CAL POLY

SAN LUIS OBISPO

Section 1

# INTRODUCTION

**Dr. Bruce Burton**
California Cybersecurity Institute

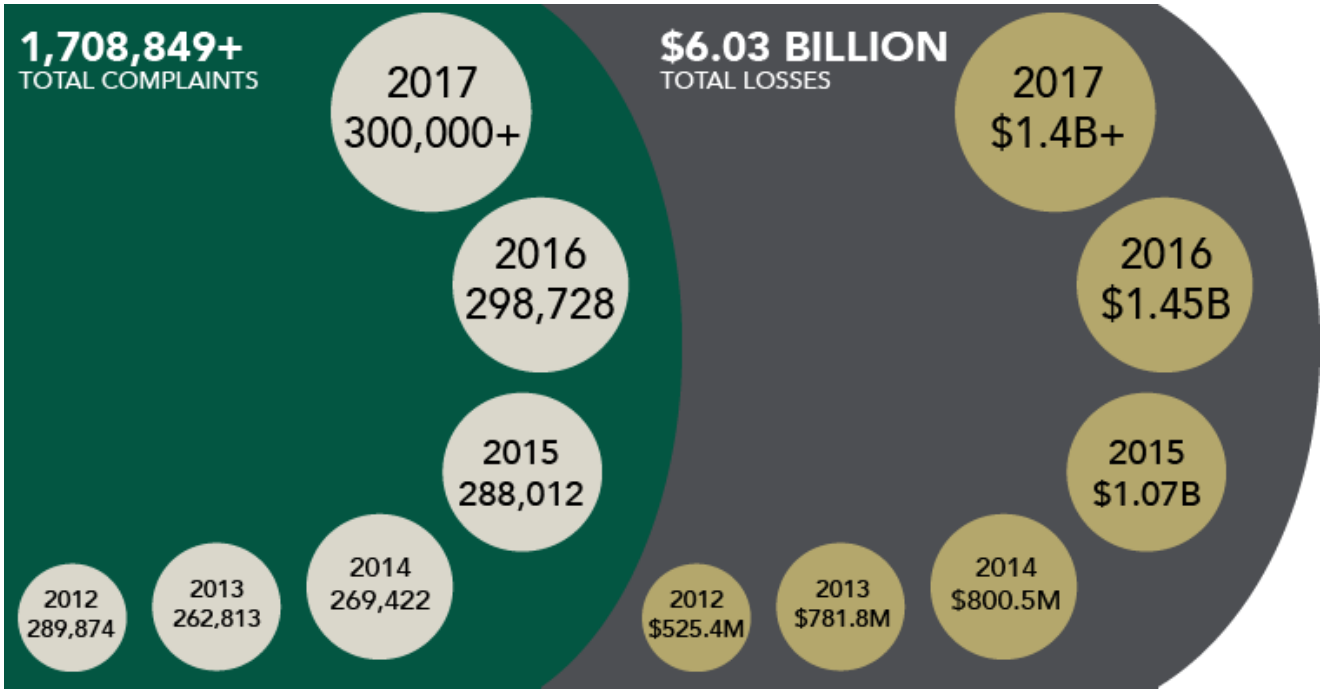
# OBJECTIVES

- Current cybersecurity statistics and implications
- Learn from past attacks
- Understand the NIST Cybersecurity Framework (CSF) & potential quick hits

Section 2

# YOUR ENTERPRISE IS UNDER ATTACK

# LOSSES DUE TO INTERNET-RELATED CRIME CONTINUE TO GROW! *




*FBI's Internet Crime Report

# 2017 REPORT – SMALL BUSINESS TRENDS

Keeper Security and Ponemon surveyed **1,040 IT and IT security practitioners** at small and medium-sized businesses (SMBs) in North American and UK. The results show:

**Cyber attacks, ransomware and disruptive technologies, such as the Internet of Things, challenge the ability of small businesses to safeguard their information assets.**

61% of SMBs have experienced a **cyber attack** in the past 12 months

54% of SMBs report **data breaches** involving customer & employee information in the past 12 months

# 2017 Report – CA Breach Law

**California law requires a business or state agency to notify any California resident whose unencrypted personal information, as defined, was acquired, or reasonably believed to have been acquired, by an unauthorized person**

**Any person or business** that is required to issue a security breach notification to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, **to the Attorney General**.

# 2017 REPORT – SMALL BUSINESS TRENDS

# 2017 REPORT – SMALL BUSINESS TRENDS

## Financial costs are growing

Costs up about 30% vs. 2016

- **$1,027,053** on average were spent by SMBs because of damage or theft of IT assets.
- **$1,207,965** on average were spent by SMBs because of disruption to normal operations.

Section 3

# PAST ATTACKS AND WHAT WE CAN LEARN FROM THEM

# TARGET DATA BREACH

# BACKGROUND – WHAT HAPPENED?

- Hackers gained access to Target's networks
- Compromised servers to allow exfiltration of customer data
- Collected personal financial data from POS terminals on millions of customers

# HOW DID IT HAPPEN?

**Unkown Date**

Target's HVAC vendor's computer systems were infected through a phishing attack

**12-02-13**

Customer credit card information was transmitted out from Target's computer system

**12-15-13**

Target acknowledges a data breach; 40,000,000 credit card records stolen

TARGET

**ALL WARNINGS IGNORED BY TARGET**

**11-30-13**

Malicious software was detected on Target servers and Target's security team was notified

**12-12-13**

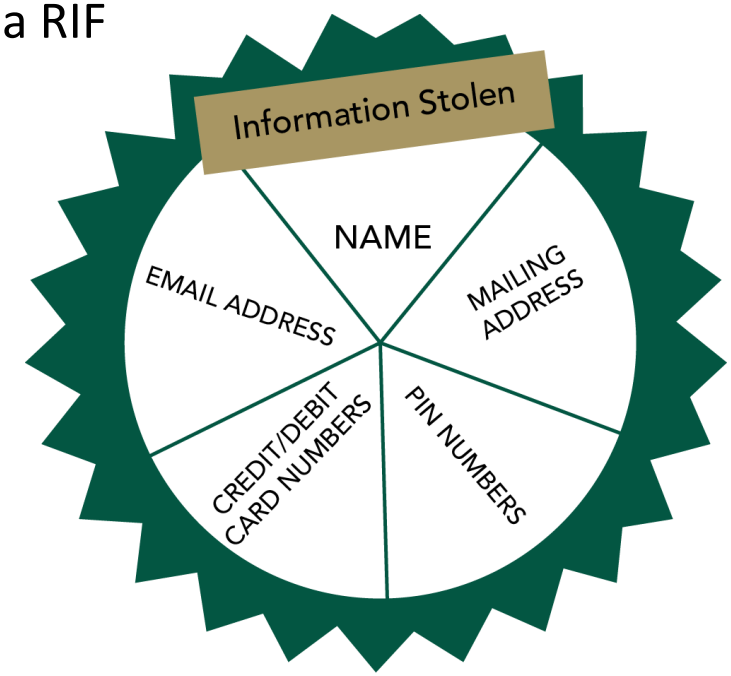
Authorities notified Target of the data breach

**01-10-14**

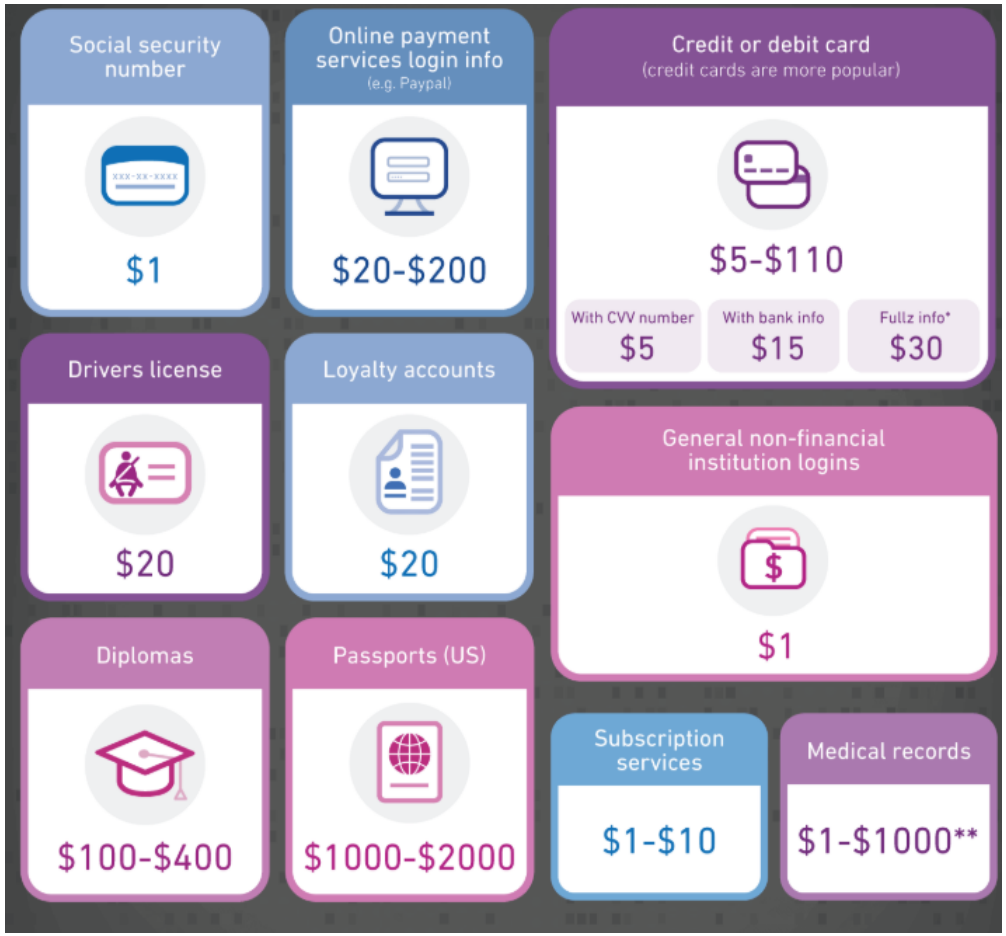
Target acknowledges 70,000,000 additional customer records were stolen

# IMPACT

- Millions of impacted customers
- Tarnished reputation
- Drop in sales transactions resulted in a RIF
- Data breach expenses > $100M
- CEO Resigned



# Personal Information is an Attractive Target



# LESSONS TO BE LEARNED FROM THIS ATTACK

- Personal financial info is an attractive target
- Users play an important role in system security
- Limiting employee/third party access to sensitive network assets is key
- Importance of team training and oversight
- Don't ignore the warning signs of a breach
- Be extremely careful if you store sensitive personal data

# COTTAGE HEALTH DATA BREACH

# BACKGROUND – WHAT HAPPENED?

- Cottage Health Systems, a medium sized health delivery organization in the Santa Barbara area learned of a data breach
- In the course of investigating the first breach, a second breach was discovered
- Both events exposed patients' medical information
- Fortunately, Cottage Health had a cybersecurity insurance policy and it covered much of the expense of the data breach

# HOW DID IT HAPPEN?

- 3rd party supplier removed electronic security protections from one of Cottage Health's servers
- Poor oversight over IT service suppliers
- Violation of other basic security principles

# IMPACT

- Huge amount of bad publicity
- Listed on the HHS "wall of shame" website
- Numerous lawsuits on behalf of impacted patients
- $2M fine from the state of CA
- Requirement to significantly upgrade their security practices

# IMPACT - CONTINUED

- Insurer sues Cottage Health for $4.125 million plus attorneys' fees
- Alleges that hospital failed to take reasonable steps to protect data
- The devil is in the details

Matthew T. Walsh, Esq. (Bar No. 208169)
**CARROLL, McNULTY & KULL LLC**
100 North Riverside Plaza, Suite 2100
Chicago, Illinois 60606
Telephone: (312) 800-5000
Facsimile: (312) 800-5010
Email: mwalsh@cmk.com

Attorneys for Plaintiff COLUMBIA CASUALTY COMPANY

**UNITED STATES DISTRICT COURT**
**FOR THE CENTRAL DISTRICT OF CALIFORNIA**

| | |
|---|---|
| COLUMBIA CASUALTY COMPANY<br>Plaintiff,<br>v.<br>COTTAGE HEALTH SYSTEM<br>Defendant. | Case No.: 2:15-cv-03432<br>**COMPLAINT FOR DECLARATORY JUDGMENT AND REIMBURSEMENT OF DEFENSE AND SETTLEMENT PAYMENTS** |

Plaintiff COLUMBIA CASUALTY COMPANY (hereinafter "Columbia") by and through its attorneys, as and for Complaint against Defendant, hereby allege as follows:

**INTRODUCTION**

1. This is a Complaint for Declaratory Judgment pursuant to 28 U.S.C. § 2201 and for Reimbursement of Defense and Settlement Payments made by Columbia on behalf of its insured.

2. This matter arises out of a data breach that resulted in the release of electronic private healthcare patient information stored on network servers owned, maintained and/or utilized by defendant COTTAGE HEALTH SYSTEM ("Cottage").

3. Cottage operates a network of hospitals located in Southern California, including Santa Barbara Cottage Hospital, Goleta Valley Cottage Hospital and Santa Ynez Valley Cottage Hospital (collectively, the "Hospitals.")

COMPLAINT FOR DECLARATORY JUDGMENT AND REIMBURSEMENT

# LESSONS TO BE LEARNED FROM THIS ATTACK

- Ignorance is not bliss... know your state laws
- Deliberate vs. accidental – self-inflicted wound
- Ensure that your customer's data is protected in accordance with industry standard security practices
- Importance of training and organizational response
- Review and negotiate cybersecurity policy terms – the devil is in the details
  - Beware of broadly worded cybersecurity/data protection exclusions
  - Guard against a misrepresentation defense

# PUPPY PALACE – CYBER ATTACK EXAMPLE


Small Business
Big Threat

# THE HOW AND WHAT

What Happened?

- Appears that the business was attacked and customer/employee info was stolen

How?

- Through a phishing attack

What Impact?

- May trigger disclosure requirement
- Future bad publicity
- Potential negative business impacts

# LESSONS TO BE LEARNED

- Importance of training – employees are your first line of defense
- Importance of good cyber hygiene
- Value of encrypting sensitive information
- Limitations of law enforcement help
- Importance of cybersecurity insurance

***60 percent of small companies are unable to sustain their businesses over six months after a cyber attack****

*U.S. National Cyber Security Alliance

Section 4

# COST-EFFECTIVE STEPS FOR CYBER RESILIENCY

# ORGANIZE YOUR CYBERSECURITY DEFENSE IN LINE WITH THE NIST CSF

The **NIST Cybersecurity Framework** (NIST CSF) provides a policy framework of computer security guidance for how private sector organizations in the United States can assess and improve their ability to prevent, detect, and respond to cyber attacks

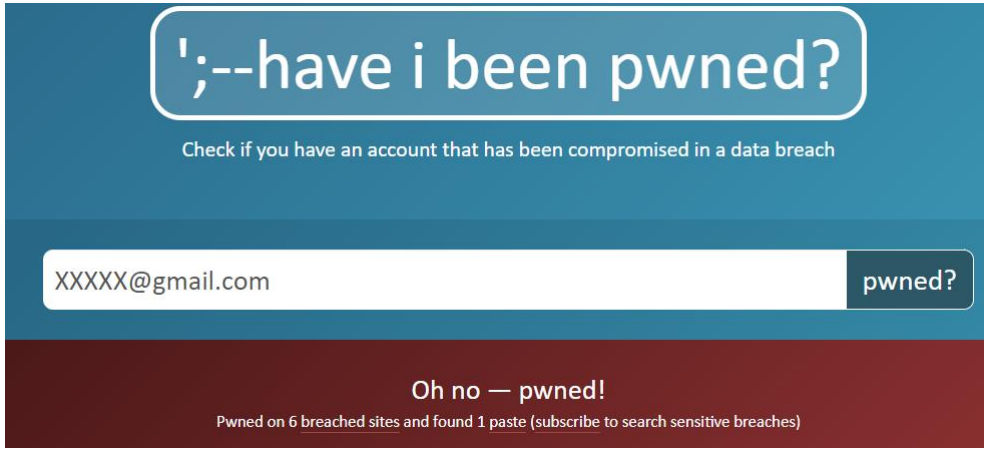
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

# NIST Cyber Security Framework (CSF)

| Identify | Protect | Detect | Respond | Recover |
|---|---|---|---|---|
| • Asset management<br>• Business environment<br>• Governance<br>• Risk assessment<br>• Risk management strategy | • Access Control<br>• Awareness and training<br>• Data Security<br>• Information protection and procedures<br>• Maintenance<br>• Protective technology | • Anomalies & events<br>• Security continuous monitoring<br>• Detection process | • Response planning<br>• Communications<br>• Analysis<br>• Mitigation<br>• Improvements | • Recovery Planning<br>• Improvements<br>• Communications |

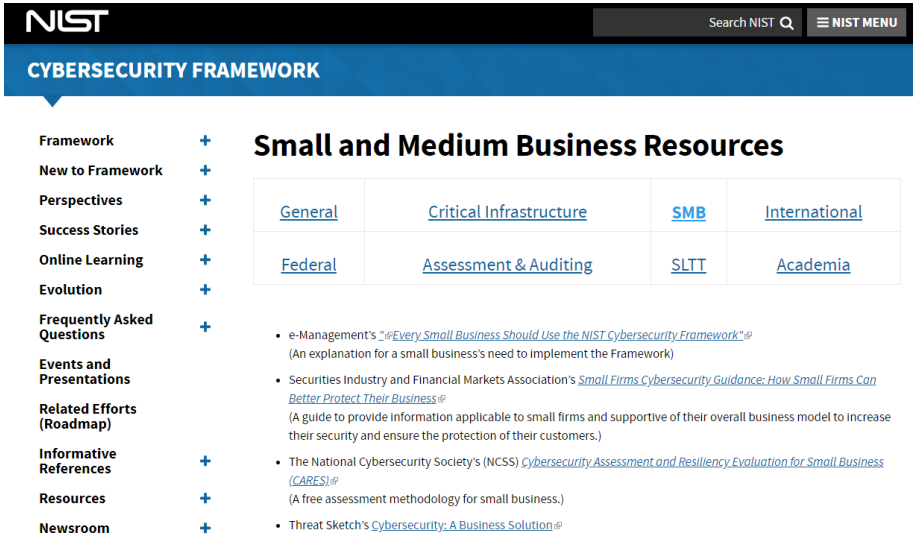
# A Word of Caution about Email/Password Accounts

- The practice of reusing passwords is common but risky!
- The website https://haveibeenpwned.com/ provides insight into both data breaches and password capture



# APPLYING THE NIST CSF

https://www.nist.gov/cyberframework/small-and-medium-business-resources



# IN CLOSING...

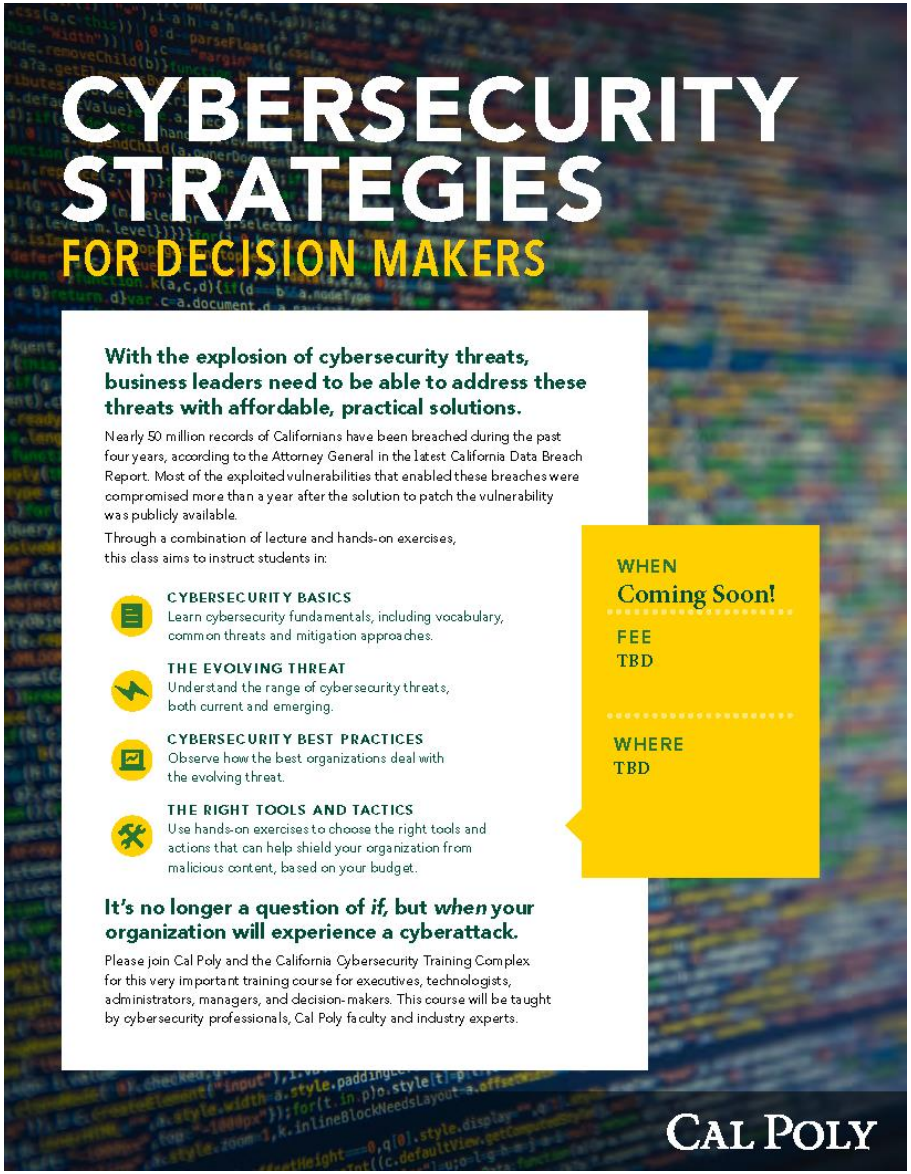
## Florida man bitten after jumping into pit at St. Augustine Alligator Farm

By: Brittney Donovan , Action News Jax

Updated: Nov 7, 2018 - 6:52 PM


***Common sense and the right actions can significantly reduce your risk of attack!***

# Coming Soon…



# CYBERSECURITY STRATEGIES

## FOR DECISION MAKERS

**With the explosion of cybersecurity threats, business leaders need to be able to address these threats with affordable, practical solutions.**

Nearly 50 million records of Californians have been breached during the past four years, according to the Attorney General in the latest California Data Breach Report. Most of the exploited vulnerabilities that enabled these breaches were compromised more than a year after the solution to patch the vulnerability was publicly available.

Through a combination of lecture and hands-on exercises, this class aims to instruct students in:

**CYBERSECURITY BASICS**
Learn cybersecurity fundamentals, including vocabulary, common threats and mitigation approaches.

**THE EVOLVING THREAT**
Understand the range of cybersecurity threats, both current and emerging.

**CYBERSECURITY BEST PRACTICES**
Observe how the best organizations deal with the evolving threat.

**THE RIGHT TOOLS AND TACTICS**
Use hands-on exercises to choose the right tools and actions that can help shield your organization from malicious content, based on your budget.

**WHEN**
Coming Soon!

**FEE**
TBD

**WHERE**
TBD

**It's no longer a question of *if*, but *when* your organization will experience a cyberattack.**

Please join Cal Poly and the California Cybersecurity Training Complex for this very important training course for executives, technologists, administrators, managers, and decision-makers. This course will be taught by cybersecurity professionals, Cal Poly faculty and industry experts.

CAL POLY

# QUESTIONS??