DELL LEADERSHIP

30,000+ customers

50+ million identities

1 billion consumers

20 of the TOP 20 Manufacturing

19 of the TOP 20 Consumer product, Financial institutions, Healthcare institutions, Transportation

18 of the TOP 20 Telecom

16 of the TOP 20 Energy

10 of the TOP 10 Technology

13 of the 15 Executive Departments of U.S. Government

International Government Organizations

97%

94%

1 billion consumers
RSA Archer customers

- **1,500+** GRC deployments
- **48** of the Fortune 50
- **92** of the Fortune 100

Customers in every marketplace:
- Public Sector
  - **100+** US Government Agencies
  - **18** States
  - **16** Cities/Municipalities
  - Foreign Government Deployments
- **10** biggest U.S. banks
- Healthcare
- Insurance
- Energy
- Transportation
- Technology
- Retail

Global operations

- **~$1B revenue**
- **2,700+** employees
- **1,000+** technology partners
- **30+** years of cybersecurity expertise
- **15+** years of risk expertise

EMC/RSA A Dell Technologies Subsidiary

RSA Archer Analyst Recognition

A Leader in:
- Gartner Magic Quadrant for Operational Risk Management Solutions (2017)
- Gartner Magic Quadrant for IT Risk Management Solutions (2017)
- Gartner Magic Quadrant for IT Vendor Risk Management (2017)
- The Forrester Wave™: Governance, Risk, And Compliance Platforms (2017)
TODAY’S PUBLIC SECTOR

• Security, Privacy and Risk Management are top priorities
• Government organizations moving from a reactive, restrictive approach that inhibits modernization and enhanced capabilities to one that’s resilient, adaptable and agile
• Increasing demand for consistent and accurate information accessible by employees and the public they serve
TODAY’S PUBLIC SECTOR

• Accelerated government adoption and expanded use of mobile, cloud, IOT, AI, Blockchain and other technologies to support operations and public access

• IT consolidation, centralization and digital modernization initiatives can be challenging, complex and introduce risks

• Government organizations are leveraging 3rd party organizations with greater frequency
THE ATTACK SURFACE IS EXPANDING AND WITH IT PRIVACY RISKS!

• Individual computers (government, personal)
• Mobile devices
• Virtualization
• Cloud computing
• Internet of Things (IoT)
ADVERSARIES COME IN MANY FLAVORS

NATION STATE ACTORS

Nation-states

CRIMINALS

Petty criminals
Organized crime

NON-STATE ACTORS

Insiders
Cyber-terrorists / Hacktivists
“It erased everything stored on 3,262 of the company’s 6,797 personal computers and 837 of its 1,555 servers. The studio was reduced to using fax machines, communicating through posted messages, and paying its 7,000 employees with paper checks.” (2014)

- Fortune, July 2015
GOVERNMENT – NATION-STATE?

OPM Hack: Government Finally Starts Notifying 21.5 Million Victims

by JAMES ENG
WANNACRY – GLOBAL IMPACT

Friday, 12 May 2017 – 230,000+ Computers In Over 150 Countries Were Infected
Why 'WannaCry' Malware Caused Chaos for National Health Service in U.K.
Atlanta officials reveal worsening effects of cyber attack

Reuters Staff

(Reuters) - The Atlanta cyber attack has had a more serious impact on the city's ability to deliver basic services than previously understood, a city official said at a public meeting on Wednesday, as she proposed an additional $9.5 million to help pay for recovery costs.

Ransomware strikes CDOT for second time even as agency still recovering from first SamSam attack

By TAMARA CHUANG | tchuang@denverpost.com | The Denver Post

PUBLISHED: March 1, 2018 at 7:36 pm  | UPDATED: March 1, 2018 at 8:57 pm
An 11-year-old hacked a replica of Florida’s voting system in 10 minutes

A hackathon highlights the real threats malicious hackers pose to our democracy.

By Jennie Neufeld | @jenni neufeld | jennie.neufeld@vox.com | Aug 13, 2018, 3:30pm EDT
Canadian banks warn data breach may have affected 90,000 customers

Cybercriminals may have the stolen data of nearly 90,000 customers from two of Canada’s largest banks in what appears to be the first significant cyberattack on a Canadian financial institution.

Bank of Montreal and Canadian Imperial Bank of Commerce (CIBC) both announced Monday they had each been contacted by fraudster’s claiming to have stolen personal and financial information of a limited number of the bank’s customers.
Canada Revenue Agency logs 2,338 privacy breaches in just under 2 years

By Monique Scotti  National Online Journalist, Politics  Global News

The personal, confidential information of over 80,000 individual Canadians held by the Canada Revenue Agency may have been accessed without authorization over the last 21 months, according to government documents made public last week.
The Marriott hack exposed the passport numbers of more than 5 million people

The hack exposed guest information dating back to 2014.

By Gaby Del Valle | @gabydvj | gaby.delvalle@voxmedia.com | Updated Jan 4, 2019, 11:02am EST
VERIZON DATA BREACH SURVEY

• In 2017 public sector organizations became the #1 target for cyber attacks

• Public Sector organizations were 3rd most data breach victims

• 21,000+ breaches were reported among 92 public sector organizations surveyed – 239 were confirmed

• **41% contained stolen PII data**
**Digital Risk Transformation**

**Digital Risk** is the risk associated with transforming traditional analogue and antiquated products, processes and services to new digital platforms using digital technology.

---

**Enablement Risks**
- Data privacy, e.g. Big Data, data warehouses, etc.
- Implementation issues with new technologies
- Third party providers (tech partners, consultants, operations support)

**Optimization Risks**
- Adoption rates and organizational change management
- Interruption or downtime due to transition
- Third party providers (partners, consultants)

**Transformation Risks**
- Poor public adoption
- Opportunity costs if wrong decision is made
- High profile, reputational risks
**Digital Risk Management (DRM)** facilitates the management of risks associated with digital business components such as cloud, mobile, social, big data, third party technology providers, operational technology (OT) and Internet of Things (IoT).

<table>
<thead>
<tr>
<th>Enterprise Risk</th>
<th>Strategic</th>
<th>Financial</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal Mgmt.</td>
<td>Performance</td>
<td>Risk</td>
</tr>
<tr>
<td>Corp Social Responsibility</td>
<td>Financial Controls</td>
<td>Fraud</td>
</tr>
<tr>
<td>Environmental</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **How are traditional risk disciplines addressing digital business initiatives?**
- **How does IoT impact the risk profile of the organization?**
- **What is the cloud strategy for the business and associated risks?**

**Is the organization making the right strategic decisions in digitizing the business?**

---

**Digital Risk Transformation**

**IT systems**

**Operational Technology**

**IoT**

**Cloud**

(e.g., SaaS, Mobile, Social)

**Physical Operations**

**Consumer Applications**

**Business Applications**

---

**How are traditional risk disciplines addressing OT?**

---

**DIGITAL RISK TRANSFORMATION**

**Is the organization making the right strategic decisions in digitizing the business?**
RISKS APPEAR ACROSS THE GOVERNMENT ENTERPRISE

- Environmental damage
- Information Security breaches
- Supply Chain Interruption
- Internal and external fraud
- Operations interruption
- Unknown, unidentified risks
- Regulatory violations, fines and sanctions
- Inefficient processes & technologies
- Poor internal controls & governance
- Human errors
- Privacy Breach
- Poor Public Service
- Litigation
- 3rd party non-performance, error or fraud
- Employee Health & Welfare
- Negative Public Reputation
- Poor Public Service
- Efficent processes & technologies
- Employee Health & Welfare
MANAGING PRIVACY RISK IS BOTH A MISSION AND A TECHNOLOGY CHALLENGE

Magnitude of risk increasing

Velocity of risk increasing

Risk Complexity increasing
Primary objective:
Detect and respond to the threat before a breach occurs but if a breach does occur, you need to know the details and exact impact.

Primary objective:
Know where data is in the enterprise and who has access and implement controls in data processing activities.

Primary objective:
Establish a risk assessment process to ensure controls are appropriately designed and implemented.

Primary objective:
Establish a compliance program to ensure controls are effective and operational.
KEY PRIVACY PROGRAM INGREDIENTS

Breach Response
- Streamline incident response and breach management processes
- Implement infrastructure that provides visibility across the enterprise
- Ensure forensic capabilities are in place to investigate properly
- Ensure logging capabilities are aligned with response needs
- Address data obfuscation and encryption controls
- Test and refine IR processes and procedures on a regular basis

Data Governance
- Maintain an accurate and complete inventory of processing activities and information assets and related 3rd Parties
- Implement risk based access and authorization
- Ensure governance processes validate access levels
- Manage notice and consent activities and retention schedules linked to the information inventory
- Assess processing activities in accordance with prevailing requirements

Risk Assessment
- Maintain assessment scopes for sensitive data environments
- Perform privacy impact assessments (PIA) and data protection impact assessments (DPIA) when required
- Identify operating conditions that may necessitate a DPIA
- Implement consistent processes for both existing environments and new initiatives

Compliance Management
- Ensure issues are managed and tracked
- Establish policies, standards and controls
- Implement training and awareness program specific to PII handling
- Streamline control testing scoping, execution, and reporting
- Look for control overlaps with other regulatory requirements to streamline and simplify your control framework

DON’T FORGET ABOUT THIRD PARTIES…
PRIVACY AND SECURITY GO HAND IN HAND
EMBRACE A SECURITY FRAMEWORK

NIST CSF addresses standards, guidelines, and best practices

Promotes the protection of information and information systems, particularly within the critical infrastructure community.
FINAL THOUGHTS

• Public demand for enhanced, secure and continual info access is constant and growing – so are cyber threats
• Privacy-Security-Risk-Audit Teams need to collaborate and work together
• Ongoing updates to policies, procedures and controls to protect data, information access and systems
FINAL THOUGHTS

• Understand your “crown jewels” (data and systems) and how they’re managed, accessed and protected
• Encryption in transit and at rest / continual verification of privileges and access
• Build in resiliency and be prepared for the inevitable, create and update contingency plans, training employees and have system and data backups in place to minimize impact
FINAL THOUGHTS

• Implement continuous data monitoring and frequent risk management reviews and conduct “what if” scenarios
• Pay close attention to your extended ecosystem and key vendors with access to and handling data
• Privacy is everyone’s business - build a culture of awareness with employee awareness training (including leadership) to mitigate and minimize data and privacy risks – people, process and technology
QUESTIONS?

THANK YOU!

Dan Carayiannis
dan.Carayiannis@rsa.com