Welcome
We Will Be Starting Shortly
Welcome and Introductory Remarks

Elisa Jillson
Federal Trade Commission
Division of Privacy and Identity Protection
Opening Remarks

Andrew Smith
Federal Trade Commission
Bureau of Consumer Protection
Presentations on Data Breaches

2018 Data Breach Investigations Report
Marc Spitler

Strategic News Bundling and Privacy Breach Disclosures
Sebastien Gay

2018 Identity Fraud: Fraud Enters a New Era of Complexity
Al Pascual

Moderators: Jared Ho, Marc Luppino
2018 Data Breach Investigations Report
Facts versus opinions.

DBIR is based on analysis of real world security incidents and confirmed data breaches.

Information is supplied by 67 partners in the latest edition, covering 1000s of companies in 65 countries.
Show me the money.
The motive behind most breaches is money.
Ransomware
If you ever want to see your precious data again…

We hate being right – back in 2013 we said: “[This may] blossom as an effective tool of choice for online criminals”

- Doubled again this year after having doubled last year.
- Responsible for 39% of all malware related breaches.
- Ransomware accounts for 85% of all malware in Healthcare.
Social Engineering
We're only human

<table>
<thead>
<tr>
<th>Frequency</th>
<th>1,450 incidents, 381 with confirmed data disclosure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top 3 patterns</td>
<td>Crimeware, Everything Else, and Cyber-Espionage represent 93% of all security incidents</td>
</tr>
<tr>
<td>Threat actors</td>
<td>99% External, 6% Internal, &lt;1% Partner (breaches)</td>
</tr>
<tr>
<td>Actor motives</td>
<td>59% Financial, 38% Espionage (breaches)</td>
</tr>
<tr>
<td>Data compromised</td>
<td>47% Personal, 26% Secrets, 22% Internal, 17% Credentials</td>
</tr>
</tbody>
</table>

Phishing and pretexting represent 98% of social incidents and 93% of breaches.
Vertical differences

The table shows how different the breakouts of actors, motives, tactics, and attack patterns look across industries. Some industries handle significant amounts of payment card data, some have databases full to the brim with personally identifiable information (PII), some protect classified information and some are lucky enough to do all of the above.
Threat Action Varieties

- Denial of Service attacks are common across numerous industries for incidents.
- Use of stolen creds and social attack related breaches plague several verticals.
- Privilege Abuse rampant in Public and Healthcare.
Questions?

www.verizonenterprise.com/DBIR
Strategic News Bundling and Privacy Breach Disclosures

Sebastien Gay
2018 Identity Fraud Study

Fraud Enters a New Era of Complexity

Javelin Strategy & Research
2017 Stood Out as Fraud Became More Pervasive Than Ever and Consumers’ Most Sensitive PII Was Compromised as Never Before

It was a year for the record books

- **6.52%** Record high identity fraud incidence in 2017
- **$16.8 billion** Total fraud losses at highest point in past four years
- **35%** Proportion of breach victims whose SSN was compromised

Source: Javelin Strategy & Research, 2018
Victims Spent More of Their Own Money Resolving Cases of Identity Fraud in 2017

Out-of-pocket costs for victims of identity fraud, 2015-2017

- 2015: $57
- 2016: $49
- 2017: $104

Source: Javelin Strategy & Research, 2018
Nearly A Third of Consumers Hit By Data Breach in 2017, Many Not for the First Time

Consumers’ Data Breach Status (2016-2017)

Source: Javelin Strategy & Research, 2018
The Equifax Breach Sent Consumers Scrambling for Information Wherever They Could Find It

Google news search in interest “data breach” (January 2013 to December 2017)

Source: Google Trends, 2018
Cynicism Regarding Breach Notifications Understandably Jumped

Agreement with: “Data breach notifications merely help organizations to save face or meet legal requirements, and do little to protect me”

Source: Javelin Strategy & Research, 2018
Concern About Fraud Also Rose Considerably in 2017

Consumers concerned about identity fraud, 2016-2017

Source: Javelin Strategy & Research, 2018
Data Breach-Fraud Connection Loosened as the Breach Population Grew and Fraud Evolved

Fraud incidence by breach notification status, 2015-2017

Source: Javelin Strategy & Research, 2018
Account Takeovers Incidence and Losses Have More Than Tripled in the Past Three Years

Account takeover incidence and losses, 2015-2017

Source: Javelin Strategy & Research, 2018
A High in New Account Fraud Victims Isn’t Accompanied by A Similar Rise in Losses

New Account Fraud Incidence and Losses, 2015-2017

Source: Javelin Strategy & Research, 2018
EAF Victims are Experiencing More Complete Impersonation as Fraudsters Close the Loop

Millions of EAF victims with fraudulent intermediary accounts opened, 2015-2017

Source: Javelin Strategy & Research, 2018
Thank You

Al Pascual
SVP, Research
Head of Fraud & Security
al.pascual@javelinstrategy.com
Presentations on Data Breaches

Panel Discussion:
Marc Spitler, Sebastien Gay, Al Pascual

Moderators:
Jared Ho, Marc Luppino
Lunch Break
11:45 am-1:00 pm
Incentives to Invest in Data Security

Panel Discussion:
Lawrence A. Gordon, Matthew P. McCabe, Tyler Moore, Sasha Romanosky, Matthew Sharp

Moderators:
Elisa Jillson, Mike LeGower
## Incentives

<table>
<thead>
<tr>
<th>Customer Trust</th>
<th>Reputation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ex Ante Compliance</td>
<td>Ex Post Liability</td>
</tr>
<tr>
<td>Customer Demand</td>
<td>Competitive Advantage</td>
</tr>
<tr>
<td>Cost Reduction</td>
<td>Cyber Insurance Coverage</td>
</tr>
</tbody>
</table>
**Benefits and Costs of an Investment in Cyber/Information Security***

Expected Benefits of Investment = \( (v - S[z, v])L \)

Optimal Investment Example**

\[ z^*(v) = \frac{1}{e} vL \]

Benefits are increasing at a decreasing rate.

100% security is not possible.

Level of investment in information security

\( z^* \) – Optimal Investment Level

\( S[z, v] \) – Revised \( v \) after \( z \) (Revised probability of breach)

\( v \) – Vulnerability (Probability of security breach)

\( L \) – Potential Loss

\( vL \) – Expected Loss

\( z \) – Level of Investment

\( z^* \) – Optimal Investment Level

\( S[z, v] \) – Revised \( v \) after \( z \) (Revised probability of breach)


YouTube Video explaining the Gordon-Loeb Model: [https://www.youtube.com/watch?v=cd8dT0FuqQ4](https://www.youtube.com/watch?v=cd8dT0FuqQ4)

BBB Recommends the Gordon Loeb Model

2017 U.S. Better Business Bureau (BBB) report recommends the Gordon-Loeb Model as "...a useful guide for organizations trying to find the right level of cybersecurity investment."
Incentives to Increase Cybersecurity Investments in Private Sector Firms*

Why Are Cybersecurity Investments So Difficult to Justify in Private Sector Firms?

- They are primarily cost savings projects rather than revenue generating projects (and savings can’t be observed)
- Costs of breaches are largely implicit (reputation & liability) vs. Explicit costs (detecting & correcting breaches)
- Most breaches impact earnings and stock prices in the short-run, but not long-run (customers & stockholders have become tolerant of breaches)
- The risk (uncertainty) of breaches can’t be measured precisely & investments are largely irreversible. Wait & see approach may be rational (deferment option)
- Externalities are important, but hard to justify

Government Regulations/Incentives Could Result in Less Cybersecurity

ISOSEC—the same quantity of security is achieved while changing inputs

Government Regulations/Incentives Could Result in More Cybersecurity

ISOSEC*

Regulation forcing security input $x_1$ to increase to $x_R$ results in a decrease in the level of security, if total level of spending (i.e., security budget, $B_1$) remains fixed and the firm was utilizing the optimal mix of inputs prior to the regulation.

Pre-regulation Security Level $L$, Security Budget: $B_1 = P_x x_L + P_y y_L$

Post-regulation Security Level $R$, Security Budget: $B_R = P_x x_R + P_y y_R$

$B_R = B_1$


Insights and Results from Gordon, Loeb, Lucyshyn & Zhou Research

Government incentives/regulations affect cybersecurity investments in private sector firms depending on:

1. Firm’s cybersecurity budget is fixed or increases
2. Firm is utilizing the optimal mix of inputs

Fixed budget/opt mix -- incent/reg: security ↓

Fixed budget/non-opt mix--incent/reg: security ↑↓

Increased budget -- incent/reg: security ↑

In 2016, NSA awarded this paper Honorable Mention for its contribution to the scientific cybersecurity literature.
Who provides (or should provide) incentives to invest in data security?

A. Culture – security professionals, executives, boards

B. Customers / consumers

C. Cyber insurance

D. Law – state statutes, data breach litigation, federal agencies, etc.

E. Other
Incentives to Invest in Data Security

Panel Discussion:
Lawrence A. Gordon, Matthew P. McCabe, Tyler Moore, Sasha Romanosky, Matthew Sharp

Moderators:
Elisa Jillson, Mike LeGower
Break
2:30-2:45 pm
Consumer Demand for Data Security

Panel Discussion:
Justin Brookman, Michael Higgins, Wiley Hodges, Kirsten Martin, Rick Wash

Moderators:
Jared Ho, Marc Luppino
Consumer Reports by the numbers

- 7m+ Subscribers
- $250m revenue
- 1m+ Survey responses
- 60 state-of-the-art labs
- 327 acres at Auto Test Center
- 7000+ products tested annually
<table>
<thead>
<tr>
<th>Test Name</th>
<th>Criteria</th>
<th>Indicators</th>
<th>Procedure Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functionality Over Time</td>
<td>The company will continue to maintain the intended functionality of the product over the product's expected life cycle.</td>
<td>Every feature of the product will continue to work for as long as I can reasonably expect; that is, the manufacturer will not 'brick' certain parts of the product.</td>
<td></td>
</tr>
<tr>
<td>Terms of Service and Privacy Policy documents</td>
<td>I can easily find, read, and understand the privacy policy and/or terms of service.</td>
<td>The Terms of service (ToS) are easy to find. The ToS are available in the language(s) most commonly conversed by the company.</td>
<td></td>
</tr>
<tr>
<td>Data control</td>
<td>I can see and control everything the company knows about me.</td>
<td>Users can control the collection of their information. Users can delete their information.</td>
<td></td>
</tr>
</tbody>
</table>

Investigation and analysis of publicly available documentation to determine what the company clearly discloses.
### Key security elements evaluated

<table>
<thead>
<tr>
<th>Use of encryption</th>
<th>Commitment to support period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resistance to attacks</td>
<td>Password rules</td>
</tr>
<tr>
<td>Vulnerability disclosure program</td>
<td>Security oversight</td>
</tr>
<tr>
<td>Automatic/push updates</td>
<td>Multifactor authentication</td>
</tr>
<tr>
<td>Best build practices</td>
<td>Reliance on 3P content or libraries</td>
</tr>
<tr>
<td>Out-of-band notice of changes</td>
<td>Updates authenticated</td>
</tr>
</tbody>
</table>
Goals

• More information to marketplace
• Empower consumers to make security-conscious choices
• Provide accountability for poor security practices
• Push companies toward stronger security
Glow Pregnancy App Exposed Women to Privacy Threats, Consumer Reports Finds

Glow has responded by fixing the problems and updating the app

By Jerry Bellinson
July 28, 2016

Glow is a mobile app designed to help women track their menstrual cycles and fertility. Like similar apps, it asks users to record the onset of their periods, along with details such as their weight and medications. Glow also asks for intimate physical details, including the appearance of their cervical mucus and the position of their cervix (the app has instructions for determining these characteristics), any history of abortions, whether they've experienced anything from diarrhea to low sex drive, their mood, and more.

Recently, Consumer Reports tested Glow for security and privacy features as part of a broader project, and found surprising vulnerabilities. One security flaw might have let someone with no hacking skills at all access a woman's personal data. Other vulnerabilities would have allowed an attacker with rudimentary software tools to collect email addresses, change passwords, and access personal information from participants in Glow's community forums, where people discuss their sex lives and health concerns.
Samsung and Roku Smart TVs Vulnerable to Hacking, Consumer Reports Finds

Security and privacy testing of several brands also reveals broad-based data collection. How to limit your exposure.
<table>
<thead>
<tr>
<th>SERVICE</th>
<th>OVERALL SCORE</th>
<th>PAYMENT AUTHENTICATION</th>
<th>DATA SECURITY</th>
<th>DATA PRIVACY</th>
<th>CUSTOMER SUPPORT</th>
<th>BROAD ACCESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple Pay</td>
<td>76</td>
<td>![Green Arrow]</td>
<td>![Green Arrow]</td>
<td>![Green Arrow]</td>
<td>![Green Arrow]</td>
<td>![Green Arrow]</td>
</tr>
<tr>
<td>Venmo</td>
<td>69</td>
<td>![Green Arrow]</td>
<td>![Yellow Arrow]</td>
<td>![Green Arrow]</td>
<td>![Green Arrow]</td>
<td>![Green Arrow]</td>
</tr>
<tr>
<td>Cash App (Square)</td>
<td>64</td>
<td>![Green Arrow]</td>
<td>![Green Arrow]</td>
<td>![Green Arrow]</td>
<td>![Green Arrow]</td>
<td>![Green Arrow]</td>
</tr>
<tr>
<td>Facebook P2P Payments in Messenger</td>
<td>63</td>
<td>![Green Arrow]</td>
<td>![Green Arrow]</td>
<td>![Green Arrow]</td>
<td>![Green Arrow]</td>
<td>![Green Arrow]</td>
</tr>
</tbody>
</table>
Security testing challenges

• Public documentation often lacking
• Lack of initial visibility into update frequency and quality
• Black box/server-side difficult/impossible to test
• Difficult to adapt and scale suite of tests to broad range of consumer products
• Score subjectivity
• How assess patched vulnerabilities
• Practices can change with little discoverability
Limitations on demand-driven approach

• Externalities not felt by consumers
• Difficulty in assessing security risks
• Testing provides imperfect information
• Attribution difficult and delayed
• Need for legal baseline security requirements
How important is perceived security to consumers making purchasing decisions?

A. Important, but they expect the firm to be responsible for security.

B. Important, and they understand that security is a shared responsibility between themselves and the firm.

C. Moderately important, and they expect firms to be responsible for security

D. Moderately important, and they understand it’s a shared responsibility.

E. Not important, because consumers don’t expect security.

F. Other
## Trade-offs

<table>
<thead>
<tr>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Productivity</td>
</tr>
<tr>
<td>Usability</td>
</tr>
<tr>
<td>Functionality</td>
</tr>
<tr>
<td>Latency</td>
</tr>
<tr>
<td>Other</td>
</tr>
</tbody>
</table>
Consumer Demand for Data Security

Panel Discussion:
Justin Brookman, Michael Higgins, Wiley Hodges, Kirsten Martin, Rick Wash

Moderators:
Jared Ho, Marc Luppino
Closing Remarks

Jim Trilling
Federal Trade Commission
Division of Privacy and Identity Protection
Thank You,
Join Us Tomorrow