RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: RMG1-R09

Assessor versus Assessed Debates on PCI DSS topics

Todd Aument

Head of Data Security Governance
Square

Jacob Ansari

Senior Manager
Schellman & Company, LLC

Who are these guys?

- Shared history of performing assessments since the beginning days of PCI DSS
- Now on opposite sides of the table
  - Todd runs GRC for fast-moving fintech firm
  - Jacob still conducts and manages assessments
- Want to share our collective insights and hard-won experience with you

Rough Agenda

- Scope and applicability: the oldest argument
- Identity and access management
- Dealing with vulnerabilities

Few caveats

- We know we won't coincidentally land on your exact scenario, configuration, or scope configuration
- We're party to some of the goods on upcoming draft of PCI DSS 4.0 standard and also the relevant NDA
- We speak for ourselves and not our employers, past or present, nor PCI SSC, card brands, the White House, etc.

Here's what we can do

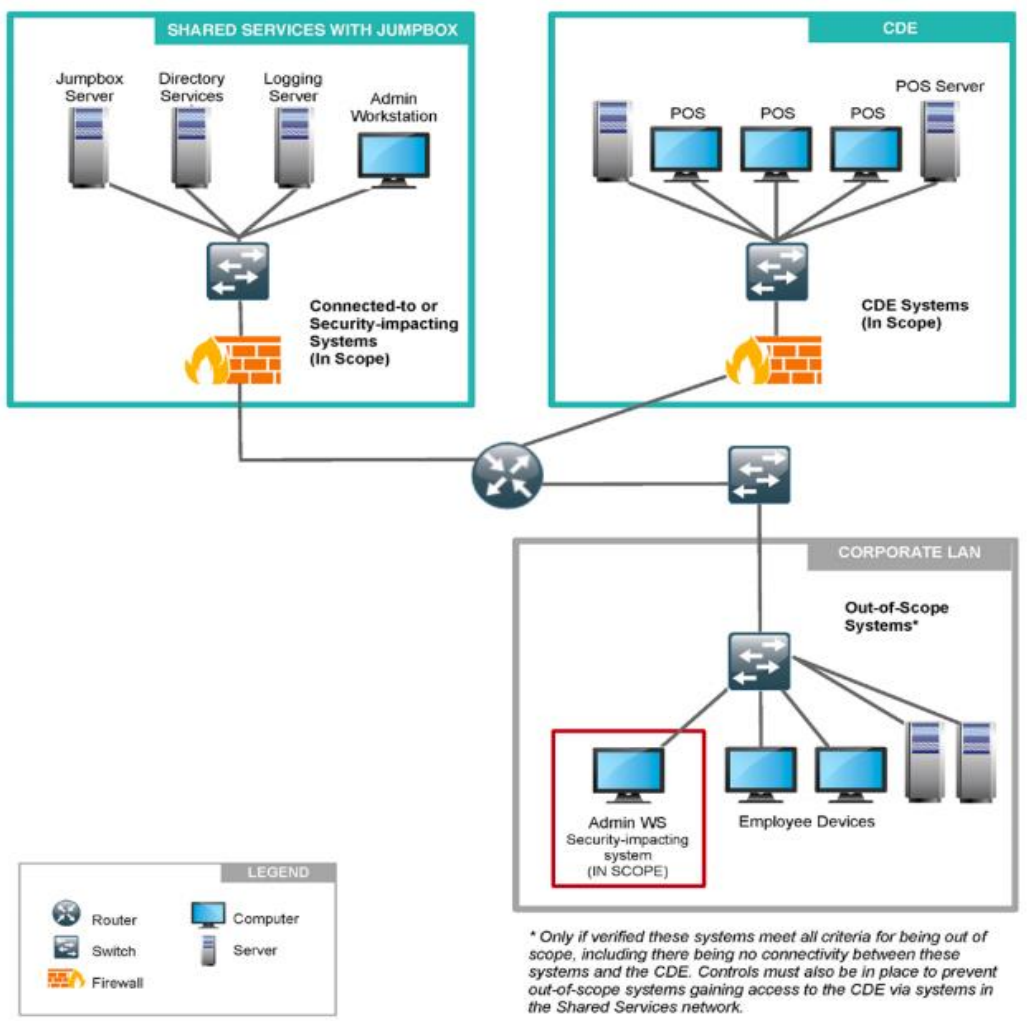
- Give you some sharpened questions to ask your teams and your assessors
- Point out some pitfalls we've encountered along the way of our journeys
- Help you break the ice on contentious topics

RSAConference2020

Scope and applicability

Want to discuss politics, religion, or scoping?

Maybe you've seen this diagram



"The PCI DSS Example Network Diagram has been extracted from the PCI SSC Information Supplement • Guidance for PCI DSS Scoping and Network Segmentation • May 2017 and appear courtesy of PCI Security Standards Council, LLC. © 2006-2020 PCI Security Standards Council, LLC. All Rights Reserved."

Scope isn’t a naughty word

- Consider the applicability of requirements to an in-scope system
- In scope means you consider it and assess it, not that you apply all requirements to it
  - Maybe some lesser set of requirements apply

RSAConference2020

Identity and Access Management

Hello?

Is it me you're looking for?

I can see it
your eyes

I can see it in
your smile

You're all I've
ever wanted

(and) my arms
are open wide

'Cause you know
just what to say

And you know
just what to do

And I want to
tell you so much

I love you

'Cause I wonder
where you are

And I wonder
what you do

Are you somewhere
feeling lonely

Or is someone
loving you?

Tell me how to
win your heart

For I haven't got
a clue

But let me start
by saying

I love you

Are you somewhere feeling lonely?

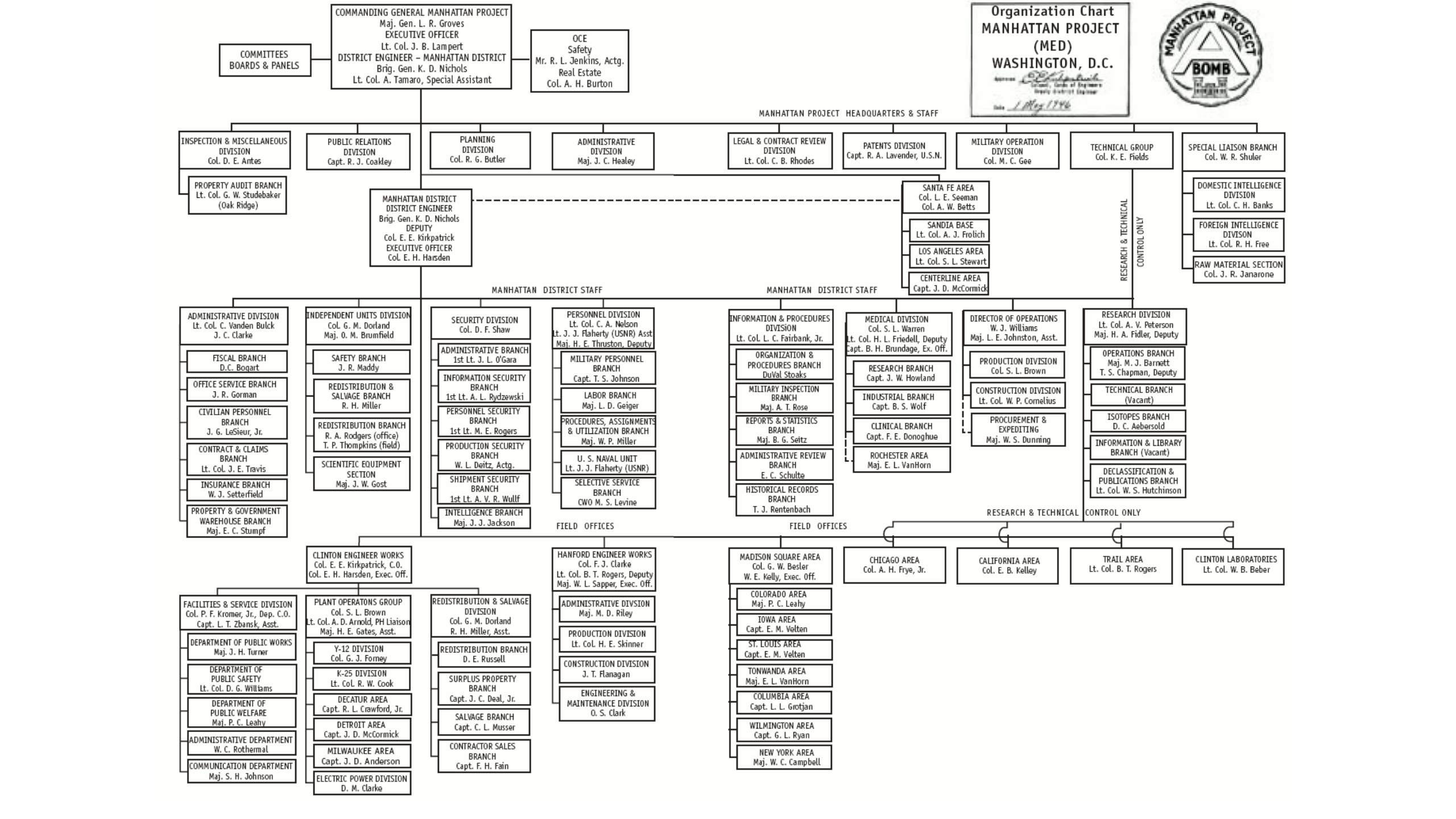
NIST 800-63B: "Do not require that memorized secrets be changed arbitrarily (e.g., periodically) unless there is a user request or evidence of authenticator compromise."

PCI DSS v3.2.1: "Change user passwords/passphrases at least once every 90 days."

DISCUSS.

Service accounts and friends

- Current version of DSS doesn’t give you much to work with
- Categorize your accounts:
  - Service
  - Default
  - Emergency access
- Control access to credentials:
  - Password vault
  - Alert on use
  - Change password values after use


Organization Chart
MANHATTAN PROJECT
(MED)
WASHINGTON, D.C.
1 May 1946
MANHATTAN PROJECT
BOMB
COMMANDING GENERAL MANHATTAN PROJECT
Maj. Gen. L. R. Groves
EXECUTIVE OFFICER
Lt. Col. J. B. Lampert
DISTRICT ENGINEER – MANHATTAN DISTRICT
Brig. Gen. K. D. Nichols
Lt. Col. A. Tamaro, Special Assistant
COMMITTEES BOARDS & PANELS
OCE
Safety
Mr. R. L. Jenkins, Actg.
Real Estate
Col. A. H. Burton
MANHATTAN PROJECT HEADQUARTERS & STAFF
INSPECTION & MISCELLANEOUS DIVISION
Col. D. E. Antes
PROPERTY AUDIT BRANCH
Lt. Col. G. W. Studebaker
(Oak Ridge)
PUBLIC RELATIONS DIVISION
Capt. R. J. Coakley
PLANNING DIVISION
Col. R. G. Butler
ADMINISTRATIVE DIVISION
Maj. J. C. Healey
LEGAL & CONTRACT REVIEW DIVISION
Lt. Col. C. B. Rhodes
PATENTS DIVISION
Capt. R. A. Lavender, U.S.N.
MILITARY OPERATION DIVISION
Col. M. C. Gee
TECHNICAL GROUP
Col. K. E. Fields
SPECIAL LIAISON BRANCH
Col. W. R. Shuler
DOMESTIC INTELLIGENCE DIVISION
Lt. Col. C. H. Banks
FOREIGN INTELLIGENCE DIVISON
Lt. Col. R. H. Free
RAW MATERIAL SECTION
Col. J. R. Janarone
MANHATTAN DISTRICT
DISTRICT ENGINEER
Brig. Gen. K. D. Nichols
DEPUTY
Col. E. E. Kirkpatrick
EXECUTIVE OFFICER
Col. E. H. Harsden
SANTA FE AREA
Col. L. E. Seeman
Col. A. W. Betts
SANDIA BASE
Lt. Col. A. J. Frolich
LOS ANGELES AREA
Lt. Col. S. L. Stewart
CENTERLINE AREA
Capt. J. D. McCormick
RESEARCH & TECHNICAL CONTROL ONLY
MANHATTAN DISTRICT STAFF
ADMINISTRATIVE DIVISION
Lt. Col. C. Vanden Bulck
J. C. Clarke
FISCAL BRANCH
D.C. Bogart
OFFICE SERVICE BRANCH
J. R. Gorman
CIVILIAN PERSONNEL BRANCH
J. G. LeSieur, Jr.
CONTRACT & CLAIMS BRANCH
Lt. Col. J. E. Travis
INSURANCE BRANCH
W. J. Setterfield
PROPERTY & GOVERNMENT WAREHOUSE BRANCH
Maj. E. C. Stumpf
INDEPENDENT UNITS DIVISION
Col. G. M. Dorland
Maj. O. M. Brumfield
SAFETY BRANCH
J. R. Maddy
REDISTRIBUTION & SALVAGE BRANCH
R. H. Miller
REDISTRIBUTION BRANCH
R. A. Rodgers (office)
T. P. Thompkins (field)
SCIENTIFIC EQUIPMENT SECTION
Maj. J. W. Gost
SECURITY DIVISION
Col. D. F. Shaw
ADMINISTRATIVE BRANCH
1st Lt. J. L. O'Gara
INFORMATION SECURITY BRANCH
1st Lt. A. L. Rydzewski
PERSONNEL SECURITY BRANCH
1st Lt. M. E. Rogers
PRODUCTION SECURITY BRANCH
W. L. Deitz, Actg.
SHIPMENT SECURITY BRANCH
1st Lt. A. V. R. Wulff
INTELLIGENCE BRANCH
Maj. J. J. Jackson
PERSONNEL DIVISION
Lt. Col. C. A. Nelson
Lt. J. J. Flaherty (USNR) Asst
Maj. H. E. Thruston, Deputy
MILITARY PERSONNEL BRANCH
Capt. T. S. Johnson
LABOR BRANCH
Maj. L. D. Geiger
PROCEDURES, ASSIGNMENTS & UTILIZATION BRANCH
Maj. W. P. Miller
U. S. NAVAL UNIT
Lt. J. J. Flaherty (USNR)
SELECTIVE SERVICE BRANCH
CWO M. S. Levine
MANHATTAN DISTRICT STAFF
INFORMATION & PROCEDURES DIVISION
Lt. Col. L. C. Fairbank, Jr.
ORGANIZATION & PROCEDURES BRANCH
DuVal Stoaks
MILITARY INSPECTION BRANCH
Maj. A. T. Rose
REPORTS & STATISTICS BRANCH
Maj. B. G. Seitz
ADMINISTRATIVE REVIEW BRANCH
E. C. Schulte
HISTORICAL RECORDS BRANCH
T. J. Rentenbach
MEDICAL DIVISION
Col. S. L. Warren
Lt. Col. H. L. Friedell, Deputy
Capt. B. H. Brundage, Ex. Off.
RESEARCH BRANCH
Capt. J. W. Howland
INDUSTRIAL BRANCH
Capt. B. S. Wolf
CLINICAL BRANCH
Capt. F. E. Donoghue
ROCHESTER AREA
Maj. E. L. VanHorn
DIRECTOR OF OPERATIONS
W. J. Williams
Maj. L. E. Johnston, Asst.
PRODUCTION DIVISION
Col. S. L. Brown
CONSTRUCTION DIVISION
Lt. Col. W. P. Cornelius
PROCUREMENT & EXPEDITING
Maj. W. S. Dunning
RESEARCH DIVISION
Lt. Col. A. V. Peterson
Maj. H. A. Fidler, Deputy
OPERATIONS BRANCH
Maj. M. J. Barnett
T. S. Chapman, Deputy
TECHNICAL BRANCH
(Vacant)
ISOTOPES BRANCH
D. C. Aebersold
INFORMATION & LIBRARY BRANCH
(Vacant)
DECLASSIFICATION & PUBLICATIONS BRANCH
Lt. Col. W. S. Hutchinson
RESEARCH & TECHNICAL CONTROL ONLY
FIELD OFFICES
CLINTON ENGINEER WORKS
Col. E. E. Kirkpatrick, C.O.
Col. E. H. Harsden, Exec. Off.
FACILITIES & SERVICE DIVISION
Col. P. F. Kromer, Jr., Dep. C.O.
Capt. L. T. Zbansk, Asst.
DEPARTMENT OF PUBLIC WORKS
Maj. J. H. Turner
DEPARTMENT OF PUBLIC SAFETY
Lt. Col. D. G. Williams
DEPARTMENT OF PUBLIC WELFARE
Maj. P. C. Leahy
ADMINISTRATIVE DEPARTMENT
W. C. Rothermal
COMMUNICATION DEPARTMENT
Maj. S. H. Johnson
PLANT OPERATONS GROUP
Col. S. L. Brown
Lt. Col. A. D. Arnold, PH Liaison
Maj. H. E. Gates, Asst.
Y-12 DIVISION
Col. G. J. Forney
K-25 DIVISION
Lt. Col. R. W. Cook
DECATUR AREA
Capt. R. L. Crawford, Jr.
DETROIT AREA
Capt. J. D. McCormick
MILWAUKEE AREA
Capt. J. D. Anderson
ELECTRIC POWER DIVISION
D. M. Clarke
REDISTRIBUTION & SALVAGE DIVISION
Col. G. M. Dorland
R. H. Miller, Asst.
REDISTRIBUTION BRANCH
D. E. Russell
SURPLUS PROPERTY BRANCH
Capt. J. C. Deal, Jr.
SALVAGE BRANCH
Capt. C. L. Musser
CONTRACTOR SALES BRANCH
Capt. F. H. Fain
FIELD OFFICES
HANFORD ENGINEER WORKS
Col. F. J. Clarke
Lt. Col. B. T. Rogers, Deputy
Maj. W. L. Sapper, Exec. Off.
ADMINISTRATIVE DIVSION
Maj. M. D. Riley
PRODUCTION DIVISION
Lt. Col. H. E. Skinner
CONSTRUCTION DIVISION
J. T. Flanagan
ENGINEERING & MAINTENANCE DIVISION
O. S. Clark
MADISON SQUARE AREA
Col. G. W. Besler
W. E. Kelly, Exec. Off.
COLORADO AREA
Maj. P. C. Leahy
IOWA AREA
Capt. E. M. Velten
ST. LOUIS AREA
Capt. E. M. Velten
TONWANDA AREA
Maj. E. L. VanHorn
COLUMBIA AREA
Capt. L. L. Grotjan
WILMINGTON AREA
Capt. G. L. Ryan
NEW YORK AREA
Maj. W. C. Campbell
CHICAGO AREA
Col. A. H. Frye, Jr.
CALIFORNIA AREA
Col. E. B. Kelley
TRAIL AREA
Lt. Col. B. T. Rogers
CLINTON LABORATORIES
Lt. Col. W. B. Beber

RSAConference2020

Vulnerability Management


tag cloud of tech service
providers hit by
ransomware
in 2019 would go here,
but our lawyers told us no.

How I learned to stop worrying and love scanning

- You may always have vulnerabilities show up in your scan results
- How long does a vulnerability stick around in your organization?
- More priority for applying fixes to software components

Variations on the theme

- Lots of pentest-like options available
- Consider the sort of testing that gives you results with the clearest picture of what an attacker could do (even if they're the most damning)
- What meets Requirement 11.3? What achieves other things?

Sounds like marriage counseling

- Plan your strategic conversations now
  - Figure out your ongoing communication
- Changes to environment and scope implications
  - Start discussing with the other party now
- Sustainability and Maturity
  - How do you demonstrate your mature understanding of risk?