

A photograph of a large, modern brick building with a curved facade and large windows. The building is identified by a large 'SF' logo on its side. The sky is blue with scattered white clouds. In the foreground, there is a paved walkway, some greenery, and a black metal structure.

Securing Santa Fe College: \$4.5M ITS Cybersecurity Investment

Building a Complete Cybersecurity Program for Santa Fe College

By David Holbrook

My Credentials & Experience

- MRI Systems Engineer
- Component-level repair, superconducting magnet ramp/shim, RF-shield design & troubleshooting
- IT & Cloud, Debian Linux servers | AWS Solutions Architect – Associate | NGINX, DICOM, APIs & web services
- Modern Stack, Docker · Kubernetes · Terraform · Traefik
- Cybersecurity
- Mitigated live SMTP injection attack, Python & Bash scripting,
- Raspberry Pi LTE router + remote diagnostic platform
- Current Role: Santa Fe College Cybersecurity Student
- Phishing campaign collaborator



The Threat Landscape – Why we are vulnerable

- 2024 U.S. losses = \$16 billion (FBI IC3)
- Phishing = #1 crime
- Average education breach $\approx$ \$4–6 million
- NetLab + Cisco labs: \$200 k/yr $\rightarrow$ unpatched 2012 R2, crashes, 1-hour reservations, incompletes, wrong grading for modern systemd, gross ADA violations (tiny nested windows)



Why Invest Now? Cyber Crime Stats



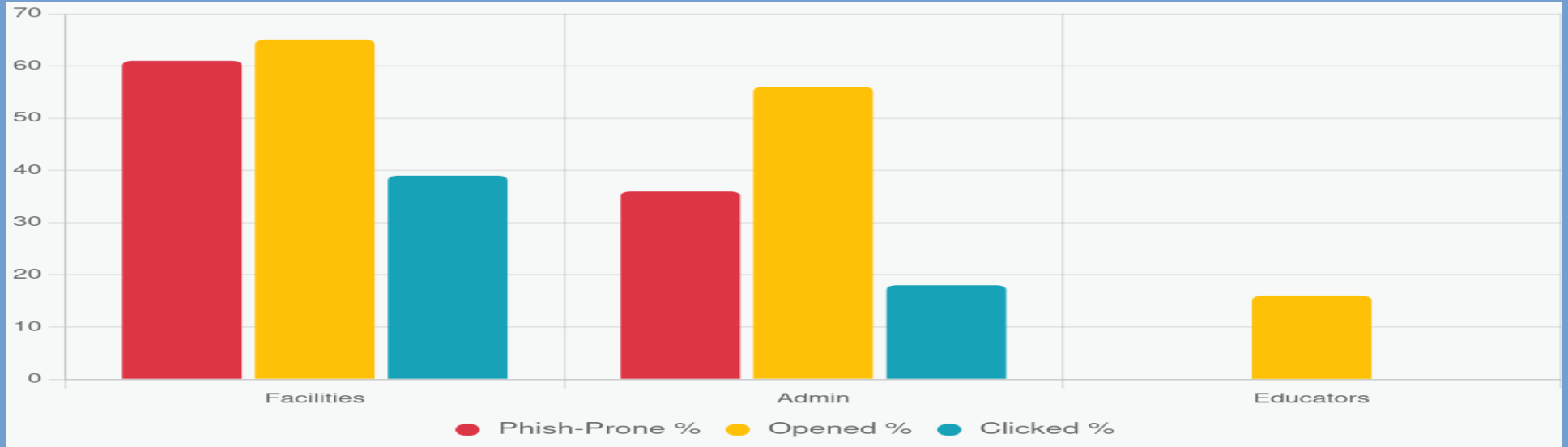
- 2024 losses = \$16 billion (up from \$3.5 B in 2019)
- Phishing = #1 reported crime every year
- Average education breach cost $\approx$ \$4–6 million
- One successful attack could wipe out years of budget.

Our Phishing Campaign: What We Did

CIS2352 + ITS Collaboration (2025)

- Collaborated: CIS2352 Ethical Hacking class + ITS using KnowBe4 platform.
- 3 simulated emails targeting Facilities, Admin and Educators (~150 users).
- Goals: Test awareness, promote on best practices, comply with FL & SF college Cybersecurity Standards.

Campaign Outcomes: Educators 0% Phish-Prone



- Facilities (Campaign 1): 61% phish-prone; 65% opened, 39% clicked, 0% reported
- Administrators (Campaign 2): 36% phish-prone; 56% opened, 18% clicked, 0% reported
- Educators (Campaign 3): 0% phish-prone; 16% opened, 0% clicked, 0% reported
- Zero reports across all = need for Hub



New Capability: Community CyberSecurity Hub

- Secure reporting forum (Discourse) – fixes 0 % reporting
- Real-time SIEM
- (Security Information and Event Management)
- Encrypted cloud bucket for evidence & student projects
- 8 defensive typo domains (\$1.3K total)

Keep CIS2352 Involved

- Students moderate forum, run simulations, analyze SIEM logs
- Proven results (0 % educator phish-prone)
- Builds our own talent pipeline
- Direct user feedback
- Introduction of fresh ideas and assessments.

\$4.5 Million Request – What It Buys

- Proven phishing reduction
- Real-time visibility + endpoint protection
- Community reporting + modern labs
- Dedicated staff + student talent

Item	Description	3-Year Cost
KnowBe4 Renewal	Phishing platform & training	\$50,000
CIS2352 Stipends	Student & faculty collaboration	\$75,000
Community Cybersecurity Hub	SIEM + Forum + Cloud storage + typo domains	\$800,000
Endpoint Detection & Response	College-wide EDR (CrowdStrike or SentinelOne)	\$1,200,000
Training & External Exercises	Advanced modules + pen-tests	\$375,000
Staff & 3-Year Runway	2 Analysts + 1 Engineer + buffer	\$2,000,000
TOTAL		\$4,500,000

We can do It for Half the price

- Replace commercial SIEM/EDR → Wazuh + Elastic (open-source, used by NASA/DoD)
- Replace NetLab >> docker (labainers/GNS3) >> \$450-500K saved
- Total Savings 2.1 Million

Questions?

David Holbrook

<https://mrIService.com>

mrIService@gmail.com

<https://github.com/MRIService>

Thank You for your time!

Bonus: What Happens Without Funding

- Status Quo = High Risk.
- No System Information and Event Management SIEM → blind to attacks in progress
- No dedicated staff → hope someone notices at 2 a.m.
- Lost student talent pipeline

References

- FBI Internet Crime Report 2024
https://www.ic3.gov/Media/PDF/AnnualReport/2024_IC3Report.pdf
- KnowBe4 Phish-Prone Percentage Benchmark Report 2025
<https://www.knowbe4.com/phish-prone-benchmark>
- NDG NETLAB+ Campus License Pricing 2024–2025 (public tier)
<https://www.netdevgroup.com/pricing>
- U.S. Cyber Crime Losses 2019–2024 (FBI IC3 historical data)
<https://www.ic3.gov/Media/PDF/AnnualReport/>
- Wazuh Open-Source SIEM & EDR
<https://wazuh.com>
- Labtainers – Docker Cybersecurity Labs (U.S. Naval Postgraduate School)
<https://nps.edu/web/c3o/labtainers>
- GNS3 Network Emulator
<https://www.gns3.com>
- Discourse Open-Source Forum
<https://discourse.org>
- ADA Section 508 & WCAG 2.1 Accessibility Guidelines
<https://www.ada.gov/resources/title-ii-primer/>
<https://www.w3.org/TR/WCAG21/>