

---

# Digital Engagement During Uncertain Times

## Part I - Cybersecurity and Privacy Issues for Municipalities

**Brandon N. Robinson**

Alabama Communities for Excellence  
(ACE)

July 14, 2017

# Agenda

---

- I. Why Do We Care?
- II. What Does It Look Like?
- III. What Do We Do?
- IV. What About Privacy?

# I. DATA BREACHES: WHY DO WE CARE?

# What data do we have?

---

## Municipalities:

- Collect, process, and store large amounts of sensitive data
- Are responsible for critical infrastructure (utilities) and essential services
- Increased mobile use / BYOD
- Increased outsourcing (vendor/cloud) functions using customer data
- Increased interactions with constituents (social media, etc.) and thus info that is arguably sensitive (and potentially valuable)!
- Unique and significant trust relationships with constituents

# What Data Do We Have?

- Human Resources: SSN, Driver's license, passport numbers, health information (PHI/PII)
- Finance Department: Bank account information
- Public Safety: Criminal/personal information, confidential information, critical infrastructure
- Parks and Rec: Credit card numbers (PCI)
- Tax Assessments: Resident information, CC numbers
- Student Information: SSN, DL numbers, health info (PHI/PII), educational records

# How much would it cost?



## Ponemon Institute, "2017 Cost of Data Breach Study: Global Overview" (June 2017)

### United States

FY 2017: **\$225**/ per capita

4 –year average: **\$216** / per capita

### U.S. Public Sector

FY 2017: **\$71** / per capita

4-year average **\$80** / per capita

\*Per capita cost is defined as the total cost of data breach divided by the size of the data breach (i.e., the number of lost or stolen records).

How much would a data breach cost?\*

HIGH END



Municipal populations in AL x \$225/per capita:

- **Smallest** (McMullen, pop. 10) = **\$2,250**
- **Largest** (Birmingham, pop. 212,237) = **\$47.753M**
- **Median** pop. 1,260 (e.g., Elmore, Rogersville) = **\$287,325**
- **Average** pop. 4,589.18 (e.g., Fayette, Adamsville) = **\$1,411,573.21**
- **Median/Average top 25 municipalities** (pop. 34,033-64,335) = **\$7.657M - \$14.475M**

\*Based on U.S. Census Bureau, Census 2010

How much would a data breach cost?\*

LOW END



Municipal populations in AL x \$71/per capita:

- **Smallest** (McMullen, pop. 10) = **\$710**
- **Largest** (Birmingham, pop. 212,237) = **\$15.068M**
- **Median** pop. 1,260 (e.g., Elmore, Rogersville) = **\$89,460**
- **Average** pop. 4,589.18 (e.g., Fayette, Adamsville) = **\$325,831.78**
- **Median/Average** Top 25 municipalities (pop. 34,033-64,335) = **\$2.416M - \$4.567M**

\*Based on U.S. Census Bureau, Census 2010



# Public Entities Among Top Three



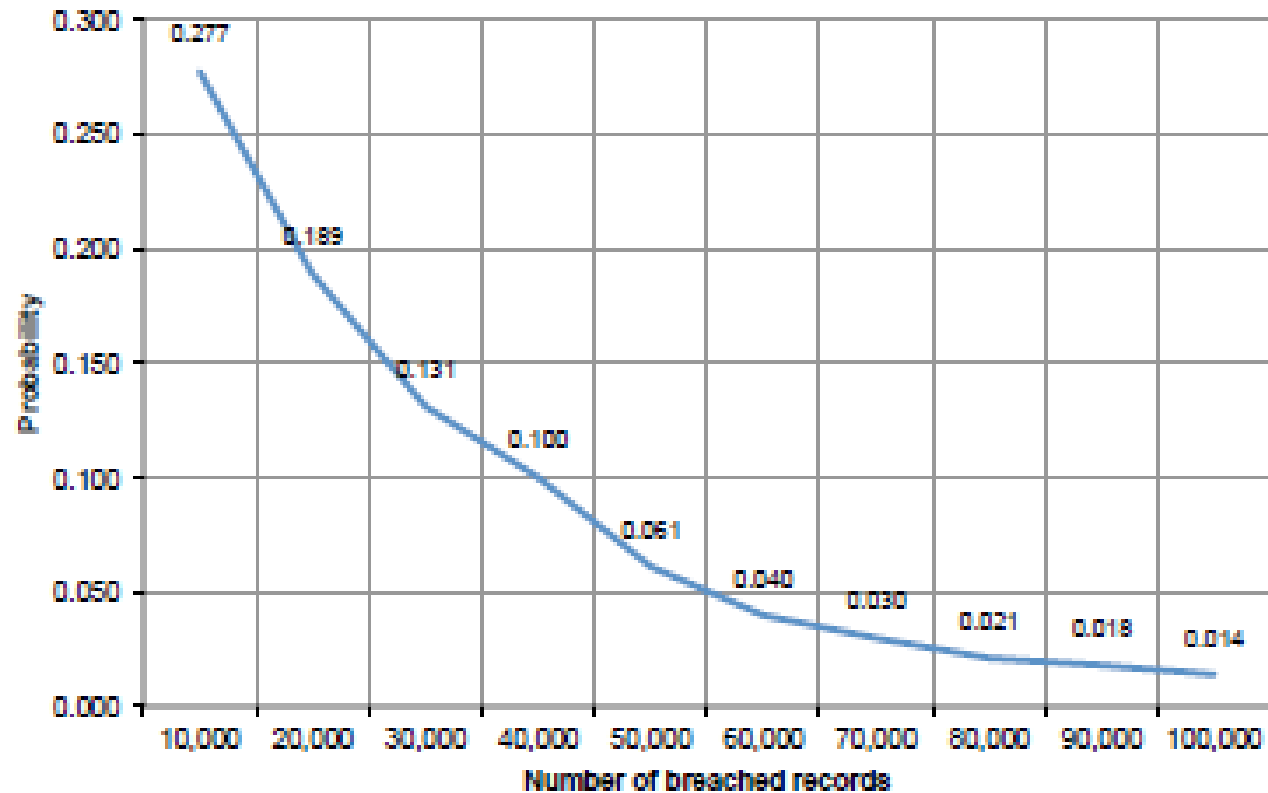
INDUSTRY	NUMBER OF SECURITY INCIDENTS				CONFIRMED DATA LOSS			
	TOTAL	SMALL	LARGE	UNKNOWN	TOTAL	SMALL	LARGE	UNKNOWN
Accommodation (72)	368	181	90	97	223	180	10	33
Administrative (56)	205	11	13	181	27	6	4	17
Agriculture (11)	2	0	0	2	2	0	0	2
Construction (23)	3	1	2	0	2	1	1	0
Educational (61)	165	18	17	130	65	11	10	44
Entertainment (71)	27	17	0	10	23	16	0	7
Financial Services (52)	642	44	177	421	277	33	136	108
Healthcare (62)	234	51	38	145	141	31	25	85
Information (51)	1,496	36	34	1,426	95	13	17	65
Management (55)	4	0	2	2	1	0	0	1
Manufacturing (31-33)	525	18	43	464	235	11	10	214
Mining (21)	22	1	12	9	17	0	11	6
Other Services (81)	263	12	2	249	28	8	2	18
Professional (54)	347	27	11	309	146	14	6	126
<b>Public (92)</b>	<b>50,315</b>	<b>19</b>	<b>49,596</b>	<b>700</b>	<b>303</b>	<b>6</b>	<b>241</b>	<b>56</b>
Real Estate (53)	14	2	1	11	10	1	1	8
Retail (44-45)	523	99	30	394	164	95	21	48
Trade (42)	14	10	1	3	6	4	0	2
Transportation (48-49)	44	2	9	33	22	2	6	14
Utilities (22)	73	1	2	70	10	0	0	10
Unknown	24,504	144	1	24,359	325	141	1	183
<b>TOTAL</b>	<b>79,790</b>	<b>694</b>	<b>50,081</b>	<b>29,015</b>	<b>2,122</b>	<b>573</b>	<b>502</b>	<b>1,047</b>

“The top three industries affected are the same as previous years: **Public**, Information, and Financial Services.”

*Verizon 2015 Data Breach Investigations Report*

# RISK = IMPACT \* PROBABILITY

..... **Figure 19. Probability of a data breach involving a minimum of 10,000 and a maximum of 100,000 records** .....



Ponemon Institute, "2017 Cost of Data Breach Study: Global Overview" (June 2017)

## Non-monetary costs

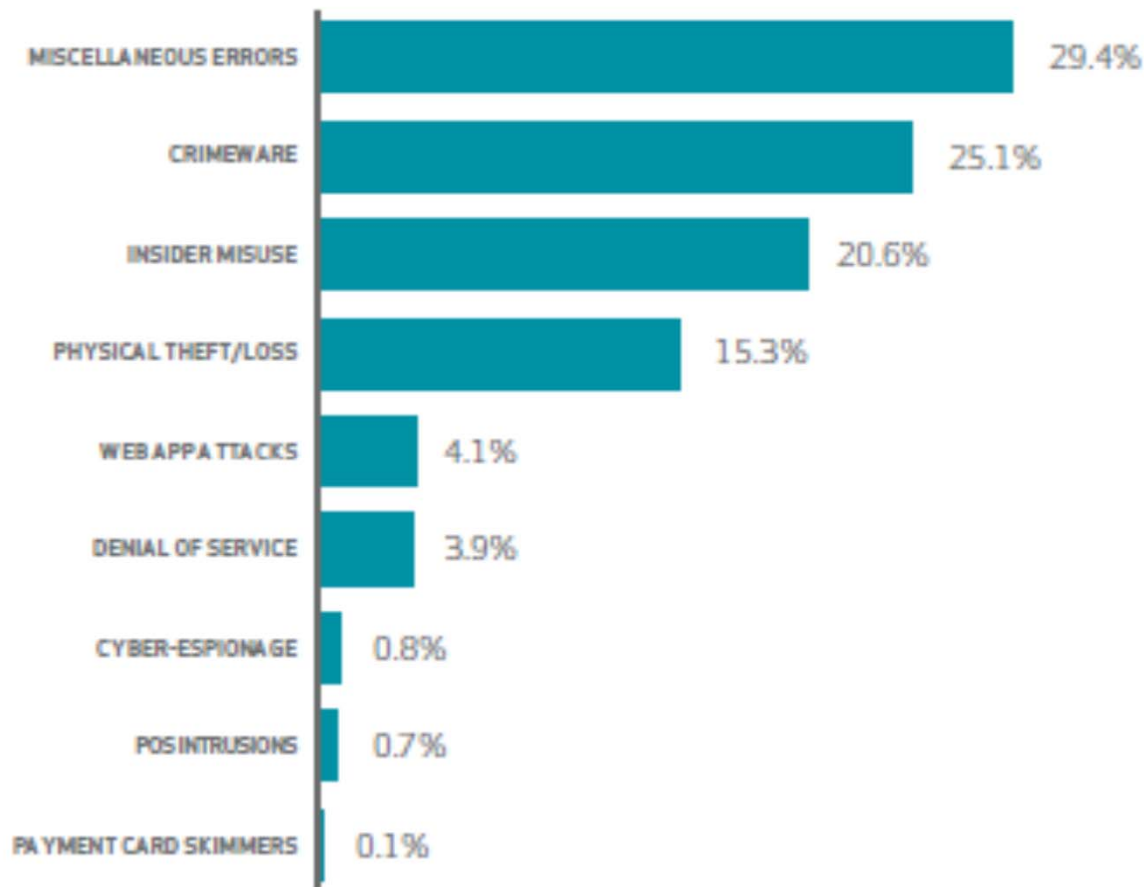
---

### Result?

- Reputational loss
- Loss of trust in data repositories
- Potential disruption in business
- Loss of resident confidence in elected officials.

## II. WHAT DOES IT LOOK LIKE?

# Most Data Breaches are Human Error

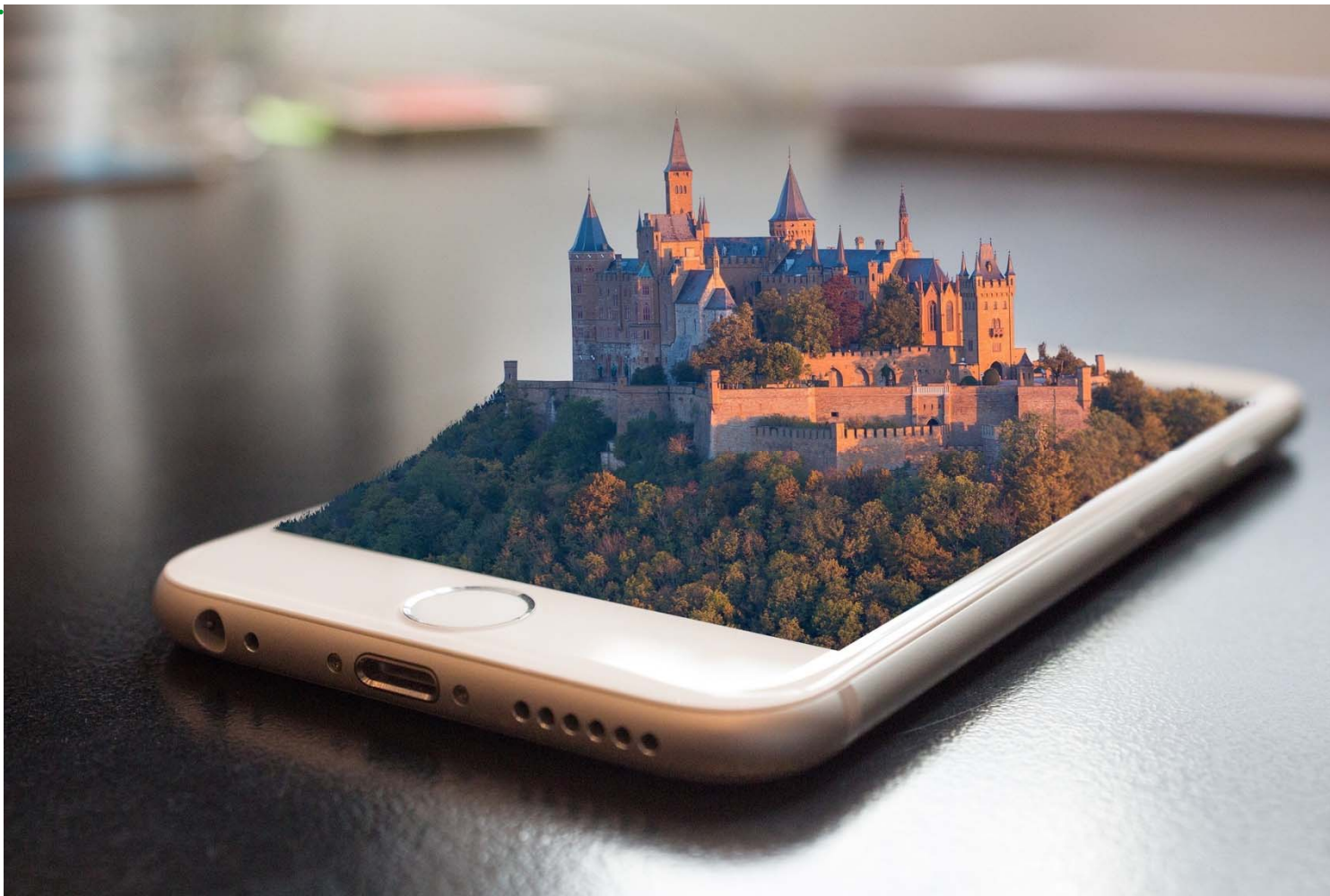


“[T]he common denominator across the top four patterns—accounting for nearly 90% of all incidents—is **people.**”

- Verizon 2015 Data Breach Investigations Report

It doesn't matter how high you build  
the castle walls...

**BALCH**  
& BINGHAM LLP



ALABAMA | FLORIDA | GEORGIA | MISSISSIPPI | WASHINGTON DC

# Phishing Email



From: IT Dept [mailto: [it@mun!cipalityal.gov](mailto:it@mun!cipalityal.gov)]

Sent: Friday, July 14, 2017 1:57pm

To: Password Check Required Immediately

Subject: Confirm your Credentials

Email address – “1” instead of “l”

Immediate action needed

To All Employees:

As part of ongoing efforts to maintain security requirements, we have updated our password policy and we need everyone to check their password immediately to ensure that its meets our minimum security requirements.

Please click here to do that: Instructed to click on a link

Check Password Hover (w/o clicking) over the link. Does it take you to the site the email indicates?

Thank you for your help in advance.

John Q. Doe, City IT Manager [or Jane P. Doe, Consultant]

# Passwords

- Bad Passwords:
  - 123456
  - Password
  - 111111
  - Admin
  - Iloveyou
  - 123123
  - Qwerty
- Good password: “I love Alabama Football and Dreamland BBQ for life!” → **IIAFaDB4I!**
- Two factor authentication



## III. WHAT DO WE DO?

# BEFORE A Breach

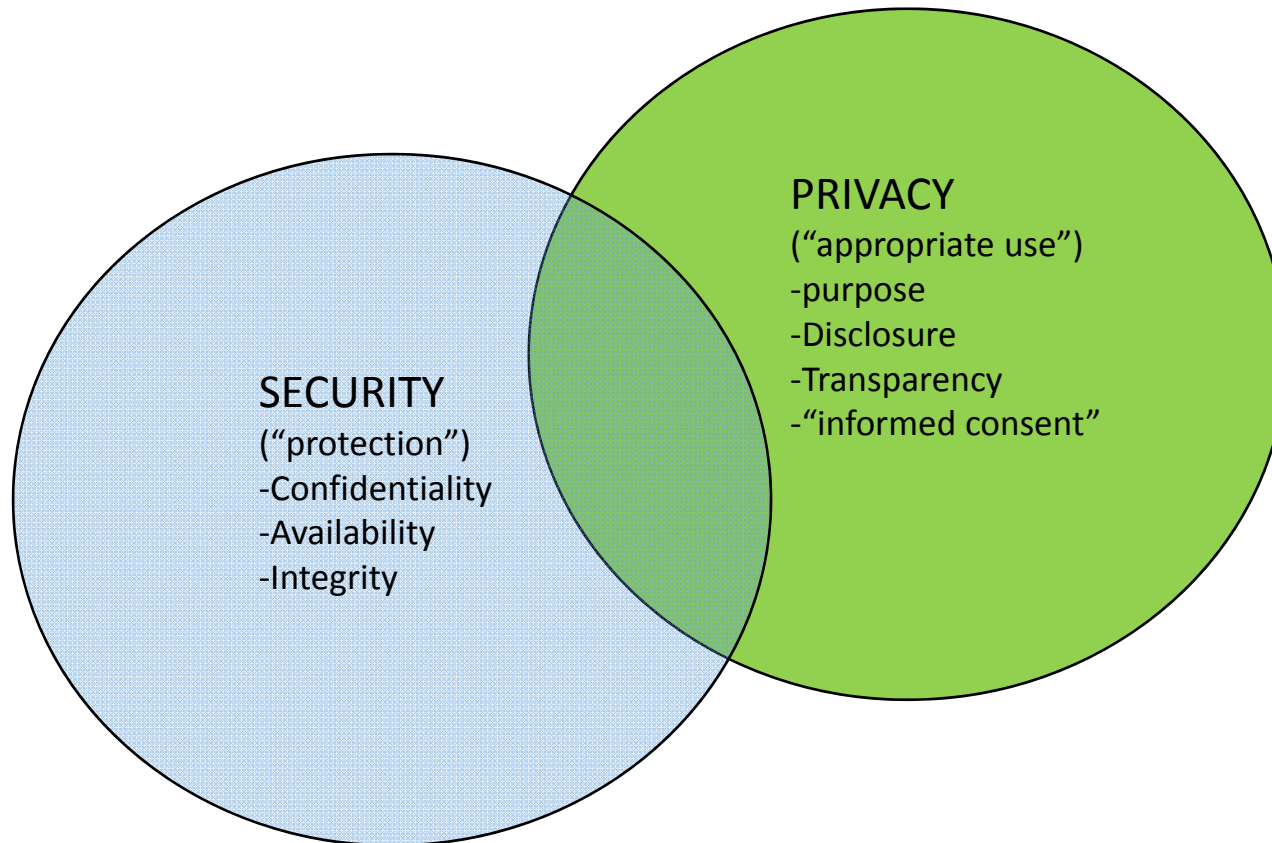
- Create an Incident Response team
- Create a plan
- Create/review policies and procedures
- Train employees on policies and procedures as well as on good info gov practices (passwords, phishing, etc.)
- Maintain a good relationship with law enforcement.
- Consider cyber insurance; review your policies
- Vendor management

## AFTER a suspected breach

- HOPEFULLY – Activate your incident response team and implement your plan. If not ... some rules of thumb:
- Engage legal counsel (attorney/client work product, privilege) – can be in-house or outside
- Investigate immediately. – identify source and compromised data, restore system integrity
- Control the story = communicate internally and externally, as promptly and accurately as possible. “art of the statement”. Review for notification obligations (no AL law, but contract/insurance?)

## IV. WHAT ABOUT PRIVACY?

Remember – it's not just about security,  
but PRIVACY too



# Privacy – It's not just about Breaches



- Businesses often focus on security without enough attention to privacy. Think FTC “unfair and deceptive”, state AGs.
- Big data, predictive analytics and the Internet of Things introduce innovative possibilities, but may also present privacy issues.
- Review policies and procedures, definitions of PII, sensitive data, how and for what purposes they collect, use, share, retain and protect such data.
- Ensure consistency between practices and policies, procedures and external representations.
- **Consider whether new or anticipated practices warrant policy changes, customer consent, or customer notifications.**

Questions?

**BALCH**  
& BINGHAM LLP

Thank You

**Balch & Bingham LLP**

**Brandon N. Robinson**

**205.226.3427 or**

**[bnrobinson@balch.com](mailto:bnrobinson@balch.com)**

ALABAMA | FLORIDA | GEORGIA | MISSISSIPPI | WASHINGTON DC

# Digital Engagement During Uncertain Times

## Part II - *Legal Pitfalls of Social Media*

**Marcus Chatterton**  
Balch & Bingham LLP  
 @mrchatterton



---

# Benefits of Social Media Engagement

- Community Engagement
- Established Communication Channel
- News Source
- PR Enhancement

---

# Pitfalls of Social Media Engagement

- Opportunity for Negative PR
  - Maintenance Obligation
  - First Amendment Concerns
  - Obligation to Maintain Records
  - Brand Erosion
  - Copycats / False Agents
-

---

# Social Media Policies

*Control expectations; follow the policy*

- Set expectations
- Avoid future disputes

---

# Social Media Policies

## *Common Elements*

- Employee Access
- Account Management / Ownership
- Acceptable Use / Employee conduct
- Content Creation / Preservation / Moderation
- Security
- Managing Interactions and Communications

---

# Public Interaction

- Official Channel of Communication
  - Agency concerns
- Emergency Notifications
  - Is there a duty?
- Event Promotion
  - Caution: Secure rights of publicity

---

# Social Media in Litigation

- Discoverable
- Admissible

Social media is fair game in litigation...

---

# Social Media in Litigation

## *Gardendale Case Study*

- Sought to form independent school district
- Subject to judicial oversight
- Social media evidence was central to the opinion

# Questions