CYBERSECURITY

Cultural Change to Support the Business

Sandra E. Paul-Blanc, CISO NARA
Dr. Philip Kulp, Cybersecurity Consultant, NARA

Agenda

- Cybersecurity culture
- Layered security
- Incident Response
- Challenges with public systems
- NARA as a target
- Emerging threats
- Wrap-up

Photo by Fauzan Saari on Unsplash

Cybersecurity Culture

- Executive buy-in
- Policy for enforcement
- Cybersecurity is a process
- Continuous enhancement and maturity
- Track latest threats
- Continuous monitoring
- Confidentiality, Integrity, and Availability
- Incident Response
- Compliance is a requirement, not a goal

Layers of Protection

- Map security to the data
- Review website/application (DevSecOps)
- Email security
- Patch, patch, patch
- Secure the humans
    - Multi-factor to avoid password loss or reuse
    - Don’t assume all users require the same level security
- Secure the endpoints
    - Workstations, mobile devices

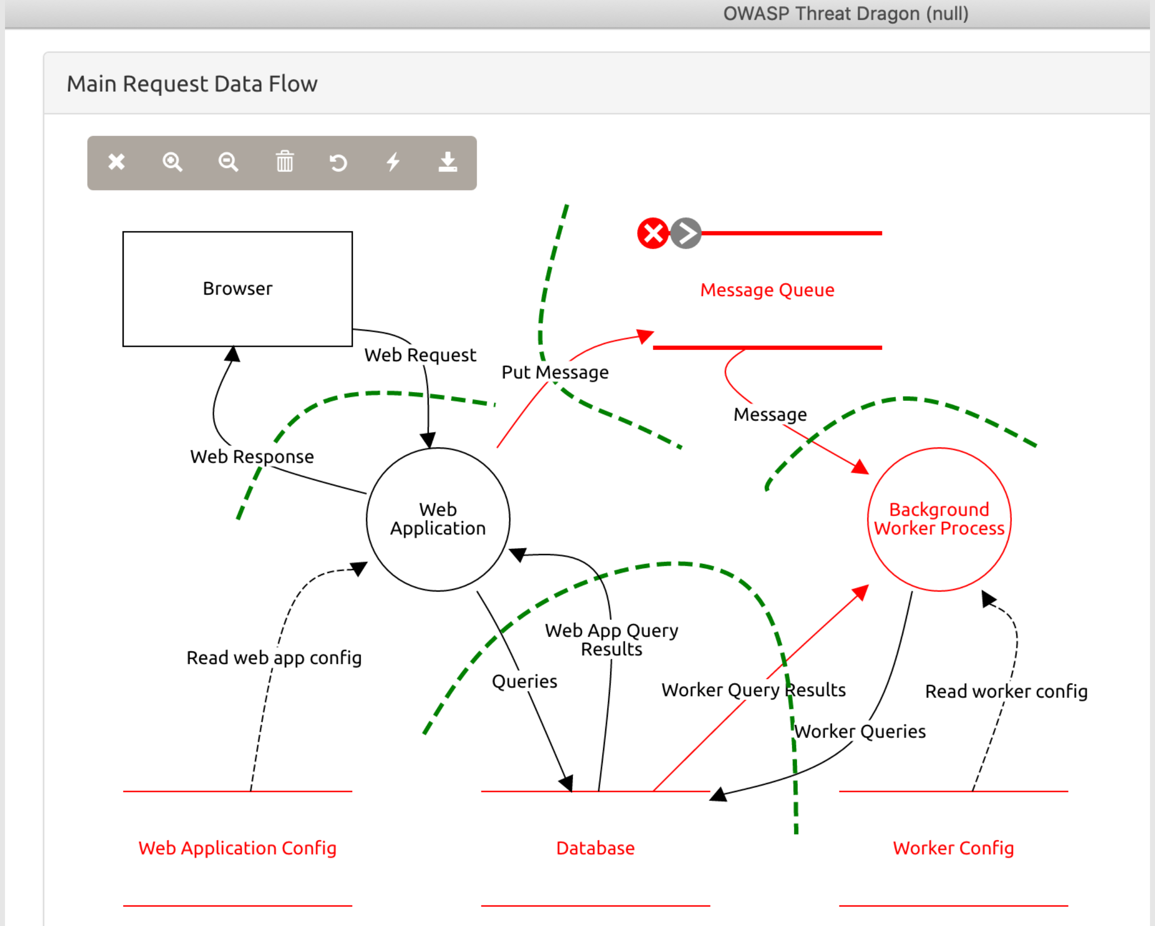
Photo by Hasan Almasi on Unsplash

Layers of Protection (cont’d)

- Secure the architecture
  - Physical, cloud, IoT
- Incident Response when things go wrong
- Don’t forget about Availability in the C,I,A triangle
  - Understand access trends
  - Load balance
- Leverage available resources
  - Establish local law enforcement, FBI contacts
  - DHS offers free services, by request only

Threat Assessment

- Enumerate applications, actors, & data
- Define trust boundaries
- Enumerate security controls
- Enumerate threats
  - Industry
  - Intelligence
- Describe gaps
- Identify mitigations



https://threatdragon.org

Security Supports Business Functions

- Understand the business
- Work with, don’t fight the business process
  - At NARA everything is a record (possibly malware)
  - Open access culture
- Find a balance for cyber hygiene
- Put effort into the greatest returns

Secure the “hardware”

- Set a policy to require compliance
  - Center for Internet Security (CIS) Benchmarks
- Maintain gold images
- Continuously test for deviations
- Internet of Things (IoT)
  - Avoid hardware with no configuration
  - Change default password, segregate
- Mobile devices
  - Limit data on foreign travel
  - Re-image after travel
  - Encrypt device
  - Whitelist apps

Photo by Obi Onyeador on Unsplash

Availability

- System and data availability
  - Know access patterns and provide enough resources
- Backups
  - Multiple methods (automated, media)
  - Segregate to avoid destruction
  - Encrypt offsite
  - Test to validate the process
- Ransomware works
  - Effective and efficient
  - New models use extortion

Email Security

- Controls to check every email
  - Block based on blacklist
  - Test attachments and links
- Outgoing email controls to protect from spoofing
- Block personal email accounts
- Outsource to cloud-based providers
  - Threat intelligence
  - Patching
  - Crowdsource protection

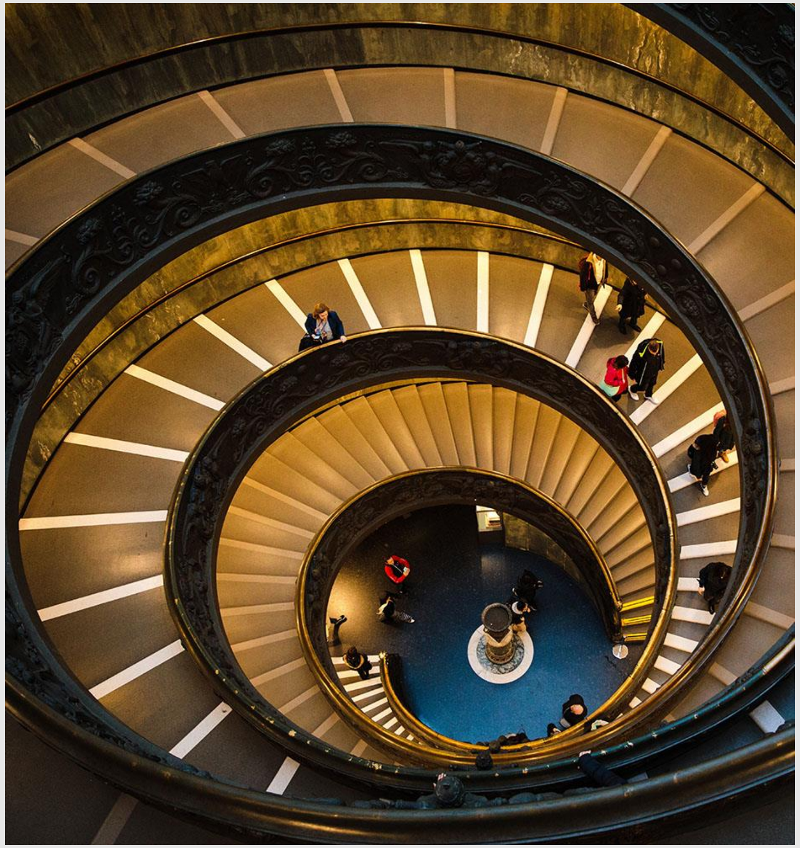


Photo by YFEI CHEN on Unsplash

Secure the Endpoints

- Basic anti-virus no longer effective (signatures)
- Behavior-based agents
- Host-based firewalls
- Application whitelisting
  - Block escalation if compromised
- Logging
  - Need information if system compromised
  - Identify lateral movement
  - Latest version of PowerShell

Secure the Humans

- Training
  - Phishing, fake websites, malicious ads, coupons
- Awareness
  - Cyber hygiene
  - Current threats
- Segregate elevated user roles
  - Administrators web browsing with privileged accounts is bad
- Successful cyberattack usually involves multiple levels of failures
  - Ransomware spread by admin credentials
  - Missing patches or other vectors for privilege escalation

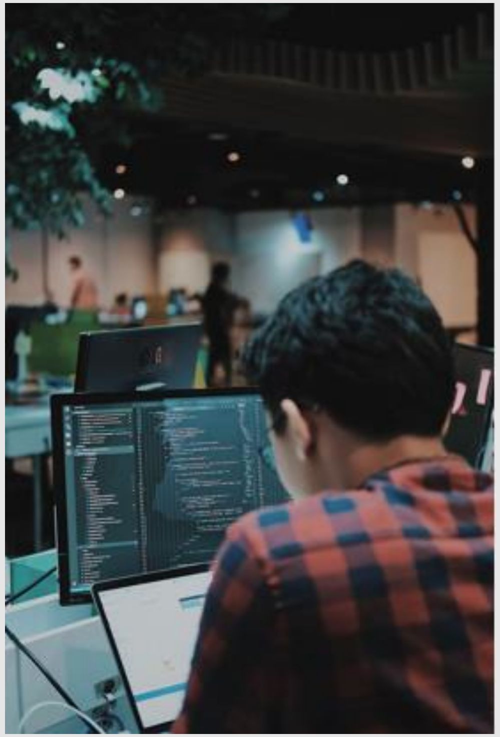


Photo by Arif Riyanto on Unsplash

Patch, Patch, Patch

- Policies for process and enforcement
- Reliable patching process
  - Monitor and validate
- Patch 3rd party software
- Monitor EOL software, hardware, operating system
- Test 3rd party libraries in custom software
- Systems must maintain support
  - Administrators, licensing, etc.

Incident Response

- Detection when controls fail
- Mitigate damage
- Train the IR personnel
- Test your IR capabilities

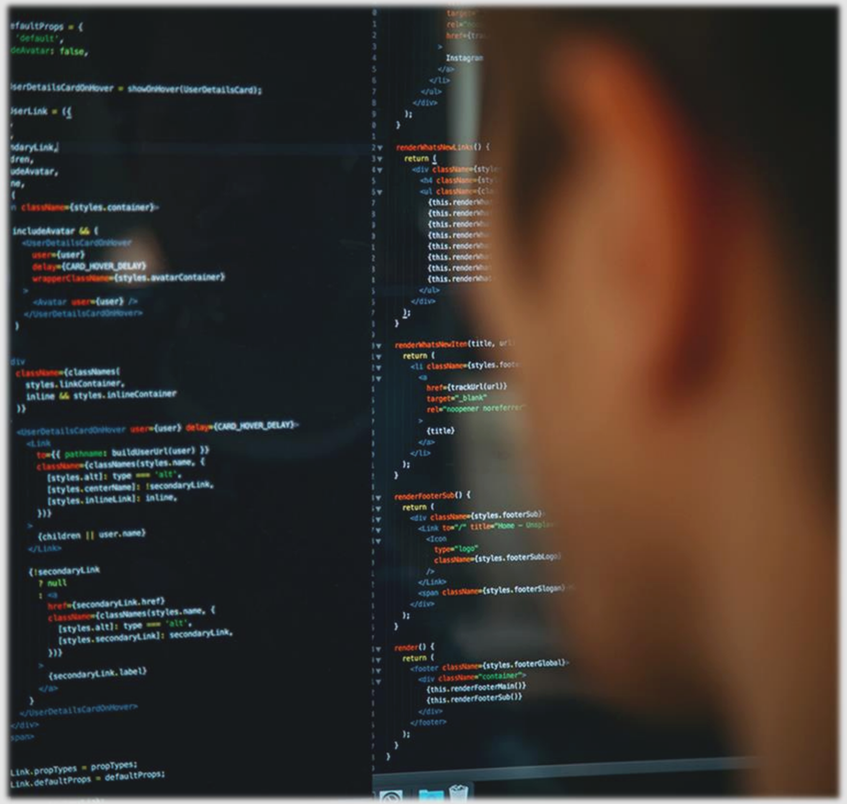


Photo by Charles on Unsplash

Mixed Data Security

- NARA has similar challenges as election data
  - Openness is our business model
  - Receive data from external sources
  - Develop unique controls, segregation, & monitoring
- Public
- Protected/Internal
- Restricted Access
  - Presidential
  - Title 13/Census
  - PII/Military records
- Classified

Public Use Systems

- Physical access to portions of the building
- Research rooms for access to the data
- Scanning and printing
- Personal imaging equipment
- Security controls
  - Isolated from network
  - Same monitoring tools
  - Limited accounts
  - Unique passwords

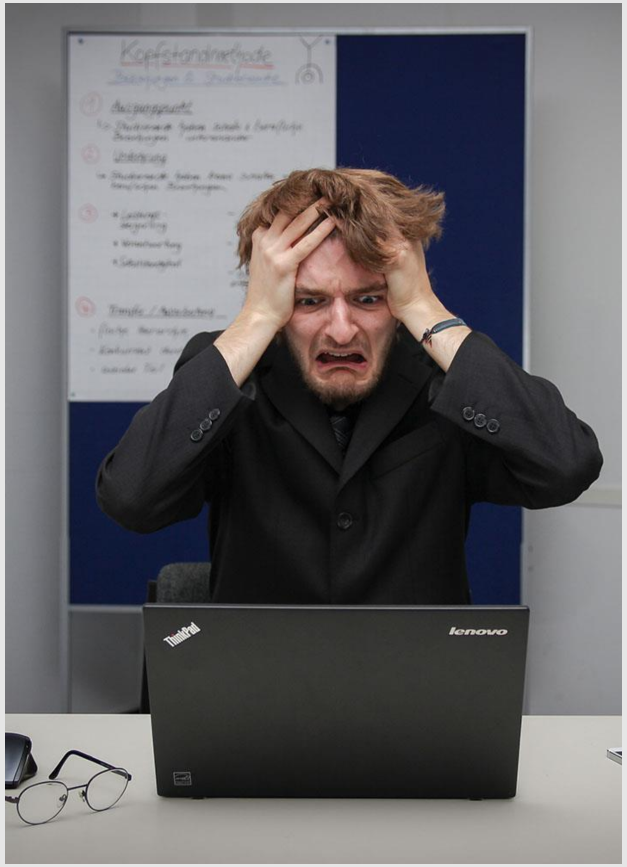


Photo by Sebastian Herrmann on Unsplash

Public Website

- NARA business is providing access to records
- National Archives catalog
- Census data (after 72 years)
- Military records
  - Limited access, but controls to segregate
  - Grant access to physical records
- Security controls
  - Segregated and limited access from internal network
  - Same monitoring agents
  - Additional tools such as WAF, DLP
  - Controls for creating website and publishing data

NARA as a Target

- All .gov systems are targets as a trophy
- Target of Anonymous
  - Increase monitoring based on threats
- Consistent stream of probes
  - Don’t call them attacks
  - Phishing
  - Scanning
- Threat modeling is important
  - Understand attackers
  - Understand attack vectors
  - Where should we allocate our resources?
  - When should we outsource?

Photo by Fauzan Saari on Unsplash

Case Study: Bad Day

- SUBJECT: ISIS posted a video on YouTube hacking NARA !!!
- re: ISIS posted a video on YouTube hacking NARA !!!
- re: fwd: re: re: ISIS posted a video on YouTube hacking NARA !!!
  - Call me
- Not a hack, but unofficial part of website
  - Reviewed the video for evidence
  - Confirmed audit of the logs
  - No detected signal from Incident Response tools
- LESSONS:
  - Follow a formal process for reviewing all website content
  - Test IR and audit capabilities
  - Identify capabilities which were missing

Case Study: Integrated Development

- Webapp developed without security review
- Assumed security review would follow happy path
- Critical finding discovered
- Deployment delayed
- Financial cost to refactor, test, & deploy
- LESSONS:
  - Engage security early and often (moved to DevSecOps)
  - Schedule should allocate time to resolve findings
  - Enforcement mechanism to fix findings

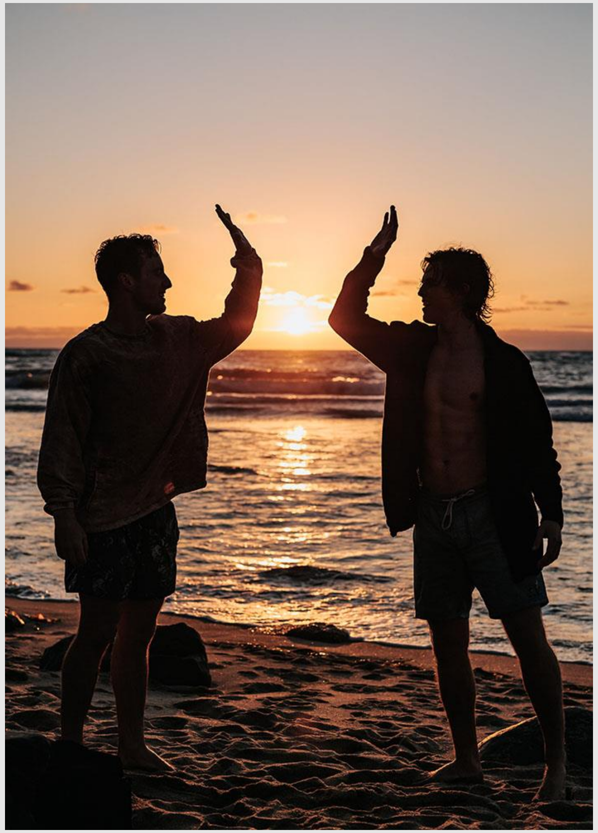


Photo by Tyler Nix on Unsplash

Case Study: Malware from Email

- Alert from workstation
- Powershell command to delete shadow copy
- Powershell parent was Acrobat
- Acrobat parent was web browser
- No log of email in email threat prevention service
- LESSONS:
  - Successful test of behavior-based agent
  - Block access to personal email
  - Disable browser history clearing
  - Disable incognito mode
  - Awareness: Mixing business and personal increases chance of phishing

Photo by Tyler Nix on Unsplash

Emerging Threats

- Business Email Compromise (BEC)
  - Spearphishing, email compromise, email spoofing controls
- Voice deepfake used to steal $243,000 [1]
- Multi—factor authentication (MFA) scams
  - SMS is no longer secure, but better than password
- Social media spearphishing
- Ransom via threat to release data
  - Payment may not avoid future ransom

[1] https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000

Final Thoughts

- Executive buy-in, awareness, policy
- Explain why security control will help the business
- Learn current threats
- Do NOT treat all users equal
- Do NOT treat all data equal
- Layered controls to avoid Single Point of Failure
- Continuous monitoring and IR when things go wrong
- Test: patching, backups, IR

Photo by Rob Schreckhise on Unsplash

Thank You!

- Sandra Paul-Blanc
- Philip Kulp
  - *linkedin.com/in/philipkulp*

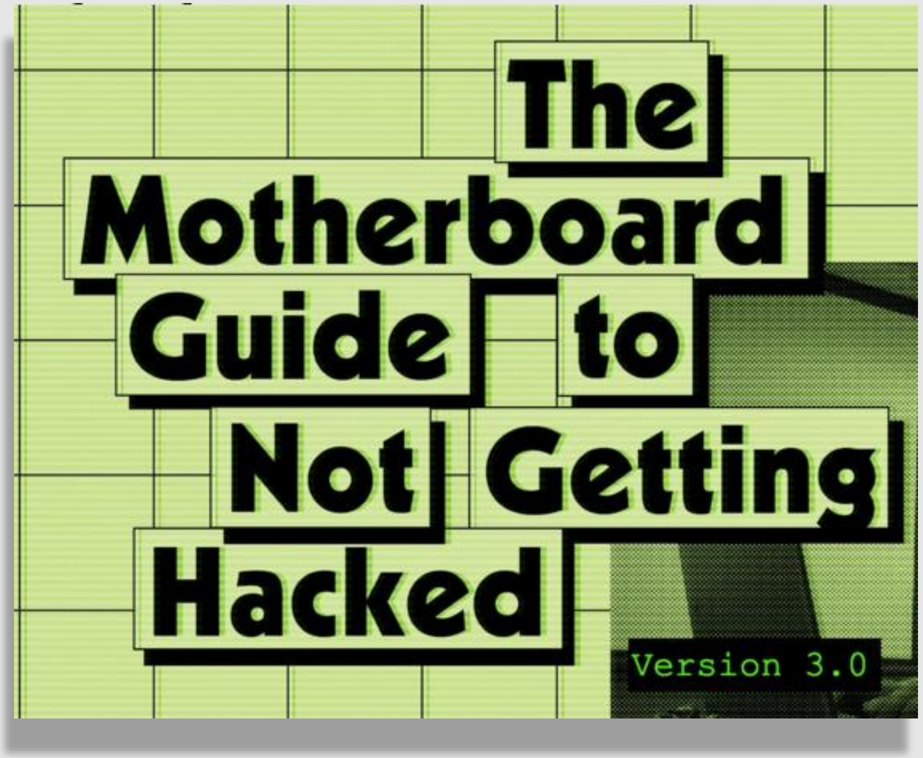
Questions?

Photo by Camylla Battani on Unsplash

BACKUP SLIDES

How not to get Hacked

- Threat Modeling: What, Who, How likely, Consequences, Effort to exert
- Keep apps up to date
- Secure passwords and do not reuse!
  - Use password apps
- Two-factor
  - OTP managers are good (don’t lose your phone!)
  - Text-based not always secure (SIM hijacking)
  - Hard tokens are great (YubiKey)
- Use anti-virus, anti-malware, adblocker (Defender is great and free)
- Minimized addon use in browsers
- Keep regular backups
- Don’t post on social media…Hey I’m going on vacation for two weeks…



https://www.vice.com/en_us/article/d3devm/motherboard-guide-to-not-getting-hacked-online-safety-guide

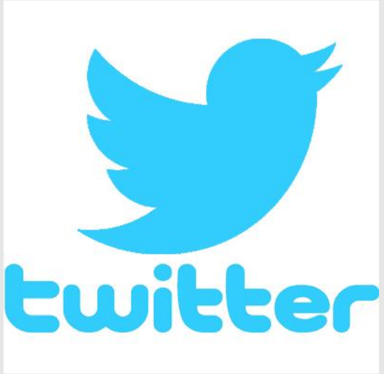
Media Security

- Incoming
  - Limit to specific workstations
- Policies for handling media
  - Encrypt mobile devices (USB, laptops)
  - Auto scan on insert
  - Disable USB or whitelist model

Photo by Brina Blum on Unsplash

Available Resources

- News Sources
- Twitter
- Podcasts

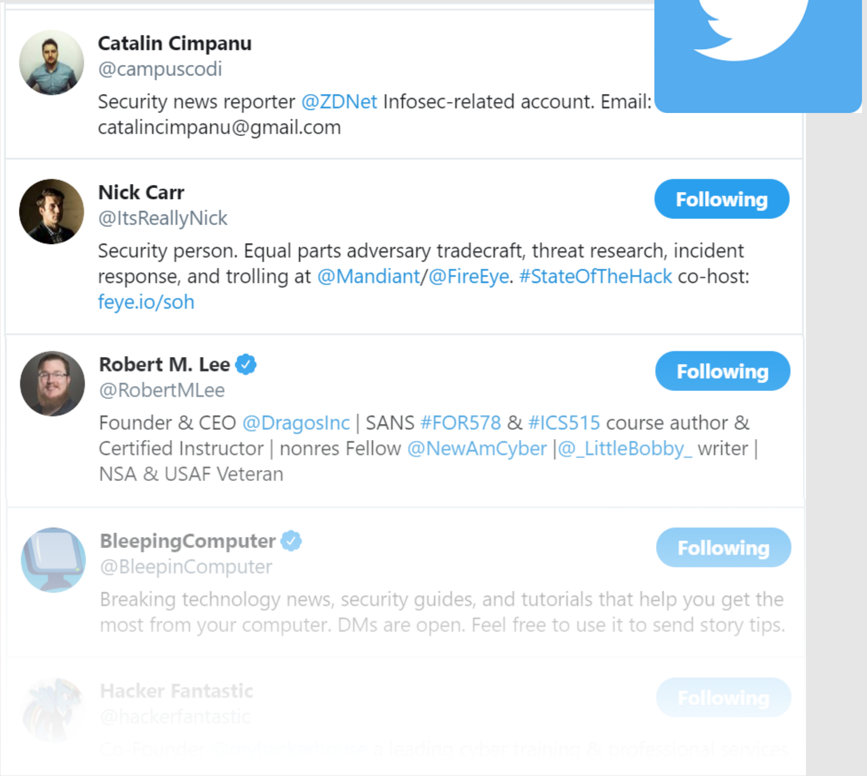


News Sources

- Bleeping Computer
  - https://www.bleepingcomputer.com/
- Motherboard by VICE
  - https://www.vice.com/en_us/topic/cybersecurity
- SC Media
  - https://www.scmagazine.com/home/security-news/
- Threat Post
  - https://threatpost.com/

Twitter

- Goal: Follow differing perspectives on cybersecurity news
- Vulnerability researchers
  - @taviso, @HackerFantastic, @FuzzySec
- Cybersecurity reporters
  - @campuscodi, @BleepingComputer, @briankrebs
- Perspectives on cybersecurity news
  - @RobertMLee, @dotMudge, @mattBlaze
- Real-world cybersecurity techniques
  - @SwiftOnSecurity – https://decentsecurity.com
- Current threats
  - @ItsRealNick, @MalwareJake
- APT and state-sponsored group tracking
  - @RidT



Catalin Cimpanu
@campuscodi
Security news reporter @ZDNet Infosec-related account. Email: catalincimpanu@gmail.com

Nick Carr
@ItsReallyNick
Security person. Equal parts adversary tradecraft, threat research, incident response, and trolling at @Mandiant/@FireEye. #StateOfTheHack co-host: feye.io/soh

Robert M. Lee
@RobertMLee
Founder & CEO @DragosInc | SANS #FOR578 & #ICS515 course author & Certified Instructor | nonres Fellow @NewAmCyber |@_LittleBobby_ writer | NSA & USAF Veteran

BleepingComputer
@BleepinComputer
Breaking technology news, security guides, and tutorials that help you get the most from your computer. DMs are open. Feel free to use it to send story tips.

Hacker Fantastic
@hackerfantastic
Co-Founder @myhackerhouse a leading cyber training & professional services

Podcasts

- StormCast
  - SANS 5-10 minutes daily
- Cyber
  - Interviews and news by VICE Motherboard
- Risky Business
  - Security concepts with journalist Patrick Gray
- Security Now!
  - Weekly in-depth discussions

Chief Information Security Officer

- Executive buy-in
- Executive awareness
- Limits
  - Can’t buy every cyber software/service on the market
  - Limited staff
  - Pushback from business owners
- Compliance
  - Federal government (cyber)
  - Federal government (records management)
  - National Archives
  - Compliance is a requirement, not a goal !!!