Legal Education Society of Alberta

62124.00

Alberta Legal Technology Conference

Edmonton, Alberta

Chair

Keith Wilson
Wilson Law Office
St. Albert, Alberta

Faculty

Elizabeth Aspinall
Law Society of Alberta
Calgary, Alberta

Richard Ferguson
Lynass Ferguson & Shocter
Edmonton, Alberta

Maura Grossman
University of Waterloo
Waterloo, Ontario

Andrew Koeman
Mincher Koeman LLP
Calgary, Alberta

Jay Krushell
Witten LLP
Edmonton, Alberta

Nathan Lee
YellowWood IT
Calgary, Alberta

Rex Shoyama
Thomson Reuters
Toronto, Ontario

Helen Voudouris
LexisNexis
Toronto, Ontario

LESA LIBRARY

LEGAL EDUCATION SOCIETY OF ALBERTA

These materials are produced by the Legal Education Society of Alberta (LESA) as part of its mandate in the field of continuing education. The information in the materials is provided for educational or informational purposes only. The information is not intended to provide legal advice and should not be relied upon in that respect. The material presented may be incorporated into the working knowledge of the reader but its use is predicated upon the professional judgment of the user that the material is correct and is appropriate in the circumstances of a particular use.

The information in these materials is believed to be reliable; however, LESA does not guarantee the quality, accuracy, or completeness of the information provided. These materials are provided as a reference point only and should not be relied upon as being inclusive of the law. LESA is not responsible for any direct, indirect, special, incidental or consequential damage or any other damages whatsoever and howsoever caused, arising out of or in connection with the reliance upon the information provided in these materials.

This publication may contain reproductions of the Statutes of Alberta and Alberta Regulations, which are reproduced in this publication under license from the Province of Alberta.

© Alberta Queen's Printer, 2019, in the Statutes of Alberta and Alberta Regulations.

The official Statutes and Regulations should be consulted for all purposes of interpreting and applying the law.

© 2019. Legal Education Society of Alberta. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise without the prior permission of the Legal Education Society of Alberta.

LESA LIBRARY

ISBN-10: 1-55093-722-7
ISBN-13: 978-1-55093-722-0

Cybersecurity Preparedness Guide

Alberta Legal Technology Conference

LESA LIBRARY

Prepared by:
Nathan Lee
YellowWood IT
Calgary, Alberta

Edmonton, Alberta – May 23-24, 2019

2019

Cybersecurity Preparedness Guide

LESA LIBRARY

CYBERSECURITY READINESS IT'S EVERYONE'S JOB

NATHAN LEE

YELLOWWOOD IT | www.yellowwoodit.ca

Table of Contents

LESA LIBRARY

CYBERSECURITY AWARENESS

71% OF DATA BREACHES HAPPEN TO BUSINESSES WITH LESS THAN 100 EMPLOYEES

"Gartner Says By 2018, 25 percent of corporate data traffic will flow directly from mobile devices to the cloud, bypassing enterprise security controls"

Smaller businesses are easy targets

Small and midsize businesses (SMBs) spend less on cybersecurity than larger organizations. Cybercriminals often target SMBs because they have a lot of personally identifiable information that can be used for identity theft, tax fraud and other financial crimes.

SMBs collect customer, employee and vendor names, addresses, social security numbers, dates of birth, driver's licenses and insurance information. This information is everything a criminal needs to commit identity theft and other cybercrimes.

Data breaches are expensive and can damage a company's reputation.

Legal, IT, breach notification and identity monitoring expenses can add up quickly.

After a data breach, customers often leave a business due to lack of trust, and negative publicity keeps newer customers from utilizing the services of the business.

60% OF SMALL BUSINESSES GO OUT OF BUSINESS AFTER A DATA BREACH

Data breaches cause owners and employees emotional stress and anxiety.

Employees are your weakest security link

95% OF DATA BREACHES ARE CAUSED BY EMPLOYEE MISTAKES.

An IBM study found that 95% of data breaches are caused by employee mistakes. These mistakes include falling victim to a phishing or ransomware attack, losing a laptop or smartphone, or sending sensitive information to the wrong recipient. Employees need security awareness training to help prevent mistakes that can lead to data breaches.

LESA LIBRARY

5 TIPS TO CYBERSECURITY

Although criminals are targeting SMBs, employing best practices can help protect your company against cyberattacks and data breaches. The following are best practices that you can take to minimize the chance of data breaches.

1 Secure Passwords

Passwords are the key to networks, customer information, online banking and social media. Password best practices include:

- **Use strong passwords.**

  Make the password at least 8 characters long. The longer the better. Longer passwords are harder for thieves to crack.

  Consider using passphrases. When possible, use a phrase such as “I went to Lincoln Middle School in 2004” and use the initial of each word like this: “Iw2LMSi#2004”.

  Include numbers, capital letters and symbols.

  Don’t use dictionary words. If it’s in the dictionary, there is a chance someone will guess it. There’s even software that criminals use that can guess words used in dictionaries.

- **Change passwords.** Passwords should be changed every 60 to 90 days.
- **Don’t post it in plain sight**. This might seem obvious, but studies have found that a lot of people post their password on their monitor with a sticky note.
- **Consider using a password manager**. Programs or Web services let you create a different very strong password for each of your accounts, but you only have to remember the one password to access the program or secure site that stores your passwords for you.
- **Consider using multi-factor authentication**. Set up multi-factor authentication that requires a code that is displayed on your phone. This way hackers cannot access an account without having physical access to your phone.

2 Encrypt Data

Lost laptops, smartphones and USB drives continue to cause data breaches. Many businesses don’t realize how much sensitive information is on mobile devices. Sensitive information could be in emails, spreadsheets, documents, PDF files and scanned images.

The best way to protect sensitive information is to use encryption. Under PIPEDA regulations, encryption prevents significant harm, which includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property. This means if a mobile device is lost or stolen and the data is encrypted, then the incident would not result in a reportable breach. Customers and affected individuals would not need to be notified.

LESA LIBRARY