2021 WCA Annual Conference

BALLROOM B

1:00 PM

to

2:00 PM

Best Practices on Cybersecurity: A Focus on Principles

About Us

- Aegis is the General Administrator for the Wisconsin County Mutual Insurance Corporation (County Mutual)
- County Mutual is a member-owned mutual insurance company and provides:
  - Liability
  - Workers' Compensation
  - Property
  - Supportive risk management and member services programs
- 52 of the 72 counties in the state
- Began providing our Cyber Enhancement Endorsement in 2014

Aegis
a Charles Taylor Company

About Us

- Excited to launch our Cyber – Resilience & Education Coordination Services (C-RECS) Program
  - Assessment services
  - Consulting & Educational

Aegis
a Charles Taylor Company

Today's Agenda

- Setting the Stage: Local Government & Cybersecurity
- Best Practices & Principles for County Leadership
- Wrap-up / Questions

Aegis
a Charles Taylor Company

A Scenario

You are your county's IT Director and you are just sitting down for Thanksgiving dinner with your family. In the middle of spooning your favorite homemade mashed potatoes, you receive a series of calls from a staff member working in 911 Dispatch. They are in a panic because they cannot access their dispatching software and calls are not coming through. You are forced to leave Thanksgiving dinner and drive to the 911 Dispatch center. You review the dispatcher's computer and confirm the dispatching software is locked – and you also notice all of the files on the network are encrypted. While you are reviewing the first computer, you get an another call from a staff member working in the Sherriff's department complaining the department's evidence tracking system is locked. You notice an oddly placed file on the desktop called README.exe. Your suspicions are high, but you click the file anyway. And then…

Aegis
a Charles Taylor Company


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

The Internet Has Changed the Way We Interact

- Lets go back 32 years to 1989—15% of households has computers
- The World Wide Web celebrated its 32nd anniversary this year—billions of people now surf the web each day
- Our daily lives are now online—and increasingly via mobile devices and the internet-of-things (IOT)—we text, email, IM, voice-over, socialize, and transact
- Our online activities leave behind a “digital footprint” which exposes us to potential risks and criminal activity

Aegis
a Charles Taylor Company

…But Presented New Opportunities for Crime

- The primary goal in creating the Internet, or World Wide Web, was to provide reliable communication between academic and military entities
- We didn’t anticipate that the Internet’s own users would someday use the network to attack one another
- The unique characteristics of digital assets have completely changed the nature of possession and theft as we know it
- Cybercriminals: An evolution from individuals to international organizations

Digital Innovation of Local Government

- Essentially, the term e-Government or also known as Digital Government, refers to ‘How government utilized IT, and other technologies, to enhance the efficiency and effectiveness in the public sector’ (Jeong, 2007).
- Transform both the back-end and front-end government processes and provide services, information and knowledge to all government customers
- Uses a range of information technologies to transform government operations in order to improve effectiveness, efficiency, service delivery and to promote democracy

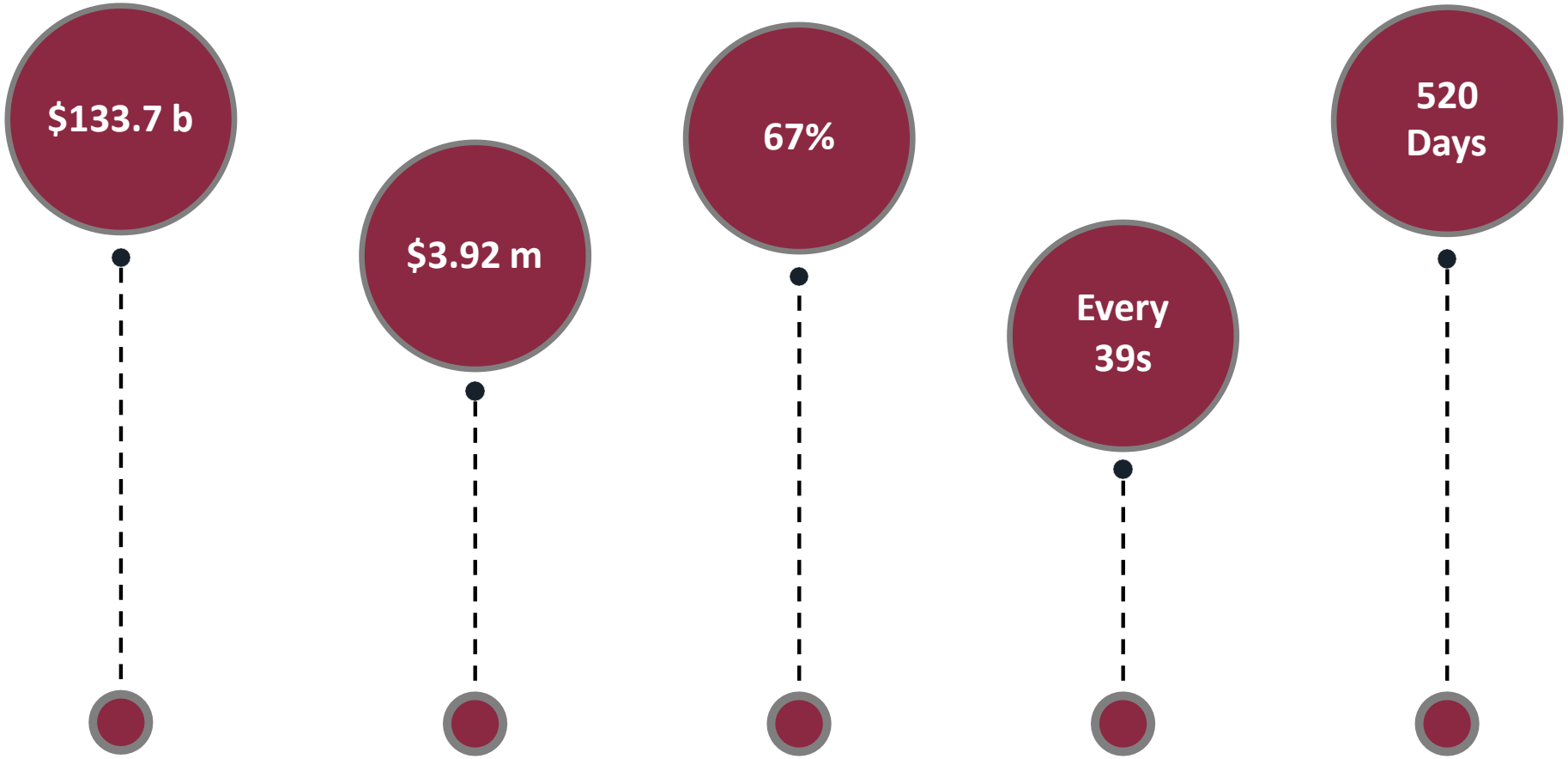
Aegis
a Charles Taylor Company

Security: An Important Local Government Challenge

- **Tradition**: Target private corporations with deep pockets.
- **Trend**: Target public entities with critical systems containing sensitive data.
  - **Resource-strapped**. Budget dollars go towards serving the needs of constituents versus a robust systems and latest technology.
  - **Open systems**. Public entity websites contain publicly accessible information (e.g. bill payment services, agendas & minutes) / Not hidden behind password protection
  - **Critical systems**. Law enforcement, EMS, nursing home/social services systems all contain critical services and sensitive data. These systems are a necessity to serve the basic functions of local government.

Aegis
a Charles Taylor Company

Local Government Cyber a Growing Concern



Aegis
a Charles Taylor Company

Approach Cyber with Risk Management

- Cybersecurity is not just limited to the IT Department – it is a countywide effort
- Incorporate cybersecurity responsibilities into every job description
- Ensure all staff are aware of cyber-related threats and provide training routinely
- Money won't fix everything – but in cybersecurity – it helps immensely. Support cybersecurity-related operating expenditures – not just capital expenditures.

Aegis
a Charles Taylor Company

Setting the Stage:
Local Government & Cybersecurity

Key Takeaways

- You can’t predict the when and how of cyberattacks. They can happen any day or time. Cyberattacks do not take holidays.
- The Internet has created many positive opportunities for society – but along with it - opportunities for cybercriminals.
- Cybercriminals find counties and other local governments as easy targets – you store lots of valuable information, short budgets and staff, and critical systems to serving your communities.
- Cybersecurity is no longer just IT’s responsibility, it is a countywide effort.

Aegis
a Charles Taylor Company

Special Considerations for Local Governments

- State and local government limitations
  - People: fewer employees to leverage
  - Funding: having to do more with less
  - IT: old(er) systems and equipment
  - Cybersecurity expertise: high demand, difficult to recruit and retain
- Leadership continuity
  - Short term costs, long term need

At the end of the day...

- We must all look towards *reasonable* cybersecurity.
- **Let's talk about what that looks like.**

Aegis
a Charles Taylor Company

Asset and Data Management

- You cannot secure what you do not know exists:
  - Inventory
    - Do you know what assets you have and where they are?
  - Responsibility/Ownership
    - Do you know who is responsible for each asset?
  - Importance
    - Do you know how important each asset is in relation to another asset?

  - (Category: Data center hardware; Asset: Core network switches; Location: Courthouse Bldg., Rm. 0001; Owner: Director Josh Dirkse; Rate: 1 (Critical))

Acceptable Use of Assets Associated with Information

- Have you defined, documented and communicated the acceptable use of assets?
  - Define and document
  - Implement appropriate controls
  - Security requirements are communicated
    - Employees and third parties
  - Accountability is key

Return of Assets

- Do you have employee exit procedures that include return of organizational assets when employment leaves the county or a vendor contract expires?
- Leadership, IT department, HR department, and Legal department must work together to establish and implement a viable exit plan for employees and vendors
  - Employee/Vendor returns all computing equipment to IT
    - Preserve the information
  - Employee/Vendor transfers all organizational information from his/her personal equipment
  - Terminate employee/vendor rights to information assets

Asset & Data Management

Key Takeaways

- It is important to: Know what you have – where it lives – how important is it – and who is responsible for it.
- Have a well-documented and thoroughly communicated acceptable use policy that includes requirements for employees and third parties.
- It is vital to have a technology exit plan for employees and vendors who will no longer work for the county.

Aegis
a Charles Taylor Company

Access Management

- Privilege Management
  - Users should be granted access based on least privilege – the most restrictive set of permissions or access rights – needed to perform assigned work tasks
  - Justified work-related reasons for access or the need to know
- Two common problems
  - Excessive privilege
  - Creeping privilege
- Periodic review of user accounts and their corresponding access rights

Access Management

Key Takeaways

Employees should only have access systems and data and the least amount of information relative to their position. Cyberattacks can be exacerbated without strict access controls as it widens the exposure points for cybercriminals.

Aegis
a Charles Taylor Company

Identity Management

- Password Management
- In recent years, there has been a significant shift in perspective and guidance
  - What is a strong password?
  - To change or not to change? How often?
  - Multi-factor authentication (MFA)
    - Is a username and password enough?

Identity Management

Key Takeaways

- Strong passwords are a must but Multi-Factor Authentication (MFA) adds an additional layer of security beyond the traditional username and password – that helps minimize unauthorized or fraudulent users/access.
- MFA is increasingly important because it is becoming a minimum requirement to qualify for Cyber Liability insurance.

Aegis
a Charles Taylor Company

Compliance Management & Vendor Governance

- Compliance: regulatory and contractual requirements
  - Federal regulatory requirements that apply to specific data owners or types (healthcare information – HIPAA)
  - Data protection clauses in contracts – POS and Payment Card Industry Data Security Standards (PCI-DSS)
- Vendor Governance
  - Managing the risk exposures of vendors who access or manage county data/systems

Aegis
a Charles Taylor Company

Compliance Management

- Federal and state regulatory requirements
- Third-party review of security
- Compliance with security policies
- Industry standard/best practices

Vendor Governance

- **Contract provisions**
  - Applicable laws
  - Standard of care for privacy and data security
  - Data uses and disclosures
  - Subcontractors
  - Service level agreements (SLAs)
  - Return or destroy data
  - Incident reporting and response
  - Audits and oversight methods
  - Risk management and cost allocation

- **Key program elements:**
  - Vendor tracking and approval
  - Pre-engagement due diligence
  - Standard contract provisions
  - Oversight and enforcement

Compliance Management & Vendor Governance

Key Takeaways

- Assess all areas of regulatory, self-imposed, and contract compliance. Compliance never rests – ensure your policies address each area, and make sure to conduct routine review and amendments.
- Engaging vendors to provide IT and data-related services changes an organization's information security risk profile. Review and negotiate contracts and conduct thorough due diligence first, and then use proper oversight and enforcement to manage this risk.

Aegis
a Charles Taylor Company

Management of Information Security Incidents and Improvements

- **Preparation**
  - Identify resources needed for incident response capabilities
  - Ensure individuals are properly training and ready to respond
  - Develop and communicate:
    - Formal detection
    - Reporting processes

Management of Information Security Incidents and Improvements

- **Detection and Analysis**
  - **Detect**
    - Reported by end users or detected (and reported) via trained IT personnel
    - Technical controls
      - Automated detection of security events coupled with near real-time reporting
      - Data aggregation tools
  - **Analysis**
    - Understand the scope of the suspected incident
    - Assess the urgency
- All data gathered helps inform prioritization and activities in the next stage

Management of Information Security Incidents and Improvements

- **Post Incident Review**
  - Hold a “lessons learned” meeting
  - Review corrective actions put in place
  - Document for metrics and historical purposes
  - Are there any high-level issues that you, the leaders, should be involved to support resolution?

Management of Information Security Incidents and Improvements

Key Takeaways

- **Preparation**: Make sure you have an Incident Response Plan, make sure it is a living document, and test it routinely.
- **Detection and Analysis**: Make sure your plan requires timely notification of incidents, which aids detection – and make sure it addresses a process for evaluating the severity of the incident – which dictates how the plan will respond.
- **Post-Incident Review**: While often overlooked, post-incident reviews help you learn how to avoid further incidents in the future.

Aegis
a Charles Taylor Company

Create a Risk Management Gameplan

Conduct an **“assessment,”** not an “audit.”

Create your personalized **cyber risk management plan**

Prioritize your organizations top cyber risks

Implement your plan and continue to **improve** on it

Remember, the headlines of major cybersecurity breaches—like the one at Yahoo—don’t tell you the full story. As a leader, you must help tell the full story for your organization, and that’s what matters.

Aegis
a Charles Taylor Company

Thank you!

Questions?

Aegis
a Charles Taylor Company