James Chad Ballay

Week 7 – Enterprise Computing

* Information classification, labeling, and handling
  + What types of information does your organization handle that requires confidentiality?

We handle PII data for our employees and customers. (SSN all the way to phone numbers and everything in between.) HIPAA data for our pharmacy business. Car data surprisingly as well due to license plate, VIN, and customer name. Supplier and vendor data as well. Many of our suppliers have NDA’s with us that limits our ability to disclose pricing and sourcing.

* + Identify types of information that the organization must handle in its daily business.

It’s Walmart so a lot of the data is daily. It may not be one specific customer’s data every day but somewhere, somehow every imaginable business process is being done multiple times. For my specific area of the business it’s the customer journey from the user accessing the Online Grocery Portal to when we put the groceries in their vehicle. There are times where I have to be able to look at a specific customer’s orders all the way to what are the metrics of our DB servers performance.

* + Is any of it considered personally identifiable information?

Yes. So much of it. Orders as they flow through the system and the names of the customers associated with them. (The phone number we text to let them know about their order’s status.) If we have a pricing or item info issue due to recall we need to identify all open transactions involved and prompt the stores to contact those customers about substitutions. Etc, etc...

* + Explain why the organization must handle the information and why it must be kept confidential.

For my team’s role we often have to look for outliers at the 99% and greater interval and figure out how our monitors failed. Maybe orders that contain alcoholic products get stuck in processing if they also have a WIC sub transaction as well. Or maybe somehow the car color selection had non-printable characters in the text field that crashed the app.

The need for confidentiality is multileveled. The first is just good business practice. Customers enter into the business relationship since they are wanting something and are willing to pay for it. Anything beyond that basic exchange of goods for money increases the complexity of the sale. Erring on the side of caution and discretion respects that equation. From the business side of the equation, once the data is out there it loses it’s usefulness as a differentiator. Maybe by analysis I’m able to figure out that Lexus car owners tend to be on time for their grocery pickups while minivan owners tend to be 5 mins late and therefore should budget our geofence alerting accordingly to maximize worker productivity. Or whatever type of specious correlations. If I disclose these then any retailer can benefit from that analysis and it ceases to be a business oppurtunity for my employer.

* List four examples of physical security measures used by your organization.

Badges and uniforms to keep customers out of the backroom. Big, loud and visible security scanners by the door to let people know we are scanning for active RFID tags. Camera feeds of yourself at the self-checkout to subtly let people know we are recording your checkout in case we need to review it for theft. Zip tags on the 18 wheeler trailer doors to ensure that nothing “falls off the back of the truck” between the DC’s and the stores. All of these can be bypassed but they keep the honest people honest.

* Identify the three phases of developing an enterprise security system and the steps involved in each phase.

Planning - What do you hope to accomplish. What are the formal requirements. What are the roadblocks to success.

Implementation – What's the solution that you are going with. How will you know if it is successful. How will you accomplish rolling out the system

Deployment – Get and document the buy in from the involved parties for the solution. Plan the release and various likely rollback or rollfoward checkpoints.

* Briefly describe a business impact analysis (BIA) and what it estimates and identifies.

Roughly it looks at disaster scenarios and the response of the business. For example, what if the New Madrid Fault Line had an earthquake? Would we notice or would it likely interrupt utilities to the datacenter near it? What business critical applications are reliant on that datacenter? Could we shift the load over to other datacenters during non-holiday loads? What about if it happened in November?

All of those types of scenarios and the questions and answers that they prompt loosely are the focus of a BIA. How do we systematically approach events that’ll impact the operations of our business. Once the risk and impact are identified what are the reasonable steps we can take now to either prevent or mitigate the rist and impact.