



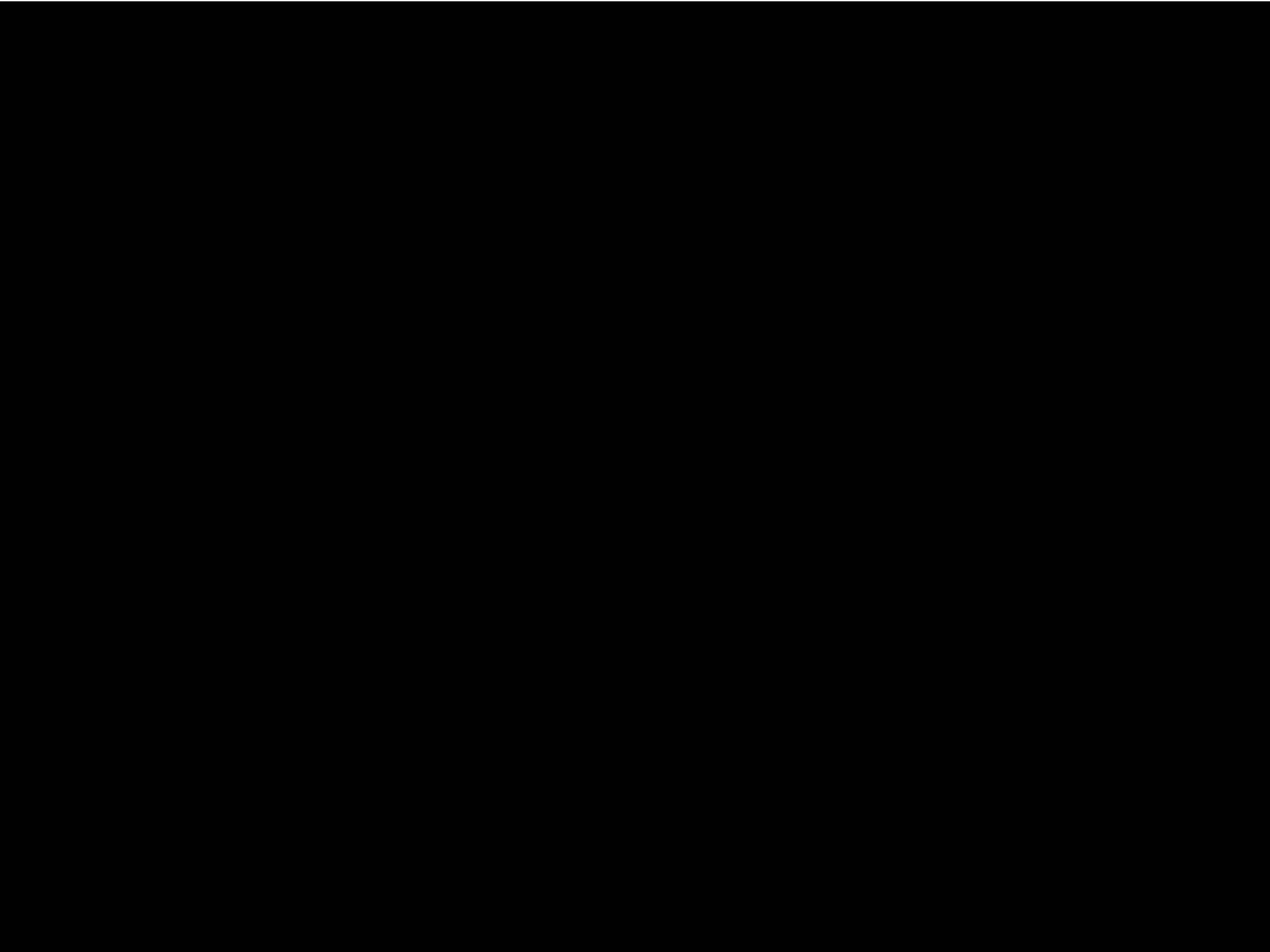
**Are You
Asking Your
IT Department
the Right Cyber
Security Questions?**



**Mr. Tom Cranmer, Chief Technology Officer
Richland School District Two**

**Mr. James Manning, Board Member
Richland School District Two Board of Trustees**

**Mr. Greg Meetze, Director of Information Technology
State Law Enforcement Division**





In today's evolving digital landscape,

Are you asking the right **cybersecurity questions?**

What **obligations** and **responsibilities** do public school districts have in protecting information?



FERPA - The Family Educational Rights and Privacy Act affords parents the right to have access to their children's education records, the right to seek to have the records amended, and the right to have **some control over the disclosure of personally identifiable information (PII)** **Violations can include the withholding of federal funds.**

COPPA - Children's Online Privacy and Protection Act is a law governing how websites, apps, and other online operators collect data and personal information from children under the age of 13. **Operators must provide notice and get parental consent before collecting information from children.** **Violations can include fines imposed by the FTC.**

HIPAA - Health Insurance Portability and Accountability Act designed to **protect personal information** and data collected and stored in medical records. **Violations can include federal fines.**

South Carolina Data Breach Notification Laws - Section 1-11-490

An agency of this state shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of this State whose unencrypted and unredacted personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person

What **obligations** and **responsibilities** do public school districts have in protecting information?

What **Sensitive Personal Data** does your district have? Districts need to know what they have, and why they need to protect it.

Employee Data:

- Social Security Numbers
- Bank Account numbers
- Health and Benefit information
- Credit Card Numbers (PCI?)
- Resumes
- Payroll History Records - W2's
- Background Check Data
- Addresses
- Date of birth
- Dependent personal information



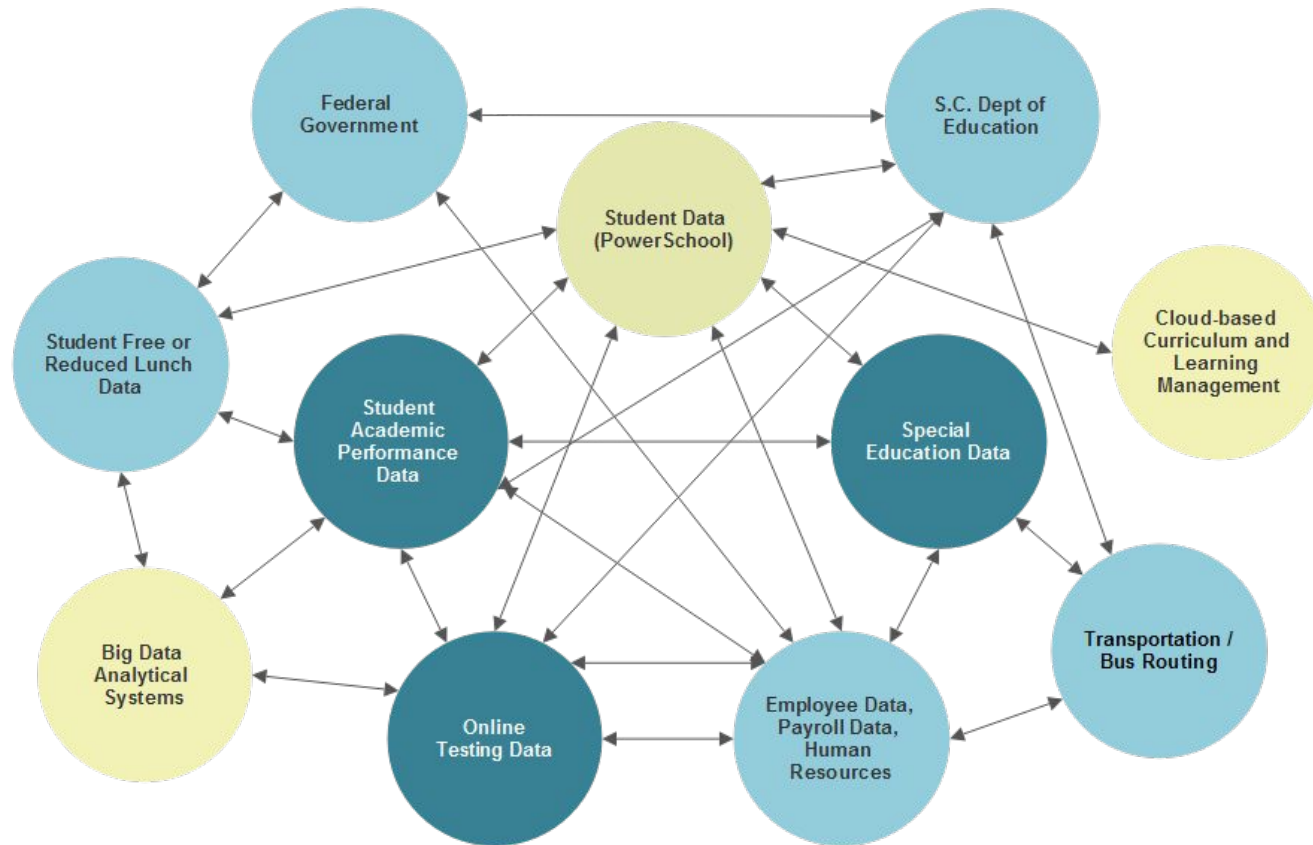
Student Data:

- Academic Data (Transcripts)
- Social Security Numbers
- Special Education Data
- Discipline Records
- Health Records
- Student ID Numbers
- Assessments
- Economic Data
- Student e-mail
- GPA
- Student Photo
- Confidential Correspondence

Parent/Guardian Data:

- Credit Card Numbers (online pay data)
- Economic Data (Free/Reduced data)

Today's **education data ecosystem** is complex, growing, and potentially vulnerable and susceptible to breaches ... *if the right precautions are not taken.*



Example School District Data Center Content

The K-12 Cyber Incident Map - 420 Incidents Since January 2016




**Map last updated: February 11, 2019

Courtesy: The K-12 Cybersecurity Center

Why a rise in education **data breaches**

Data Point: Educational institutions are the third most frequent target of hackers, just after healthcare and financial services.

- The industry chronically **lacks the IT resources** for acceptable defenses.
 - The biggest challenge is implementing robust security protocols while maintaining a **culture of openness**.
 - The industry is based on the free exchange of information.
 - Students and **staff may be unsophisticated about technology** and have limited technical skills.
 - Students with technical skills may attempt **hacking exploits for amusement**.
 - Systems are **highly distributed** across multiple schools in a district.
 - Users frequently have multiple roles within a school system, **complicating identity management**.
 - There's a significant **change in the user population** every year due to students graduating and new students enrolling.
 - **Remote access** is required, with students and parents accessing systems from home computers and smartphones.
- 

What are the **threats** facing school district networks and systems?

Data Breach	<ul style="list-style-type: none">• Incident where information is stolen or taken from a system without the knowledge or authorization of the system's owner.
Denial of Service	<ul style="list-style-type: none">• When a server is deliberately overloaded with access requests such that the website shuts down.
Spoofing and Phishing	<ul style="list-style-type: none">• The use of an email that is forged to appear legitimate and to deceive the user into divulging sensitive info (passwords, bank acct information)
Spear Phishing	<ul style="list-style-type: none">• Targeted form of Phishing by sending an email that appears to be from a colleague or acquaintance, and asking the user to send or divulge sensitive information.
Malware/Scareware	<ul style="list-style-type: none">• Illicit software that damages or disables computers or scares/tricks a user into purchasing unwanted or unneeded software.
Ransomware	<ul style="list-style-type: none">• A form of malware that encrypts user data, then demands payment of a ransom for the user to regain access to their data.
Unpatched or Outdated Software	<ul style="list-style-type: none">• Vulnerabilities occur when unpatched or outdated software has not been updated to include the latest updates.
Removable Media	<ul style="list-style-type: none">• Media devices that can be connected to computers: Flash Drives, CD's, DVD's, and external hard drives, can be stolen or lost.

The **cost** of data breaches

School Districts face **costs** as a result of data breaches.

Detection and escalation: Activities that enable a district to **detect and report the breach** to appropriate personnel within a specified time period. Examples: Forensic and investigative activities, Assessment and audit services, Crisis team management, and Communications.

Post data breach response: Processes set up to **help individuals affected by the breach to communicate with the district**, as well as costs associated with **remedy activities**. Examples: Help desk activities/inbound communications, Credit monitoring and identity protection services, and **Legal expenditures**.

Notification costs: Activities that **enable the district to notify individuals** who had data compromised in the breach (data subjects). Examples: **Emails, letters, outbound telephone calls**, or general notice that personal information was lost or stolen, Communication with regulators; determination of all regulatory requirements, engagement of outside experts

Excerpt Source: IBM/Ponemon Study: Cost of a Data Breach, 2018

Who in the organization is responsible for a **data breach**?

It's Sunday night, and your favorite team just narrowly lost the game. Who is responsible for the loss? Do you blame the field goal kicker who missed the potential winning kick in the closing seconds? Maybe you blame the quarterback, who always seems to accrue too much credit or blame due to the position, regardless of his performance. Maybe the officials? How about the coach who was in charge of the game plan or the general manager who chose the players?

Cybersecurity is a **shared responsibility** across every function and level of an organization.

Accountability starts with the superintendent and the school board.

Cybersecurity is a **practiced culture** within the organization that must start at the top.

If management does not take cybersecurity **seriously**, neither will the front-line employees.

From the former CEO of Equifax after its massive data breach:

"Let me say clearly: As CEO I was ultimately responsible for what happened on my watch. Equifax was entrusted with Americans' private data and we let them down. To each and every person affected by this breach, I am deeply sorry that this occurred. Whether your personal identifying information was compromised, or you have had to deal with the uncertainty of determining whether or not your personal data may have been compromised, I sincerely apologize."

Courtesy: securitymagazine.com

What can be done to **mitigate the risks**?

Begin with the **right questions**.



Key Question

What is our current **Cybersecurity posture**?


Your specific cybersecurity posture will indicate **how healthy or resilient** your district is when it comes to cybersecurity.

How well can your district **defend** itself **against cyberattacks**, breaches, and intrusions?

What is the basic **security status** of our school district's **networks, information, and systems**?

What resources do we have? (e.g., **people, hardware, software, policies**)

What **capabilities are in place** to manage the defense of the district and **to react** as the situation changes?



Key Question

What is our current **Cybersecurity posture**?

Defining your cybersecurity posture is important because it will **guide your entire cybersecurity strategy**, determine your cybersecurity projects, **and influence your cybersecurity spending** throughout the years.

It will help districts **define where they are** in terms of their cybersecurity posture, **what gaps they're currently facing** and what steps they need to take to improve their cybersecurity posture going forward.

Organizations with a **low** cybersecurity maturity level typically have weak cybersecurity defenses, are at high risk and need significant improvement.

Organizations with a **medium** cybersecurity maturity level typically have average cybersecurity defenses, and have taken several steps in securing their mission-critical assets.

Organizations with a **high** cybersecurity maturity level typically have strong cybersecurity defenses and have implemented the necessary strategies, processes and procedures to optimize their cybersecurity posture.

Key Question

What is our current **Risk Level**?

“Other than fully disconnecting from the internet, there is no way to foolproof your school district from a cyberattack.”

- In discussing risk, all key roles should have a seat at the table.
- IT leadership should work with district leadership to **gain a shared understanding** of the importance of defining what the risk truly is.
- Understanding your data: The What, Where, When, Why and Who?
- There are no unaffected parties when it comes to managing cyber risk.



Key Question

What is our current **Risk Level**?

- Risk Appetite: **How much risk can we tolerate?**
- Determining cyber risk **cannot be a point-in-time exercise**. It must become an ongoing process involving constant evaluation and re-evaluation.
- **Practical Levels of Investment:** How much are we willing to invest or spend to manage the risk?
- **What is Reasonable?** A small school district cannot implement comparable security standards to that of a mega retailer, but maintains responsibility nonetheless.
- **Right Sizing and Due Diligence.** Are we using qualitative and quantitative measures to reasonably mitigate risk?



Key Question.

What are our current practices for **data backup and retrieval**?

What is our current **data backup** and **data recovery** plan?

Do we have **offsite copies** of our data?

What is the **geographical disparity** of the copies?

Do we have **cloud-based storage** of our backups?

How often is the data backup up?

How much data would we conceptually lose in a cyber attack?

How much time would we lose, and how rapidly could we restore our mission critical systems and be back up and running?

Is **snapshot data protection** an option?

Is the plan **documented**?

Has the **plan been tested** and **validated**?



Key Question

Do we have a cyber attack / breach **response plan**?

What **procedures will we use** if we experience a cyber attack or data breach?

Who will be **involved and what are the roles** and responsibilities?

What are the established **reporting and notification** protocols? (Who, internally, get's the call?)

How do we **identify the vulnerabilities** that were exploited?

Have you reviewed the **security policies of cloud providers**?

Do we have **written procedures** or policies that govern what actions are taken?

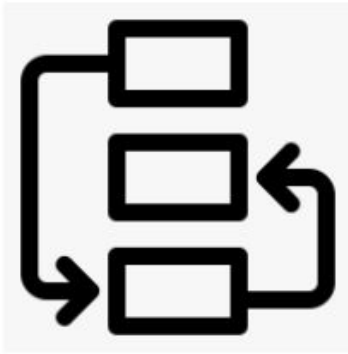
Who will **oversee the recovery steps**?

Have you considered what might happen if a cyber attack occurred during student testing? How would you recover?



Key Question

Do we have a cyber attack / breach **incident response plan**?



Communications.

What procedures should be used for **conducting communications and public relations outreach**?

Understand the severity of the incident.

Determine the scope of what happened before communicating the incident.

Serious breaches may include the notification of law enforcement. Law enforcement forensics can help with determining the scope of damage.

Assemble the communications strategy: Stakeholders, other districts, 3rd party vendors, SC DoE, Cloud providers.

Plan for managing the media.

Begin problem solving and working to remedy the breach.

Key Question

What is our business continuity plan for the **critical assets**?

Acknowledge and plan for disasters beyond Cyber attacks. (e.g. hurricanes, tornados, earthquakes, etc.)

Which **mission critical systems** must be recovered first? (safety & security systems, finance, payroll, student information systems)

What plans are in place to **recover the mission critical systems** and services?

Are there spare **hardware and software resources** on hand to effectively recover critical systems quickly?

What are the roles and responsibilities for executing the recovery plan?



Key Question

Do we have a cyber insurance policy **in place**?

Consider the potential financial losses that can occur from a cyber attack. Protecting the district and the stakeholders during and after a cyber attack is critical.

- **Credit Monitoring** services for affected individuals
- **Legal Liability**
- **Call Volume:** Can you handle the call volume internally? Is there a contingency plan?
- **Costs for notifications**
- Costs for **involving legal guidance?**



What **incidents/losses** does the insurance cover?

How does the **potential for local negligence** affect insurance claims?

Key Question

What **user training** and **awareness** programs are in place?

Acknowledge that user training may one of the best lines of defense for preventing cyber incidents.

The majority of **cyber attacks attempt to exploit the human factor** through Phishing attempts and other efforts.

Malicious hackers and **attackers seek to trick users** into granting them access to a digital resource, long before they will try to hack their way in.

Are your employees savvy enough to spot the risks?



"Ransomware is unique among cybercrime because in order for the attack to be successful, it requires the victim to become a willing accomplice after the fact." – James Scott

Key Question

What **external partnerships** can we establish to help us to be better prepared?

Partner with the experts.

- Consider conducting an External Security Audit
- Conduct tests to measure the vulnerabilities of your school district.
- Security consultants and services available through state contract.
- Obtain references through SCDOE CISO.
- Consider partners with experience in the education vertical, as our line of business and needs differ significantly from other government and private organizations.




Key Question

How can you test your plan?

Tabletop exercises can help **validate the plan**, and/or expose weaknesses to be addressed.

Tabletop exercises are meant to help organizations **consider different risk scenarios** and **prepare** for potential cyber threats.

Tabletop exercises can **test the various protection strategies in place**: Malware attack, Ransomware, Incident Response.



In Summary

Scenario: In a court of law, can you confidently answer the following question:

“What did you do in advance to prevent this type of data breach?”

Do:

Set a goal to build and maintain a culture of Cyber Threat Intelligence: Is there a process in place to proactively understand and manage the threat environment?

Establish Information Security: Are there processes in place to protect, detect, respond and remediate threats?

Promote a Culture of Awareness: Is there an awareness of the importance of security and do all insiders understand their role in maintaining that security?

Design and Practice Incident Response: Is there a documented plan in place as to how to respond to an incident? Is there an adequate and tested disaster recovery process?

Don't

Don't become complacent about cyber security. It's not a matter of “if”, but a matter of “when”.

Don't assume someone else has the responsibility to maintain and protect your data.

Don't wait until you are confronted with an incident to seek advice.



In Summary . . .

Scenario: In a court of law, can you confidently answer the following question:

“What did you do in advance to prevent this type of data breach?”

Do:

Set a goal to build and maintain a culture of Cyber Threat Intelligence: Is there a process in place to proactively understand and manage the threat environment?

Establish Information Security: Are there processes in place to protect, detect, respond and remediate threats?

Promote a Culture of Awareness: Is there an awareness of the importance of security and do all insiders understand their role in maintaining that security?

Design and Practice Incident Response: Is there a documented plan in place as to how to respond to an incident? Is there an adequate and tested disaster recovery process?

Don't

Don't become complacent about cyber security. It's not a matter of “if”, but a matter of “when”.

Don't assume someone else has the responsibility to maintain and protect your data.

Don't wait until you are confronted with an incident to seek advice.

