VRSA

Virginia Risk Sharing Association

Cybersecurity: Identifying and Responding to Current Threats for Local Governments

Presented by:

Darius Davenport
&
Karen Cole

This presentation is for educational purposes only. It is not legal advice for any particular situation. Laws change all the time. Always verify that information is accurate and up to date before you rely on it.

DISCLAIMER

Cybersecurity Is Not Just an IT Issue…

Headlines

Hit with ransomware attack, Howard University forced to cancel classes

Warren County recovering from March computer infiltration

Virginia Tech Says It Was Targeted in Two Recent Cyberattacks

Smyth County Schools' computers targeted by ransomware

Fairfax County Public Schools hit by Maze ransomware

Ransomware attack leads to shutdown of major U.S. pipeline system

After cyberattack, stolen Chatham County data and sensitive documents posted online

Water Plant Cyberattack Is Wake Up Call, 20 Years in the Making

New Kent County Public Schools victim of ransomware attack

$600,000 payment for turf football field stolen from Spotsylvania

Why does this matter?

- Local governments hold significant amounts of sensitive data
  - Public Safety
  - Legal
  - Health
  - Financial
- Older, more vulnerable computer systems
- Valuable data
- Disruption
- Virginia Public Procurement Act
- Freedom of Information Act

Impact of an Attack

- When any type of cyber event happens, it just does not affect one part of the organization…
  - Leadership – Board/Council concerns, press inquires, management of employee issues and response
  - Finance – Emergency funds, insurance claims, internal controls review, audit issues
  - Legal – Lawsuits, breach reporting, regulatory issues, HB1290, contract issues
  - Employees – Citizen inquiries and backlash, stress on operations, concerns for their positions
  - IT & Cybersecurity – Identification of entry/control exploited, containment, digital forensics and investigation, clean up, and ***new normal***

Cybersecurity Breach – If only I'd known!

Most shared comments after a cyber attack or data breach has occurred.

"I wish I had:

- Really known how long I could go without being able to operate key business functions. I cannot go without email and phone service for 3 days!"
- How much it would cost my locality in lost revenue and how much my insurance policy did not cover.
- All of the people who would have to be involved to get me back up and running."
- How long it would take to get back to "normal" operations."

Now imagine all of this and then having to report a data breach and manage the press and breach notifications.

Top Exploits for Localities

10% increase in average total cost of a breach from 2020-2021 (Government = $1.93 per record to recover. 78.7% increase in 1 year)

Business Email Compromise (BEC) had the highest average of total cost of exploit to victim.

Compromised credentials was the most frequent attack vector followed by phishing.

287 Days – Average number of days to identify and contain a data breach. (212 days to identify. 75 days to contain.)

Top Issues –

- Third-Party Vendor controls ineffective or not compliant
- Lack of internal controls – policies, procedures, and plans
- Lack of monitoring and response capabilities

Source: Cost of a Data Breach Report 2021 by Ponemon Institute

Business Email Compromise

Business Email Compromise (“BEC”)

- BEC is a type of email scam in which a attacker obtains access to a business email account or creates an email account to imitate an employee of an organization for the purpose of defrauding the organization

- BEC attacks are designed to trick employees, customers or vendors into wiring payment for goods or services to alternate bank accounts.

Examples of BEC

- Examples:
  - Posing as an employee seeking a direct deposit change
  - Posing as a contractor/vendor seeking a change in financial wiring instructions
  - Posing as an employee requesting payment of a fake invoice or a doctored invoice

Hypothetical Scenario

Hypothetical 1: BEC

- Your town has been upgrading computer systems. Monday, the Town gets an invoice from the Town's IT vendor, Jonathan, at Jonathan@jonathanIT.com requesting payment for $50,000 for additional computer components.

Questions & Answers

- **Are there any issues with the request for payment?**
- Are you expecting the invoice?
- Do you have a system to receive notice of payments that need to be made?
- Do you recognize the sender?
- Is the senders email address correct?
- Learn a zero trust concept with email communications
  - Zero Trust: An operating model that assumes that user identities on the network may already be compromised. Therefore, security solutions rely on artificial intelligence and analytics to continually monitor and validate access and activities. (Not as scary as it sounds!)

Hypothetical 1: BEC

- Johnathan, sends another email to the Town indicating that he would like to update the company ACH information with the Town. The Finance Technician directs Johnathan to the ACH form on the Town's website and request a voided check to complete the process.

Questions & Answers

- **Are there any red flags with the IT vendor?**
  - Johnathan@johnathIT.com is not the same as Jonathan@JonathanIT.com
- **Is there an issue with a Finance Form being publicly available?**
  - Yes
  - Finance staff emails should be kept internal
- **Is it better if the Finance Technician email forms on request?**
  - No

Hypothetical 1: BEC

- Johnathan, returns the ACH form and the voided check. The payment is now to be sent to Greendot Bank. The Finance Technician updates the information in the finance system. The payment is processed during the next check run.
- The next day, Jonathan calls the Town, notifying them that he never received the payment.

Questions & Answers

- **Once the Finance Technician had the updated form and voided check, was there anything else that could have been done before processing the payment ?**
  - Get contact information from the original form to call and verify the changes.
  - Check the grammar in the email and form.
  - Check the forms and the checks for a manipulated appearance.
  - Any request for a financial transfer to Greendot Bank is inherently suspect!

- **Do you still need to pay Jonathan?**
  - Maybe

Questions & Answers

- **What do you do next?**
  - Call the bank immediately!
  - Call your insurance carrier
  - Use your Incident Response Plan

- **Why should you call the bank?**
  - The bank ***might*** (emphasis added) be able to recall the payment.
  - Time is of the essence.
  - You have minutes to hours, not days, to stop the transaction.
  - The longer you wait, the less likely the funds will be returned.

Questions & Answers

- **Why should you call your carrier?**

- Your insurance carrier may have resources (legal, data forensics, call centers, etc.) that can assist in the containment, remediation, recovery and notification process.
- Not notifying your carrier could result in policy exclusions.
- Incident response requires immediate action and the application of external resources.

FBI, Private Industry Notification

“From 2018 through 2020, the FBI observed increases in business email compromise (BEC) actors targeting state, local, tribal, and territorial (SLTT) government entities for financial gain due to vulnerability exploitation and transparency requirements. The COVID-19 pandemic exacerbated these cybersecurity challenges as SLTTs shifted a significant portion of their workforce to remote work.”

Preventing This Attack

Security Awareness Training – General User and Role Specific

Updated Finance procedures (with information security considerations) ensuring for checks and balances.

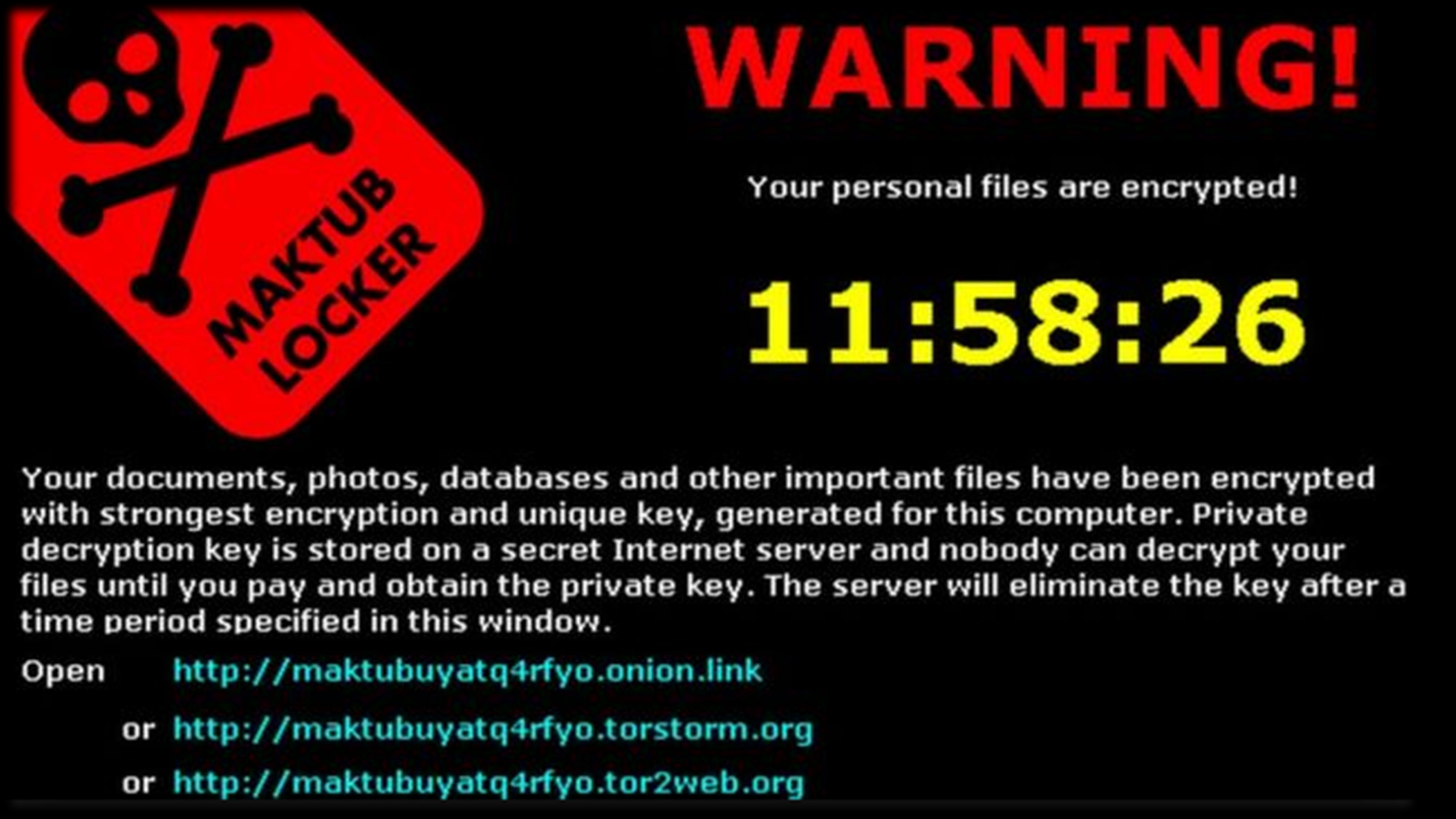
Cybersecurity Incident Response Plan – To detect, respond, and recover from an event. Should align with locality’s continuity management reporting structure and recovery plan.

Self-learning email security platform that detects advanced threats

Ransomware

Ransomware

- Ransomware is a **form of malicious software (“malware”)** designed to block access to a computer system or data, often by encrypting data or programs on information technology systems to extort ransom payments from victims in exchange for decrypting the information and restoring victims' access to their systems or data



WARNING!

Your personal files are encrypted!

11:58:26

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer. Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key. The server will eliminate the key after a time period specified in this window.

Open http://maktubuyatq4rfyo.onion.link

or http://maktubuyatq4rfyo.torstorm.org

or http://maktubuyatq4rfyo.tor2web.org

Hypothetical Scenario

Hypothetical 2: Ransomware

- An employee in your department calls the help desk stating that her computer rebooted and is now displaying a message that says her personal files are now encrypted and that she has 1 day, 23 hours and 20 minutes to pay a ransom of 2 bitcoin in order to obtain the decryption key. Three other staff members also report to your IT director that they can no longer access files in the shared department folder. They are all receiving the same ransomware message.

Questions & Answers

- **Once you hear about this incident from employees?**
  - Activate your Incident Response Team (This should not be the first time they are meeting.)
  - Contact your cybersecurity partner to stop further spread of the attack while maintaining forensic data. (They can also gather information while the IRT is being assembled.)
  - Call your Data Counsel

- **Who makes up the Incident Response Team (IRT) and what is their role?**
  - Your ITR should be made up of your leadership team, IT, HR, Data Counsel and external data forensics professionals. Their job is to stop the incident, investigate, restore data, and make any necessary notifications.
  - Your internal IT staff likely is not equipped to respond to a sophisticated attack alone no matter what they say.

Questions & Answers

- **Do you call your insurance carrier?**
  - Call them immediately!

- **Why should you call your carrier?**
  - Your insurance carrier may have resources (legal, data forensics, call centers, etc.) that can assist in the containment, remediation, recovery and notification process.
  - Not notifying your carrier could result in policy exclusions.
  - Incident response requires immediate action and the application of external resources.

Questions
& Answers

Actions CIOs and Cybersecurity Professionals Perform

- Disconnect system(s) from network
- Take screenshots of ransom note
- Capture BTC addresses, email addresses, file extensions for FBI or other law enforcement entities
- Conduct memory capture before shutting down
- Forensic imaging of hard drives (no wiping) which are then kept in a secure location.
- Power down infected servers
- Utilize vetted cybersecurity professionals to assist in response.
- Cooperate with outside counsel and engage law enforcement as needed/instructed

Hypothetical 2: Ransomware

- You receive a call on your cell phone from the Director of Public Safety who notifies you that ransomware notices are appearing on the city’s public safety computer systems. Computer systems in the police, and fire departments are now displaying the ransomware message informing users that their files are being encrypted. You attempt to call the Chief of Police at his desk, but the phone call does not go through.

Questions & Answers

- **Do you pay the ransom?**
- The FBI will never advocate for paying ransoms
- This is an organizational decision
- You may have to reevaluate this decision based on the severity of the attack
- There are potential serious implications for paying a ransom
- Paying the ransom does not guarantee (1) you will be able to decrypt or (2) that you will not be extorted again

Hypothetical 2: Ransomware

- As computer and communication systems across the city begin to slow and fail, employees begin to call and email each other speculating that the city may be experiencing a data breach. A handful of employees begin to report that they received an email from the hacker stating that they have taken files from the City’s servers and that the hackers will dump those files into a dark web marketplace if the ransom is not paid.

Questions & Answers

- **Do you communicate with the hacker?**
  - Wait as long as possible to communicate with the hacker
  - Data security firm/professional negotiator (crypto-wallet)

- **Do you contact law enforcement?**
  - Yes – you are a victim
  - Law enforcement and data forensics firms are great resources because they have a wealth of knowledge regarding malware variants and hacker modes of operation

Questions & Answers

- **Is it time to give in and pay the ransom?**
  - FBI will not advocate paying a ransom
  - Make the hacker provide a sample of data to prove they actually have acquired data

- **Are there other law enforcement resources?**
  - Virginia Fusion Center
  - Virginia National Guard

Preventing This Attack

Get XDR: Extended Detection and Response (XDR) ensures that end user systems are equipped with configuration control, threat blocking, threat detection, URL/content control, and continuous monitoring.

Self-learning email security platform that detects advanced threats. (Can be partnered with XDR.)

Implement an information security program that adheres to a recognized industry standard. This includes policies, procedures, risk assessments, and plans (such are Incident Response).

Know your insurance company’s process for handling incidents and include actions in your Incident Response Plan.

Have your own vetted and knowledgeable Digital Forensics & Incident Response resource to work on your behalf when needed.

Office of Foreign Asset Control

U.S. Department of Treasury, OFAC

- Sanctions range from cautionary letters to civil penalties up to $311,562
- In determining sanctions, OFAC looks to factors such as:
  - Willful or reckless violation of law
  - Harm to OFAC’s sanction program objectives
  - Circumstances and characteristics of violator
  - Adequacy of violator’s OFAC compliance program
  - Remedial response

U.S. Department of Treasury, OFAC

- Recommendations
  - Get a Data Security Attorney if you experience a ransomware attack
  - Contact OFAC if a Banned Person or Entity is involved
  - Engage law enforcement
- OFAC considers full and timely cooperation with law enforcement as a significant mitigating factor when evaluating sanctions

Cyber Risk Insurance

Cyber Risk Insurance

- Cyber risk insurance is a broad term that encompasses a variety of insurance products which mitigate the financial and other risks that emanate from the use of electronic data and its transmission

- There is no one size fits all policy

How Cyber Insurance Can Help

- Easing the financial burden of a loss
- Mitigation of the data incident:
  - Forensic investigative activities
  - Crisis management
  - Business disruption
  - Notification to affected individuals and regulatory bodies
  - Regulatory fines
- Access to knowledgeable cyber risk claims professionals who can coach you through the incident response process and ensure compliance with state and federal laws

Insurance Considerations

$ They have a responsibility to keep the fund solvent.

Insurance is not a substitute for an information security program and supporting technology.

Results of forensic investigations can be used to deny claims. Partner with legal counsel to reduce your risk.

Accuracy in completing underwriting questionnaires important! If you do not know or it is not clear, then you need to ask. Ambiguity can result in denied claims.

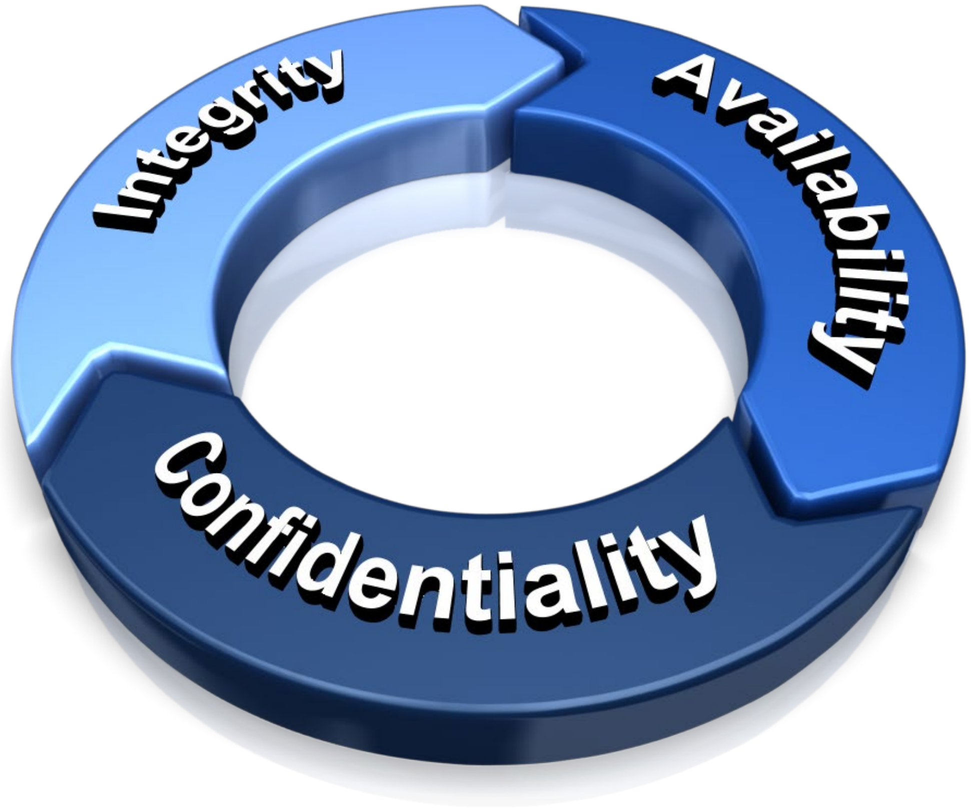
Building Protection Into Your Organization

What do you need to be secure?

- **Confidentiality:** To protect data against unintentional, unlawful, or unauthorized access, disclosure, or theft. Ex. Unauthorized copying or removing data from an environment.
- **Integrity:** To protect the accuracy and the validity of data. Ex. Unauthorized adding of extra zeros to a paycheck.
- **Availability:** Maintaining the availability of data in alignment to the needs of the organization. Ex. Denial-of-Service attack,

There are some attacks that affect more than one area. Ex. Ransomware

All parts of the circle must be present for information security and cybersecurity to be achieved.



Anatomy of an Average Locality

Has a small IT staff (1 – 5 people) or they use an IT services company.

Enforces password management, but not necessarily access management (reviewing and removing access in a timely manner).

Perform patch management (software updates for security).

Has anti-virus software but uses outdated detection technology so viruses still get through.

Has a server(s) – file, email, and/or domain servers and Active Directory.

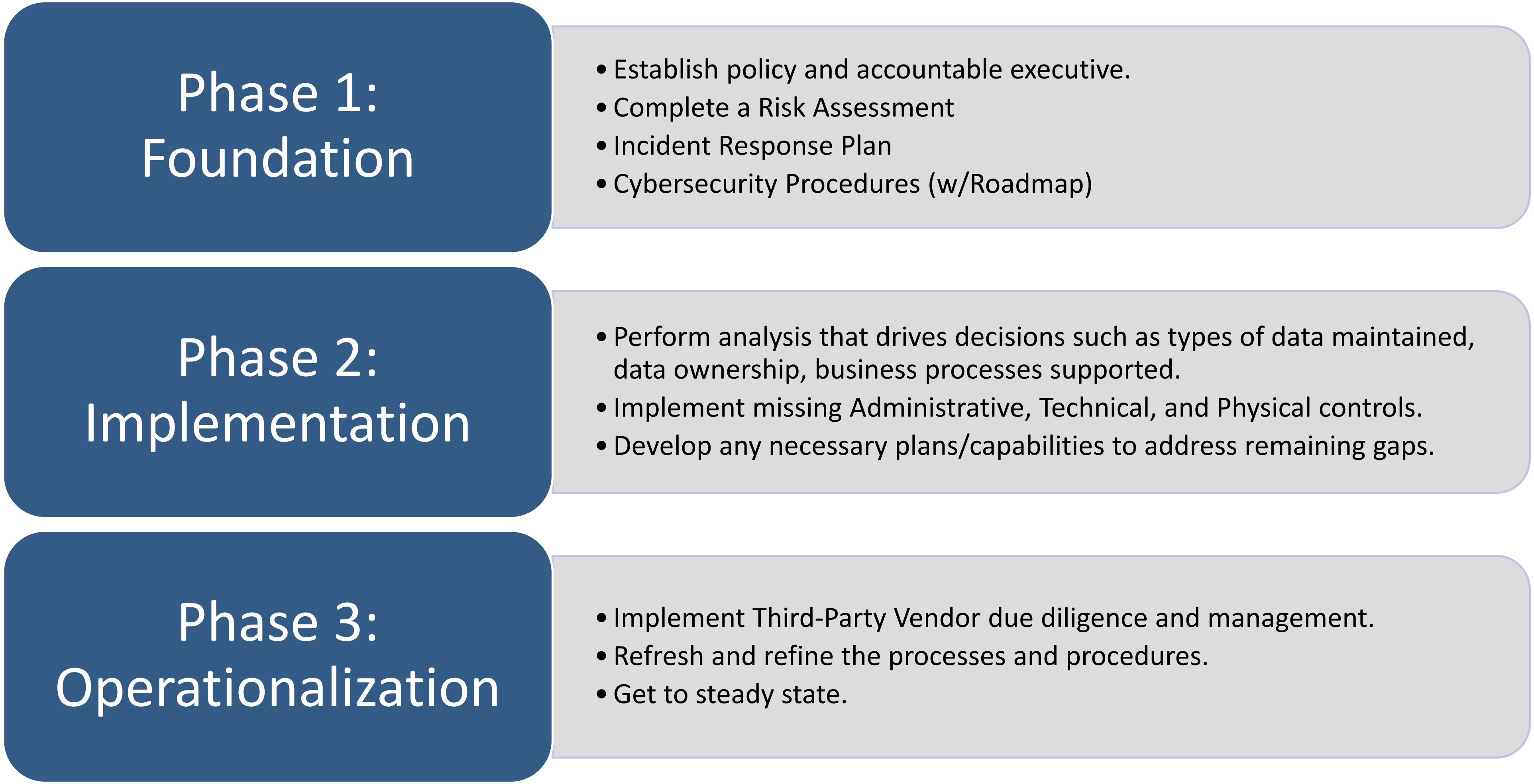
Stores business documents on a file server, on computers and laptops that have citizen or other business sensitive information.

Has identified that they may have cybersecurity vulnerabilities, but no one assigned to ensure that they are investigated and remediated.

Limited policies and procedures – not always written down. No incident response plans or specific cyber training. *No formal Information Security Program*.

Does not have cyber threat or data loss prevention technologies in place.

Common Steps withing a Three Phase Building Process for Cybersecurity Program



Phase 1: Foundation

- Establish policy and accountable executive.
- Complete a Risk Assessment
- Incident Response Plan
- Cybersecurity Procedures (w/Roadmap)

Phase 2: Implementation

- Perform analysis that drives decisions such as types of data maintained, data ownership, business processes supported.
- Implement missing Administrative, Technical, and Physical controls.
- Develop any necessary plans/capabilities to address remaining gaps.

Phase 3: Operationalization

- Implement Third-Party Vendor due diligence and management.
- Refresh and refine the processes and procedures.
- Get to steady state.

Things To Keep In Mind About GRC and Program Management

- **One vs. Many:** It is possible (and recommended) to have one Information Security Program that meets multiple regulatory standards.
- **Must Be Customized:** The program is a reflection of your organization and decisions you have made. You cannot fast track program development by "find and replace" from a template.
- **Right-sized:** It can be right-sized to fit your organization and integrated with your operations to reduce impact on employees.
- **Cost Sensitive:** It does not have to be expensive and time consuming, just effective and compliant.
- **Executive Support & Ownership Outside of IT:** Wherever possible, information security should be "owned" by an executive outside of IT. However, they are a very active participant. For small organizations, there are hybrid approaches that work well (ex. different owners for information security management vs. operations)
- **Effort Decreases Over Time:** It takes more effort to implement a program that it does to maintain it.
- **Third-Party Vendors:** This program will cover data sharing with third-party vendors and ensure that they are protecting your data as required.

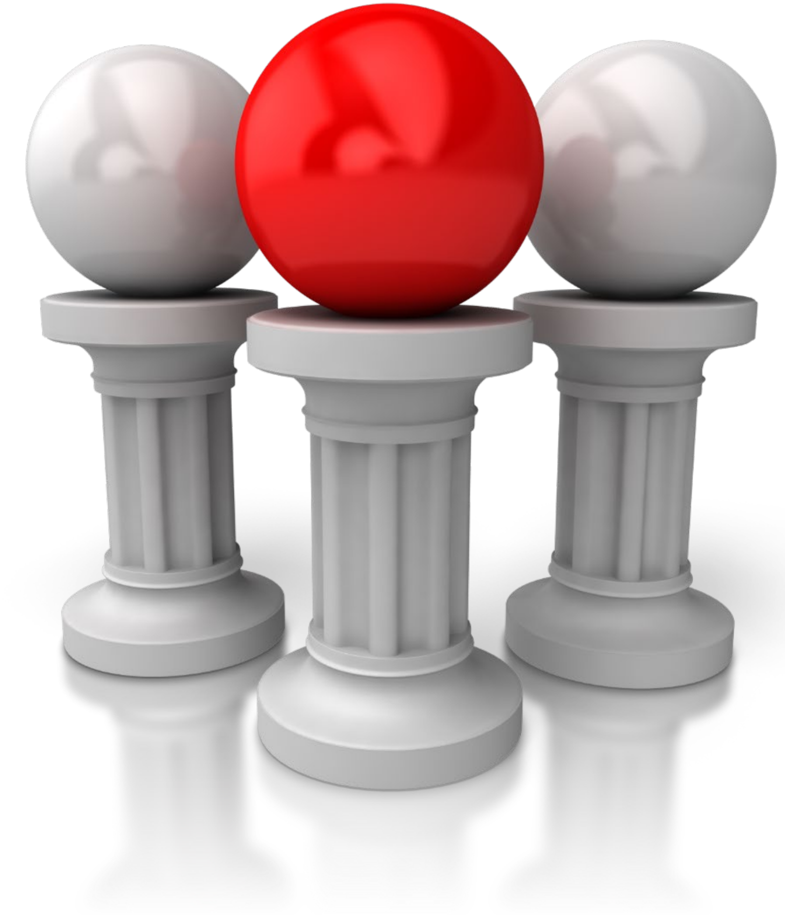
Management Elements of an Information Security Program

Develop a multi-year Roadmap (or have one developed) that details all of the activities needed to address your cyber risk.

1. **Board Policy** – Statement of Board support and commitment to provide resources. **Appoints an accountable executive** for the information security program. Determines **roles and responsibilities** for management and employees (very high-level).
2. **Information Security Policies and Procedures** –Covers controls such as **access management**, **awareness and training**, **data protection**, **threat detection and response**. Policies are **reviewed annually.** Procedures are high-level and operationally focused. Detailed how-to actions handled in "run-books."
3. **Incident Response Plan –** Plan detailing the **actions** that will be taken to **identify**, **respond**, and **recover** from a data breach or cybersecurity event. Will be refreshed and refined as the program is implemented.
4. **Business Impact Analysis** – Commonly referred to as a BIA. Interviews and data collection from management about **recovery of all processes** (i.e., critical, essential, routine, ad hoc). BIA report provided to head of the organization for sign-off. Serves **multiple purposes** – continuity of operations planning, succession planning, and information security.

Management Elements of an Information Security Program

5. **Data and System Classification** – Documentation of parameters of systems and location of all data – focus on confidential/sensitive. Data collection relies heavily on interviews with department managers and executives. **Input from County/City/Town attorney** to ensure coverage of legal drivers. Head of the organization appoints Data and System Owners – representatives that make ***business decisions*** about the systems and data.
6. **Risk Assessments** – Operational (adherence to proper cybersecurity protocols), system, and infrastructure. Data typically collected and analyzed by a **knowledgeable information security resource**. Briefings received by **management**. Information security resource should **recommend treatment options**. Risk decisions made by **executive leadership**.
7. **Develop of Program Plans**: This includes the development of IT Disaster Recovery, System Security, 3rd Party Vendor Management, Configuration and Change Management, Threat Detection, Vulnerability Management and Data Protection plans. Additional plans are developed based upon the need of the organization. Leadership is not responsible for reading or managing these plans. However, they are **responsible for ensuring that they are completed**, and that leadership is **apprised of risks** identified and remediated as part of the development as well as **ongoing compliance**.



Management Elements of an Information Security Program

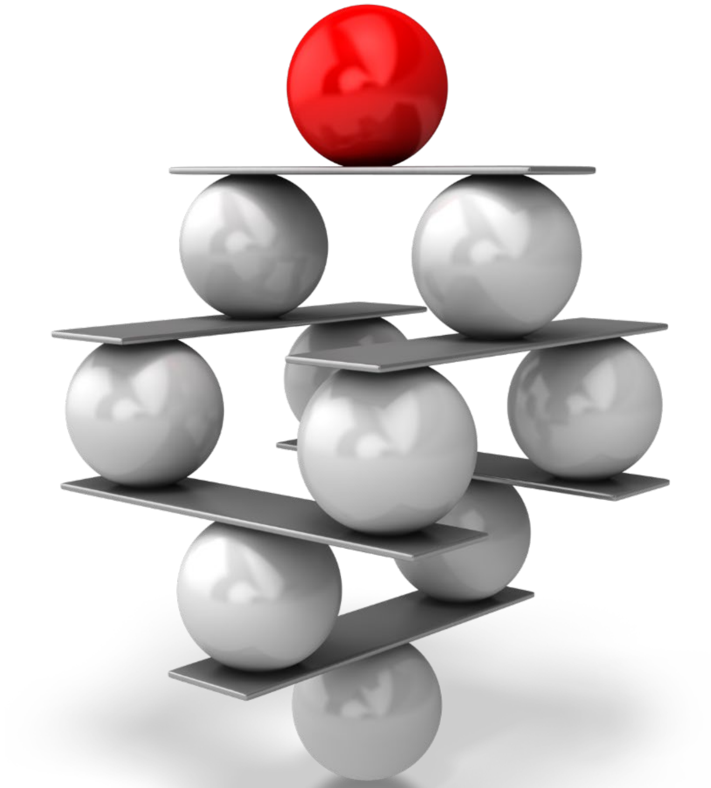
8. **Training** – These include initial efforts to make sure that people know **how to adhere to the information security program,** how to **identify threats** (e.g., phishing emails, scams) and **what to do** if there is an issue. Also known and Security Awareness and Training. Leadership needs to ensure that employees are trained, and this includes enforcement.

   Content should be engaging. Video, case studies, games.

   End users should be tested on their skills – phishing tests, drop a jump drive in the parking lot. If they make a mistake, don't shame – make it a **teachable moment**.

9. **Exercises** – This allows people to practice their roles and responsibilities to detect, identify, respond, and recover from incidents. Can include tabletop (talk through exercises) up to full response and recovery exercises.

10. **Operational Management** – Includes activities to implement the program into the organization to ensure it becomes part of regular operations and not a once-and-done deal.



Important: It takes far more effort and time to build a program than it does to maintain it. If you go longer than 2 years, without management activity, much of the program work will need to be redone.

Common Program Tools That Are Approved By Management

These activities should be included in the locality's strategic plan.

Directly align with other digital initiatives.

- **Defense-in-Depth Strategies** – Multiple, overlapping defenses – some visible, some "behind the scenes". Zero Trust Architecture (ZTA) is an excellent DiD strategy (prove to me that you're permitted to access this system/data).
- **Cybersecurity Monitoring – Different** from network monitoring. Should not be done by network administrators – since they are in the environment all the time and may miss risks. Also, they are focused on network management, not security management.
- **Endpoint Detection and Response** – First line of protection for servers and other endpoints that includes threat blocking, script control, USB device security, and ransomware protection**. More than antivirus**.
- **Vulnerability Scanning** – This is a regular (monthly) activity where the operating environment is scanned for threats and issues that could be exploited by a hacker. Leadership needs to be aware of major issues and risks coming out of this activity and apprised of plans for remediation.
- **Penetration Testing** – A test where an "ethical hacker" acts as a real hacker to try to find and exploit vulnerabilities in the IT environment. Tests the true state of security. They take care not to introduce any downtime and to immediately notify leadership if there is a critical issue/vulnerability/threat that needs to be remediated. Management should always be briefed out on the results of these tests.
- **Backups** – Monitor baseline traffic flow to backups – (depending on backup type) if ransomware cannot encrypt backups directly, it may try to overwrite backups with junk; one victim caught the malicious activity because it saw an unusual spike in backup activity. Ensure immutability!
- **Data Loss Prevention** – prevents movement of sensitive data outside of where it's permitted to be stored and accessed.

Name	Contact Info	
Darius Davenport, Esq., CWM, PLC	ddavenport@cvm-law.com	757-623-3000 (Office)
Karen Cole, CEO of Assura	Karen.cole@assurainc.com	804-767-4521 (Office)