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**

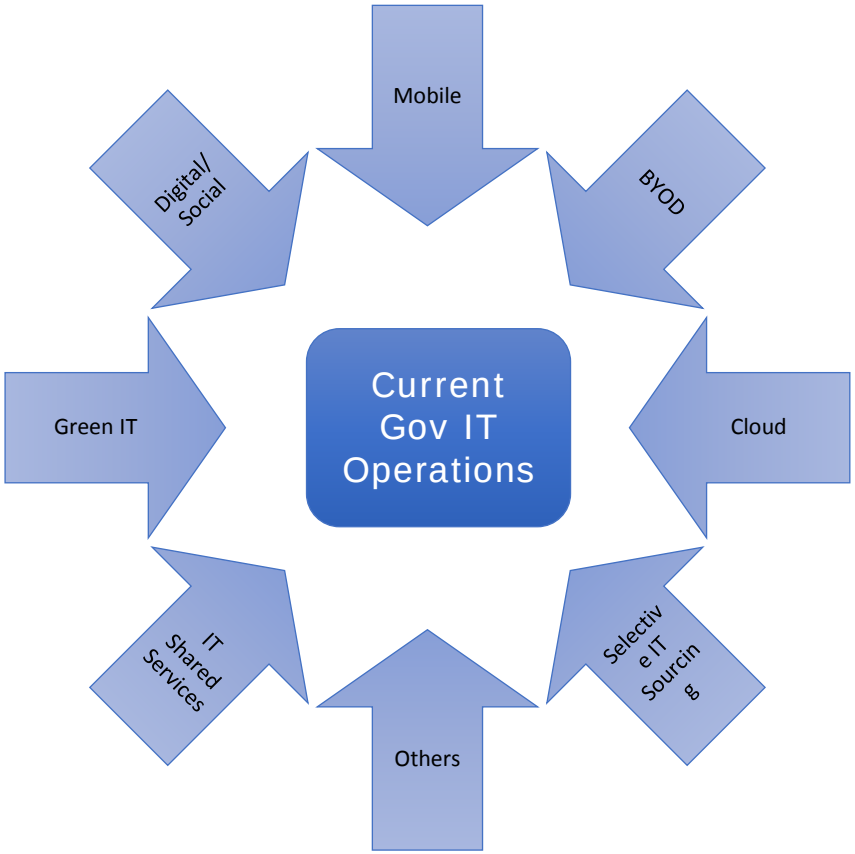
Erica Elleby

- **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

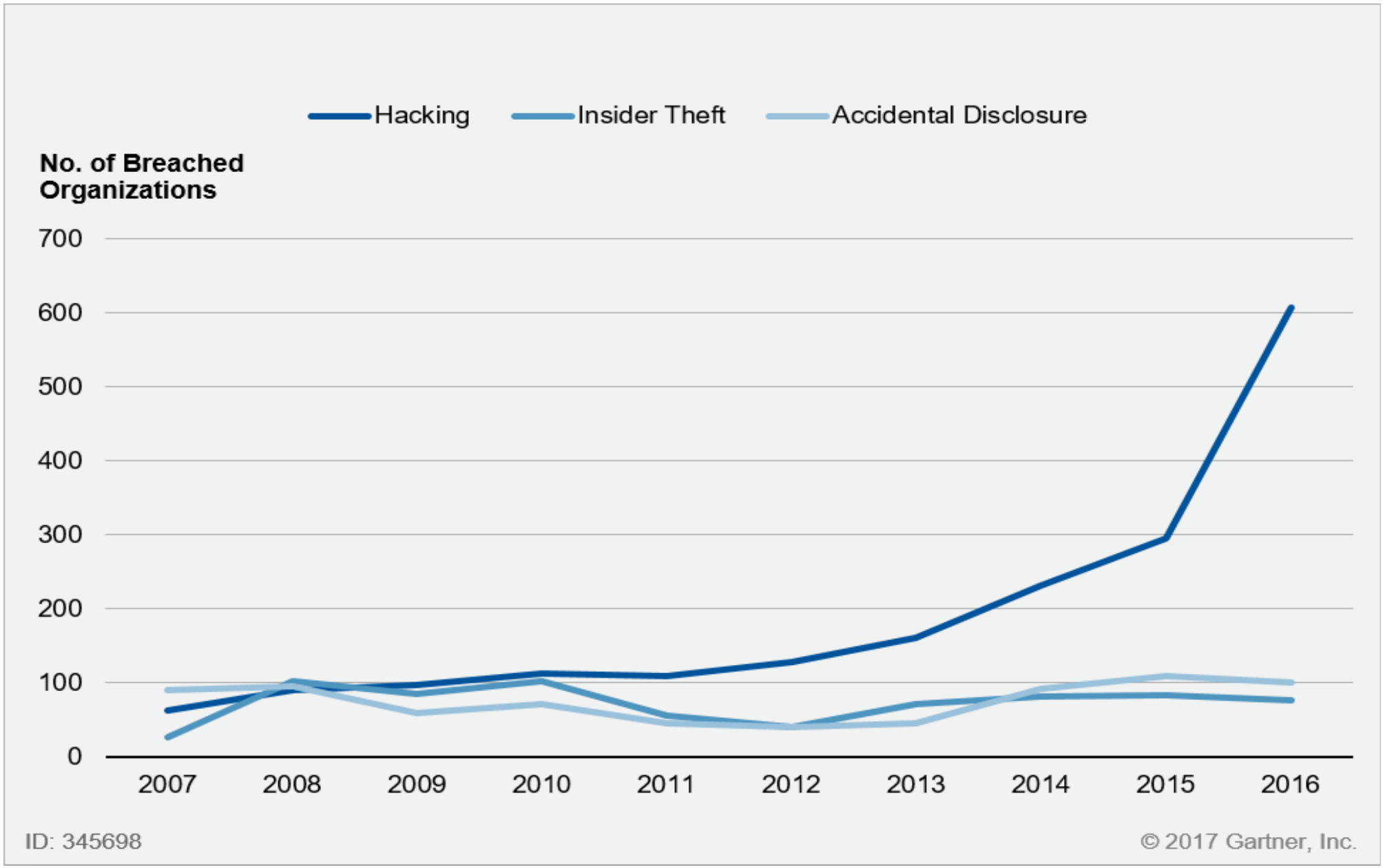
- **External influences will impact our future direction as much as (or more) than maintaining existing technology environments**

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

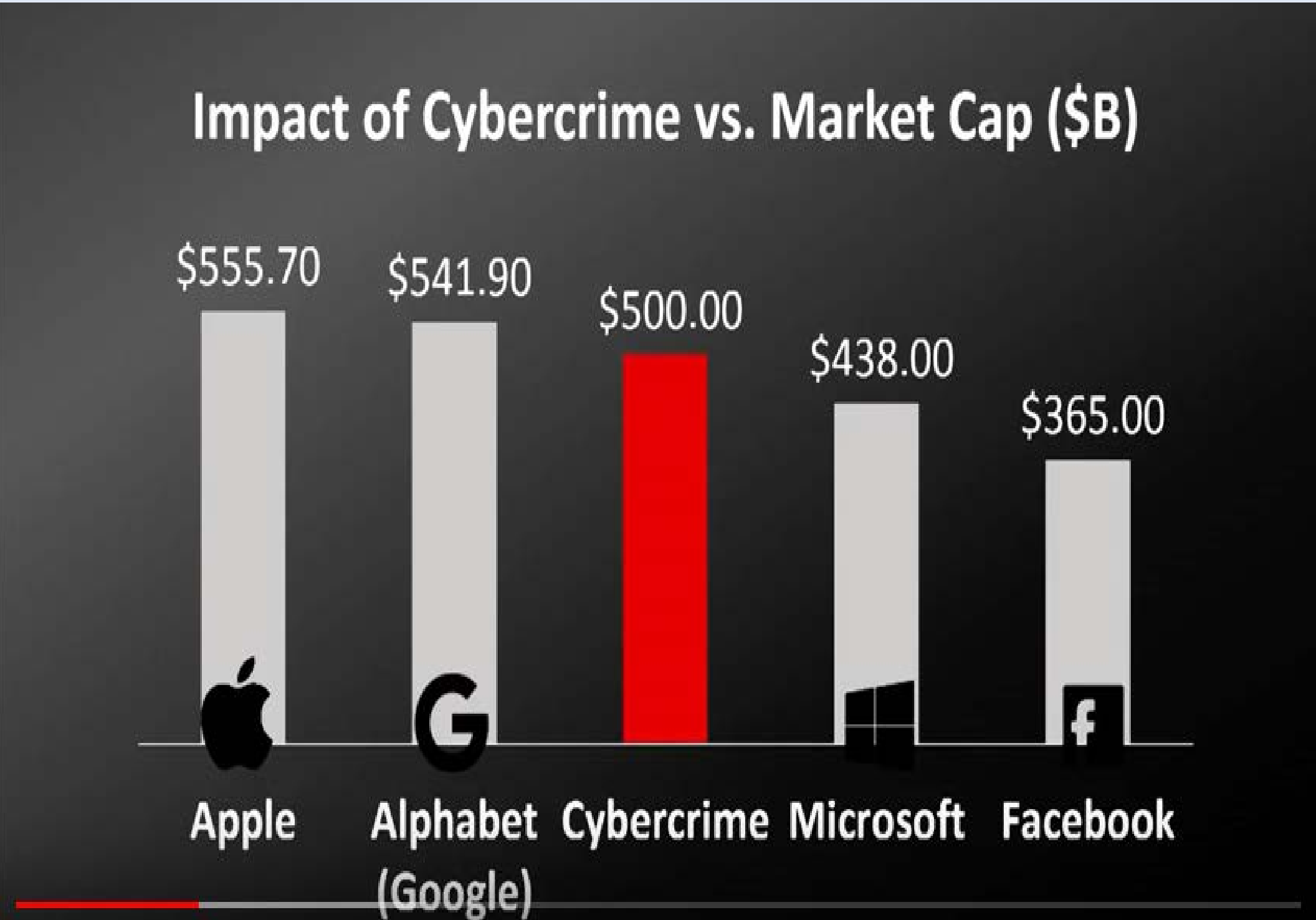



RANSOMWARE
PRESS ANY KEY!

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



Cybercrime: Third Largest Market Cap (2016 data)



https://breachlevelindex.com/

DATA BREACH STATISTICS

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

DATA RECORDS LOST OR STOLEN SINCE 2013

9,727,967,988

ONLY 4% of breaches were "Secure Breaches" where encryption was used and the stolen data was rendered useless.

DATA RECORDS ARE LOST OR STOLEN AT THE FOLLOWING FREQUENCY

EVERY DAY

4,825,381

Records

EVERY HOUR

201,058

Records

EVERY MINUTE

3,351

Records

EVERY SECOND

56

Records

*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]

gemalto
security to be free

RECORDS BREACHED IN THE YEAR 2017

2,600,968,280

NUMBER OF BREACH INCIDENTS

1,765

PERCENTAGE OF BREACHES WHERE NUMBER OF COMPROMISED RECORDS WAS UNKNOWN

55.9%

PERCENTAGE OF DATA BREACHES WHERE ENCRYPTION WAS USED

3.1%

DATA RECORDS WERE LOST OR STOLEN WITH THE FOLLOWING FREQUENCY

EVERY DAY
7,125,940

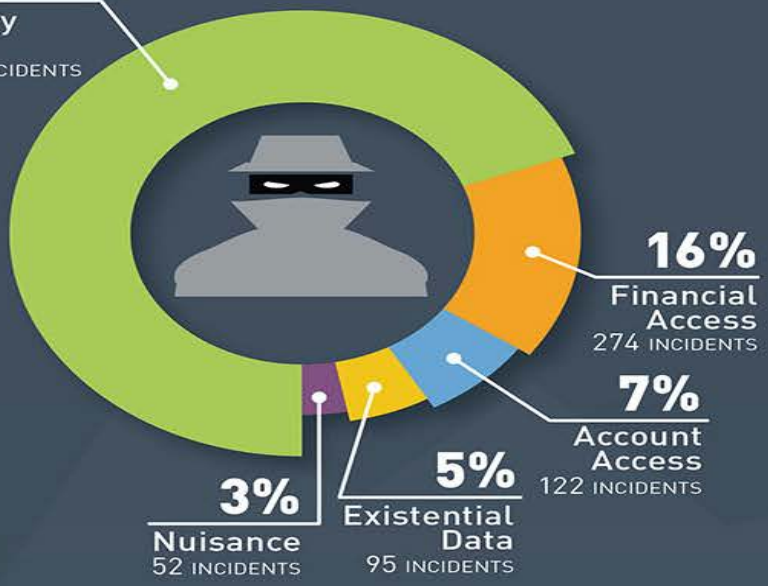
EVERY HOUR
296,914

EVERY MINUTE
4,949

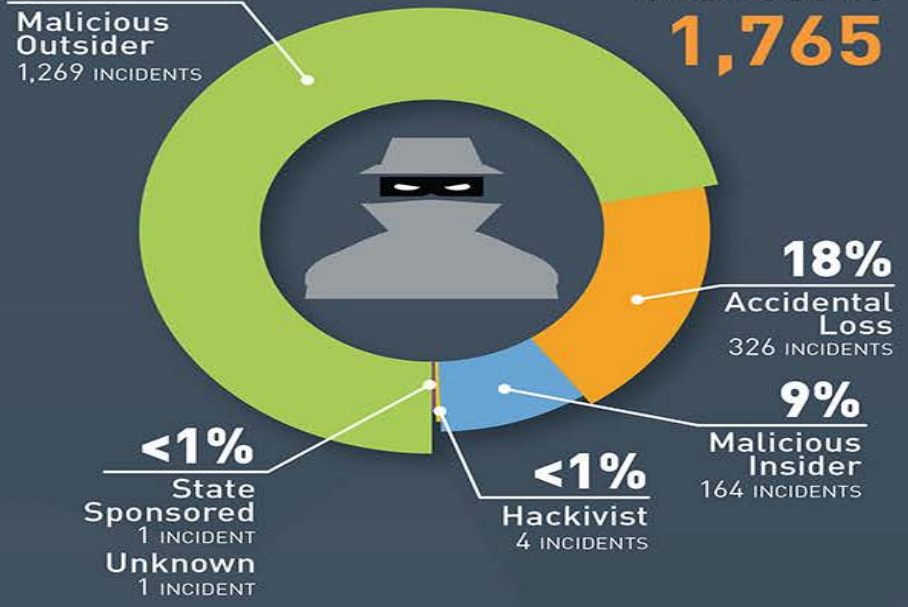
EVERY SECOND
82

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

Number of Breach Incidents by Type



Number of Breach Incidents by Source



Number of Breach Incidents by Industry

HEALTHCARE 471 INCIDENTS 27%	TECHNOLOGY 130 INCIDENTS 7%	HOSPITALITY 36 INCIDENTS 2%
FINANCIAL 219 INCIDENTS 12%	PROFESSIONAL 92 INCIDENTS 5%	INSURANCE 22 INCIDENTS 1%
EDUCATION 199 INCIDENTS 11%	OTHER 68 INCIDENTS 4%	NON-PROFIT 21 INCIDENTS 1%
RETAIL 199 INCIDENTS 11%	INDUSTRIAL 60 INCIDENTS 3%	SOCIAL MEDIA 9 INCIDENTS <1%
GOVERNMENT 193 INCIDENTS 11%	ENTERTAINMENT 46 INCIDENTS 3%	

BREACHLEVELINDEX.COM

Ransomware the favorite attack method used against businesses

400

Nearly 400 variants of ransomware were cataloged in the fourth quarter of 2016 alone.

267%

Ransomware distribution increased by 267 percent between June and November 2016.

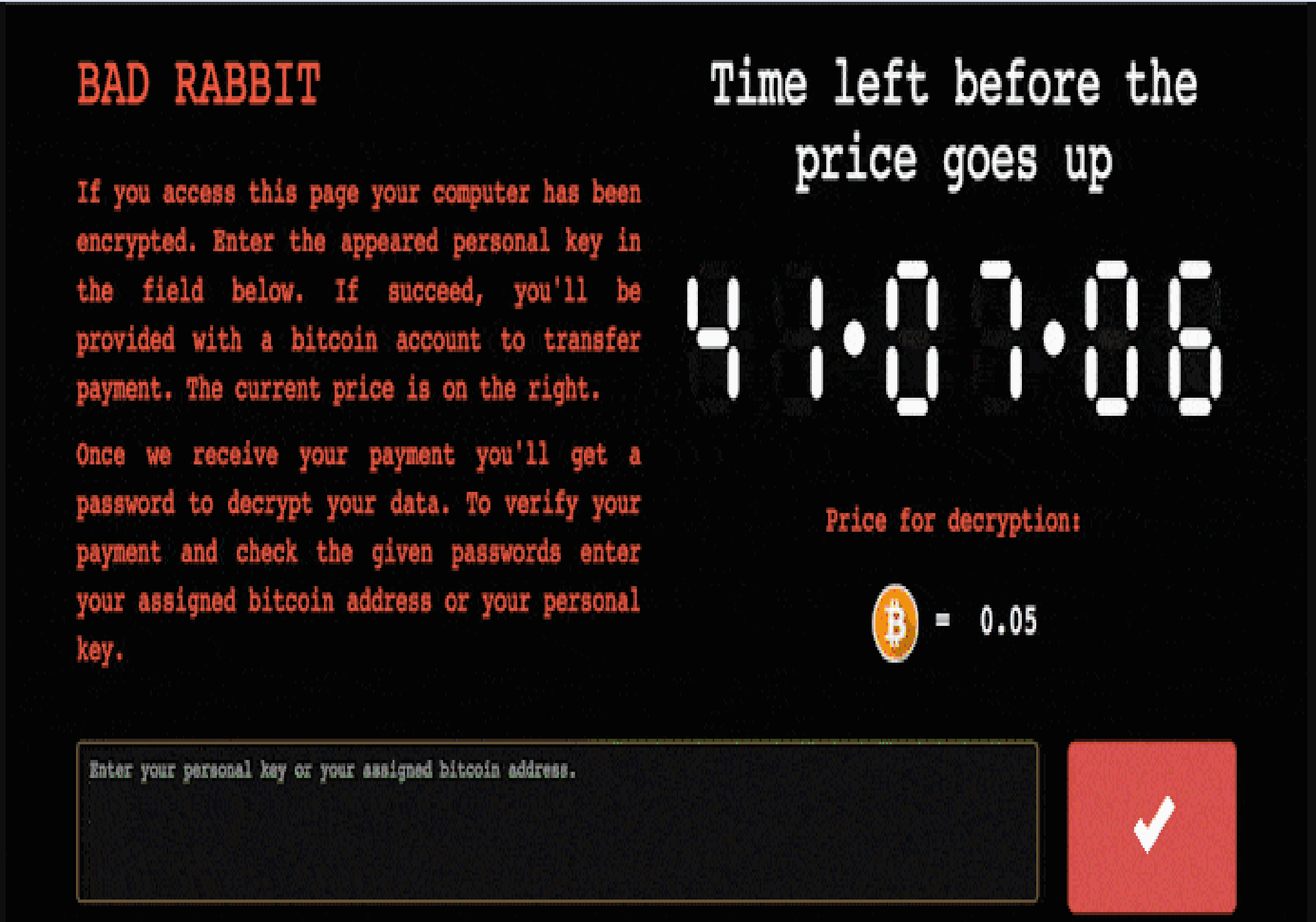
12.3%

Globally, 12.3 percent of enterprise detections were ransomware, compared to only 1.8 percent on the consumer side.

Malwarebytes

Ransomware: More Devastating & Widespread

Ransomware: More Devastating & Widespread



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

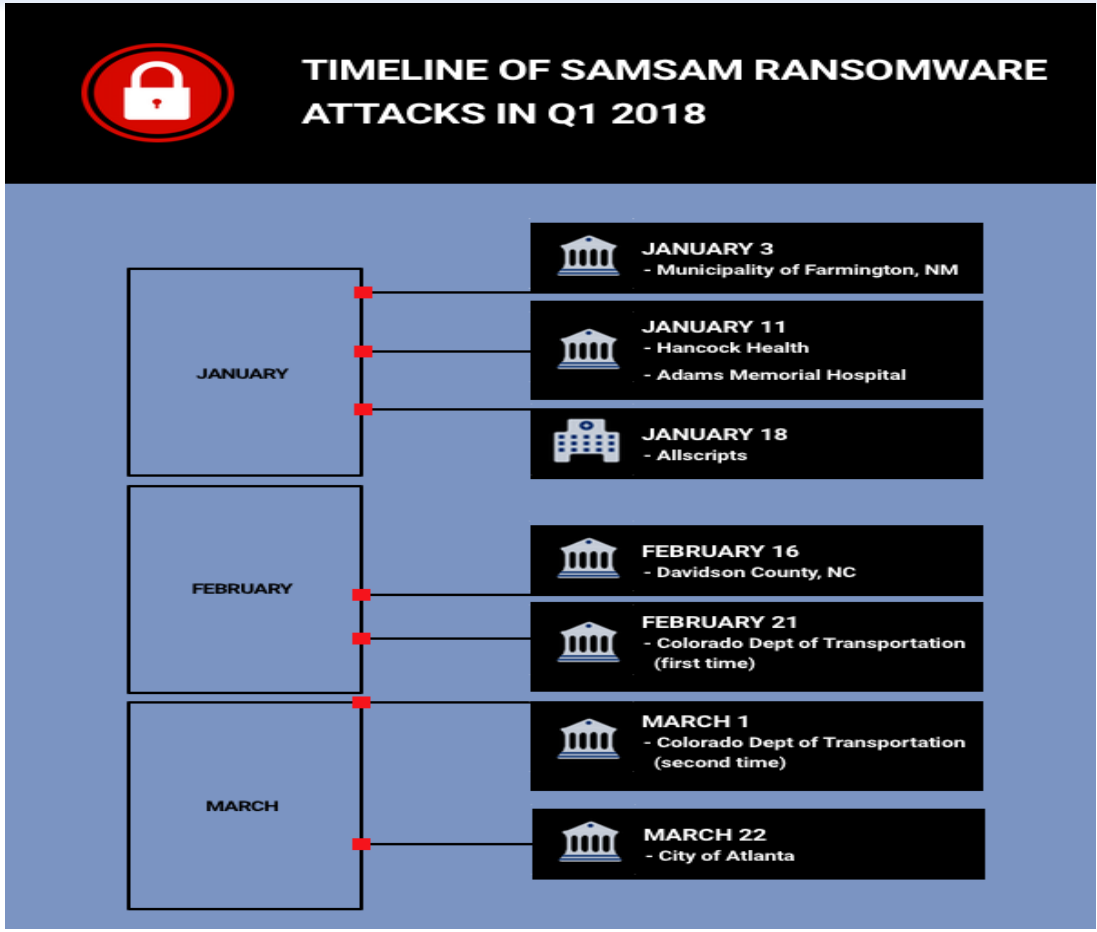
SamSam Ransomware has infecting :

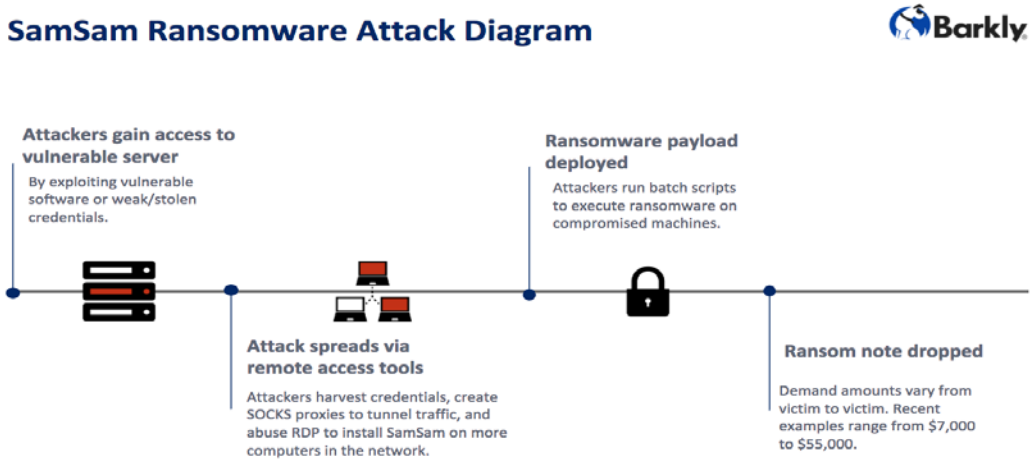
- City of Atlanta
- Davidson County in North Carolina
- US Hospital (Hancock Health)
- The Colorado Department of Transportation (CDOT) not once but twice in February

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 well-versed in evading antivirus, and may infect victims multiple times
5. SamSam can be stopped

Today's advanced attacks routinely bypass antivirus. 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.





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

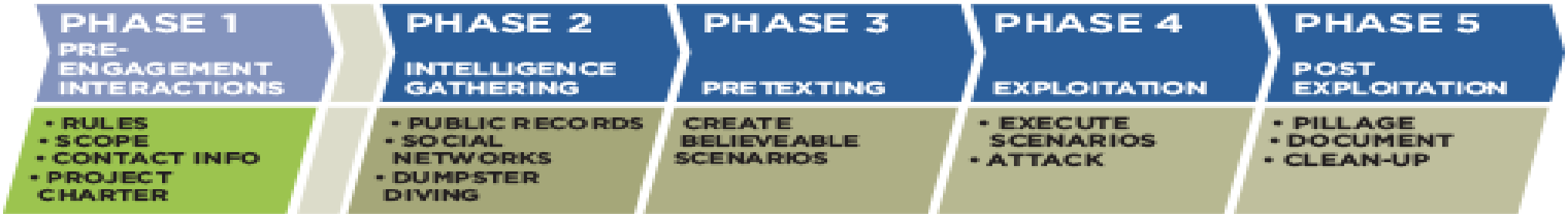
- All three are critical threats to the public sector
  - **Extortion**: Freeze the ability to provide public services (safety, health & welfare, commerce)
  - **Theft**: Cash and information
  - **Exploitation**: Override protections or alter political outcomes
- Public Consequences
  - Loss of services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

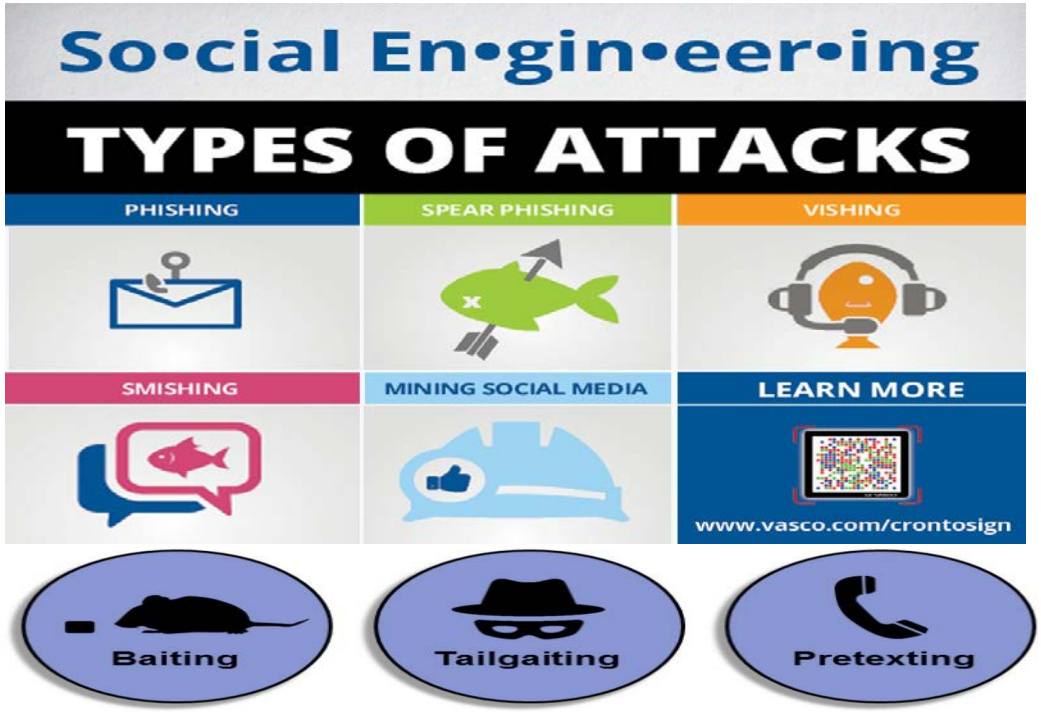
Why is Public Sector a Target?

- 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)

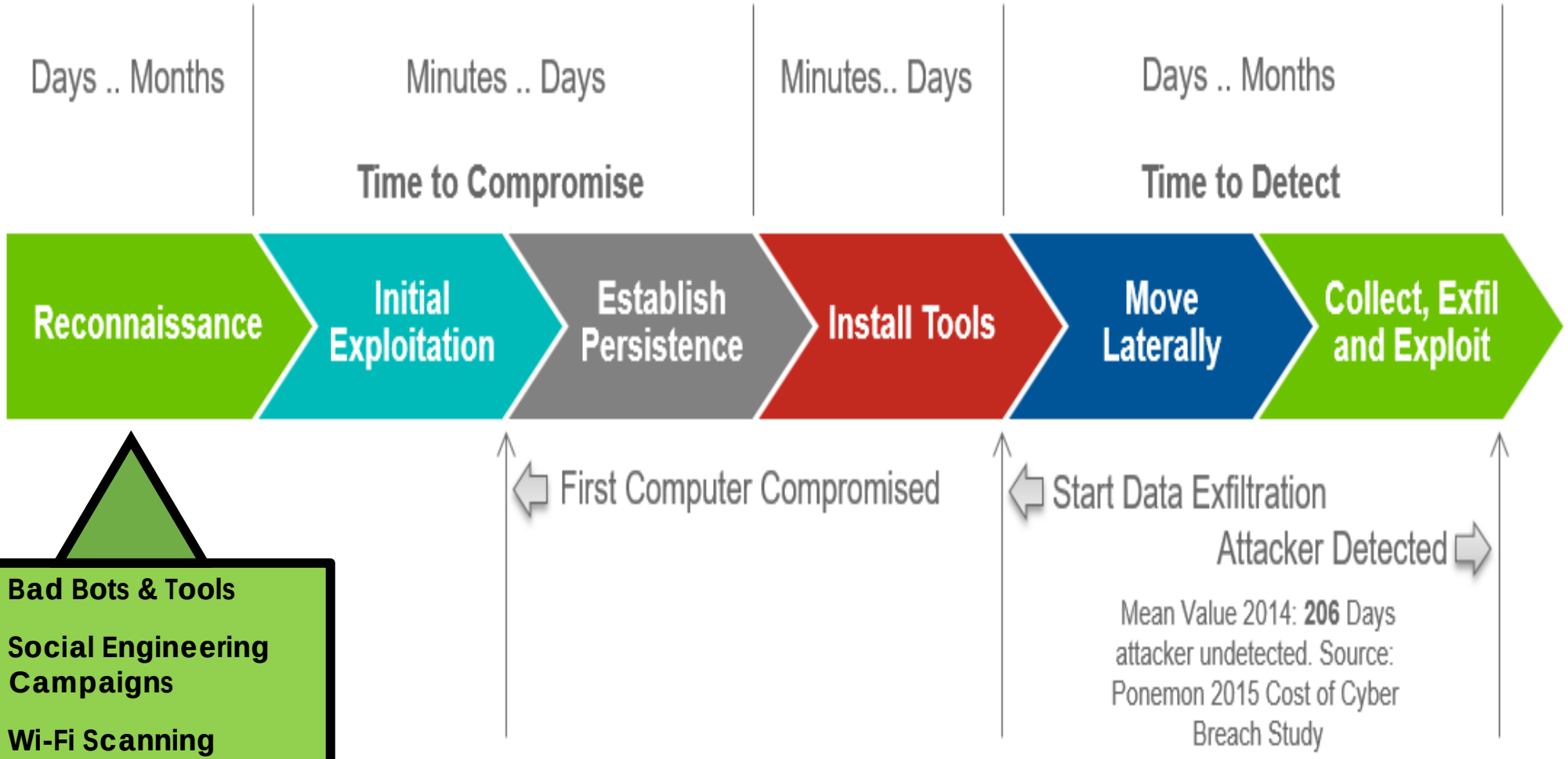




75%+

of all network intrusions are due to compromised user credentials

Phases of a Cyber Attack



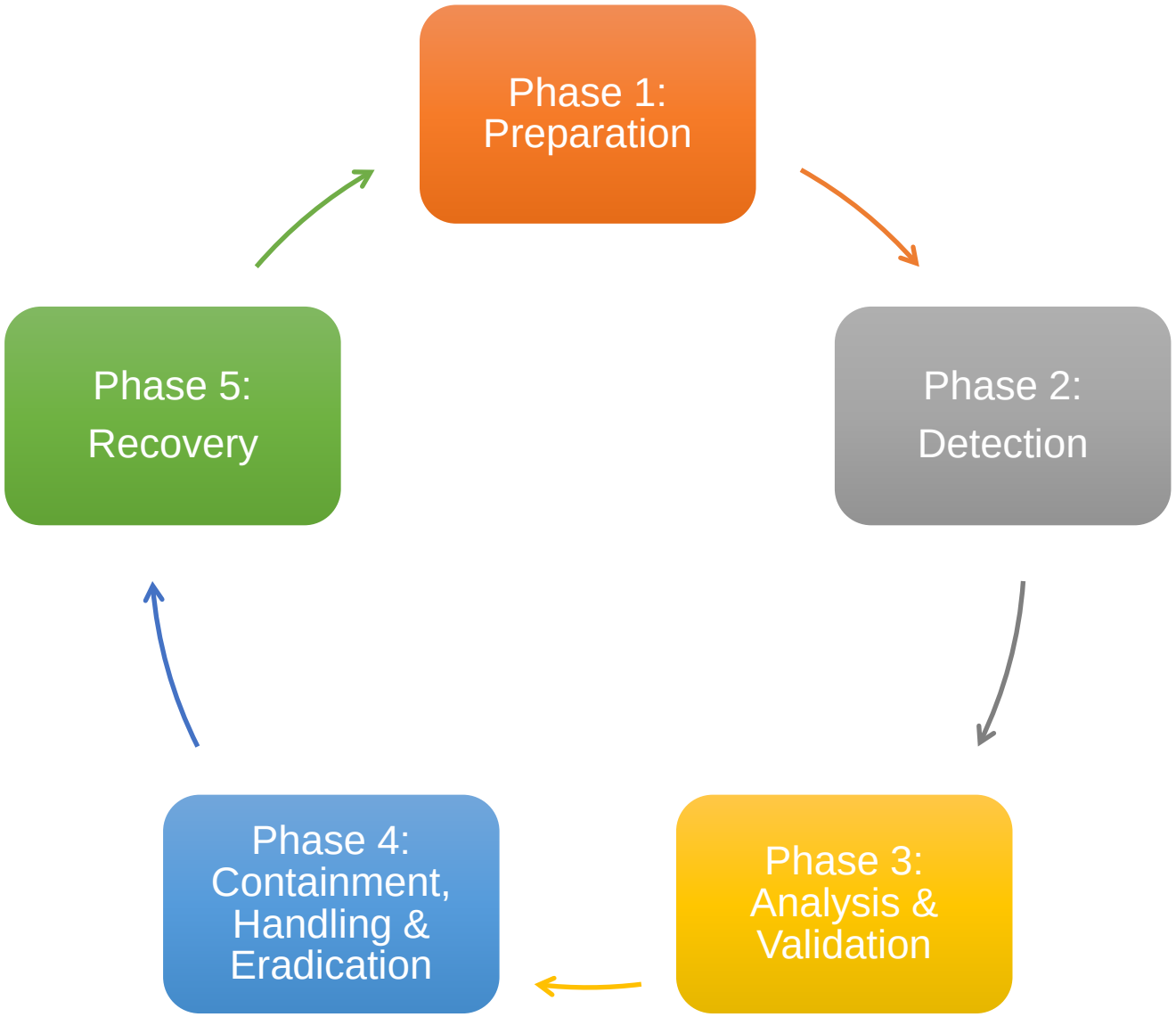
Mecklenburg County

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

Phase 1: Preparation



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

Phase 1: Preparation

Phase 2: Detection

What preparation did we have?

When did we know this was happening?

What did we do to contain the damage?

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:

<u>Mecklenburg County would not pay</u>

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**

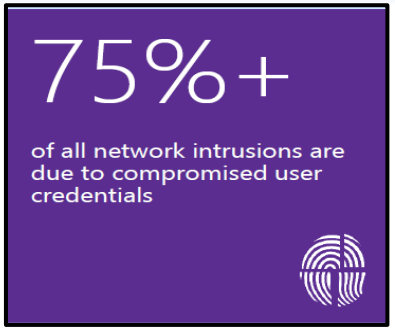
- **Reset all system accounts and passwords**
- **Tightened 'In-bound' and 'Outbound' Firewall rules**
- **Executed Restoration Procedures**
- **All: communication**

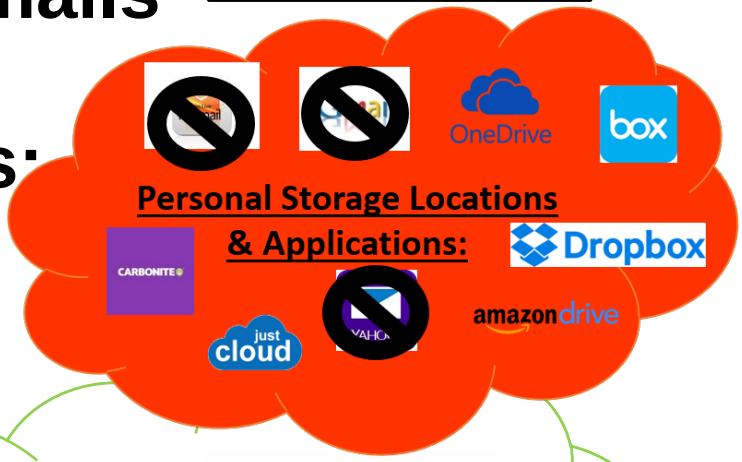
https://www.mecknc.gov/news/Pages/Countywide-system-outage.aspx

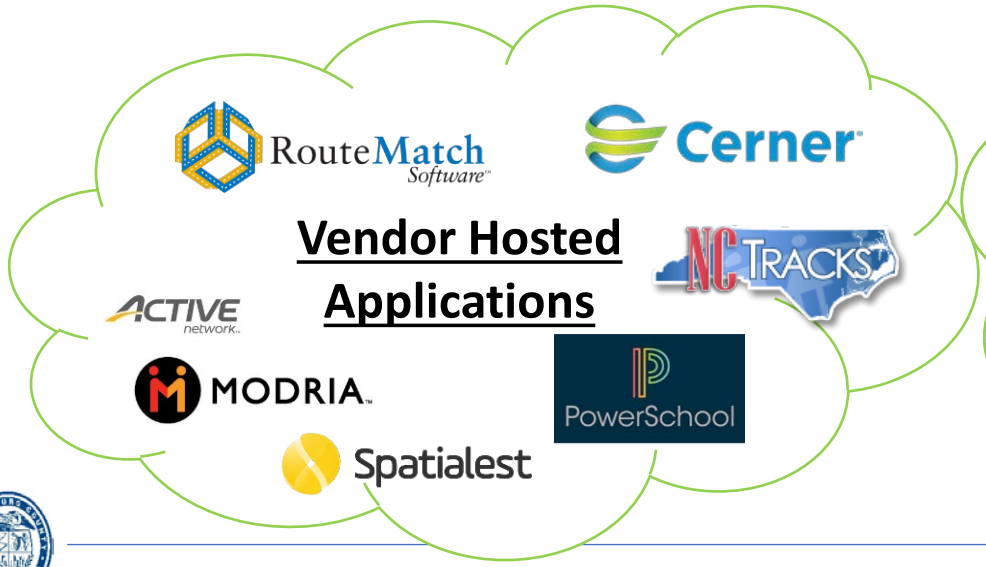
Identified "New Normal" Security Practices

Phase 5: Recovery

- **Implemented extended password length**
- **Significantly restrict international emails**
- **Policy & Perimeter Security changes:**
  - **External email alerting**
  - **Non-County web-based email elimination**
  - **Eliminate email auto-forwarding**







CHANGE: "New Normal" Security Practices

Phase 5: Recovery

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

Organizational	Define and communicate vision and strategy	Build commitment to vision and strategy	Ensure reward and recognition structure aligns with intended results
Team	Translate strategic goals to team responsibilities	Address impact of the changes to work and the team	Build High Performing Teams
Individual	Address "me" issues	Clarify roles and responsibilities	Reward and reinforce desired behaviors and values

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.

Mecklenburg County Hack Attack

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**
- **We were Lucky – No Data Loss**

Mecklenburg County Hack Attack

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.**

Mecklenburg County Hack Attack

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

Mecklenburg County Hack Attack

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**

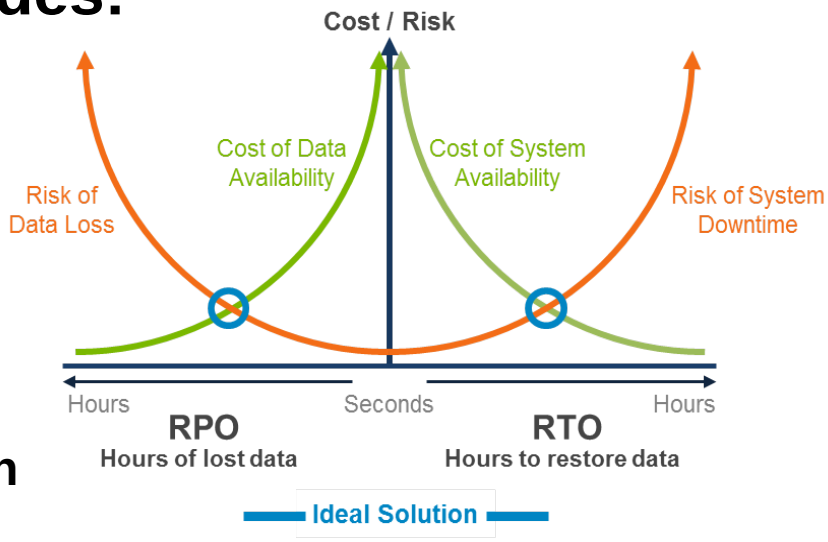
Vendor Management

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 management-level 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**



What Should the Public Sector do?

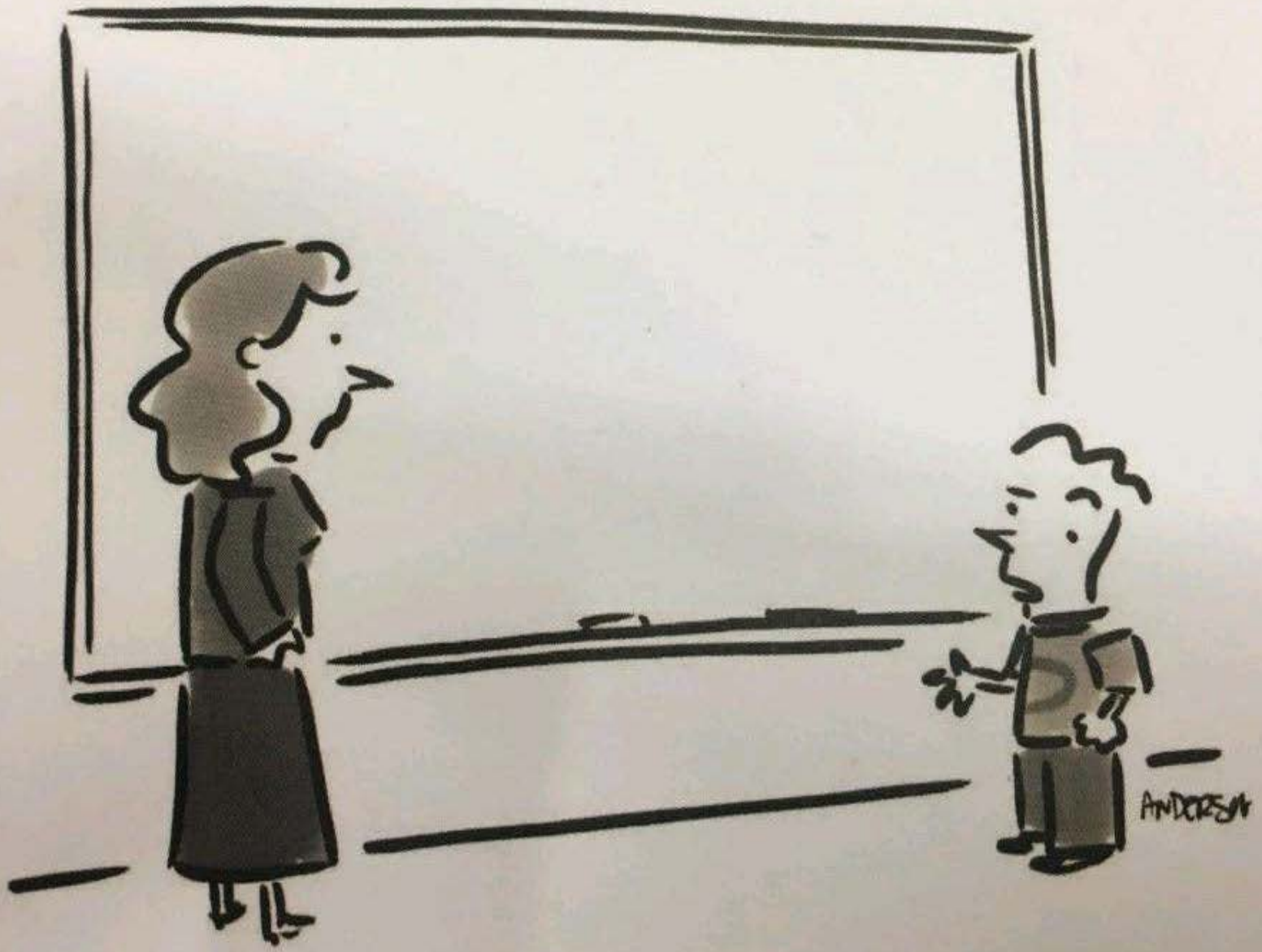
- Have a candid conversation about enterprise risk of Cybercrime with all functions at the table
- Prioritize critical functions (external and internal)
  - Less about IT tools, more about operations and protecting the public
- Update continuity of operations plans
  - How will you operate under no or 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.



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

Thank You!