



**STRENGTH
MATTERS®**

Financial
Management
Conference

Overcoming Cybersecurity Challenges of a Remote Workforce

Alex Santiago, Senior Associate, AAFCPAs

September 6, 2022

Brief Timeline & Relation to Cybersecurity

- Born and raised in Lawrence, MA.
 - Growing up, I learned through observation that people do bad things for many reasons
 - Taught me to remain skeptical of people's intentions
- Enlisted in the Marines in 2002 as served 11 years in aviation maintenance administration
 - Exposure to policy and procedure
 - Importance of inventory control
 - Using what you have, to make things better
- A deployment to Afghanistan is when I started to take IT and security more seriously.
 - Must keep client/server active and available at all costs

Brief Timeline & Relation to Cybersecurity

- Transferred to New Orleans in 2010.
 - Auditing. Interacting with someone who works a program and questioning them on how they do it
 - BS in Computer Information Systems, 2013
 - CompTIA Security+ certification (since expired)
- Civilian Sector – GI Bill
 - Tried for an InfoSec job first, instead worked in IT
 - I've always been "good with computers"
 - Only increased my IT security skills
 - Northeastern, GradCert in Information Security Management, 2021
 - A few months after graduation, I assumed my current role.
 - Master's student in informatics
- Reside in Boston's South End
- B&ITC IT Security Practice at AAFCPAs

CH-46E Phrog







AAFCPAs
Fenway Night
(Historical
Night, 28-5)

What is Cybersecurity?

- Even I still difficulty explaining what cybersecurity is
 - Defined by NIST as “Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.”
 - Starts with the confidentiality, integrity, and availability (CIA)
- Security is built-in to our lives
 - We practice it every day (locking doors, maintaining privacy)
 - Same concept, except it's our data and systems

Cybersecurity, Information security, or IT Security?

- Complex and cool sounding naming schemes but we're not always coding or hacking
- It's more of a disciplined approach towards working with the organization's willingness to adopt an effective cybersecurity program
 - Management holds a key to the success of an information security program
- No legal requirements to comply with specific frameworks
 - (HIPPA exception)
- Interpretation of controls left to the security pro
 - Frameworks do exist (CIS 8, NIST, etc.)

Confidentiality, Integrity, Availability

- Try to think of 1 experience in your life where CIA applied.
- We're constantly practicing these steps, but we may not realize it
- If you're able to think of an experience in your life where you used one, you're practicing cybersecurity. If you were able to connect all 3, you're a cybersecurity pro.

Remote Work. Where Were You When It Happened?

- Worked as an IT administrator when COVID first hit
 - Software company specializing in catastrophic event modeling
 - No pandemic event modeling at that time
- Unique setup with desktop computers only
 - No Work from Home
 - No laptops
- Almost overnight, we switched to Teams
 - Demonstrated the features, and functionality, and integration with M365 through user training

Remote Work. Where Were You When It Happened?

- No Laptops. All personal devices
 - Two IT workers to assist all 40 with remote connection from personal devices
- What about equipment?
 - Dual monitors
 - Webcams
 - Mouse, keyboard

Cloud Computing

- Our ability to WFH is largely due to the use of cloud computing
- Some organizations have transitioned completely to the cloud
 - AAFCPAs – No physical servers
 - AAF Clients – Consulting with transition
 - Virtual Workstations
- New security concerns with cloud computing
 - Access Control
 - Cost Management
 - Appropriate cloud storage permissions
 - Misconfigured security settings

Cloud Computing

API Name	Instance Memory	vCPUs	Windows On Demand cost	Windows SQL Std On Demand cost
c5.12	Min Mem: 0	Min vCPUs: 0	Filter..	Filter..
c5.12xlarge	96.0 GiB	48 vCPUs	\$3101.040000 monthly	\$7305.840000 monthly

<https://buckets.grayhatwarfare.com/>

Search Files

Docs / API

Top Keywords



AWS Buckets

143114 Of 443691



Azure Blobs

7960 Of 82756



Digital Ocean Spaces

1978 Of 7081



Last Update

19 Jul 2022

Cloud Computing

Date	Total	AWS 1	AWS2	AWS3	AWS4	AWS5	AWS6	AWS7	AWS8
Year to Date Total	\$ 576,150.74	\$ 70,475.32	\$ 9,157.01	\$ 32,160.07	\$ 227,737.21	\$ 195,066.88	\$ 18,930.68	\$ 14,390.89	\$ 8,232.68
Previous Month Total	\$ 105,463.66	\$ 13,840.17	\$ 836.68	\$ 3,822.09	\$ 41,021.89	\$ 41,174.68	\$ 2,495.10	\$ 1,155.58	\$ 1,117.49
Current Month to Date Total	\$ 75,938.66	\$ 9,162.47	\$ 188.67	\$ 1,576.68	\$ 46,175.29	\$ 17,778.26	\$ 545.81	\$ 284.17	\$ 227.32
45 Day Total	\$ 184,156.56	\$ 23,605.58	\$ 1,104.30	\$ 5,557.18	\$ 87,351.21	\$ 59,626.26	\$ 3,511.38	\$ 1,877.48	\$ 1,523.16
45 Day Median	\$ 938.46	\$ 207.68	\$ 21.75	\$ 40.89	\$ 30.12	\$ 222.33	\$ 94.07	\$ 17.20	\$ 25.29
45 Day Maximum	\$ 57,772.18	\$ 3,827.22	\$ 47.22	\$ 1,594.71	\$ 45,943.91	\$ 6,646.35	\$ 233.25	\$ 260.48	\$ 68.60
2021-08-10	\$ 18.05	\$ 3.88	\$ 0.27	\$ 1.09	\$ 0.88	\$ 6.58	\$ 3.63	\$ 0.48	\$ 1.25
2021-08-09	\$ 929.11	\$ 562.49	\$ 13.64	\$ 24.19	\$ 19.65	\$ 188.51	\$ 86.76	\$ 12.31	\$ 21.57
2021-08-08	\$ 1,363.32	\$ 910.56	\$ 21.76	\$ 40.83	\$ 30.32	\$ 221.90	\$ 95.65	\$ 17.10	\$ 25.19
2021-08-07	\$ 1,359.55	\$ 910.76	\$ 21.85	\$ 40.88	\$ 30.40	\$ 217.55	\$ 95.62	\$ 17.20	\$ 25.29
2021-08-06	\$ 1,431.39	\$ 910.70	\$ 21.83	\$ 40.87	\$ 30.28	\$ 215.68	\$ 95.65	\$ 91.11	\$ 25.27
2021-08-05	\$ 835.43	\$ 283.14	\$ 21.76	\$ 40.75	\$ 29.91	\$ 290.30	\$ 67.23	\$ 77.16	\$ 25.19
2021-08-04	\$ 2,086.17	\$ 807.54	\$ 21.82	\$ 40.86	\$ 30.02	\$ 1,115.54	\$ 25.33	\$ 17.17	\$ 27.90
2021-08-03	\$ 4,762.56	\$ 246.67	\$ 22.15	\$ 40.89	\$ 29.81	\$ 4,355.30	\$ 25.34	\$ 17.18	\$ 25.24

Eventually, We Settled In

- Microsoft Teams
 - Morning meetings
 - Screen sharing
 - Chats
- Equipment became available
- Routine of day-to-day remote work



Happiness Study

- Tracking Happiness surveyed 12,455 employees and asked, “if you look at your work, how would you rate your happiness on a scale from one to 10?” and “How much of your work is currently done remotely or from home?”
- Key findings from the study were
 - The ability to work remotely increases employee happiness by as much as 20%
 - Millennials are happiest when working remotely.
 - Returning to office-based work after the pandemic reduces employee happiness
 - Employee happiness decreases as commute times increase
 - Happiness at work is significantly correlated to overall life happiness

Challenges of Remote Work

- It doesn't work without internet
 - Communication
 - Teams, Zoom, Slack? How?
 - New societal norms
 - Do we turn our video on?
 - What do we wear?
 - "Let me share my screen here", "You're on mute"
 - "Please excuse my pet"
 - Privacy concerns
 - Webcam
 - Sound
 - Household members listening in on business calls
 - Do we lock our computer?
-
- Remote Connection (VPN)
 - How are you accessing corporate data?
 - Hardware requirements
 - Webcams, monitors, desks, chairs, microphones
 - Physical impact
 - My office chair was so much more comfortable, ergonomics
 - Weight gain
 - Isolation
 - Limited socialization outside of household members
 - How do we secure organizational data being accessed on personal devices?

Challenges of Remote Work

- How do we manage our remote workforce?
- How do we measure performance when we can't observe employees?
- What are the ethical implications of monitoring software?

Benefits of Remote Work

- Screen sharing
 - No one leaving fingerprints on my screen
 - Users got comfortable controlling another desktop session
- No commute
 - Gain back hours of your life
 - Some people enjoy a commute
- Less distraction
 - No outside stimulation
 - May even be more productive

Microsoft 365 / Google Workspace

- Corporate accounts can sync on personal devices
- Consider implementing a BYOD policy that enforces the use of separation on personal devices, and ensures they meet a minimum standard
- Recommend Center for Internet Security (CIS) benchmark audit

Remote Work Vulnerabilities

- You are the biggest threat to security of remote work
 - Falling for phishing
 - Using weak, shared passwords
- Endpoint weaknesses
 - In 2006, VA employee's personal laptop and external drive were stolen
 - PII for 26 million veterans
- Zoom Bombing
- Accessing corporate data on personal devices

Phishing Study

- Columbia University CS students performed a study in 2011 over the course of a year
- Performed on “4,000 unwitting students, staff, and faculty”

TABLE I

THE NUMBER OF RESPONSES FOR EACH ROUND FOR THE FIRST EXPERIMENT TO MEASURE THE USER RESPONSE TO PHONY PHISH.

Decoy Type	1 st Round	2 nd Round	3 rd Round	4 th Round
Email with internal URLs	52	2	0	NA
Email with external URLs	177	15	1	0
Forms to obtain credentials ²	39/20	4/1	0	NA
Beacon Documents	45	0	NA	NA

TABLE II

THE NUMBER OF RESPONSES FOR EACH ROUND FOR THE SECOND EXPERIMENT TO MEASURE THE USER RESPONSE TO PHONY PHISH.

Decoy Type	1 st Round	2 nd Round	3 rd Round	4 th Round
Email with internal URLs	69	7	1	0
Email with external URLs	176	10	3	0
Forms to obtain credentials	69/50	10/9	0	NA
Beacon Documents	71	2	0	NA

Bowen, B. M., Devarajan, R., & Stolfo, S. (2011, December 19). *Measuring the human factor of Cyber Security - Columbia University*. Retrieved September 7, 2022, from http://ids.cs.columbia.edu/sites/default/files/metrics_hst.pdf

Remote Availability of Communication Tools

- Communication redundancy is key. Not all eggs in 1 basket.
- If Teams is your phone, video and message application what happens if Microsoft goes down?
- Business Continuity Plans, Disaster Recovery
 - Plan for worst case scenarios
 - Test your recovery plans

Accessing with Personal Devices

- A survey of 3,000 remote office workers and IT pros conducted by CyberArk in 2020 found that
 - 77% of remote employees use unmanaged personal devices to access corporate systems
 - 93% have reused passwords across devices and applications
 - 29% admitted that they allow other members of their household to use their corporate devices for activities like schoolwork, gaming and shopping
 - 37% insecurely save passwords in browsers on their corporate devices

QR Code for
Polling
Questions



What Can We Do to be More Secure?

- Understand we are the first line of defense
- Implement an efficient InfoSec policy.
 - It starts here
- As humans, we practice security daily. Our data is quickly becoming an extension of our minds
 - Apply the same level of importance to your systems and data as you do your physical items
- Train your employees annually
- Remain vigilant and skeptical
- Secure access to operating systems
- Continue questioning of the validity of phishing emails
 - Users are good at alerting IT
 - Understand attackers are getting more sophisticated with their approach

Information Security Policy

- Foundation of your infosec program
- Establish employees responsible for infosec in your organization
- Address common areas
- Distribute to all employees and new hires
- Consider one primary policy containing relevant areas
 - Access control, data classification, awareness and training, etc.



From: Kerri Dupre <kdupre@aafcpas.com>

Sent: Friday, August 12, 2022 11:32 AM

To: Brenna Mellen <bmellen@aafcpa.com>

Subject: Response Required

*** This message originated outside our environment. Do not click any hyperlinks, respond, or open any attached files unless you have validated that the message is legitimate. ***

Hello Brenna,

I'm planning to surprise several employees with a present as a token of appreciation for their hard work and commitment, and your confidentiality would be appreciated so as not to ruin the surprise.

I will need you to make an online purchase on my behalf for Visa gift cards so they can spend it on whatever they prefer (stores, Amazon, dining, Etc.) [Here is an online store I have bookmarked](#) . I currently cannot make the purchase myself due to my busy schedule.

Email me once you get this, I am unable to take phone calls right now as I am on an important meeting.

Kind Regards,

Note: My working hours may not be the same as yours. Please do not feel obligated to reply outside of your normal work schedule

Kerrie Dupre

Board President

AAFCPAs

50 Washington Street

Westborough, MA 01581

d. 774.512.4183 | X0501 | m. 617.867.5309

[kdupre@aafcpa . com](mailto:kdupre@aafcpa.com) | [Linked In](#)

What's Out There? How Do They Do It?

- Vulnerabilities
 - OWASP Top 10
 - Qualys for External and internal
- Social Engineering
- Phishing
- Ransomware
- Brute force password cracking

2021

- A01:2021-Broken Access Control
- A02:2021-Cryptographic Failures
- A03:2021-Injection
- A04:2021-Insecure Design
- A05:2021-Security Misconfiguration
- A06:2021-Vulnerable and Outdated Components
- A07:2021-Identification and Authentication Failures
- A08:2021-Software and Data Integrity Failures
- A09:2021-Security Logging and Monitoring Failures*
- A10:2021-Server-Side Request Forgery (SSRF)*

Inventory Your Devices

- Know what systems, data, and users are in your organization
- Consider LAN Sweeper
 - Not too pricey
 - Easy to maintain
 - One of the most powerful cybersecurity tools
 - No more spreadsheets

LAN Sweeper

lansweeper

Search...

DashboardAssetsReportsSoftwareScanningHelpdeskKnowledgebaseCalendarDeploymentConfigurationEnterpriseCommunity

Asset options

New asset

New Location

Edit asset

Rescan Asset

Wake on Lan

Refresh Warranty

QR Code (JPG)

QR Code (PDF)

Create new ticket

Deploy Package

Basic actions

Ping

Pathping

Traceroute

NBTstat

HTTP

HTTPS

SSH (putty)

Telnet

Remote desktop

Open CS

Open Admin\$

Computer management

Services management

Event viewer

Shared folders

link to helpdesk

Reboot

Shutdown

Abort shutdown

Advanced actions

Device tester

Test connection

FTP

HTTP port 8080

Download more actions at Lansweeper.com

D003 - Windows 10 Pro N (64 bit)

192.168.2.103 - LS - Build Server Monitor

SummaryConfigSoftwarePerformanceUptimeLocationEvent logReportHistoryDocsCommentsScan time

Asset type: Windows

Last user: D003\lan

OS: Windows 10 Pro N (64 bit)

Build: 10.0.17134.648

Version: 1803

Domain: LS

Manufacturer: Dell Inc.

Model: OptiPlex 9020M

Memory: 8 GB DDR3

Processor: Intel Core i7-4785T CPU @ 2.20GHz

Motherboard: Dell Inc. 0Y5DDC

Graphics: Intel(R) HD Graphics 4600 1 GB

Audio: Intel(R) Display Audio

Realtek High Definition Audio

Antivirus: Windows Defender Enabled & Up To Date

Network: Intel(R) Ethernet Connection I217-LM - 98:90:96:CE:64:7C

192.168.2.103 C2960X2 10110 | GigabitEthernet1/0/10 (Gi1/0/10)

26/03/2019 12:01:03

Harddisk: C: SSD 500

212.8 GB free of 465.3 GB

Scan status:

Scan server: tst-w10-esben

State: Active

IP Location: Local Subnet - Ethernet0

Asset location: Undefined

Serial: G7YRD52

Express Code: 353-101-642-94

Uptime: 0 day(s) 5 h 9 m

First seen: 28/01/2019 16:47:39

Last seen: 26/03/2019 12:02:42

Purchased: 10/05/2015

Warranty: 11/05/2018

Custom1: production

Asset groups

Default group

production

Warranty Service

Ship date: 10/05/2015

Purchase country: Belgium

Start date	End date	Service
10/05/2015	11/05/2023	Dell Digital Delivery
10/05/2015	11/05/2018	Onsite Service After Remote Diagnosis (Consumer Customer)/ Next Business Day Onsite After Remote Diagnosis (Commercial Customer)
10/05/2015	11/05/2018	Next Business Day ProSupport

Relations

Date	Type	Asset / User	Comments
28/01/2019	Connected To	Dell Inc. 4FNJT5AQD0VS	
28/01/2019	Connected To	Philips 16843009	

Patching Your Inventory

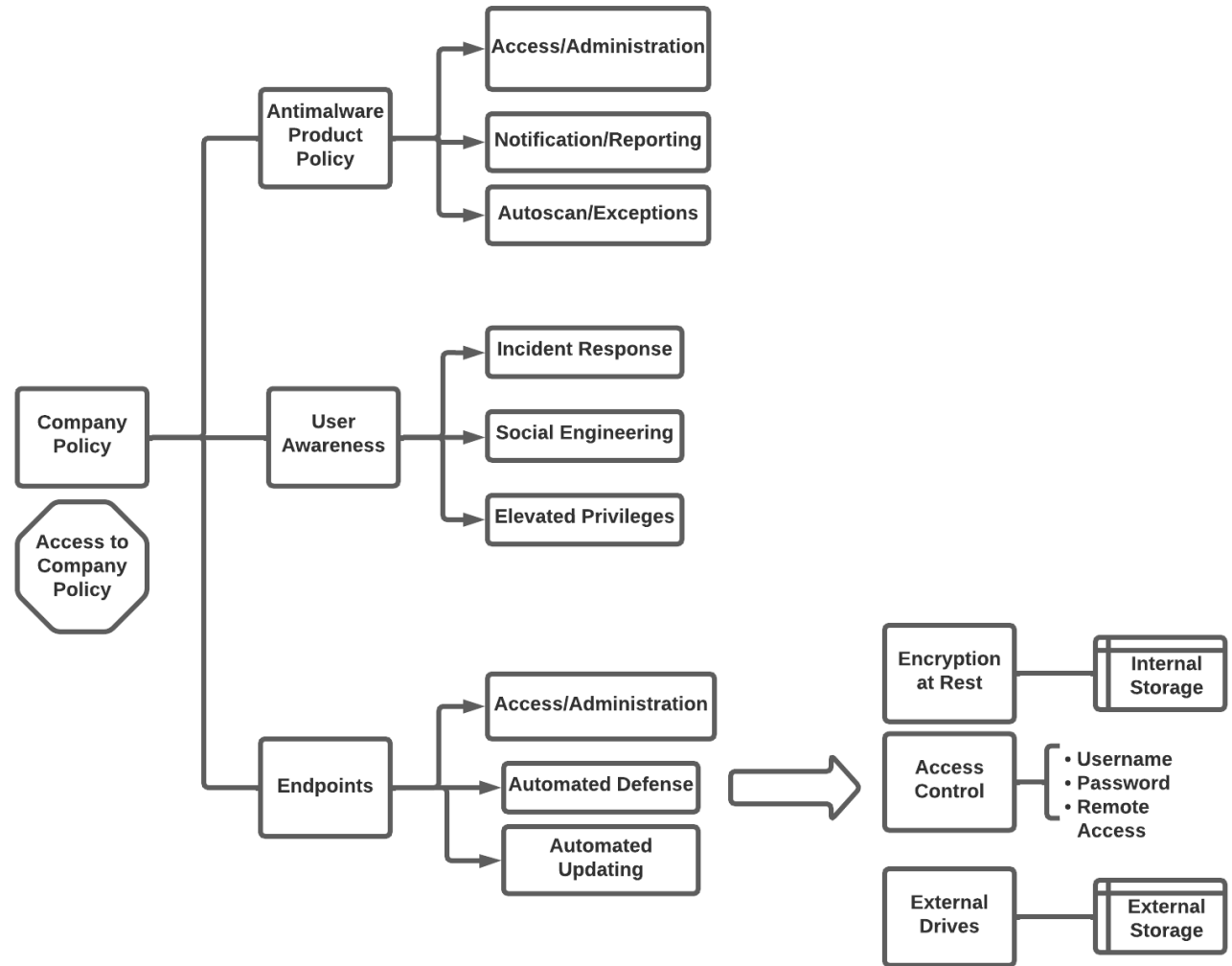
- Updates keep computers more secure and reduces risk
- Your IT team knows this is a difficult process, but a plan must be implemented
- Some of the responsibility is on the end user. If your machine is prompting to install updates, save your work and apply the patches
- Security updates address potential and confirmed vulnerabilities



Secure Your Endpoints

- Common answer to “what do you define as an endpoint?” is:
 - Anything that can access corporate data
- Antimalware
- Strong authentication
- Encryption at rest
 - Laptop hard drives can be accessed if removed

Endpoint Protection






Awareness

- Train your users on common attacks
- Train your IT staff on cybersecurity (CompTIA Security+, CISSP, Certified Ethical Hacker
 - Send them to bootcamps for cert training
- Annual training highlighting common threats

Auditing

- Start with an internal audit of your infrastructure and network
- 3rd party auditor to take an unbiased look at your systems and infrastructure
- Consider performing a CIS Controls assessment with your IT team
 - Very thorough assessment
 - Broken down by size of organization
 - Written in language non-technical people can understand
 - Visually easy to read and track
 - Will raise a lot of questions if done honestly, and correctly

CIS Controls Version 8

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
1.1	Establish and Maintain Detailed Enterprise Asset Inventory	Devices	Identify			

Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.

Penetration Testing

- Can identify weaknesses in network
- Cyber Liability insurance often asks if the client has had a pentest performed.
- Internal
- External
- WiFi

Continuous Vulnerability Scans

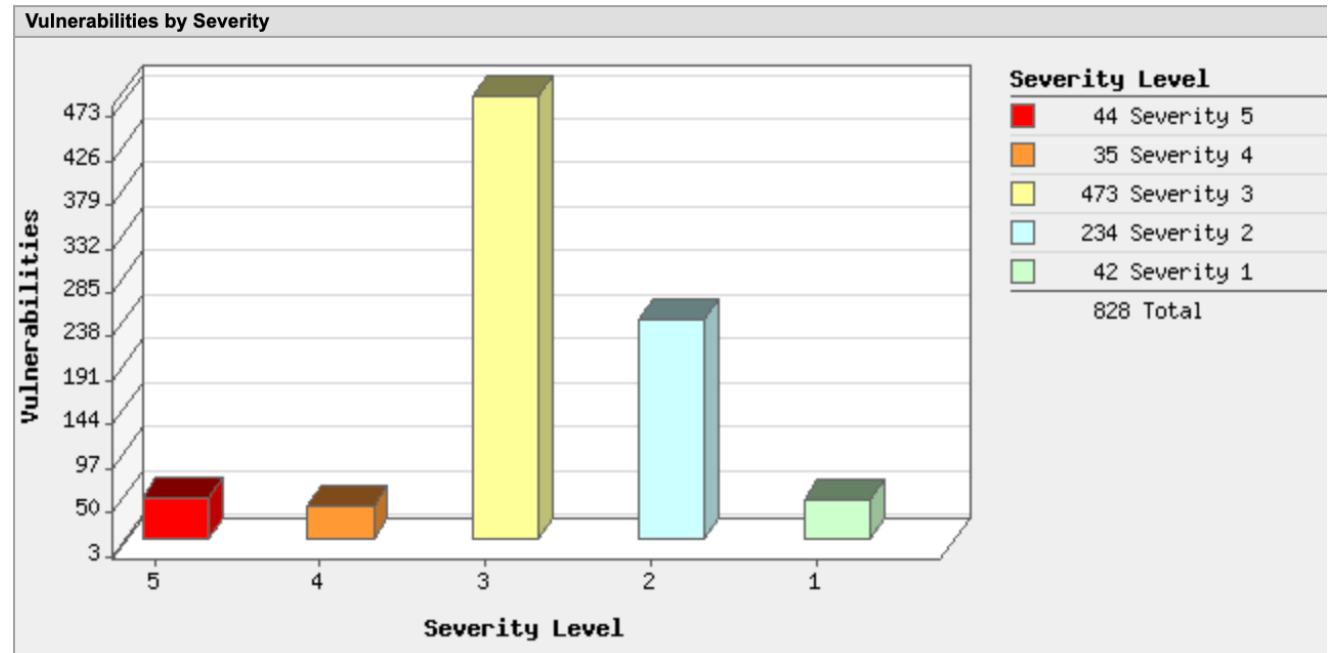
- Often, a single scan of your network is not good enough.
- Quarterly, bi-annually to stay on top of vulnerabilities discovered in your network
- Tracking progress of vulnerability remediation
 - A non-technical table provided to management
 - What vulnerabilities exist in your network and are they being remediated?

What Tools Do We Use

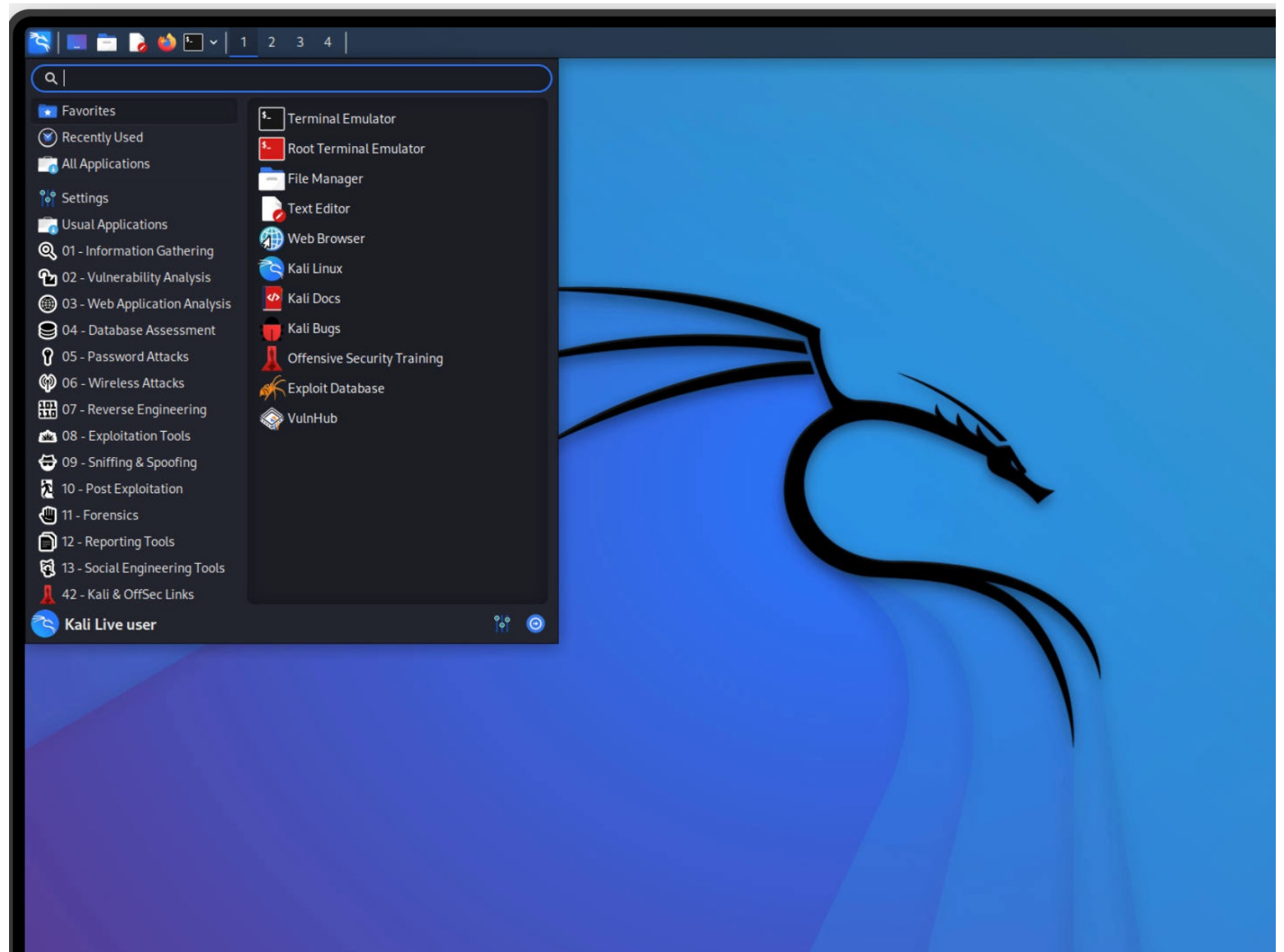
- Metasploit, Kali Linux, Qualys, Nessus Tenable
- Often, it's the determination and technological capabilities of the attacker
- Exploit vulnerabilities
- Social engineering
- People skills

Vulnerability Scanners

Internal, external, web application



Kali Linux



Wireless Hacking

- Are you using secure wireless for your corporate network
- Is there a guest network?
- Can personal devices access internal wireless network?
- WPA2 enterprise or WPA2 personal?

Social Engineering

Social Engineering Explained

Also known as human hacking, social engineering is the manipulation of someone to divulge confidential information that can be used for fraudulent purposes.



The social engineer gathers information about their victims.



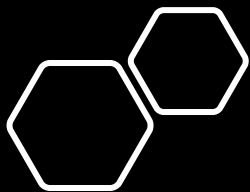
The social engineer poses as a legitimate person and builds trust with their victims.



The social engineer gathers information about their victims.



The social engineer poses as a legitimate person and builds trust with their victims.



Conclusion and Discussion

- Thanks to everyone for attending!