

Don't be the next cyber statistic!

Why Cybersecurity Is A Shared Responsibility

Presented by:

Brian Lau
DIRECTOR

Michael Esolda
PUBLIC SECTOR
CYBERSECURITY ADVISOR

28 WORLDS FAIR DRIVE
SOMERSET NJ 08873

732.507.7346
D2CYBERSECURITY.COM



Who We Are

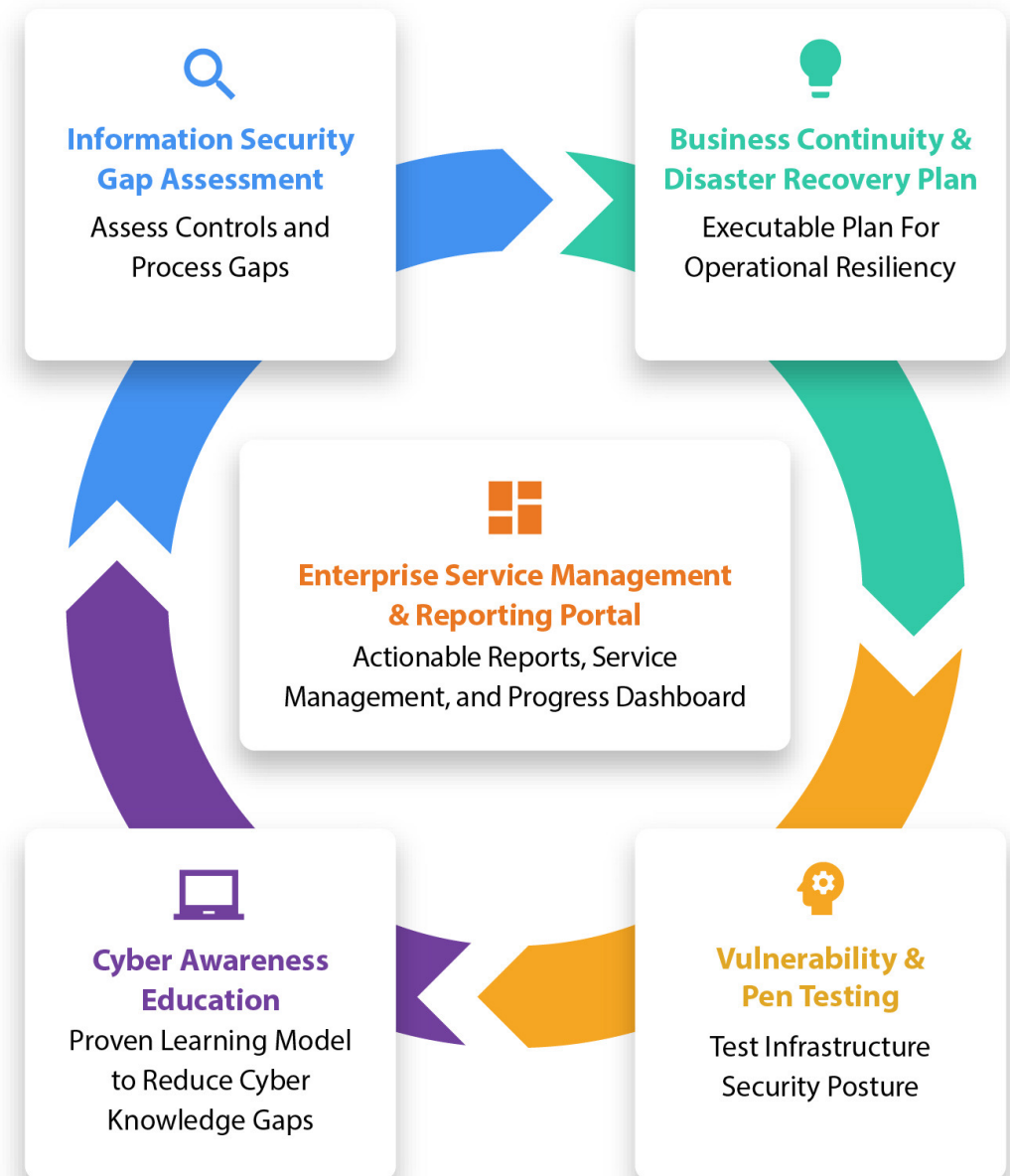
- NJGMIS Member since 2018
- We are a woman and minority-owned small business enterprise certified with the Women's Business Enterprise National Council (WBENC) and National Minority Supplier Development Council (NMSDC). Located in Somerset, NJ.
- Our clients range from Exelon, largest power holding company in the US, to small and local towns near you
- We work with all levels of the organization to implement Cybersecurity controls and changes
- D2 works with over 65% of NJ municipalities and 1/3 of all NJ public entities in NJ.
- Worked with the IT angle, procurement, Insurance, Higher Education



D2's holistic approach to risk reduction

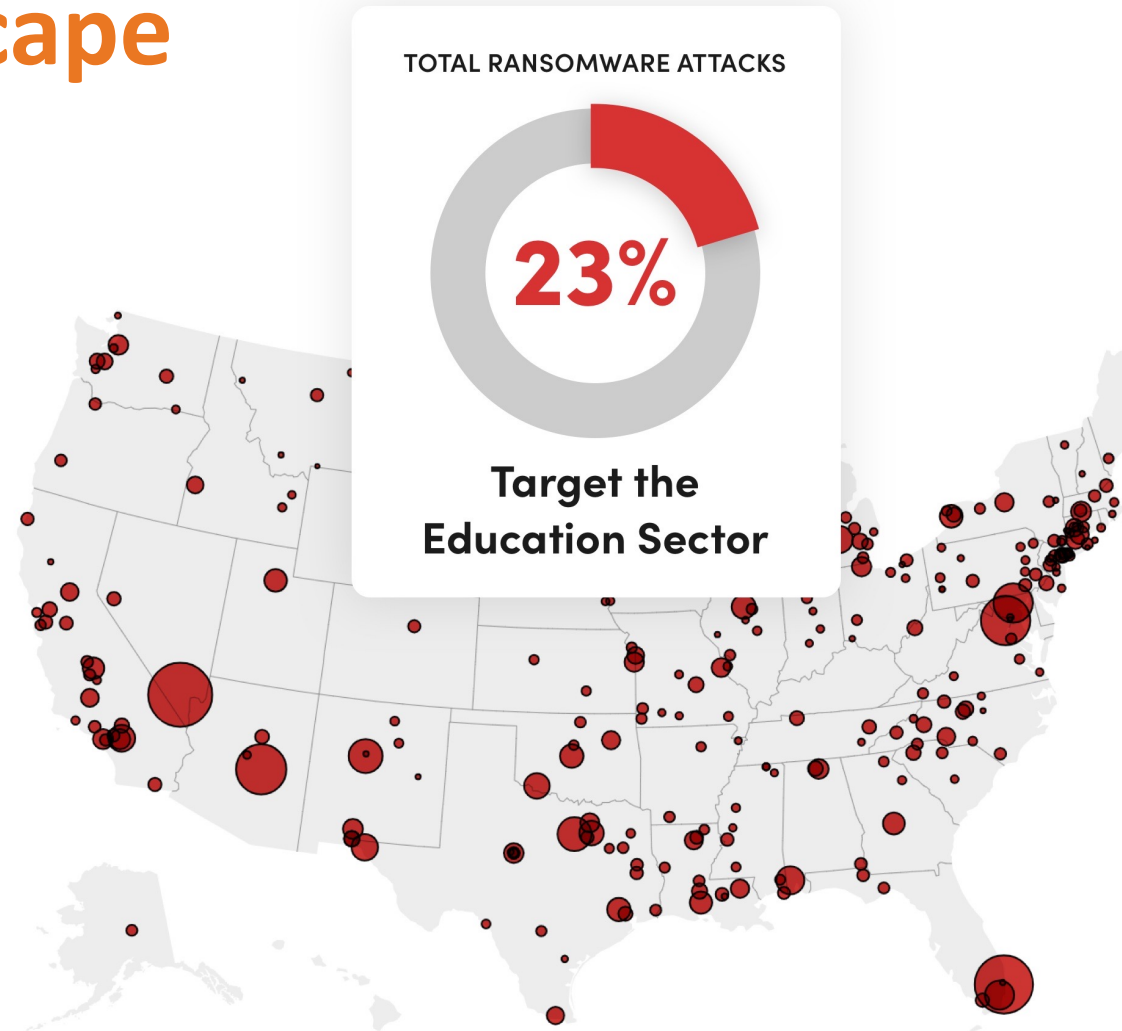
We provide Proactive / Preventative end-to-end services to reduce risk and vulnerability, while increasing operational continuity for over **500** municipalities and school districts in NJ.

Cybersecurity does not occur in a vacuum, success in protecting your infrastructure at all levels is inextricably linked to both technology and the human factor.



Cybersecurity Threat Landscape

- Cybersecurity is still lacking within the Public Sector – over 1500 individual distinct local government agencies in NJ.
 - Local Municipalities
 - K-12 Schools
 - County Government
 - Utilities and Authorities
 - Public Safety
- There are only “Best Practices”
- Insurance has been paying most of the bills – they main industry driving the requirements
- The average cost of a data breach is projected to reach 4.2M in 2023
- Public sector saw a 95 increase in Cyber attacks in 2022 compared to the same period the pervious year.



*Verizon’s Data Breach Investigations Report, Kaspersky 2021, IBM Cyber Report 2022

<https://securityintelligence.com/news/cyberattacks-rise-sharply-against-governments-schools/>

Brett Callow, a ransomware analyst at the cybersecurity company Emsisoft.

Allan Liska, Senior Security Architect, Recorded Future (September 6, 2022)

Why are hackers targeting the Public Sector?

- Lack of budget and attention applied to cybersecurity has created a “soft” target for hackers.
- Vast quantities of valuable Personal Identifier Information (PII)
- Citizen / Employee Data - Social security numbers, Credit cards, Health information etc.
- Financial Information - Banking Info, Mortgage, Tax, information, etc.
- Public Safety Information - Dash Cam Footage, Police Records, personal info, etc.
- Last year, NJCCIC received 375 confirmed cyber incident reports. That fails to capture the full scope.



Who is driving the changes in Cybersecurity

- **Only Guidelines to Follow**
 - NJCCIC - DHS
 - CIS / MS-ISAC
 - NASCIO
 - CISA
- **Insurance Carriers**
 - Driving standards
 - Providing Offsetting financial risk
- **Either your JIF or your Insurance carrier if you have insurance directly**
 - Financial Protection
 - Risk Transfer
 - Compliance Requirements



Nassau County Cyber Incident

- Nassau County – Sept 8th, 2022
- This compromised the license numbers of 470,000 and 26,000 social security numbers belonging to county employees and retirees.
- Brought their 911 infrastructure back to Pen and paper. It took them two weeks to fully restore.
- The Clerk and Comptroller was asking for improved security, tabled 3 times and voted down once.
- What did the town do? They offered free Credit Monitoring....
- Citizens are responsible for their own Cyber controls and their towns.

CYBER ATTACK



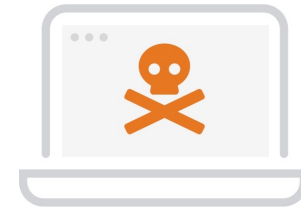
Today's 3 biggest cybersecurity threats



Social Engineering Attacks



Data Breaches



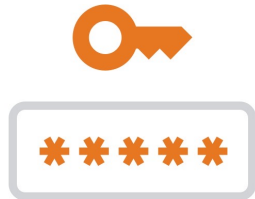
Ransomware Attacks



“It would be hard to think of any threats bigger than cyber threats. You can bolster, reinforce, train and bring in technology, but it only takes that one lapse.”

Chris Rein
New Jersey's Chief Technology Officer (CTO)

Insurance is leading the way to setting controls and practices in place



Password Management

- ✓ Complexity Requirements
- ✓ Period Expiration



Basic Security Tools

- ✓ Anti Virus
- ✓ SPAM Filtering
- ✓ FireWall



Basic Patching

- ✓ Critical Patches within a month



Incident Response Plans

- ✓ Basic Plan

What is now required for a quote

Employee Training

Off Network Back Ups

- ✓ All Data
- ✓ 3-2-1 Rule
- ✓ Weekly
- ✓ Tested Quarterly

Multi Factor Authentication

- ✓ Remote Access
- ✓ Access to off network back ups
- ✓ Privileged Users

End Point Detection and Response

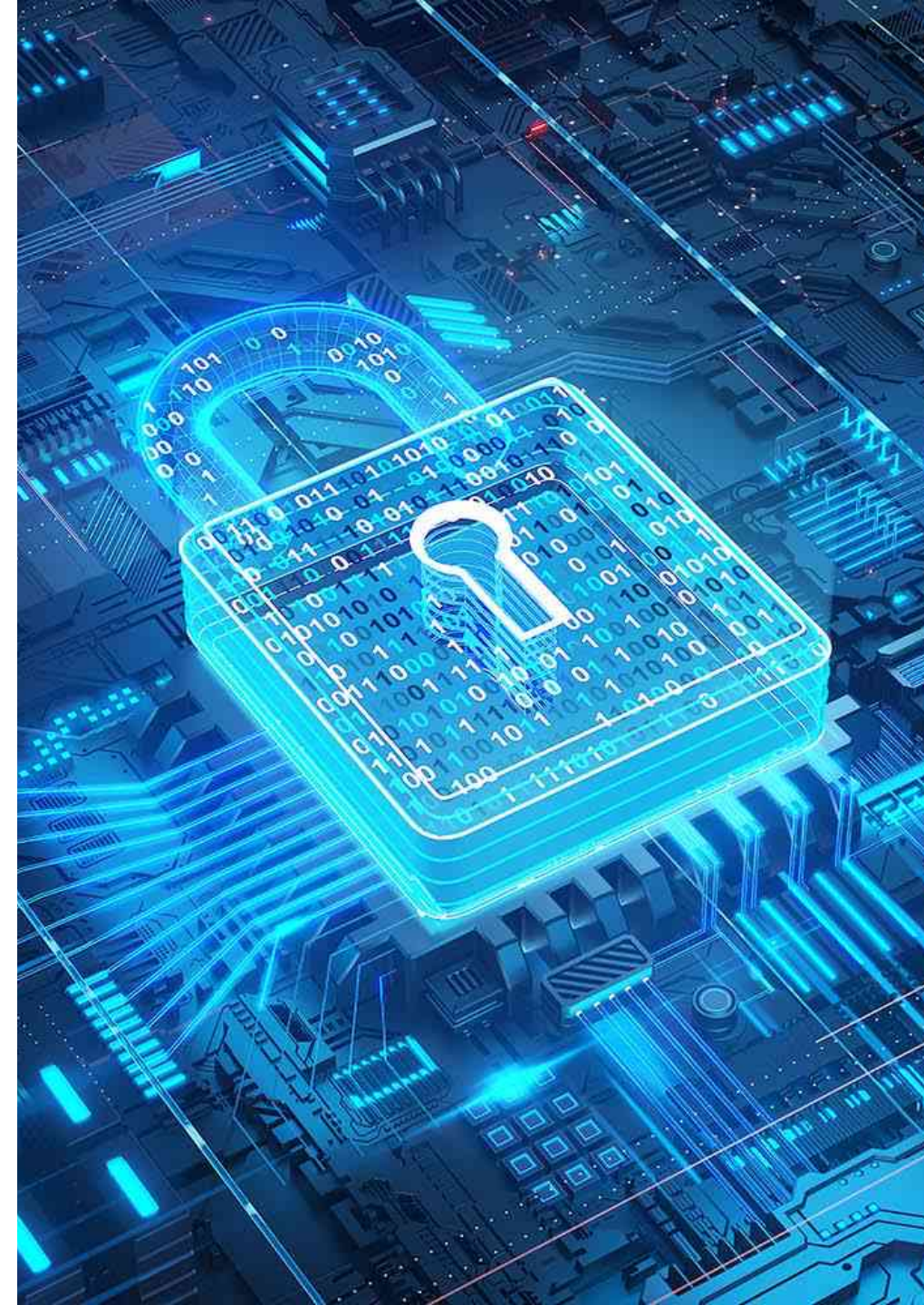
- ✓ Network Monitoring and Support



What requirements are coming next

What is already becoming the new normal

- ✓ Multiple Off-Network Back-Ups
- ✓ Incident Response Plan Testing
- ✓ Access Privileges Controllers
- ✓ Third Party Security Audits
- ✓ Data Encryption
- ✓ Operation Technology
- ✓ Asset Privilege Controls
- ✓ Denial of service (DoS) detection



Why cybersecurity is a Leadership Imperative

It's more than just an IT concern; it underscores business requirements

- Leadership needs to start the conversation:
 - Focus on awareness of the threat
 - Create a desire for change by emphasizing organizational benefits and potential impacts of a successful attack
 - Increase knowledge that supports a Call-To-Action
- Build relationships within your organization outside of your department – are critical to a successful cyber program
- Removing barriers
- Develop and execute a risk-based cyber program

Key individuals, and how their roles can prevent a Cyber incident



Mayor / Public Entity Leader / Superintendent

- Establish a need and culture for Cybersecurity from the top down
- Improve the communication and cooperation between departments to make an effective culture change



Business Administrator

- Share mandatory cybersecurity controls from Insurance Policies and understand the ramifications of these controls on business functionality. Generally, the lead for their individual Joint Insurance Fund.
- Needed to understand how to procure cost effective technology and security products and services for all departments
- Drive funding towards Cybersecurity controls

Key individuals, and how their roles can prevent a Cyber incident



IT Director / Managed Service Provider (MSP)

- Advocate and understand the Cybersecurity Controls and Measure
- Implement the technologies and safeguards
- Communicate security controls effectively, do not talk technical
- Join and share ideas with thought leadership groups such as NJGMIS, NJCCIC, etc.



Council Members / Legislative

- Drive discussion on Cybersecurity and know what their town is doing? Ask the question!
- Shift and manage budget that may have already been earmarked
- Potentially need to raise taxes to address security gaps
- Change and write new policy to address Cybersecurity

How to allocate and find funds for Cybersecurity improvements

Resources and Strategies that you can use

- Develop a roadmap to figure out quantify the risks you want to avoid
- Find out what Insurance provisions you currently have and ask your insurance company what the new requirements are.
- Talk to your surrounding towns and piers and see what they have done
- Get similar minded folks within your Public Entity to champion the effort with you – don't worry you are not alone.
- Talk to your Joint Insurance Fund (JIF)

Utilize Free Resources

- NJCCIC
- CISA

How to allocate and find funds for Cybersecurity improvements

Cost savings within a Public Entity

- Finding Buying and Saving Technology for Schools and Government Agencies which will identify and seek removal of bureaucratic obstacles to acquiring technology.
- Unfunded mandates and guidelines
- Improving services / contracts
- Improving technology could be cheaper than maintaining old technology

Purchasing these programs

- Grants - DHS and FEMA provided final approval of the NJ SLCGP Strategic Plan and 4 first-year projects that were submitted by the NJ SLCGP Planning Committee
- State COOPs for easier and fast purchase with preapproved prices that do not have to go out to bid.
- D2 is apart of Cyber JIF, NJ Purchasing Cooperative

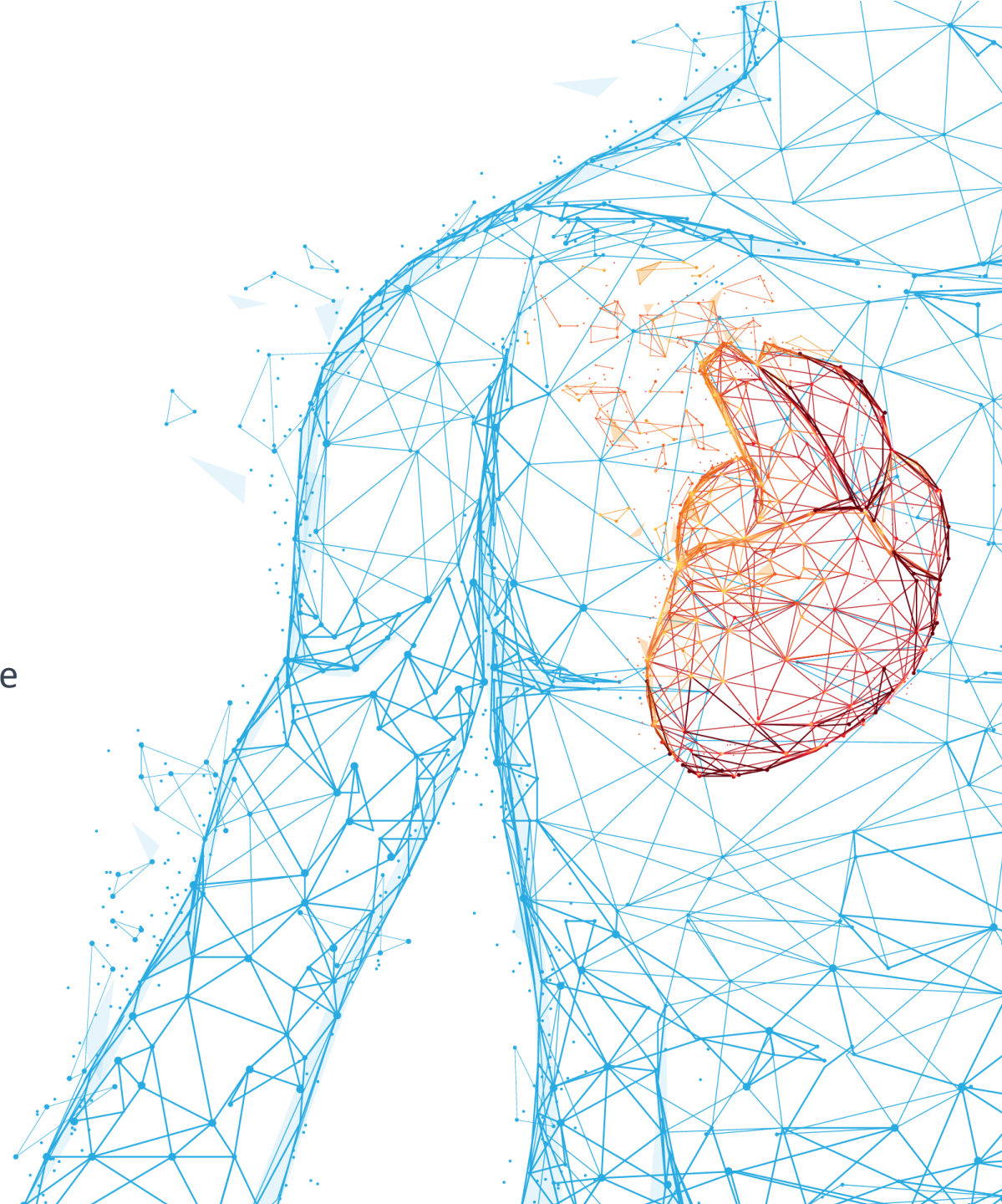
Contract Vehicles and Purchasing



Think of cybersecurity like you do YOUR health

**“An ounce of prevention is worth a pound of cure”
– Ben Franklin**




- It is very costly to start addressing Cyber issues after years of bad habits and technology implementations
- There is no “one” pill / software you can buy to eliminate the program.
- You have annual health screenings; why not conduct an annual assessment of your cybersecurity program and attack surface?
- It is never too late to have the conversation.
DO SOMETHING NOW!



If you are interested? Come talk to us.

Conferences D2 will be at

- NJSBA Workshop 2023
- NJ League of Municipalities 2023
 - NJGMIS TEC 2024
 - TECHSPO 2024
 - NJAC 2024

Name	Email
Brian Lau Director	 brianlau@d2cybersecurity.com  (609) 915-2758
Michael Esolda Public Sector Cybersecurity Advisor	 mesolda@d2cybersecurity.com  (732) 713-3030

THANK YOU FOR YOUR TIME

Questions & Answers



D2 | CYBERSECURITY

Thank You

Brian Lau
DIRECTOR

Michael Esolda
PUBLIC SECTOR
CYBERSECURITY ADVISOR

28 WORLDS FAIR DRIVE
SOMERSET NJ 08873
732.507.7346
D2CYBERSECURITY.COM