

Enterprise Security: Just How at Risk Are You?

FEI Austin Webinar: 5/18/2021



Acumera is a registered trademark, and the Acumera logo is a trademark of Acumera, Inc.
Other marks possibly appearing in this document are the property of their respective owners.

What are the threats and concerns you should be aware of in today's increasingly virtual business environment?

How do you evaluate the security risk level for your company's network and business?



Thank you to the FEI Austin Sponsors

Platinum Sponsors



Gold Sponsors



CPE Credits

CPE Credits

Today's Professional Development session is worth 1.0 Continuing Professional Education (CPE) credits (pending approval).

To be eligible for CPE credit, you must:

- Answer **at least 3 of the 5 polling questions** (during the webinar) and have a total viewing time of **at least 50 minutes**.
- Participants will receive a CPE notification email when the credits are available.
(Typically, in 7-10 business days).
- We are unable to grant CPE credit in cases where technical difficulties preclude eligibility. CPE Program Sponsorship guidelines prohibit us from issuing credit to those not verified by the technology to have satisfied the minimum requirements as stated.
- In accordance with the standards for the National Registry of CPE Sponsors, CPE credit will be granted based on a 50-minute hour.

POLL #1 -

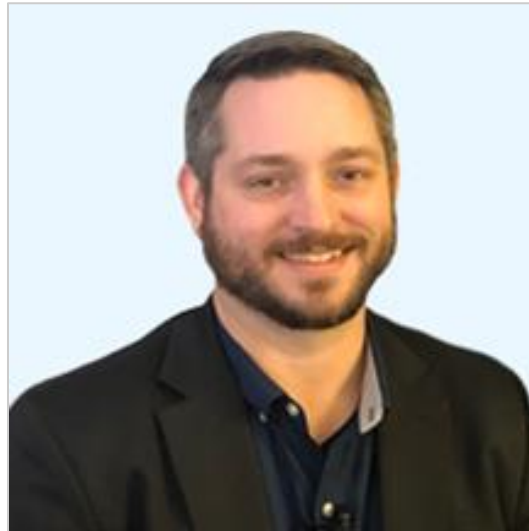
Do you wish to earn CPE credit today?

Source: <https://www.zdnet.com/article/google-north-korean-hackers-targeting-researchers-now-pretend-to-be-from-offensive-security-firm/>

The Acumera team



Bill Morrow
CEO



DeWayne Mangan
VP, Infrastructure &
Client Support





Robin Campana
CFO

Acumera: an industry leader

- Leading managed network service provider since 2002
- Listed on the [Visa](#) and [Mastercard](#) global registries of PCI compliant service providers
- [Participating organization](#) on the PCI Security Standards Council
- Level 1 PCI certified service provider
- Best-in-class network operations center (NOC)



Trusted by top brands

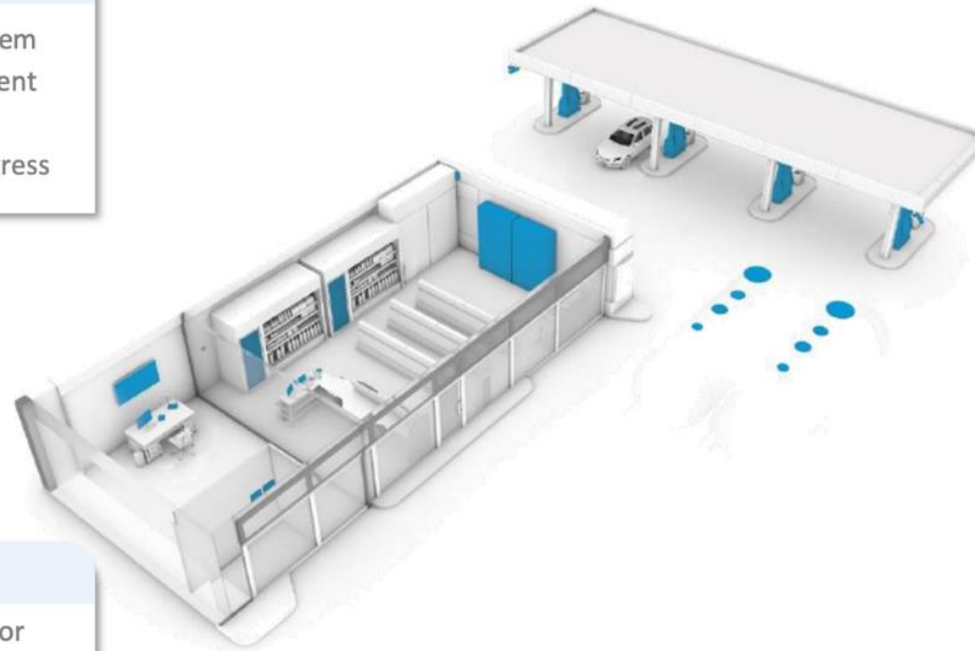
Convenience Store	  
Petroleum	  
Food Service	   
Manufacturing	  
Retail	  
Unmanned Sites	  
Service Providers	 

- 10,000 locations under management
- Locations in every state of the US, Canada and Mexico
- Technology certified for US, Canada, the UK and all of Europe
- Adding 300 plus locations per month
- 70,000 Edge Computing Workloads in the field

A unique approach

Above-Store Level

- » Operations support system
- » Digital estate management
- » Vendor integration
- » Secure analytics data egress



Store Level

- » Extensive cybersecurity
- » PCI DSS compliance
- » Ephemeral remote access
- » Payment security
- » Loyalty integration
- » Loss prevention
- » Equipment visibility

Below-Store Level

- » Customer counting / door monitoring
- » Space / cooler temperature monitoring
- » Energy consumption monitoring

Specialized Workloads

- » Fuel gauging and analytics
- » Dispenser monitoring
- » Safes and cash recyclers

Succeeding through COVID-19

Distribution Strategies⁽¹⁾

Direct

75%

- » Direct sales to multi-site enterprise and SMB operators
- » Enterprise sales to corporate headquarters of multi-site operators and other large offices

Channel

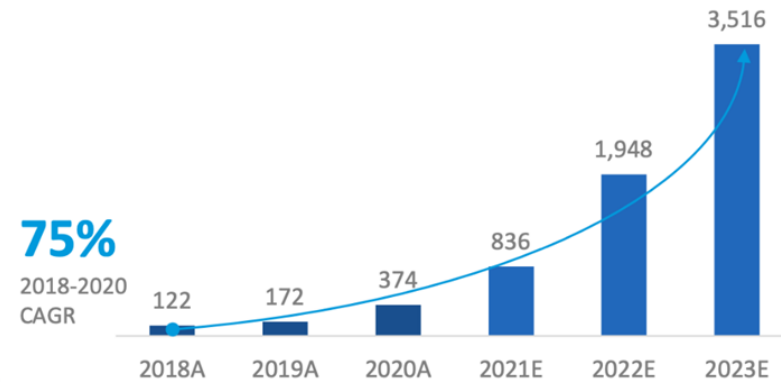
25%

- » Leverage existing channel partners to expand salesforce and improve site coverage
- » Sign up new channel partners to compound growth in new sites

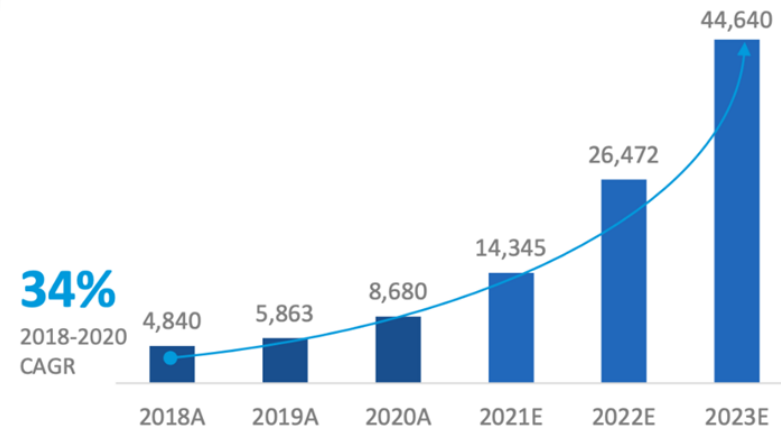
Target Verticals



Customer Count (EoY)



Active Sites (EoY)



Network security is crucial for all businesses



Multisite Businesses

- Clinics
- Dental Offices
- Auto Dealers
- Car & Truck Rental
- Printing/Graphic
- Graphic Design
- Vision Centers
- Flower Shops



Corporate & Regional Offices

- Business Services
- Real Estate Offices
- Law Firms
- Construction Co.
- Insurance Co.
- Mortgage Co.



Manufacturing

- Furniture
- Industrial Machinery
- Medical Devices
- Chemical
- Refinery
- Pharmaceuticals

POLL #2 -

Which one of these security firms is NOT a trustworthy source of information?

- The Sysadmin, Audit, Network, and Security Institute
- Cybersecurity and Infrastructure Security Agency
- SecuriElite
- Bleeping Computer

Source: <https://www.zdnet.com/article/google-north-korean-hackers-targeting-researchers-now-pretend-to-be-from-offensive-security-firm/>

Threats and Concerns?

New compliance frameworks	Increased activity by nation state actors	Governmental & regulatory changes
PCI DSS 4.0 General Data Protection Regulation (GDPR) California Consumer Privacy Act (CCPA) John Deere	Colonial Pipeline (Russian / Darkside) Solarwinds (Russia / Turla) 100% increase between 2017-2020 ¹	Cybersecurity Maturity Model Certification (CMMC) Executive Orders

¹<https://www.securitymagazine.com/articles/94995-academic-study-highlights-100-rise-in-nation-state-attacks-over-three-years>

Threats and Concerns?

- Permanence of virtual workforce & impacts of rushed work-from-home deployments
- 5G / increased impacts of IoT
- Legacy systems / integration with public cloud
- Public cloud migration / knowledge gaps
- Tool sprawl
- Availability of IT security personnel

Learning Objectives

How do you evaluate the security risk level for your company's network and business?

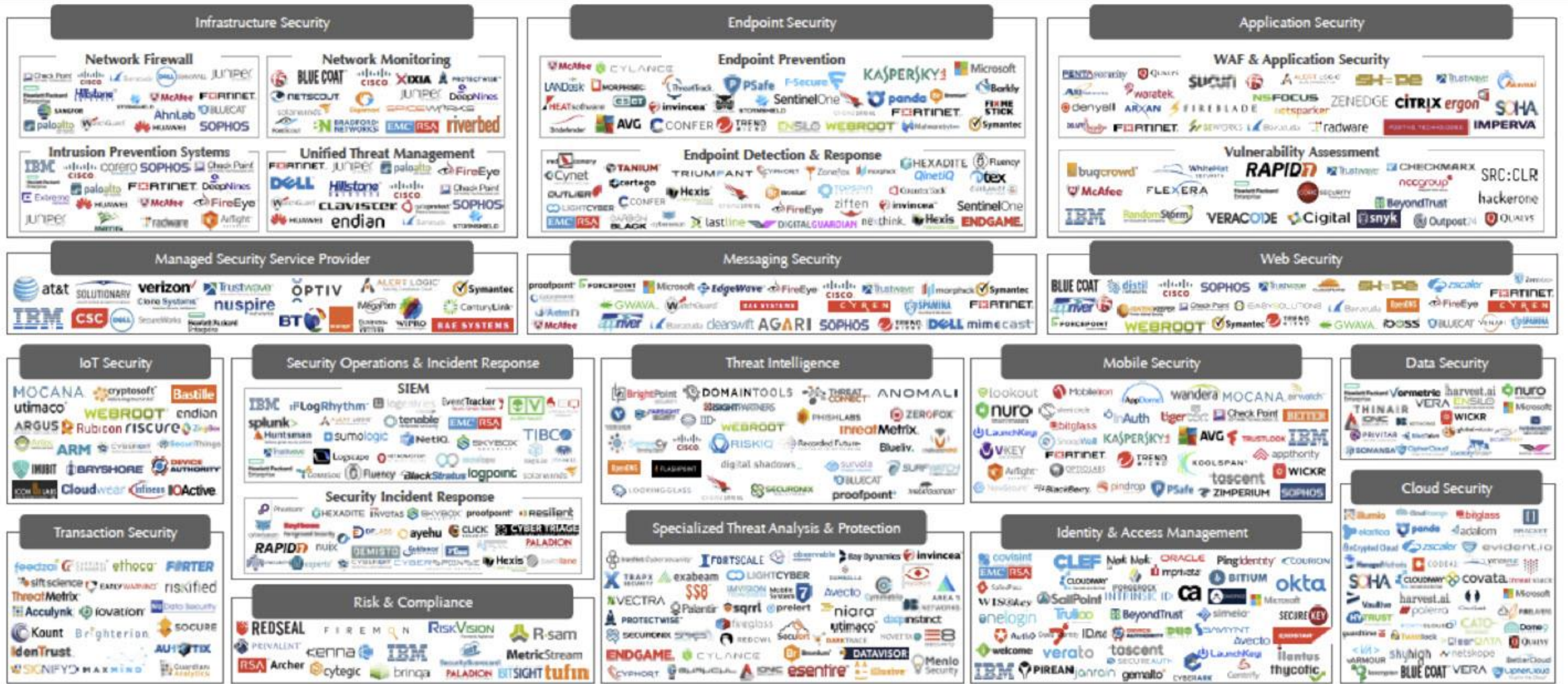
- Audit security tool usage & effectiveness
- Use a compliance framework
- Ensure you have complete network visibility
- Be proactive
- Choose trusted partners

POLL #3 -

Have you deployed a new IT security tool in the last twelve months?

Examples: new antimalware engine, new ransomware protection, new cloud access security broker, change out of firewall/edge security vendor, etc

Security Tool Usage / Cybersecurity universe



Security Tool Usage / Cybersecurity universe

- Best of Breed: SIXTEEN categories (in this model)
 - 1-1.5 FTE per tool
 - The accretive effect of tooling
 - Most organizations only use 30% of each tool's capabilities
- Platform approach
 - Broader coverage, targeted features
 - Fewer FTE, easier to outsource
 - When is good enough, good enough?

Source: <https://thecyberwire.com/podcasts/cyberwire-x/10/notes>

Security Tool Usage / Cybersecurity universe

Key Takeaways:

- Know the critical areas to secure for your business
- Have something, and use that something
- Don't underestimate the value of TRAINING as a cybersecurity defense

Source: <https://thecyberwire.com/podcasts/cyberwire-x/10/notes>

POLL #4 -

How concerned are you about the security of your work-from-home infrastructure?

- Not at all concerned
- Somewhat concerned
- Only a little concerned
- <startled> Huh? Sorry, I'm currently napping because of all of the sleep I've lost about this

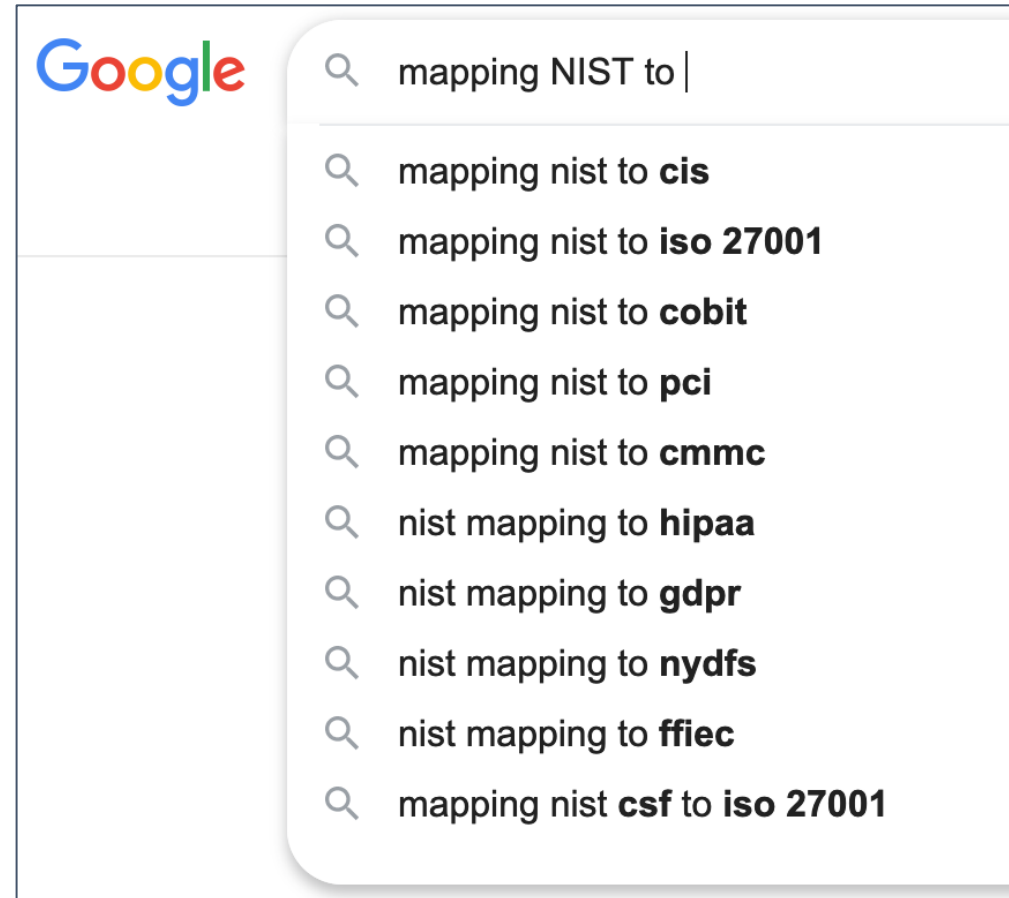
IT security frameworks

- PCI-DSS
- NIST
- CIS Benchmarks
- FedRAMP
- HIPAA
- SOX
- SOC I/II/III
- AT-101
- ISO 27001
- CMMC
- ...

- Why?
- How do you choose?
- What if I have one forced on me?
- Should I create my own?

IT security frameworks

- PCI-DSS
- NIST
- CIS Benchmarks
- FedRAMP
- HIPAA
- SOX
- SOC I/II/III
- AT-101
- ISO 27001
- CMMC
- ...



IT security frameworks

- PCI-DSS
- NIST
- CIS Benchmarks
- FedRAMP
- HIPAA
- SOX
- SOC I/II/III
- AT-101
- ISO 27001
- CMMC
- ...

Key takeaways:

- Frameworks provide consistency & baseline
- You should always try to do more
- When documenting your controls, always track the framework reference

Network visibility & reporting

“On average, companies take about 197 days to identify and 69 days to contain a breach according to IBM.”

- Growing complexity of the digital estate

Sources:

<https://www.varonis.com/blog/data-breach-response-times/>

https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf

Network visibility & reporting

“On average, companies take about 197 days to identify and 69 days to contain a breach according to IBM.”

- Growing complexity of the digital estate
- Blending day-to-day support with security response
 - The systems you use for support are the systems you'll use for investigations
 - Use it or be confused by it

Sources:

<https://www.varonis.com/blog/data-breach-response-times/>

https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf

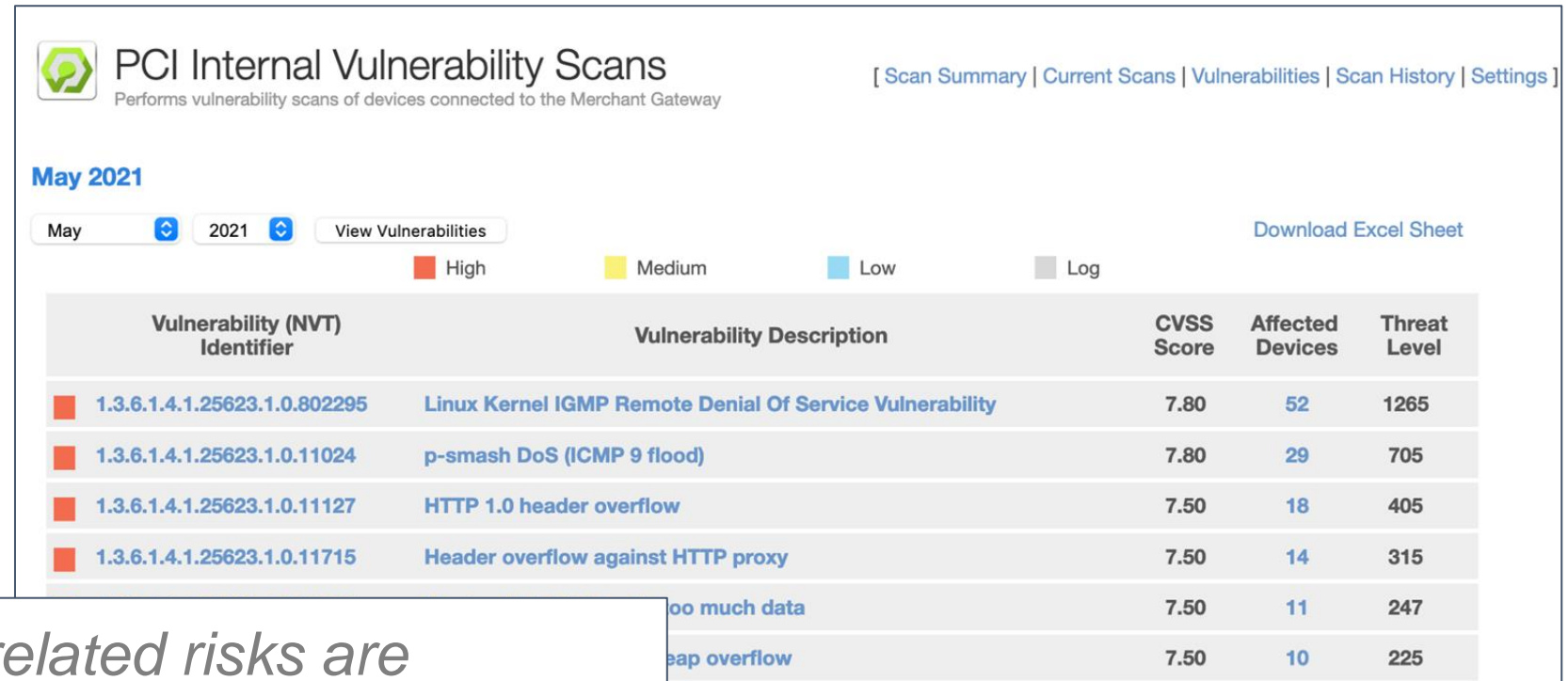
POLL #5 -

What is your favorite phishing email/text/phone call opening line?

- *I am writing this message to you with sadness*
- *Because you illegally downloaded files, your Internet access will be revoked*
- *USPS package AF456-78-21 delivery has delayed.
More info abc.xy/AF456*
- *We have been trying to reach you about your car's extended warranty*

Be proactive

- Table-top exercises
- Scanning
- Training



The screenshot shows the 'PCI Internal Vulnerability Scans' dashboard for May 2021. It includes a navigation menu, a legend for severity levels (High, Medium, Low, Log), and a table of vulnerabilities. The table columns are Vulnerability (NVT) Identifier, Vulnerability Description, CVSS Score, Affected Devices, and Threat Level.

Vulnerability (NVT) Identifier	Vulnerability Description	CVSS Score	Affected Devices	Threat Level
1.3.6.1.4.1.25623.1.0.802295	Linux Kernel IGMP Remote Denial Of Service Vulnerability	7.80	52	1265
1.3.6.1.4.1.25623.1.0.11024	p-smash DoS (ICMP 9 flood)	7.80	29	705
1.3.6.1.4.1.25623.1.0.11127	HTTP 1.0 header overflow	7.50	18	405
1.3.6.1.4.1.25623.1.0.11715	Header overflow against HTTP proxy	7.50	14	315
	oo much data	7.50	11	247
	heap overflow	7.50	10	225

*“Studies show security-related risks are **reduced by 70%** when businesses invest in cybersecurity awareness training.”*

Choosing a trusted partner

- How do their services work?
 - Support vs Managed Services
- Do they have a compliance framework?
 - Is the evidence readily available?
 - How much does it cover?
 - Are they willing to engage with your internal & external audit staff?
- How transparent are they with their services?
 - Do you have visibility?

Learning Objectives - Review

How do you evaluate the security risk level for your company's network and business?

- Audit security tool usage & effectiveness
- Use a compliance framework
- Ensure you have complete network visibility
- Be proactive
- Choose trusted partners



acumera.net

512.687.7410

sales@acumera.net

Complimentary Consultation

Email fei@acumera.net to schedule a complimentary security consultation as a thank you for your attendance today!



acumera.net

512.687.7410

sales@acumera.net