Sonoma Valley Hospital

Cybersecurity Challenges

July 2021

Sabrina Kidd & Jane Wong

Sonoma Valley Hospital

- SVH is a full-service acute care district hospital located in the city of Sonoma, CA providing compassionate care to the 42,000 residents of the Sonoma Valley Health Care District.
- 24 acute care beds (18 medical-surgical + 6 ICU)
  - 1 hospitalist on duty
  - 1 ED physician on duty
  - Numerous specialist consults available
    - General & Orthopedic Surgery, Cardiology, Radiology, Lab, Physical Therapy, Wound care, Occupational Health on site
    - Neurology (stroke) and Infectious Disease via Telemedicine from UCSF
    - 27 bed skilled nursing facility on site (under contracted management)

Sonoma Valley Hospital-UCSF Affiliation

- Affiliated with UCSF in 2018
  - Focus on shared quality and best practices.
- Deepened affiliation with UCSF in 2021 to include a Management Service Agreement for Leadership
  - CEO, CFO, CMO employed by UCSF
  - Director of IT Services in process (added after Cyberattack)
- Shared telemedicine services for Infectious Disease and Neurology including medical directorships specific to SVH.

Sonoma Valley Hospital

- Funding:
  - Revenues from services
  - Parcel tax
  - Charitable bequests and donations for capital expenditures
  - 2009 GO bond ($35 Million) used to retrofit and renovate the facility to meet 2013 state disaster standards
- IT Budget:
  - Fiscal Year 2021: $3M = 5.2% of $58M Operational Expenses Budget
  - Fiscal Year 2020 (and prior) IT budget was ~500K LESS
  - Increase in budget is for security measures

University of California San Francisco

University of California, San Francisco is the leading university exclusively focused on health.

UCSF Medical Center ranks among the top 10 hospitals nationwide for the care it provides and is among the leading medical centers across all 15 specialties ranked by U.S. News & World Report.

UCSF Health includes UCSF Medical Center, UCSF Benioff Children's Hospitals in San Francisco and Oakland, the Langley Porter Psychiatric Hospital and Clinics, and the UCSF Dental Center. The health system also includes affiliations with top-tier hospitals and physician groups throughout the Bay Area to bring specialty care to patients close to home.

University of California San Francisco

- According to the 2021-2022 U.S. News & World Report rankings, UCSF was recognized as the:
  - #2 medical school in primary care
  - #4 medical school in research
  - #2 Doctor of Pharmacy program
  - #1 graduate research education in bioscience and biochemistry
  - #1 graduate research education in infectious disease, immunology, and molecular biology
  - Among top ten in its Master of Nursing, gerontology, family nursing, and mental health specialties

Constant Threat Landscape

- Devastating supply-chain attacks (SolarWinds, Accellion etc.)
- Attackers targeting systems that accommodate remote workers (Pulse Secure VPN, Citrix, etc.)
- Ransomware actors' trend toward multifaceted extortion
- Dwell time reduced – attackers break-in, deliver payload, get out
- Healthcare 3rd most targeted industry in 2020, compared to 8th in 2019

How it all started

- Unusual network activities were detected on October 11, 2020
- Ransomware note was discovered
- SVH Senior leadership was notified
- Incident Command Center protocol initiated

SONOMA VALLEY HOSPITAL
SONOMA VALLEY HEALTH CARE DISTRICT
Healing Here at Home

Containment Actions

- All computer systems were taken offline
- Hospital went on downtime protocol
- Except mammography, patient care continued with down time procedures
- Cyber security experts were engaged
- UCSF leadership helped navigate throughout the 100 days
- Engaged an external recovery team within a week
- Breach management & notification with Cyber attorney
- Cyber insurance company was notified
- Law enforcement agency was notified

SONOMA VALLEY HOSPITAL

What we know

- Started with a phishing email
- Privileged IT account was then used to gain access to other systems
- Some data was encrypted by the threat actors:
  - Shared drive
  - Fuji migration data
- Backup data was lost

Recovery & Notification Process

- Recovery:
  - Multiple teams are involved during recovery (approx. 4 months)
    - UCSF
    - External Recovery team
    - Sonoma Valley staff
    - Consultants for staff augmentation
- Notification:
  - Regulatory reporting to all government agencies
  - Impacted individuals for information breach
  - Office of Civil Rights (OCR) Audit

SONOMA VALLEY HOSPITAL
SONOMA VALLEY HEALTH CARE DISTRICT
Healing Here at Home

Moving Forward – (In Progress)

Improve internal IT processes

Periodic validation of backup

Keep up with security patches

Build a sustainable plan to avoid end of support/end of life software and hardware (desktops, network)

Implement

Multi-factor authentication with regular password changes

Secured email

Offsite backup

24 hour security monitoring (in place)

Security training/education for all staff

SONOMA VALLEY HOSPITAL
SONOMA VALLEY HEALTH CARE DISTRICT
Healing Here at Home

IT Investment in a community hospital

- Budget is small
- IT team is small (7 individuals)
- Knowledge is less deep than it should be
- Reliance on external vendors
- No dedicated cybersecurity lead/officer
- Hard to keep up with all the threat intelligence
- Balancing act
- Leverage affiliation