Preventing & Mitigating Cyber Attacks

South Carolina Association of Counties

August 6, 2018



"Accelerating Speed to Strategic Value Utilizing Quarterly Governance"



Mecklenburg County Government

- Largest population in North Carolina over one million residents
- Includes City of Charlotte and 6 other towns
- Major county services
 - Health & Human Services
 - Criminal Justice Services
 - Land, Use and Environmental Services
 - Parks & Recreation
 - Tax Assessment & Collection
- \$1.7 Billion Operating Budget







Erica Elleby

- Began local government career at Mecklenburg County, NC in 2001.
- Director of Business Operations and IT Controller for Mecklenburg County's Information Technology Services
- Responsible for enterprise technology spend, IT vendor management and asset management
- Local Government Experience
 - Strategic Planning & Performance Management
 - Application Management & Support
 - IT Strategy & Planning
 - Vendor Management
 - Budgeting



Technology Pressures Facing Government

 External influences will impact our future direction as much as (or more) than maintaining existing technology environments

• These forces will drive future technology policy, planning, investments and *RISK Management Strategies*





i5q+3r6MVMLa1V/Mpa0NxoXWqy1A9brbUQJmERJNwaOCuVubOwI5JhRdtAm1EZ74vxTvsaNJqj0ygFTyZTFRU5sAYtWfh/NRkg8q5fF 11wyua+616itPoZw1hPshGeVmbC+MLjtRYES5HoBM0Fa0Mo+Q+2nmU+4Pvhb33E2Ew9izNayFjwQ0gcwvjUBQUYV/FuFyLPcdp1jHAC I/CCbmpHye5RUaeOT/G6yPezgZFEfqS2CE8nz9GBt+ab3Pbo9On2MMyGn1h7zTNyzIBOKb07FqQFbsXCMgCKz4b+iQwIAtv6z7TFMBa WS6UJEA/4jdrS1390g8g1cWm0J7LYVvQThyzBt61KDPExN6 Y+6NtXFqS901XNREf3kIjnaKWiKzBSbVWleTXnl2Hxt/ghl Db+geLNkXIR5T5BDR9ZLdr2sOM5WZXGp7i05EFFFgisV 2017tHHjFn1SBPUgoF/3GhmMyOC9dG0708gxz+v5e9/75 :sFC/8myp//VPLFK0wx2sgA+SGbYLj9KAFveev5vD/PR eCzhuTc+N7vkxi/pkmUA5YtBeHUG7OKTQt2tIQDM5/V E3NPwXT0v9b Ct6yWJ11EjUI3i1KrjUe2Aj5ZiacGpRAp14KEhFRHf wgYJ1Y30axS DHMPFsQ9b4AtTfIbgZtu1QGjfTVOq+jdZeAWBfcZ/LI 17bHyiRKih8FuaWgegyYLtSSD18PYKVtSWBFZ+1IZ0p goD7wbga4ndvpUL wDftdtG5yGMHbMdZRz/hYv0IAprhi6kBosCdfeB9xX jeqNVgFLj4gcOeOdaKWw10cp4OuSed7IGV/y6Pzhq uc2vBVG/JzpQkz2 thFc5i2zHpbFcGwTpTtwqF0v7jAHMmj2yg715n1dfv TPW5Fu2yyxC79YaasImkxc9XSe1u63G3Kx0k3m08dRtbhhEQf4rM9TDLvLg1 eM2T2NtB15HVnk8ThZ40Z7F6Crnghtgzk0x1RagnkE zOtP1SmgX1/BEeRB4PkBG6fSufCOK/wgcDHexCuyeHxoS+jtL/nkN14xTkseScY GyDsCzrpDGFEiMeGcXtBWO+R0bgnup4fMyk7U+ k1k4Pi86UzV3z67CY10DIDgxoFyA3awS7TdvdV3/boP+qGA0wB+PGXPNiC9TIoZ6P3PFbUSrf1GCcxe10jKMfYncAAzqDh0rkFo4MC KgIr0yqv2/uRVgMXg41xi5Tc4xDdAza+45Nw34PwVxcUPRJNgubbsXVbTanJWLqVaD06xU2N8m8jwYA/03hD8iKaIQjT+y43q/zzG1 Ayg9wmuDfg00HLhT4Gwj/6qLe0ofc1khjY6756JQADkMxKDubmCTL6UgAMoeF2P5GXYQh31cB04n1Cy4Ua3D3UJjsGe5U/YozY6e0C waVPZT/Z6Wow/G8I1aaK003Rqo8tL+HqyIHNCRMIul0pDEB+6XPzXqkUhNfptYRzSGsV9ZpHi/h/eMNFlJxamtM6y/iZOX3d49reDT /+Mpmi+pLq0pC9gJJg38H6PuUZS0U0XlTGbeLnx9u0TbB8vo7ZrVjmdMrehvZ1FI+WiplgRT3Suvlzz6rgC47pD6M3GvG4VCm0MOF5v h4itLIx009jevudvwLoLUjZ0VzGro8UfN9G3Av7Eo7nJfLqYBit54HPF9TVXSIUeGykkHnt2wuqfQd9FJJmgynvpsRiB3Su4Ez7mmh .sD8BkuBqEBlQv0qKv0tfjHa0078KovcDkzbEDY/TpedLxfBJEJcYU6zhyWCzX7zsXX5xc7mhq0BStc0B7aE29K0gtvrf/iRuILJLyI wiRXMPcFcgnaqGg1ZBsJbZTG+qoCKDo3Nj1IzmnJPvnLp7fNZjZYuFP5bjVb4jbFs6si1RnZh19Fd1f6SdNZSH+Nw8xCL9j4pBJ5ok PiBVCdq4UuLEawlvXLaZe24FAEdbpDNgJT4BqtOArcVxHUOsTtU1qsARqUd0Zmyf5a9YnByQGTI6rrICRiAFZj1+teNJiA2T3ntTME +JCATdOUyHx13Ks/tCyIA6BBMW6NVg/VLKnfFzyCPdkZfRLa7WUjVqgXhASRXys7xR9677Mp37+nEaFdbrwVIiN9hhG6HSJ9YkV6ts zonnljHpP2GhLf8F0BZtkRN4TEOspjjWgmYSroNRTqxFKbuf6yXWh8Rjnjb9p3D4c+9xNzNqVq9vkqLqmQIwsbNwVkx7Nzw1ak/7UE AjS/FsgXHmK7+fttlHamsk2lCFV@VCWRmGK26BHZgheCbYG8845f4gYhVg907DH7fVsSpb223ym6mkoYZg30geZtNsOpte/9xnTsME bYE71yIId/noyN93za 72) Jgfvit irtypicu (t3 xy30p) FeX0 jikR01 m AFcc/rx51 PgqC lpk YSH CREJnjWnYGpwQyKFlLxC TOJB1y3IuPXETYS5S] HCCCS/ 9M d7k/Vta FK0/mJ9tL Fumm J/G /3 jLv1 cmtD rv Dnr g wL3k eV06eKQYps2dyg3eCy3s R/vo8ye+4HPMLShv36 jix G nU2R dAecia nwwbe czD 7.60 vgM8 Fz /F ut nSG1 ji xg vbe g/wjoiADFPjPvhc6kKkE Ivd5TF571b42TK263yihGcvziaD20DA04UxCcvKHMpiuwJ/bBG4/v8AVgEkRKZgCaFiLvFaFKbvEDIvo38+sH7Lb+PL7HSy7v155SFy fk86q06AyaIblvRj09dv5TzjL6XyygF4XiYjlgxkMCUyQZ9/d5ehMUPLo4c4hIXAXuKHfUUHvtXv2qdhbEGn1vycsYP9jrmxfqNNYI i6e8VtLynWmJ2SdoR1411hZYP9TgwJF00K2pCeQo4c8VpdtZNeqdUaYPT3LtNJm17kAaf0Fg9iXoKqnvOYmBg1NGUUTqHTK30Xi2fRs PW8tCg1H+QuqY/b1MwgsAoFF835uZrmyCS7z9wNsfa0RPtYKiZS6J6/RRTUmgHiKu8utg56F1Tchek01B9umUgfga4Udm4QS9OoZHR M3+6yLRTrQxToXNDzLuqixNB7N1kUC+5vI/CXgGeZuzcuEGWV9Sb0ofr4DcdROytQQY1wvQmfki1QrCTMwDBIWC1qx+4tdgV4g4k6A nxf/Gq/ovJYwooGdOYkrDoW8NbIpsrLkHOiZXgRvnz9gzrEm]BoP7uHZuKU/19Sa/imwyyTuGrfisfvOwtMR078RB811H8vOfgi+gE

Number of Organizations in the U.S. That Suffered a Data Breach



Cybercrime: Third Largest Market Cap (2016 data)

Impact of Cybercrime vs. Market Cap (\$B)



Apple Alphabet Cybercrime Microsoft Facebook (Google)

https://breachlevelindex.com/

DATA BREACH STATISTICS

DATA RECORDS LOST OR STOLEN SINCE 2013

Some 9.7 billion data records have been lost or stolen since 2013.



DATA RECORDS ARE LOST OR STOLEN AT THE FOLLOWING FREQUENCY



*Due to legal requirements, not all breaches are reported or publicly disclosed. Regional differences of data may not accurately reflect total data breaches that occur. Statistics presented are based on the Breach Level Index [breachlevelindex.com] © 2018 Gemalto NV_

2,600,968,280

NUMBER OF BREACH INCIDENTS

PERCENTAGE OF BREACHES WHERE NUMBER OF COMPROMISED RECORDS WAS UNKNOWN

55.9%

PERCENTAGE OF DATA BREACHES WHERE ENCRYPTION WAS USED

3.1%

NG FREQUEI A RECORDS WERE LOST OR STOL

EVERY DAY 7,125,940

EVERY HOUR 296,914

EVERY MINUTE 4,949

EVERY SECOND 82 LESS THAN 4 % of breaches were "Secure Breaches" where encryption rendered the stolen data useless



Ransomware the favorite attack method used against businesses



detections were ransomware, compared

to only 1.8 percent on the consumer side.

Malwarebytes

Ransomware: More Devastating & Widespread



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

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



Check Payment

Decrypt

Copy

Ransomware: More Devastating & Widespread

BAD RABBIT

If you access this page your computer has been encrypted. Enter the appeared personal key in the field below. If succeed, you'll be provided with a bitcoin account to transfer payment. The current price is on the right.

Once we receive your payment you'll get a password to decrypt your data. To verify your payment and check the given passwords enter your assigned bitcoin address or your personal key.

Time left before the price goes up

Price for decryption:



Enter your personal key or your assigned bitcoin address.



Annabelle Ransomware includes everything but the kitchen sink when it comes to screwing up a computer. This includes terminating numerous security programs, disabling Windows Defender, turning off the firewall, encrypting your files, trying to spread through USB drives, making it so you can't run a variety of programs, and then to sweeten the pot, it overwrites the master boot record of the infected computer with a silly boot loader



ANNABELLE RANSOMWARE

SamSam Netting \$325K in 4 Weeks

SamSam Ransomware has infecting :

- City of Atlanta
- Davidson County in North Carolina
- US Hospital (Hancock Health)
- The Colorado Department of Transportation (CDOT) not once but twice in February

5 Things to Know about SamSam Ransomware

- 1. SamSam has been on a tear in 2018
- 2. SamSam is primarily targeting healthcare and government organizations
- 3. SamSam is not spread via spam emails
- 4. The attackers behind SamSam are wellversed in evading antivirus, and may infect victims multiple times
- 5. SamSam can be stopped

Today's advanced attacks <u>routinely</u> <u>bypass antivirus</u>. To stop them, organizations need to invest in smarter, stronger endpoint security that has the ability to block not just executables, but malicious activity in real-time.



MeckNC.gov



TIMELINE OF SAMSAM RANSOMWARE ATTACKS IN Q1 2018





Cybercrime

- Cybercrime industry is BIG business looking for new victims
- It can operate incognito and hide behind foreign boundaries
- Well financed and getting more sophisticated and tenacious in its approach





Cybercrime



Cybercrime has three main purposes *Extortion, Theft, and Exploitation*

- All three are critical threats to the public sector
 - Extortion: Freeze the ability to provide public services (safety, health & welfare, commerce)
 - Theft: Cash and information
 - Exploitation: Override protections or alter political outcomes
- Public Consequences
 - Loss of services
 - Loss of life
 - Loss of trust
 - Loss of taxpayer \$



Why is Public Sector a Target?

- Provide valuable, time critical services
- Have valuable information that can be sold multiple times (personal / HIPAA / PCI)
- Have ability to pay (big budgets / pass through lots of \$)
- Large workforce trained to "be helpful" Phishing targets
- Likely to have under invested in cyber protection and recovery systems
- Likely allowing employees to practice unsafe cyber practices
- Weak(er) crisis management plans & continuity of operations plans





Costs of Data Breach

- Life or Death impacts to individuals
- Reputation damage / negative publicity
- Lost / compromised data
- Lost productivity
- Potential further affects on clients (e.g. identify theft)





SOCIAL

The clever manipulation of the natural human tendency to trust.



75%+

credentials

of all network intrusions are due to compromised user

PHASE 1	PHASE 2	PHASE 3	PHASE 4	PHASE 5
PRE- ENGAGEMENT INTERACTIONS	INTELLIGEN CE GATHERING	PRETEXTING	EXPLOITATION	POST EXPLOITATION
RULES SCOPE CONTACT INFO PROJECT CHARTER	PUBLIC RECORDS SOCIAL NETWORKS DUMPSTER DIVING	CREATE BELIEVEABLE SCENARIOS	• EXECUTE SCENARIOS • ATTACK	PILLAGE DOCUMENT CLEAN-UP

So•cial En•gin•eer•ing

TYPES OF ATTACKS





Phases of a Cyber Attack



Mecklenburg County

Mecklenburg County's Ransomware Attack

- Ransomware attack—December 5, 2017
- Mecklenburg County network credentials were compromised by cyber criminal(s) using a social engineering Phishing attack
- The criminal(s) utilized harvested user sign-on credentials to gain un-authorized access to Mecklenburg County systems
- The criminal(s) then planted Ransomware to 'Freeze' select systems and then demanded payment to 'Unfreeze'
- 48 Servers encrypted—Over 200 systems impacted





Cyber Incident Response Plan





Cyber Incident Response Plan

	Information Technology	Business Owners
Phase 1: Preparation	Facilitate, Make Plans & Be Ready	Be Ready to implement response & communications plan —timing is everything
Phase 2: Detection	Identify & Respond	From first alert—follow the plan and communicate
Phase 3: Analysis & Validation	Investigative Process for Digital Forensics	Provide information to support Analysis—help prioritize. Identify manual procedures and controls for business continuity.
Phase 4: Containment, Handling & Eradication	Utilizing a Controlled, Methodical, Secure Process	Clean up and restoring services, procedures to support data integrity and internal controls and customer service
Phase 5: Recovery	'New Normal' Standard Operating Practices	'New Normal' Standard Operating Practices, Training, Build Resilience





Preparation & Detection

What preparation did we have?

When did we know this was happening?

What did we do to contain the damage?



Phase 2:

Detection

Phase 1: Preparation

Detection and Analysis

Phase 2: Detection Phase 3: Analysis & Validation

Backups: Server team stood up a new database environment & we restored database backups for various systems which ran overnight

Gained additional insights from various sources regarding potential risks & benefits of paying ransom. Engaged Experts (Microsoft, FBI, Fortalice, TrendMicro, Others)

Based on risk / benefit analysis and input from numerous discussions with County Executive Leadership, decision was made and communicated that:

Mecklenburg County would not pay



https://www.nytimes.com/2017/12/06/us/mecklenburg-county-hackers.html



Containment, Handling, and Restoration

Utilizing a Controlled, Methodical, Secure Process

- Isolation of "Clean" systems vs. "Not Clean" (which remained quarantined)
- Restored "Clean" data into "Clean" environments
- Reset all system accounts and passwords
- Tightened 'In-bound' and 'Outbound' Firewall rules
- Executed Restoration Procedures
- All: communication



https://www.mecknc.gov/news/Pages/Countywide-system-outage.aspx



Identified "New Normal" Security Practices

Phase 5: Recovery

75%+ Implemented extended password length network intrusions are due to compromised user credentials Significantly restrict international emails box Policy & Perimeter Security changes; Personal Storage Locations External email alerting & Applications: 🐼 Dropbox Non-County web-based email elimination amazondrive • Eliminate email auto-forwarding Microsoft Dynamics S 🕻 Route Match Cerner[®] **OneDrive** Microsoft Cloud Vendor Hosted for Business TRACKS **Applications** Diffice 365 \mathbb{D} MODRIA. Skype PowerSchool for Business Spatialest MeckNC.gov

CHANGE: "New Normal" Security Practices

Phase 5: Recovery

CHANGE

NOTHING

NOTHING

WILL Change

Executive Alignment & Sponsorship
On-going Communication & Target Dates
Training & Support



Implement A Layered Security Approach

Goal: Reduce an Attacker's Chance of Success While Increasing an Attacker's Risk of Detection

IT Security utilizes a layered model to address security concerns across the enterprise. Due to the highly dynamic nature of information security, specific items on this diagram are frequently updated; however, security initiatives should align with one or more of these layers as an area of focus.



IT Services Team

What Went Well

- Treated as a County crisis Not an IT issue
 - ✓ Daily command center engaged throughout
- Communication strategy came from the Top early and timely frequency (email & telephony was essential)
- Had strong back-ups and ability to restore
- Had practiced IT and Department COOP's (table top exercises)
- Had strong relationship with Forensic IT companies (on the job within hours)
- Had Cyber Insurance



Lessons Learned?

- If you have valuable data (personal, HIPPA, PCI), provide critical infrastructure services, or have the ability to pay, you are a cybersecurity target – You are probably being watched and tested as we speak.
- Cyber criminals are highly sophisticated and persistent in our case, they spent considerable time looking for a way in – moved quickly once in.
- Your employees will fall for phishing (no matter how much training you do).
- Your employees are unaware of file sharing and other social media risks – you may be surprised at how much unauthorized file sharing is going on: personal storage, Dropbox, etc.



Lessons Learned

- If (when) you are hacked, be aware that your IT access will be blocked (inbound and outbound) by 3rd parties. You will need to prove to each provider that it is safe to restore access (can take weeks)
 - Banks
 - State, Federal, Local systems (even, in our case, cities and towns within our County)
- You will be inundated with assistance and advice (these were unanticipated management communication challenges)
- Be prepared for counter attacks



Preparation for Next Time

- Quickly adopt "New Normal" security standards
 - Revise employee and IT policies
 - IT security & infrastructure strategy and investments
 - External vulnerability reviews and testing of IT controls
- Update COOP plan to include Cybersecurity lessons learned
 - Prioritization of system restores
 - Increased capacity for system restoration (speed)
 - Scheduling exercise to test and improve
- Shared perspective with Risk Management team, Cyber Insurance provider and others





Vendor Management

Third-party vendor relationships can create additional risks to your organization. Best practices to manage third-party vendors:

- Establish a tone at the top with managementlevel oversight
- Ensure appropriate investment and staffing
- Conduct third-party screening, onboarding, and due diligence during RFP process
- Align vendor IT security plan with organization



Disaster Recovery & COOP Plans

- Structured and documented approach for responding to unplanned incidents
- Step-by-step plan that minimizes the effects of an incident or disaster
- Typically, disaster recovery planning involves analysis of business processes and continuity needs
- Disaster Recovery Plan checklist includes:
 - Definition of what constitutes a 'disaster'
 - Recovery Time Objective (RTO)
 - Recovery Point Objective (RPO)
 - Identify most serious threats & vulnerabilities
 - Disaster recovery strategies
 - Cybersecurity integrated into DR & COOP plan
 - Response team roles and responsibilities



Cost / Risk



What Should the Public Sector do?

- Have a candid conversation about enterprise risk of Cybercrime with all functions at the table
- Prioritize critical functions (external and internal)
 - Less about IT tools, more about operations and protecting the public
- Update continuity of operations plans
 - How will you operate under no or restricted IT functionality?
 - How will you record activity?
 - Financial controls?
- Get a baseline assessment of your critical IT infrastructure
- Move your workforce to a "new normal"
- Educate your workforce / vendors
- Restrict access / dual authentication
- Assess Cybersecurity Insurance coverage



What Should the Public Sector do?

- Reduce attacker chance of success and increase risk of detection
 - Prevention, Policy, Security, Monitoring, and Response
 - Layered approach to security (endpoint, perimeter, network, application, data)
 - Multi-year strategic plan of investment based on risk
 - Penetration testing
- Prepare for the unexpected (annual tabletops)
 - Crisis Management Plan
 - Continuity of Operations Plans
 - Cyber Security Plans
 - Incorporate additional skepticism thinking



Skepticism is the process of applying reason and critical **thinking** to determine validity. It's the process of finding a supported conclusion, not the justification of a preconceived conclusion.

C MARK ANDERSON, WWW.ANDERTOONS.COM



"Before I write my name on the board, I'll need to know how you're planning to use that data."

Thank You!

