Oncology Consultants
Overcoming Cancer.™

“SOS”

Strategies for Surviving a Cyber Attack

-A Cybersecurity Thriller-

Alti Rahman, MHA, MBA, CSSBB

Oncology Consultants

Oncology Consultants
Overcoming Cancer.™

Disclosure of Conflicts of Interest

Alti Rahman, MHA, MBA, CSSBB has no relevant financial relationships to disclose.

Oncology Consultants
Overcoming Cancer.™

THE FULL PICTURE

Oncology Consultants
Overcoming Cancer.®

CELEBRATING 40 YEARS 1982 - 2022

Oncology Consultants is the

LARGEST

independent practice in Houston

21 PHYSICIANS

18 ADVANCE CARE PROVIDERS

15 MEDICAL CLINICS + INFUSIONS

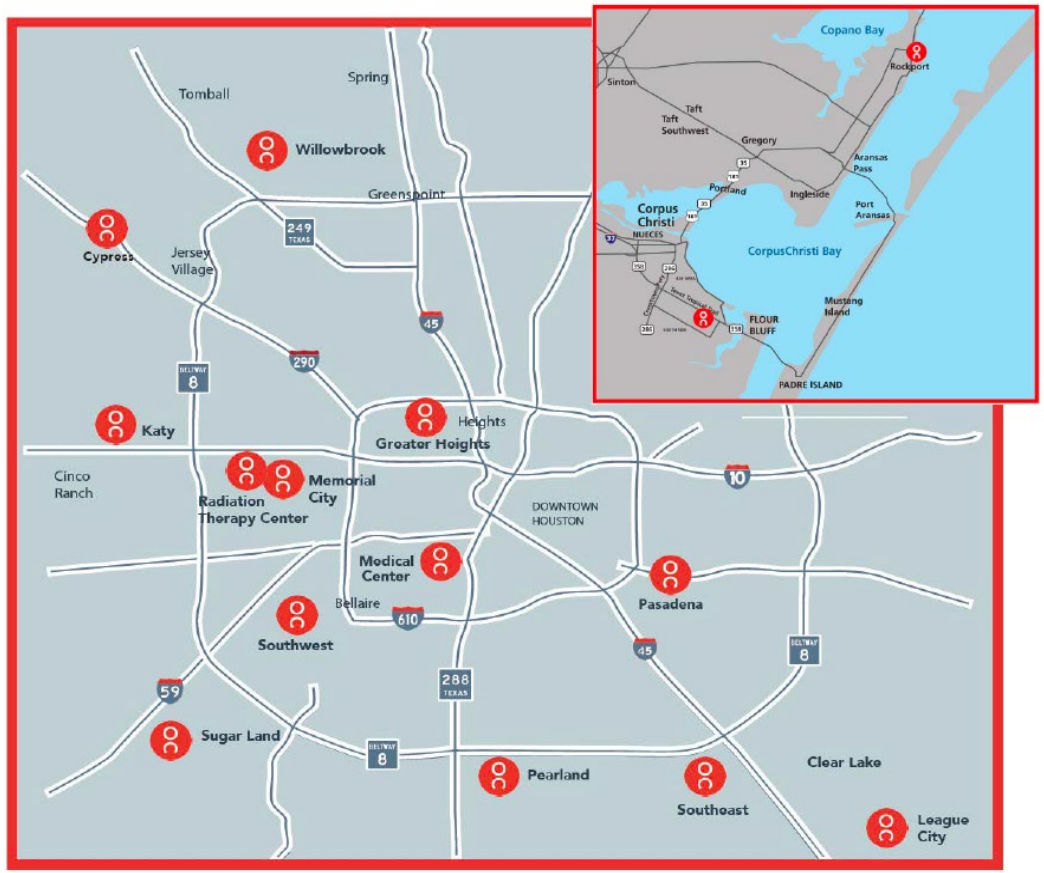
3 RETAIL PHARMACIES

3 IMAGING CENTERS

2 RADIATION CLINICS

2 RESEARCH HUBS *OVER 34 TRIALS

LOCATIONS



A little bit about me…

Education

• **CSSBB, Certified Six Sigma Black Belt** University of Houston	2012
• **MHA/MBA** University of Houston Clear Lake (UHCL) at Texas Medical Center	2010
• **BS** Psychology and Biology, Houston Baptist University	2005

Industry and Network

• COA Board of Directors	2020-Present
• President, Coalition of Hematology and Oncology Practices	2019-Present
• Director at Large, Gulf Coast Medical Group Management Association	2016-2017
• CO Chair for CAN, Community Oncology Alliance	2016-Present
• Board Member of the Oncology Circle Advisory	2016-Present
• Treasurer for the National Cancer Care Alliance (NCCA) https://nccalliance.org/	2015-Present
• Six Sigma course instructor for Medical Group Management Association (MGMA)	2014-Present
• Steering Committee Board Member for McKesson Specialty Health	
• Guest Instructor, University of Houston Clear Lake	2010-Present
• Member, American College of Healthcare Executives (ACHE)	2008-Present
• Member, Medical Group Management Association (MGMA)	2008-Present

Tales of a Cyber SecurITy Breach

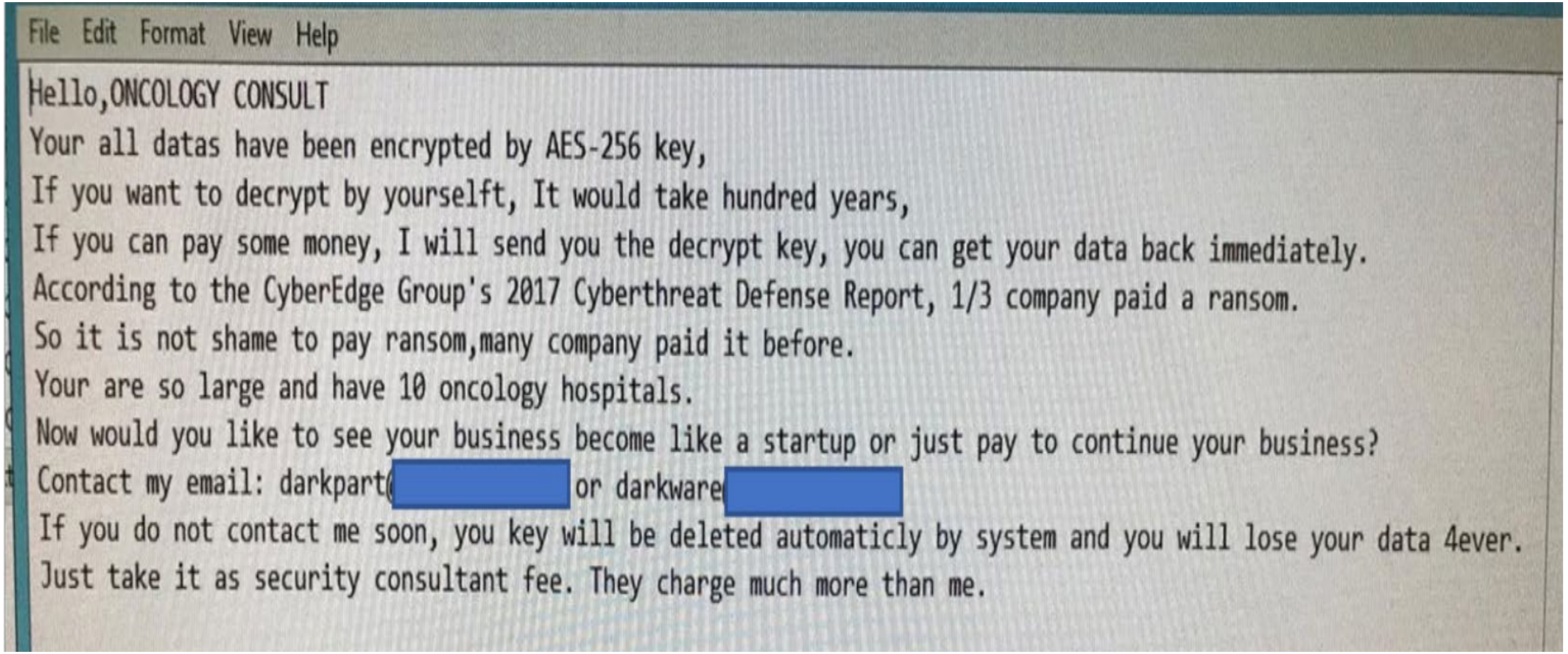
Disclaimer

I am not an Expert in Cyber Security Response, Forensics and Risk Mitigation Services. My primary IT experience is that I spent my "**adolescent"** years playing computer games and building custom computers and sold them to friends/family so I could pay for Big Mac Meals at McDonald's.

One Beautiful Monday Morning….

- Monday - June 18, 2017
- @7:30AM
  - “Hi Alti, I can not log in to my email and the pharmacy system seems to be down, do you know anything ?”
- @7:45AM
  - “Hi Alti, I can not log in to NextGen (Billing), do you know anything ?

!!!!PAY AND GET YOUR DATA BACK!!!



Immediate Impact

- Business:
  - Inability to communicate via email
  - Inability to send claims out, process payments, run reports
  - Inability to process new pharmacy prescriptions
  - Inability to access over 30 years of documents (Procedures, Spreadsheets, Power Point, Memo's, Meeting Minutes, on and on and on….)
- Patients: No impact to cloud based EMR system

Ride the Bike and Build the Bike **at the Same Time!**

- No Email
- No Billing
- No Reports
- No Pharmacy System
- No Documents

Patient Care

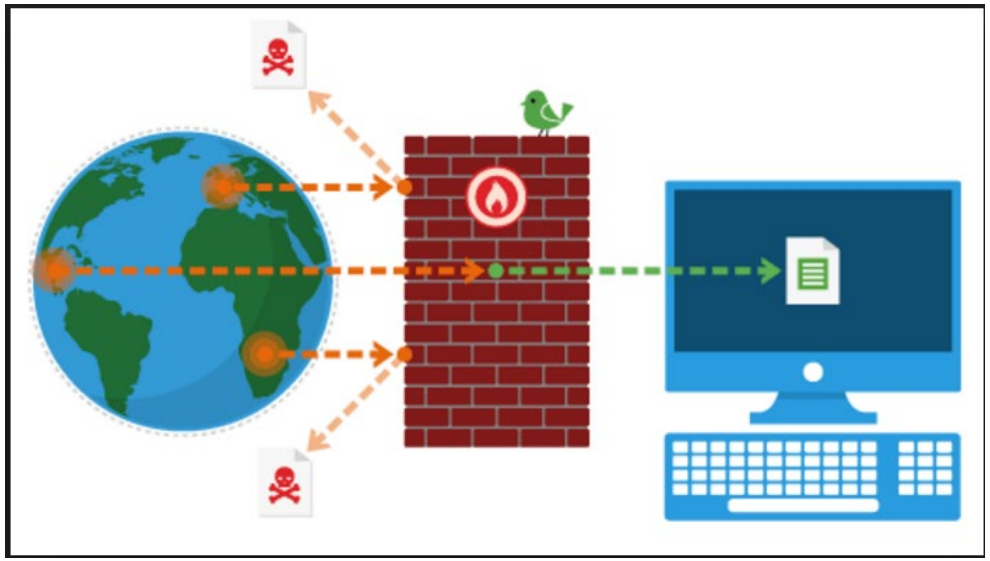
- OIG Inspection
- Breach Notification
- ……..
- Ongoing Attack
- ……..
- Meet Payroll
- ……..
- Pay Drug Invoices

Steps Taken (Short Term 1-2 weeks)

- Communications
  - Teleconference Hotline Created to received and disseminate communication to physicians and staff (updated 2-3 times per day)
  - Transition to Cloud Based email (Office 365)
- Incident Response (IR):
  - Located and retained an Incident Response Firm
  - FBI engaged
  - Legal services (OCR Response, patient notifications, HIPAA breach notification)
  - Deployment of additional Malware tools to servers, Server scans, server architecture reconfigured
- Billing
  - Transition to Clearinghouse based Billing
  - Within 2-3 days from incident response
- Software platform rebuild
  - Pharmacy software rebuild

Carbon Black

Steps Taken (Long term: 1-6 months)



- Email with Microsoft cloud services
- New Billing Platform (Centricity) hosted in the cloud, launched in 2 days
- Malware Protection (AMP)
- Improved Firewall Configurations
- Cyber Security Partnership with Firm Guardian
- Active Open Case with the FBI

Response to the Attackers: A Bad Auction

- June 19th, 2017 **$2 Million dollars** or else all data would be deleted
- August 4th, 2017 **$300,000** or else they release data to the "internet"
- August 7th, 2017, Hackers stated they sent emails to journalists and lawyers
- August 24th, 2017, **$500,000** "Final Offer", hackers stated "don't have time for you, we have new clients"
- September 13th, 2017, "we are too busy now, don't have time to leak your data, give us new offer"…."We will make time to leak data…"

Never Respond without guidance from law enforcement

We Never Paid!

Breach Notification….then came the OIG

What we Did

- Have a cybersecurity lawyer retained
- Initiate the HIPAA breach notification process
- Expect a follow up from an OIG investigator
- Expect to receive “Data Requests” with expected 1.5 week turnaround time
  - Documentation on incident dates and actions (Timeline)
  - Risk Analysis – Numerical ratings of Impact x Likelihood
  - Documentation of physical, administrative, and technical safeguards
  - Company HIPAA Policies and procedures
- Data requests will continue to be requested until OIG is satisfied with answers. OC’s investigation lasted about 10 months
- Showing willingness to cooperate and punctuality of organized/accurate request is KEY!

Interesting Statistics

- Cost of Breach can be about $408 per patient record
- $5 billion in costs
- 2019 Data Breaches
  - AMCA DATA BREACH: 25 MILLION PATIENT
  - DOMINION NATIONAL: 2.96 MILLION PATIENTS
  - INMEDIATA HEALTH GROUP: 1.5 MILLION PATIENTS
  - UW MEDICINE: 973,024 PATIENTS
  - OREGON DEPARTMENT OF HUMAN SERVICES: 645,000 PATIENTS
  - UCONN HEALTH: 326,629 PATIENTS

https://www.healthcarefinancenews.com/node/139027

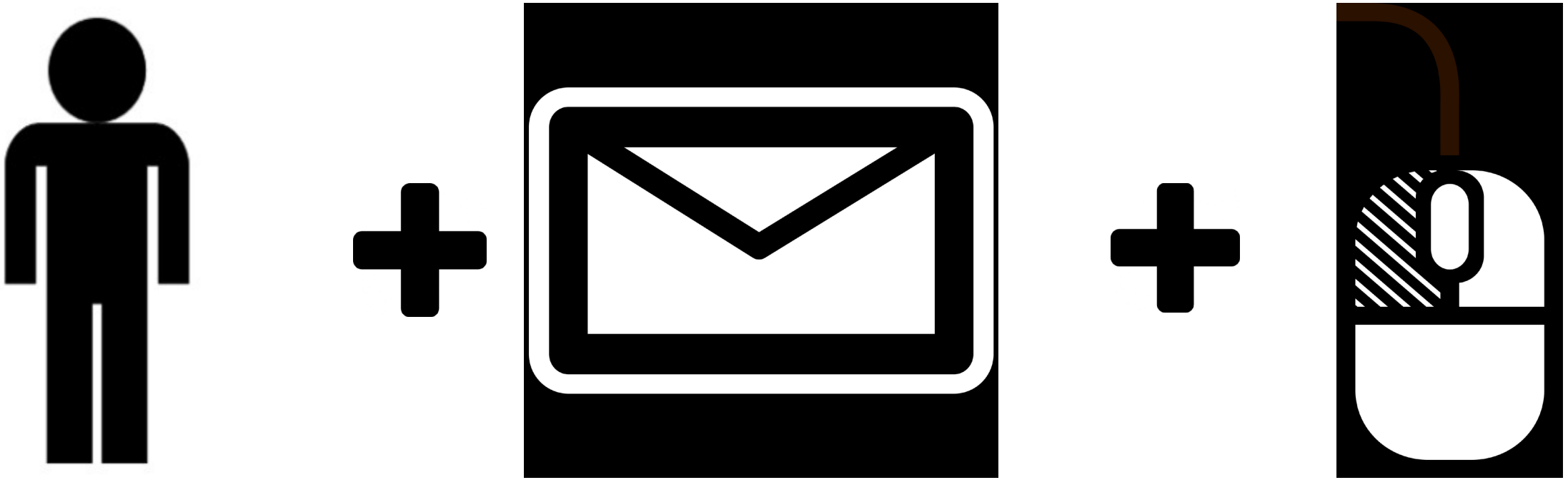
Fast Forward 6 months after Breach

- Hackers went away to attack others….
- FBI Investigation Ongoing…..
- Cyber Security PTSD for those that survived!
- Focus on Recovering AR from Legacy Systems using unaffected AR Data

It’s all about Culture

All it Takes is One….

One Person, One Email, One Click…



Total Access

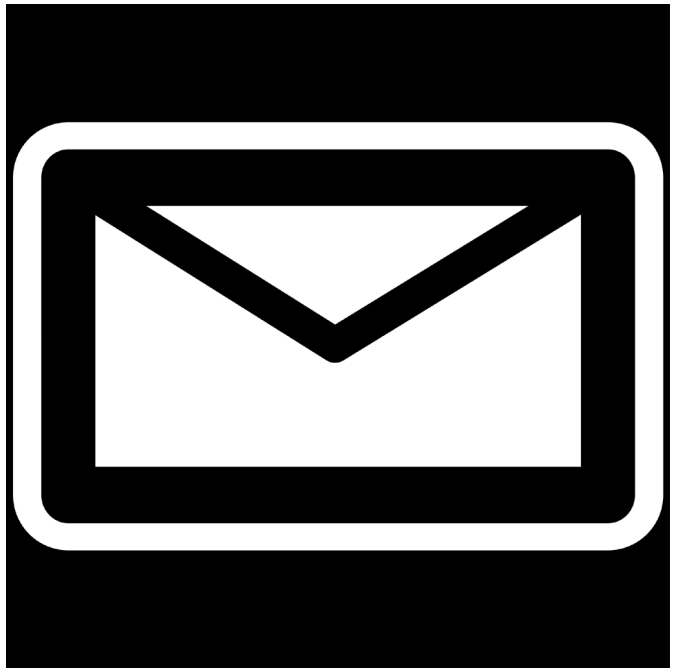
Moving Forward: It Could Happen Again

- We are not:

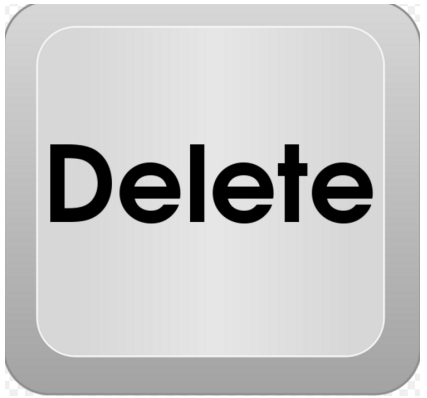
4 Steps For Enhanced Cyber Security

Step # 1, “Delete or Report”
One Person, One Email, ~~One Click~~ Delete or Report…

+



+



Step #2 – Non Work Related Internet Browsing….

-Against Employee Policy, Don't Do it-

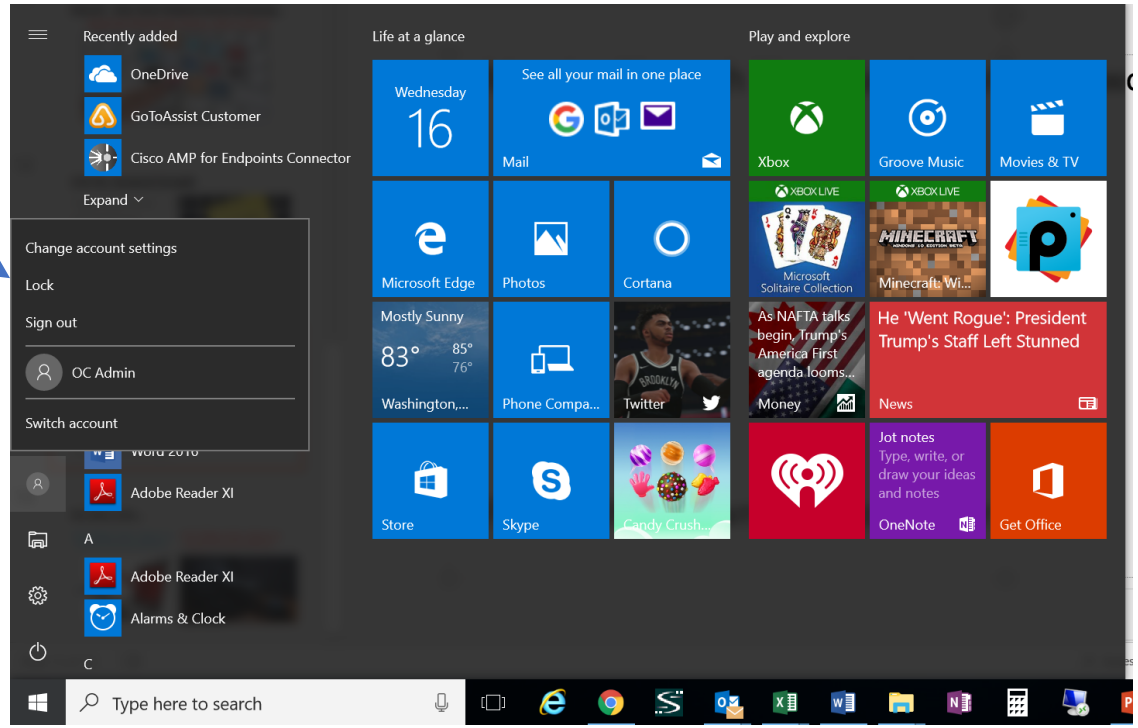
STEP #3, Password Strength

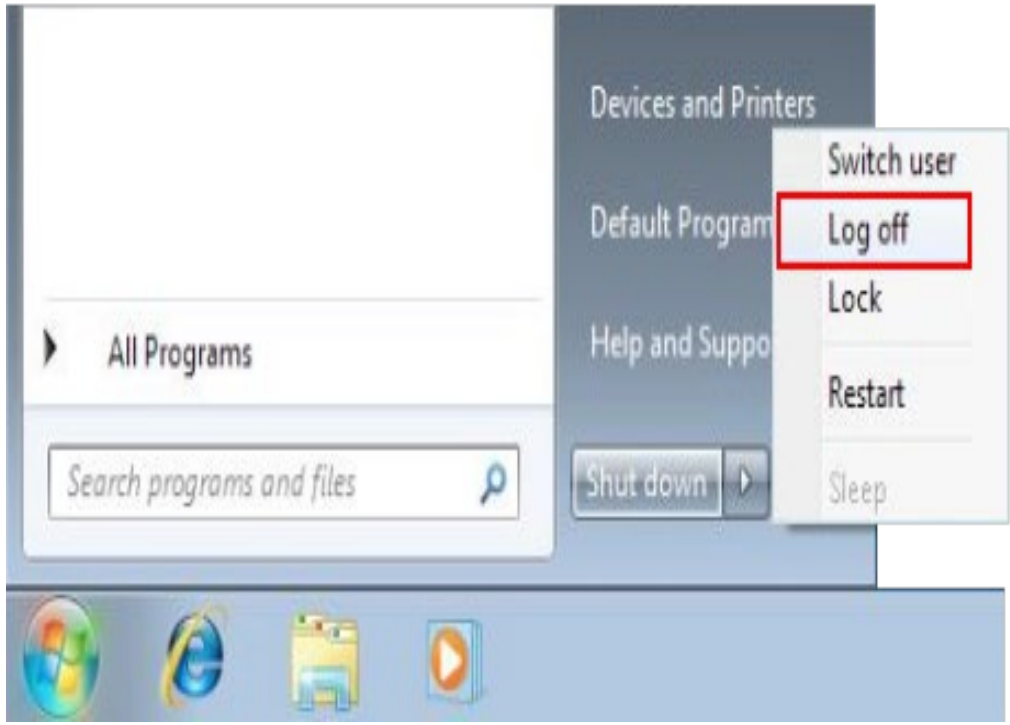
- 7 alphanumeric characters
  - (_ _ _ _ _ _ _)
- One Capitalized Letter
- One Special Character (!@#)
- IamBatman1!- Good Password
- A1234567! – Not so Good

Oncology Consultants
Overcoming Cancer.™

Step 4, Log off (Mon-Thurs), Shutdown (Friday)

- Monday Through Thursday, **Log off your workstation**





- Friday, **Shut Down your computer**

Quarterly Information Security Reviews

Cybersecurity Practices for Small Health Care Orgs

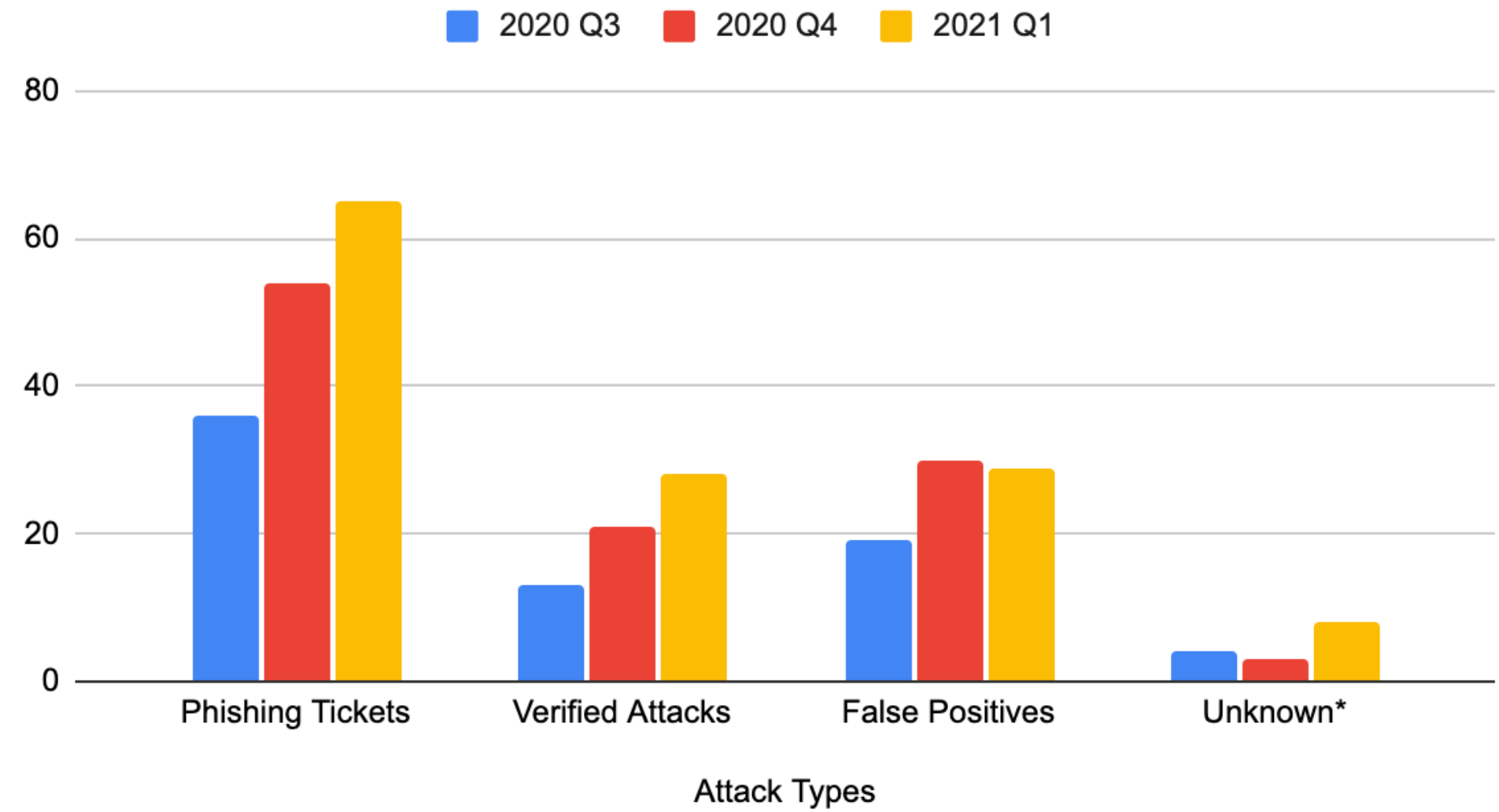
1. Email Protection Systems
2. Endpoint Protection Systems
3. Access Management
4. Data Protection and Loss Prevention
5. Asset Management
6. Network Management
7. Vulnerability Management
8. Incident Response
9. Medical Device Security
10. Cybersecurity Policies

Reference: Technical Volume 1: Cybersecurity Practices for Small Healthcare Organizations published by HHS

High Risk

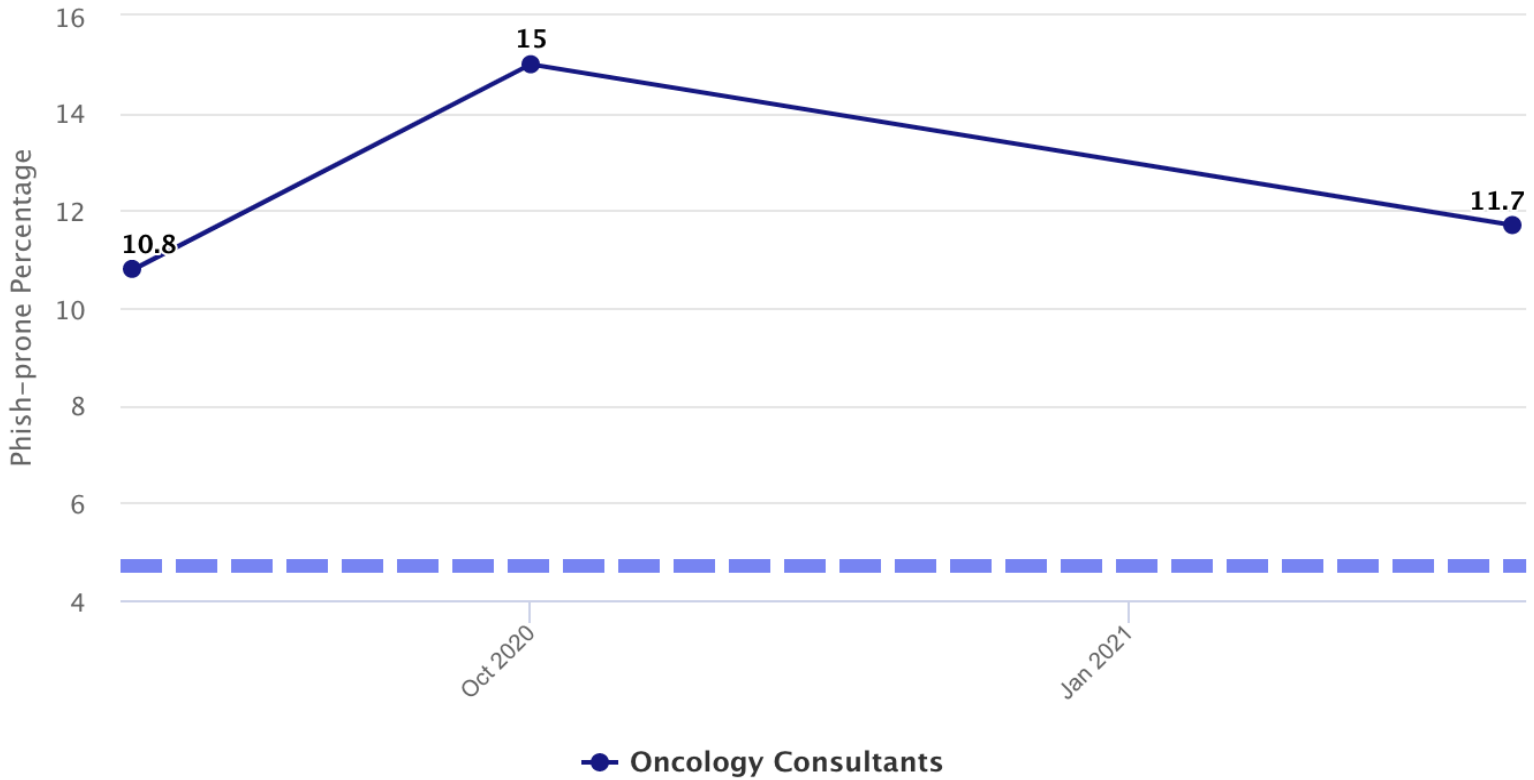
	Mitigated	Requires Attention
Email Protection	• Email security protection • Intregration of phishing campaigns and training videos.	• Email encryption (when applicable)
Vulnerability Management	• Quarterly vulnerability scans identify areas of improvement • Vulnerability Inventory within FirmGuardian's systems	• Remediation for patchable assets by end of Q3. • Un-patchable assets will require replacement.
Data Protection and Loss Prevention	• Physical Loss - Bitlocker selected for company-wide rollout	• Lack of data classification and associated policy • Lack of protection against data emailed out of company • Lack of enforcement of USB drives

Phishing Attacks - July '20 to March '21



Oncology Consultants
Overcoming Cancer.™

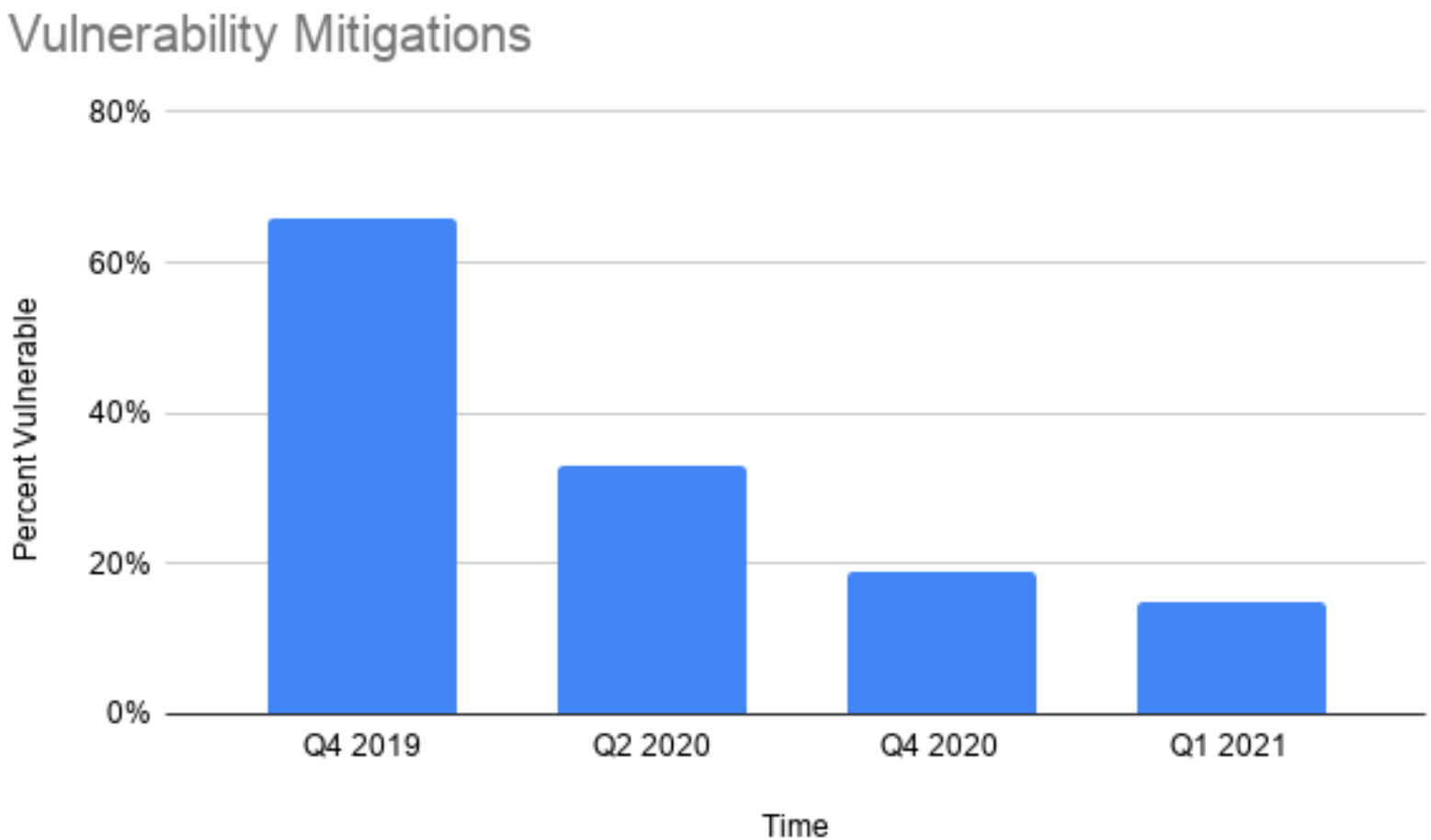
Overall Phish-prone Percentage (Selected Accounts and All Users)



Industry Benchmark Data

Most Recent Phish-prone % for All Users	12.1%
Industry Phish-prone %	4.7%

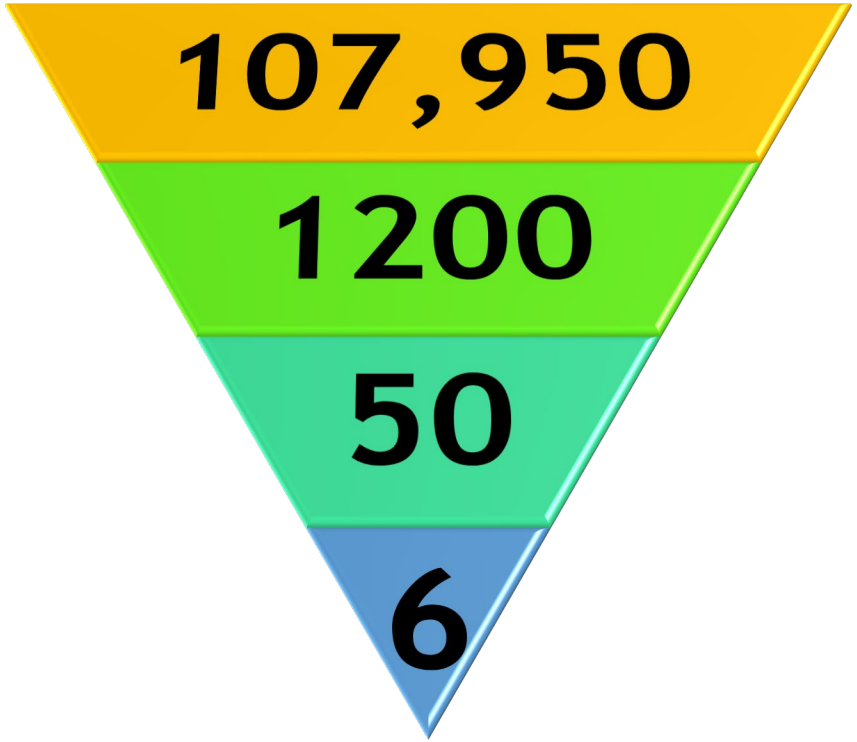
Industry	All Industries
Organization Size	Medium (250 - 1000
Program Maturity	1 Year



*Percentage of Devices where vendor support has expired

Oncology Consultants
Overcoming Cancer.™

Endpoint Security Monitoring



Alerts

Investigations

Malware Stopped

Security Risk Reports

2020 Q2 Investigations: 452 | SRR's 2

Medium Risk

	Mitigated	Requires Attention
Endpoint Protection	• All devices are loaded with Anti-malware and threat response solutions • Capable to quarantine compromised or lost devices • Can push software on to devices	• Finalize BitLocker Rollout (see chart) • Approval of Software (OpenDNS)
Network Management	• New Wireless Access Points installed at Corpus and Precision Center.	• Fundamental redesign of the network to address security and speeds • Wireless Access Points need to be replaced due to security and age. • Guest wireless not available at all sites.

Low Risk

	Mitigated	Requires Attention
Access Management	• Multifactor Authentication rolled out company wide.	• Strong password policies not in place • Lack of corporate solution for managing passwords • Lack of single sign-on options • Retire Legacy Authentication (MEDIUM RISK)
Asset Management	• Basic device inventory management in place • New custom fields being used to track additional data points	• Lack of protection from rogue plugged in devices • Need Centralized Inventory Ledger

Low Risk

	Mitigated	Requires Attention
Incident Response	• Knack website in-place to handle incidence response	• Additional workflow for incident response would benefit the process
Medical Device Security	• Providers of medical devices have established BAAs and VSAs.	• Lack of inventory and ongoing traffic monitoring of medical devices. • Need network segmentation
Cybersecurity Policies	• Code of conduct and acceptable use in place	• Additional policies need to be established and enforced: Cybersecurity Standards, System Access, Secure Communications, Device Usage, Server Backup, Two Factor Authentication

All it Takes is One….

- All it Takes is One…Person to Protect the Entire Network

- All it Takes is One…Person to Expose the Entire Network

Questions