NIST CSF and Compliance in Higher Education:
Or how I learned to stop worrying (so much) and just manage risk

Hunter Ely
Security Architect
Business Challenges…. Compliance Edition!
Compliance Does Not Equal Security

By Josh Lefkowitz on May 21, 2018

Can We Cease Check-Box Compliance?

Some indicators show a transition to risk-based management driving security decisions, but compliance checklists still pay the infosec bills.

For years now, security insiders have railed against the check-box compliance ethos, warning enterprises that simply chasing after regulatory lists won't ever

Stop Thinking of Compliance as a Checkbox

Many of today’s executives view compliance as a check-box – and move on after the main
Higher Education Business Challenges

Meet Business and Security goals

Reduce cyber risk

Achieve Compliance
Issues with Common Compliance Approach

- Checkbox or “good enough” approach
- Not focused on cyber risk reduction
- Not focused on preventing threats
- Sub-optimal use of staff resources
What is the NIST Cybersecurity Framework?

- Initially released in February 2014, the CSF was developed in response to an Executive Order which directed the Federal Government to work with private industry to protect the nation’s Critical Infrastructure.

- The NIST CSF is a voluntary framework providing guidance on the management and reduction of Cybersecurity risk.

- While it is not a one size fits all framework. It outlines a series of guidance points to allow organizations, both private and public sector, to mature their Cybersecurity practices in a common and well understood format.
Overview of NIST CSF Stages

Identify
- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

Protect
- Access Control
- Awareness and Training
- Data Security
- Information Protection P&P
- Maintenance
- Protective Technology

Detect
- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes

Respond
- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

Recover
- Recovery Planning
- Improvements
- Communication
New Approach to Compliance

- Good Cyber Hygiene
- Reduce Cyber Risk
- Threat Prevention
Prevention Mindset

- Complete Visibility
- Integration/Automation
- End to End Prevention
Benefits of Threat Prevention Approach

- Improved Productivity
- Data Protection
- Better Cybersecurity
Critical Success Factors

- Increase Visibility
- Improve Cyber Hygiene
- Evolve Continuously
Stop Attacks With a Platform Approach

**Unmatched Protection**
Visibility and control everywhere: on-premises, other campuses, mobile, cloud

**Tightly Integrated**
Save time and reduce complexity by replacing disconnected tools

**Accurate and automated**
Analytics trigger automation for immediate, effective actions

BUILT FOR SIMPLICITY
Next-Generation Firewall as a Security “Hub”

Consistent Visibility and Control

Integrated Services Replace Disconnected Tools

Automation With Analytics Deliver Immediate Preventions
Modern Endpoint Protection beyond Antivirus

Block ransomware, exploits and fileless threats

Stop spread of threats with shared intelligence

Detects and responds to attacks with machine learning
The Journey to the Cloud

Access
Connect users and transport data to and from the cloud

SaaS Applications
Discover and control the use of third party applications running in the cloud

Cloud Applications
Design, build, deploy, and run applications in the cloud
Secure the Future with Autonomous Security build on AI and ML

Stitches data for enterprise-wide view

Harnesses AI and machine learning for rapid insight

Orchestrates and automates to speed resolution

BREAK SILOS AND DELIVER RADICAL SIMPLICITY
Securing Your Transformed Enterprise

Hybrid data center
Internet Perimeter
Branch & mobile
5G & IoT
Endpoint

DATA LAKE

SECURE THE ENTERPRISE

Detection & response
Automation & orchestration
Network traffic & behavioral analytics
Threat intelligence

SECURE THE FUTURE

Secure access
SaaS
Public cloud
Palo Alto Networks: Automated protection that propels education.

The cybersecurity challenge in education merely starts with the 21st century classroom – it encompasses a city-like array of campus functions, the curriculum needs of our future workforce, and the safety of our nation’s research and intellectual property. We provide a holistic security operating platform that arms educational institutions to protect every possible step in a student’s educational journey, and the societal impacts they will create.

K-12
We create a secure modern learning environment, unconstrained by physical location.

Doctoral Research Universities
We protect our nation’s pipeline of critical research and intellectual property.

Universities & Colleges
We solve the conundrum of a fast, open, and collaborative campus that is also secure and resource efficient.

Community & Trade Colleges
We provide the curriculum and labs to build our cyber workforce of the future.
THANK YOU

Email: hely@paloaltonetworks.com | Twitter: @PaloAltoNtwks