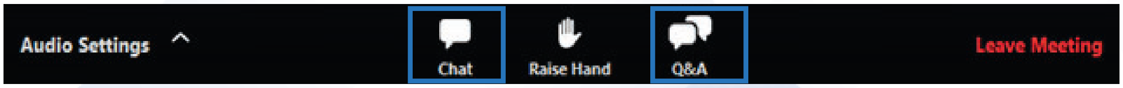
Critical Insight®

AWC
ASSOCIATION
OF WASHINGTON
CITIES

Cyber Survivability for Local Government

Zoom webinar technical tips

- Plug your device into a power source
- Connect your device directly into your internet connection instead of using wireless to avoid audio and video quality issues and interruptions
- You can **submit questions for the speaker** via the **Q&A feature**
- Please use the **Zoom chat feature** for any **technical issues** or questions



Select **Chat**, type your question or comment into chat pane, and hit **Enter**.

Select **Q&A**, type your question in the Q&A pane and hit **Enter**

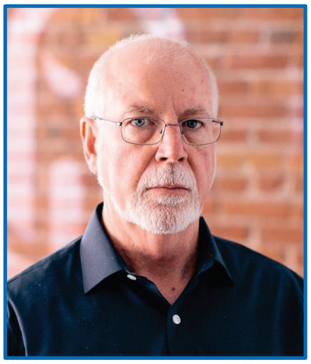
Disclaimer

Disclaimer: The information contained in this presentation is for general educational purposes only and is not intended to be legal advice. Please consult legal counsel for advice about specific questions.

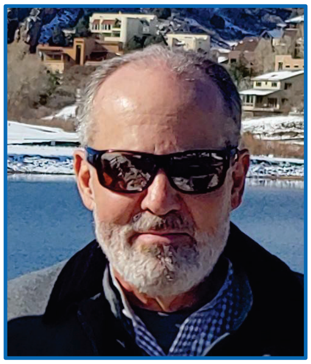
Agenda

- Introductions
- Headlines
- What's in the infrastructure bill
- Using a framework for budgeting
- 10 things insurance companies want to see
- PISCES: free security monitoring
- Q/A with the panel

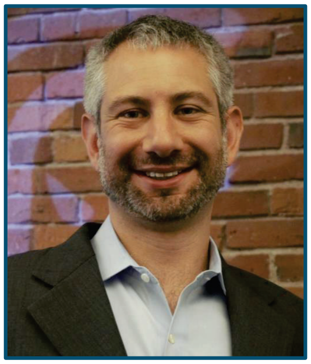
Panelists



Mike Hamilton
Critical Insight Founder



John Traeger
City of Issaquah CIO



Jake Milstein
Event Host, Critical Insight

Critical Insight

Public Sector Problems

- Hire & retaining talent
- Significant compliance needs
- Cities & Counties can’t be treated like companies. They hire, purchase, and run differently
- Services & capitol purchases are difficult

Critical Insight

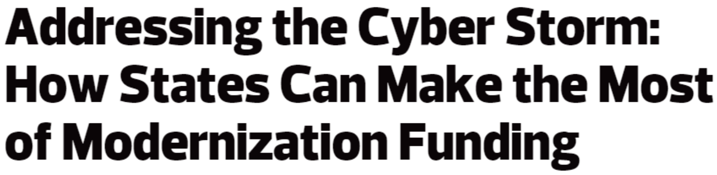
Public Sector Solutions

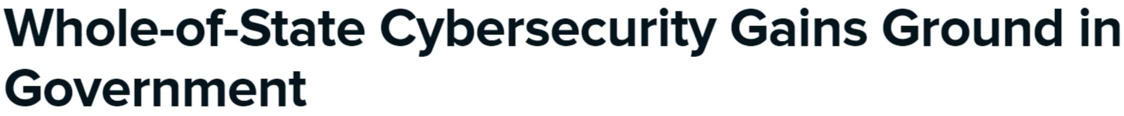
- CI provides gives you a security team
- CI assists with audit-readiness & training
- CI has dozens of years of public sector experience. Co-founder Mike Hamilton was City of Seattle CISO
- CI is easy to buy. Contract vehicles & GPOs

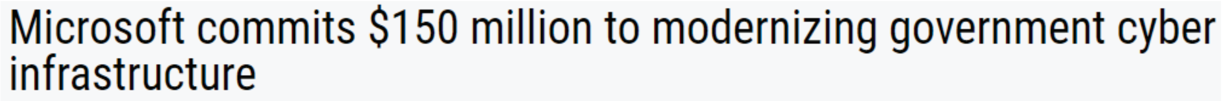
Glossary

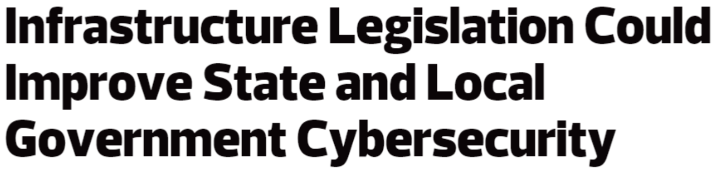
- **Phishing:** A criminal's method for tricking you into giving up a password. Usually comes through email or social media.
- **Ransomware:** Should be called Cyber-Terrorism or Cyber-Extortion. A criminal locks up a network and/or files and then extorts the victim to unlock (note: don't trust criminals to keep their word)
- **Business Email Compromise (BEC):** When a criminal pretends to be a business you already know to steal money. Sometimes involving taking over one of your vendors.
- **Multi-Factor Authentication (MFA or 2FA):** More than just a password, something that proves in 2 ways that you are who you say you are. Generally, 2 of these: (1) something you know (2) something you have (3) something you are.

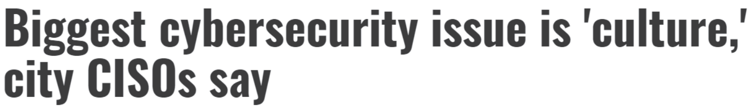
News In Context


Addressing the Cyber Storm: How States Can Make the Most of Modernization Funding

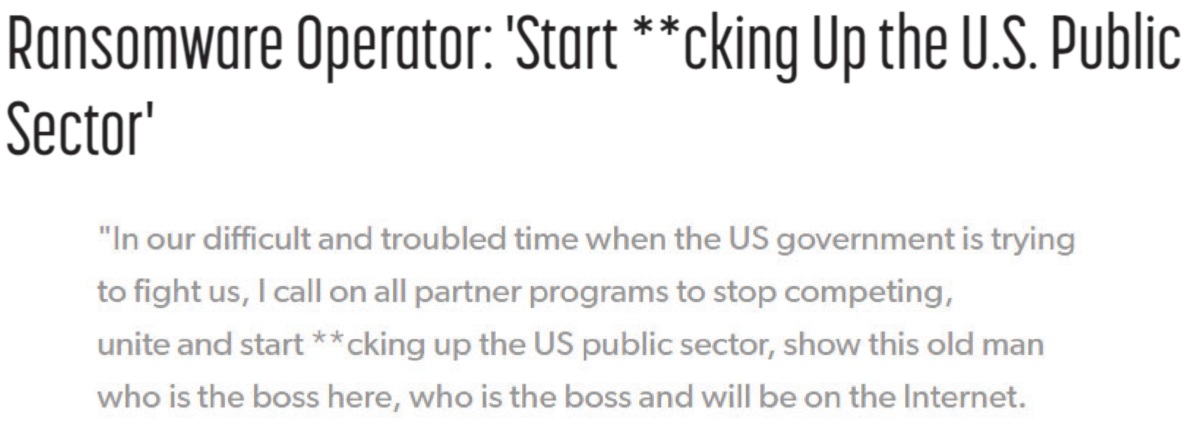

Whole-of-State Cybersecurity Gains Ground in Government


Microsoft commits $150 million to modernizing government cyber infrastructure


Infrastructure Legislation Could Improve State and Local Government Cybersecurity


Biggest cybersecurity issue is 'culture,' city CISOs say

Also, This



Ransomware Operator: 'Start **cking Up the U.S. Public Sector'

"In our difficult and troubled time when the US government is trying to fight us, I call on all partner programs to stop competing, unite and start **cking up the US public sector, show this old man who is the boss here, who is the boss and will be on the Internet.

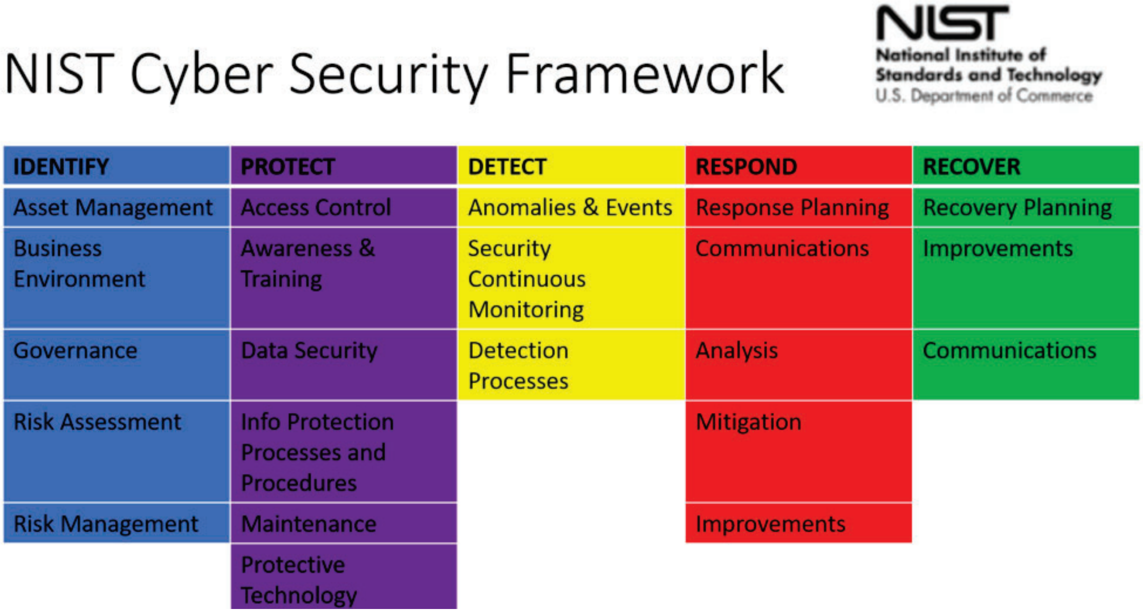
The Infrastructure Bill

- Section 70612
- $1.8B for states, local governments, Tribes
- Grants will be distributed by States
- A justification plan is required
- Grant funding duration is 2 years, renewable (annually, strangely)
- September 2023 deadline for plan submission
- No one knows what the state will require
- There are exceptions

``(j) Limitations on Uses of Funds.-- ``(1) In general.-- Any entity that receives funds from a grant under this section may not use the grant-- ``**(A) to supplant State or local funds; ``(B) for any recipient cost-sharing contribution; ``(C) to pay a ransom; ``(D) for recreational or social purposes; or ``(E) for any purpose that does not address cybersecurity risks or cybersecurity threats on information systems** owned or operated by, or on behalf of, the eligible entity that receives the grant or a local government within the jurisdiction of the eligible entity.

``(i) Review of Plans.-- ``(1) Review as condition of grant.–
**``(A) In general.--Subject to paragraph (3), before an eligible entity may receive a grant under this section, the Secretary, acting through the Director, shall-- ``(i) review the Cybersecurity Plan of the eligible entity, including any revised Cybersecurity Plans of the eligible entity; and ``(ii) determine that the Cybersecurity Plan reviewed under clause (i) satisfies the requirements under paragraph (2).** ``(B) Duration of determination.--In the case of a determination under subparagraph (A)(ii) that a Cybersecurity Plan satisfies the requirements under paragraph (2), the determination shall be effective for the 2-year period beginning on the date of the determination.

Creating That Plan

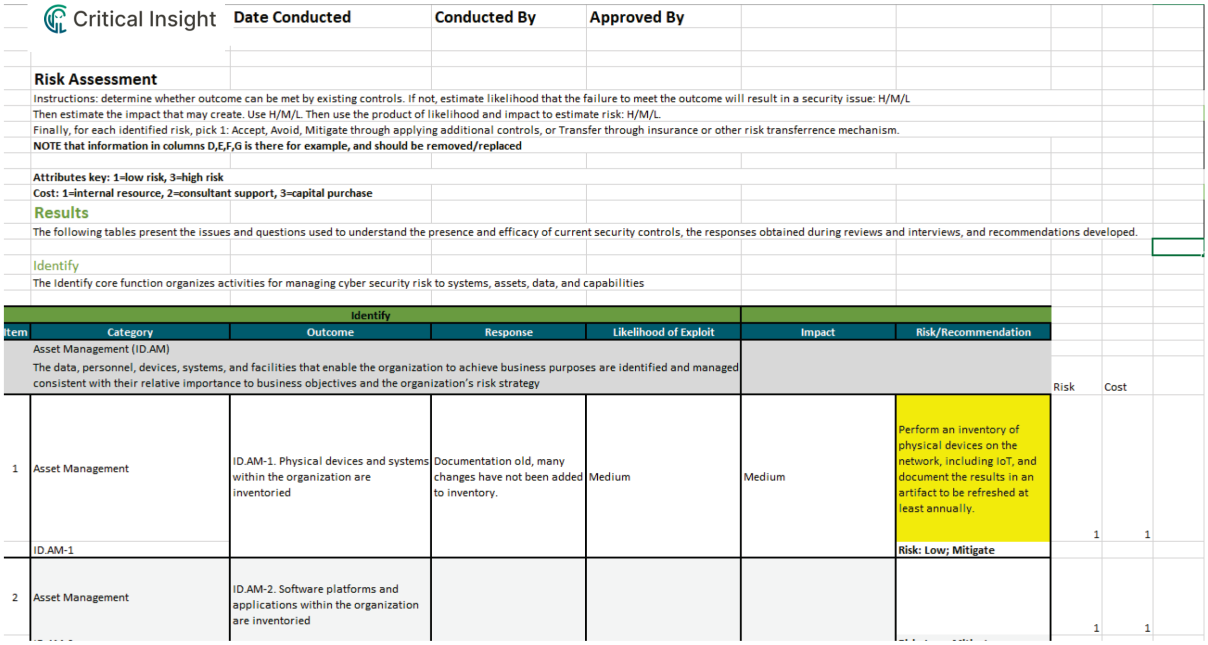


NIST Cyber Security Framework

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Asset Management	Access Control	Anomalies & Events	Response Planning	Recovery Planning
Business Environment	Awareness & Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management	Maintenance		Improvements	
	Protective Technology			

Assess, Resource, Prioritize



Critical Insight

Date Conducted	Conducted By	Approved By

Risk Assessment

Instructions: determine whether outcome can be met by existing controls. If not, estimate likelihood that the failure to meet the outcome will result in a security issue: H/M/L

Then estimate the impact that may create. Use H/M/L. Then use the product of likelihood and impact to estimate risk: H/M/L.

Finally, for each identified risk, pick 1: Accept, Avoid, Mitigate through applying additional controls, or Transfer through insurance or other risk transferrence mechanism.

NOTE that information in columns D,E,F,G is there for example, and should be removed/replaced

Attributes key: 1=low risk, 3=high risk

Cost: 1=internal resource, 2=consultant support, 3=capital purchase

Results

The following tables present the issues and questions used to understand the presence and efficacy of current security controls, the responses obtained during reviews and interviews, and recommendations developed.

Identify

The Identify core function organizes activities for managing cyber security risk to systems, assets, data, and capabilities

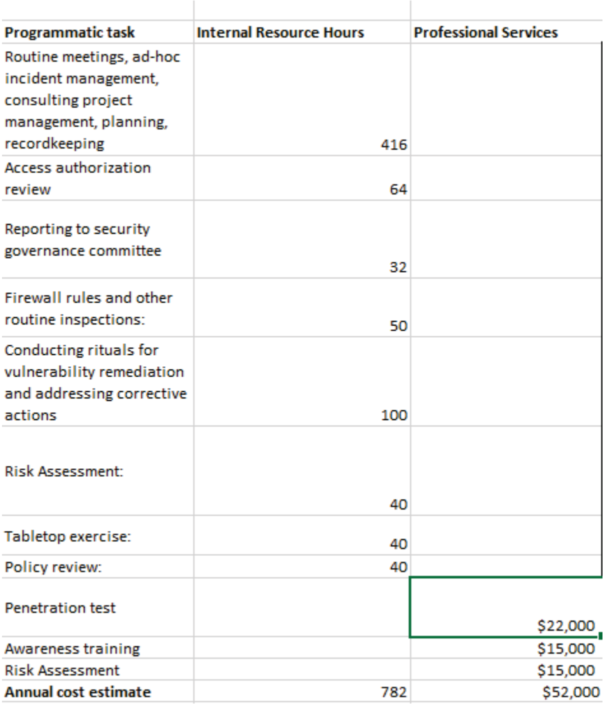
Identify								
Item	Category	Outcome	Response	Likelihood of Exploit	Impact	Risk/Recommendation		
	Asset Management (ID.AM) The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy						Risk	Cost
1	Asset Management ID.AM-1	ID.AM-1. Physical devices and systems within the organization are inventoried	Documentation old, many changes have not been added to inventory.	Medium	Medium	Perform an inventory of physical devices on the network, including IoT, and document the results in an artifact to be refreshed at least annually. **Risk: Low; Mitigate**	1	1
2	Asset Management	ID.AM-2. Software platforms and applications within the organization are inventoried					1	1

Determine whether outcomes are currently being met

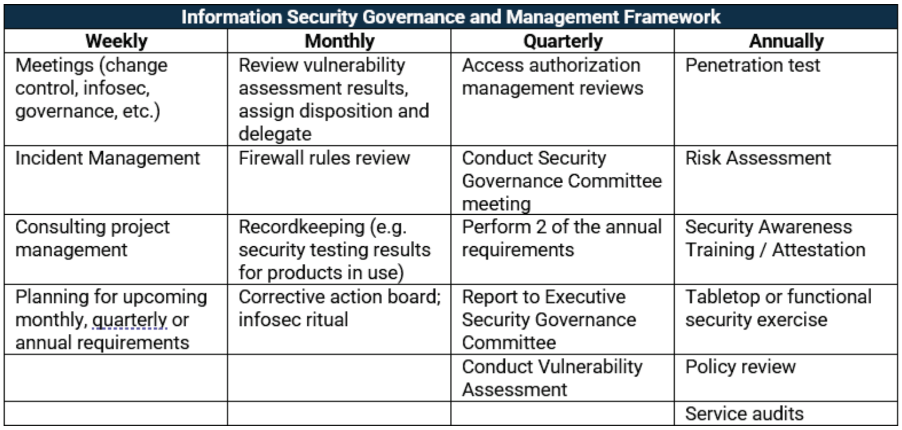
If not, denote the disposition and corrective action required

Determine how the "fix" will be resourced: internally, use of professional services, capital purchase

Governance and Management



Programmatic task	Internal Resource Hours	Professional Services
Routine meetings, ad-hoc incident management, consulting project management, planning, recordkeeping	416	
Access authorization review	64	
Reporting to security governance committee	32	
Firewall rules and other routine inspections:	50	
Conducting rituals for vulnerability remediation and addressing corrective actions	100	
Risk Assessment:	40	
Tabletop exercise:	40	
Policy review:	40	
Penetration test		$22,000
Awareness training		$15,000
Risk Assessment		$15,000
Annual cost estimate	782	$52,000



Information Security Governance and Management Framework			
Weekly	**Monthly**	**Quarterly**	**Annually**
Meetings (change control, infosec, governance, etc.)	Review vulnerability assessment results, assign disposition and delegate	Access authorization management reviews	Penetration test
Incident Management	Firewall rules review	Conduct Security Governance Committee meeting	Risk Assessment
Consulting project management	Recordkeeping (e.g. security testing results for products in use)	Perform 2 of the annual requirements	Security Awareness Training / Attestation
Planning for upcoming monthly, quarterly or annual requirements	Corrective action board; infosec ritual	Report to Executive Security Governance Committee	Tabletop or functional security exercise
		Conduct Vulnerability Assessment	Policy review
			Service audits

- Someone in the organization must be accountable for ensuring that required activities are occurring

- Annual requirements may be performed by professional services – estimate costs

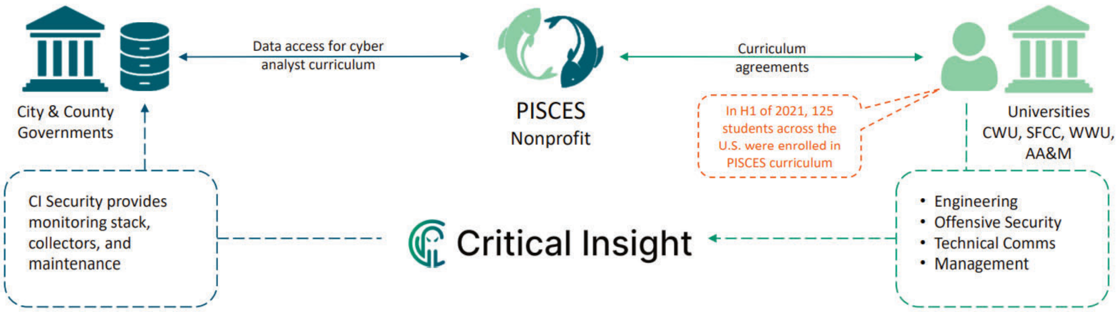
- Make sure that governance activities are included for communicating risks to executive management

What Insurance Companies Want

1. Follow the NIST Cybersecurity Framework
2. Engage External Expertise
3. Have Demonstrably Secure Backups
4. Have 24/7 Monitoring
5. Use Proactive Defense
6. Multi-Factor Authentication is a Must
7. Staff Cyber Security Awareness Training
8. Deploy Endpoint Protection
9. Vulnerability Management
10. Documented Incident Response Plans

A compendium of information provided by Aon/Stroz-Friedberg and communicating with our customers on their challenges

For Small Jurisdictions – PISCES



Data access for cyber analyst curriculum

City & County Governments

PISCES Nonprofit

Curriculum agreements

In H1 of 2021, 125 students across the U.S. were enrolled in PISCES curriculum

Universities CWU, SFCC, WWU, AA&M

CI Security provides monitoring stack, collectors, and maintenance

Critical Insight

- Engineering
- Offensive Security
- Technical Comms
- Management

- Public Infrastructure Security Cyber Education System
- No cost for local governments sub-150 employees
- 2 or 3-year contract, renewable
- Metadata and IDS alerts extracted from the network – no content
- Students at 5 universities evaluate and investigate alerts
- Oversight Analyst and Community Liaison for reporting
- Expanding into Colorado, then 2 other states

Critical Insight®

Jake@criticalinsight.com
206 718 9602 cell

Michael.Hamilton@criticalinsight.com

Walla Walla County, WA

“Everything comes down to relationships. As long as you guys have my back, I can do my real job, which is to support the citizens.”

-Chad Goodhue, IT Manager

Wenatchee, WA

“The value to me is that 24x7 we have an extra set of eyes on our network activity to monitor the logs. We have artificial intelligence that goes through the logs, but the fact that we have real eyes around the clock is just invaluable to me.”

-Dale Cantrell, Director of Information Systems

Upcoming Training

- Don’t Fall For It! Cybersecurity Awareness Training

  Every other Friday!

Critical Insight Total Security Solutions

24x7 Managed Detection & Response

Incident Preparedness

❑ IR Plan Development
❑ IR Plan Review
❑ IR Tabletop Exercise *(must be accompanied with IR Plan review or development)*
❑ Rapid Quarantine Playbook Development

24x7 Threat Detection and Analysis

❑ Network Infrastructure (PCAP & Logs)
❑ Defender for Endpoint
❑ MCAS / O365
❑ AWS (Amazon Web Services)
❑ Azure
❑ IoT Security

Containment

❑ Rapid Quarantine Playbook Execution

Eradication, Recovery, and Post-Incident Activity

❑ IR Retainer
❑ IR Assistance

Strategic Program Development

Assessments

❑ Focused Security Assessment
Standard, Work from Home, CMMC, SSAE18 SOC2
❑ Security Risk Assessment
HIPAA, NCUA, PCI, NIST, CIS20, Cloud Environment

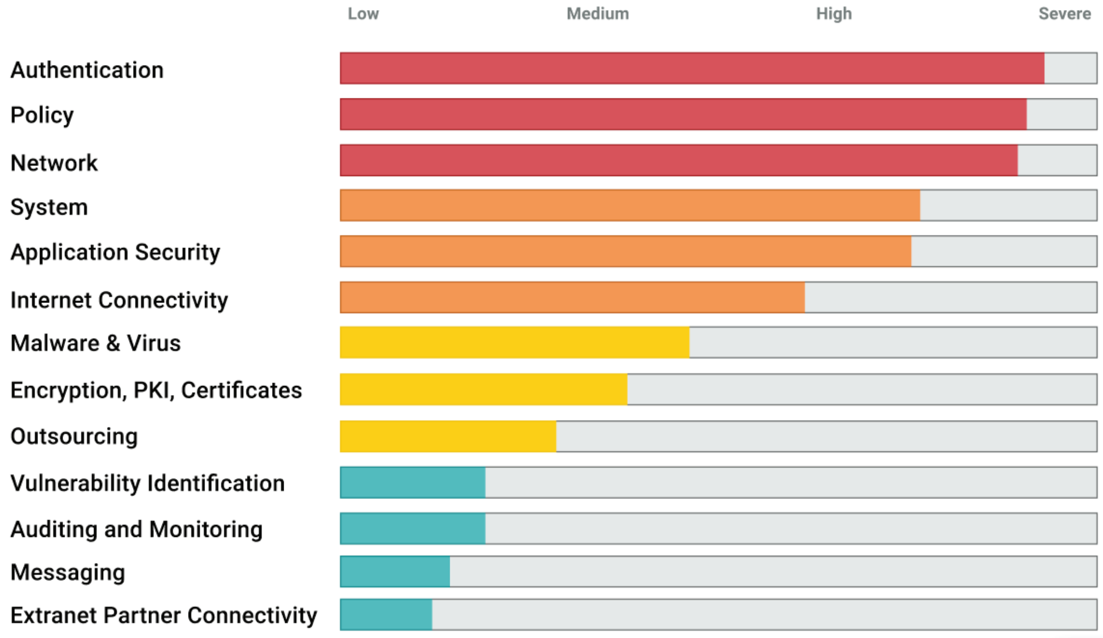
Testing

❑ External / Internal/ Cloud
❑ Continuous Vulnerability Identification
❑ Wireless, Phishing, Password Cracking
❑ Web Application Security
❑ Social Engineering

Compliance and Hygiene

❑ vCISO / oCISO
❑ Co-Managed Security Solutions
❑ Policy Review & Development
❑ Security Awareness Training
❑ Log Retention & Compliance Review

13 Point Assessment


Low
Medium
High
Severe
Authentication
Policy
Network
System
Application Security
Internet Connectivity
Malware & Virus
Encryption, PKI, Certificates
Outsourcing
Vulnerability Identification
Auditing and Monitoring
Messaging
Extranet Partner Connectivity