Potential
*Estimated global spend as reported by IDC (11% CAGR)
1.5T

*Estimated global cybercriminal revenue as reported by Bromium
*Estimated global damages as reported by Cybersecurity Ventures*
Dollars Related To Cybercrime & Cybersecurity

- **Damages**
  - 2016: $3000 Billion
  - 2017: $3500 Billion
  - 2018: $4000 Billion
  - 2019: $4500 Billion
  - 2020: $5000 Billion

- **Revenue**
  - 2016: $1500 Billion
  - 2017: $1750 Billion
  - 2018: $2000 Billion
  - 2019: $2250 Billion
  - 2020: $2500 Billion

- **Security**
  - 11% Growth Rate
Recently confirmed Myspace hack could be the largest yet

Sarah Perez  @sarahintampa  /  2 years ago

You might not have thought of – much less visited – Myspace in years. (Yes, it’s still around. Time, Inc. acquired it and other properties when it bought Viant earlier this year.) But user data never really dies, unfortunately. For Myspace’s new owner, that’s bad news, as the company confirmed just ahead of the Memorial Day holiday weekend in the U.S., that it has been alerted to a large set of stolen Myspace username and password combinations being made available for sale in an online hacker forum.

The data is several years old, however. It appears to be limited to a portion of the overall user base from the old Myspace platform prior to June 11, 2013, at which point the site was relaunched with added security.
Weebly hacked, 43 million credentials stolen

Kate Conger, Katie Roof  2 years ago

The web design platform Weebly was hacked in February, according to the data breach notification site LeakedSource. Usernames and passwords for more than 43 million accounts were taken in the breach, although the passwords are secured with the strong hashing algorithm bcrypt.

Weebly said in an email to customers that user IP addresses were also taken in the breach.

“We do not believe that any customer website has been improperly accessed,” Weebly said in the notice to users.” The company also said that it does not store credit card information, making fraudulent charges unlikely.

LeakedSource said it received the Weebly database from an anonymous source and notified Weebly of the breach. In addition to the customer notification emails, LeakedSource claims that password resets are being issued — but, if you’re a Weebly user and you don’t receive a password reset, you probably want to change your password anyway.

Meanwhile, LeakedSource also identified data from Foursquare, claiming that 22.5 million accounts were compromised in December 2013. The social media company disputes the findings, claiming that email addresses and other data were not exposed.
Emails

The security flaws at the heart of the Panama Papers

By MATT BURGESS and JAMES TEMPERTON

Wednesday 6 April 2016
Every single Yahoo account was hacked - 3 billion in all

by Selena Larson  @selenalarson

October 4, 2017 6:36 AM ET
Uber hid a hack that exposed data of 57 million users and drivers for more than a year

- Hackers stole data from 57 million Uber users and drivers in 2016.
- The hackers stole names and driver's license numbers of around 600,000 drivers in the U.S., as well as rider names, email addresses and mobile phone numbers.
- The company paid hackers $100,000 to delete the data and keep the breach quiet, and did not report the breach.

Anita Balakrishnan | Deirdre Bosa
Published 5:02 PM ET Tue, 21 Nov 2017 | Updated 9:24 AM ET Wed, 22 Nov 2017
Hacker steals data from up to 100,000 Bell Canada customers in second breach in eight months

BCE says hackers got hold of up to 100,000 customer names and email addresses, and a limited number of phone numbers, user names and/or account numbers.
The Equifax hack could be worse than we thought

by Donna Borak and Kathryn Vasel  @CNNMoney

February 10, 2018: 10:43 AM ET
Twitter advising all 330 million users to change passwords after bug exposed them in plain text

There’s apparently no evidence of any breach or misuse, but you should change your password anyway

By Chaim Gartenberg | @cgartenberg | May 3, 2018, 4:21pm EDT
Hackers threaten to reveal personal data of 90,000 Canadians caught in bank hack

BMO and Simplii say thieves stole information, demanded $1M ransom for safe return

Pete Evans · CBC News · Posted: May 29, 2018 11:25 AM ET | Last Updated: May 30

On The Money
Hack victim
Air Canada says 20,000 mobile app users affected by data breach

By Maham Abedi
National Online Journalist, Breaking News  Global News

Air Canada customers hacked in cyber attack
Facebook Network Breach Impacts Up to 50 Million Users
THOUSANDS of hours wasted
BILLIONS of records breached
BILLIONS of dollars spent
TRILLIONs of dollars lost
TENS of convictions
Is this what SUCCESS looks like?
Pause
A short tangent...
Large Research Organization

Global Reach

Cloud Focus
History
New capabilities
Top problem
Biggest opportunity
How did we get here?
The goal of cybersecurity

Protect the confidentiality, integrity, and availability of information
CIO

CISO

Service Delivery

System Support

System Development
RACI for customer facing solutions
Can We Do That?
Joe
CISO, OurCo
170

*Number of days to detect a persistent threat on network as per Ponemon, 2018*
“Let’s start a threat hunting program”

“What will we need?”

“Some new tools & 2 team members...”
- Generate stronger analytics
- Expand AppSec program
- Fill open requisitions for SOC
- Deploy shelfware
- Create threat hunting team?!?
IT Employees
Cybersecurity
1:50:750

You  IT  Employees
A Lack Of People
Can you find these people?
Confront the Cybersecurity Talent Shortage

June 23, 2017
Contributor: Kasey Panetta
There are currently more than 348,000 open security positions, according to CyberSeek. By 2022, there will be 1.8 million unfilled positions, according to the Center for Cyber Safety and Education. As companies evolve toward digital business and bimodal setups, these skills are becoming more difficult to find and more expensive to hire, particularly in rural areas.

Companies need to be able to attract this type of talent, or risk being a part of the business strategy.

**Confront the Cybersecurity Talent Shortage**

June 23, 2017

Contributor: Kasey Panetta
ANALYSIS

Research suggests cybersecurity skills shortage is getting worse

New data from reveals growing skills gaps that represent an existential threat. What should organizations do?
* Graduates in cybersecurity from Canadian universities per year as per Universities Canada, 2018
Can you find these people?
Can you keep these people?
Will these people actually help?
Malware starts via phishing as per Verizon DBIR, 2018
Phishing awareness campaign
| .accountant | .education | .jetzt | .school |
| .apartment | .energy | .kim | .soccer |
| .associates | .engineering | .lawyer | .surf |
| .bingo | .enterprise | .love | .surf |
| .boutique | .fish | .maison | .theater |
| .brussels | .fitness | .memorial | .today |
| .careers | .flights | .network | .vacations |
| .clinic | .glass | .one | .video |
| .consulting | .global | .parts | .webcam |
| .degree | .gripe | .party | .wiki |
| .dog | .hockey | .porn | .wtf |
| .download | .how | .rentals | .yoga |
|         |          |        | .zone |
Runs counter to the idea of a link
2.77%

*Effectiveness of phishing training by McCoy et al., 2017*
Web attacks use stolen credentials as per Verizon DBIR, 2018
Password awareness campaign
This does not give me confidence in your password security, @YourAlberta. (cc. @troyhunt)
Runs counter to math & psychology
86% * Of passwords are reused or simple as per Troy Hunt, 2018
Ugh, Users
Us vs. Them
“Users” are the problem
“Users” are the problem
* Forgotten common sense
Us vs. Them
Containment
“This system needs to be deployed.”

“When?”

“Monday...”
Stage

Run
Resolution Cost—Workflow Stage

* NIST Planning Report 02-3
Late stage risk assessments limit options
Bolt-on
Resolution Cost—Workflow Stage

* NIST Planning Report 02-3
Resolution Cost—Workflow Stage

* NIST Planning Report 02-3
<table>
<thead>
<tr>
<th></th>
<th>Elite</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Deployment Frequency</strong></td>
<td>On-demand (multiple deploys per day)</td>
<td>Between once per hour and once per day</td>
<td>Between once per week and once per month</td>
<td>Between once per week and once per month</td>
</tr>
<tr>
<td><strong>Lead time for changes</strong></td>
<td>Less than one hour</td>
<td>Between one day and one week</td>
<td>Between one week and one month</td>
<td>Between one month and six months</td>
</tr>
<tr>
<td><strong>Time to restore service</strong></td>
<td>Less than one hour</td>
<td>Less than one day</td>
<td>Less than one day</td>
<td>Between one week and one month</td>
</tr>
<tr>
<td><strong>Change failure rate</strong></td>
<td>0-15%</td>
<td>0-15%</td>
<td>0-15%</td>
<td>46-60%</td>
</tr>
</tbody>
</table>

*2018 State of Devops report from DORA*
Early security intervention opens up new options

Can you **keep** up with development cycles?

Can you speak developer?
What now?
You can’t scale...**automate**

User’s ≠ problem...**educate**

Not collaborating...**participate**
The goal of cybersecurity

Make sure that systems work as intended

...and only as intended
Thank you

Read more at
https://markn.ca
Reach me online
@marknca