NVBDC Services Committee

Cybersecurity 201
Building & Operating Your Security Posture

NVBDC.ORG

Today’s Agenda

- Opening Remarks
- Meet Our Presenter
- Presentation
- Q&A
- Wrap-Up

NVBDC Services

In 2026, NVBDC is launching new international initiatives to expand global market access and exporting opportunities for certified veteran-owned businesses.

Connects NVBDC-certified Veteran-Owned Businesses with global buyers and distributors.

Offers financing, insurance, and loan guarantees to help VOBs compete globally.

Supports veteran-owned businesses with export loans and international training.

Expands NVBDC's international network across 195 countries.

NVBDC

Today’s Webinar Includes Live Polls

Polls will appear in a *Slido* pop-up throughout the presentation.

When prompted, please keep the pop-up open and join the conversation!

NVBDC Services

Meet Our Presenter

Mike Rutallie
Founder & CEO
ValorPoint

NVBDC Services

CYBERSECURITY FUNDAMENTALS 201

CYBERSECURITY FOR SMB · LEVEL 2

Building & operating your security posture, for small business.

MIKE RUTALLIE · CISSP
Founder & CEO, Valorpoint

VALOR POINT

YOUR PRESENTER

Mike Rutallie

Founder & CEO, ValorPoint

CISSP	Certified Information Systems Security Professional
M.A.	Michigan State University: Masters in Management, Leadership, and Strategy
CAPT	Air Force Officer: Cybersecurity Director, Cyber Defence Operations
Exp	20+ years leading teams in Cyber, IT Infrastructure, & Software Development

VALOR|POINT

NVBDC Certified · SBA SDVOSB Certified

you

OPENING · TODAY'S FOCUS

101 WAS THE BASICS.
201 BUILDS THE PROGRAM.

This is an awareness session, not a compliance-readiness course.

WHERE WE LEFT OFF · 101

- Threats to SMBs, email & account security, device security, backups
- Payments, AI tools, incident-response basics
- The 80% of risk closed by 20% of effort

WHAT 201 ADDS

- Frameworks to score yourself: NIST CSF 2.0 and CIS IG1
- Governance basics which insurers and clients ask for
- The compliance frameworks you should recognize
- Third-party risk, monitoring & MDR, operational IR

WHAT THIS IS NOT

- A compliance implementation course
- Legal or compliance advice for your business
- A replacement for engaged counsel where regulations apply

Takeaways: You will receive 3 takeaways related to Incident Response, Vendor vetting, and a Self-Assessment

OPENING

WHY BUILD A PROGRAM, NOT JUST A CHECKLIST

Security stopped being an IT cost. It's now a condition of doing business.

INSURERS

Cyber liability is now a core underwriting requirement.

- No written program = difficult or no renewal.
- MFA and backups are basic requirements
- Gaps can lead to massive premium hikes.

ENTERPRISE CLIENTS

You are a link in your clients' supply chain.

- Align with known frameworks
- Third-party tools are used to grade your company.
- "Working on it" could cost you a contract.

FEDERAL CONTRACTS

Federal security mandates are strictly enforced.

- CMMC is mandatory for DoD work.
- Fed contracts follow

  Basic - FAR 52.204-21
  CUI data - NIST 800-171
- Flow-down rules apply to subcontractors.

$255K+

Remember the average cost of an SMB breach?

Building a program is often cheaper than an incident, and increasingly cheaper than losing the contract.

The point: when insurers, clients, and the government all check, security becomes a revenue gate.

POLL 01 · PULSE CHECK

WHERE ARE YOU TODAY?

Pick the one that fits best.

- **A** Have basic cybersecurity tools in place · no written policies or assessment
- **B** Written policies created · not aligned with any framework
- **C** Working toward a specific framework · CMMC, NIST CSF, ISO 27001, CIS, SOC 2, HIPAA
- **D** Already aligned with a framework

KNOW WHERE YOU STAND.

01

You cannot improve what you have not measured. Today, you measure.

PART 01 · MEASURE YOURSELF

TWO FRAMEWORKS BUILT FOR SMBS

Both free. Both built for businesses without a security team.

NIST CSF 2.0 + SP 1300

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Six plain-English functions your insurers, clients, and government already speak.

Start here: the Small Business Quick-Start Guide (SP 1300). The SMB on-ramp to the same six functions.

FREE · NIST.GOV/ITL/SMALLBUSINESSCYBER

CIS Controls v8.1 + IG1

CENTER FOR INTERNET SECURITY

Start here: Implementation Group 1: the essential set of roughly 56 safeguards for limited-resource orgs.

The free workbook tags every item by priority, so you know what to do first.

FREE · CISECURITY.ORG/CONTROLS

NIST tells the story your insurers and clients understand. **CIS** tells you how to do it.

Source: NIST CSF 2.0 · NIST SP 1300 · CIS Controls v8.1

NIST CSF 2.0

How to frame business risk.

01 GOVERN
Who owns risk? What's our policy and tolerance?

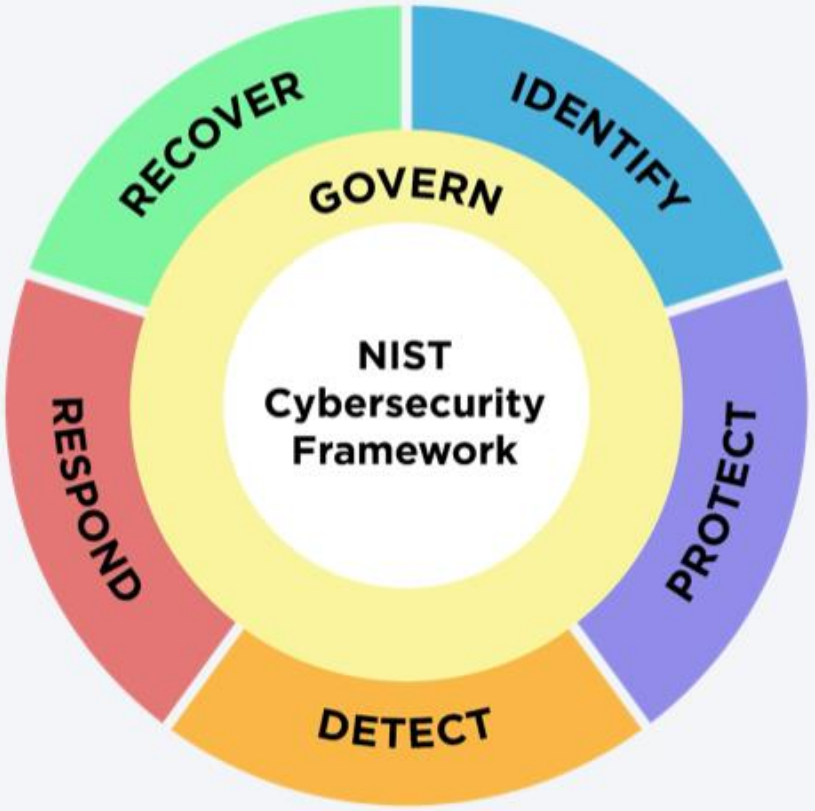
02 IDENTIFY
What do we have? What matters most?

03 PROTECT
Safeguards: access, data, training.

04 DETECT
Find the bad activity.

05 RESPOND
Contain. Communicate. Learn.

06 RECOVER
Restore. Improve. Keep operating.



Source: NIST Cybersecurity Framework 2.0 · NIST SP 1300

PART 01 · CIS IG1

CIS IG1: THE ESSENTIAL SET

56 IG1 safeguards across 15 of the 18 controls.
Start with these six.

CIS Center for Internet Security®

01
KNOW YOUR DEVICES
List every computer, phone, tablet.

02
KNOW YOUR SOFTWARE
What's installed and who uses it.

03
LOCK DOWN ADMINS
Few admins. MFA on all of them.

04
MFA EVERYWHERE
Email, banking, cloud, accounting.

05
BACKUP YOUR DATA
And test a restore.

06
TRAIN YOUR PEOPLE
Short, regular, documented.

Download the the **CIS CONTROLS v8.1:** https://www.cisecurity.org/controls/v8-1

Source: Center for Internet Security · CIS Controls v8.1 · Implementation Guide for SMEs

PART 01 · TAKEAWAY 1

THE 90-MINUTE SELF-ASSESSMENT

One sitting. One person. One honest score.

OPEN THE WORKSHEET

Takeaway 1: Security Posture Self-Assessment.

SCORE 0 TO 3

Each of the six NIST functions. 0 is not in place, 3 is formal and verified.

THE THREE LOWEST

Those functions are where the next quarter goes.

THREE GAPS EACH

Specific safeguards drawn from CIS IG1.

SET OWNER AND DATE

That is your next 90 days. Owner, due date, done.

#	Question (plain English)	Maps to (CIS IG1)	Score 0–3
GOVERN			
G1	Someone is clearly accountable for security decisions	CSF GOVERN · CIS 14/17	3
G2	Core policies exist in writing, signed & dated (acceptable use, access, data handling, IR)	CIS 14	2
G3	We know which compliance rules could apply to us (state breach, CMMC, GDPR…)	CSF GOVERN	1
IDENTIFY			
I1	We keep a current list of all work devices (computers, phones, tablets)	CIS 1	3

FUNCTION	SCORE	FOCUS?
GOVERN	2.0	◄ FOCUS
IDENTIFY	2.7	
PROTECT	2.0	◄ FOCUS
DETECT	0.5	◄ FOCUS
RESPOND	2.0	◄ FOCUS
RECOVER	2.5	

An assessment by your own IT provider is not an independent assessment. · Source: NIST SP 1300

PART 02 OF 08

GOVERNANCE & COMPLIANCE AWARENESS.

02

Policy, plus the compliance frameworks you should recognize.

PART 02 · GOVERNANCE

POLICY IS A CONTROL

Three reasons it matters more than you think.

IT IS A CONTROL

NIST counts written policy as a control to score the GOVERN function. No policy, no score.

INSURERS REQUIRE IT

2026 renewal questionnaires assume AUP, access control, IR, and data handling in writing.

ENTERPRISE CLIENTS REQUIRE IT

Procurement asks. Be able to answer confidently.

THE FOUR POLICIES EVERY SMB NEEDS

Acceptable Use : what employees can and can't do with systems and data.

Access Control: who gets in, how it's granted, how it's revoked.

Data Handling : what you have, where it can live, what can be done with it (e.g. sharing).

Incident Response : who decides, who calls who, what gets documented.

Start with templates from SBA, CISA, SANS. Cut what doesn't apply. Sign, date, store. · CIS Controls v8.1 (03, 05, 06, 17)

THE COMPLIANCE LANDSCAPE

Recognize them when they show up.

STATE BREACH LAWS

Trigger: you hold personal data of US residents in any of the 50 states.

Call your Insurance carrier + legal counsel within hours. The clock starts at awareness.

CMMC 2.0

Trigger: you handle FCI/CUI on a DoD contract (in contracts since Nov 2025).

Check for the CMMC clause.
If present: explore certification paths

SOC 2

Trigger: an enterprise client asks for it, not a law.

Don't start until 3+ clients ask. Depends on what customer data you store/access.

GDPR

Trigger: you process data of EU residents.

Selling online? Check for EU customers.
72-hour breach notice if hit.

EXPORT ONLY

EAR

Trigger: you export commercial or dual-use tech. Screen every export against the BIS Entity List. May need a license.

EXPORT ONLY

ITAR

Trigger: you handle defense articles or technical data. Register with DDTC first. "

This training is not legal or compliance advice. Engage qualified counsel.

POLL 02 · COMPLIANCE REALITY

WHICH REGULATIONS MIGHT APPLY TO YOUR BUSINESS?

Multi-select. Don't overthink it.

- **A** State breach notification laws
- **B** CMMC 2.0 · DoD supply chain
- **C** SOC 2 · asked for by enterprise client
- **D** GDPR · EU residents in your data
- **E** EAR · commercial / dual-use export
- **F** ITAR · defense articles or technical data
- **G** None of these (yet)

DOMAIN & EMAIL AUTHENTICATION.

03

101 protected your inbox. 201 protects your domain.

PART 03 · DNS

EMAIL AUTHENTICATION PROTOCOLS

Three DNS records which stop different attacks on your email.

SPF

SENDER POLICY FRAMEWORK

Lists which servers may send email from your domain, blocking servers that spoof you.

DKIM

DOMAIN KEYS IDENTIFIED MAIL

Cryptographically signs every email so the recipient can verify nothing was tampered with.

DMARC

MOST IMPORTANT OF THE THREE

Tells recipients what to do if SPF or DKIM fails: monitor, quarantine, or reject, and reports who's sending as you.

WHY YOUR DNS/DOMAIN RECORDS ARE HIGHLY SENSITIVE

ROOT OF IDENTITY

Technical proof of genuine business email. Keys to your domain's reputation.

AUTHORITY TO ACT

Modifying SPF allows attackers to send messages as you.

DIRECT FRAUD ACCESS

Lack of DMARC enforcement enables the "easy version" of BEC.

Sources: RFC 7208 (SPF) · RFC 6376 (DKIM) · RFC 7489 (DMARC)

PROTECT YOUR DOMAIN

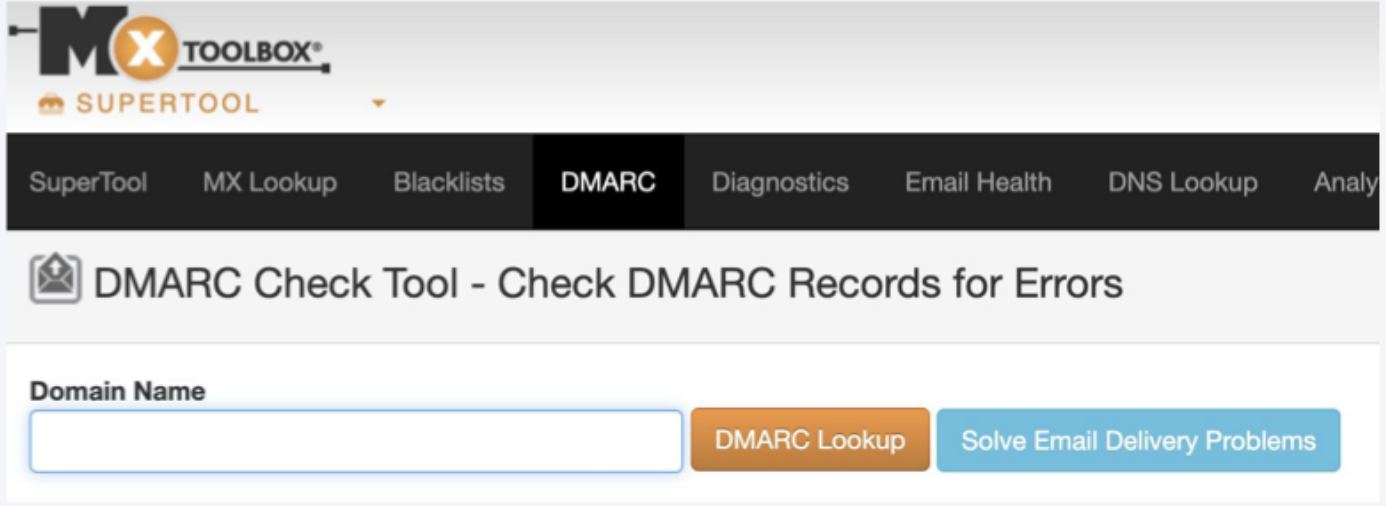
In 2024 Domain authentication went from best practice to table stakes.

CHECK YOUR DOMAIN IN 60 SECONDS

MXToolbox.com: run SPF, DKIM, DMARC checks.

Dmarcian.com: free DMARC+SPF+DKIM analyzer

https://dmarcian.com/domain-checker/



DMARC Enforcement

NONE

- Monitor only
- Collect reports
- No enforcement

QUARANTINE

- Partial enforcement
- Treat as suspicious
- Send to spam/junk

REJECT

- Full enforcement
- Block failed mail
- Strongest protection

CLOUD & SHARED RESPONSIBILITY.

04

Your provider secures the cloud. You secure what you put in it.

THE SHARED RESPONSIBILITY MODEL

Same model for Microsoft 365, Google Workspace, AWS, Azure, GCP.

PROVIDER'S JOB

- Physical security of data centers.
- Platform availability and patching.
- Network and DDoS protection at the perimeter.
- Encryption at rest (provider-managed keys).

YOUR JOB

- User identity, MFA, account management.
- Permissions on every file, share, folder.
- External sharing policies.
- Endpoint security on devices accessing the cloud.
- **Backup of cloud data:** yes, even in M365 and Workspace.

Microsoft and Google don't backup your data the way you think. That's your job.

· Microsoft Shared Responsibility · Google shared-fate model

PART 04 · CLOUD AUDIT

THE FIVE MOST COMMON MISCONFIGURATIONS

Found in nearly every SMB cloud audit. Fix this ASAP.

01

NO ADMIN MFA

Global admin without MFA, or a shared admin account.

02

LEGACY AUTH ON

POP3, IMAP, SMTP AUTH still on. They bypass MFA.

03

OPEN SHARING

Anyone shares anything. No expiration, no review.

04

NO LOGIN RULES

Same login allowed from any country, device, or time.

05

SHORT LOG RETENTION

Default is often weeks. When you need them, they're gone.

PRO TIP: Unlicensed ADMIN account on Microsoft/Google

Microsoft and Google provide free "Admin-only" or "Cloud Identity" licenses specifically for console management. Use these for a dedicated admin account to ensure your daily-driver account for email and apps are strictly separated from sensitive global administrative access.

Sources: Microsoft Secure Score baselines · CIS Microsoft 365 Foundations Benchmark

NETWORK SECURITY.

05

Four network security concepts. Whether you manage it yourself or hand it to an IT provider.

FOUR CONCEPTS WORTH KNOWING

You don’t have to build these. You should ask for them.

DNS FILTERING

A free, network-level control that blocks known malicious domains before they reach any device.

DEFAULT CREDENTIALS

Routers, cameras, printers, and access points ship with factory passwords attackers already know. Ask when yours were last changed.

KNOWN VULNERABILITIES (CVEs)

Attackers use documented weaknesses, not secret ones. MITRE publishes vulnerabilities known as CVEs. Ask your IT provider if they track it for your hardware.

SEGMENTATION

Separate networks for guests, payments, operations, and IoT. A breach in one can't reach the others.

Sources: CIS Controls v8.1 (03, 12, 13) · MITRE CVE Program (cve.org) · Cloudflare / Quad9 DNS filtering

PART 05 · Segmentation

SEGMENTATION CREATES BARRIERS

No new hardware. Most business firewalls/Wifi already support this.

01 GUESTS ON THEIR OWN WI-FI

Never the business network. Most routers already do this today.

02 ISOLATE YOUR IOT

Cameras, smart TVs, and thermostats on their own VLAN or guest network.

03 SEPARATE PAYMENTS

If you take credit cards, PCI requires it. It also limits the blast radius.

04 PRESS YOUR IT PROVIDER

Ask if segmentation is actually configured, not just assumed.

ASK: "If one laptop gets infected, what else can it reach, and how do you know?"

A specific answer means it's configured. A vague answer is your gap.

Source: PCI DSS v4.0 · CIS Controls v8.1 (12, 13)

THIRD-PARTY & SUPPLY-CHAIN RISK.

06

Their security is now your security. Your risk is the sum of your vendors' risk.

PART 06 · THE SHIFT

REVIEW: YOUR RISK IS THEIR RISK

Attackers stopped breaking down the front door.
They walk in through your vendors.

YOUR IT PROVIDER

Has admin access to everything you own. They are the keys to your entire digital kingdom.

YOUR SOFTWARE VENDORS

A compromised update ships malware straight into your network. Trusted software is the perfect Trojan horse.

YOUR DATA PLATFORMS

Contains client and employee data. A breach potentially exposes information under NDA or privileged data which you are accountable for.

~1/3 Roughly a third of breaches now involve a third party, **double the prior year.**

Source: Verizon 2025 Data Breach Investigations Report

PART 06 · TAKEAWAY 2

THE FIVE-QUESTION VENDOR REVIEW

For any vendor that touches your data or systems. Ask before you sign.

1. Can you share a SOC 2 report or security summary?
2. Do you enforce MFA on your own systems and admins?
3. How and when will you notify us of a breach?
4. Where is our data stored, and is it encrypted?
5. Who has access to our data on your side, and how is it controlled?

You're not auditing them. You're watching **how they answer.** Specific = mature. Defensive or vague = your risk.

POLL 03 · GUT CHECK

COULD YOU ANSWER THESE FIVE QUESTIONS ABOUT YOUR OWN VENDORS?

A Yes · we review vendors before we sign

B Some · for the big ones, not all

C No · but we have a list of our vendors

D No · and I'm not sure who all our vendors are

Reference: The Five Questions

1. Can you share a SOC 2 report or security summary?
2. Do you enforce MFA on your own systems and admins?
3. How and when will you notify us of a breach?
4. Where is our data stored, and is it encrypted?
5. Who has access to our data on your side, and how is it controlled?

PART 06 · EMERGING RISK

AI IS A VENDOR TOO

It is likely that every AI tool your team uses is a third party.

RISK 01

DATA LEAKAGE

Staff paste client data, financials, or code into public AI tools, where it may train the model.

RISK 02

SHADOW AI

Tools adopted without review. You can't secure what you don't know is in use.

RISK 03

AI SUPPLY CHAIN

You inherit their dependencies. Vulnerabilities in a vendor's base model or training data flow directly to you.

THE FIX

A one-page AI policy

Don't ban AI. That just creates shadow AI. Govern it.

- ✓ **Approved tools only.** Name what the team may use.
- ✓ **Never paste** client data, financials, or code into public tools.
- ✓ **Business accounts** with training opt-out, not personal logins.

Source: NIST AI Risk Management Framework (AI RMF 1.0)

PART 06 · EXPORT-CONTROLLED ONLY

IF YOU EXPORT: DUE DILIGENCE IS REQUIRED

SCREEN EVERY PARTY

Check customers, vendors, and partners against the BIS Entity List and OFAC SDN list. The free Consolidated Screening List covers both.

Free tool · trade.gov/csl

CONTROL TECHNICAL DATA

Export-controlled data has access rules, including who may view it from abroad, even remotely.

bis.doc.gov · pmddtc.state.gov

DOCUMENT EVERYTHING

Keep dated records of every screening. "We checked" without proof is not a defense.

ofac.treasury.gov

Penalties can be **criminal**, not just civil. When in doubt, get export-control counsel before you ship.

This is awareness, not legal advice. · Sources: BIS (15 CFR 730–774) · DDTC (22 CFR 120–130) · OFAC

KNOW YOUR THIRD-PARTY RISK SCORE.

See your score for free to know what clients and insurers see about you.

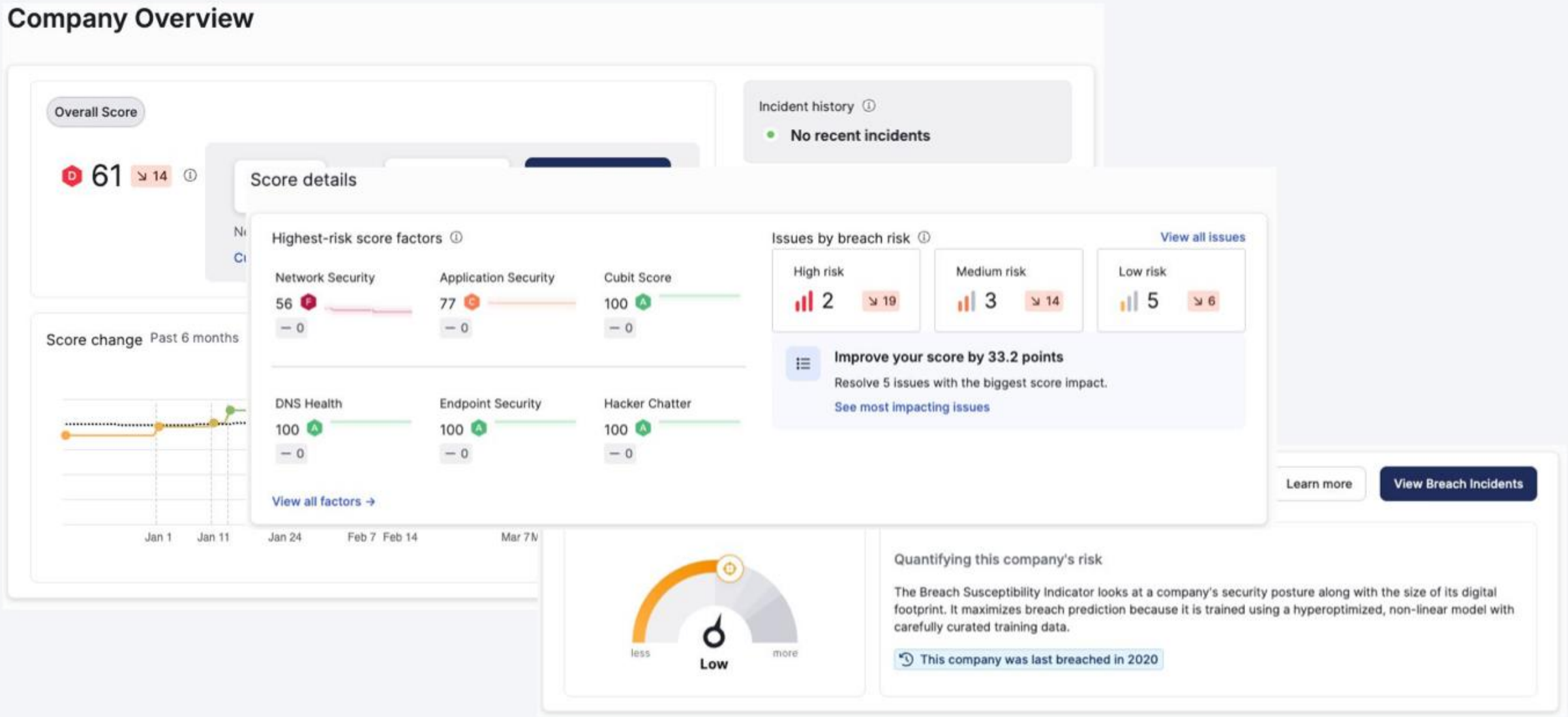
Multiple TPRM platforms enable you to:

- **Visibility:** Monitor your own rating; what score vendors see about you.
- **Benchmark:** Compare your own security posture against industry standards.
- **Audit:** Perform rapid due diligence on potential vendors before signing.

UpGuard	riskrecon mastercard	BITSIGHT	Security Scorecard
upguard.com	bitsight.com	securityscorecard.com	riskrecon.com

A score doesn't mean pass or fail, but gives an idea of the vendor's cybersecurity posture.

Sources: SecurityScorecard (securityscorecard.com) · UpGuard (upguard.com) · RiskRecon by Mastercard (riskrecon.com) · Bitsight (bitsight.com)



Sources: SecurityScorecard (securityscorecard.com) · UpGuard (upguard.com) · RiskRecon by Mastercard (riskrecon.com) · Bitsight (bitsight.com)

MONITORING & DETECTION.

07

The average breach goes undetected for months. The goal: cut that to hours.

PART 07 · THE GAP

LOGGING IS NOT DETECTING

Most SMBs collect logs no one ever reads. That's evidence, not defense.

WHAT MOST HAVE RIGHT NOW

Log Aggregation: A central record of Firewall, M365, and Workspace events that happened, **after the fact.**

Standard Retention: Logs are often overwritten in weeks, erasing critical evidence before you even know you were hit.

Passive EDR/Antivirus: Software installed on devices that blocks known threats but remains silent during sophisticated, "low and slow" attacks.

WHAT THEY ACTUALLY NEED

Continuous Visibility: Automated systems monitoring telemetry from every endpoint to spot anomalies in real-time.

Rapid Response: Expert analysts who can instantly isolate a compromised machine the second a suspicious alert fires.

Uninterrupted Vigilance: Coverage that doesn't sleep. Protecting your network at **2 a.m. on holidays**.

~200 days

Median time to identify and contain a breach.
The tools to shrink that are now affordable at SMB scale.

Source: IBM Cost of a Data Breach Report 2024

PART 07 · THE ANSWER

DON'T BUILD A SOC. BUY MDR.

Managed Detection & Response: a 24/7 security team you rent, not hire.

WATCHES THE MUNDANE

Real analysts checking logs and alerts of your endpoints and cloud, 24/7/365.

RESPONDS, NOT JUST ALERTS

They isolate the infected machine instead of emailing you.

PRICED FOR SMBS

Per endpoint, per month. Far less than one analyst's salary.

EDR is the tool. **MDR** is that tool plus the people who watch it. **You want the people.**

MDR is often offered as an add-on service directly by EDR vendors.

BEFORE YOU SIGN

Ask three questions

01 **Do humans respond, or do you only get an alert?**

02 **What is your mean time to respond?**

03 **Can you actively isolate a device, or only notify us?**

Source: CIS Controls v8.1 (08, 13)

INCIDENT RESPONSE.

08

101 covered the basics. 201 makes it operational, well before you need it.

THE INCIDENT-RESPONSE LIFECYCLE

Four phases, straight from NIST. Decide them now, not at 2 a.m.

01

PREPARE

Plan, contacts, and backups in place before anything happens.

02

DETECT & ANALYZE

Know it's happening and understand the scope.

03

CONTAIN

Isolate the affected systems to stop the spread.

04

ERADICATE

Remove the threat and clean compromised systems.

05

RECOVER

Restore normal operations and verify functionality.

06

POST-INCIDENT

Lessons learned and process improvements.

The phase that saves you is **Prepare.** Everything else is easier because of it.

Source: NIST SP 800-61r3 (Incident Response Recommendations & Considerations)

THE ONE-PAGE INCIDENT PLAN

Printed. In a binder. Not in the cloud you can't reach during a ransomware attack.

WHO DECIDES

The one person who declares an incident and can authorize spend.

WHO YOU CALL

IT/MDR, cyber-insurance hotline, attorney, key clients.

INSURANCE FIRST

Call the carrier hotline **before** you act. They bring the experts and they're (hopefully) paying.

WHAT YOU DO

Disconnect, don't power off. Powering off can destroy forensic evidence.

WHAT YOU DON'T DO

Don't pay, don't negotiate, don't post until counsel and the carrier weigh in.

WHERE IT LIVES

On paper, offline. The plan you can't open is no plan at all.

Build it from Takeaway 3: the one-page incident-response template. · Source: NIST SP 800-61r3

PART 08 · THE HARD PART

COMMUNICATING UNDER PRESSURE

The breach is technical. The damage is reputational. Decide the rules now.

01 LEGAL DUTIES HAVE CLOCKS

State laws, GDPR (72 hrs), and contracts set deadlines. The clock starts at awareness.

02 COUNSEL REVIEWS FIRST

What you say early can create liability. Get the message reviewed before it goes out.

03 TELL CLIENTS YOURSELF

Honest and early beats silent and exposed. Reach them before they read it elsewhere.

04 ONE SPOKESPERSON

Brief the team. Everyone else routes questions to that single person.

Run a tabletop exercise

Practice and test your reaction before a real incident occurs. A low-stakes way to find gaps in your plan and build team muscle memory.

This is awareness, not legal advice. Your obligations depend on your data, your states, and your contracts.

WRAPPING UP

NEXT STEPS.

BRINGING IT TOGETHER

YOUR NEXT 90 DAYS

Don't try to boil the ocean. Do these, in this order.

THIS WEEK

1. Run the self-assessment (Takeaway 1).
2. Check your domain: SPF, DKIM, DMARC.
3. Confirm MFA on every admin account.

THIS MONTH

1. Write the four core policies.
2. Run the 5-question review on your top vendors (Takeaway 2).
3. Fill in the Incident Response Plan (Takeaway 3).

THIS QUARTER

1. Work through the findings from the self-assessment.
2. Run a tabletop exercise
3. Ensure compliance with your Cyber Insurance policy.

MAKE PROGRESS: Three lowest scores. Identify gaps inside each. **Execute.** That's the whole program.

POLL 04 · YOUR COMMITMENT

WHAT'S YOUR FIRST MOVE THIS WEEK?

Pick one. Then actually do it.

- **A** Run the self-assessment and get my score (Takeaway 1)
- **B** Check my domain · SPF, DKIM, DMARC
- **C** Confirm MFA on every admin account
- **D** Send the vendor review questions to my top vendor (Takeaway 2)
- **E** Print the one-page incident plan (Takeaway 3)

RESOURCES

TAKE THESE WITH YOU

Three worksheets and the free tools we referenced today.

TAKEAWAYS

01 Security Posture Self-Assessment: score the six NIST functions.

02 Five-Question Vendor Review: for every vendor that touches your data.

03 Incident Response Plan: who decides, who you call, what you do.

FREE RESOURCES

NIST: nist.gov/itl/smallbusinesscyber
(CSF 2.0 + SP 1300)

CIS: cisecurity.org/controls
IG1 workbook

MXToolbox: mxtoolbox.com
Check your domain for SPF, DKIM, DMARC today

FTC: ftc.gov/cybersecurity
Guides and videos for non-technical owners

GCA Toolkit: gcatoolkit.org/smallbusiness
CIS-based, Mastercard-backed, no IT required

Everything here is free. The only cost is deciding to start.

QUESTIONS & DISCUSSION

NOW IS THE TIME.
BUILD YOUR PROGRAM.

Questions???

MIKE RUTALLIE · CISSP
Founder & CEO, Valorpoint · mike.rutallie@valorpoint.co

NVBDC Events

View All Events & Register Today!

NVBDC.org/events

Upcoming Mastering Resources Webinars:

- **From Foundation to Growth: Building Talent with H.O.P.E. and Vanguard Rising**
  Thursday, June 25 – 11:00 a.m. to 12:30 p.m. ET

Upcoming Digital Readiness Webinars:

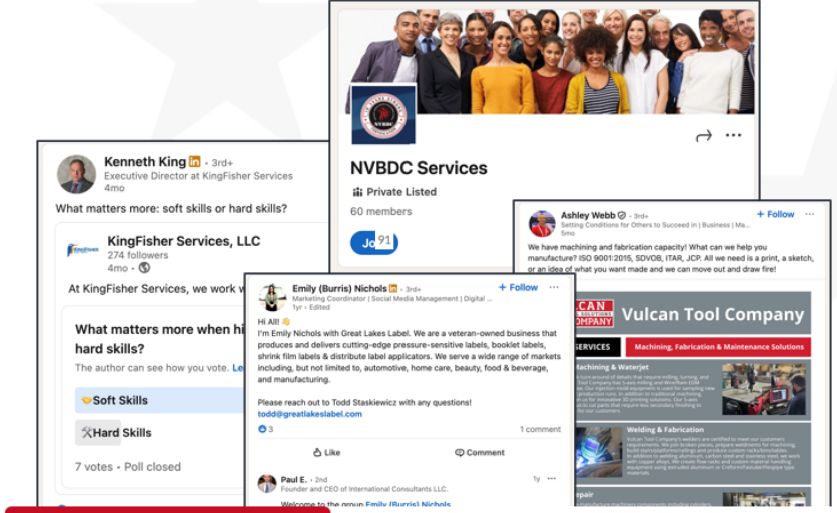
- **AI Advantage 101: Using Artificial Intelligence To Grow and Scale**
  Tuesday July 14, 2026 – 11:00 a.m. to 1:00 p.m. ET

- **AI Advantage 201**
  Thursday July 23, 2026 – 11:00 a.m. to 1:00 p.m. ET

Missed a webinar or want to rewatch? Access recordings at NVBDC.org!

Stay tuned, more powerful webinars are on the way!
We're continuing to equip veteran business owners with the digital training, tools, resources and insights needed to scale both domestically and internationally.

Veteran-to-Veteran LinkedIn Group



LinkedIn®

A place for NVBDC Certified SD/VOB's to connect, build relationships and share business successes and challenges.

Corporate Members are encouraged to join and participate in the conversation!

Join NVBDC Services LinkedIn Group

NVBDC Services

We value your feedback!

Scan here or visit
bit.ly/49cMMKn

Please take a moment to complete our post-event survey. It only takes a few minutes and helps us improve future programming, resources and engagement opportunities.

Your input helps us better serve the Veteran business community!

NVBDC Services

Meet the Team

John (“JT”) E. Taylor
Services Committee Chairman
NVBDC Board of Directors

Annette Stevenson, US Army Veteran, CPSD, C.P.M.
NVBDC Board of Directors
Services Committee

David Brazda
Co-Treasurer, NVBDC
NVBDC Board of Directors

LTC (Ret) Kathryn M. Poynton
Director, MVO Task Force
NVBDC Board of Directors

Tammi Hart
Senior Vice President, NVBDC
Services Committee

Toni Moses
Relationship Manager,
Certification Committee
Services Committee

Thank You For Joining Us Today!

Cybersecurity 201
Building & Operating Your Security Posture