Worldwide Legal and Regulatory Update regarding Cybersecurity and Privacy

- The zExchange, New Era Software
- November 22, 2016

Steven Ringelberg

Atlas Cybersecurity

Ringelberg & Associates

Washington, DC

steven@stevenringelberg.com

+1 616 227 6403

AGENDA

- About me
- Criminal Offenses
- US Update
- European Update
- Rest of the World

About Me

Founder, Director, Atlas Cybersecurity, 2015 - Present
Security Consulting with Correlog and Sycnsort among others.

Founder, Member. Ringelberg & Assocaites, 2015 Present
Data Breach Preparation and Response.

Previous

Chief Operating Officer and General Counsel
Vanguard Integrity Professionals, 2007 - 2015

Chief Administrative Officer
Exstream Software (now part of HP), 2006 -2007

Director and General Counsel
Honkworm, 2001 - 2006

Director and General Counsel
eTechnologies, 1998 - 2001

European Counsel
Baan Software (now part of Infor), 1996 - 1997

Corporate Attorney
Microsoft EMEA, 1992 – 1996.

- Education
  - J.D., New York University School of Law
  - B.A, Oberlin College

- Bar Admissions
  - The State of New York
  - The District of Columbia

YOU NEED PERMISSION

- Tuesday, September 27, 2016
- City of Hamburg, Germany
- What's App
- Facebook
- No sharing of data without explicit permission from the individual human being

You can go to jail if you . . .

Share user ids and passwords with another person?

United States v. Nosal. July 2016

The Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030.

The CFAA imposes criminal penalties on whoever "knowingly and with intent to defraud, *accesses a protected computer without authorization*, *or exceeds authorized access*, and by means of such conduct furthers the intended fraud and obtains anything of value . . . ." *Id.* § 1030(a)(4) (emphasis added).

Point One: If you are "authorized" to access a computer, you are authorized to access the "entire" system.

Point Two: You can only but "authorized" by the entity that owns the "computer." Not simply by somone who has themselves been "authorized."

You can go to jail if you . . .

Use a stolen password to access the Houston Astros
July 2016

46 Months in Jail.
2 years probation
$280,000 fine.

St. Louis Cardinal's scouting executive.

You can go to jail if you . . .

Disable 90% of Citibank's network by erasing configurations of just 10 routers. July 2016

21 months in Jail.

Terminated IT department employee.

THE 4TH AMENDMENT TO THE US CONSTITUTION

- The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized

MICROSOFT CASE: JULY 2016

- Data Center in Europe.
- MSFT received US government request for access to customer data.
- MSFT refused.
- Court ruled that the request did not have to be complied with in respect to data stored outside of the territory of the United States.

CISA

Cybersecurity Information Sharing Act of 2015. December 2015

1. DHS is in “charge.”
2. Limited Antitrust Exemptions.
3. Voluntary
4. Disclosure of “threat information”
5. Delete any personally identifiable information.

OMB CIRCULAR A-130. JULY 28, 2016

- **Applies to All Federal Agencies, and all private sector companies that process or store data for Federal Agencies.**
- **Three main goals:**
  - Real Time Knowledge of the Environment.
  - Proactive Risk Management.
  - Shared Responsibility.

GDPR – EUROPEAN GENERAL DATA PRIVACY REGULATION

- Will replace the EU Data Privacy Directive and the various national implementations.
- Applies to anyone that collects data of EU citizens: regardless of where the server with the data resides.
- No further action required by member states to implement.
- Stricter Security Requirements.
- More “guidance” on appropriate security measures.
- Reduction in regulatory overlap.
- Codifies the “right to be forgotten”

GDPR ARTICLE 32

- **Delineates the GDPR's "security of processing" standards.**
- **"Controllers" and "processors" are required to "implement appropriate technical and organizational measures" taking into account "the state of the art and the costs of implementation" and "the nature, scope, context, and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural presons."**
- **GDPR provides specific suggestions for what kinds of security actions might be considered "appropriate to the risk," including:**
  - The pseudonymisation and encryption of personal data.
  - The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
  - The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
  - A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

GDPR ARTICLE 34. BREACH NOTIFICATION

- **If the controller has determined that the personal data breach "is likely to result in a high risk to the rights and freedoms of individuals," it must also communicate information regarding the personal data breach to the affected data subjects "without undue delay."**
- **Exceptions to Notification:**
  - (1) the controller has "implemented appropriate technical and organizational protection measures" that "render the data unintelligible to any person who is not authorized to access it, such as encryption"; (2) the controller takes actions subsequent to the personal data breach to "ensure that the high risk for the rights and freedoms of data subjects" is unlikely to materialize; or (3) when notification to each data subject would "involve disproportionate effort," in which case alternative communication measures may be used.
- **Assuming the controller has notified the appropriate supervisory authority of a personal data breach, its discretion to notify data subjects is limited by the DPA's ability, under Article 34(4), to require notification or conversely to determine it is unnecessary under the circumstances.**

GDPR ARTICLE 79

- **Fines for violation of the GDPR may go up to 4% of worldwide turnover. HUGE!**

EU US “PRIVACY SHIELD”

- To replace EU US “safe harbor” agreement that was found to be defective by the EU Court of Justice.
- Similar to old “Safe Harbor” but the US government had to agree to more restrictions on its ability to access data on EU citizens.

BRAZIL

- Law “12.735” was passed in 2012 concerning “cyber crime,” but as of yet, no government agency has been tasked with enforcing it.

PCI-DSS 3.2

- Payment Card Industry – Data Security Standards
- Why comply? Lower credit card processing rates.
- PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data. PCI DSS applies to all entities involved in payment card processing — including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD).

PCI-DSS 3.2

- **High-level overview of the 12 PCI DSS Requirements**
- 1. Install and maintain a firewall configuration to protect card holder data.
- 2. Do not use vendor-supplied defaults for system passwords and other security parameters.
- 3. Protect stored cardholder data.
- 4. Encrypt transmission of cardholder data across open, public networks.

PCI-DSS 3.2

- **High-level overview of the 12 PCI DSS Requirements**
- 5. Use and regularly update antivirus software.
- 6. Develop and maintain secure systems and applications.
- 7. Restrict access to cardholder data by business need-to-know.
- 8. Assign a unique ID to each person with computer access.

PCI-DSS 3.2

- **High-level overview of the 12 PCI DSS Requirements**
- 9. Restrict physical access to cardholder data.
- 10. Track and monitor all access to network resources and cardholder data.
- 11. Regularly test security systems and processes.
- 12. Maintain a policy that addresses information security.

PCI DSS 3.2 CHANGES

- SSC has announced that the PCI DSS has reached a point of maturity. Consequently, they no longer plan to release major revisions to the standard on a three-year cycle, but will instead issue releases more often with fewer changes between them..

PCI DSS 3.2 CHANGES

- The extension of the SSL/early TLS dates to June 30, 2018 will be reinforced.
- Multi-factor authentication requirements for accessing the cardholder data environment, which were already in place for remote access scenarios, will be extended to include local access.
- There will be some new Appendices in the DSS, including one dedicated to SSL/early TLS and one that brings DESV requirements into the DSS.
- Rules around displaying card numbers will be modified to accommodate an upcoming change to card number standards.

PCI DSS 3.2 CHANGES

- **PCI SSC Data Security Standards**
  - https://www.pcisecuritystandards.org/security_standards/index.php
  - https://www.pcisecuritystandards.org/pci_security/

Thank you!

Steven@stevenringelberg.com

616 227 6503

Spike Ringelberg. 1998 – 2016