


☐

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

6/1/2018

PROTECTION CRIMINAL DDOS PHISHING ATTACK  SunStone Consulting

GROUPS HACKING FIREWALL MALWARE

CYBERCRIME

COMPUTER INFECTED TROJAN VIRUS

NETWORK DIGITAL DETECTION

HACKER INTERNET INTRUDER SPYWARE SPAM

☐

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.

*Virus 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

*Adressa Expert Solutions, PuntBlauw

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-leaks/>

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-leaks/>

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.informationweek.com/11/2016/01/26/quest-diagnostic-data-breach-backdoor/

DATA BREACH EXAMPLES (CONT)

✓PENALTY...

- ❖ACTIONS STILL PENDING

✓PREVENTION...

- ❖PATCH AND UPDATE SERVERS, REVIEW APPLICATIONS FOR POSSIBLE SECURITY ISSUES

*http://www.informationweek.com/11/2016/01/26/quest-diagnostic-data-breach-backdoor/

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.informationweek.com/11/2016/01/26/quest-diagnostic-data-breach-backdoor/

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.informationweek.com/194442
 x830m/194442/194442-Data-Breach-Examples/

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.informationweek.com/194442
 x830m/194442/194442-Data-Breach-Examples/

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.informationweek.com/194442
 x830m/194442/194442-Data-Breach-Examples/

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.informationweek.com/healthcare/2014/05/24/healthcare-cloud-systems-are-on-the-rise/

WHERE ARE WE GOING?

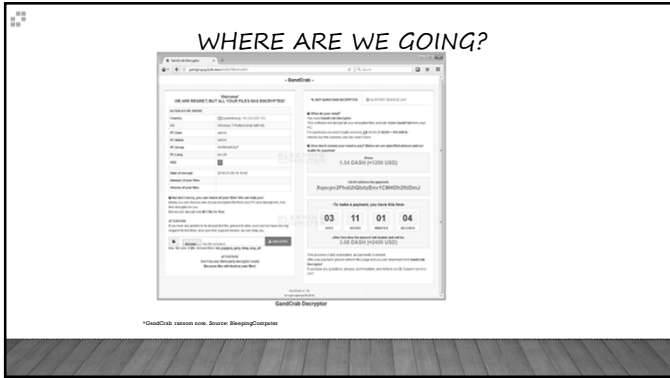
✓ ISSUES...

- ❖ 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?

✓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

April 16, 2018 Cybersecurity Framework Version 1.1

Table 6. Function and Category Objectives Identifiers

Function	Category	Objective	Control
Identify	Asset	CA-100	Asset Management
		CA-101	Business Processes
		CA-102	Resources
		CA-103	Risk Assessment
		CA-104	Risk Management Strategy
	System	CA-105	Supply Chain Risk Management
		CA-106	System Management and Assessment
		CA-107	Incidents and Events
		CA-108	Information Protection Processes and Procedures
		CA-109	Information Security
Protect	Data	PR-100	Privacy Technology
		PR-101	Encryption and Decryption
		PR-102	Security of Information
		PR-103	System and Information Integrity
		PR-104	System and Information Integrity
	Equipment	PE-100	Equipment Planning
		PE-101	Equipment and Component Acquisition
		PE-102	Equipment and Component Maintenance
		PE-103	Equipment and Component Disposal
		PE-104	Equipment and Component Security
Personnel	PS-100	Management	
	PS-101	Incident Response	
	PS-102	Recovery Planning	
	PS-103	Incident Response	
	PS-104	Continuity	

* NIST, April 2018

ADDRESSING THE THREATS CYBERSECURITY FRAMEWORK - NIST

April 16, 2018 Cybersecurity Framework Version 1.1

Table 7. Control Objectives

Control Objective	Control Objective Description	Control Objective Reference
CA-100	Asset Management	CA-100
CA-101	Business Processes	CA-101
CA-102	Resources	CA-102
CA-103	Risk Assessment	CA-103
CA-104	Risk Management Strategy	CA-104
CA-105	Supply Chain Risk Management	CA-105
CA-106	System Management and Assessment	CA-106
CA-107	Incidents and Events	CA-107
CA-108	Information Protection Processes and Procedures	CA-108
CA-109	Information Security	CA-109
PR-100	Privacy Technology	PR-100
PR-101	Encryption and Decryption	PR-101
PR-102	Security of Information	PR-102
PR-103	System and Information Integrity	PR-103
PR-104	System and Information Integrity	PR-104
PE-100	Equipment Planning	PE-100
PE-101	Equipment and Component Acquisition	PE-101
PE-102	Equipment and Component Maintenance	PE-102
PE-103	Equipment and Component Disposal	PE-103
PE-104	Equipment and Component Security	PE-104
PS-100	Management	PS-100
PS-101	Incident Response	PS-101
PS-102	Recovery Planning	PS-102
PS-103	Incident Response	PS-103
PS-104	Continuity	PS-104

* NIST, April 2018

ADDRESSING THE THREATS CYBERSECURITY FRAMEWORK - NIST

April 16, 2018 Cybersecurity Framework Version 1.1

Table 8. CIS Control 13: Data Protection

CIS Sub-Control	Asset Type	Security Function	Title	Description
13.1	Data	Identify	Maintain an Inventory of Sensitive Information	Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located inside or at a service provider's premises.
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 special access systems (operational needs for the network) by the business and needing to occasionally use the system or completely unclassified and powered off and need not.
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 Systems' External Removable Media's Hardware 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
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

"GrandCrah, Saturn, and Data Keeper: 3 New Ransomware-as-a-Service Platforms Gaining Steam", <https://blog.hackyr.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/evgdpracademy/knowledgebase/a-summary-of-10-key-gdpr-requirements/>

ChangeWave 4SI 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>
