Not today…Breaches!

Kimberly Rehberg
City Attorney
City of Durham, North Carolina

Marcus E. Ray
Vice President of Sales
GoSecure, Inc.

Blake Pennington
Senior Assistant City Attorney
City of Fayetteville, Arkansas







DATA BREACH

Confidential, private, protected, or sensitive information being exposed to a person not authorized to access it.

https://en.wikipedia.org/wiki/Data_breach

TOP 5 BREACH PATHWAYS - 2024



1. Stolen/Compromised Credential
2. Phishing/Email Compromise/Social Engineering
3. Unknown ‘Zero Day’ Vulnerabilities
4. Malicious Insider
5. KNOWN – Unpatched Vulnerability



FBI Most Wanted = Cyber (122)

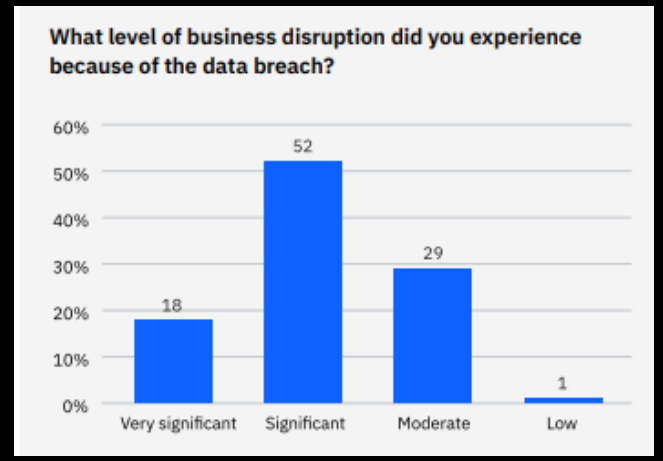
https://www.fbi.gov/wanted/cyber

BREACHES BY THE NUMBERS

- 2024 avg cost of breach - $4.8 Million (US = $9.3M)
- Government/Municipality in Top 10 industries attacked
- 3.4 billion daily spam emails
- Time to Recover from Breach – 152 Days
- Time to Identify and Contain a Breach – 258 Days
- Organizations with Significant/Very Significant disruption after a breach – 70%

Top 5 countries and regions 2024 vs 2023

#	Cost change	2024	2023
1	↓	**United States** $9.36	**United States** $9.48



https://table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf

COMMON LANGUAGE

Phishing

GOAL = Get someone to click, open, or download an attachment infected with malicious software (“malware”)

- Smishing - text
- Vishing – voice

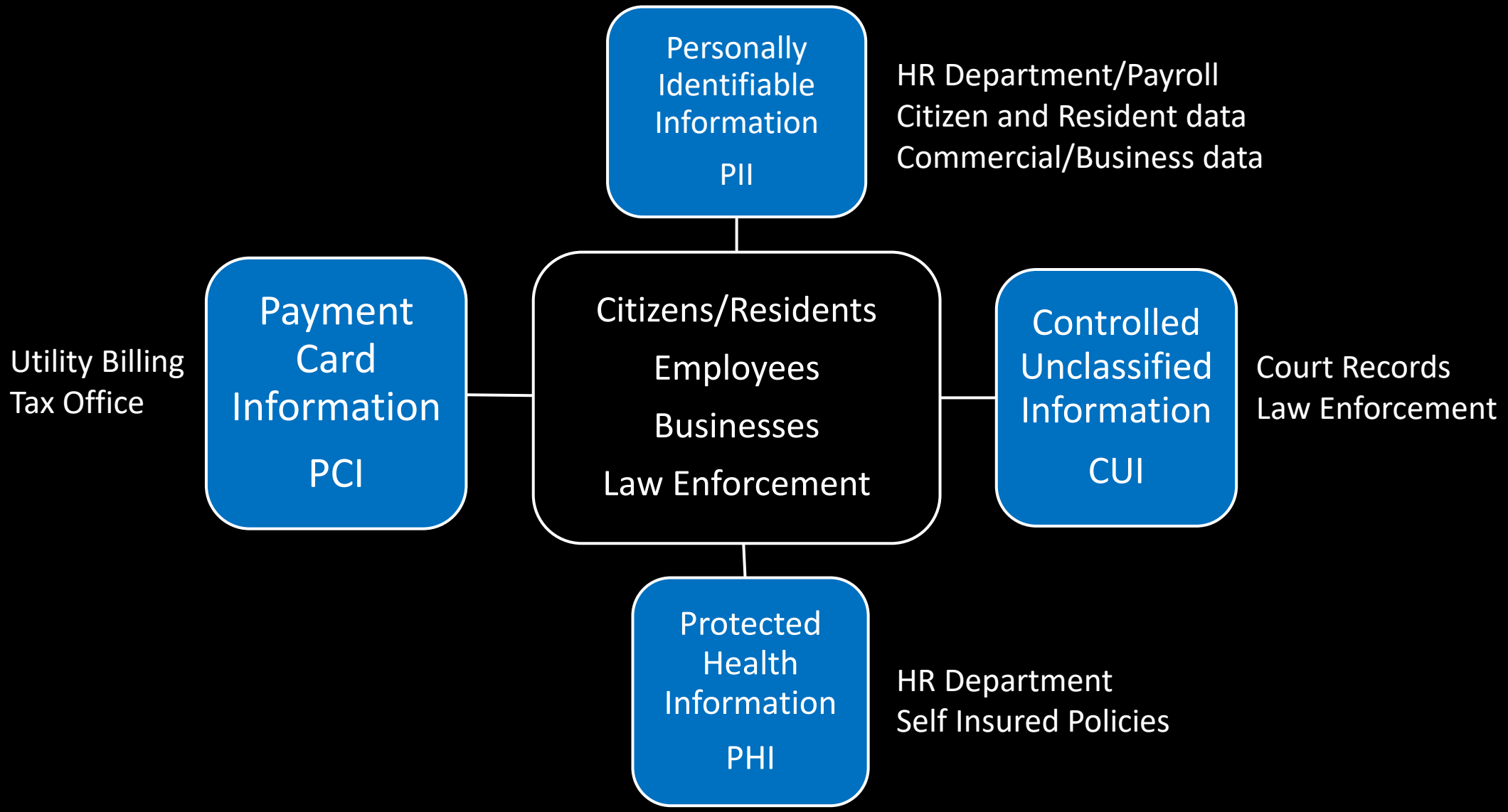
Spoofing

GOAL = Gain personal or business information

Ransomware

GOAL = Hold computer system or files hostage until the victim pays money

SENSITIVE DATA TYPES



DURHAM'S CYBER ATTACK

Day 1 Timeline

- 10:00 pm—Attack commenced
- 10:06 pm—Monitoring service notes "suspicious activity"
- 10:42 pm—Network switch cut

Aftermath

- Day 1—75% of City's IT assets locked down through encryption
- Day 2—War room established in early morning hours
- Day 4—City phone system restored and back online; City insurer notified of attack
- Day 10—Full recovery and re-networking of all IT assets

DURHAM'S CYBER ATTACK

What We Did Well

- Moved quickly
- Great backup strategy
- Prioritized backup investments
- Cyber insurance
- Communicated effectively with the workforce

Lessons Learned

- Simple anti-virus software is not enough; EDR software is critically important
- Get next generation firewalls installed ASAP
- Train . . Train . . . Train
- Systems admins need 2 accounts

FAYETTEVILLE'S CYBER ATTACK

Day 1 Timeline

- 4:30 am – Attack commenced
- 7:00 am – All systems off
- 8:30 am – Insurance company contacted
- 1:00 pm – Internal leadership convened

Aftermath

- Day 2 – Began using some systems
- Day 3 – Shut down all systems again
- Day 8 – Police and Fire systems restored
- Day 18 – Functionally restored city-wide

FAYETTEVILLE'S CYBER ATTACK

What We Did Well

- Great backup strategy
- Cyber insurance
- Supportive leadership
- Leveraged relationships with other government entities
- Cloud-based applications

Learning Opportunities

- Communications strategy
- Planning for loss of technology
- Premature systems restart

THE POWER OF COMMUNICATION

What can you do before a Breach?

1. **Develop your communications and reporting strategy - ‘you do not have luxury to be silent’**
2. **Increase encryption level & have immutable backups (backups = cannot be altered/changed)**
3. **Conduct a Breach Readiness Assessment**
4. **Develop an Incident Response Plan**
5. **Identify parties you will need to contact**
6. **Secure an Incident Response Retainer –** under contract w/lower hourly rate than active incident rate and can start immediately

Actions to take during a Breach

Secure your operations

- Disconnect from Internet, do not wipe drives/destroy evidence
- Assemble the team (War Room) and put on the coffee
- Work the Incident Response Plan

Fix Vulnerabilities

- Segmentation/Forensics/Patching

Notify Appropriate Parties - Communicate

- Legal Requirements – State & Federal (Local FBI/U.S. Secret Service)
- Local Law Enforcement
- Affected businesses/individuals
- Public – Share what you can while protecting criminal investigation (regular cadence)

Actions to take after a Breach

Harden systems

- Vulnerability Scanning/Patching
- Managed Endpoint Detection & Response (EDR) in place
- Penetration Test Environment (Internal/External/Applications)

Communication

- Public -Designated person to release information (PR)
- Private - Letters of Notification to affected parties
- Federal - (FTC) - www.IdentifyTheft.gov

Security Awareness Training/Tools

- Structured Training with Random PHISH campaigns

THANK YOU!

Kimberly Rehberg kimberly.rehberg@durhamnc.gov Marcus Ray mray@gosecure.net Blake Pennington bpennington@fayetteville-ar.gov

APPENDIX

The First 24 Hours

Chaos

- Know your Incident Response Plan
- Triage (unplug—do not wipe)
- Forensics
- Communication
- Restoration
- Staffing plan

The First 24 Hours

Triage

- Call your cyber insurance
- Build your teams, it is a marathon
- Legal
- Forensics
- Build relationships with vendors now, you will need them

The First 24 Hours

Forensics

- Unplug do not wipe drive
- Takes time to research, identify expert (IRR) for forensics
- Logging, you need to make sure you are logging appropriate systems and have logs offloaded, stored in cloud, something to protect logs
- May not solve the question on what happened, but it will confirm you are following cyber policies and SOP’s

The First 24 Hours

First Responder

- Can you function without connectivity
- Perform tabletop exercises in preparation for a cyber event
- Exercise allows you to sort strengths/weaknesses and identify point person for event
- NIMS/ICS training can help

The First 24 Hours

Communication and Reporting

Internal

- Have all staff's mobile numbers
- Establish a sit-rep cadence (every morning/evening)

External

- IRP - Develop simple scripts in your so you do not have to come up with text in the middle of an incident
- Identify who is going to communicate with public (do Media Training!)
- FBI and other agencies – Regulatory requirement

IT Department = Have a plan

Restoration

- Prioritize/tier plan for restoration
- Backups/Snapshots
- Immutable backups!
- 24x7, you need a staffing plan or a relationship with a vendor that can help you bring systems back online

IT Department = Have a plan

Build Relationships

- Meet your local FBI cyber agent
- Did you know the FBI has a very good recovery rate on accounts payable fraud if they are notified within 24 hours?
- Build an internal culture where people talk about cyber and openly report issues (cyber training helps this!)
- Have contact information for your leadership team
- Develop relationships with other agency professionals, like we are doing today!
- Build your “bench”! This gives you a resource to call when you see something strange, or need to brainstorm on a policy

IT Department = Have a plan

Basics

- MFA
- Expanding to SAS and desktops
- Managed Detection AND Response Solution in Plan (big ticket) Vulnerability Identification and Management Practices
- Printed Copy of Incident Response Plan (IT, Mayor's office, Situational Room)
- Practice it, tabletop IRP plans
- Updated SOP/Policies to support cyber
- Understand how to file a claim

IT Department = Have a plan

Basics 2.0

- Have an Incident Response Team/technology vendor selected before you need it
- Can you process payroll manually if needed? How are hours captured/hosted?
- Patch Management!
- Desktop images, keep them updated, PC/laptop drivers.