Province of British Columbia
21st Annual Privacy and Security Conference

Privacy Implications Post-Cyber Breach
IBM X-Force Incident Response and Intelligence Services (IRIS)

Hussain Virani
Managing Consultant
X-Force IRIS

Over 15 years experience in Information Technology and Security

Experience across multiple industries – both in the public and private sector.

Certifications:
B.Tech.
Computer Forensics
CISSP
Overview

• Problem statement
• Current legislation in Canada and abroad
• Best practices from the viewpoint of incident response
• Case study
• Questions
• Breaches are on the rise, along with increasing levels of personally identifiable information (PII) being exposed
• PII is one arguably of the toughest data types encountered during a cybersecurity incident
• Privacy legislation is consistently encountered during incident response
• Fines and sanctions are growing
• Human error remains the leading cause of data breaches
Current Legislation

Canada:
- Personal Information Protection and Electronic Documents Act (PIPEDA, Federal)
- Personal Information Protection Act (PIPA, British Columbia)

Europe:
- General Data Protection Regulation (GDPR)

United States of America:
- California Customer Protection Act (CCPA)
Best Practices

• Best Practice #1:
  – Always be mindful of privacy and data governance laws
    » Canada: PIPEDA, PIPA
    » EU: GDPR
    » US: CCPA

• Best Practice #2:
  – Classify and identify your organization’s data before, rather than during, or after a breach
Best Practices

• Best Practice #3:
  – Rehearse your incident response plans, crisis management strategy, and playbooks specifically for PII incidents

• Best Practice #4:
  – Conduct regular live-fire tabletops and cybersecurity simulations focused on data privacy
Case Study: Ashley Madison

- Adult online dating site, geared towards infidelity
- Widespread breach of PII 2015 of use records
- PII included names, e-mail addresses, passwords, and other identifiable data entries
- The breach data was connected to a search interface available to the public
- Data was posted online and remains to this day as part of breach archives
Case Study: Ashley Madison

Overall impact:

- Damage to affected Users’ reputation
- Damage to organizations the User represents
- Public embarrassment of Self
- Loss of employment
- Divorce proceedings and legal action
Conclusions

• Breaches happen, get used to it
• The frequency of breaches is growing
• It’s not about your password anymore
• Breaches can, in some cases, ruin lives
• Cyber hygiene matters, be careful online
• Use common sense, the Internet is not anonymous
Thank you

Follow us on:

ibm.com/security
securityintelligence.com
ibm.com/security/community
xforce.ibmcloud.com
@ibmsecurity
youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2020. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM’s current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

IBM Security