What You Don’t Know Can Really Hurt You...
How to Secure What Matters Most

David W. Gould
WW Sr. Director
Micro Focus Secure Content Management Solutions
Please Sit Down ....

Are creating less information this year than last?

Don’t have any initiatives relating to application modernization?

Are not concerned about information risk?

Don’t have to manage information to comply with retention laws or legal discovery?

How many of you work in places that...
Thank You....
Why Bad Guys Want Our Personal Information

- Because they can
- Monetization
- Political advantage
**Data Breaches 2019**

**Blur**
January 2, 2019: It didn’t take long for the first major breach announcement of 2019. Blur announced a breach after an unsecured server exposed a file containing 2.4 million user names, email addresses, password hints, IP addresses, and encrypted passwords. The password management company urged their users to change their Blur login credentials and enable two-factor authentication.

**DiscountMugs.com**
January 4, 2019: Online retailer of custom mugs and apparel, DiscountMugs.com was hacked for a four-month period in the latter half of 2018. The company announced that it had discovered malicious card skimming code placed on its payment website. Hackers were able to steal full payment card details (number, security code, and expiration date), names, addresses, phone numbers, email addresses, and postal codes.

**Oklahoma Department of Securities**
January 17, 2019: Millions of government files, including records pertinent to FBI investigations, were left unprotected on an open storage server belonging to the Oklahoma Department of Securities (ODS). The oldest records exposed dated back to 1986 and ranged from personal data to login credentials and internal communication records.

**BlackRock Inc.**
January 22, 2019: As many as 20,000 financial advisers had their information leaked by the world’s largest asset manager, BlackRock. The company posted confidential sales documents related to advisers who work with BlackRock’s iShares unit. Names, emails, and assets managed by advisers were among the information exposed.

**Rubrik**
January 29, 2019: IT security and cloud data management provider, Rubrik exposed a massive database containing customer information including names, contact information, and other details related to corporate accounts. The data leak was discovered on an unprotected Amazon Elasticsearch server that didn’t require a password.
Data Breaches 2019

Houzz
February 1, 2019: Popular home improvement startup, Houzz announced a data breach affecting users of the platform. In a statement, the company said that information such as names, city, state, country, profile description, username, and hashed passwords were taken by an unauthorized third party.

Dow Jones
March 1, 2019: A database containing 2,418,862 identity records on government officials and politicians from every country in the world was leaked online from a Dow Jones watchlist. The watchlist is compiled from publicly available information on prominent individuals who have the ability to embezzle money, accept bribes, or launder funds.

Federal Emergency Management Agency (FEMA)
March 22, 2019: Survivors who sought shelter assistance after hurricanes Maria and Irma, as well as California wildfires, have had their PII exposed in a FEMA privacy incident. About 2.5 million disaster victims had information like names and addresses, bank account information and birth dates shared with a contractor, leaving them unprotected.

Zoll Medical
March 20, 2019: The personal information of 277,319 patients has been exposed by a Zoll Medical data breach. The medical device manufacturer headquartered in Chelmsford, MA announced that data from emails was leaked during a server migration, including names, addresses, dates of birth, and medical information. Some patients also has their SSN exposed.

Facebook
March 21, 2019: Facebook has admitted that since 2012 it has not properly secured the passwords of as many as 600 million users. These passwords were stored in plain text and able to be accessed by more than 20,000 of the company’s employees. If you use Facebook, change your password.
Pay Fines
Litigation
Operational Cost
Reputation
Data privacy and compliance regulations over time:

- **1995**:
  - Victoria Electronic Records Standards

- **1999**:
  - Gramm-Leach-Bliley Act

- **2000**:
  - MoREQ
  - Health Insurance Portability & Accountability Act
  - ISO 15489

- **2001**:
  - Sarbanes-Oxley Act
  - ISO 27001

- **2002**:
  - Dept of Defence 5015.2
  - Open Government
  - Foreign Intelligence Surveillance Act Amendment

- **2003**:
  - Federal Rules of Civil Procedure (Amend)

- **2006**:
  - PIPEDA Act (Canada)
  - SARBANES-OXLEY ACT
  - ISO 9001
  - Dodd-Frank Wall Street Reform Act
  - Foreign Intelligence Surveillance Act Amendment

- **2008**:
  - ISO 27001

- **2010**:
  - Dodd-Frank Wall Street Reform Act
  - Foreign Intelligence Surveillance Act Amendment

- **2015**:
  - NOTIFIABLE DATA BREACHES SCHEME AUSTRALIA PRIVACY ACT
  - EU-US DATA PRIVACY SHIELD
  - Protection of Personal Information (Japan)
  - NARA US GOVT CAPSTONE
  - General Data Protection Regulation

- **2016**:
  - California Privacy Act

- **2018**:
  - Australia Privacy Scheme
  - China Cyber Security Law

- **2019**:
  - Australian Privacy Scheme
Who does it affect?
State of California residents

California Citizens Rights
1. Knowing personal information is being collected.
2. Knowing if that information is sold or disclosed and to whom.
3. Access to what is collected (within 45 days).
4. Request not to have personal data collected.
5. Request to have personal data deleted.
6. Equal service, even if exercising privacy rights.

Corporate Obligations
1. Disclose what specific personal information is collected.
2. Inform consumers the purpose and use of the data collected.
3. Upon request from the consumer, disclose and deliver personal information collected at no charge.*
4. Retain any personal information collected.
5. Manage and maintain all personal information collected.
6. Inform consumers of data breaches.

Businesses with...
$25M+ Annual Gross Revenue.
Personal information bought, sold or shared on more than 50k of annual revenues derived from selling personal information.

When does it become law?
JULY 1, 2020
AB 375 (ALSO KNOWN AS)

Fines & Sanctions
Penalties of up to $7,500 per record in intentional violation of any provision of the CCPA
Privacy Regulations Around The World

Robust
- China
- Argentina
- Finland
- Iceland
- Japan
- New Zealand
- Morocco
- Hungary

Heavy
- USA
- EU
- UK
- Turkey
- Australia
- Canada

Moderate
- Russia
- Brazil
- Saudi Arabia
- South Africa
- Egypt
- Chile

Limited
- Zimbabwe
- India
- Khazakstan
- Madagascar
- Indonesia
- Thailand
- Pakistan

Source: DLA Piper
## Differences between GDPR and CCPA*

<table>
<thead>
<tr>
<th></th>
<th>GDPR</th>
<th>CCPA</th>
<th>Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scope</strong></td>
<td>EU personal data processed</td>
<td>California residents’ personal data collected</td>
<td>Narrower</td>
</tr>
<tr>
<td><strong>Right to Access</strong></td>
<td>Right to access all EU personal data processed</td>
<td>Right to access California personal data collected in last 12 months</td>
<td>Broader</td>
</tr>
<tr>
<td><strong>Right to Portability</strong></td>
<td>Must export and import certain EU personal data in user-friendly format</td>
<td>All access requests must be exported in user-friendly format. No import requirement.</td>
<td>Similar</td>
</tr>
<tr>
<td><strong>Right to Correction</strong></td>
<td>Right to correct errors in EU personal data processed</td>
<td>Not included in CCPA</td>
<td>Absent</td>
</tr>
<tr>
<td><strong>Right to Stop Processing</strong></td>
<td>Right to withdraw consent or otherwise stop processing of EU personal data</td>
<td>Right to opt-out of selling personal data only; must include opt-out link on website</td>
<td>Narrower</td>
</tr>
<tr>
<td><strong>Right to Stop Automated Decision Making</strong></td>
<td>Right to require a human to make decisions that have a legal effect</td>
<td>Not included in CCPA</td>
<td>Absent</td>
</tr>
<tr>
<td><strong>Right to Stop Third Party Transfer</strong></td>
<td>Right to withdraw consent for data transfers</td>
<td>Right to opt-out of selling personal data to third parties</td>
<td>Broader</td>
</tr>
<tr>
<td><strong>Right to Erasure</strong></td>
<td>Right to erase EU personal data, under certain conditions</td>
<td>Right to erase personal data collected, under certain conditions</td>
<td>Similar</td>
</tr>
<tr>
<td><strong>Right to Equal Services and Price</strong></td>
<td>At most, implicitly required</td>
<td>Explicitly required</td>
<td></td>
</tr>
<tr>
<td><strong>Private Right of Action Damages</strong></td>
<td>No floor or ceiling</td>
<td>Floor of $100 and ceiling of $750 per consumer per incident</td>
<td></td>
</tr>
<tr>
<td><strong>Regulator Enforcement Penalties</strong></td>
<td>Ceiling of 4% of global annual revenues</td>
<td>No ceiling -- $7,500 per violation</td>
<td></td>
</tr>
</tbody>
</table>

*Source: PWC
Right to Portability
Right to Portability
• How does AT&T let Verizon know?
• Where does Verizon look?
  • How does Verizon transport the data to AT&T?
• When does Verizon store the data?
• Who tells the consumer?
Information risk encompasses all challenges resulting from the need to control and protect information assets
Managing Information Risk – What We See In The Global Market

Transitioning from nice to do to must do

Managing only what is known to discovering what is not known

Information security now has a lock-down mentality

Managing for information risk is now an imperative
The Pitfalls of Today’s Disjointed Solutions

Disconnected

No Scalability

Manual Process
The Complexity of Global Compliance Mandates

- Consumer Rights
- Legal Interpretation
- Worldwide Impact
- Business Readiness

Upstate vs. Downstate

- Safe Value Creation
- Loss of Trust
Simple Truths About Managing For Information Risk

You cannot/don’t need to protect all data

You cannot protect or delete data that you don’t understand

Most effective way to protect data is to delete it once eligible

Data can be only deleted defensibly by using policy
Four Key Questions

What Do I Need to Protect?

How do I Find It?

Once I find it, how do I manage it?

How long do I keep it?
How can managing for Information Risk be good for business?

- Enhance compliance profile
- Manage content as part of a lifecycle
- Reduce operating cost
- Optimize content for productivity
How can managing for Information Risk be good for business?

Reputation
Data Management -- Users and Value

- Creators
- Consumers
- Custodians
- Controllers

Information Management

- Value from Data
- Value from Operations

Value from Operations

- Predictive Analytics
- Data Classification
- Operational Reporting, Diagnostics
- Telemetry
- System Monitoring
the Game of LIFE
INFORMATION

the Game of LIFE

MANAGEMENT

CYCLE
Information Lifecycle Management Defined

A comprehensive approach to managing the flow of an information system's data and associated metadata from creation and initial storage to the time when it becomes obsolete and is deleted.
The ILM Lifecycle

Information changes over time

Goal: Allow for policy driven long-term management

ILM is not just about compliance; it's about productivity

- Identify
- Classify
- Manage
- Retain
- Consign
Holistic Data Governance – Solution Architecture

Unstructured Data Repositories

File Analysis/Reporting
- Identify
- Analyze
- Categorize
- Curate

Structured Data Repositories

Structured Data Management
- App Retirement
- Data extraction
- Data Masking

Content Management
- Lifecycle Management
- Intelligent Archiving

Manage in-Place
- Policy-based
- Workload Sensitive

Apply policy to manage in place

Declare content and records

Identify PII, PCI, PHI

Manage in-Place

Auto classify
- Policy
- Security
- Redaction
- Encryption
- Authorized access
- Reporting
- Audit logs

Defensibly Dispose

Valid Data

Legacy Data and ROT

Connect

Extract

Redundant, Obsolete & Trivial (ROT)

Declare content and records

Manage in-Place

Defensibly Dispose

Connect

Extract
DLCM & Security platform

Data Repositories
- Applications
- Files
- Email
- Messaging
- Document Management
- SharePoint
- Social Media
- Web Content
- Data Warehouses

Find

Classify

Data Encryption

Govern
- Apply Retention rules
- Compliance, Legal Hold & Audit

Analyse

Action

Record Repository

Data Archive

Eligible Records

Read

Declare

Apply

Store
What are the key stages in DLCM and how are we handling them?

**Data initiation**
- Audio / visual & alphanumeric
- +1000 different file types
- End point device generation
- In what silo?
- What language & volume?

**Data connection & classification**
- Find the silos
- Connect to source
- Cross-refer to other client data
- Cleanse the ROT
- Structured or Unstructured
- ? How sensitive

**Policy Execution**
- Policy can be law / regulation / corporate rule
- Execution engine available?
- Who can access?
- Automated policy execution?
- Audit trail of policy enforcement?

**Storage**
- Records for business use?
- Archive – tiered storage
- Cost of storage
- Back up & recovery
- Cloud migration – or ROT?

**Defensible Deletion**
- Retention Schedule Statutory compliance
- Data Privacy “ purpose limitation”
- Litigation defence
- M & A enablement – keep / destroy
Marketing drafts the FY18 budget and go to market and saves it on the department share. A draft is saved to the Marketing OneDrive for Business folder. VP of Marketing reviews FY18 plans, recommends changes. Add 3+ versions. Versions are sent via email to Field Marketing and Digital Marketing to update plans. The Product Marketing lead updates changes and saves a copy to the department file share. The Marketing team makes final changes. Converts the document to PDF and posts to the FY18 Executive Leadership folder. FY18 passes and this folder is stagnant.
Protect what matters – structured data

1. Legacy application storing customer accounts and receivables uses SQL as its backend database, writes out data blobs.

2. Data analyst inside the business imports slices of data into a Hadoop data lake store.

3. Data is split into separate projects and analyzed by finance and marketing teams.

4. Finance and Marketing Executives receive a couple different reports off the data.

COST CONTAINMENT
IT MODERNIZATION
Identify redundant data and remediate for compliance archiving and/or app retirement

RISK DETECTION
Discover, sample & review PI/ PII & sensitive data

ANONYMIZE
Anonymize and tokenize personal data at the source in the data lake and what is stored in Secure file repository

COMPLIANCE
Apply policy to critical data sets and manage that in the secure repository

LIFECYCLE MANAGEMENT
Manage lifecycle of final reports in data repository as a record.
+ Dispose data based on policy ensuring compliance.
Compliance & governance have many similarities

Capture
- Regulated data
- Sensitive data
- Data with no value
- Unneeded apps

Classify
- Move/back up
- Dispose (apps or data)
- Encrypt
- Quarantine
- Redact
- Inform/notify
- Monitor/supervise

Control
- Protect data
- Lower risk
- Lower cost
- Streamline processes

Manage information in accordance with internal & external mandates
What Is Your Role In All This?

Connect policy to action
Focus on all challenges
Agent for change
The Micro Focus Solution: Secure Content Management
IT Modernization
Helping customers on their IT modernization, business optimization journey and shift to cloud - while supporting new deployment and consumption models.

Data Preservation
Visibility across both structured and unstructured sources, to identify and secure high-value assets and sensitive information.

Information Risk
Applying policy to high-value assets, sensitive data, and official records – while managing that data, in Content Manager, or in-place in Office365.

Lifecycle Management
Extending analytics and reporting to assist customers with traditional content management tasks, but evolving the user experience to meet expanding workload challenges for data discovery, preservation, retention and data disposition.
Secure Content Management: Areas of differentiation

Key Stakeholders

- CISO
- CIO
- CCO/DPO

Records/Compliance
LOB/Department

Problems we help solve

- PII detection
- Auto-classification
- Masking
- Encryption
- ROT detection

RISK REDUCTION

BUSINESS OPTIMIZATION

DATA GOVERNANCE

- Data Access Gov.
- Records Management
- Long term retention

DATA PRESERVATION

- Lifecycle Mgmt
- Application retirement
- Personal Data Mgmt

Servicing the following industries

- Legacy Data Clean-up
- Data Preservation
- Cost containment

Pan Enterprise with Data Governance Concerns
Secure What Matters Most!

Thank you!

David W. Gould
WW Sr. Director
Micro Focus
Secure Content Management Solutions
david.wil.gould@microfocus.com