BIRMINGHAM BUSINESS JOURNAL

Table of Experts Series

DATA PROTECTION

GETTY IMAGES

SPONSORED CONTENT

MEET THE EXPERTS

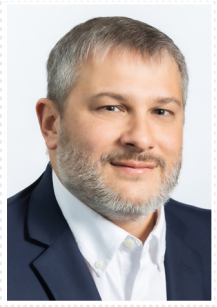
Matt Adams
Information Security Manager
Warren Averett Technology Group

Matt Adams serves as the Information Security Manager for Warren Averett Technology Group. He has over 25 years of experience in Information Technology, including over 14 years working for Rheem Manufacturing Co in their technology department.

His primary responsibilities are technical security assessments and sales engineering in support of the Technology Group's managed services. He focuses on building secure IT solutions that help clients take advantage of their technology to grow their business.

He has an extensive background in network infrastructure and cybersecurity that aids the Technology Group with designing, implementing and assessing client networks.

Matt resides in Coosada with his wife, and they enjoy traveling.



Brian Jackson
President and Chief Operating Officer
Abacus Technologies

Brian serves as the President and Chief Operating Officer of Abacus Technologies. In this role he oversees all executive decisions and operations of the company along with providing client solutions and client development

With over 15 years of experience, Brian has been able to use his knowledge of Accounting and Technology to provide client technical solutions across various organizations and industries.

He began his career in technology by implementing accounting systems, business intelligence solutions, and developing system integrations. Brian now works with clients to implement and support business applications, as well as the computer hardware, network infrastructure, cloud solutions and cybersecurity.

Q: What are some of the most important considerations for a company regarding data protection?

» **BRIAN JACKSON (President and COO, Abacus Technologies)**: Know what data you need to protect. Have a good policy that defines storage, retention and the transfer of that data. Since most data is handled through users, you need a policy to fall back on for compliance and continuity.

» **MATT ADAMS (Information Security Manager, Warren Averett Technology Group)**: First, know what data is being stored and where. That can help organizations make informed decisions about how to protect it. Protecting your data against external threats should be a consistent occurrence. Companies can do so by regularly updating security measures such as two-factor authentication, firewalls and anti-malware solutions. They might also want to implement advanced security solutions such as the Trusted Platform Module, and adopt a Zero Trust architecture. You should also encrypt your data – both data in motion and data at rest. This can add an additional layer of protection. Encrypting storage devices and servers as well can aid in data protection when data is being transmitted. Finally, educate your employees. Cybersecurity education begins at the employee level. Organizations should have an ongoing training program that informs all employees of compliance regulations and security best practices.

Q: What are the different types of data a company has, and what is the strategy for protecting the various types?

» **ADAMS**: Companies with various forms of data can categorize them by type, sensitivity and value to the organization. This can help companies understand their data's value, determine if the data is at risk, and implement controls to mitigate risk. There are several regulatory mandates such as SOX, HIPAA, PCI DSS, CMMC, and GDPR that have specific rules that apply to data governance. A strategy for protecting these various types of data is to organize it into three categories that prioritize by sensitivity level: high, medium and low. High-sensitivity data is the type that, if compromised or destroyed in an unauthorized transaction, would have a catastrophic impact on the company or individuals. These include financial records, intellectual property or authentication data. Medium-sensitivity data is intended for internal use only, but if compromised or destroyed, would not have a catastrophic impact on the company or individuals. These include emails and documents with no confidential data. And low-sensitivity data is intended for public use, such as public website content.

» **JACKSON**: Not all data is sensitive, but it does have value. Data can be sold or used for gain, but also may be weaponized against a person or organization. Classifying all your data can be an overwhelming task. I would suggest first identifying the data which is accessed most frequently, then focus your efforts on classifying and protecting it. Data which is rarely accessed could be taken off system and secured in whole. Typically, most organizations regularly access only about 30 to 40 percent of their data.

Q: What are the key components of data protection needs?

» **JACKSON**: There are four of them. First, you need a current inventory of your data to understand what you need to protect. Whether applications, unstructured file shares, online repositories, user desktops or email, it must be discovered. Second, determine what data is accessed most frequently. Utilize a retention policy to delete or archive data that is rarely accessed. Third, focus on the most frequently used data, since this represents the most risk to your organization. Finally, utilize a software or service to help continuously monitor your digital risk.

» **ADAMS**: For optimal data protection, companies should consider implementing a policy that sorts, identifies and categorizes the data by assigning it an associated risk factor. Companies should also have a plan for data

SPONSORED CONTENT

storage management, data access management, a verification system, data breach prevention, data backup and data recovery.

Q: What types of companies or partners can help businesses with their data protection needs?

» **ADAMS**: There are many types of industry experts – backup specialist, data access specialist, data breach prevention specialist, etc. – who can assist companies with data protection plans. The best plan of action is to partner with a company that can offer a full team of specialists and provide a technical assessment of your company's data. This partner should also be able to review the company's data to determine risk and provide a road map for protecting the data.

» **JACKSON**: Organizations will need both technical and compliance focused resources to develop a comprehensive plan to manage their digital risk. An organization needs to completely understand legal and regulatory requirements, then utilize a technical resource to apply the appropriate controls. However, the most important resource in this effort may be their own employees.

"Thanks to the uptick in remote working, systems that were once protected by the corporate security defenses are now in unprotected homes, coffee shops or just about any place that provides free Wi-Fi. These systems and their users are exposed daily to a barrage of social engineering attacks."

MATT ADAMS

Q: Beyond regulations, what are other important reasons companies should focus on data protection?

» **JACKSON**: Data can be weaponized against a person or organization in many ways. When encrypted it can be used to extort money since it may be required to complete critical business transactions. Intellectual property can be stolen then sold to a competitor threatening market share. A disgruntled employee may take customer lists, product

SPONSORED CONTENT

information or confidential data with intention to harm their former employer. Each company must complete its own digital risk analysis to determine the right approach for protecting their data.

» **ADAMS**: Many companies consider regulatory requirements as troublesome. However, these regulations can help streamline and improve several core business activities. Ensuring data is protected cannot only help companies streamline their processes, but it can increase the trust and credibility of an organization, which can enhance the enterprise and increase brand reputation.

Q: How expensive can a data breach be for businesses or employers?

» **ADAMS**: The average cost of a data breach has reached an all-time high of $4.35 million, and 83 percent of organizations responding to a recent survey have had more than one breach. Breaches are not only costly from the perspective of downtime or ransomware recovery, but also due to lost business opportunities because of brand or reputation damage.

"We need to provide education specific to the risks of the organization. Empower employees with knowledge but also provide them with an avenue for reporting threats. Let's make them part of the solution and not the focal point of the problem."

BRIAN JACKSON

» **JACKSON**: There are many statistics that can provide an average cost of each record lost or the total cost of handling a breach. It is always less expensive to be proactive with security than reactive. Spend money on your terms, and not on the terms of the adversary.

Q: Are there any new threats or concerns that are becoming more notable?

» **JACKSON**: Ransomware and extortion schemes remain at the top of the list. I believe that social engineering targeted at specific individuals is an emerging threat. If the adversary can compromise the personal life of an employee, they could use them as a vehicle to exfiltrate data without ever entering the network. Educating employees, creating a culture of security and providing a psychologically safe workplace helps mitigate the risk of this threat.

» **ADAMS**: Thanks to the uptick in remote working, systems that were once protected by the corporate security defenses are now in unprotected homes, coffee shops or just about any place that provides free Wi-Fi. These systems and their users are exposed daily to a barrage of social engineering attacks. From October 2020 to April 2021, social engineering attacks like phishing and email impersonation increased nearly 200 percent.

Q: What are some of the new laws and regulations companies need to be aware of?

» **ADAMS**: On June 3, the U.S. Senate and House released a draft of the American Data Privacy and Protection Act, a watershed privacy bill that would introduce a federal standard. Currently, a hodgepodge of industry-specific and state laws makes up the backbone of American privacy regulations and rights, so a national framework for privacy would establish a uniform system for this core American right. Each organization should review their industry-specific and state-mandated laws to ensure they are protecting their data in accordance with the latest standards.

» **JACKSON**: This is one of the most difficult but important areas when it comes to data breaches. Organizations should seek legal advice since laws differ for each state, government agencies and even countries. Non-compliance brings risk to the organization and could make a data breach exponentially more expensive.

Q: What are some new, innovative ways for companies to train employees on data security?

» **JACKSON**: We need to provide education specific to the risks of the organization. Empower employees with knowledge but also provide them with an avenue for reporting threats. Let's make them part of the solution and not the focal point of the problem. Promote policy, provide risk-based education, and build a culture of security starting from the top.

» **ADAMS**: Employee IT security training is the first line of defense in the fight to keep enterprise data secure. Each untrained employee can be considered a security risk, much like an unsecured server or a workstation without anti-virus

protection. One of the latest and most effective methods of training is to enroll every employee in an anti-phishing training solution. These solutions can mimic phishing emails and send them to employees to make sure they are staying vigilant against phishing attacks. With most training solutions, if the employee falls for the phishing attempt by clicking on a link, they will be subsequently taken to a training video that explains what they clicked on and how to identify and avoid these types of emails in the future.

Q: How can a company defend against a data breach? How big of a role does cybersecurity play?

» **ADAMS**: There are several strategic methods for a company to defend against a data breach, but the best defense is a good offense. A good offense can restrict access to only the people and systems that need access to data. For example, if 1,000 people have access to data on a system containing personal information, then you have 1,000 potential vulnerabilities. If you reduce the number to 10 people, then you have significantly reduced the risk of data loss. Another strategic method is to improve your general security. This is a huge and multifaceted topic, but in short, it's using techniques like better architecture, firewalls, VPNs, traffic monitoring and restriction. Even routine updates can make a big difference. Also make sure to evaluate your third parties carefully. Even a cursory connection to an unsecured organization can be a threat to your business. Since systems are constantly changing and cyber criminals are discovering new techniques to take advantage of vulnerable systems, cybersecurity must continue to evolve. Each system should be audited and reevaluated based on the latest information available, to provide the best defenses against a data breach. Cybersecurity is an ever-changing landscape and should be a key aspect in every company's information technology budget and planning process.

» **JACKSON**: Start with understanding your risk. Then put the technology, people and processes in place to mitigate those risks. Data protection is part of a comprehensive security strategy, although I believe it is the hardest to implement simply.

Q: What should businesses do when a data breach happens? How can they reduce their liability and potential costs?

» **JACKSON**: All businesses should have a documented incident response plan. Being proactive and planning for an incident will help exponentially when the inevitable occurs. Cyber liability insurance is still a great value when looking at the potential costs of a breach. Businesses need to understand that the cost of a breach may not only be the ransom, but may include breach notification, identity protection, forensics, legal and technical cost. The costs can add up quickly.

» **ADAMS**: If your organization experiences a data breach, the most important thing to remember is to not panic. Evaluate which systems have been compromised and immediately stop using them, or networks that might contain compromised systems. Next, consult your legal counsel or cyber insurance provider. They can usually provide assistance in the form of data forensics teams or other similar services to guide your organization in responding to the incident. If you find your organization does not have adequate legal counsel or cyber insurance providers, you can seek out external experts in the areas of forensics, legal, information security, human resources and communications. In a breach situation, it's important to seek expert advice rather than attempt to find and fix the issues on your own. You can also contact your local FBI field office if you or your organization is the victim of a network intrusion, data breach or ransomware attack. It's important to remember that companies have a part to play in reducing the liability and potential cost to their organizations. Each time they use data, send data or create a new system to store or transmit data, they should consider what would happen to the organization if this data were to fall into the hands of a cybercriminal. Companies should also be continually looking at their data usage to determine if it could be at risk and how to better secure it. Cybercriminals work 24/7/365, don't take vacations or holidays, and will use every opportunity they can find to compromise and steal your data. So as business and IT professionals, we should all work just as tirelessly to protect our organization's data. »