Kathleen Mullin

Practical Experience from a CISO Implementing a Comprehensive Framework
March 30, 2018

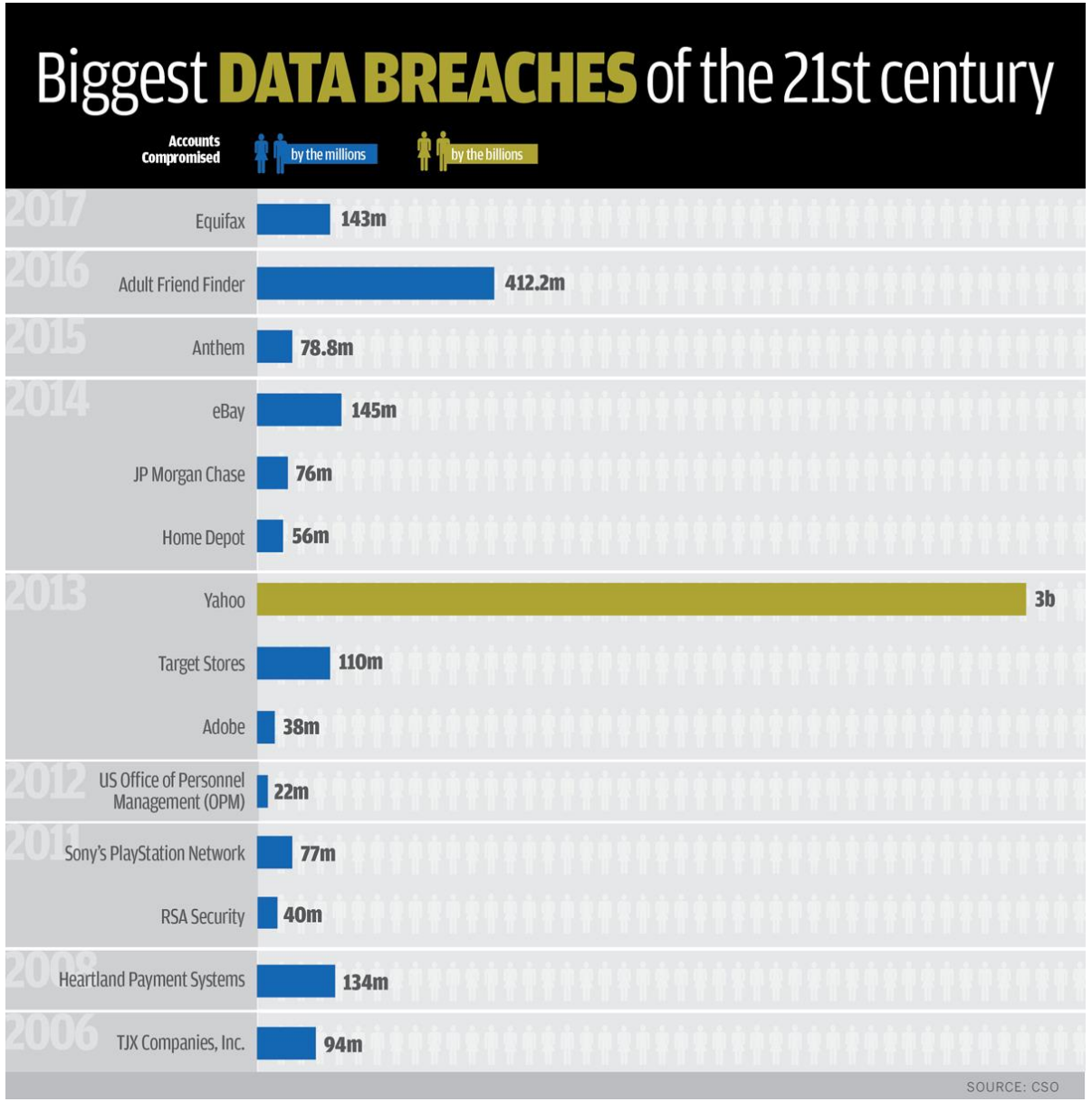
Establish Trust

Lockheed Martin

Cyber Kill Chain®

Biggest Data Breaches

CSO from IDG



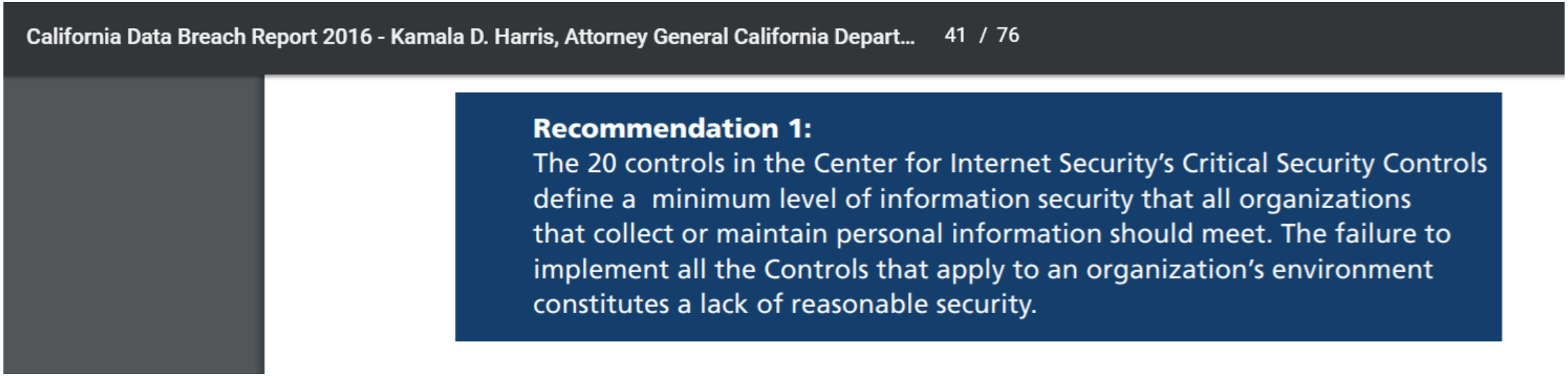
2017's Largest Announced Breach

- Apache Struts Vulnerability (CVE-2017-5638) March 10, 2017
- DHS sends notification to Equifax and others about the Apache vulnerability
- Unauthorized Access May 13, 2017 – July 30, 2017 through a vulnerability in the Online Disputes Portal
- Suspicious activity noticed Saturday July 29, 2017 and internally investigated and blocked on July 30, 2017
- Mandiant – FireEye contacted August 2, 2017
- CIO Sells stock August 25, 2017
- Breach announced September 7, 2017
- September 2017 CIO and CISO announce retirement and CEO steps down
- Former CIO indicted for insider trading March 2018

2015's Largest Announcement

- The Anthem breach began February 18, 2014
- Was discovered January 27, 2015
- Announced February 3, 2015
- 78.8 million consumer records
- $115 million dollar settlement announced in June of 2017

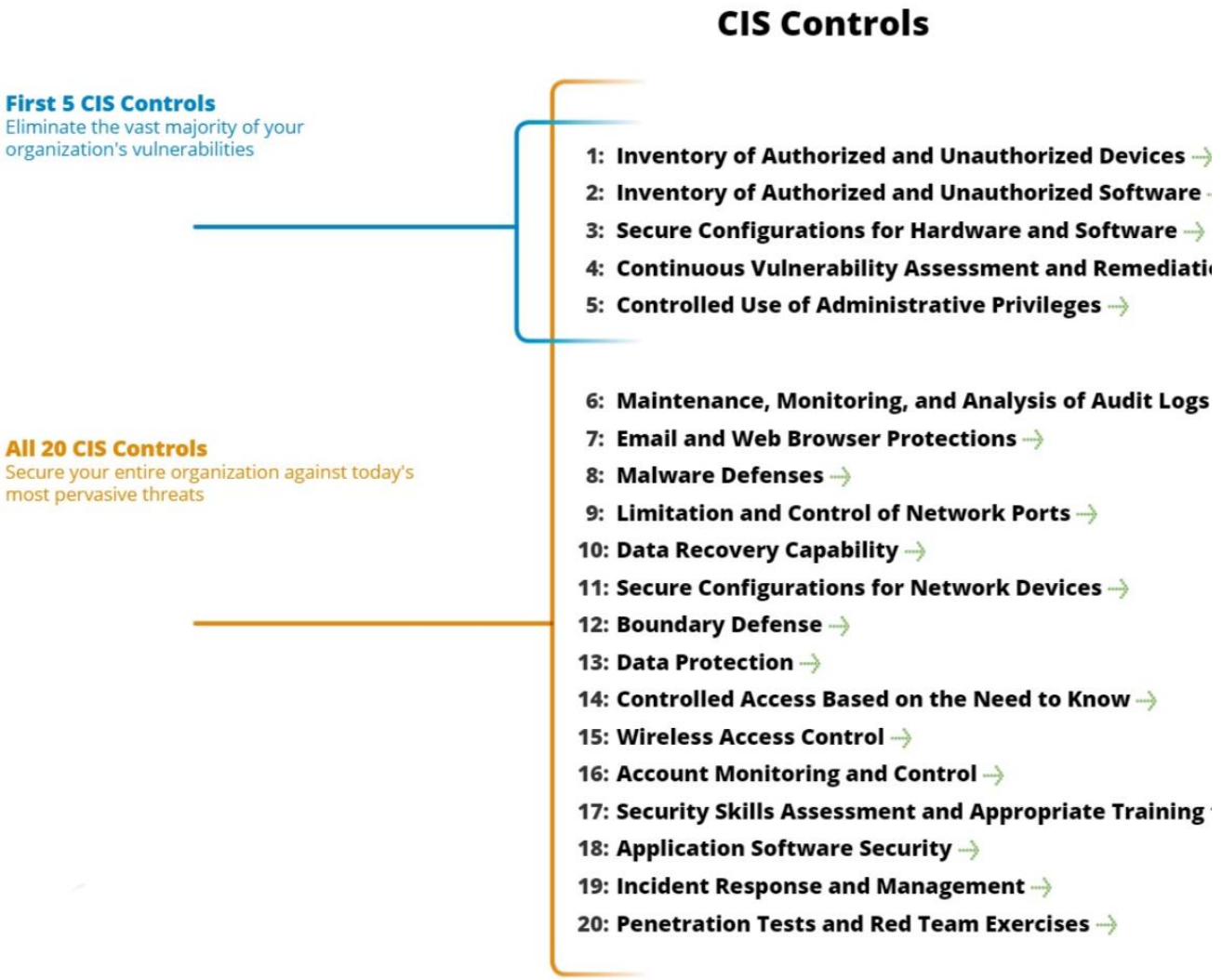
The CIS Top 20 (formerly SANS 20) are a minimum baseline



The CIS States

"Organizations that apply just the first five CIS Controls can reduce their risk of cyberattack by around 85 percent."

"Implementing all 20 CIS Controls increases the risk reduction to around 94 percent"



The Center for Internet Security Critical Security Controls Version 6.1				
Family	**Control**	**Control Description**	**Foundational**	**Advanced**
Critical Security Control #1: Inventory of Authorized and Unauthorized Devices				
System	**1.1**	Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to an organization's public and private network(s). Both active tools that scan through IPv4 or IPv6 network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.	**Y**	*Use a mix of active and passive tools, and apply as part of a continuous monitoring program.*
System	**1.2**	If the organization is dynamically assigning addresses using DHCP, then deploy dynamic host configuration protocol (DHCP) server logging, and use this information to improve the asset inventory and help detect unknown systems.	**Y**	
System	**1.3**	Ensure that all equipment acquisitions automatically update the inventory system as new, approved devices are connected to the network.	**Y**	
System	**1.4**	Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device. The inventory should include every system that has an Internet protocol (IP) address on the network, including but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over-IP telephones, multi-homed addresses, virtual addresses, etc. The asset inventory created must also include data on whether the device is a portable and/or personal device. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to the organization's network.	**Y**	
System	**1.5**	Deploy network level authentication via 802.1x to limit and control which devices can be connected to the network. The 802.1x must be tied into the inventory data to determine authorized versus unauthorized systems.	**Y**	*Authentication mechanisms are closely coupled to management of hardware inventory*
System	**1.6**	Use client certificates to validate and authenticate systems prior to connecting to the private network.		**Y**
Critical Security Control #2: Inventory of Authorized and Unauthorized Software				
System	**2.1**	Devise a list of authorized software and version that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses. This list should be monitored by file integrity checking tools to validate that the authorized software has not been modified.	**Y**	*File integrity is verified as part of a continuous monitoring program.*

HITRUST latest version includes

16 CFR Part § 681 Identity Theft Red Flags

23 NYCRR Part 500 New York State Department of Financial Services

201 CMR 17.00 (State of Massachusetts Data Protection Act)

AICPA Trust Services Principles and Criteria

CAQH CORE

CIS Critical Security Controls v 6 (formerly SANS Top 20) (*Current ver. 6.1 , ver. 7 being release March 19, 2018*)

CMS Information Security ARS v2 --Appendix A Minimum Security Requirements for High Impact Data (*CMS has replaced the ARS with v3.1 which no longer contains Minimum Security Requirements for High Impact Data*)

COBIT 4.1 (*Deprecated*) COBIT 5 (*Current*)

CRR V2016

CSA Cloud Controls Matrix v3.0.1 (*Current*)

FedRAMP

FFIEC IS v2016

GDPR - EU General Data Protection Regulation

Guidance to render PHI Unusable, Unreadable, or Indecipherable

HIPAA Security Rule, HIPAA Breach Notification Rule, HIPAA Privacy Rule

HITRUST De-Identification Framework v1

IRS Publication 1075 v2014, (*Updated September 2016, effective September 30, 2016*)

ISO 27799:2008 (*This standard has been replaced by ISO 27799:2016*)

ISO/IEC 27001:2005 (*Deprecated*) ISO/IEC 27001:2013 *Current*)

ISO/IEC 27002:2005 (*Deprecated*) ISO/IEC 27002:2013 *Current*)

Joint Commission - Information Management (IM)

MARS-E v2

NIST Framework for Improving Critical Infrastructure Cybersecurity v1 (*new update v 1.1 in Spring 2018*)

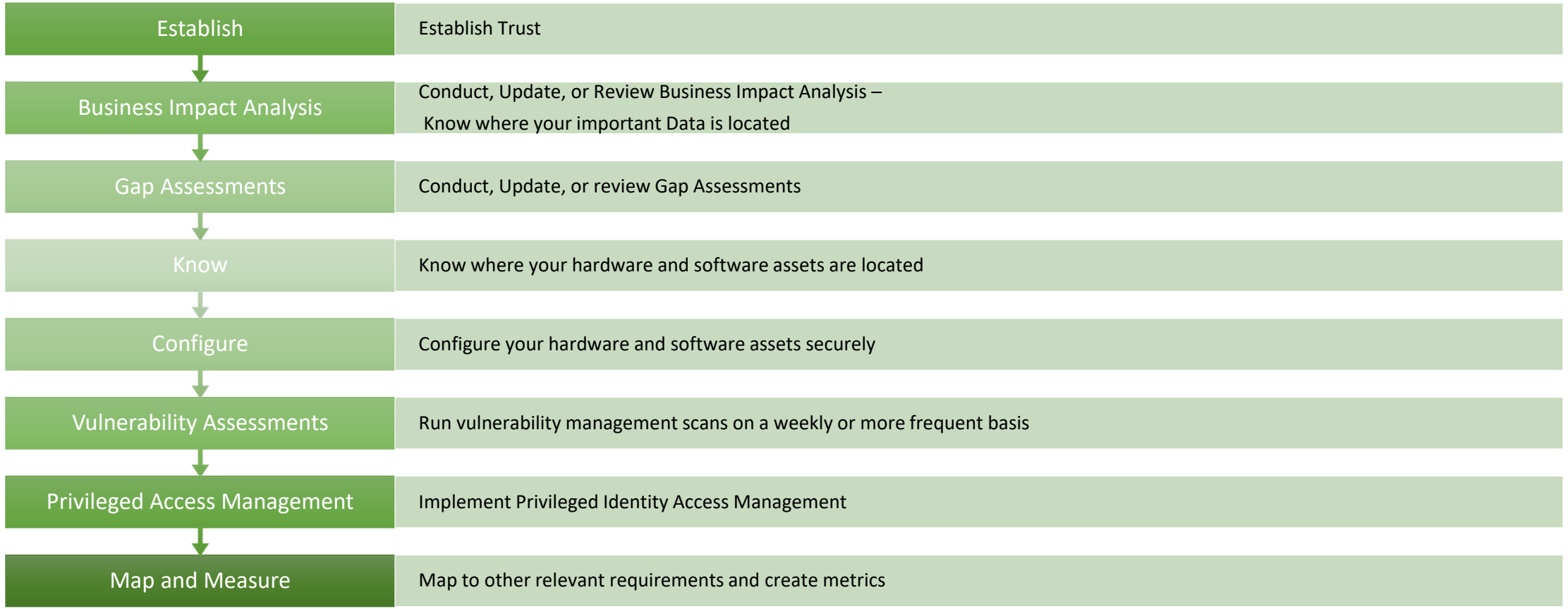
NIST SP 800-53 R4 (Moderate Level Baseline)

NRS 603A (State of Nevada - Security of Personal Information)

PCI DSS 3.2 Requirement – TLS 1.1 or higher

Migration completion date - June 30, 2018 for transitioning from SSL and TLS 1.0 to a secure version of TLS (currently v1.1 or higher but it really should be 1.2).

This impacts older versions of Windows Explorer usually running on XP for external clients accessing web sites but can also impact some internally developed code.



Leverage what exists and build on it

Questions