



# DATA SECURITY: YOUR NUMBER ONE PRIORITY





---

Presented by

**Daniel M. Andrea, CPA, CITP, CISA**

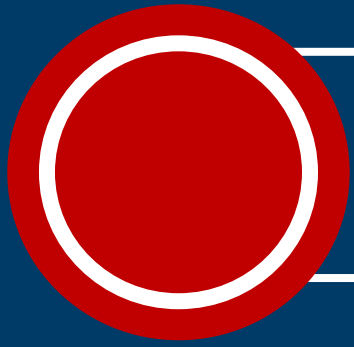
Dan has over 30 years of experience in public accounting and specializes in the performance of forensic accounting and litigation support procedures, SOC examinations, internal accounting controls assessments and information technology consulting services.





# DATA SECURITY: YOUR NUMBER ONE PRIORITY





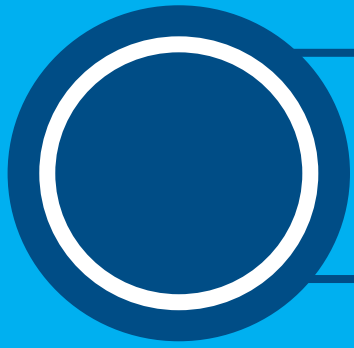
## AGENDA

- Cyber Security vs. Data Security
- Regulations, Regulations, Regulations
- Data Security implementation program
- My data is breached – now what?



# CYBER SECURITY VS DATA SECURITY



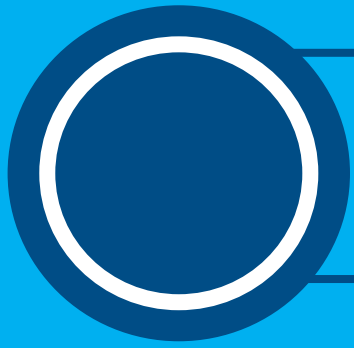


## CYBER SECURITY VS. DATA SECURITY

# CYBER SECURITY



The ability to protect or defend the use of cyberspace from cyber attacks

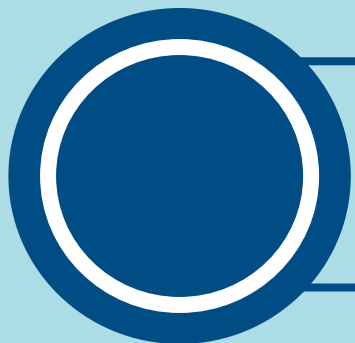


## CYBER SECURITY VS. DATA SECURITY

# DATA SECURITY

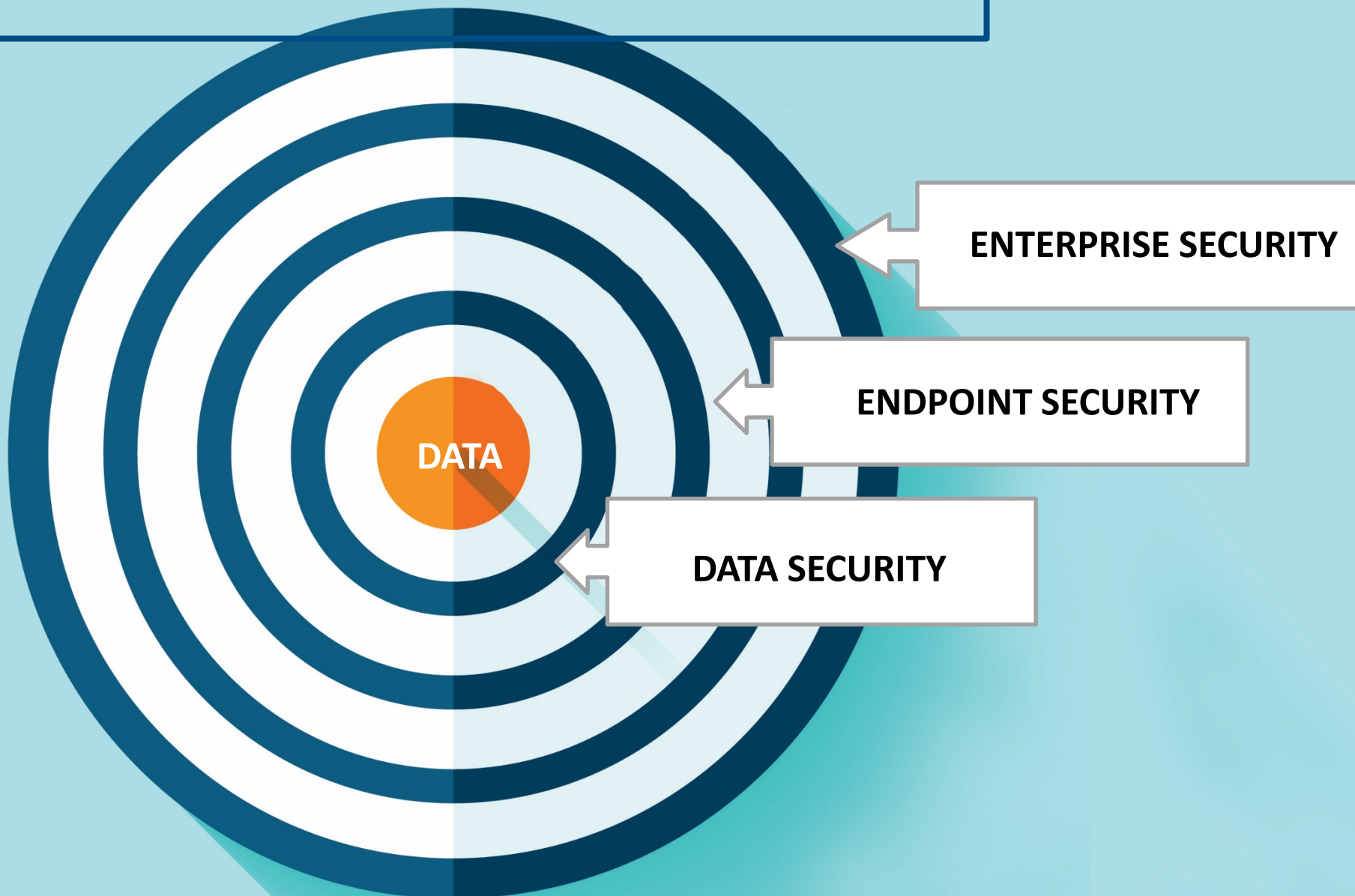
The **protection** of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide security, confidentiality, integrity, and availability









# CYBER SECURITY VS. DATA SECURITY

Data  
Security  
Model





# CYBER SECURITY VS. DATA SECURITY

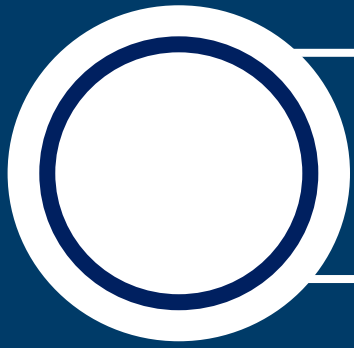
-  Not all Cyber security attacks impact data (for example: DoS Attacks)
-  Data security “attacks” can be inside or outside the organization
-  Data Security “attacks” are much harder to prevent
-  Assess Data Security from the Inside to the Outside versus from the Outside to the Inside



**REGULATIONS,  
REGULATIONS,  
REGULATIONS**







# REGULATIONS, REGULATIONS, REGULATIONS

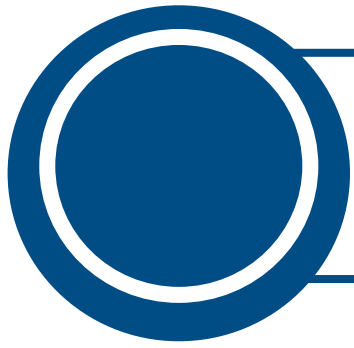
- Focused on personal information (“PI”) or protected health information
- Federal Level
- State Level
- International Level
- Governance responsibilities



# DATA SECURITY IMPLEMENTATION PROGRAM



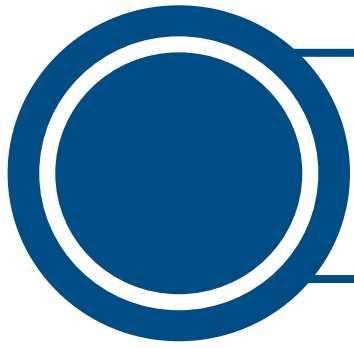




# DATA SECURITY: IMPLEMENTATION PROGRAM

## OVERVIEW

1. Develop a Data Classification Model/Policy
2. Data Inventory and Data Mapping Process Flows
3. Risk Assessment
4. Physical, Logical Access and Process Controls
5. Monitoring



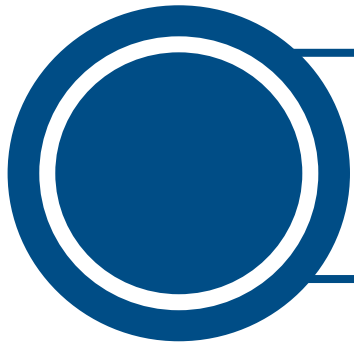
## DATA SECURITY: IMPLEMENTATION PROGRAM

1

# Develop a Data Classification Model/Policy

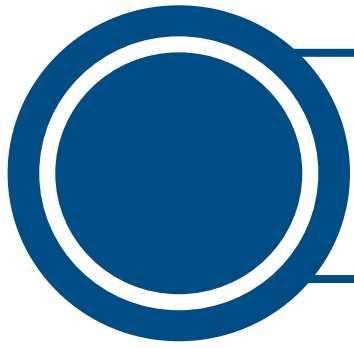
- Data Classification is the classification of data based upon its level of sensitivity and the impact to an organization should the data be disclosed, altered or destroyed without authorization
- Drives your data security efforts since it provides a quantifiable method for allocation of resources
- Data should be classified based upon your organization's needs – there is not necessarily one hard and fast categorization model





# Data Classification Model/Policy:

- Restricted Data
- Private Data
- Public Data



## DATA SECURITY: IMPLEMENTATION PROGRAM

2

# Data Inventory and Data Mapping Process Flows

- Document the process flow for each piece of data identified in the data classification
- This should lead you to every location that the data is held (if done correctly)





# DATA SECURITY: IMPLEMENTATION PROGRAM

## DATA MAPPING PROCESS FLOW EXAMPLE

### Sample Data Mapping Record (Impact Assessment)

#### Overview

Process Review	Volume of Data	Type of Data	Description of Processing	New/Existing Data?	Security	Who can access?	Information Owner	Observations	Actions	Compliant?
Payroll – core	114 per month	Hardcopy data for new starters (P45/46 etc.), Hardcopy data for commissions. Electronic data for core tasks, emailed pay slips.	Monthly processing of payroll information for staff including commissions, SSP, SMP, leaver and holiday pay. New starters/leavers processed as required	Both (if new starters)	Core Sage payroll data files encrypted. Pay slips password protected. Data directory restricted access. Finance only given sufficient data to do management accounts.	Operations Director, MD only through core Sage applications. MD, OD & head of tech ops for network file location.	Operations Director	Linking Sage payroll to NAV would reduce finance need to see data to do management accounts.	Investigate Payroll – NAV link	Compliant

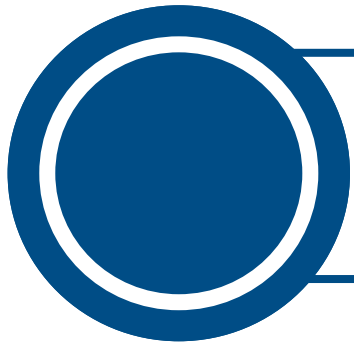


# DATA SECURITY: IMPLEMENTATION PROGRAM

## DATA MAPPING PROCESS FLOW EXAMPLE

Data Flow								
Who are the data subjects?	How do you get it?	Where does it go through your organization?	How is it stored?	Does it leave your organization?	Does it leave borders?	Observations	Actions	Compliant?
Staff	Data provided by staff on joining via HR platform and P45/P46	Manually keyed from subject provided data into Sage Payroll, stored on Group drive (encrypted and restricted). Pay slips sent as password protected emails. Reports stored on network, relevant data keyed into online banking for payment. Relevant data keyed into Pension online portal for payment. Relevant data passed to finance team for management accounting. Relevant data passed via Sage to HMRC for FPS submissions. Selected data given to HM Gov for annual earnings survey	Manual data held in locked HR cabinet. Electronic data in restricted/encrypted network location. Restriction persisted into on and offsite backups.	Partial data is sent to HMRC for reporting purposes (FPS/year end etc.). Partial data is sent to Pension provider (name, address, NINO, contribution). Partial data is sent to SAYE provider (name, address, NINO, contribution). Sample data observed by auditors but in-house.	No	It is assumed that staff have “joined the dots” in some cases where data is sent to other processors (e.g. via SAYE) this should perhaps be more clear	Improve visibility of the data flow to the data subjects but documenting where it may be sent and what data is sent.	Investigate





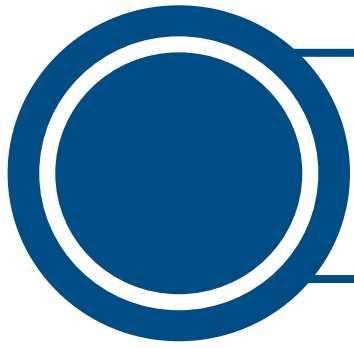
## DATA SECURITY: IMPLEMENTATION PROGRAM

### 3

## Risk Assessment

- Driven off of Data Mapping and Classification
- Risk Assessment
- Implement measures to eliminate/mitigate risks
- Implement measures to detect potential incidents



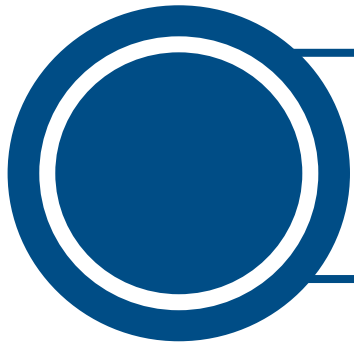


# 4

## Physical, Logical Access and Process Controls

- Develop based upon Risk Assessment and Data Classifications
- Restricted data should get most focus
- Cost/benefit of each control



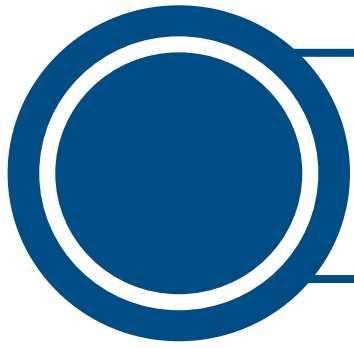


# DATA SECURITY: IMPLEMENTATION PROGRAM



## Physical Controls

1. Secured Data Centers or Server Area
2. Secured desktops and laptops – encryption
3. Clean Desk Policy
4. Locked desks/cabinets
5. Shredding Bins (NOT recycling bins!)
6. Access to sensitive areas restricted by card readers or other devices
7. Video Cameras
8. Prohibition against unescorted visitor access
9. Limit removable devices
10. Printer controls (queues)

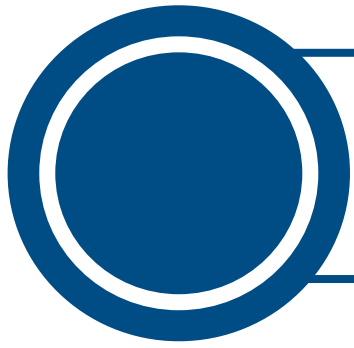


# DATA SECURITY: IMPLEMENTATION PROGRAM

**B**

## **Logical Access Controls**

1. Controls at the perimeter (firewalls, IDS/IPS etc.)
2. Network Segmentation
3. Encryption at Rest, In Use or in Transit
4. Passwords/Passphrases related controls
5. Multi-Factor Authentication
6. Access based on the Principle of Least Privilege
7. De-identification of data
8. Email encryption
9. Secured portals for data sharing
10. Security Training

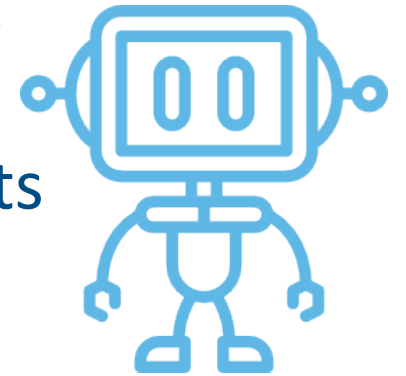


# DATA SECURITY: IMPLEMENTATION PROGRAM

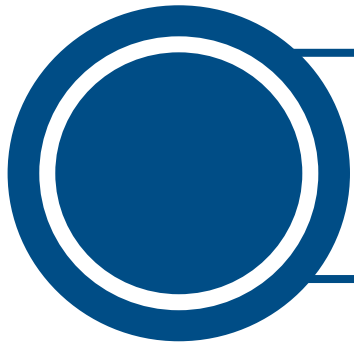


## Process Controls

1. Data Access Requests
2. Data Retention Policy
3. Data Destruction Policy
4. Application Development process controls
5. Change in Access Requests





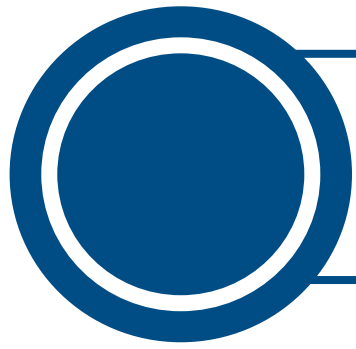


## DATA SECURITY: IMPLEMENTATION PROGRAM

### 5

## Monitoring

- Continuous – need to monitor internally and externally
- Assess modifications due to changes in business operations or requirements, regulations, environment, etc.
- Exceptions/Events should be dealt with in accordance with your Incident Response Plan (discussed in a little while)



## DATA SECURITY: IMPLEMENTATION PROGRAM

# Monitoring Controls

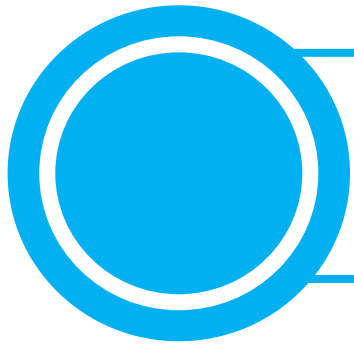
1. FAM (File Access Monitor) utilities
2. DLP (Data Loss Prevention) utilities
3. Social Engineering Testing
4. 3<sup>rd</sup> Party  
Examinations/Assessments
5. Vendor Management Program
6. Account Privilege/Access Reviews
7. Penetration testing
8. SIEM (Security Information and  
Event Management) tools
9. ISAC (Information Sharing and  
Awareness Centers) monitoring



**MY DATA IS  
BREACHED:  
NOW WHAT ?**



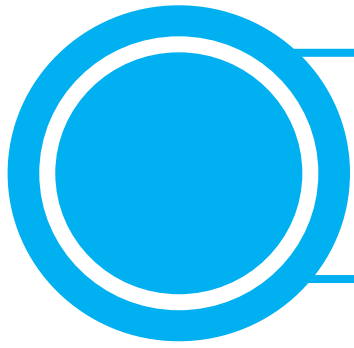




## MY DATA IS BREACHED: NOW WHAT ?

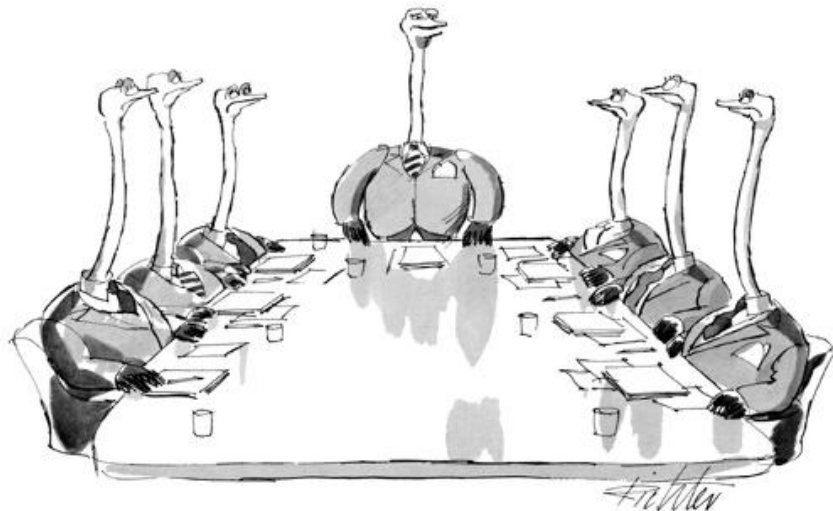
**Do you ?**

1. Have an Incident Response Team and Plan?
2. Have data backups that are tested?
3. Know the magnitude (HINT: data mapping and inventory )?
4. Insurance to cover the breach?
5. Disaster Recovery Plan?



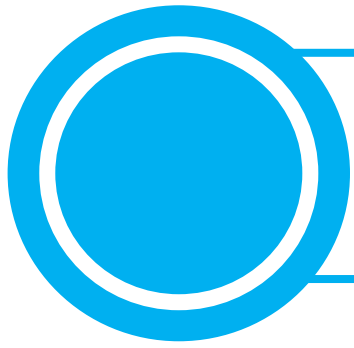
# MY DATA IS BREACHED: NOW WHAT ?

Or do you....



*"The motion has been made and seconded that we stick our heads in the sand."*



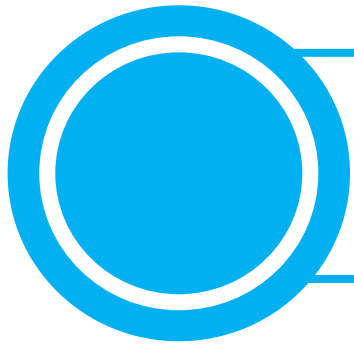


## MY DATA IS BREACHED: NOW WHAT?

### **Build Your Incident Response Plan**

- Build an Incident Response Team
- Comprised of All Key Stakeholders (internal/external)
- Define Incident Scenarios
- Scenarios should be linked to Data Classification
- Build an Incident Response Plan (“IRP”)
- Test the IRP

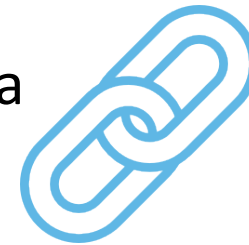




# MY DATA IS BREACHED: NOW WHAT?

## Test The IRP

- Should be done at least annually
- Build realistic scenarios based upon Data Classification
- Conduct test
- Conduct Post-Mortem (“lessons learned”)
- Modify IRP and Risk Assessment as appropriate
- Know the laws at the federal, state and local jurisdiction relevant to you
- Consider cyber insurance



## KEY TAKEAWAYS



Data Security  $\neq$  Cyber Security



Data Classification will help you focus on what is most important



Data Mapping and Inventory will help you understand the magnitude of your security needs



Physical, Logical Access AND Process Controls are critical



If you don't have an IRP – GET ONE NOW !

# Let's Connect



dandrea@KahnLitwin.com



888-KLR-8557

[KahnLitwin.com](http://KahnLitwin.com)

