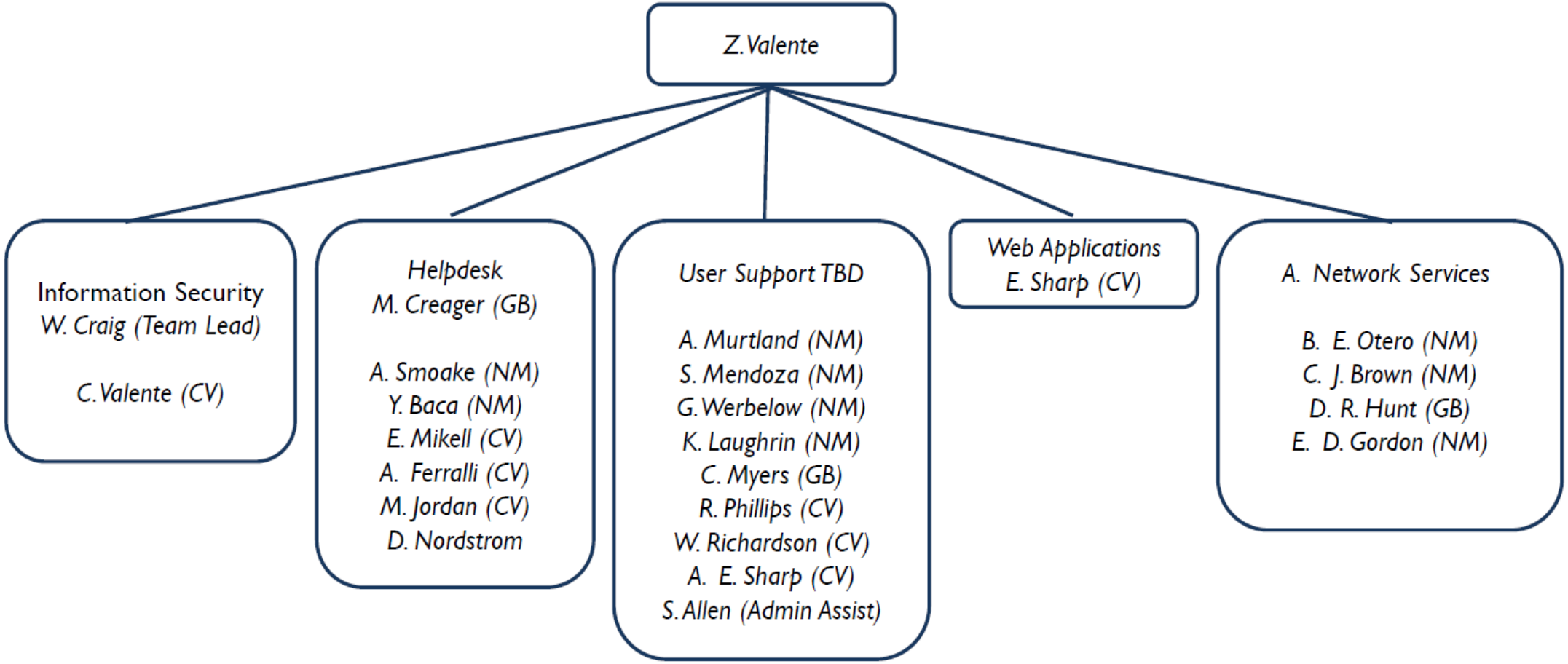
CIS Data Access & Cyber Security

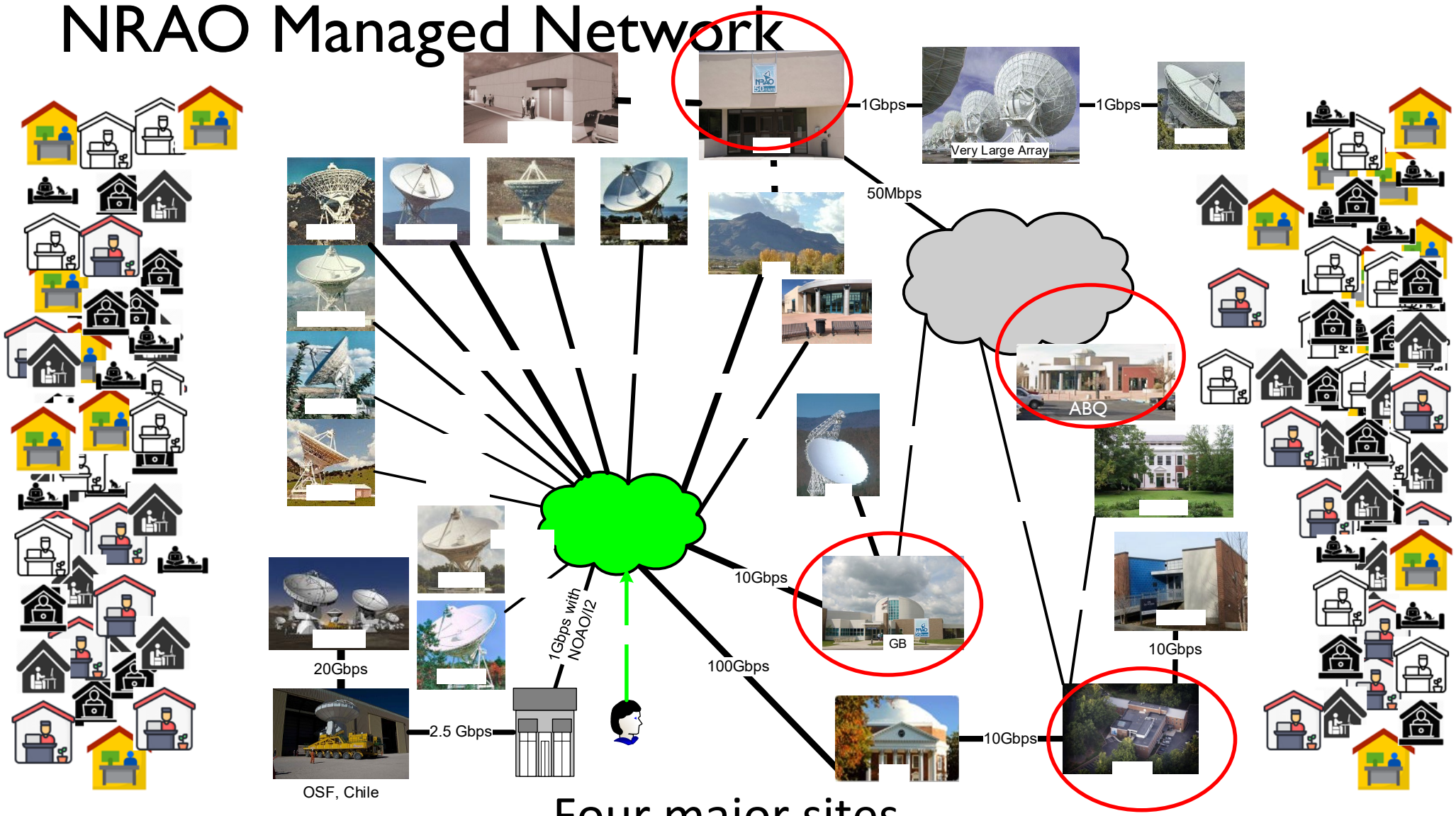
Wade Craig

Information Security Officer (NRAO/GBO)

Computer Information Services Organizational Chart



NRAO Managed Network



Four major sites

Seismic shift in employee access with telework and cloud services

What do we need to know?

- Understand that breaches will occur and will negatively impact our business
  - The goal is to minimize the blast radius
- Understand that we are a target
  - Open Science is clearly in the sights of bad actors (Gemini, ALMA)
  - Managers typically have greater levels of access and are higher value targets
- Approximately 60% of all data breaches originate from unauthorized access
  - Current or former employee or third party
- Regulatory compliance (NIST 800-171, ISO 27001, etc.) is good, but it's not enough—you need:
  - Monitoring, detection and response
  - Disaster Recovery and Business Continuity plans
- Cyber liability insurance premiums keep increasing and cover less and less

What can we do?

- Ensure that we are conducting security education and awareness training
- Conduct risk and vulnerability assessments
  - Identify gaps
  - Remediate those gaps
- Patch management
  - Roll out patches/updates ASAP
  - This often means downtime
- Ensure we have 24x7x365 monitoring, detection and response in place
- Ensure we have an appropriate Cyber Incident Response Plan and test it
- Mandate only approved devices on our network
- Mandate multifactor, encryption and principles of least privilege

Cyber Security Best Practices and Tips

- You are the #1 defense when it comes to safe computing
  - Make sure that you, and only you, are using your Observatory-issued computing equipment
- Read and adhere to the Observatory's Information Security Policies
- Do not share your passphrase/passwords with anyone
  - CIS will never ask for your passphrase, and it should be unique to the Observatory
  - Treat it like you would your debit card PIN
- Connect your Observatory-issued device to the AnyConnect VPN so it receives patches and security updates
- Don't use your @nrao.edu account for personal banking, personal websites, etc.
  - Treat it like you would company letterhead
- Don't change permissions on your (Filer) home directory!
  - Make subdirectories if you want to lock down, or open up permissions.
- No illegal file sharing – don't violate copyright
  - On our systems *OR* on our networks (your gear or ours)

Email Security

- All staff have an Exchange mailbox in the Microsoft 365 cloud.
  - For your E-mail, we utilize Exchange Online in the M365 Cloud
- Incoming Mail is thoroughly scanned
  - Mail scanned by Microsoft as well as on-premise MailScanner and SpamAssassin
  - Detected viruses are removed (quarantined) and replaced by notice
  - Likely spam (junk e-mail) is ***tagged*** ("{SPAM?}")
    - *Junk mail/SPAM is not automatically deleted and will go to your Junk folder*
- {External} tag appended to E-mail subject line if *not* originating from our network
  - AUI and JAO are "External". Tag is for *information* but helps determine phishing attacks
- Be aware of ***Phishing***
  - Don't get scammed!
  - Don't compromise your credentials!
  - Don't get your files infected or encrypted!
  - Don't trust email ***From:*** and ***To:*** fields – these are easy to forge
  - **Please ask if you have doubts!**
- Mail is a poor, inefficient, and insecure way of sharing documents
  - Use SharePoint and send a link instead! *Point* at your document, don't attach it

Threat profile: Top Attempted Exploits

These are the top attempted/blocked exploits against NRAO Infrastructure for week of January 29 – February 5, 2026

Threat	Threat Type	CVE ID	Threat Score	Threat Level	Incidents
PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	IPS	CVE-2017-9841	4,550	Critical	91
EICAR_TEST_FILE	Malware		1,950	Critical	39
Hikvision.DS.CVE-2017-7921.Authentication.Bypass	IPS	CVE-2017-7921	1,900	Critical	38
DZS.GPON.Remote.Code.Execution	IPS	CVE-2018-10561 CVE-2018-10562	1,800	Critical	36
D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution	IPS	CVE-2015-2051 CVE-2019-10891 CVE-2022-37056 CVE-2023-35723 CVE-2024-33112 CVE-2025-63932	1,800	Critical	36
NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution	IPS		1,400	Critical	28
PTZOptics.PT30X.param.Authentication.Bypass	IPS	CVE-2024-8956	1,200	Critical	24
Cisco.IOS.HTTP.Command.Execution	IPS		300	Critical	6
ThinkPHP.Controller.Parameter.Remote.Code.Execution	IPS	CVE-2019-9082 CVE-2018-20062	250	Critical	5
WordPress.HTTP.Path.Traversal	IPS	CVE-2019-9618 CVE-2022-4101 CVE-2018-16283 CVE-2018-16299 CVE-2020-11738	150	Critical	3
Apache.HTTP.Server.mod_proxy.SSRF	IPS	CVE-2021-40438	150	Critical	3
ownCloud.graphapi.GetPhpInfo.php.Information.Disclosure	IPS	CVE-2023-49103	50	Critical	1
WordPress.Plugin.Userpro.Authentication.Bypass	IPS	CVE-2017-16562	50	Critical	1
Zyxel.zhttpd.Webserver.Command.Injection	IPS		50	Critical	1
blocked-connection	Blocked by Firewall Policy		8,578,794,210	High	285,959,807
gitcdn.xyz	Malicious Websites		11,730	High	391
Apache.HTTP.Server.cgi-bin.Path.Traversal	IPS	CVE-2021-41773 CVE-2021-42013	7,140	High	249
PHP.Malicious.Shell	IPS		3,450	High	144
SystemBC.Botnet	IPS		2,040	High	68

Multiple real-time security feeds informs and pushes real-time address Blocking Policies to the Firewall. Attacking systems are subsequently automatically blocked by the firewalls.

Threat profile: Heat Map

10 second snapshot of attempted threats against the NRAO (Feb 5, 2026 at 14:45EST

QUESTIONS?