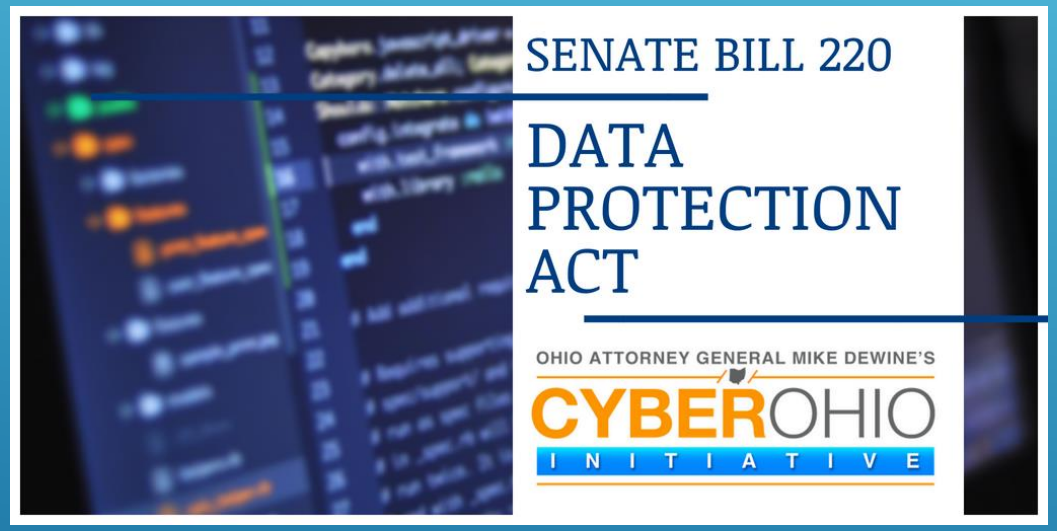
THE DATA PROTECTION ACT

Ohio Senate Bill 220 (2018)



Allen Perk
CEO - XLN SYSTEMS
Over 40 years in Information Technology
16 Year Member of NFIB

YOUR PRESENTER

Allen Perk, CEO with XLN SYSTEMS

- BS Degree in Systems Analysis from Miami University
- 40 years in Information Technology
- Founded XLN SYSTEMS in 1991
- Small Business advocate since 2003

I sit on the following Boards;

- Franklin University Center for Public Safety and CyberSecurity Awareness
- CyberOhio – Ohio Attorney General
- National Federation of Independent Business (Ohio)

PLEASE NOTE ……

This presentation is for your information and may contain comments not authorized by the authors of SB220, Franklin University, CyberOhio or the NFIB.

However, comments are attributable to XLN SYSTEMS

Like many presentations, you should follow up with your own research to determine what is and what is not pertinent for you and your business.

HIGH PROFILE CYBER BREACHES

IRS	2019	-	Face Time issue with 3rd Party Listening without your Knowledge
Ashley Madison	2015	-	4 Million user personal information
Columbus Library	2018	-	4000 Employees W-4 Information including SSN
Equifax	2017	-	148 Million accounts with Financial information exposed
Exactis	2018	-	340 Million ….. Email, physical address, phone, personal information including children's names
FaceBook	2018	-	87 Million member records leaked
Have I Been Pwned	2018	-	772 Million Email Accounts with 21 Million Unique Passwords
IRS	2015	-	700,000 personal data taxpayer accounts
LinkedIN	2016	-	164 million email addresses and passwords exposed
Marriott	2018	-	500 Million …. Payment Card Info, Passport Numbers, Names, email
MyHeritage	2018	-	92 Million …. Family tree, hashed passwords, DNA & email accounts

HIGH PROFILE CYBER BREACHES

Orbitz	2018	-	880,000 Names, birthdates, payment card info
Panera Bread	2018	-	37 Million Customer Records
Saks Lord Taylor	2018	-	5 Million Credit and Debit Cards leaked
Sony	2014	-	85 million records, including Social Security numbers, health histories, banking details, and account passwords
State of Ohio	2017	-	Websites Department of Corrections, Casino Control, Governor John Kasich and First Lady Karen Kasich by I S I S
Target	2013	-	70 million customers' information compromised, 40 million credit card numbers stolen
TicketFly	2018	-	27 Million Customer & employee Data
T-Mobile	2015	-	15 million Social Security numbers
Uber	2017	-	57 Million names, email addresses, and phone numbers (Also they CONCEALED the hack for one year)
UnderArmour	2018	-	150 Million …. Usernames, email accounts and hashed passwords
Yahoo	2014	-	3 Billion passwords and security questions

CYBER SECURITY CULPRITS

- Over 61%
  - Internal to the Organization
    - On Purpose
    - Lack of Knowledge
    - By Pure Accident
- Remaining 39%
  - True Cyber Pirate Professionals
  - Bored “Do Nothings” Living in Mom & Dad’s Basement
  - Foreign Mischief Makers
  - Organized Crime

THE DATA PROTECTION ACT

- Ohio Senate Bill 220:
  - Introduced as a result of (then) Attorney General DeWine's CyberOhio Initiative
    - Launched in September, 2016
    - To promote collaborative talks on cybersecurity initiatives between industry professionals and the government
  - Provides an "Affirmative Defense" to covered entities that implement a specified cybersecurity program
  - Allow transactions recorded by blockchain technology under the Uniform Electronic Transactions Act,
  - Alter the definition of 'key employee' under the Casino Gaming Law
  - Signed into Law by the Governor - August, 2018

THE DATA PROTECTION ACT

- Legal Details
  - Applies only to tort claims (*i.e.*, negligence and invasion of privacy claims)
  - Requires the covered entity to plead an Affirmative Defense to a lawsuit
    - the business would still have the burden of establishing that its cybersecurity program reasonably conform with the chosen security framework.
  - **Does not provide a business with blanket immunity to a data breach lawsuit**
  - Does not apply to contract-based claims, such as those that could arise from a business-vendor dispute or between a business and its customers where a contractual relationship is alleged.

THE DATA PROTECTION ACT

- Provides an ***incentive*** to Government & Businesses, particularly small government agencies & Small Businesses, to ***implement*** an Industry Security Standard through voluntary action
- Does not take a "one-size-fits-all" approach
  - Focus is on the Size, Complexity and Nature of the business
- Entity must ***reasonably conform*** to the Standard
  - Original text was "Substantial Compliance"

- NIST 800-171
- NISTIR 7621 REV 1
- NIST 800-53
- FedRAMP
- HIPAA
- Gramm Leach Bliley (GLB)
- PCI

THE DATA PROTECTION ACT

- Why Small Business
  - Produce 46% of private sector output
  - Create 63% of all new jobs
  - There are 28 million of them in the United States
    - From the SBA – Small Business Administration
  - Generally, CyberSecurity is not a high priority
  - Owners wear multiple hats
  - Focused on making Payroll & getting the next Project
  - Don't know what they Don't know
  - Cyber pirates now have their eye on you

THE DATA PROTECTION ACT

- Duty to Report
  - Current Law – Ohio Revised Code 1349.19 (2006)
    - To report cyber breaches involving Ohio residents, to Ohio residents, no later than 45 days following the discovery of the incident – This is applicable to ALL COMPANIES in Ohio.
      - Exemptions are:
        - Legitimate Law Enforcement needs
        - HIPAA covered entities
        - Financial Institutions subject to Federal Law requirements
    - Those breaches that involve "personal information" 1359.19(A)(7)
        - SSN
        - Drivers License Number
        - Account/Debit/Credit card numbers
        - Employee Files

THE DATA PROTECTION ACT

- Going forward in this presentation, I will be following the **NIST 800-171** standards (due to **NIST 800-171** being the most widely used and easiest standard for compliance).
- In order to comply or conform to this **NIST 800-171** standard, one can follow these general points:
    - Perform a series of non-technical components
    - Complete several technical checks & modifications
    - Employee training
    - Develop an overall CyberSecurity Plan
    - Follow-Up with any updates or revisions to the NIST 800-171 standards

THE DATA PROTECTION ACT

Perform a Series of Non Technical Components

- Identify who has access to your confidential data
- Require individual computer accounts for each employee
- Create / Update an Employee Manual
- Install Surge Protectors & Battery Backups
- Properly dispose of old computers, storage devices, and digital files
  - Including Copy Machines & Printers
  - How are Computer Files truly deleted
- Create / Update a Response Document in case of a Cyber Incident
  - Protect => Respond => Recover

THE DATA PROTECTION ACT

Perform a Series of Non Technical Components - continued

- Use File Cabinets with a Lock & Key
- Have and utilize paper shredders
- Conduct online business more securely
  - e.g. Have only one internet facing bank account

THE DATA PROTECTION ACT

Complete Several Technical Checks & Modifications

- May or may not need a 3rd party computer engineer

- Utilize automatic patching of OS & Software
- Activate and Configure a Firewall on your internal network
  - Change the username and password from its default
- Secure your Wireless Networks
  - Set up a password, don't leave it open
  - If needed, create a 2nd (or 3rd) separate isolated network for Guests
- Use encryption when required
- Instead of Passwords, consider PassPhrases
  - 14 – 20 characters are VERY difficult to break

THE DATA PROTECTION ACT

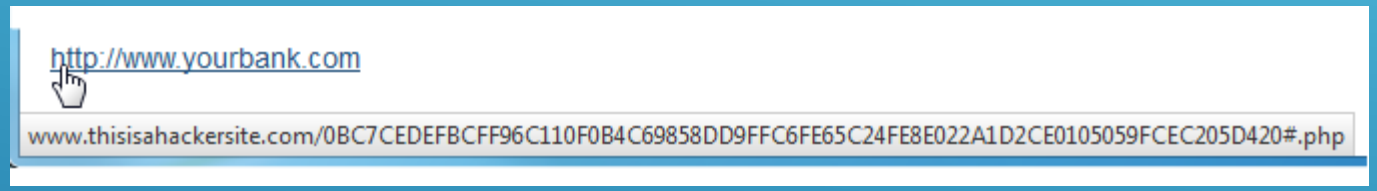
Employee Training

- Set up Web & Email filters
- Learn to spot Phishing attempts
  - Columbus Library System
  - Mouse Over
- Be careful when downloading files, music, etc.
  - Do not open or download files from an unknown sender
- Be careful NOT to give out personal or business information
- Ethics & moral principles of conduct
- Instead of Passwords, consider PassPhrases
  - 14 – 20 characters are VERY difficult to break

THE DATA PROTECTION ACT

Mouse Over ….. but DO NOT CLICK

Again, 'mouse over' the link - www.yourbank.com - Now look at the bottom left of your screen. In that location will be the web address the link will take you to IF YOU CLICK THE LINK.



If the web address looks odd or is really long or has many running characters and numbers, chances are it is NOT the Bank's web address.

THE DATA PROTECTION ACT

Follow Up

- Cyber Security is a Journey – not a Destination
- Stay up to Date
- Requires you to ***reasonably conform*** to the latest version of the chosen framework ***no later than one year after the published date*** of the latest version of said framework

THE DATA PROTECTION ACT

Benefits / Results

- Peace of Mind knowing you have addressed the risk
- Created an "Affirmative Defense" to a cause of action sounding in tort
  - A defense in which your attorney can protect you
  - So long as you have provided "Reasonable" defenses and can document such
  - NOTE: Do not confuse with the legal term "Safe Harbor"
- Built a cyber defense with only a minor investment in:
  - Time
  - Money
- Win / Win ….. for you and your customers.

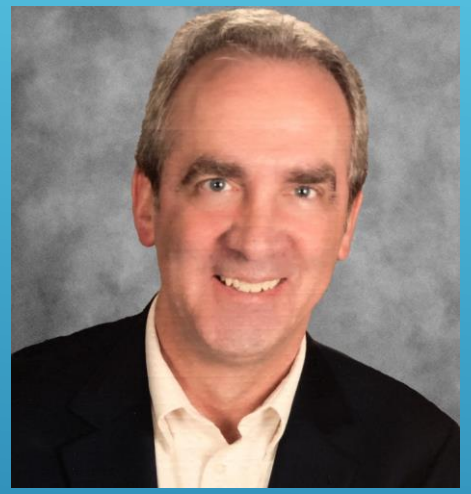
THE DATA PROTECTION ACT

Recap

- Choose an Industry Standard Cyber Security program
  - Based upon the Size, Complexity, Scope, and Resources available to the Entity
- Work the Plan
  - Much of the Plan can be done without tech guru's
  - Use experts on those tasks that require such expertise
  - Provide training to your employees
- Follow up and **Maintain your Plan**
  - Security is not a Destination, it's a Journey
- Win / Win ….. for you and your customers.

THE DATA PROTECTION ACT

- **Questions & Comments**



- Allen Perk - CEO, XLN SYSTEMS
  - Allen.Perk@XLNsystems.com
  - www.XLNsystems.com

- National Federation of Independent Business