numbers matter
- Transparency
- Customer 1st
- Upper limit reached






The Learn-as-you-Go Model doesn't Work

Equifax – a Lesson in Cyber Breach Preparedness

What Happened

-  **Board Oversight & Tone from the Top**
-  **Cyber Breach Playbook**
-  **Communications**
-  **Hygiene**
-  **Potential Insider Trading**

What We Learned

-  **Preparedness**
Proper threat briefings, business reviews & culture are essential
-  **Planning**
Only works if you train & follow the playbook during an incident
-  **Pre-positioned**
Prepare for impact to business: 'www.equifaxsecurity2017.com -?'
-  **Process & Technical stuff matters**
Proper patching, TVM and so forth can and do make a difference
-  **Business Transparency**
(Communications to Customers, Shareholders, Suppliers & Communities you serve)

The Learn-as-you-Go Model doesn't Work

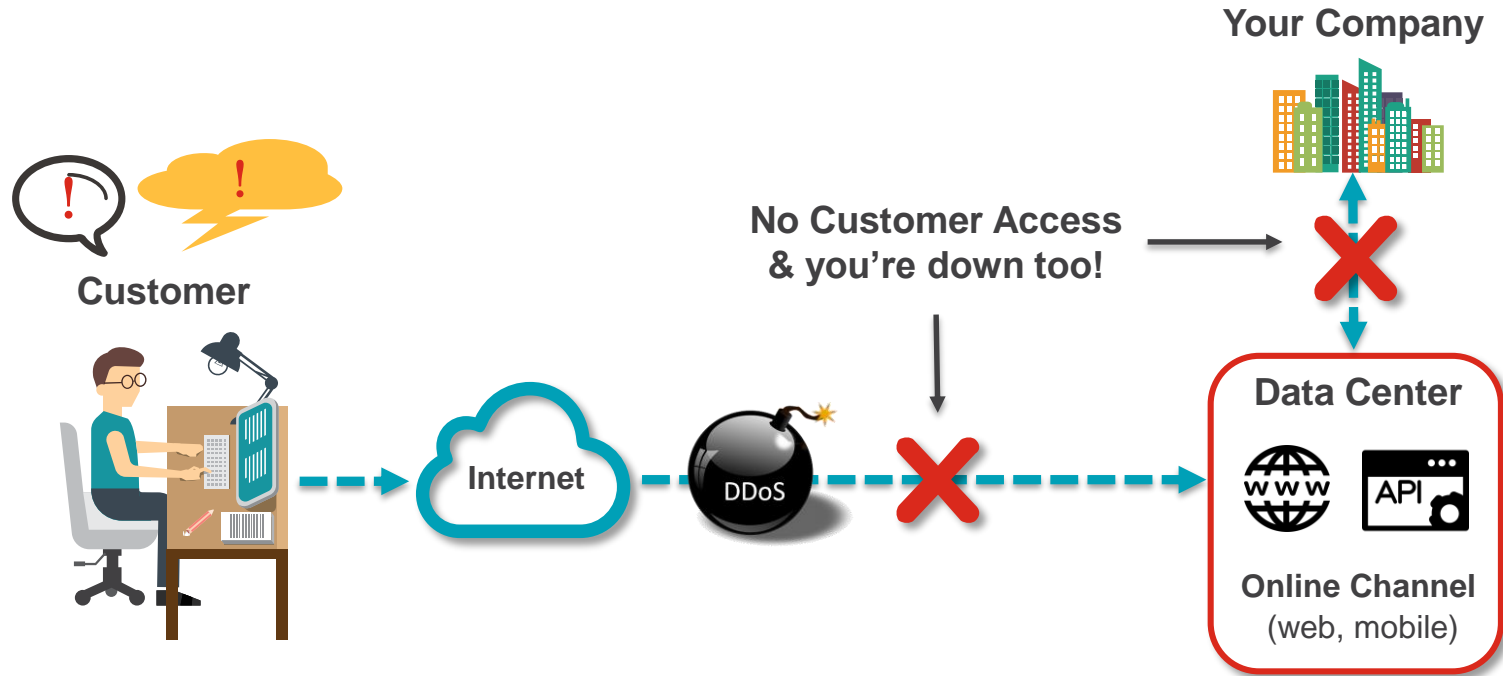
Cyber Breach Example – The D-DDOS Scenario

Let me set this up...

- Your business sustains a D-DDOS attack, but you think it's a DDOS attack.
- Your customers are impacted, IT is running around trying to restore service.
- Call centers are receiving complaints:
 - lower customer satisfaction, unlikely to recommend and driving up cost.
- Magically, systems are restored 3 hours later...
- People are asking what happened, yet are so happy everything is back up!

So what does it look like from a customer perspective...

Process & Tech Stuff Matters – What “Bad” looks like to your Customer



Really? Now I can't even get to their website!!!

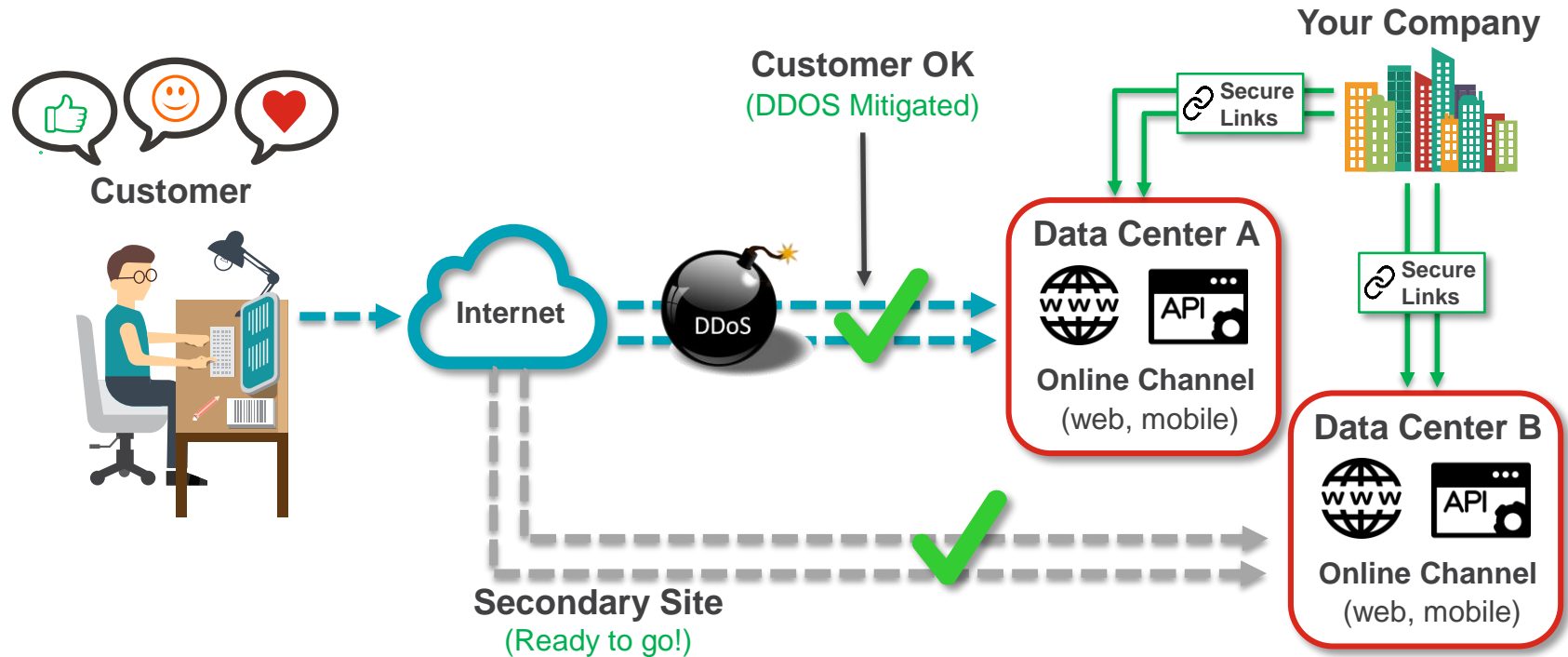
Cyber Breach Exercise – The D-DDOS Scenario – the Impact

Let me set this up...

- 47 days later, you are contacted.
- An unknown party has stolen 2.1M of your customer records.
- The unknown party demands \$3MM in bitcoin or they go to the media...
- Your reaction – maybe E and/or F (ignore or retire immediately)?
- Turns out the 1st “D” in DDOS is ‘DEADLY’...
- Time to use the ‘learn-as-you-go model’ (we know how that story plays out...)

So what does good look like to your customers?

Process & Tech Stuff Matters – What “Good” looks like to your Customer



Whether On-Premise, outsourced Data Center or Cloud... Resilience Matters!

Cyber Breach Wrap Up

- 01** Customers matter
- 02** Don't let the bad guys steal our Moms' stuff
- 03** Tone from the top is essential
- 04** Planned cyber resiliency is key (process & tech stuff matters)
- 05** Thank you for coming on the journey today

Seeing Atlantic Canada businesses thrive is what motivates us!

We're committed to solutions in Atlantic Canada that:

- Provide local data centre and cloud services within our national data centre infrastructure;
- Focus on secure, dedicated connectivity as well as high-performance Internet access;
- Bring to our business customers mobile solutions on the cutting edge of innovation;
- Reflect our commitment to the region through our 1500 regional employees;
- And we're committed to doing it all securely.



