To Trust of Not To Trust
What Every Startup Needs To Know About Privacy and Cybersecurity
CONNECTS Seminar at Carnegie Mellon: OCTOBER 10, 2019
John Funge, DataTribe
# Biggest Data Breaches of the 21st Century

<table>
<thead>
<tr>
<th>Year</th>
<th>Company</th>
<th>Lost Records (million)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018</td>
<td>Marriott</td>
<td>500</td>
</tr>
<tr>
<td>2017</td>
<td>Equifax</td>
<td>143</td>
</tr>
<tr>
<td>2016</td>
<td>Adult Friend Finder</td>
<td>412</td>
</tr>
<tr>
<td>2015</td>
<td>Anthem</td>
<td>79</td>
</tr>
<tr>
<td>2014</td>
<td>Ebay</td>
<td>145</td>
</tr>
<tr>
<td>2014</td>
<td>JP Morgan Chase</td>
<td>76</td>
</tr>
<tr>
<td>2014</td>
<td>Home Depot</td>
<td>56</td>
</tr>
<tr>
<td>2013</td>
<td>Yahoo</td>
<td>3000</td>
</tr>
<tr>
<td>2013</td>
<td>Target Stores</td>
<td>110</td>
</tr>
<tr>
<td>2013</td>
<td>Adobe</td>
<td>38</td>
</tr>
<tr>
<td>2012</td>
<td>OPM</td>
<td>22</td>
</tr>
<tr>
<td>2011</td>
<td>Sony Playstation Net</td>
<td>77</td>
</tr>
<tr>
<td>2011</td>
<td>RSA Security</td>
<td>40</td>
</tr>
<tr>
<td>2008</td>
<td>Heartland Payment Sys</td>
<td>134</td>
</tr>
<tr>
<td>2006</td>
<td>TJX Companies</td>
<td>94</td>
</tr>
</tbody>
</table>

HERE’S WHAT WE KNOW ABOUT RUSSIA AND THE DNC HACK
22 Million Affected by OPM Hack, Officials Say

The extent of the hack has finally been revealed.
“Mark Zuckerberg declared in 2010 that privacy is no longer a “social norm,” but bought the four houses abutting his Palo Alto home to help ensure his own privacy.”

Schneier, Bruce. *Data and Goliath*
“I believe there's an opportunity to set a new standard for private communication platforms…”

Mark Zuckerberg, A Privacy-focused Vision for Social Media, March 2019
“It takes 20 years to build a reputation and five minutes to ruin it.”

Warren Buffett
What We’ll Talk About

• Big Picture
• Few Startup Axioms
• Privacy
• Security
• Questions
Big Picture
“Privacy doesn’t just depend on agency; Being able to achieve privacy is and expression of agency.”

Danah Boyd quoted in *Data and Goliath* by Bruce Schneier
So, how does this apply to startups?
Axiom 1: Focus
Axiom 2: Stage Appropriateness
Axiom 3: You’ll not end up where you think
Axiom 4: Find trustworthy trail guides early
Privacy
Context

• Ever Increasing Digitalization of Life
• Identity Resolution
• Cloud Computing → Democratizing Big Data
• GDPR & CCPA
• Social Credit Score In China
• AI
• No System is 100% Secure
Regulations and Trends

• There Are Many, It’s Sort of a Mess

• Some Key Regulations To Be Aware Of
  • State-level Data Breach Laws
  • General Data Protection Regulation (GDPR)
  • Fair Credit Reporting Act (FCRA)
  • Gramm-Leach-Bliley
  • Can Spam Act
  • Telephone Consumer Protection Act
  • Children’s Online Privacy Protection Act (COPPA)
  • Health Insurance Portability and Accountability Act (HIPPA)
  • Federal Election Commission

• Trends
  • National “GDPR-like” Regulation Coming to U.S.
  • California Consumer Privacy Act (CCPA)
Making Sense of It All

• Minimize what you collect
• Handle sensitive data with care
• Carefully evaluate privacy trade-offs
• Diligently protect
Key Concepts In CCPA

• Right to access
• Right to deletion
• Right to knowing if sold, and for what purpose
• Right to opt out
“Toxic Data” & Data Breach Laws

• **Personal Information:** An individual’s first name or first initial and last name plus one or more of the following data elements: (i) Social Security number; (ii) driver’s license number or state-issued ID card number; or (iii) account number, credit card number or debit card number combined with any security code, access code, PIN or password needed to access an account; generally applies to computerized data that includes personal information. Personal Information shall not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.

• **Breach of Security:** The unlawful and unauthorized acquisition of personal information that compromises the security, confidentiality or integrity of personal information.

Security
# A Simple Way of Breaking It Down

<table>
<thead>
<tr>
<th></th>
<th>Offense</th>
<th>Defense</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nation-State</td>
<td><img src="image" alt="Checkmark" /></td>
<td><img src="image" alt="Checkmark" /></td>
</tr>
<tr>
<td>Companies &amp; Criminals</td>
<td>Criminals</td>
<td>Companies</td>
</tr>
<tr>
<td>Kids in the Basement</td>
<td><img src="image" alt="Checkmark" /></td>
<td>--</td>
</tr>
</tbody>
</table>
Who is a CISO?
What is OPSEC?
General Guidelines

- Focus on doing the basics well
- Invest where there is risk
Top 5 Checklist
From Harvard Belfer Center Cybersecurity Campaign Playbook

1. Establish a culture of security awareness
2. Use the cloud
3. Use two-factor authentication
4. Encrypted messaging for sensitive comm.
5. Plan and prepare

Source: https://www.belfercenter.org/cyberplaybook
Frameworks to Know About

• NIST
  • https://www.nist.gov/sites/default/files/documents/cyberframework/cy
    bersecurity-framework-021214.pdf

• System and Organization Controls (SOC)
  • Part of SSAE 16 by American Institute of CPAs
  • https://www.aicpa.org/soc
Third Party Ecosystem Risk

At Dropbox, the security of your data is our highest priority.

See why millions of people and organizations trust us with their most important work.

Visit the Business Trust Guide
Customers & Partners Will Hold You Accountable

• Limitation of Liability. EXCEPT WITH RESPECT TO CLAIMS OF INDEMNITY, BREACH OF CONFIDENTIALITY, BREACH OF DATA SECURITY OBLIGATIONS, AND ARISING FROM A DATA INCIDENT (AS SET FORTH IN SECTION XX), IN NO EVENT SHALL EITHER PARTY BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS/REPUTATIONAL HARM, REVENUE, DATA, OR USE, INCURRED BY OTHER PARTY OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. EXCEPT WITH RESPECT TO CLAIMS OF INDEMNITY, BREACH OF CONFIDENTIALITY, BREACH OF DATA SECURITY OBLIGATIONS, AND ARISING FROM A DATA INCIDENT (AS SET FORTH IN SECTION XX), TOTAL LIABILITY FOR A SERVICE IS LIMITED IN ALL CASES AND IN THE AGGREGATE TO THE AMOUNT OF FEES ACTUALLY PAID BY COMPANY FOR THE CORRESPONDING SERVICE DURING THE TWELVE (12) MONTHS PRECEDING THE DATE OF THE EVENT THAT IS THE BASIS FOR THE FIRST CLAIM.

Be Vigilant of Open Source Tools You Use
Cyber Risk Insurance
“Complexity is the worst enemy of security…”

Schneier, Bruce. *Data and Goliath*
“We will bankrupt ourselves in the vain search of absolute security.”

Dwight D. Eisenhower
Thank You

John Funge
DataTribe
john.funge@datatribe.com