Keep Your Cyber Plate Clean: Best Practices to Pass your next Audit

HELLO!

Bernadette Kucharczuk, CGCIO
City of Jersey City, IT Director
20+ years of experience, appointed in November 2017

Jean-Guy Lauture, CGCIO
Township of Bloomfield, IT Director
20+ years of experience (8 years in Public Sector), appointed in Dec 2011

Lee Micai, CGCIO
Mercer County Board of Social Services, Department Head, MIS
20+ years of experience, appointed in February 2016

Jim E. Pacanowski II, CGCIO
Ventnor City, IT Network Admin
20+ years of experience

01 LAWS/LEGISLATION

02 COMPLIANCE

03 HYGIENE

04 TRAINING

05 RESOURCES

06 BEST PRACTICES

“Passwords are like underwear: don’t let people see it, change it very often, and you shouldn’t share it with strangers.

847,376 complaints from the American public
7% increase from 2020
$6.9 billion potential losses

19,954 business e-mail addresses compromised
$2.4 billion adjusted losses

2,690 reported ransomware attacks in 2021
1,389 reported ransomware attacks in 2020
92.7% rise in ransomware attacks

649 reported ransomware attacks to critical infrastructure between June and December 2021

22 reported ransomware attacks to US state or local government in 2022

01 | LAWS/LEGISLATION

02 | COMPLIANCE

03 | HYGIENE

04 | TRAINING

05 | RESOURCES

06 | BEST PRACTICES

LAWS/LEGISLATION

- **H.R.3684 – Infrastructure Investment and Jobs Act**
  - https://www.congress.gov/bill/117th-congress/house-bill/3684/text

01 LAWS/LEGISLATION

02 COMPLIANCE

03 HYGIENE

04 TRAINING

05 RESOURCES

06 BEST PRACTICES

COMPLIANCE

What needs to be done to comply;

- Check with your JIF to determine their level of compliance
  - Is it an all or nothing?
  - Or is it a Tiered compliance program?
- Does your compliance affect your Cyber Deductible?
  - Is it reduced for each level of compliance?
- Are you required to add or amend Cyber Policies?
  - Master Technology Policy
  - Technology Practice Policy
  - Cyber Response Plan

MINIMUM LEVEL OF COMPLIANCE – TIER 1

Minimum Back-Up Practices

1. Use of standardized system images or virtualized desktops.
2. Back-up copy of all application software must be available.
3. Daily incremental back-ups with a minimum of 14 days of versioning on off-network device of all data files.
4. Weekly, off-network, full back-up of all data files.
5. All back-ups are spot-checked monthly.
6. Third-party application data must also be backed-up to the same standards.

Patching Practices

1. The municipality patches all operating an application software with the latest versions.
2. The municipality uses automatic updating where applicable, particularly as related to security patches.
3. All security and critical updates and patches are installed as soon as prudent and practicable following release.
4. The municipality annually reviews all non-standard applications for possible replacement/upgrade.

Defensive Software

1. The municipality's antivirus and firewalls are enabled for all desktops and laptops.
2. The municipality's antispam and antivirus filters are enabled for the email server.
3. The municipality's firewalls are enabled on all active ports, and unused ports are closed.
4. Firewall rules and policies are reviewed or reassessed at least twice per year.
5. Microsoft Office applications open all downloaded files in "Protected Mode".

Security Awareness Training

1. All computer users receive annual training of at least one hour on at least the following topics:
   a. Password Construction
   b. Identifying security incidents
   c. Social Engineering attacks
   d. Business email compromise

Backups – Backups – Backups

- The key to all things Cyber
- Off site backs a must
  - Cloud options or second site
- Need to test restores too!!
- Are 3rd party or Cloud platforms Backed up
  - Have you checked their compliance

Patching

- Is all your Hardware up to Date??
- WSUS Server or Manual – both work
- Hardware Replacement schedule

Defense is the Best Offense! ☺

- Firewalls/Routers - Cisco/Palo
  - Alto/Fortinet/Sonicwall/More
- Antivirus - Sophos/Bit
  - Defender/Symantec/McAfee
- Email
  - Spam Filters

Training

- Formalized at least once/year – we are on #2
- Does your JIF do it or a comply – Knowb4,etc.

MINIMUM LEVEL OF COMPLIANCE – TIER 1

Password Strength

1. The municipality has a password policy that minimally meets the requirements outlined in the Password Policy under the MEL's Master Technology Policy Ver 2.2.

Email Warning

1. The municipality has implemented an automatic warning label to all emails coming from outside of your organization.

Cybersecurity Incident Response Plan

1. Management/Governing Body adopts a cybersecurity incident response plan to direct staff and guide technology management decision making when a cybersecurity incident takes place. This must include at a minimum the items in the MEL's Cybersecurity Incident Response Plan.

Technology Practices Policy

1. Management/Governing Body adopts a technology practices policy, which must at a minimum include the items in the MEL's Master Technology Policy Ver 2.2 respective to Tier 1.

Government Cyber Memberships

1. The municipality is registered with the New Jersey Cybersecurity & Communications Integration cell (NJCCIC).
2. The municipality is registered with the Multi-State Information Sharing & Analysis Center (MS-ISAC) and any other ISAC relevant to your organization's operations.

Password – Strong and Complex?

- Pass phrases/ long passwords / Complexity
- How often do you change? Not often enough?
- Part of Policy – Part of Group Policy

Email Disclaimer

- Do you have a warning or disclaimer on your email to warn users of emails coming from outside your organization

Response Plans

- What are you going to do when one happens
- Adopted policies

Policies

- Are there any policies that are mandated
- Do you have a master policies that covers all areas of Cyber

Cyber Memberships

- These are all free to government
- Offer many free and paid programs – MDBR
- NJ-GMIS – a great avenue to help

NEXT LEVEL OF COMPLIANCE – TIER 2

Server Security

1. The municipality's servers and network equipment are protected from unauthorized access.

Access Privilege Controls

1. Users with administrative rights are limited to those who need them.
2. Non-administrator users are granted limited access rights based on job function and responsibilities.
3. Access rights are updated upon any personnel status change action.
4. Access rights for each individual are reviewed at least every six (6) months.

Technology Support

1. The municipality has qualified staff or contractor(s) to provide technology support and guidance.

System / Event Logging

1. The municipality has appropriate system and event logging in place to detect and/or capture system/network performance and security anomalies.

Protected Information

1. The municipality has a process that ensures all files containing Personally Identifiable Information (PII) or Protected Health Information (PHI) are password protected or encrypted.

Remote Access

1. The municipality requires the use of a Virtual Private Network (VPN) when remotely accessing the municipal network or cloud-base applications. This also includes adopting a Remote Access Policy. (refer to Remote Access Policy – VPN in the Master Technology Policy Ver 2.2).

Access Controls – Physical & Virtual

- Are your server rooms and wiring closed secure
- Are use access and rights limited
- Do users have local Admin Rights – Do they need it?
- Verify periodically & Remove when not needed

Contractors

- What is their response time
- Do they have remote access – How do you monitor

Logging

- There are so many devices that log things
  - Firewalls, Servers, Routers
- Need to periodically review – Who Does it?
  - Kiwi Syslog/Splunk/Netrix/Solarwinds

Protected information

- PII & PHI Info
  - Is it secured/Protected/Encrypted
  - If in Cloud, verified vendor compliance?

Remote Access

- Do you allow remote access
- Is your VPN secure

NEXT LEVEL OF COMPLIANCE – TIER 2

Leadership Expertise

1. The municipality's senior management has access to resources with expertise in their respective fields to support technology decision making, i.e., risk assessments, planning, budgeting, etc.

IT Business Continuity

1. The municipality's Emergency Management/Continuity of Government (CoG) plan shall Include an IT Business Continuity Plan as part of their Disaster Recovery section.

Banking Controls

1. The municipality has implemented internal controls to minimize fraudulent banking transactions.

Technology Practice Policy

1. The Management/Governing Body has adopted the MEL's Information Technology Policy as respects to Tier 2.

Leadership/Administration

- Are they on Board/ Are they knowledgeable
- This is the key to it all!!!
- IT needs a seat at the table

Continuity

- Does IT work with your OEM to ensure part of your Disaster recovery plan
- IT has its hands in almost every part

Banking

- Do you do online banking/Wire Transfers
- Is it secure?
- Who has access?
- Separate PC with controls in place

Policies

- Does your JIF require a Tech Policy?
- Is it part of your Master Policy?

HIGH LEVEL COMPLIANCE – TIER 3

Network Segmentation

1. The municipal network is segmented, separating critical units (finance, police, utility, etc.) to minimize the spread of a cyber-attack.

Remote Access

1. The municipality has implemented the use of Multi Factor Authentication (MFA) when remotely accessing municipal resources and/or accessing third-party applications that pass or store protected and or financial information.

Remote Access Policy

1. The municipality has adapted a Remote Access Policy that includes Multi-Factor Authentication and minimally includes the items in the Remote Access Policy – MFA in the MEL's Master Technology Policy Ver 2.2.

Password Integrity

1. The municipality has implemented a process where employees can periodically validate their credentials against **HaveIBeenPwned** or a similar email breach service.

System and Event Logging

1. Logs are reviewed every three (3) months by the IT professional.

3rd Party Risk Management

1. The municipality has access to the MEL's 3rd Party Risk Assessment Tool to assess a vendor's risk when issuing new or renewing contracts.

Network Segmentation

- Are your remote location on separate Subnets/Networks
- Still able to communicate with each other
- Depending on size/location not within building

Remote Access

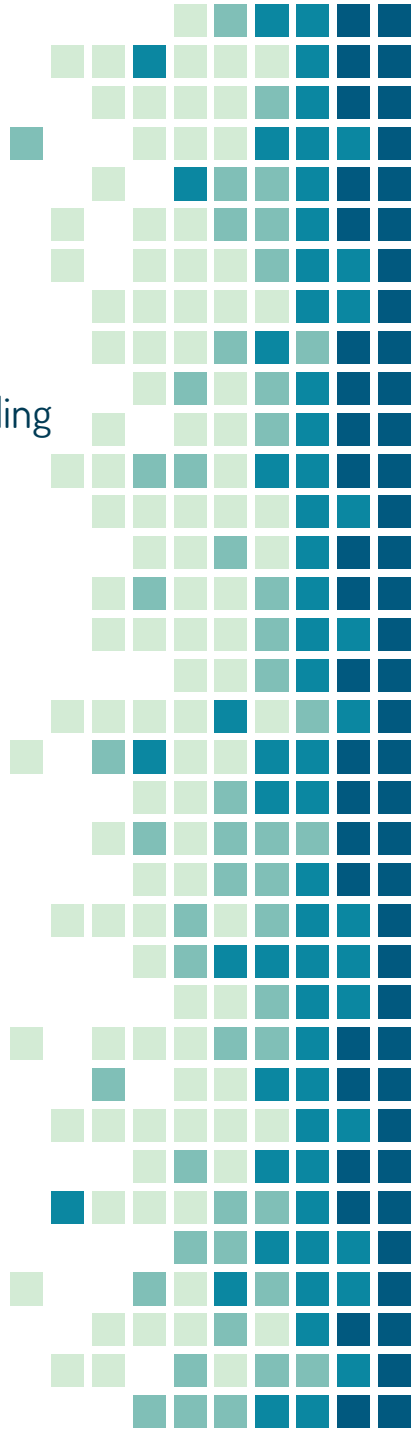
- Multi-Factor Authentication a must today!!
- VPN/remote Access control
- Email needs MFA as well
  - 0365 has built in but not robust
- Various 3rd party Authenticators
  - DUO/Google/Microsoft

Integrity – Has your email been compromised

- Users need to verify if their email has been compromised – you will be surprised!!!

3rd Party vendors

- How confident are you with your vendors
- What kind of background checking is done
- Need to look at their cyber compliance
- They hold and control your data



SCORE CARD

Physical Security

Item	Yes	No
Do you have policies and procedures to address authorized and limited access to facilities, including data centers		
Are visitors escorted in and out of controlled areas		
Are PC screens automatically locked after an idle period		
Do you have policies covering laptop, tablet, or mobile device security		
Do you have a current emergency evacuation plan		
Do you have an accurate up to date inventory of all electronic equipment		
Do you have an accurate up to date asset tag inventory of all essential equipment		
Are your data closets and/or server rooms equipped with intrusion alarms		
Are unused network access ports physically disabled		
Is your data center/server room locked at all times		
Do you have environmental controls dedicated to your data closets and server rooms		
Do you have fire suppressions systems dedicated to your data closets and server rooms		
Are default security setting changed on software and hardware before they are placed in operation		
Are policies and procedures in place to control equipment plugged into the network		
Is your physical facility monitored and reviewed via camera systems		
Totals		

Personnel

Item	Yes	No
Does your staff wear ID Badges		
Do you check credentials of external contractors		
Do you have policies to address background checks of contractors		
Do you have policies addressing background checks of employees		
Do you have a policy for unauthorized use of “open” computers		
Do you have a policy and procedure in place to handle the removal of employees who retire, are terminated, or leave including passwords and access to systems		
Do you have an acceptable use policy that governs email and Internet access		
Do you have a policy governing Social Media use and access by employees		
Are employees required to sign an agreement verifying they have read and understood all policies and procedures		
Are these policies and procedures reviewed with employees at least annually		
Totals		

Account and Password Management

Item	Yes	No
Do you have policies and procedures covering authentication, authorization, and access control of personnel and resources to systems		
Are policies in place to ensure only authorized users have access to PC’s		
Are policies and procedures in place to enforce secure, appropriate, and complex passwords		
Are information systems such as servers, routers, and switches protected with basic or better authentication mechanisms		
Has the default “Administrator” account been disabled and/or deactivated		
Are all access attempts logged and reviewed		
Are employees required to change their passwords on a routine schedule		
Are employees prevented from using previous passwords		
Are all passwords on network devices encrypted		
Do you have legal and/or policy notifications on all log-in screens that is seen and accepted prior to access to any network device		
Totals		

Data Security

Item	Yes	No
Do you have policy for information retention		
Do you have policies and procedures for management of personal private information		
Do you have a policy for disposing of old and outdated equipment		
Do you have policies and procedures in place for the secure destruction or sanitation of media and/or drives before they are removed, sold or disposed of		
Is access to data or systems accessed remotely both from a dedicated link and encrypted		
Do you have policies and procedures in place to ensure that documents are converted into formats that cannot be easily modified before they are circulated outside the network		
Are documents digitally signed when they are converted to formats that cannot be easily modified		
Is access to critical applications restricted to only those who need access		
Are UPS batteries used on all critical equipment		
Totals		

SCORE CARD

Network Security		
Item	***Yes***	***No***
Is Network traffic regularly monitored for patterns		
Do critical systems have redundant communication connections		
Does your network utilize redundant DNS servers in case of interruption to one server		
Is your DNS servers reviewed on a periodic basis for anomalies and consistency		
Is your Active Directory reviewed periodically for anomalies and consistency		
Are all unnecessary services disabled on servers		
Does your network utilize redundant domain controllers in case of interruption to one server		
Are there policies and procedures governing the use of wireless connections to your network		
Are wired and wireless networks within your organization segregated either physically or virtually through routers, switches, or firewalls		
Do you employ firewalls on your network to control access and traffic		
Are firewalls configured to only allow traffic from approved lists		
Are Network Security Logs reviewed regularly		
Are web filters used to restrict uploading of confidential information		
Are web filters used to restrict downloading of unapproved material		
Are content filters used to restrict web activity		
Are filters or firewalls used to filter executable or malicious email attachments		
Are policies and procedures in place for software patches and updates		
Are policies and procedures in place for hardware patches and updates		
Are your security polices reviewed on a yearly basis		
Are current and up to date Antivirus solutions loaded on all computers		
Are Antivirus and other security software updated with current patches on a regular basis		
Do you use Spyware and Malware Software		
Are all computers current with all security and operating system patches and updates		
Do you employee “Least Privilege” access and review access privilege periodically		
Do you have an accurate and up to date software inventory list		
Totals		

Disaster Recovery/Network Maintenance		
Item	***Yes***	***No***
Do you have a current Continuity of Operations Plan (COOP)		
Do you have a current Continuity of Government Plan (COG)		
Do you have a current Disaster Recovery Plan		
Do you have an Emergency Management Communications Plan		
Do you have an Emergency Plan to cover Internal & External Communications		
Do you have an Emergency Response Plan		
Are all your Emergency Plans stored in a remote location		
Are your Emergency plans tested at minimum annually		
Do you have a current detailed network topology		
Do you have a current floor plan with all data equipment labeled		
Have all cables and equipment been physically labeling in wiring closets		
Totals		

Awareness and Education		
Item	***Yes***	***No***
Do you provide training on a regular basis		
Do you provide training on computer security		
Do you provide training on data breaches		
Do you provide training on password security		
Do you provide training on email and social media security		
Are employees restricted from saving sensitive data on CD’s, DVD’s, Flash Drives, or other removable media unless it is required		
Do you have policies and procedures in place to prevent downloading and execution of executable files without being scanned and reviewed by IT		
Are all employees trained on the procedures for notification in case of a breach or attack		
Do you provide training on Social Engineering including phone and email solicitation		
Do you provide training on the use of data processing programs including security implications of document file types		
Totals		

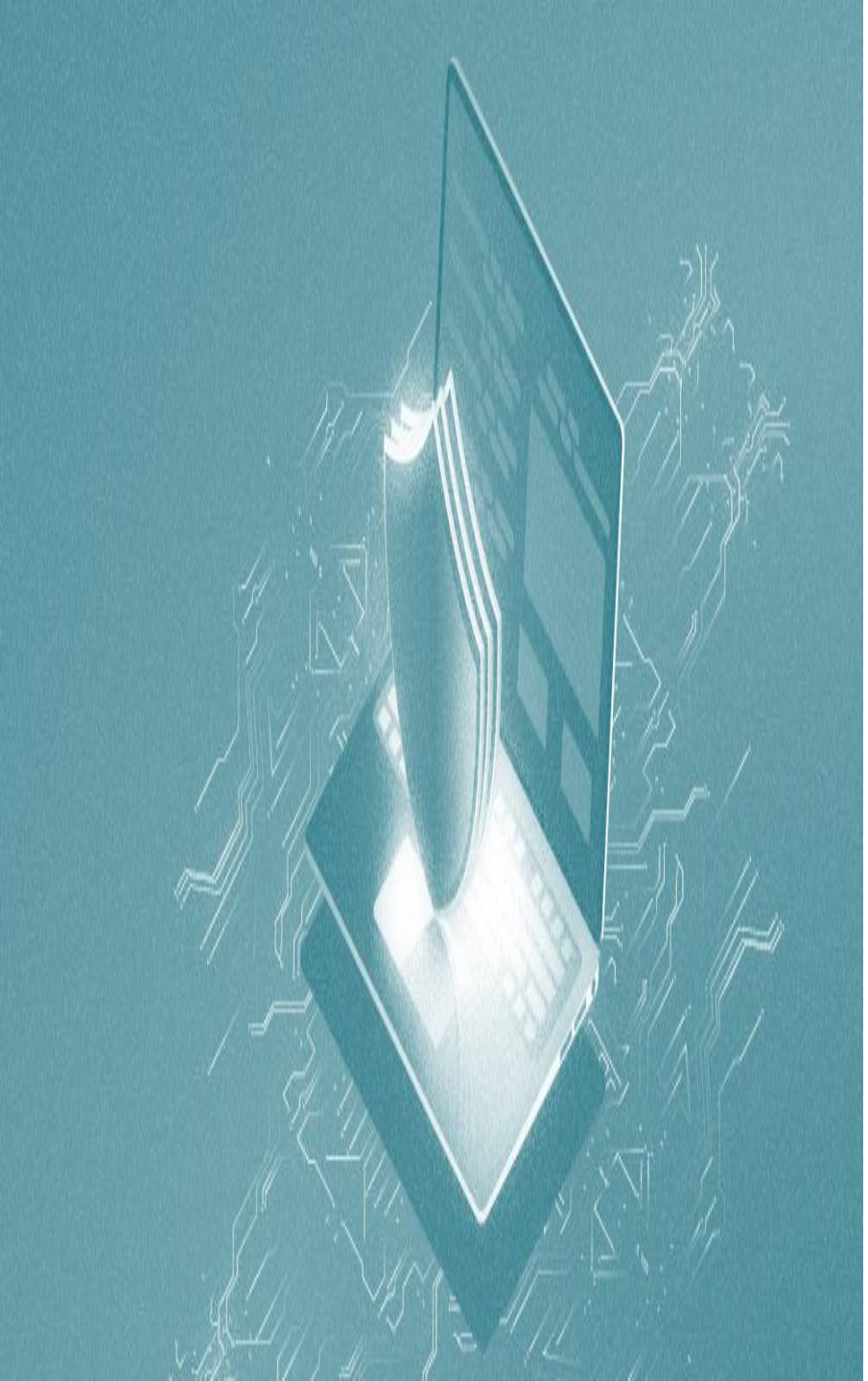
SCORE CARD

Backups		
Item	***Yes***	***No***
Are backups completed on a daily basis		
Do you have policies and procedures in place that govern backups		
Are operating systems, programs, and operating information backed up as well as data		
Are configurations of switches and routers backed up		
Are backups tested regularly – at least monthly		
Are backups transferred to a remote device or location that is kept offsite		
Do you have a process for creating backup copies of critical data		
Are backup solutions updated to the current firmware or software patches		
Are backup logs reviewed regularly for compliance and successful completion		
Do you have a policy in place governing who have access to backups		
Totals		

Scoring of the Cyber Security Checklist

Category	***Yes***	***Possible***
Physical Security		15
Personnel		10
Account and Password Management		10
Data Security		9
Network Security		25
Disaster Recovery/Network Maintenance		11
Awareness and Education		10
Backups		10
Grand Total		**100**

Score	Risk Level	Comments
0-50	High Risk	Network, policies, and procedures need immediate attention
51-70	Medium Risk	Network, policies, and procedures need addressing to improve compliance
71-80	Moderate Risk	A number of areas are where they need to be but others need addressing
81-90	Low Risk	Most of you procedures are in place, but a little tweaking needs to be done
91-100	Secure Network	Your network and its policies and procedures are in place. You need to address some fine details



WHERE DO YOU RATE?

- There are lots of similar type of checklists available
- The Key is to see how your compliance holds
- MS-ISAC has a yearly review – No Cost – Just join up
  - NCSR
  - National Cyber Security Review
- See how you rate with others
- Where your compliance falls


01
LAWS/LEGISLATION
02
COMPLIANCE
03
HYGIENE
04
TRAINING
05
RESOURCES
06
BEST PRACTICES

WHAT IS CYBERSECURITY HYGIENE?

- Achieving the best possible security readiness can be complex and overwhelming, with so many recommendations and the ever shifting threat landscape.
- Beginning with a simple understanding of cybersecurity standards can help.
- I am offering a basic starting point for organizing and managing a security program using established processes, policies and practices to set and prioritize cyber hygiene tasks.

BASICS OF CYBERSECURITY HYGIENE

Backups

- Regularly back up important files to a separate, secure location that would remain safe and isolated if the primary network were compromised. **ALWAYS TEST YOUR BACKUPS**

Education

- Having a continuous program that engages and educate on the latest trends about cybersecurity and social engineering **(IMPLEMENT A SOCIAL-ENGINEERING AND CYBERSECURITY TRAINING PROGRAM)**

Encryption

- When you can encrypt, you should encrypt **(THIS IS A RULE AND NOT AN EXCEPTION)**

Firewalls

- Make sure firewalls and routers are properly set up and configured to keep bad actors out of private systems. **DON'T TRUST, YOU MUST VERIFY**

BASICS OF CYBERSECURITY HYGIENE

Password Hygiene

- Consider rules that includes enforcing minimal requirements, such as length, complexity and time of password changes. MFA is now the new norm and minimal requirement

Email Security and Filtering

- Is an array of technologies, techniques and practices to keep cybercriminals from gaining unauthorized access to email accounts and message content. And like all cyber hygiene measures, email security is the joint responsibility of organizations and individuals. **(Can be frustrating to End Users, But communicate the importance of filtering emails.)**

BASICS OF CYBERSECURITY HYGIENE

Endpoint Security

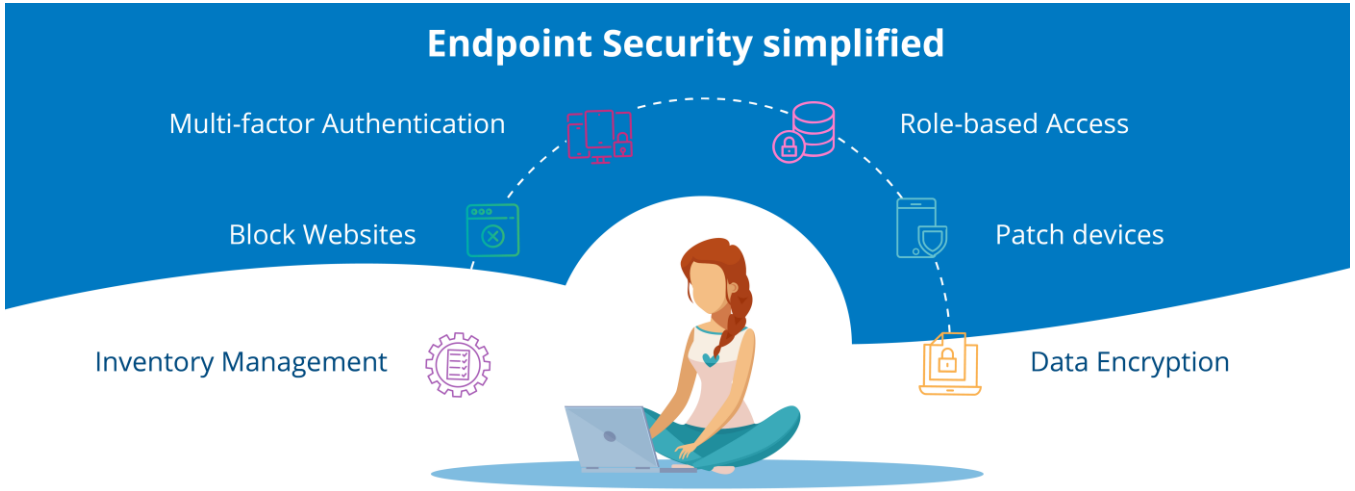
- Whatever touches your network, should have a managed / monitored endpoint protection.

Network Segmentation

- Where possible, segment your network. This is also a great network management strategy.

Secure Remote Access

- Organizations are now embracing remote work. Securing this workforce is critical.



BASICS OF CYBERSECURITY HYGIENE

Website and Online Discretion

- Be careful not to post any information a bad actor could use to guess or reset a password, or otherwise gain access to user accounts. Follow best practice rule for website posting. Be aware of what personal information is already available online, which cybercriminals could use in social engineering attacks

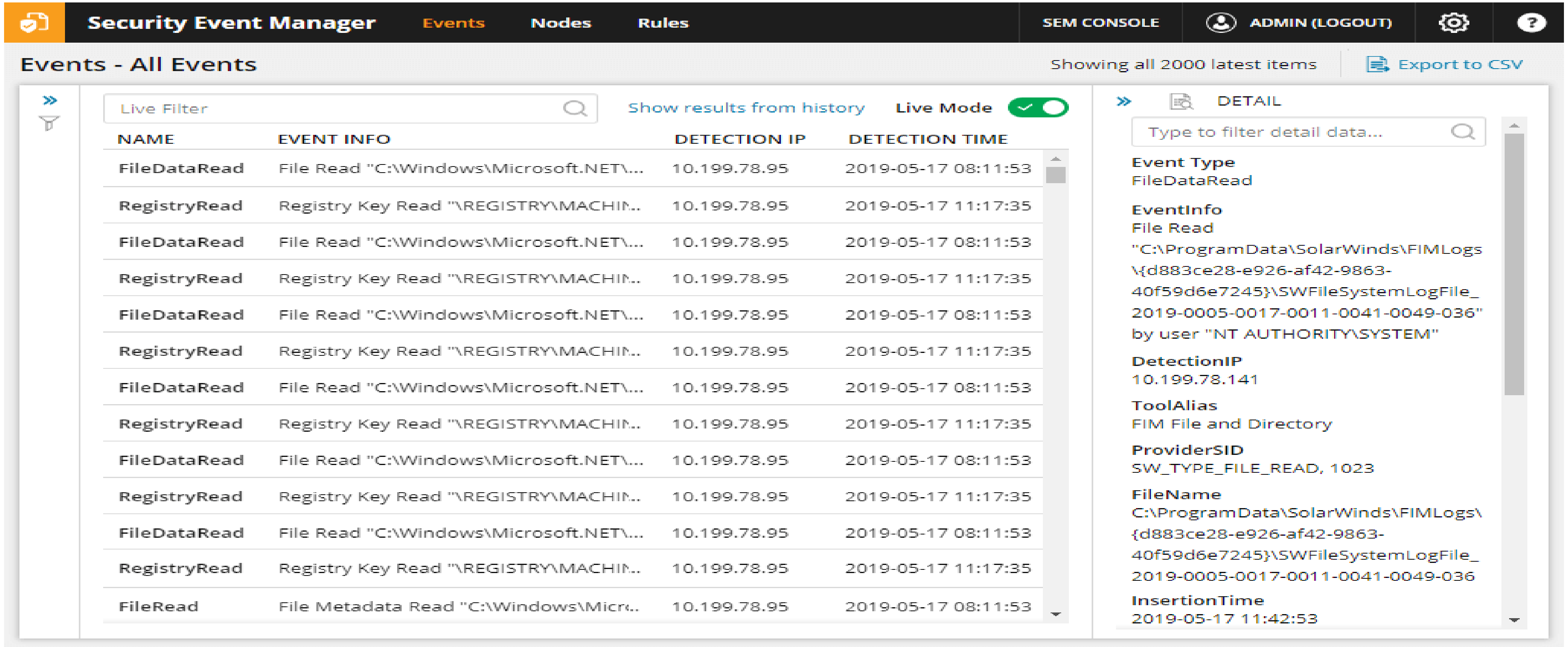
Patch Management

- Install any available software updates and security patches on both company-owned devices and any personal devices used for work. Try to implement a WSUS Windows Server Update Services. Make sure that you monitor, research and push out critical updates.

BASICS OF CYBERSECURITY HYGIENE

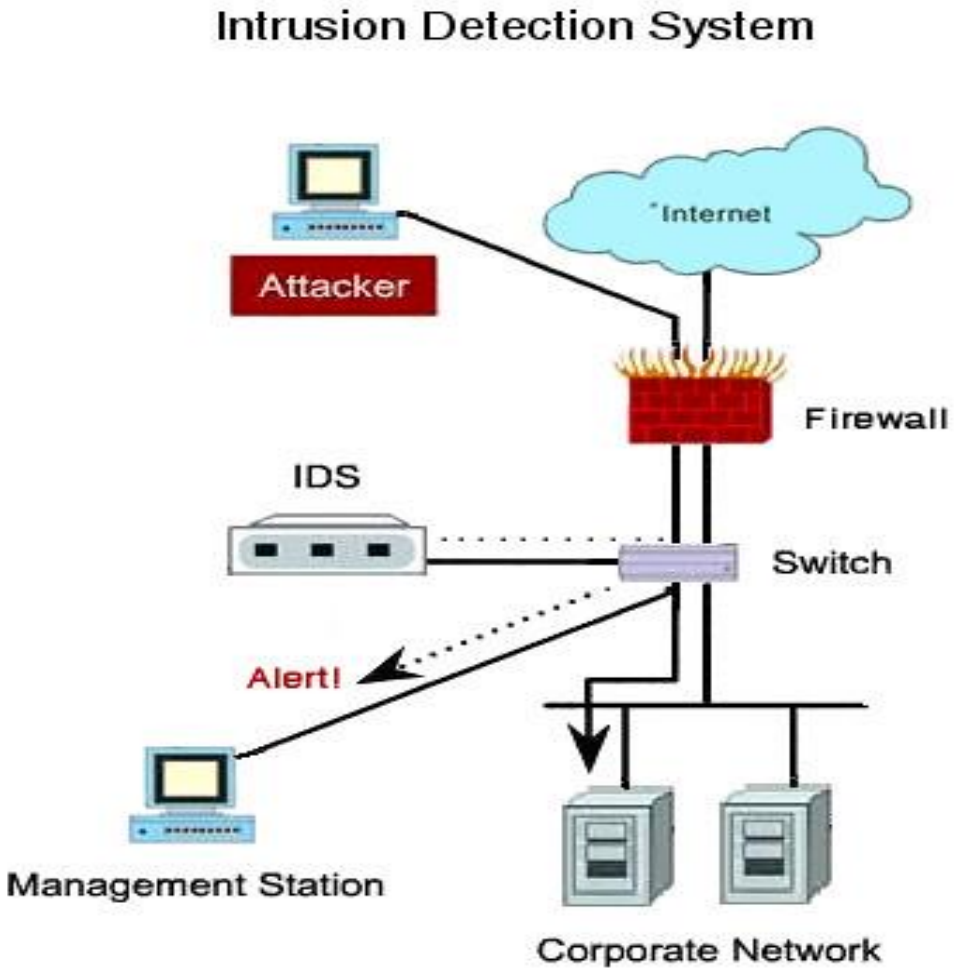
Security Log Management

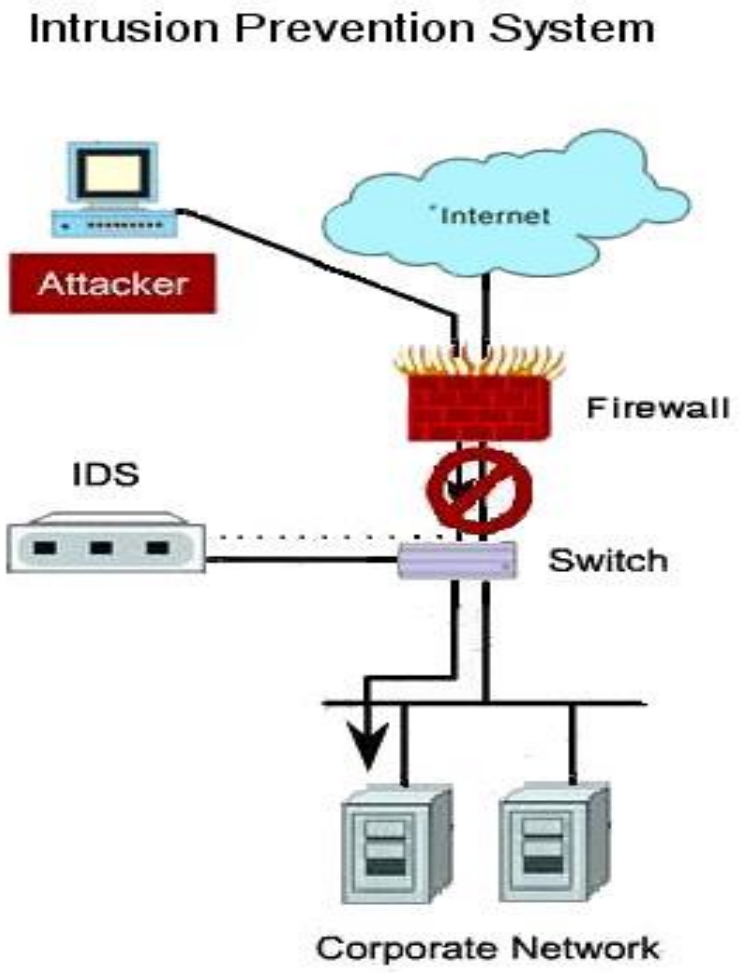
- A cybersecurity program is only as good as its ability to recognize inappropriate or suspicious activity in the IT environment. Best practices for security log management include logging and storing the right events, ensuring the accuracy and integrity of logs, analyzing log data to identify problems and using logging tools to manage event volume.



INTRUSION DETECTION AND PREVENTION SYSTEMS

Why do you need both IDS and IPS?





INCIDENT RESPONSE (IR) and STRATEGY

The basics tenets of a Incident Response and Strategy framework

- When not if an organization suffers a security event, it needs a ready incident response (IR) and management strategy to mitigate risk to the business. The breach can include financial losses, operational disruptions, regulatory fines, reputational damage and legal fees, an IR team needs a combination of executive, technical, operational, legal and public relations expertise.

01 | LAWS/LEGISLATION

02 | COMPLIANCE

03 | HYGIENE

04 | TRAINING

05 | RESOURCES

06 | BEST PRACTICES

WHAT IS SECURITY AWARENESS TRAINING?

- Security awareness training programs are designed to help users and employees understand the role they play in helping to combat information security breaches.
- Research suggests that human error is involved in more than 90% of security breaches.
- Security awareness training helps to minimize risk thus preventing the loss of PII, IP, money or brand reputation.
- An effective awareness training program addresses the cybersecurity mistakes employees may make when using email, and the web.

TRAINING STRATEGY

1. First, Don't Blame Your Employees
2. Invest in Employee training
3. Make Cybersecurity awareness a Priority
4. Get Buy-in From the Administration
5. Password Security Training and Best Practices
6. Training Employees to Recognize Phishing and Social Engineering Attacks and Trends
7. Make Cyber Security a Part of Your Onboarding Process
8. Perform Simulated Cyber Attacks and Phishing
9. Make sure your Cybersecurity Employee Policy is Followed
10. Train and Train often (Once a Month) is recommended

TRAINING TOPICS

- Phishing awareness
- Social Engineering
- Use of Social Media
- Password Creation and Management
- Privacy issues
- Compliance (HIPAA, PCI, etc.)
- Acceptable Use of Information Technology and Services
- Identity Theft
- Information Classification and Handling
- Virus/Hoaxes/Spyware/Spam/ Malicious Software
- Teleworking/Working Remotely
- Mobile Device Security
- Personal Device Use in the Workplace
- Incident Identification and Reporting
- Contingency Plan

METHODS FOR DELIVERING TRAINING

- Information Security open house events
- Web-based or Instructor led presentations
- Periodic company newsletter announcements
- Posters and signs strategically placed around the organization
- Notices posed during logon
- Quarterly Information Security newsletters
- Email notifications
- Department meetings
- Corrective training following an information security incident
- Security messages within system banners
- Brown-bag presentations
- Awards program
- Video presentations

01 LAWS/LEGISLATION

02 COMPLIANCE

03 HYGIENE

04 TRAINING

05 RESOURCES

06 BEST PRACTICES

FREE RESOURCES

No-cost cybersecurity resources;

- New Jersey Cybersecurity & Communications Integration Cell (NJCCIC)
- Multi-State Information Sharing & Analysis Center (MS-ISAC)
- Cybersecurity & Infrastructure Security Agency (CISA)
- NJ-GMIS

NEW JERSEY CYBERSECURITY & COMMUNICATIONS INTEGRATION CELL (NJCCIC)

- Bulletins, Alerts, Advisories
- Threat Briefings
- Risk Assessment & Management Services
- Attack Surface Management
- Security Scorecard
- Incident Reporting
- Limited Incident Response
- Statewide Threat Grid
- Training - Instructor-led, Self-paced, Cyber Range

Membership:

- https://www.cyber.nj.gov/members/

To report an incident or request assistance:

- https://www.cyber.nj.gov/cyber-incident/
- NJCCIC@cyber.nj.gov

NJCCIC

MULTI-STATE INFORMATION SHARING & ANALYSIS CENTER (MS-ISAC)

- Network Monitoring Services
- Research & Analysis
- Cyber Alerts & Advisories
- Threat Intelligence
- Web Defacements
- Account Compromises
- Hacktivist Notifications
- Domain And IP Monitoring
- Malicious Domain Blocking And Reporting
- CIS Configuration Benchmarks

Membership:

- https://learn.cisecurity.org/ms-isac-registration

To report an incident or request assistance:

- Phone: 1-866-787-4722
- Email: soc@cisecurity.org

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (CISA)

- Risk and Vulnerability Scans
- Web Application Scans
- Remote Penetration Testing
- Phishing Campaign Assessments
- Incident Response Tabletop Exercises
- Cyber Resilience Review

Advanced Malware Analysis Center:

- https://malware.us-cert.gov

To report an incident or request assistance:

- Phone: 1-888-282-0870
- Email: CISAServiceDesk@cisa.dhs.gov
- Website: https://www.us-cert.gov/forms/report

NJ-GMIS - LEADERS in GOVERNMENT TECHNOLOGY

- NJ-GMIS is an association of public sector technology leaders.
- Annual conference providing educational sessions, networking opportunities, discussions of trends and emerging technologies.
- Virtual Round-table Series for Public Sector Technology Professionals.
- GMIS International hosts a similar 3-day annual conference which brings together public sector IT professionals throughout the world.
- Award scholarships for members enrolled in the CGCIO "Certified Government Chief Information Officer" certificate program.

Membership:

- Visit https://www.gmis.org.
- Click 'Membership'
- Choose 'Agency Membership'
- Annual fees start at $100 and are based on your agency's annual technology budget.

GMIS NEW JERSEY
An Association Of Government IT Leaders

01 LAWS/LEGISLATION

02 COMPLIANCE

03 HYGIENE

04 TRAINING

05 RESOURCES

06 BEST PRACTICES

BAD PRACTICES

- Use of unsupported (or end-of-life) software
- Use of known/fixed/default passwords and credentials
- Not employing multi-factor authentication for all devices, systems, and services
- Clicking links that come through unsolicited, suspicious emails
- Downloading attachments without first verifying the sender
- Using weak or easy-to-guess passwords
- Poor physical management/control over devices
- Improper privileges to network resources
- Not encrypting data between networks
- Storing critical files on unencrypted cloud servers.
- Not installing robust networking monitoring and antivirus on all servers and computers.
- Insufficient staff training around social engineering and phishing campaigns.
- Not updating to the latest security patches
- Not keeping solid backups.

BEST PRACTICES

- Patch…patch…patch
- Enabling advanced logging for all systems (including cloud assets)
- Create a watch list for high-value accounts
- Test end user cyber awareness through extra phishing exercises and short videos
- Apply Zero Trust – Removing administrative access for accounts that don't need it
- Enabling MFA and strong passwords on all accounts
- Enabling and testing offsite backups
- Verifying with legal & leadership necessary cyber insurance policy coverage
- Implementing effective network segmentation
- Installing advanced endpoint protection on all hosts

HELP!!

What if you believe you have been hit by a ransomware or other cyber-attack?

Do you know who to reach out to for assistance?

- New Jersey Cybersecurity & Communications Integration Cell (NJCCIC)
- Multi-State Information Sharing & Analysis Center (MS-ISAC)
- Cybersecurity & Infrastructure Security Agency (CISA)
- NJ-GMIS
- Your cyber insurance carrier
- Your local FBI agent
- The National Guard
- State, local, tribal, and territorial (SLTT) governments

BEST PRACTICES RESOURCES

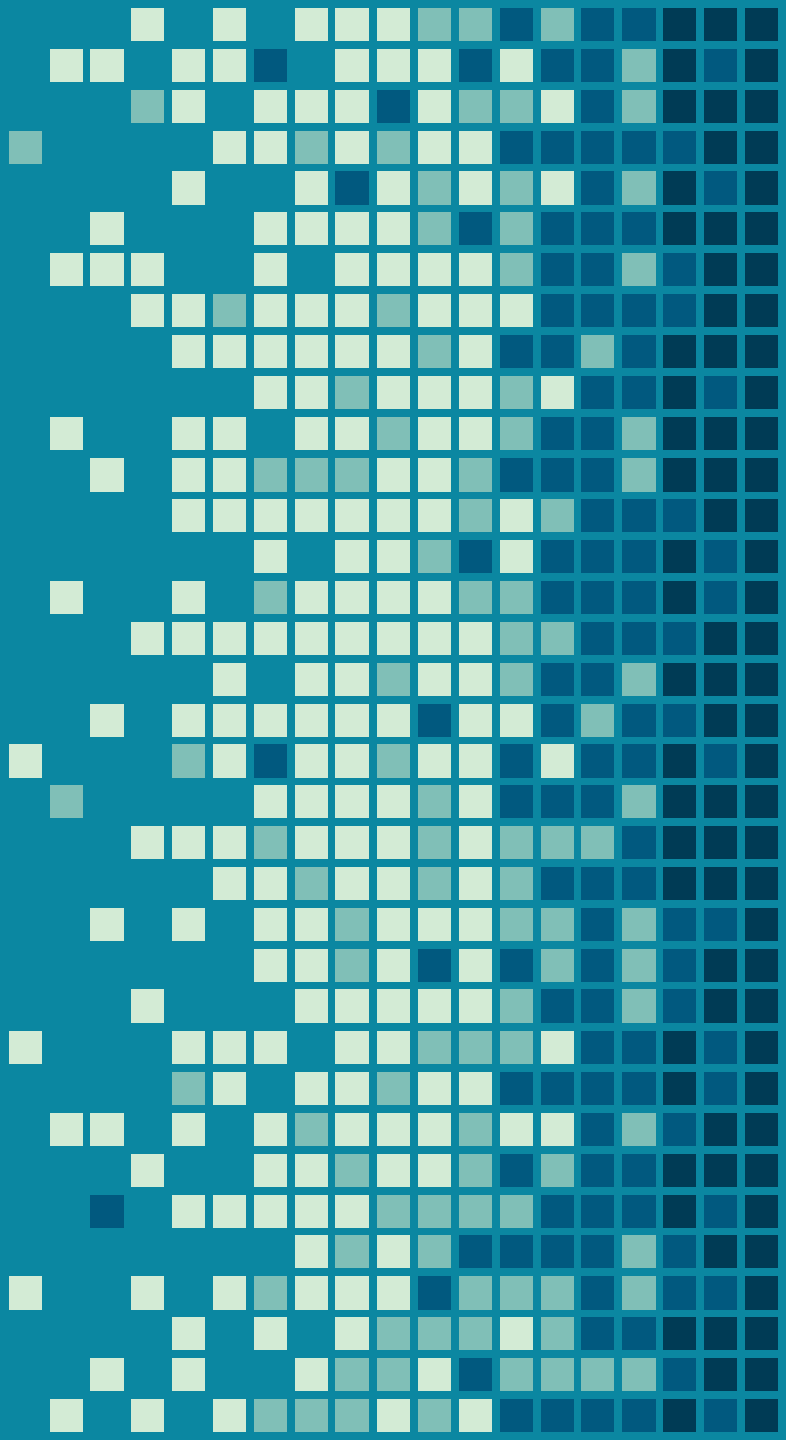
- Cyber Resilience Review (CRR) - https://us-cert.cisa.gov/resources/assessments
- Cyber Security Evaluation Tool (CSET) - https://us-cert.cisa.gov/ics/Assessments
- Cybersecurity Best Practices - https://www.cyber.nj.gov/learn/cybersecurity-best-practices/#the-basics
- Cybersecurity Resources Guide - https://www.cisecurity.org/wp-content/uploads/2020/07/MS-ISAC-Cybersecurity-Resources-Guide-2020-0720.pdf
- External Dependencies Management (EDM) - https://us-cert.cisa.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-EDM.pdf
- Managing Cyber Threats through Effective Governance - https://www.cisecurity.org/insights/white-papers/managing-cyber-threats-through-effective-governance
- Nationwide Cybersecurity Review - https://www.cisecurity.org/ms-isac/services/ncsr/
- Navigating New Challenges This Academic School Year - https://www.cyber.nj.gov/informational-report/navigating-new-challenges-this-academic-school-year
- NIST Cybersecurity Framework Policy Template Guide - https://www.cisecurity.org/wp-content/uploads/2020/07/NIST-CSF-Policy-Template-Guide-2020-0720-1.pdf

BEST PRACTICES RESOURCES

- Phishing Campaign Assessment (PCA) – https://us-cert.cisa.gov/resources/ncats#Phishing%20Campaign%20Assessment%20(PCA)
- Ransomware: Risk Mitigation Strategies – https://www.cyber.nj.gov/mitigation-guides/ransomware-risk-mitigation-strategies
- Risk & Vulnerability Assessment (RVA) – https://us-cert.cisa.gov/resources/ncats#Risk%20and%20Vulnerability%20Assessment%20(RVA)
- Stop Ransomware – https://www.cisa.gov/stopransomware
- STOP. THINK. CONNECT.: https://www.CISA.gov/stopthinkconnect
- Supply Chain Cybersecurity Resources Guide – https://www.cisecurity.org/wp-content/uploads/2020/11/Supply-Chain-Cybersecurity-Resources-Guide.pdf
- Vulnerability Scanning Service (CyHy) – https://us-cert.cisa.gov/resources/ncats#Cyber%20Hygiene
- Workshops – https://us-cert.cisa.gov/resources

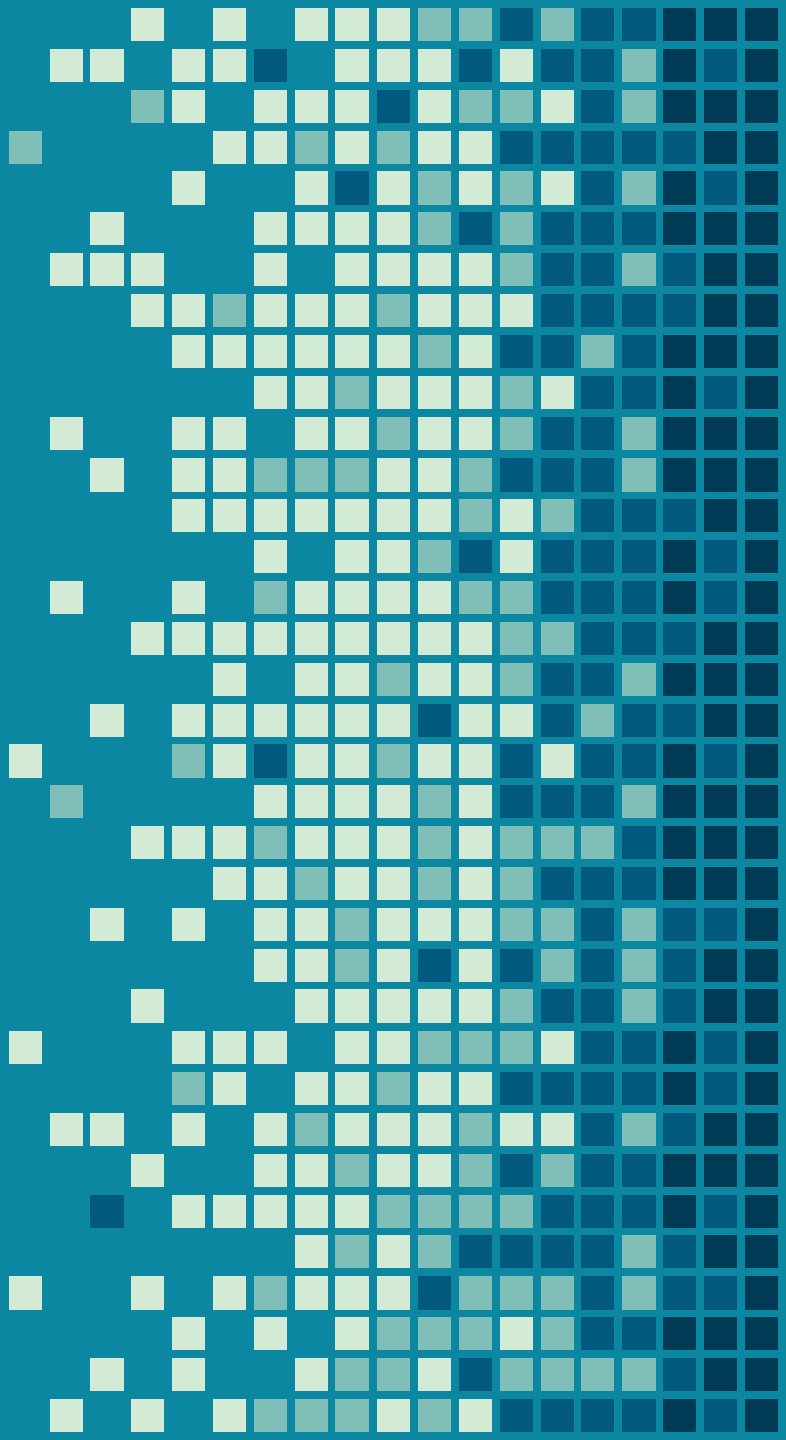
TAKEAWAYS

- **Work with your JIF/Cyber Insurer**
  - Determine what they require
  - What is your level of coverage
  - What is your deductible
- **Policies**
  - What do you need
  - Do you have them in place
- **Training**
  - Your #1 key to keeping your network secure
  - You are one click away from a breach or an attack!!
- **Multi-Factor Authentication**
  - This is a must! Probably the most important item in Cyber right now!!
  - Use an Authenticator tool not just text messages or emails



TAKEAWAYS

- **Backups**
  - Be prepared
  - Don’t just think you are OK
  - Test your backups
- **Updates**
  - All of your equipment needs to be up to date
  - Things change daily



THANKS!

Any questions?

Bernadette Kucharczuk, CGCIO – bkucharczuk@jcnj.org
Jean-Guy Lauture, CGCIO – jlauture@bloomfieldtwpnj.com
Lee Micai, CGCIO – lmicai@mcboss.org
Jim E. Pacanowski II, CGCIO – jpacanowski@ventnorcity.org