Security, Privacy and Governance in the Age of Innovation

Galina Datskovsky, Ph.D., CRM
CEO, Vaporstream
Technology in the 21st Century

• **Drivers**: Competitive differentiation and broader reach, customer satisfaction, employee efficiency

• IDC’s Third platform of Technology has led the way to innovation
  • Cloud, Social, Mobility and Big Data

• The Nexus of Forces or Platform has fueled innovation such as
  - Internet of Things (IoT)
  - Advanced Analytics
  - A.I.
  - Mobile Apps
  - New Collaborative Tools
Planning for New Technology

• The evolution of technology is:
  - Continual
  - Aggressive
  - Disruptive

• The impact to IT and Governance policies must be evaluated, planned for and executed with precision.

• Any new technology must be evaluated in light of the following areas and employees trained appropriately:
  - Compliance requirements and policy enforcement
  - Security considerations/possible gaps
  - Impact to cybersecurity and response plans
Don’t be a Nay-Sayer

- Employees are driven by convenience and efficiency to get their jobs completed successfully
- Policies that disallow use of a technology tend NOT to work
- Reality:
  - People do it anyway
  - It is the responsibility of the organization to protect corporate data and find a safe and compliant way to do business
Cloud is Here to Stay & Feeds Innovation

• By 2018, more than 60% of enterprises will have at least half of their infrastructure on cloud-based platforms. 

• By 2019, more than four-fifths (86 percent) of workloads will be processed by cloud data centers; 14 percent will be processed by traditional data centers.

1. Source: Forbes Tech Roundup Jan 2015
2. Source: Cisco Global Cloud Index: Forecast and Methodology, 2014–2019
Enablement of the Internet of Things

• IoT connects cars, homes, wearables, industrial machinery and everyday objects to the cloud

• IDC estimates that global spending on IoT devices and services will rise from $656 billion in 2014 to $1.7 trillion in 2020.

• The world of IoT brings much excitement and expected efficiency however there are many considerations:
  • Data management
  • Data analytics
  • Information governance and compliance
  • Security and incident prevention
  • Privacy
The Social Connection Fuels New Innovation

- **Facebook:** >1.6 billion active monthly users; 1.6 billion mobile active users
- **Twitter:** >3.5 million monthly active users, 500 million tweets per day and 200 billion tweets per year
- **LinkedIn:** >414 million members in over 200 countries with executives from all Fortune 500 companies
- **Instagram:** >400 million active monthly users, 40 billion photos shared to date, an average of 80 million photos shared per day
- **WhatsApp:** >1 billion active monthly users, 1 million daily registrants, 30 billion messages sent daily
- **YouTube:** >1 billion users, 4.6 billion videos viewed per day, over 400 hours of video uploaded per minute
Big Data and Analytics

• In information technology, **big data** is a collection of data sets so large and complex that it becomes difficult to process using on-hand database management tools or traditional data processing applications. The challenges include capture, curation, storage, search, sharing, analysis, and visualization. (Wikipedia)

• **Dark Data** is like that furniture you have in that Dark Cupboard. Dark data is the cute name given to all that data an organization gathers that is not part of their day to day operations. It is old stuff, stuff that turned up in the mail that you kept, ‘just in case’. It is data that you didn’t erase, because “it might come in handy some time”. (Gartner Blog by Andrew White)

• According to IDC, the big data technology and services market is expected to grow at a compound annual growth rate (CAGR) of 23.1% between 2014-2019 with annual spending reaching $48.6 billion in 2019.
BYOD is associated with the top security concerns for most corporate CISOs.

By the end of 2016 four in ten organizations will rely exclusively on a policy of Bring Your Own Device (BYOD)\(^1\)

By 2020 85% of businesses will have some kind of BYOD or Corporate Owned Privately Enabled (COPE) programs in place\(^1\)

\(^1\text{http://www.gartner.com/newsroom/id/2466615}\)
The Next Wave of Enterprise Communication: Text and Chat

• Text is quickly becoming the “new email”

• Text messages have a **98% open rate** and a **45% response rate**, while email has only a **20% open rate** and a **6% response rate**\(^2\)

• Worldwide in 2015, over **8.3 trillion text messages were sent.**
  - That's almost **23 billion messages per day**
  - Almost **16 million messages per minute**\(^1\)

• Instant messaging still beats this number, at **50 billion per day, or 1.5 trillion per month**\(^3\)

---

\(^1\) 2015 Portio Research.
\(^2\) 2015 Mobile Marketing Watch
Lessons Learned: Over 30 Yrs. of Email

• Exposure by emails that are copied, taken out of context, and propagated intentionally and unintentionally. Hitting SEND=Loss of content control
• Emails frequently represent business records or evidence that is discoverable
• Emails that are left unencrypted can be exploited in unintended ways
• Recent Example: The Sony Pictures data breach and recent outbreak of Ransomware

Other email data leak examples are documented in Forester Report studies sited in:
The Expectation of Privacy

- HIPAA, FINRA
- General Data Protection Regulation (GDPR)
  - Adopted by the European Parliament April 2016
  - Extends the scope of the EU data protection law to all foreign companies processing data of EU residents
  - The regulation does not apply to the processing of “personal data” for national security activities or law enforcement
  - “personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer’s IP address”
- So-called right to be forgotten was replaced by a more limited right to erasure
Secure Mobile Messaging

- **Security & Privacy.** Enables secure, encrypted, confidential communications. Prohibits screen shots, obscures images and separates message and header information to further protect information.

- **Sender Control.** Keeps the sender in control at all times, prohibiting recipients from copying, printing, forwarding or saving messages to prevent misuse and unwanted propagation.

- **Ephemerality.** Removes messages from devices and servers after a predefined period of time, minimizing concerns surrounding lost or stolen devices.

- **Compliance.** Retains a copy of messages in client designated repository of records to ensure compliance.

- **Deployment.** Enterprise deployment via MDM, helps containerize deployment and enforce enterprise security and governance policies.
Using a Proven and Familiar Framework

<table>
<thead>
<tr>
<th>Generally Accepted Recordkeeping Principles®</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accountability</td>
</tr>
<tr>
<td>Integrity</td>
</tr>
<tr>
<td>Protection</td>
</tr>
<tr>
<td>Compliance</td>
</tr>
<tr>
<td>Availability</td>
</tr>
<tr>
<td>Retention</td>
</tr>
<tr>
<td>Disposition</td>
</tr>
<tr>
<td>Transparency</td>
</tr>
</tbody>
</table>

About ARMA International and the Generally Accepted Recordkeeping Principles®
ARMA International (www.arma.org) is a not-for-profit professional association and the authority on information governance. Formed in 1955, ARMA International is the oldest and largest association for the information management profession with a current international membership of more than 10,000. It provides education, publications, and information on the efficient maintenance, retrieval, and preservation of vital information created in public and private organizations in all sectors of the economy. It also publishes Information Management magazine, and the Generally Accepted Recordkeeping Principles®. More information about the Principles can be found at www.arma.org/principles. Replace this with a link to the arma principles page.
Principle of Protection

• Mobile Device Management Solution
  - Ensure corporate data and apps reside separately from private ones
  - Ensure encryption is enabled on the corporate side
    - Enables ability to wipe corporate data if phone is lost or stolen
  - Ensure phone and/or corporate apps are pin code protected
    - Enable handing phone to a third party without compromising corporate apps or data

• Secure Mobile Messaging
  - Encrypt in transit and on device
  - Prevent propagation: control forwarding, store and print even on devices beyond organization’s control
  - Capture message and retain per policy in a single secure repository, not on devices
Principle of Compliance

• Ensure communications are captured: healthcare, financial services, etc.

• Legal and regulatory requirements FRCP, SOX and HIPAA

• Audit messages to comply with internal policies and legal considerations
Principle of Availability

- Enabling mobile communications provides timely, efficient communications that can be instant, accurate and secure

- Information is made available just in time for many urgent and confidential conversations
Principle of Retention and Disposition

• Mobile communications should be retained on mobile devices only as long as they are useful for active communications

• A retained secure copy should be kept under the organization’s control for legal, regulatory, fiscal, operational, and historical requirements and disposed once organization retention policies have been fulfilled
People, Process and Technology

• Policies for device management and control
  - Define data ownership - for example: data in the employee’s BYOD or COPE managed device belongs to the company and can be cleared at corporate discretion

• Policies for message retention
  - Define how email and mobile messages are retained for corporate use and regulatory purposes

• Policies for application usage
  - Define which applications should be used for business email, mobile messaging and chat

• Audit for compliance
Questions

Galina Datskovsky, Ph.D., CRM
CEO, Vaporstream
www.Vaporstream.com

If you have any remaining questions after the webinar, please send them to Nicole@vaporstream.com