A DAY AT THE BREACH

CYBERSECURITY & DATA PRIVACY CASES AFFECTING RETAIL & HOSPITALITY

WELCOME

Adam J. Russ

Frantz Ward LLP – Cleveland, Ohio

TRENDS IN CYBERSECURITY

Investigations by industry are **among the highest** in the Retail-Hospitality sector ***globally***

Investigations by Industry are **at the highest** in the Retail-Hospitality sector ***nationally***

Tailored phishing emails are more common

Telephone phishing emails are more common

DATA BREACHES ARE ON THE RISE

THE CHALLENGE

The technological pace is increasing

It is estimated that there will be **17.4b more devices** than the number of humans projected by 2020. [1]

By 2018, **70%** of mobile professionals will conduct all of their work on personal smart devices. [2]

1. Source: U.S. Census Bureau, International Database - http://www.census.gov/data/developers/data-sets/international-database.html/
2. Source: Gartner http://www.gartner.com/technology/topics/

ALFA International
The Global Legal Network
Local Relationships Worldwide

DATA BREACHES ARE ON THE RISE

THE CHALLENGE

Accelerating cyber threats

49% of Businesses reported being the victim of a cyber ransom attack in 2016

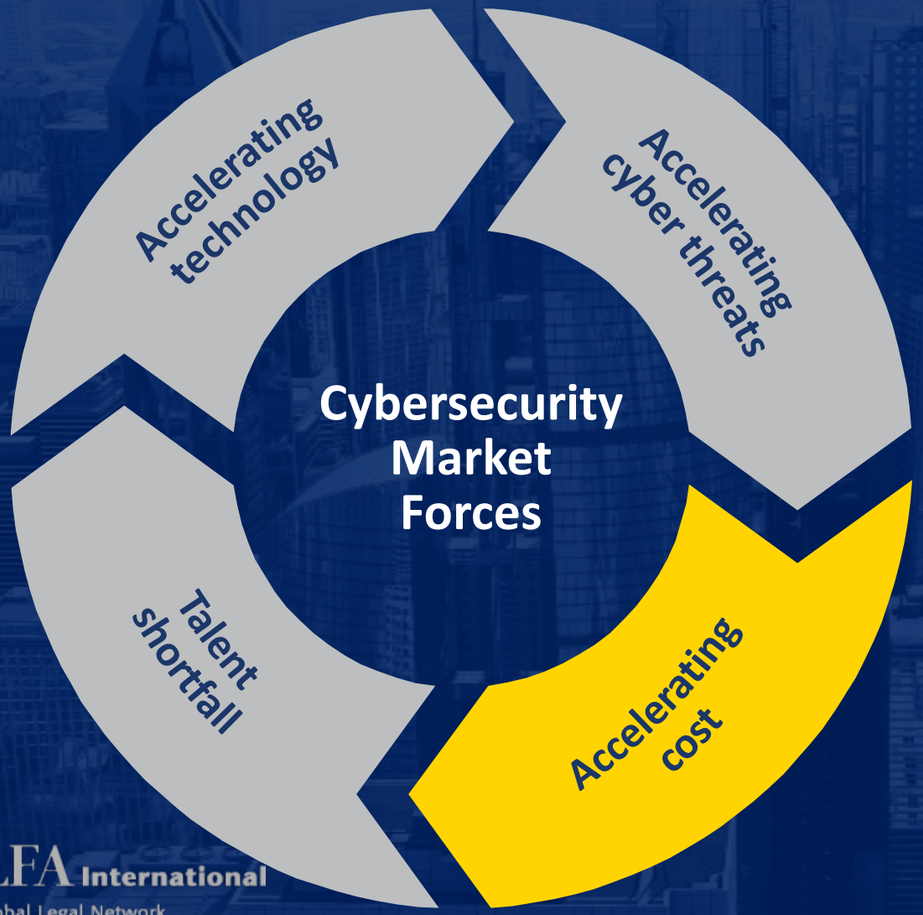
Source: TechRepublic 2017 article ”49% of businesses fell victim to cyber ransom attacks in 2016
https://www.techrepublic.com/article/49-of-business-fell-victim-to-cyber-ransom-attacks-in-2016/

ALFA International
The Global Legal Network
Local Relationships Worldwide

DATA BREACHES ARE ON THE RISE

THE CHALLENGE

Creating greater cost drain



Attacks and breaches by 2019 will cost businesses

$2.1T

every year.

Source: Forbes.com 2017 article ”Cyber Crime Costs Projected to Reach $2 Trillion by 2019” – https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#114dbaeb3a91

ALFA International
The Global Legal Network
Local Relationships Worldwide

DATA BREACHES ARE ON THE RISE

THE CHALLENGE

Creating greater resource drain

There will be an estimated

shortfall of 1.8m

professionals in the global information security workforce by 2022.

Source: 2017 Global Information Security Workforce Study (GISWS)

DATA BREACHES ARE ON THE RISE

- Since January of 2017, at least 16 major retailers were hacked and likely had information stolen from them
- A report from cybersecurity firm Shape Security showed that almost 90% of the login attempts made on online retailers' websites are hackers using stolen data
- Many of these breaches were caused by flaws in payment systems that were taken advantage of by hackers

TRENDS IN CYBERSECURITY

RECENT CYBERSECURITY & DATA PRIVACY EVENTS

ALFA International
The Global Legal Network
Local Relationships Worldwide

ORBITZ

ANNOUNCED: March 1, 2018 - someone had gained unauthorized access to one of its legacy travel booking platforms

IMPACT: Breach exposed the details of 880,000 customers' payment cards between October 1, 2017 and December 22, 2017

TAKEAWAY: Outdated legacy software and systems might have created the security risk – examine old systems and storage

SAKS FIFTH AVENUE / LORD & TAYLOR

ANNOUNCED: March 28, 2018 – Breach actually occurred in May 2017

IMPACT: Third-party called "Fin7" posted to underground market hub, called "BIGBADABOOM-2," which advertised the details of five million payment cards for sale

AT RISK: Fin7 released the details of 125,000 cards stolen from the two luxury department stores

TAKEAWAY: Create stronger malware precautions on point-of-sale systems / insist on chip & PIN, not swipe

PANERA BREAD

ANNOUNCED: April 2, 2018 - notified of a data leak due to flaw contained on website

IMPACT: At the time, it said personal information, including names, addresses, and partial credit card numbers may have leaked, though the company says the investigation is ongoing

AT RISK: Unknown. "Our investigation is continuing, but there is no evidence of payment card information nor a large number of records being accessed or retrieved." Conduct regular penetration tests!

SEARS HOLDINGS

ANNOUNCED: April 2018 - alerted customers of an undisclosed "security incident"

IMPACT: The incident affected up to 100,000 shoppers who bought items online from September 27, 2017 to October 12, 2017

ADIDAS

ANNOUNCED: June 2018 - an "unauthorized party" said it had gained access to customer data on Adidas' US website

adidas GROUP

IMPACT: Adidas did not say exactly how many customers could have been affected by the breach, but an Adidas spokeswoman confirmed it is likely "a few million."

AT RISK: The data that is potentially at risk includes customer contact information, like email addresses and physical addresses, as well as login information, like usernames and passwords.

MACY'S

ANNOUNCED: July 10, 2018

"We have investigated the matter thoroughly, addressed the cause and, as a precaution, have implemented additional security measures. Macy's, Inc. will provide consumer protection services at no cost to those customers. We have contacted potentially impacted customers with more information about these services."

Customers shopping online at macys.com or bloomingdales.com between April and June 2018 could have had their personal information exposed

CHEDDAR'S SCRATCH KITCHEN

ANNOUNCED: Notified by government officials in August 2018 that they were a target of a cyber attack

IMPACT: Customers who visited Darden Restaurants-owned Cheddar's Scratch Kitchen between November 3, 2017, and January 2, 2018, may have had their credit-card information stolen

AT RISK: Darden estimates that 567,000 payment card numbers could have been compromised

FACEBOOK & GOOGLE+

ANNOUNCED: Facebook discovered on September 25, 2018, that attackers exploited software vulnerability

ANNOUNCED: October 8, 2018 – Google+ to shutdown due to breach (since 2015)

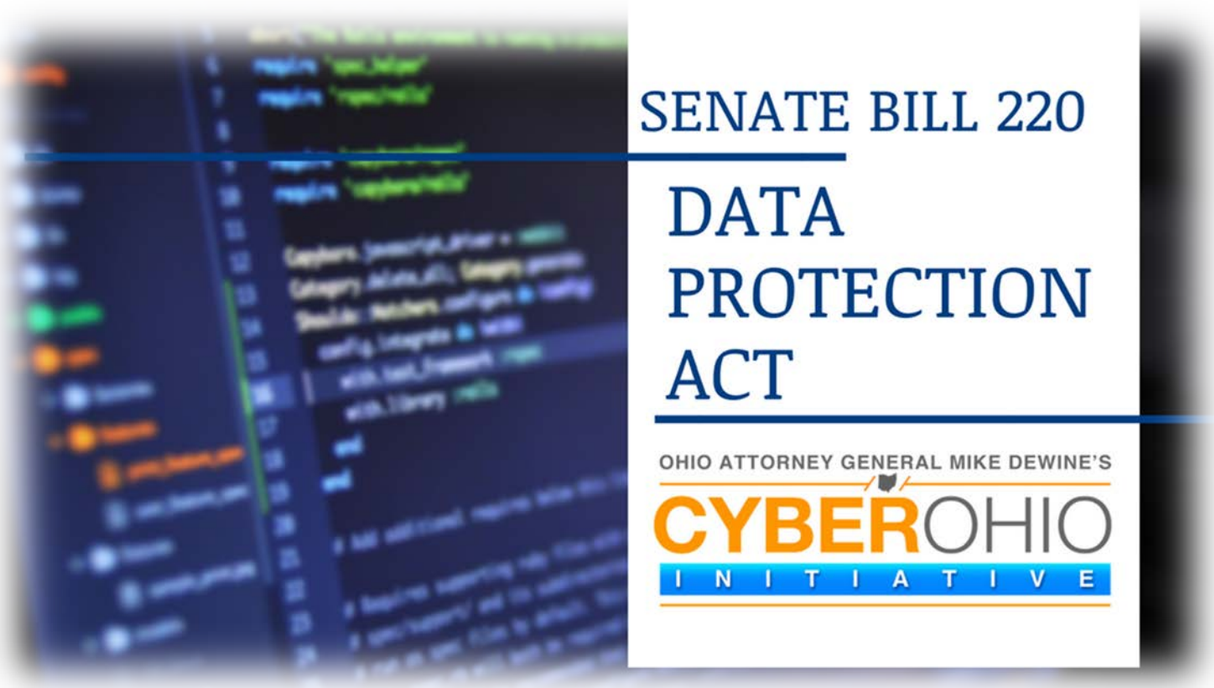
IMPACT: Hackers gained access to nearly 50 million Facebook user accounts. For Google+, 496,951 users' full names, email addresses, birth dates, gender, profile photos, places lived, occupation and relationship status were potentially exposed

TAKEAWAY: To be determined…

OHIO DATA PROTECTION ACT

THE OHIO DATA PROTECTION ACT

SIGNED: Signed into law by Governor Kasich on August 3, 2018



WHAT IS IT? **First of its kind safe harbor against data breach lawsuits for businesses that implement and maintain cybersecurity programs that meet certain industry-recognized standards**

Fundamentally different than punitive approaches other states have taken – *e.g.*, California Consumer Privacy Act imposes penalties and obligations on California businesses

THE OHIO DATA PROTECTION ACT

EFFECTIVE DATE: November 2, 2018

BENEFIT: Provides an affirmative defense to certain tort claims related to cybersecurity

The law does not require businesses to comply with the Ohio DPA

Rather, a business that can demonstrate its cybersecurity program meets certain enumerated standards is eligible for the defense to liability for the breach

THE OHIO DATA PROTECTION ACT

NOT ONE-SIZE-FITS ALL: Recognizing that different businesses have different needs, the law accounts for individual factors

FLEXIBILITY: business can choose from different cybersecurity frameworks as the foundation for a program, allowing it to tailor its program based on particular industry / circumstances

TWO INCENTIVES:
(1) Opportunity for businesses to evaluate and improve their current program, which lessens the likelihood of a breach
(2) If a breach still occurs, DPA provides a safe-harbor against tort claims asserting that the business has adequate security measures

THE OHIO DATA PROTECTION ACT

EIGHT AVAILABLE FRAMEWORKS FOR AFFIRMATIVE DEFENSE TO CERTAIN TORT CLAIMS

- CENTER FOR INTERNET SECURITY'S CRITICAL SECURITY CONTROLS FOR EFFECTIVE CYBER DEFENSE
- FEDERAL INFORMATION SECURITY MODERNIZATION ACT
- FEDERAL RISK AND AUTHORIZATION MANAGEMENT PROGRAM'S SECURITY ASSESSMENT FRAMEWORK
- GRAMM-LEACH-BLILEY ACT'S SAFEGUARDS RULE
- HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT
- HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT'S (HIPAA) SECURITY RULE
- INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO)/INTERNATIONAL ELECTROTECHNICAL COMMISSION'S (IEC) 27000 FAMILY – INFORMATION SECURITY MANAGEMENT SYSTEMS STANDARDS
- NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY'S (NIST) CYBERSECURITY FRAMEWORK

NOTE: *PCS DSS IS NOT AN ELIGIBLE FRAMEWORK*

THE OHIO DATA PROTECTION ACT

FIVE FACTORS TO CONSIDER

- THE ORGANIZATION'S SIZE AND COMPLEXITY
- THE NATURE AND SCOPE OF ITS ACTIVITIES
- THE SENSITIVITY OF THE PERSONAL INFORMATION PROTECTED UNDER THE PROGRAM
- THE COST AND AVAILABILITY OF TOOLS TO IMPROVE ITS INFORMATION SECURITY
- THE RESOURCES AVAILABLE TO THE ORGANIZATION.

THE OHIO DATA PROTECTION ACT

RECAP: WHAT DOES THE ODPA DO?

DOES NOT CREATE "MINIMUM STANDARD"

DOES NOT MODIFY OHIO'S CURRENT NOTIFICATION LAW – O.R.C. 1349.19

DOES PROVIDE AFFIRMATIVE DEFENSE TO TORT ACTIONS UNDER OHIO LAW

CREATES INCENTIVE TO REVIEW CURRENT CYBERSECURITY PROGRAM

IMPLEMENT QUALIFYING CYBERSECURITY PROGRAM FOR AFFIRMATIVE DEFENSE

QUESTIONS

ALFA International
The Global Legal Network
Local Relationships Worldwide