NWACC – Risks & Trends

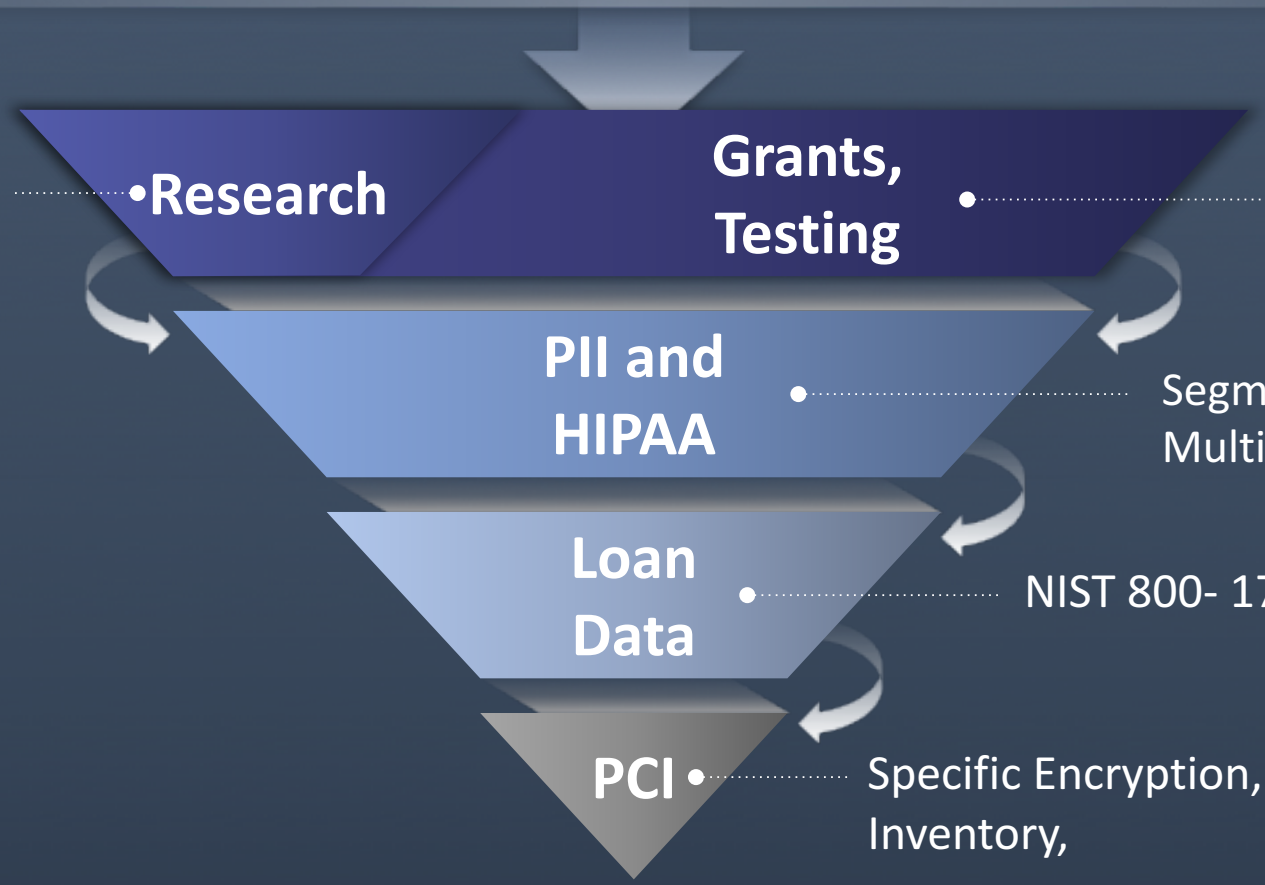
Jeff Fawcett Cisco Director

Cybersecurity

University Risk

Use Case Solutions

Who is your threat?



Zero Trust Network Model

Segmentation, DLP, Multifactor Authentication

NIST 800- 171

Specific Encryption, 2FA, Inventory,

Practical Best Practices..Current State..Gaps

Cisco technologies now in use
3rd Party technologies in use
Working on
Gaps

Identify Asset Management Risk Strategy Governance	**Protect** Counter Measures, Access Control, Data Security	**Detect** Anomalies, Events, Processes, Cont Monitor & Block	**Respond** Planning, Communications, Mitigations	**Recover** Contain, Speed, Improvements
Encryption, VPN, Executive Leadership Involvement; NIST 800-53 and SANs 20 are lists that bad actors know. CMMI level 3 is great goal.		Privilege Escalation; Monitoring Continuously Log Admin Activities	Track Malware (SEP) Incident Response (CISCO) Forensics (Encase);	Documented Playbook Use of FBI processes
Integrity; NAC; Your security is as good as what your auditors know to look for. Procurement not following guidelines; No approved application list from Security Group.		Malware WEB Security (WSA);	Cloud Web Security (Cisco) With 30 departments - coordination?	Network Behavior Analysis Advanced Mal Protection (AMP)
Identity, Authentication (ISE), Inventory (LANsweeper), Insider (Varonis), Patching (?); Harden Configs; Governance; Mobile (AirWatch)		WEB/CloudWeb Security (CASB); Proactive Threat Hunting; Email Security (IronPort), NGIPS (Firepower)		Contain your exflows (OpenDNS)
Watch DNS Inflows; End Points have no Admin Rights Information/Data Classification (Top 50)		Info/Data Classification, Monitoring (LogRythm), Counter measures Comprehensive DLP (Office 365 DLP email); Watch DNS Outflows		

Least Privilege, Security solutions should have analytics and be shared. (AMP); Secure your SAP database;
One policy engine pushing to all devices; RBAC; Least Privilege; Intelligence that is Integrated

Track Malware; Your infrastructure should be broken up into logical enclaves;
Security solutions should have analytics and be shared. Track Malware; Your infrastructure should be broken up into logical enclaves (segmentation);
All end point devices have a certificate (to get on the network; End to End Communications Network sharing all security related data for visibility/Intel.

Security Policies. Email Security (IronPort); Security Policies; Analytics to tie this all together (visibility and context); Security Policies, Risk, Compliance (Approva); Education; RBAC, Intelligence is integrated (Dell SecureWorks); Use Netflows and PCAP; Countermeasures (Rapid7) PEN Testing (Pony Express)

Where and What is Your Risk at The University? That Should Drive Your Priorities..

- Research?
- Healthcare?
- Student Loan Financial Loans (NIST 171)?
- Compliance - PII/PCI/NIST/HIPAA
- Understand Risk and Gaps – Strategy - Jose
- Insider…. East-West
- IoT (Bldg Automation, Cameras, Digital Signage)
- Encrypted traffic moving through and out of your network

Cybersecurity Trends in Higher Education

- Targeted Ransomeware – those who will pay
- They want your Intellectual Property (Grants, FDA, Research)
- PCI is so yesterdays issues, lets talk Student Financial Loan Data
- How do they get in?
  - Poison Well sites
  - eMail links
  - Stolen Credentials
- Analytics and Identity

What Are Other Universities Doing

- Multi-factor your Admins (but not finger prints) when they login, track their logs
- Seeing the need for a comprehensive Insider Threat program
- Track anyone with admin rights (2fa) that access key servers and databases.
- Watching your exflows is effective
- Understand Risk and Gaps – Strategy – Focus on what to prioritize and address, not what is wrong
- Block TOP and XYZ Domains (95% bad) - from our ATA folks.
- SIEM vs Analytics correct proportions
- Automated attacks defended by automated defenses (machine learning, behavior detection)
- Moving to an integrated threat defense (end to end framework, automated, and communicative)

What Are Other Universities Doing

- Analytics is the new security approach as SIEMs are becoming dinosaurs, Splunk is the first step
- Reduce the # of security vendors, and drive visibility and context plus lower their overall costs
- How we build better visibility, context, and enforcement
- Starting to look at logically segmenting their network (more than Firewalls, ACLs, VLANs) your network (by App, Data, Users) using visibility, Isolation, policy enforcement, and Identity

Educational Use Cases

- Long term impact to business goals, like loss of research
- Loss of grants due to poor security (as determined by the Agency)
- Protect the brand name! – Don’t find out you have been breach from the FBI
- Responding to Breaches in the proper manner
- Moving to the cloud securely
- Protecting Sensitive Intellectual Property (Content)
    - Student loan fraud
    - Using the loan information for other fraud.
- East-West (lateral) movements (insiders or students)

Educational Use Cases

- Reducing # of vendors and overlap. KISS
- Vendors, Suppliers, and Contractor entities with enterprise backbone access
- Automating to address the skilled staff shortages - outsourcing
- Look for APT's - in our infrastructure, people to hunt for threats (ATA, Stealthwatch)
- Need a secure system to let in Vendors and Contractors but control what servers and applications they can use
- Application Security

Some Best Practices Suggestions

- Analytics is the new security approach.
- Logically Segment your network (by App, Data, Users) using visibility, Isolation, policy enforcement, and Identity
- Patch management done right will harden your security
- Monitor your DNS and use Netflow to improve security
- Multi-factor your Admins when they login, track their logs
- Integrity, privilege escalation moves the security needle
- Lock down your MDM tool/dashboard
- CMMI baseline
- Secure/segment your library!

Summary - Practical Holistic, Move the Needle Security Investments

- Attack probability. Understand who is coming after just you. What are their capabilities? Potential loss. Liability to litigation. What do you need to address that
- NAC to allow registered devices
- Use DNS protection, large majority of breaches (90%) involve DNS (ingress, egress)
- Top 5 (Other colleges):
  - A Cybersecurity framework, leveraging Cybersecurity Analytics, fast to detect, block, and mitigate
  - Penetration Testing, Exflow Analysis, Securing DNS
  - Incident Response Preparation, Privilege Escalation Monitoring
  - Cyber Range Training, Education
  - Basic Logical Segmentation
  - Remove Admin rights