The Security Development Life Cycle

Tyler Chotikamars

University of Arizona Global Campus

CYB 301 Introduction to Cyber & Data Security

Bipin Bhatt

July 19th, 2021

Data is all around us. In a way we too are data, we create data and are represented by it. Unfortunately, there are people in the world who have figured out how to abuse data to gain money or national intelligence. Security systems are critical to allowing data to be safe and secure. A system development life cycle (SDLC) is a process that is developed to ensure that data is handled and disposed properly. The real question is, how can we implement the SDLC in a proactive way that will help users and protect institutions assets?

The SDLC is different for everyone, but they include main steps such as the initiation, development, implementation, maintenance, and disposal. During the initiation phase the institution establishes the need for a SDLC and begins security planning. At this point in the phase the type of data that is going to be collected, travel, and stored is decided along with who the Information System Security Officer is. With a security system being implemented things such as potential threats, constraints, and requirements are considered. It is important to note that the CIA triad (confidentiality, integrity, and availability) should be acknowledged at this stage. Another important thing to consider early on would include any government regulations and policies that must be followed. The next phase is development where a system is either designed, purchased, or developed that can analyze risk and supplement the overall security. Within the risk assessment the institution can figure out what assets, people, and operations can be targeted because of an information security attack. Within this part of the process a security plan is established based on the requirements for the information system. The next step within the SDLC is the implementation phase. This is where the security systems are installed and tested. Any new controls are configured and tested to ensure that security professionals know how to use the tools and to prove that they work. Following up the implementation phase is the

operations/maintenance phase. Within this phase the entire system is developed and tested. This includes the addition or subtraction of any parts of the system and is also where the organization can monitor and configure the system. All changes are documented, and all modifications are made within this period. The final phase of the SDLC is the disposal phase. Within this step plans for discarding the current system are made as well as the transition into the new system. Within this process the data can be archived, discarded, or destroyed. With the digital landscape everchanging, there is no definitive end to any system. The disposal of a system includes the termination of the system and the preservation of important information. Here the data can be transferred to the new system in accordance with the institutions security requirements (Radack, 2009).

Saying that we are simply not at risk of a cyber-attack would be ignorance at it is best. There are many ways that a company could be considered at risk and the best thing we can do at our company is mitigate the risk that comes with any impending attacks. In order to assess the risk, we must look at the whole infrastructure of the business and how the internet is used in tandem with it. This is because the issue of cyber security is not just a cyber issue, but it affects the whole business. A couple things that can be considered at risk within a network could be a user workstation and a payroll department printer. As for what entity would do such a thing, nation-states, hacker groups and even individuals are capable of planning out and carrying attacks. Within an IT infrastructure vulnerabilities like network cables and wireless user devices pose as hubs for hackers to connect to and abuse, there was even a case where hackers used a fax machine to carry out their attack. The two risks that we will be assessing is the possibility of a network attack and social engineering attacks. These attacks can prove to be detrimental to the company in terms of server down time and to the protection of user/sensitive data. A clear

vulnerability that is associated with social engineering attacks are employees. Employees can be easily tricked or even convinced to leak sensitive data or even be paid out to plug in hardware with malicious data. Another vulnerability lies within the network security, where in this case an outsider can disable the companies, network causing downtime. Since there are laws and regulations that we must abide by, it will be harder to protect ourselves from people who do not have to abide by the same rules. However, there are many things that institutions and companies can do to prevent catastrophes from happening. Making sure that having the physical infrastructure to the network is safe and secure along with educating and working with employee's are good deterrents to attacks like these. Having policies in place to protect the users and the company is an important safeguard that also follows regulations and laws that comply with governance.

To put our risk assessment to good use we must come up with a means of implementing the risk management process. For the organization to do this they must first create a secure infrastructure. A viable means of securing the physical network is to keep the environment secure. This can include logging who enters and exits the room as well as making sure only authorized personnel are allowed into restricted access areas. Another good implementation is to inform employees of the possibilities there are that comes with working with the organization. This includes having them understand what phishing links are and creating a workplace environment that allows employees to feel valued. Implementing a satisfaction survey could help disgruntled employees turn into loyal ones who would rather be willing to work with an organization rather than against. The implementation of the risk management process can also include limiting bring your own device policies to mitigate risk. Within a network attack wireless access points could be accessed and spread viruses within the network. With a risk profile in

hand, we can install the software and tools necessary to protect our hardware and data.

As mentioned previously, the policies that institutions set are important for following the regulations set in place and for protecting users as well as the institutions/companies. The goal for our organization is straightforward and progressive. Our company goal is to allow individuals to encrypt and secure their own personal data as a means of securing ownership and privacy. This can be done through end-to-end encryption between the client and the server where each of them holds a key. Since our organization does not hold the encryption key there is no way for us to spy on our customers, therefore guaranteeing privacy. The guarantee for privacy is important to us because there are always newer hacks and ways to attack consumers. Since our organization cannot see the customers private data there is no way that we could leak or even view it. This goal aligns with our values and our overall mission. If our organization can achieve this goal, then for our customers it means they will have a secure means of storing sensitive data.

While we strive to hit our goals, our objective is to create an anonymous platform where data is encrypted and stored (while still being in accordance with government laws and policies). We believe that in today's age of technology that it is easy to carry out attacks to steal someone's identity. There are too many companies that treat a data breach like a symptom rather than something that is preventable. Which is why our objective to help the average user of the internet keep their private online data protected from malicious entities. We believe that users should have the right to protect their own property where people cannot steal sensitive information, documents, or spy on others.

A regulation that we must follow includes the general data protection regulation guidelines. This regulation is a part of the data protection act, where users can submit a subject

access request (SAR). This regulation has been enacted by the government to protect the fundamental freedom of natural persons regarding the right to protect personal data. This regulation applies to our company because we will comply with the government to succeed, our platform is not to be used for criminal activities. This regulation applies to our company because government entities must submit a SAR to obtain a customer's information. Without the subject access request there is no way for the government to acquire private information without carrying out an attack of their own.

A law that we will abide by includes Nevada's Senate Bill 220. This bill requires website operators to honor opt-out procedures. Our company collects certain personal data which can be sold to third parties, the Senate bill proposed legally obligates our organization to allow users to opt out if they so choose. With this bill senate being in place, the users have more control and say over what they are exposed too, where in many cases advertisements are pushed without consent. This will become increasingly relevant as people adopt newer technologies and as developers try to find new ways to integrate ads in a non-invasive way. This law applies to our company because targeted advertising is integrated within our business model as a means of capturing profits to run our servers. However, we do believe in allowing people to have the right to control when ads occur and what ads do. If our customers decide to opt-out, then we cannot collect personified data that are sold to third parties.

Stakeholders will be interested in our company because we provide human right of ownership and privacy that consumers are losing within today's internet space. With how open the internet and along with the tools that are publicly available, it has become easier to steal other people's work to the thief to claim as their own. Our platform also provides security for conducting business, which is invaluable within our world of constant data breaches and attacks

that we live in. With our invasive big tech is becoming in terms of how they use consumers data, it is clear to see that people who invest in our company value security and privacy.

Securing personal information is one of our biggest values within our organization. Policies are constantly updated within our company, but one policy includes authorized access. Only authorized users can access personal user files, this is as easy as giving only one encryption key to the user and keeping one locked away in case of the government requests it. Another policy we have in place is our password policy, since security is valued within our organization there must be rules for which passwords are deemed useable or unusable. We recommend that customers do not re-use passwords, but we require that it has 10 values, one uppercase letter, one lowercase letter, two different special characters, and a number. This policy also includes a 5 time try for each account once a day, if the user exceeds 5 tries for a password they will be locked out for the remainder of the day. The main rule in our password policy is no dictionary words, this makes it harder for brute force hackers to access private data. In addition to these two policies, we have created a private phrase policy. Within this policy the user must record a private phrase and store it somewhere safe, this private phrase will be used to recover any accounts. Without a private phrase and a password, it will be impossible to recover any account. These policies are in place to help protect the users and their accounts since the data is supposed to be private, we would like to ensure that no one else but the customer has access to their data.

An industry standard that aligns with the policies we have chosen included antivirus protection, the encryption of data, and the deletion of redundant data. Some other common policies that we align with include lawful collation and processing and spread data storage. With data being spread out through multiple locations, it minimizes the impact of a data breach (Wiley, 2017).

A security model that is useful for people within the information technology space is the CIA triad. Their security model is composed of confidentiality, integrity, and availability. Our company values all of these and that is why is pertains to our organizations as it should pertain to all major tech companies. Keeping confidentiality is important in today's age where people have the freedom to shop around for services. Information that must be kept confidential would include anything personally identifiable and even personal photos. Data that is transmitted between the server and user must not be tampered with to ensure integrity. This includes transmission sent from our severs to the customers client and then back. As for availability, it is important for customers to be able to access their data when it is convenient for them. It is important for security professionals to have availability to security systems as well. For our organization to succeed we need to announce when our servers will be down and make sure that any other downtime is mitigated as much as what is in our control. Our system development life cycle ensures that the CIA triad is being met. By keeping a secure system and logging all the events that happen within it we ensure the integrity of the network servers. The disposal of the security system once transitioned to a new system maintains confidentiality since the data is properly accounted for and then moved onto the new system. Access is a given when working with the system development life cycle if the authorized user has access to the physical components of the network. When we look at our WAN network, we see the CIA triad being implemented perfectly. In this case our WAN network can effectively keep information confidential with our encryption system. We can also ensure integrity by allowing users to see the servers they are communicating with as well as making our server addresses public. Finally, we give the user full access by granting them a key to the encryption. The strength and

bandwidth of a WAN is dependent of the hardware, but the standards of our network keep up with the CIA triad.

References:

TestOut. (2017). *Security pro courseware.* TestOut. https://www.testout.com/courses/security-pro

Wiley. (2017). *The Cyber Risk Handbook.* John Wiley and Sons.

Rackade. (2009). *The System Development Life Cycle.* NIST Special Publication (SP).