Discuss the specific recommendations that you would make based on your personal experience and research.

I think it's surprising that a lot of the security issues weren't addressed before there was a breach, especially considering that Clive is a security manager. There are a few gut recommendations I'd make immediately in this situation:

1. Whenever you're working with third-party software it should be fully vetted. You really need to know what you're working with, and if they allow SQL injection then that's a serious security concern. Especially if there isn't any way to audit SQL transactions from this software!
2. Whenever you're setting up a technology, make sure all optional features are turned off, and only turned on if a need is found for them. That's one of the first steps when setting up a server, virtual machine, or sql server for me. All optional features are off until they're needed.
3. DON'T SHARE PASSWORDS OR ACCOUNTS!!! That leads to a lack of accountability and observability! I feel like that should be a no-brainer, but oh well. I'd strongly recommend using an IAM (Identity & Account Management) system, that way you can set role-based permissions for accounts. You can also log access from these accounts, and directly tie actions to an individual.
4. Least privilege principle! Not everyone needs access to everything under the sun. This also includes service accounts, not all applications need write access to a database, or even direct SQL access.
5. I'm assuming that if 25 people are sharing an account and password, that the password was easy to memorize and never rotated. Require password rotation every three months with strict guidelines (16 characters with at least 1 number, 1 capitalized character, and 1 special character).

Discuss the impact (from the perspective of various stakeholders) of the lack of access controls and auditing.

This is a PR nightmare if there was a leak of customer PII (personally identifiable information). Then if it was leaked about how lax the security was around this data, the company would have trouble recovering. For example, it's one thing to be breached by a malicious actor who jumped through hoops to hit your system with ransomware, it's another thing to fumble customer information due to negligence. So, business stakeholders would be in hot water. If the company is public, I'm certain the stock price would drop.

Customers are going to be hurt by this if social security info or bank account information was stolen. If their social security information was stolen, then the company would have to provide a service like "LifeLock" (I believe Experian did something like this) to try to mitigate lawsuits/recover appearances.

How can technology be used as an enabler and facilitator of effective access controls and auditing?

Technology is really the only enabler and facilitator of effective access controls and auditing. Unless you padlock each computer and require a signed document for everything you do on it. IAM is incredibly important, you always need to be able to identify and authenticate users of your system. I don't know how you'd keep your system secure otherwise. There are tools for this out there, Microsoft's authenticator is a robust piece of software that allows for biometric and 2 factor authentication. Google also has their own authentication software. There are also password managers that allow for generation of truly random passwords, and secure storage of those passwords.

Being able to identify users is crucial for auditing. How are you supposed to determine who performed actions on your system without accurately being able to determine their identity? There are a number of auditing tools out there as well. If you're working in a cloud-based environment, most cloud providers offer advanced log querying options.

How can you apply the lessons that you learned from the story to your own company problem?

It helped me come up with some access control guidelines. This information needs to be well defined and agreed upon. Access control is so important, and I feel like I take it for granted since the company I work for does such a good job of it. Heartland Escapes is already slated to have role-based access control and Azure Active Directory from the migration design, but I think I'll make sure to drive home the importance of these structures.