SECURITY BREACHES

MUNICIPAL & STATE AGENCIES

PRESENTED

RON P MENARD

SECURITY BREACH 101

Goal and Intent Today

- Share specific info RE: Security Breaches – Local and State Governments
- Dial up a Dialog that you can leverage with Stake Holders RE: Security Awareness
- Supply Insight – Address Breach Mitigation – Funding, Personnel and Vendor Selection
- Provide Tips for pairing Municipal Security Systems with Vendor Solutions
- Road Map Breach Mitigation – 10 steps to Managing and Event & Recovery

SECURITY BREACH 101

Data Breaches – How relevant to Municipal Government

1. Private vs. Public Sector Targets – Reports indicate that the type's of attacks and hacker payloads have different scopes. What constitutes a Breach?
2. Reports indicate Hackers applying more sophisticated attacks against Private Sector vs. Public Sector.
3. FBI Surveys show Social and Economic factors often driving Private Sector attacks.

SECURITY BREACH 101

Data Breaches – How relevant to Municipal Government

Types of Breaches Reported

1. MS-ISAC report Local / State attacks indicate opportunistic in nature. Often causing havoc with systems without significant loss of data or monetary extortion.
2. Hacktivism and Doxing are two methods being used to impact social and economic factors. Public Sector has had minimal financial impact in comparison to Private Sector targets.

SECURITY BREACH 101

Data Breaches – Private Sector Impact

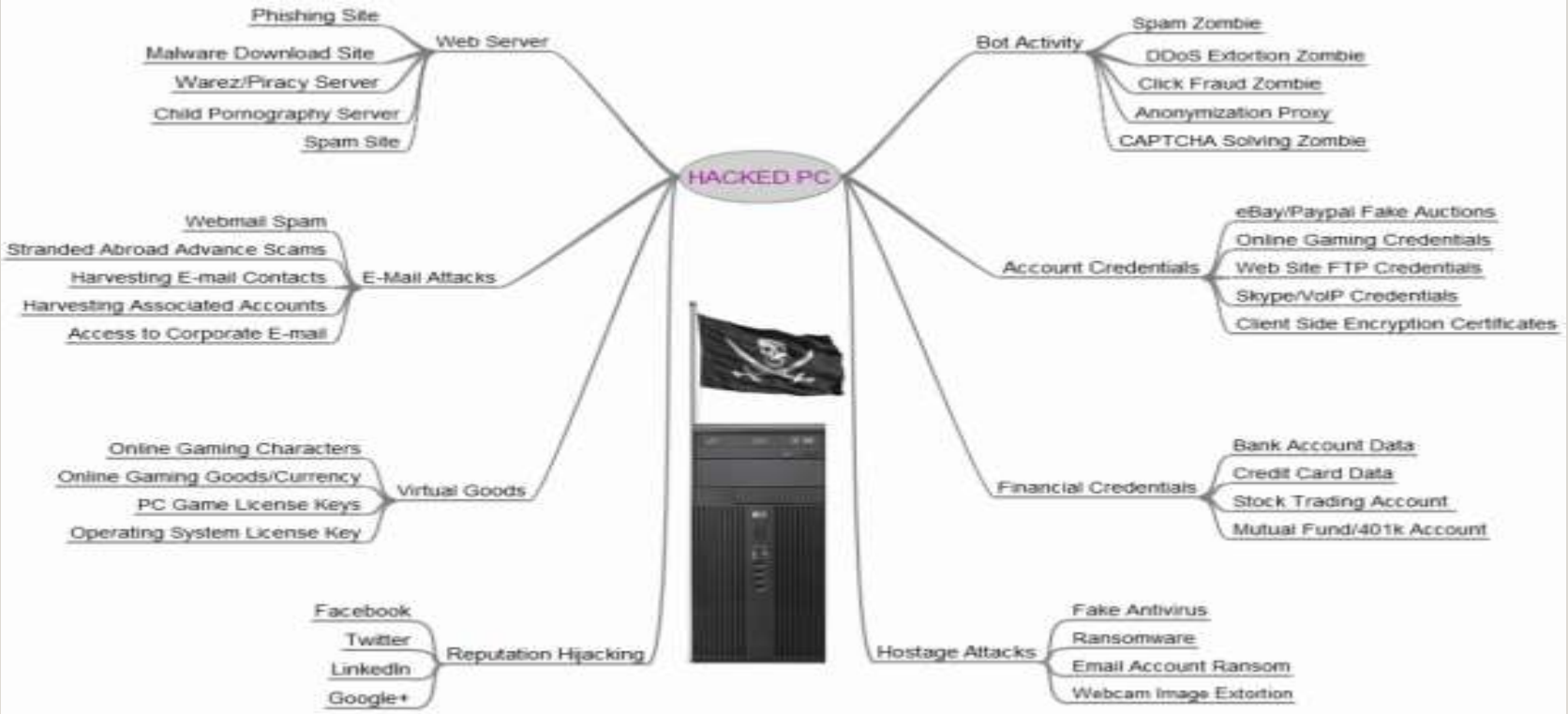
1. Open Sources Reports indicate that in 2014 over 904 million records were accessed illegally within first 6 months
2. Increase of 95% over 2013 during the same timeframe.
3. FBI indicated of those companies breached 90% attacks could have been prevented via Personnel training on “Transaction and Access” Policies, Security Patching.
4. Broader Review – Suggest 37% breaches – inside component, 12% lost mobile devices, 29% Failure Internal Controls and Common Best Practices.

DATA BREACH 101

Survey Says – Houston we have Disconnect

- Confidence in a cohesive plan in place – Executives vs. IT Staff 60/29%
- Level of support to fund and adopt Mitigation – In Place?
- Believe the policies, controls and systems in place are adequate?
- Adoption of Solutions driven by tunnel vision – Security Collaboration?
- Cloud based solution providers – Integration of Existing Security?
- Solutions incorporate End Point Security – Encryption Levels?

HACKTIVIST BENEFITS



SECURITY BREACH 101

Suggested Best Practices

- Low Hanging Fruit – Password protection, Encryption, manage Mobile device Security.
- Isolation of Online Systems – Dedicated a computer for Online Transactions.
- Separate Computers / Networks – Further Isolate online transactions.
- Ensure Firewalls are installed both local and at the Gateway.
- Ensure Patch Management /End Point Software – Aligned with Solution Provider requirements

SECURITY BREACH 101

Additional Requirements

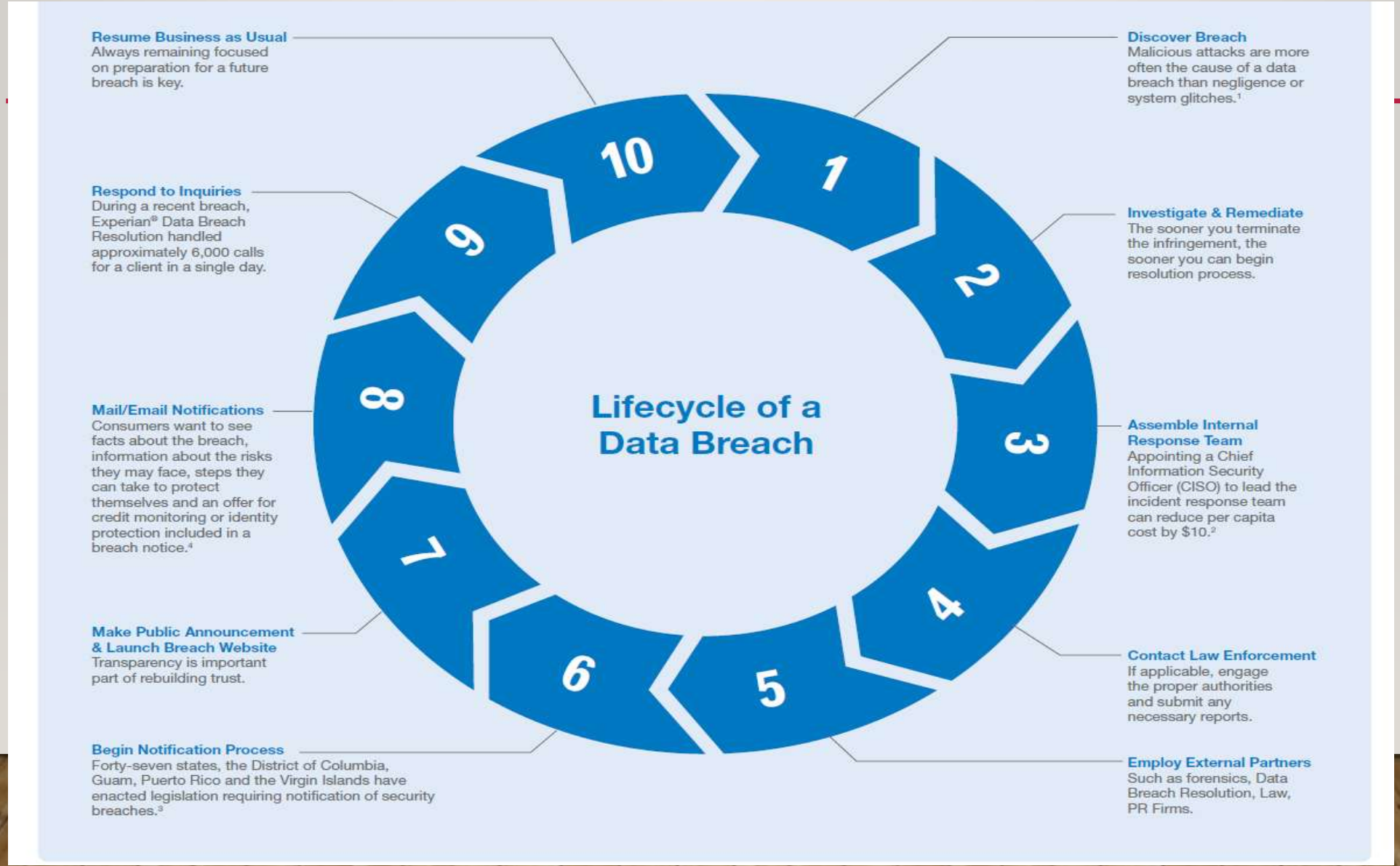
- Transaction Policies – Ensuring Users follow approved guidelines for Int/Ext Transactions
- Umbrella Policies – Educate and Train personnel on approved procedures dealing with constituents data, account access methods and escalation notifications
- Reporting and Alerts – Leverage system automation – ID vendor solutions and Notification options
- Develop a security / compliance Team – In House stake holders Engage vendors manage alerts
- Develop Breach Mitigation Response plans – Test them annually.

SECURITY BREACH 101

Reviewing a 360 Degree Breach Mitigation

1. From Discovery to Business as Usual
2. Remediation, Notifications, Containment, LLEO, Team Deployment – Partner Interaction,
3. Let’s review a Breach life cycle.

DATA BREACH 101



DATA BREACH 101

- So what can we do: Begin a dialog with stake holders.
- Look critically at department, vendor and existing policies
- Engage security vendors - look at security audits – Leverage the MA State Community Compact – Shared state resources to meet this universal need.
- Review new solutions collaboratively with Technology Departments.
- Join the MS-ISAC – ITS FREE! Offers wide range of services including monitoring
- Document your initiatives and due diligence. As a public official we are tasked with the care of Constituent data and funds. Documentation is your “Get out of Jail Free Card”

DATA BREACH 101

Reference Materials and Documents

- **Additional Resources:**
- Online Trust Alliance 2015 Data Breach and Response Plan: http://bit.ly/1DKegRV
- Experian Data Breach Response Guide: http://bit.ly/1J90MSX
- Better Business Bureau: What to Do if Your Customer Data is Stolen: http://go.bbb.org/1MsG42S
- Best Practices for Victim Response & Reporting of Cyber Incidents: http://1.usa.gov/1HM2jsx
- https://www.youtube.com/watch?v=Srh_TV_J144
- http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

DATA BREACH 101

Reference Materials and Documents

- https://www.pcicomplianceguide.org/pci-faqs-2/
- https://msisac.cisecurity.org/
- https://msisac.cisecurity.org/newsletters/2016-03.cfm
- https://www.fas.org/sgp/crs/secrecy/RL34120.pdf
- http://www.marketingresearch.org/legal-article/massachusetts-data-security-obligations-and-breach-notification-requirements