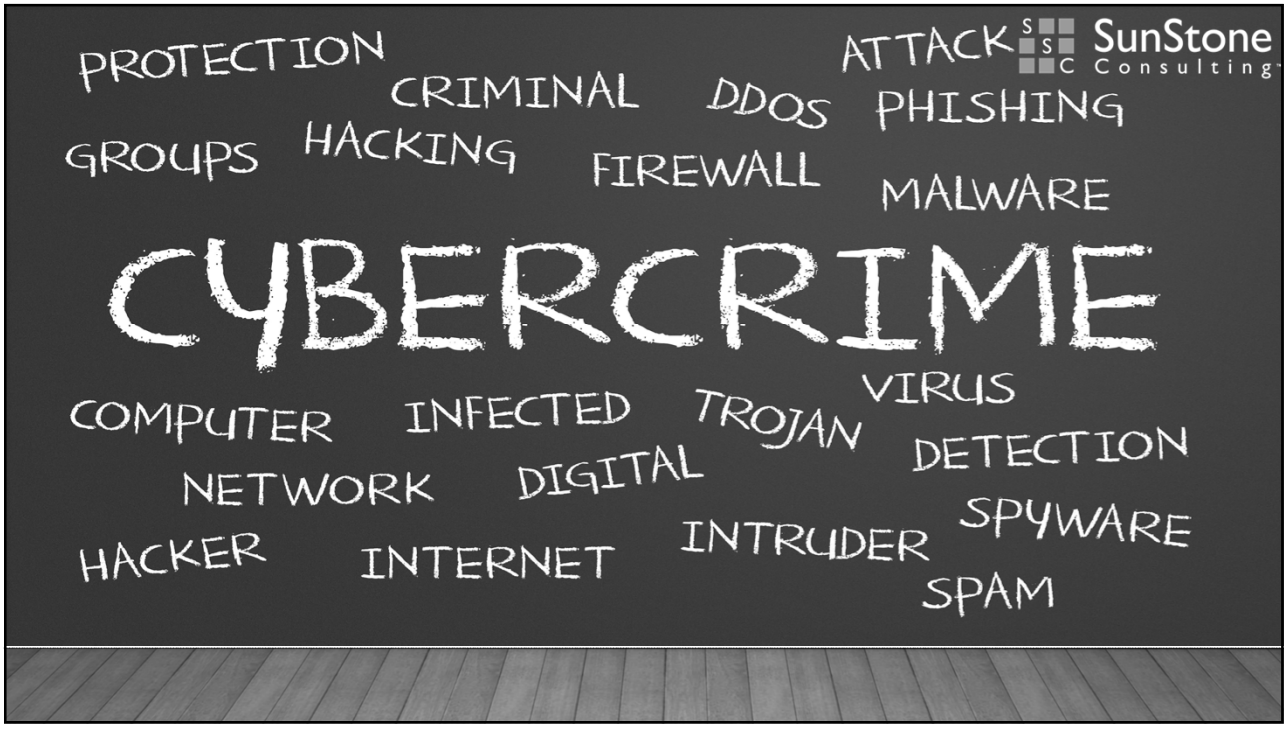
Cybersecurity & Threat Risks: Where are we and where are we going?

6/1/2018



DATA CAN "SLEEP WALK"–KEEP IT SAFE

- ✓UNINTENTIONAL DATA LOSS
  - ❖CONFIDENTIAL DATA LEAVES THE COMPANY – WITHOUT AUTHORIZED PERMISSION
  - ❖SYSTEMS ARE PURCHASED WITHOUT KNOWLEDGE OR SIGN-OFF BY IT (SHADOW IT)
    - ➢DATA STORED OUTSIDE OF IT CONTROLS IN THE CLOUD
  - ❖3RD PARTY VENDOR CONCERNS

DATA CAN "SLEEP WALK"–KEEP IT SAFE

- ✓PROTECTING DATA IS CRITICAL TO AN ORGANIZATION
  - ❖PRIVACY CONCERNS
  - ❖INTELLECTUAL PROPERTY
  - ❖MANY LAWS PROTECTING – NEWLY ADDED GENERAL DATA PROTECTION REGULATION (GDPR)
  - ❖GDPR PENALTIES – GREATER OF $20 MILLION (US) OR 4% OF VIOLATORS ORG GLOBAL REVENUE

DATA CAN "SLEEP WALK"-KEEP IT SAFE

- ✓WHAT IS GDPR?
  - ❖THE EUROPEAN UNION'S GENERAL DATA PROTECTION REGULATION (GDPR), IS THE BASIC FRAMEWORK FOR PROTECTION OF PERSONAL INFORMATION OF EU CITIZENS.
  - ❖THE GDPR LAYS OUT DETAILED REQUIREMENTS GOVERNING THE COLLECTION, USE, SHARING AND PROTECTION OF PERSONAL INFORMATION.
  - ❖GDPR WAS ADOPTED IN APRIL 2016 AND WENT IN FORCE ON MAY 25, 2018.

*virtu Corporation

DATA CAN "SLEEP WALK"-KEEP IT SAFE

- ✓GDPR – FORCES COMPANIES TO CONTROL THEIR/OTHERS DATA
  - ❖LAWFUL, FAIR AND TRANSPARENT PROCESSING
  - ❖LIMITATION OF PURPOSE, DATA AND STORAGE
  - ❖DATA SUBJECT RIGHTS
  - ❖CONSENT
  - ❖PERSONAL DATA BREACHES
  - ❖DATA PROTECTION IMPACT ASSESSMENT
  - ❖DATA TRANSFERS
  - ❖DATA PROTECTION OFFICER
  - ❖AWARENESS AND TRAINING

*Advisers Expert Solutions, Punit Bhatia

DATA CAN "SLEEP WALK"–KEEP IT SAFE

- ✓GDPR – IS IT COMING TO THE USA?
  - ❖MAYBE…
    - ➢FACEBOOK AND CAMBRIDGE ANALYTICA FALLOUT
    - ➢RESEARCHERS IN 2014 ASKED USERS TO TAKE A PERSONALITY SURVEY
    - ➢APP WAS ALLOWED TO COLLECT USER DATA
    - ➢50 MILLION RAW PROFILES HARVESTED – 270,000 USERS HAD CONSENTED
    - ➢LEARNED ABOUT IT IN 2015 – DATA SHOULD HAVE BEEN DELETED – VERIFY IT WAS DELETED???
    - ➢WHAT WILL HAPPEN???

DATA BREACH EXAMPLES

- ✓ACCIDENTALLY PUBLISHED…
  - ❖RED CROSS BLOOD SERVICE – AUSTRALIA
  - ❖OCCURRED OCT 2016
  - ❖UNSECURED DATA WAS POSTED ON A WEBSITE BY A CONTRACTOR
  - ❖LEAK INCLUDED ID INFO "PERSONAL DETAILS" OF 550,000 DONORS
  - ❖INCLUDED ANSWERS TO QUESTIONNAIRE WITH VERY PERSONAL INFO
  - ❖LARGEST DATA LEAK IN AUSTRALIA
  - ❖SECURITY PROFESSIONAL WAS CONTACTED BY SOMEONE WHO ACQUIRED THE INFORMATION. SECURITY PRO PART OF THE LEAK. SENT 1.74 GB FILE INC "AT RISK SEXUAL ACTIVITY"

*http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

DATA BREACH EXAMPLES (CONT)

- ✓PREVENTION…
  - ❖IMPLEMENT THE APPROPRIATE CONTRACTUAL REQUIREMENTS OR CONTROL MEASURE IN ORDER TO PROTECT PERSONAL INFORMATION THAT IS HANDLED BY A THIRD PARTY PROVIDER.

*http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

DATA BREACH EXAMPLES (CONT)

- ✓HACKED…
  - ❖QUEST DIAGNOSTICS – NEW JERSEY
  - ❖OCCURRED NOV 26, 2016
  - ❖ACCESSED MYQUEST BY CARE360 INTERNET APPLICATION
  - ❖OBTAINED PHI DATA OF APPROXIMATELY 34,000 INDIVIDUALS
  - ❖THE ACCESSED DATA INCLUDED NAME, DATE OF BIRTH, LAB RESULTS, AND IN SOME INSTANCES, TELEPHONE NUMBERS.

*http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

DATA BREACH EXAMPLES (CONT)

- ✓PENALTY…
  - ❖ACTIONS STILL PENDING
- ✓PREVENTION…
  - ❖PATCH AND UPDATE SERVERS, REVIEW APPLICATIONS FOR POSSIBLE SECURITY ISSUES

*http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

DATA BREACH EXAMPLES (CONT)

- ✓INSIDE JOB…
  - ❖FRENCH POLICE HEALTH INSURANCE
  - ❖OCCURRED JUNE 2, 2016
  - ❖PERSONAL DETAILS OF 112,00 FRENCH POLICE OFFICERS UPLOADED TO GOOGLE DRIVE
  - ❖DISGRUNTLED WORKER UPLOADED DATA
  - ❖LUCKILY THE FILES WERE PROTECTED BY A PASSWORD

*http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

DATA BREACH EXAMPLES (CONT)

- ✓PREVENTION…
  - ❖BLOCK ACCESS TO FILE SHARING SITES, MONITOR FOR DATA LEAKAGE

*http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

DATA BREACH EXAMPLES (CONT)

- ✓LOST/STOLEN DEVICE AND MEDIA…
  - ❖ADVOCATE HEALTH CARE
  - ❖OCCURRED JULY 2013 AND NOV 2013
  - ❖BREACH INVOLVED ELECTRONIC HEALTH INFO OF 4 MILLION PEOPLE

*http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

DATA BREACH EXAMPLES (CONT)

- ✓THREE SEPARATE EVENTS…
  - ❖FOUR UNENCRYPTED LAPTOPS WITH PERSONAL HEALTH INFORMATION WERE STOLEN FROM AN ADMINISTRATIVE OFFICE IN PARK RIDGE.
  - ❖UNAUTHORIZED THIRD PARTY ACCESSED THE NETWORK OF AN ADVOCATE BUSINESS ASSOCIATE, POTENTIALLY COMPROMISING THE INFORMATION OF MORE THAN 2,000 PATIENTS
  - ❖UNENCRYPTED LAPTOP WITH PERSONAL INFORMATION OF MORE THAN 2,200 INDIVIDUALS WAS STOLEN FROM THE VEHICLE OF AN ADVOCATE MEDICAL GROUP EMPLOYEE

*http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

DATA BREACH EXAMPLES (CONT)

- ✓PENALTY…
  - ❖PAID $5.55 MILLION TO HHS
- ✓PREVENTION…
  - ❖"POLICIES AND PROCEDURES AND FACILITY ACCESS CONTROLS TO LIMIT PHYSICAL ACCESS TO THE ELECTRONIC INFORMATION SYSTEMS HOUSED WITHIN A LARGE DATA SUPPORT CENTER," ACCORDING TO OCR.
  - ❖ENCRYPTION ON ALL ENDPOINT DEVICES.

*http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

DATA BREACH EXAMPLES (CONT)

- ✓POOR SECURITY…
  - ❖MADE KNOWN – JAN 2017
  - ❖SWEDISH TRANSPORT AGENCY – ''KEYS TO THE KINGDOM''
  - ❖INFORMATION ABOUT ALL VEHICLES IN THE COUNTRY – INCLUDING POLICE AND MILITARY – WAS MADE AVAILABLE TO IT WORKERS IN EASTERN EUROPE
  - ❖OUTSOURCED IT MAINTENANCE WITHOUT PROPER SECURITY CLEARANCE CHECKS
  - ❖ADMINISTRATORS IN THE CZECH REPUBLIC WERE GIVEN FULL ACCESS TO ALL DATA AND LOGS
  - ❖IT IS NOT KNOWN WHETHER THE SECURITY GLITCH CAUSED ANY MAJOR DAMAGE

*http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

DATA BREACH EXAMPLES (CONT)

- ✓PREVENTION…
  - ❖FULLY VET ALL YOUR VENDORS AND UNDERSTAND HOW THEY WILL HANDLE YOUR DATA
  - ❖**ASSIGN DATA ACCESS PRIVILEGES APPROPRIATELY**

*http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

WHERE ARE WE GOING?

- ✓CLOUD SOLUTIONS ARE CATCHING ON IN HEALTHCARE
  - ❖CLOUD SYSTEMS TO MANAGE AND EXCHANGE DATA ARE ON THE RISE
  - ❖ANALYTICS HAS BEEN ON THE RISE – 3RD PARTY CLOUD SYSTEMS

*http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

WHERE ARE WE GOING?

- ✓ISSUES…
  - ❖SHARED SECURITY MODEL
  - ❖INFORMATION BEING TRANSPORTED AND STORED – WHERE IS IT?
  - ❖NEW POTENTIAL POINTS OF FAILURE IN SECURITY PROCESS – LEARNING CURVE

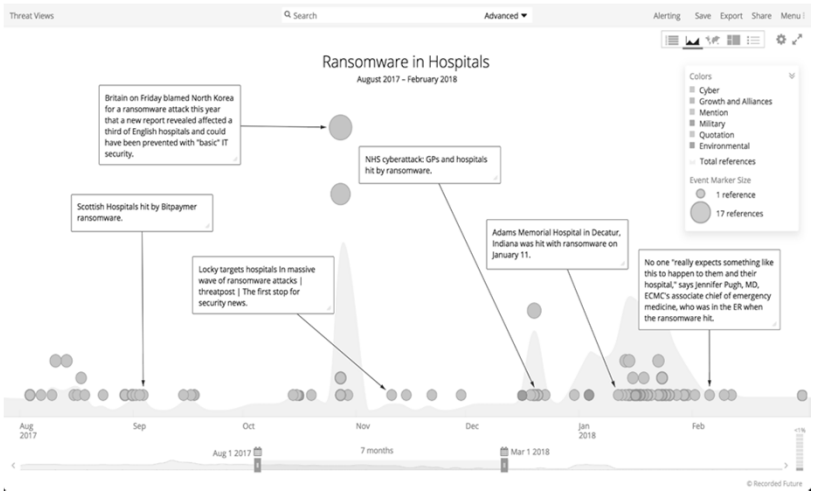
WHERE ARE WE GOING?

- ✓OLD FRIENDS GETTING MORE PREVALENT (PHISHING AND RANSOMWARE)
  - ❖RANSOMWARE AS A SERVICE –
    - ➢DEVELOPED BY MALWARE AUTHORS THEN DISTRIBUTED TO OTHER CRIMINALS TO TAKE PART IN ATTACKS VIA THE DARK WEB
    - ➢THE MAIN DEVELOPER GETS A CUT OF THE ACTION FOR SUCCESSFUL RANSOM PAYMENTS
    - ➢USE OF PORTALS TO DEPLOY AND TRACK THE RANSOMWARE

WHERE ARE WE GOING?

- ✓RANSOMWARE AS A SERVICE (EXAMPLES) –
  - ❖GRANDCRAB
  - ❖SATURN
  - ❖DATA KEEPER

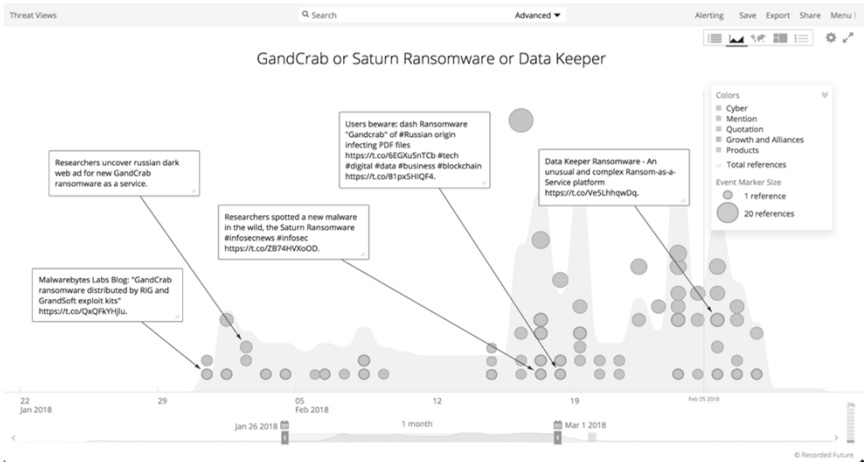
WHERE ARE WE GOING?



*https://www.recordedfuture.com/ransomware-trends-2018/

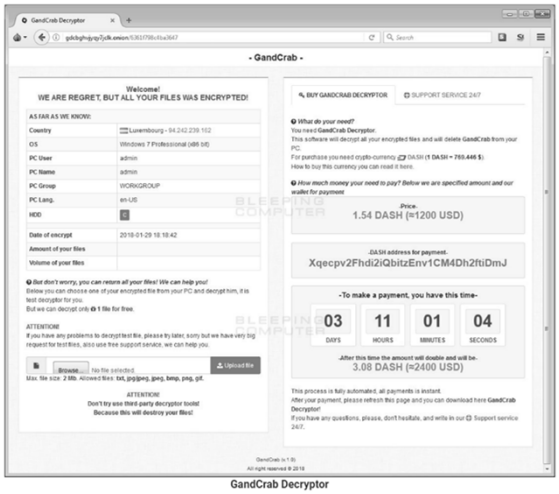
WHERE ARE WE GOING?

✓ MENTIONS OF GANDCRAB, SATURN, AND DATA KEEPER RANSOMWARE FAMILIES.



*https://www.recordedfuture.com/ransomware-trends-2018/

WHERE ARE WE GOING?



GandCrab Decryptor

*GandCrab ransom note. Source: BleepingComputer

WHERE ARE WE GOING?

- ✓COIN MINING IS CATCHING ON
  - ❖CRYPTOCURRENCIES ARE DIGITAL CURRENCIES: THEY ARE CREATED USING COMPUTER
  - ❖PROGRAMS AND COMPUTING POWER, AND RECORDED ON THE BLOCKCHAIN.
  - ❖TO CARRY OUT THIS ACTIVITY COMPUTING RESOURCES ARE REQUIRED. GOTTEN ON WEBSITE VISITS OR RUNNING IN BROWSERS.
  - ❖NOT ILLEGAL AND VALID WAY TO PAY FOR WEBSITE USAGE – MUST BE DISCLOSED

WHERE ARE WE GOING?

- ✓COIN MINING IS CATCHING ON
  - ❖CYBER CRIMINALS SURREPTITIOUSLY INSTALL MINERS ON VICTIMS' COMPUTERS OR INTERNET OF THINGS (IOT) DEVICES WITHOUT THEIR KNOWLEDGE.
  - ❖COINHIVE IS A CRYPTOCURRENCY MINING SERVICE THAT RELIES ON A SMALL CHUNK OF COMPUTER CODE DESIGNED TO BE INSTALLED ON WEB SITES. (MONERO CRYPTOCURRENCY)

WHERE ARE WE GOING?

- ✓INTERESTING STATS ON IOT
  - ❖AN ESTIMATED 25 BILLION DEVICES WILL BE CONNECTED TO THE INTERNET BY 2021, UP FROM 6 BILLION IN 2016. TOTAL SPENDING ON IT, INCLUDING DATA CENTER SYSTEMS, ENTERPRISE SOFTWARE AND CONNECTED DEVICES IS EXPECTED TO REACH $4 TRILLION IN 2021, UP FROM $3.4 TRILLION IN 2015*.

*ChangeWave Investing

WHERE ARE WE GOING?

- ✓INTERESTING STATS ON IOT
  - ❖IOT BUDGETS ARE SET TO RISE AN AVERAGE OF 34% OVER THE NEXT 12 MONTHS, AND THE MOST NOTABLE BENEFICIARIES WILL BE THESE VERTICAL INDUSTRIES: B2B SOFTWARE AND SERVICES (LEADING AT +41%), MANUFACTURING (+37%), HEALTHCARE (+29%) AND UTILITIES (LAGGING AT +20%).*

*ChangeWave Investing

ADDRESSING THE THREATS

CYBERSECURITY FRAMEWORK – DEFINITION

- ✓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. IT "PROVIDES A HIGH LEVEL TAXONOMY OF CYBERSECURITY OUTCOMES AND A METHODOLOGY TO ASSESS AND MANAGE THOSE OUTCOMES."*

* Wikipedia

ADDRESSING THE THREATS

CYBERSECURITY FRAMEWORK – NIST

Table 1: Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

* NIST, April 2018

ADDRESSING THE THREATS
CYBERSECURITY FRAMEWORK – NIST

Function	Category	Subcategory	Informative References
PROTECT (PR)			**NIST SP 800-53 Rev. 4** AT-3, IR-2, PM-13
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected	**CIS CSC** 13, 14 **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 **ISA 62443-3-3:2013** SR 3.4, SR 4.1 **ISO/IEC 27001:2013** A.8.2.3 **NIST SP 800-53 Rev. 4** MP-8, SC-12, SC-28
		PR.DS-2: Data-in-transit is protected	**CIS CSC** 13, 14 **COBIT 5** APO01.06, DSS05.02, DSS06.06 **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** SC-8, SC-11, SC-12
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	**CIS CSC** 1 **COBIT 5** BAI09.03 **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.4.4.1 **ISA 62443-3-3:2013** SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7 **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16
		PR.DS-4: Adequate capacity to ensure availability is maintained	**CIS CSC** 1, 2, 13 **COBIT 5** APO13.01, BAI04.04 **ISA 62443-3-3:2013** SR 7.1, SR 7.2 **ISO/IEC 27001:2013** A.12.1.3, A.17.2.1 **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5
		PR.DS-5: Protections against data leaks are implemented	**CIS CSC** 13 **COBIT 5** APO01.06, DSS05.04, DSS05.07, DSS06.02 **ISA 62443-3-3:2013** SR 5.2 **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4,
			A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	**CIS CSC** 2, 3 **COBIT 5** APO01.06, BAI06.01, DSS06.02 **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8 **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 **NIST SP 800-53 Rev. 4** SC-16, SI-7
		PR.DS-7: The development and testing environment(s) are separate from the production environment	**CIS CSC** 18, 20 **COBIT 5** BAI03.08, BAI07.04 **ISO/IEC 27001:2013** A.12.1.4 **NIST SP 800-53 Rev. 4** CM-2
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	**COBIT 5** BAI03.05 **ISA 62443-2-1:2009** 4.3.4.4 **ISO/IEC 27001:2013** A.11.2.4 **NIST SP 800-53 Rev. 4** SA-10, SI-7

* NIST, April 2018

ADDRESSING THE THREATS
CYBERSECURITY FRAMEWORK – NIST

CIS Control 13: Data Protection				
CIS Sub-Control	Asset Type	Security Function	Title	Descriptions
13.1	Data	Identify	Maintain an Inventory Sensitive Information	Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider.
13.2	Data	Protect	Remove Sensitive Data or Systems Not Regularly Accessed by Organization	Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.
13.3	Data	Detect	Monitor and Block Unauthorized Network Traffic	Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.
13.4	Data	Protect	Only Allow Access to Authorized Cloud Storage or Email Providers	Only allow access to authorized cloud storage or email providers.
13.5	Data	Detect	Monitor and Detect Any Unauthorized Use of Encryption	Monitor all traffic leaving the organization and detect any unauthorized use of encryption.
13.6	Data	Protect	Encrypt the Hard Drive of All Mobile Devices.	Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.
13.7	Data	Protect	Manage USB Devices	If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.
13.8	Data	Protect	Manage System's External Removable Media's Read/write Configurations	Configure systems not to write data to external removable media, if there is no business need for supporting such devices.
13.9	Data	Protect	Encrypt Data on USB Storage Devices	If USB storage devices are required, all data stored on such devices must be encrypted while at rest.

* Center for Internet Security, CIS Controls V7

ADDRESSING THE THREATS
CYBERSECURITY FRAMEWORK – NIST

CIS Control 14: Controlled Access Based on the Need to Know				
CIS Sub-Control	Asset Type	Security Function	Title	Descriptions
14.1	Network	Protect	Segment the Network Based on Sensitivity	Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).
14.2	Network	Protect	Enable Firewall Filtering Between VLANs	Enable firewall filtering between VLANs to ensure that only authorized systems are able to communicate with other systems necessary to fulfill their specific responsibilities.
14.3	Network	Protect	Disable Workstation to Workstation Communication	Disable all workstation to workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems, through technologies such as Private VLANs or microsegmentation.
14.4	Data	Protect	Encrypt All Sensitive Information in Transit	Encrypt all sensitive information in transit.
14.5	Data	Detect	Utilize an Active Discovery Tool to Identify Sensitive Data	Utilize an active discovery tool to identify all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider and update the organization's sensitive information inventory.
14.6	Data	Protect	Protect Information through Access Control Lists	Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.
14.7	Data	Protect	Enforce Access Control to Data through Automated Tools	Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.
14.8	Data	Protect	Encrypt Sensitive Information at Rest	Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.
14.9	Data	Detect	Enforce Detail Logging for Access or Changes to Sensitive Data	Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).

* Center for Internet Security, CIS Controls V7

ADDRESSING THE THREATS

DATA LOSS PREVENTION (DLP)– DEFINITION

- ✓DATA LOSS PREVENTION (DLP) IS A SET OF TOOLS AND PROCESSES USED TO ENSURE THAT SENSITIVE DATA IS NOT LOST, MISUSED, OR ACCESSED BY UNAUTHORIZED USERS.*

* digitalguardian.com

ADDRESSING THE THREATS

DATA LOSS PREVENTION (DLP)

- ✓ISACA'S DATA LEAK PREVENTION WHITE PAPER IDENTIFIES THREE KEY OBJECTIVES FOR A DLP SOLUTION:
  - ❖LOCATE AND CATALOG SENSITIVE INFORMATION STORED THROUGHOUT THE ENTERPRISE. (IDENTIFY)
  - ❖MONITOR AND CONTROL THE MOVEMENT OF SENSITIVE INFORMATION ACROSS ENTERPRISE NETWORKS. (DETECT)
  - ❖MONITOR AND CONTROL THE MOVEMENT OF SENSITIVE INFORMATION ON END-USER SYSTEMS. (PROTECT)*

* https://www.isaca.org/KnowledgeCenter/Research/Documents/Data-Leak-Prevention_whp_Eng_0910.pdf

ADDRESSING THE THREATS

DATA LOSS PREVENTION (DLP)

✓THE WHITE PAPER PROVIDES GUIDELINES FOR IMPLEMENTING DLP. THESE GUIDELINES ARE:

- ❖DATA CLASSIFICATION SHOULD BE THE FIRST STEP OF THE PROGRAM.
- ❖DEFINE AND IMPLEMENT DATA CLASSIFICATION AND PROTECTION POLICIES.
- ❖IMPLEMENT AND CONFIGURE DLP SOLUTIONS PER POLICY.
- ❖IDENTIFY AND MONITOR THE RISK ASSOCIATED WITH LIMITATIONS OF DLP SOLUTIONS IN PROTECTING THE ORGANIZATION'S DATA.

ADDRESSING THE THREATS

DATA LOSS PREVENTION (DLP)

✓THREE PRIMARY STATES OF DATA ARE:

- ❖DATA AT REST (ID, LOCATE, LOG)
- ❖DATA IN MOTION (MONITORING NETWORK TRAFFIC)
- ❖DATA IN USE (ENDPOINTS)

ADDRESSING THE THREATS

BUSINESS BENEFITS OF DLP

- ✓PROTECT CRITICAL BUSINESS DATA & INTELLECTUAL PROPERTY
- ✓IMPROVE COMPLIANCE
- ✓REDUCE DATA BREACH RISK
- ✓ENHANCE TRAINING & AWARENESS
- ✓IMPROVE BUSINESS PROCESSES
- ✓OPTIMIZE DISK SPACE & NETWORK BANDWIDTH
- ✓DETECT ROGUE/MALICIOUS SOFTWARE

CONTACT INFORMATION

BOB MARCAVAGE

CIO – SUNSTONE CONSULTING LLC

BOBMARCAVAGE@SUNSTONECONSULTING.COM

RMARCAVAGE@GMAIL.COM

HTTPS://WWW.LINKEDIN.COM/IN/MARCAVAGE/

717.433.6006

Endnotes and Web Links…

"Mistakes Happen – Mitigating Unintentional Data Loss", Michael Van Stone, CISA, CISSP, CPA, and Ben Halpert, ISACA Journal, Vol 1, 2018

"Information is beautiful", Founded by David McCandless, http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

"Protecting Data in the Healthcare Industry", An Osterman Research White Paper, July 2017

"GrandCrab, Saturn, and Data Keeper: 3 New Ransomware-as-a-Service Platforms Gaining Steam", https://blog.barkly.com/gandcrab-saturn-data-keeper-ransomware-as-a-service-2018

"5 ransomware Trends to Watch in 2018", Allan Liska, https://www.recordedfuture.com/ransomware-trends-2018/

"Symantec ISTR April 2018", https://www.symantec.com/security-center/threat-report

"Framework for Improving Critical Infrastructure Cybersecurity", Version 1.1, National Institute of Standards and Technology, April 2018

"CIS Controls Version 7". Center for Internet Security

Advisera Expert Solutions Ltd, Punit Bhatia, https://advisera.com/eugdpracademy/knowledgebase/a-summary-of-10-key-gdpr-requirements/

ChangWave 451 Alliance, ChangeWave Weekly Update, http://www.changewave.com/

"What is Data Loss Prevention (DLP)?, Ellen Zhang, https://digitalguardian.com/blog/what-data-loss-prevention-dlp-definition-data-loss-prevention

ISACA Journal, Volume 6, 2017, Sunil Bakshi, Help Source, https://www.isaca.org/Journal/archives/2017/Volume-6/Pages/helpsource.aspx