Topic: Bringing Methodology Back to Cyber Security

Date: 13 June 2018 Time: 10:10-10:50AM, PST

Location: https://caecommunity.zoom.us/my/caeforum (Login as “Guest” & enter your name. No password needed.)

Audience: All levels

Presenter(s): Stacey Lee-Curbean, University of Maryland University College

Description: Technological advancements have made it easy for users to provide all types of information that is stored and retrievable on demand; however, this ease can make us susceptible to the malicious intent of others. Whether you create an account to access content from a website, make an online purchase, or provide social media comments, once submitted this information can’t be recalled. In many cases, the information that we provide is stored redundantly. So, is there such a thing as a total “Delete”? Though we can’t erase our digital footprint, it is our responsibility to learn how others capture, manage, store, deliver, and preserve the information that we provide. We must become champions of our cyberspace destiny; not just yours, but for the generations to come.

Structured documents are databases

Unstructured documents are images and videos

Information can be collected without your consent

Collection of contents in apps

Whenever you log-in.

Tech advancements

Smart Devices

Allows collection of data

Social media

Allows collection and storing of data

*Looking up a product in a website, then advertisement in FB pops up related to the product lookup.*

*Content can be bought and sold*

*IoT is a huge network of connected devices*

*Devices include = tablets, cellphones, refrigerators, wearables, jet engines*

*IoT produces an enormous amount of data*

*Hacking on the toaster.*

*Military was tracked thru wearable – not secure*

Digital Footprint

Passive footprint

* Time-based
* Logged in to compete a specific activity
* Examples: Amazon, Macys

Active Footprint

* Continuous
* Logged in continuously; not necessarily to complete a specific activity
* Examples: Facebook, Twitter, LinkedIn, SnapChat, eHarmony, Blogs, YouTube, Email

*Make sure your online portrait is accurate, because many employers use your profile.*

*Or school or security clearances.*

*So we have to be careful what we post, or what we affiliate with.*

Content management lifecycle

* Begins when data is created
* Ends with destruction (from original source of collection) or permanent storage (where no longer used)

*Is content really destroyed? We don’t really know.*

Content Management Lifecycle 5 phases

* Collection
* Management
* Storage
* Delivery
* Preservation

Collection

* Website data
* Offline/CRM data
* Purchase data
* Social data
* Smart TV data
* 3rd-party data
* Mobile data

*Once Alexa is ON, it could listen.*

Management - content management is your responsibility

PII – Personally Identifiable Information

Before providing info online, find out

* What information is collected
* Why the information is being collected
* How information is shared
* Who will have access to your information

*It may be time-consuming on that privacy notice, still take once in a while to read the content.*

S – know the Source

U – Understand what private info is being collected

R - Research

E – Evaluate

Storage

* Computer
* CD/DVD
* Database/Data Warehouse
* Cloud
* Server
* Mobile and Portable Storage Devices

*When we provide content, sometimes your information is stored in a data warehouse.*

*Cloud is convenient because it can be accessed anywhere, anytime.*

Cloud Storage

* Google drive
* Dropbox
* Copy
* Yunio
* SpiderOak
* Evernote
* Mediafire
* M
* Box
* Onedrive

*Ensure have an encrypted software.*

Delivery – how the right content is delivered to the right receiver

* Paper
* Internet
* Intranet
* Email
* Mobile Device
* Fax

Preserve

* Archive – *transferring file from an active system to another for future use. i.e. lawsuit*
* Backup
* Paper

Where is your information?

* Cloud
* Messaging -> phone
* Social Media -> US server
* Financial Services -> Eurpean server
* Documents
* Online Shopping

Protecting your information

* Secure information offline
* Keep personal information in safe place
* Limit what you carry
* Lock and password protect your computers
* Safe disposal of computer and mobile devices
* Secure information online
* Encrypt data
* Use strong passwords and keep private
* Limit personal information shared on social media
* Two-factor Authentication
* Secure Devices
* Keeps devices on your person and password protected
* Use security software
* Avoid phishing emails
* Verify mobile apps before installing
* Secure laptops, mobile devices, and portable devices
* Read privacy policies
* Limit use of public Wi-Fi

*Most free public Wi-Fi doesn’t protect devices.*

*Disable Wi-Fi when not in use, sometimes it auto connects of the*

Clark:

May I suggest to use <https://duckduckgo.com/> as your search engine. This search engine doesn’t track your searches. It blocks advertiser tracking.

Clark:

How about the problem of signing in with same passwords in different websites?

How about doing the “sign in with Facebook/GitHub”?

*Not sure if it is safer, but at least I sign up individually so that other parties (i.e., Facebook or Github) can’t track.*