Southern New Hampshire University
IT 549: Foundation in Information Assurance

Final Project

Information Assurance Plan

Carl B. Wade
10-4-2016

Table of Contents

Overview of Goals and Objectives

The goal of every business dealing with confidential information is to ensure that unauthorized people do not gain access to confidential information. These goals are not different when dealing with the Printing Industry. Printing companies deal with a lot of different types of confidential information. Some are simply company secretes that they do not want their competitors to know others are customer's personal information that should not be known to the public. The biggest section of the Printing Industry that deals with confidential information is companies that are involved with database publishing. "Common examples are mail order catalogues, direct marketing, report generation, price lists and telephone directories. The database content can be in the form of text and pictures but can also contain metadata related to formatting and special rules that may apply to the document generation process. Database publishing can be incorporated into larger workflows as a component, where documents are created, approved, revised and released." (Wikipedia, 2016)

Confidentiality, Integrity, and Availability of Information

When creating an information assurance plan, it is extremely important to follow the CIA model. All data that is being printed should remain confidential. In database publishing, customer's data is the most valuable asset and liability to the company. The customer's data is the driving force behind the service the company sells. In other words, no data means no income. On the other hand, if the customer's information is not protected there are legal ramifications to such actions. With information ranging from addresses, credit card numbers, bank accounts, social security numbers, it is critical to keep the data confidential. In some ways confidentiality ties into data integrity in database publishing. When dealing with confidential information the

company must ensure that the correct data is sent to the correct person. For example, the company must ensure that Bob's bank account does not accidently get sent to Alice in her monthly bank statement. The company must ensure the integrity of the database. The value of the service preformed is only as good as the integrity of the database. If that data does not remain accurate, there will be legal ramifications. Today most, if not all, database publishing is done using digital technology. This allows for each document to be created separately but printed together. This is done by creating templates that contain information that will be printed on every document (static text/graphics) and also tags that tell the printer where to print the personal information (dynamic text/graphics). The dynamic tags tell the digital press's raster image processor (RIP) what information it needs to grab from the database and also the location of the database. The RIP then uses a secure network to grab the required information, processes the data, and generates a file that is sent to the press to be printed. Without the secure network, the RIP cannot access the database to obtain the required information or send any files to be printed on the digital press. To ensure that the company remains in business it is critical that the CIA model is followed. Deviating from this model will result in losses that will shut down the operations of the business. These loses could result from a lack of confidence in the customer or a result of legal actions. According to Vincent R. Johnson at Harvard," there may be a legally enforceable data-protection obligation based on a voluntary assumption of duty principles. Where the possessor of a database makes affirmative representations that it keeps data private and a customer relies on those representations, a court might reasonably interpret such a privacy policy as an undertaking to exercise reasonable care, and might conclude that a breach of that duty would support a tort cause of action." (Johnson, 2010)

Current Protocols and Policies

There are laws in place to help shape company's information assurance policies. In particular the Privacy Act of 1974. "The Privacy Act of 1974, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual." (U.S. Department of Justice, 2016) These laws give requirements for handling of the documents, background checks for employees handling the documents, and also handling of the waste of the documents.

Even with federal laws shaping the company's information assurance policies, there are still some areas to expand additional security and also some holes that can be exploited by people. One such area is allowing press operators to have personal property. Such items like pen and note pad, USB thumb drive, cell phones, lunch box, thermal coffee mugs, and so on. Since video recording is prohibited under the Privacy Act of 1974, monitoring of press operators must be performed visually by humans. Humans are flawed and people can use such personal objects to copy confidential information. I believe that such personal property should be banned to avoid such a situation. Also each operator should be searched before and after the shift to ensure that the policy is followed and that information is not being removed by unauthorized methods. There are some barriers that must be overcome to add these or any additional policies. The fist barrier is cost; not only in any additional staff needed but also in additional training. The second barrier is the potential of turnover of staff. Some employees may not agree with the new policies and end up quitting as a result of them. While others may need to be terminated due to disregarding

the new policies. The third barrier is a potential in loss of production. There will be a timeframe needed for adjustment to the new policies. Change does not happen overnight and people generally resist change as much as possible. When the new policies are enacted, there will be a drop in production until the employees adjust to the change and it becomes the new norm. However, even with these barriers, information assurance must be top priority to ensure the CIA model is followed. A disregard to information assurance will result in a permanent closure of the company.

Information Security Roles and Responsibilities

When discussing the roles and responsibilities of key leaders in database publishing company, the information assurance is broken up into three parts. Those parts are the database side, network side, and the production side. Each play a different role in keeping data confidential, intact, and accessible.

Responsibilities of Key Leaders

For the database side of things, the database is governed by the database administrator. “The data administrator finds out or assigns who owns which data elements and who can create, change, and delete what… Do appropriate people have the right permissions to read the data they need? This implies, quite correctly, that the data administrator creates the security policy for the database, although others will likely implement it.” (Cox, 2000) The database administrator is the gatekeeper of the database and they are responsible for all the data inside of the database. They must ensure that only authorized people are able to access the data that they are authorized to access. For example, the company will be involved in many different projects at the same time and if the system is not managed correctly an authorized user may gain access to data that they are not authorized to have. Printer 1 is an authorized user and the database administrator must ensure that they only have access to data for Project 1 (the one they are working on) and not Project 2, 3, 4… etc. Some other responsibilities for the database administrator include:

- Back up and recover the database.
- Install and configure Oracle software.
- Create new databases.

- Design the database schema and create any necessary database objects.
- Formulate optimal application SQL.
- Ensure database security is implemented to safeguard the data.
- Work closely with application developers and system administrators to ensure all database needs are being met.
- Apply patches or upgrades to the database as needed.

(TechTarget, 2006)

These roles cover all of the goals in information assurance. They are responsible for confidentiality, integrity, and accessibility of the data within the database.

The following are job titles and respected responsibilities of the key leaders for the database side:

- Senior Database Administrator – Lead the maintenance, security, and operational execution of government information system databases
- Database Administrator – Works under the Senior Database Administrator to develop and implement information technology strategies, platforms, and solutions that meet current and future business needs

For the networking side of things, the network administrator must ensure that the network is always operational when needed. According to Oracle, "As a network administrator, your tasks generally fall into the following areas:

- Designing and planning the network
- Setting up the network

- Maintaining the network
- Expanding the network

Each task area corresponds to a phase in the continuing life cycle of a network. You might be responsible for all the phases, or you might ultimately specialize in a particular area, for example, network maintenance." (Oracle, System Administration Guide, 2010) The main responsibility for the network administrator is to ensure a constant and secure connection between the database and file preparer and then the printing press. They are responsible for confidentiality, integrity, and accessibility of the data within the network.

The following are job titles and respected responsibilities of the key leaders for the network side:

- Network Engineer – Implement and manage enterprise networking solutions with high reliability and availability, introduce new networking technologies or enhance existing technologies to transform existing capabilities and services, support of the Network, IP and related security services issues, resolve complex system and network issues and outages when needed
- Network Administrator – Works with the Network Engineer to configure, install and maintain network hardware and infrastructure, install new hardware and software upgrades for all layered products after presenting a plan for user testing and migration to the new product level

For the production side of things, the production managers are responsible for the actions of the print workers. They are responsible for training the workers on the security procedures, and also ensure that the workers follow the procedures. These procedures ensure that the workers

print the data and also dispose of any waste in a secure manner. They are responsible for the confidentiality of the data within the production floor.

The following are job titles and respected responsibilities of the key leaders for the production side:

- Production Manager – Interviewing, hiring, and training production employees; planning, assigning and directing work to ensure production is done in a timely manner
- Production Supervisors – Works with the Production Manager to ensure production goals are met, ensure all safety and security policies are being followed

Key Ethical and Legal Considerations

There are two main consequences for a lack of information assurance within the database publishing industry. The first is the company will be open to a lawsuit from the customer or fines from the government. Depending on the sensitivity of the data that can be tens of thousands of dollars up to millions of dollars. The second is criminal charges for the individuals who are responsible for the data breech. According to the U.S. Department of Justice, "Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000." 5 U.S.C. § 552a(i)(1).

"Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than $5,000." 5 U.S.C. § 552a(i)(2).

"Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000." 5 U.S.C. § 552a(i)(3). (U.S. Department of Justice, 2016)

In Kentucky, there are laws that companies must follow in an event of a data breach. These laws clearly define what a data breach is, each party involved in the breach, and the action that much be performed. According to the Security Breach Notification Laws of Kentucky, a data breach is defined as "unauthorized acquisition of unencrypted and unredacted computerized data that compromises the security, confidentiality, or integrity of personally identifiable information maintained by the information holder as part of a database regarding multiple individuals that actually causes, or leads the information holder to reasonably believe has caused or will cause, identity theft or fraud against any resident of the Commonwealth of Kentucky. Good-faith acquisition of personally identifiable information by an employee or agent of the information holder for the purposes of the information holder is not a breach of the security of the system if the personally identifiable information is not used or subject to further unauthorized disclosure" (NCSL, 2016) Information holder (the party liable to the data breach) is defined as, "any person or business entity that conducts business in this state" (NCSL, 2016) Personally identifiable information is defined as "individual's first name or first initial and last name in combination with any one (1) or more of the following data elements, when the name or data element is not redacted: 1. Social Security number; 2. Driver's license number; or 3. Account number or credit or debit card number, in combination with any required security code, access

code, or password to permit access to an individual's financial account." (NCSL, 2016) The information holder is required to do the following after a data breach, "following discovery or notification of the breach in the security of the data, to any resident of Kentucky whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (4) of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system" (NCSL, 2016) Failure to follow these local laws will result in the same penalties under the Privacy Act of 1974.

Key Components of Information Assurance

In regard to the database there are a few tasks that can be performed to ensure the data within the database stays confidential, unaltered, and accessible. The first is to ensure that the database is accessible only within the company's network. This will ensure that all data is only accessible to authorized people within the company and outside hackers will not be able to access the data. The second is to use Role-Based Access Control to control the user's interaction with the database. According to Jacobs, "In role-based access control, the focus is on users and on the jobs users perform. A collection of application specific operations (procedures of privileges) is defined as a role. Subjects derive their access rights from the role they are preforming. Roles, procedures, and data types are used as intermediate layers to structure access control." (Jacobs, 2016) This will ensure that each user will only have access to the data they are authorized to access and also only edit data that they are authorized to change.

In regards to the network there are a few tasks that can be performed to ensure the data within the network stays confidential, unaltered, and accessible. The first is to create a separate

secured network for the connection between the database and other workers. This will ensure that the database will never be connected to the outside world. The second is to use passwords that are hashed with salt to protect access to the database. Even with the database not connected to any outside networks, there must be steps to prevent attacks from within the company as well. Third is to encrypt the network used to transfer the data from the database to the workers and then to the press. This is another step to minimize as much risk of inside attacks or tampering as possible.

In regards to the production area there are a few tasks that can be performed to endure the data within the production area stays confidential. The first is to ensure proper training is performed so that every worker knows the procedures necessary to keep the data confidential. Most of the mistakes that lead to a possible information leak are a result of poor training. The second is for managers and supervisors to perform periodical checks on the workers to ensure all procedures are being followed and correct any deviations. This covers proper printing and waste handling procedures are being followed.

Risk Assessment

According to Symantec, Risk = Assets x Threats x Vulnerabilities. “Essentially, these algorithms assist the user in quantifying the combination of asset criticality, threat level and actual vulnerability for every informational asset in the network.” (Symantec, n.d.)

Analysis of Environment

Figure 1 shows the workflow of the Database Publishing Production.

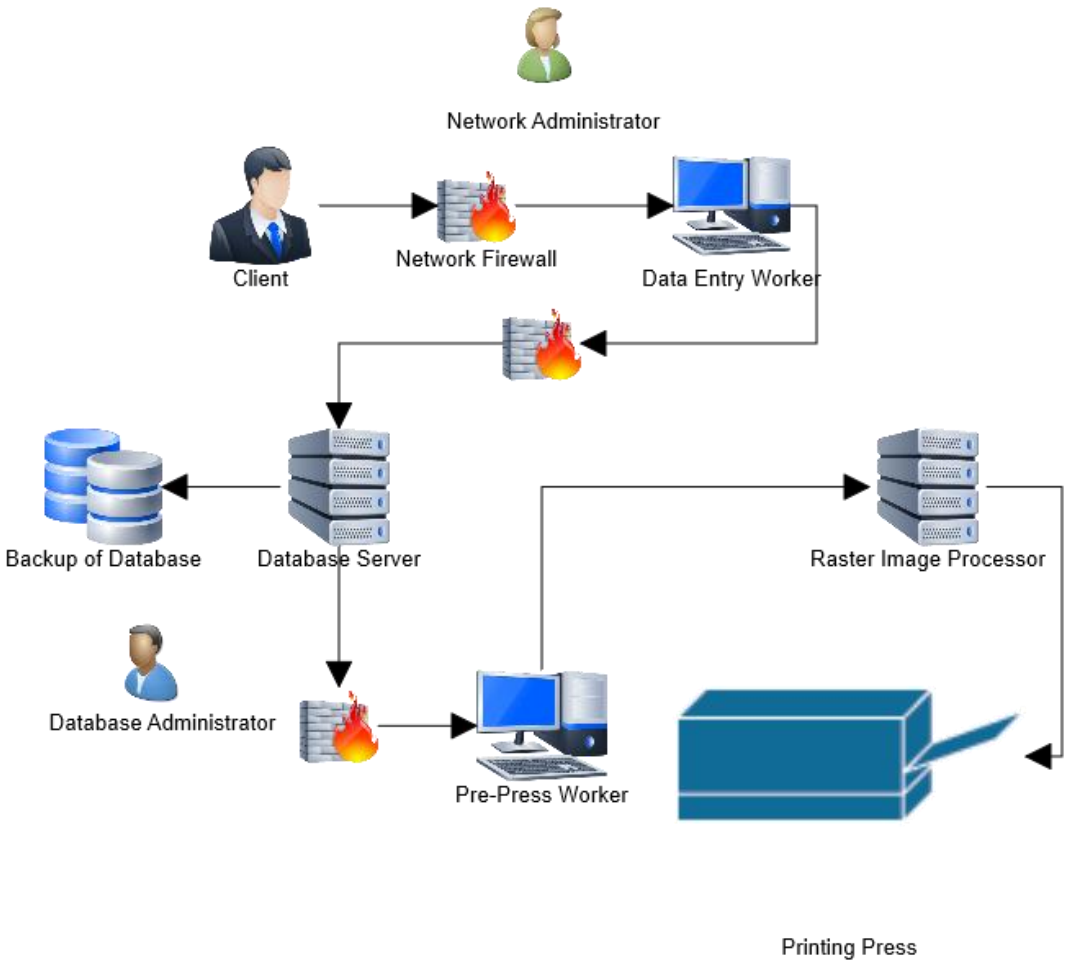

Figure 1 - Workflow of a Database Publishing Shop.

The client sends the information needed to be printed over a secure file transfer protocol. This is the only connection to the outside world. The network administrator monitors the network to

ensure the connection and transfer of data is secure. They are also responsible for the network uptime and resolves any issues. The data gets sent to a data entry worker and gets entered into software that securely enters the data into the database server. The database administrator oversees the data transfer to ensure that only authorized users are entering or requesting files from the database. They also ensure that each role have the proper rights to the database and corrects any issues. The server is backed up by the database administrator on a regular schedule to ensure that no data is lost due to a server failure. The Pre-Press worker pulls the required database file and attaches it to a template then send both files to the Raster Image Processor. The Raster Image Processor takes the two files and produces a single file for the digital press. The single file is sent to the digital press for printing.

Threat Environment

According to Schulman, there are ten most common database security failures:

- Excessive privileges (Users are granted rights to the database that are beyond what is required for the job)
- Privilege abuse (Users use their rights to gain more information than needed)
- Unauthorized privilege elevation (Attackers use variabilities in database management software to change their rights to the database)
- Platform vulnerabilities (Vulnerabilities in the computer's operating system that lead to unauthorized data access)
- SQL injection (Attackers send unauthorized database quarries to gain privileges to the database)
- Weak audit (Bad database auditing system can lead to security issues)

- Denial of service (Attackers prevent authorized access to the database through use of buffer overflows, data corruption, network flooding or resource consumption)
- Database protocol vulnerabilities
- Weak authentication
- Exposure of backup data (insecurely storing database backups)

(Schulman, 2007)

Best Approaches

To deal with all issues involving privilege issues (excessive, abuse, unauthorized, etc.) the database administrator needs to create and enact control policies. According to Schulman, "The solution to this problem (besides good hiring policies) is query-level access control. Query-level access control restricts privileges to minimum-required operations and data. Most native database security platforms offer some of these capabilities (triggers, RLS, and so on), but the manual design of these tools make them impractical in all but the most limited deployments." (Schulman, 2007)

According to Microsoft, to counter SQL injection attacks, you need to:

- **Constrain and sanitize input data.** Check for known good data by validating for type, length, format, and range.
- **Use type-safe SQL parameters for data access.** You can use these parameters with stored procedures or dynamically constructed SQL command strings. Parameter collections such as **SqlParameterCollection** provide type checking and length validation. If you use a parameters collection, input is treated as a literal value, and SQL Server does not treat it as executable code. An additional benefit of using a parameters collection is that you can enforce type and length

checks. Values outside of the range trigger an exception. This is a good example of defense in depth.

- **Use an account that has restricted permissions in the database.** Ideally, you should only grant execute permissions to selected stored procedures in the database and provide no direct table access.
- **Avoid disclosing database error information.** In the event of database errors, make sure you do not disclose detailed error messages to the user.

(Microsoft, 2005)

To deal with the weak password issue, the best policy is using a multi-factor authentication. For example, using a user's password with a one-time random key token that is sent only to the user. This will ensure that only authorized people are gaining access to the database. Depending on the sensitivity of the data, a smart card could also be used with fingerprint scanner.

The biggest security issue does not come from outside threats but from inside workers. Employees have access to the data and could easily steal the information. Strong hiring policies along with intense background checks can extremely reduce this risk. The next issue comes from human error as a result of having a lack of knowledge. This can be accidently deleting data to improperly disposing of waste. The only way to overcome this risk is to have proper training for all employees to ensure they know all the policies and consequences for failure to follow such policies.

Risk Matrix

	Impact				
LIKELIHOOD	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Extreme (5)
Rare (1)	Low	Low	Low	Low	Low
Unlikely (2)	Low	Low	Low	Medium	Medium
Possible (3)	Low	Low	Medium	Medium	Medium
Likely (4)	Low	Medium	Medium	High	High
Almost certain (5)	Low	Medium	Medium	High	Extreme

Risk Area	Risk Description	Likelihood	Impact	Risk	Mitigating Actions	Responsibility
Excessive privileges	User gain unnecessary privileges to the database	Rare	Extreme	Low	Database Administrator ensures all users have the correct amount of privileges	Database Administrator
Privilege abuse	Users use their privileges to gain more data than what is necessary	Possible	Major	High	Create access control policies that apply not only to what data is accessible, but how data is accessed	Database Administrator and Production Managers/Supervisors
Unauthorized privilege elevation	Attacker changes user privileges to the database	Possible	Major	High	Use query-level access control and traditional intrusion prevention systems	Database and Network Administrators
Platform vulnerabilities	Vulnerabilities in the computer's operating system that lead to unauthorized data access	Unlikely	Moderate	Low	Keep all computers up to date and use intrusion prevention systems	Information Technology Department
SQL injection	Attacker sends unauthorized quarries to gain privileges to the database	Possible	Moderate	Medium	Use Query-level access control systems	Database and Network Administrators

Weak audit	Bad database auditing system can lead to security issues	Likely	Major	High	Use network-based audit appliances	Database Administrator
Denial of service	Attackers prevent authorized access to the database through use of buffer overflows, data corruption, network flooding or resource consumption	Likely	Extreme	High	Monitor the network and place connection rate controllers	Network Administrator
Database protocol vulnerabilities	Vulnerabilities in database protocols may allow unauthorized data access, corruption or availability	Unlikely	Major	Medium	Database Admin can parse and validate SQL requests to ensure they are not malformed	Database Administrator
Weak authentication	Users having weak passwords	Almost Certain	Extreme	Extreme	Use a multi-factor authentication and hashing passwords with salt	Everyone
Exposure of backup data	Insecurely storing database backups	Likely	Extreme	High	Encrypting the backups will ensure no unauthorized user can use the backup	Database Administrator
Virus/Malware	Programs that alter the functions of a computer to benefit the attacker	Possible	Moderate	Medium	All computers must be up to date on the anti-virus software and also have proper firewall policies	Information Technology Department
Natural Disasters	Disasters caused by the weather	Unlikely	Minor	Low	Backup the database on a regular basis	Database Administrator

Statements of Policy

Computer Security is only as strong as its weakest link. When security is compromised it is vital to have a well thought out plan of recovery and a well-trained team to execute the plan. Logical steps to be prepared are:

1. Develop your documented program.
2. Select core cybersecurity Team members.
3. Train Cybersecurity Team members on the program.
4. Conduct practice drills on responding to incidents.
5. Put contracts in place with companies who you may need for technical support.

(Smith, 2016)

Incident Response Protocols

Network security is a responsibility shared among everyone in the company. It is critical for everyone to report any unusual activity on their workstation computers to the IT department. The IT department will examine the computer to determine if the activity is due to user error or is an attack. If the IT department identifies the incident as an attack or feels that the situation is outside their knowledge, then they will turn the incident over to either the Network Administrator or the Cybersecurity team.

When an attack is confirmed documenting the incident is vital. The following information should be collected immediately following a confirmed attack:

- Incident Title
- Date/Time Discovered
- Type of Incident (virus, hacker, etc.)

• Entry Point into your system

• Who is the perpetrator (If Known)

• System/Hardware/Software Impacted

• Description of the attack

• Narrative of problems it caused the organization

• What was done to contain it

• How was the problem eradicated/removed

• How was recovery achieved

• What was done to prevent recurrence

• Any reference documents used

(Smith, 2016)

Documentation is vital in the response to any attack because if no, or little, data is collected on the attack it is impossible to fully prevent future attacks.

Disaster Response Protocols

According to the Department of Homeland Security, there are only three common natural disasters to plan for in Kentucky. Those disasters are: Tornadoes, Thunder/Lighting Storms, and Floods. (Department of Homeland Security, 2009)

The most important asset in a Database Publishing Print shop is the database. Without the data no printing can occur. It is vital for the entire database to be securely backed up on a regular schedule and that backup should be securely backed up offsite. This ensures that all data can be recovered from any natural disasters; even if the database and/or the servers are fully destroyed. The backup schedule will depend on how often data is modified/added on the server. If the data

is not modified frequently then a daily onsite and a weekly offsite backup will be enough. However, if the data is modified frequently, then the backup schedules will be changed to a 12-hour onsite backup and daily offsite backup. The importance of the backups is to ensure that the data can be recovered. Even if the entire print shop is destroyed, the data from the backups can be used to continue the operations of the business. Depending on the data being printed, jobs can be outsourced to other print shops (or locations) temporally. This will ensure that the business continues until the print shop is restored.

Access Control Protocols

Access to the database is critical for some workers in the organization. However, not everyone needs access to the database or to all the data in the database. The first step in securing the data base is to ensure that only authorized users have physical access to the database. This will ensure that data cannot be copied directly from the server. No amount of computer security will stop a person who has physical access to the server from stealing data from the server to an external hard drive. After the server is secured physically by being in a locked room, then the next step is to secure the server virtually. According to Oracle, there are a few things that should be done to secure a database virtually:

- Place Controls for Privileged Accounts
- Place Controls for Maintenance
- Place Controls for Database Configuration
- Perform Run-time Privilege Analysis

(Oracle, Oracle Database Vault with Oracle Database 12c, 2015)

"Privileged user accounts are common place in all databases and are used by DBAs for daily tasks such as user management, performance tuning, replication, patching, backup and recovery, space management, startup and shutdown" (Oracle, Oracle Database Vault with Oracle Database 12c, 2015) These accounts should be guarded and monitored at all times. These accounts are often targeted by attackers due to their unimpeded access inside the database. Not only should the privileged accounts be analyzed but also every account to ensure no one have unauthorized access to the data.

"Periodic access to production environments by IT support staff or application DBAs is a common requirement and is typically associated with patching activity or diagnosing a performance issue. This task may typically involve recreating indexes and triggers, patching PL/SQL packages, or adding new tables, views, and other objects." (Oracle, Oracle Database Vault with Oracle Database 12c, 2015) If the database is not maintained, then no amount of security placed will prevent an attack using unpatched packages.

"Technical controls can prevent changes that could lead to an insecure database configuration, prevent configuration drift, reduce the possibility of audit findings, and improve compliance. Changes to database structures such as application tables and roles, privileged role grants, and ad hoc creation of new database accounts are just a few examples of configuration drift that can have serious consequences." (Oracle, Oracle Database Vault with Oracle Database 12c, 2015) Proper database security starts with proper setup. If the database is not setup with security in mind, then it will be open to attacks. SQL Command Controls, Account Management Controls, and Database Role Controls can be used to prevent unauthorized access. With all these tools combined every authorized personal should have access to the data that they need to perform their tasks.

The most important aspect of securing a database is ensuring that only authorized personal have access to the data within a database. This is not limited to only people who are outside of the company. It is important to terminate any accounts (logins and passwords) of any former employee. This will ensure that no former employee will be able to access the database or network; especially if the termination created the former employee to be disgruntled towards the company.

Method for Maintaining the Information Assurance Plan

The best way for any Information Assurance Plan to be successful is to ensure that every team member is fully knowledgeable on their part in the Plan. Training should not be a one-time event but rather a continuous thing to ensure that no one forgets their part and when changes are made to the plan then the information on the changes gets out to everyone in a timely manner. Another unfortunate part of Information Assurance is that it is not a set it up once and forget it. Each member of the Cybersecurity team should be actively involved in keeping up to date on known attacks and update the Information Assurance Plan as necessary. The Network Administrator should be actively involved in keeping the network secure and work with other team members to reduce any risked caused by human error. With training and actively looking to improve security as a top priority, then the Information Assurance Plan will reduce the risk of an attack to as low as possible. Failure to do so will result in exposing the data to high risks.

Conclusion

Data breaches are becoming a more common occurrence as technology is becoming a more critical part of our everyday lives. These breaches are a result of attackers gaining access to systems that are not fully secure. Sometimes these attacks can have lasting impacts for years. The only way to reduce the impact, or even prevent an attack, is to create, implement, and update an Information Assurance Plan. Without a plan there is no way to protect the company from any attack; whither it is from within or from the outside.

Works Cited

Cox, T. B. (2000, March). *White Paper: The role of the database administrator*. Retrieved from CompouterWeekly: http://www.computerweekly.com/feature/White-Paper-The-role-of-the-database-administrator

Department of Homeland Security, T. (2009, Jan 29). *KENTUCKY*. Retrieved from Ready: https://www.ready.gov/kentucky

Jacobs, S. (2016). *Engineering Information Security.* John Wiley & Sons, Inc.

Johnson, V. R. (2010, June 25). *Cybersecurity, Identity Theft, and the Limits of Tort Liability*. Retrieved from Harvard.edu: https://cyber.harvard.edu/cybersecurity/Cybersecurity,_Identity_Theft,_and_the_Limits_of_Tort_Liability

Microsoft. (2005, May). *How To: Protect From SQL Injection in ASP.NET*. Retrieved from Microsoft: https://msdn.microsoft.com/en-us/library/ff648339.aspx

NCSL. (2016, January 4). *SECURITY BREACH NOTIFICATION LAWS*. Retrieved from NCSL: http://www.lrc.ky.gov/Statutes/statute.aspx?id=43326

Oracle. (2010). *System Administration Guide*. Retrieved from Oracle: https://docs.oracle.com/cd/E19455-01/806-0916/6ja85398i/index.html

Oracle. (2015, May). *Oracle Database Vault with Oracle Database 12c*. Retrieved from Oracle: http://www.oracle.com/technetwork/database/options/database-vault/database-vault-wp-12c-1896142.pdf

Schulman, A. (2007, April 24). *Top 10 database attacks*. Retrieved from BCS: http://www.bcs.org/content/ConWebDoc/8852

Smith, J. (2016, Jan 29). *Cybersecurity – Incident Response*. Retrieved from National Cybersecurity Institute: http://www.nationalcybersecurityinstitute.org/government/cybersecurity-incident-response/

Symantec. (n.d.). *Assets, Threats and Vulnerabilities: Discovery and Analysis*. Retrieved from Symantec: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Risk_Management.pdf

TechTarget. (2006, August). *Key roles of database administrator*. Retrieved from TechTarget: http://searchoracle.techtarget.com/answer/Key-roles-of-database-administrator

U.S. Department of Justice, T. (2016, June 14). *Overview of The Privacy Act of 1974 (2015 Edition).* Retrieved from U.S. Department of Justice: https://www.justice.gov/opcl/overview-privacy-act-1974-2015-edition

Wikipedia. (2016, July 4). *Database publishing*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Database_publishing