HOW ARE YOU INSURING AGAINST DATA BREACHES?

Overview: Data breaches are inevitable, making protection against outside threats essential. But what if the breach happens internally? Taking the correct measures now can help mitigate the impact of internal breaches and protect for the future. The ability to record network traffic, view how records were accessed and by whom, and produce compliance reports are just a few of the benefits of implementing auditing software.

We buy insurance for protection against the cost of things we hope will never happen. But we know they will happen to someone, at some time, so we purchase protection which is less costly than enduring the loss. Data breaches do happen, and they are expensive and damaging to all involved. Sadly, they happen frequently, and we do have procedures to mitigate the loss. We continue our war against the outside threat of hackers, putting in firewalls and instituting physical security. All of this does a great job of protecting us and more importantly those that have put their trust in us. We should be, and we believe we are, always looking for ways we can do better. As threats evolve, so must our methods.

An area that is not always given enough attention is the insider threat. As we mentioned above, we provide for physical security and training to make sure those dealing with the public don't fall prey to those using pretexting, but things happen. What can we do to limit our loss when all else has failed and a breach occurs? How can we respond quickly and definitively when confronted with someone inside our perimeter defense that has access and has breached our data and our trust? Any way we can limit our exposure matters. Any way that we can produce a list of only the customer data

accessed by this person limits the exposure and increases the trust the public has in the organization.

What is needed is a way to simply and efficiently record the activity on the system of record, the mainframe. A means to be able, if necessary, to start with a breached record and tie it back to anyone who viewed it, or to take the opposite approach and produce actual screens of activities carried out by a suspected person. By having this means we can quickly isolate the damage and begin the repair, allowing us to meet reporting deadlines and have confidence in our investigation. It would provide evidence which would help in prosecution if necessary. These abilities would be the difference between announcing that we know we were breached, sometime, by someone and so we have to assume it could be all records – or – we can state we know who did it, during which timeframe, and which records were accessed. Instead of notifying and entire customer base of the breach, we can notify only those who will have a concern.

Fortunately, this solution exists and is being used by many for the assurance they need. BMC AMI DevX Application Audit can:

- Efficiently record network traffic and application screens, archiving them for investigation.
- Provide insight into user behavior, such as which data a particular user viewed and how it was accessed.
- Leverage SIEM integrations like BMC AMI Datastream for z/OS provide application-level insight for identification and reduction of cybersecurity threats.
- Provide the intelligence and reporting required for HIPAA, GDPR, and Australian NDB scheme compliance.
- Eliminate dependency on specialized mainframe knowledge.
- Maintain Separation of Duties between system administrator and auditor.

Beyond this there is a unique benefit from this form of “insurance.” Once you have implemented the recording and periodic searching of activity you will also put a warning on the screen to inform those who log in that their activities will be recorded and searched. This warning serves as a valuable deterrent to the malicious breach of data by a trusted user. Someone with criminal intent will realize it is not worth the risk of exploiting the data.

Unfortunately, data breaches are bound to happen and can be especially disruptive if they originate internally. The key to minimizing their impact and deterring future malicious activity lies in the ability to identify their origins and scope. With the right tools, your organization can respond to these breaches and implement measures to mitigate future risk, giving your customers, as well as your employees, peace of mind that their data is safe.