Current Structure

The current structure of Implements of Honor puts every division on the same level and network. The senior vice president of each department has the same power as all the others. They all report to the CEO of the company. The CEO oversees making every decision for Implements of Honor. The six departments are Manufacturing, Design, IT, HR, Engineering and Quality, and Marketing.

NIST Special Publication 800-12 lists responsibilities of different roles in an organization. It states that the Chief Executive Officer (CEO) is responsible for everything in an organization's information security by doing tasks such as ensuring proper safeguards and training (Nieles et al., 2017).

Another role in NIST Special Publication 800-12 is the Chief Information Officer (CIO) who is responsible for allocating resources for protection, protecting systems with approved plans, and implementing an organization-wide information security plan. The CIO has the responsibility to ensure that information in the organization is protected (Nieles et al., 2017).

Implements of Honor have no CIO which is putting information at risk because the CEO does not have the responsibility of implementing a security plan that they ensure is followed. Changes should be made to the organizational structure to help ensure that information security is stronger in this organization.

McCumber Cube

The McCumber Cube has 3 sides that are Goals, States, and Safeguards. Each side has 3 sections that relate to the side.

The side of Goals includes confidentiality, integrity, and availability (Golovatenko, 2018). Implements of Honor are not following this as effectively as they should be.

Confidentiality is not being followed if designs are ending up on the market from other companies, meaning information is not being kept secret. This also means that data integrity is not there because if other companies are getting access to designs, they could be changing them without Implements of Honor realizing and they are not protected properly. Also, without proper security there is no guarantee that data is always available like it should be.

The next side of the McCumber cube is states. This describes the states of data that are in an organization. The states are data at rest, data in transit, and data that is being processed (Golovatenko, 2018). Data at rest and in transit should both always be encrypted so it cannot be read by people who are not supposed to have access to the data. Since other companies seem to have gained access to the designs that Implements of Honor has created, this means that there is a lack of encryption somewhere and data is not protected from outside the organization correctly. Processing data encryption is something that Implements of Honor might be able to do if they have the resources for that, but it is not necessary.

The final side of the McCumber cube is Safeguards. The sections of Safeguards are Policy and Procedures, Human Factors, and Technology (Golovatenko, 2018). Policies and procedures need to be implemented at Implements of Honor to ensure best practices are followed to keep systems safe and up to date. Human factors include what choices the employees make regarding data security and if they follow the policies and procedures that exist to keep data safe. Employees should be trained in the policies and what is and is not acceptable to the company. Technology includes where things are stored and how recent the technology is and if it is up to date. Implements of Honor needs to create clear policies that things will be updated every so often to ensure that there are no missing patches putting the organization at risk.

Cyber Kill Chain

The steps of the Cyber Kill Chain are reconnaissance, weaponization, delivery, exploitation, installation, command and control, actions on objective (Lockheed Martin, 2011). In relation to Implements of honor the Cyber Kill Chain is not able to be stopped as well as needed. Reconnaissance can be done with information that is found on the internet so that is not able to be stopped as much. Weaponization is where Implements of Honor could start to stop attacks. Weaponization is where the vector for attack is chosen so Implements of Honor could have policies to keep attack vectors tracked and secure. Delivery is how the method of attack gets into the network. Some methods of delivery include emails or USB sticks. This can be limited with good procedures in place. Installation is when the attack method installs software on the computer. For example, an employee of Implements of Honor plugs in an infected USB drive or clicks on a bad link that triggers malware to start installing. Command and control is where the attacker gathers and collects information about the company and the network to further exploit the company and get valuable information from them. Actions on objective is where the attacker gets information and spreads it to others like selling proprietary designs or using them to compete with Implements of Honor. Currently without a CIO there are no strong procedures in place to stop the Cyber Kill Chain at any step.

Proposed Changes

Changes should be made to the structure of this organization. These changes should involve a change in structure so there is a Chief Information Security Officer (CISO) that oversees keeping the networks and information safe. Changes should also be made to include strong secure hardware and policies that are enforced across the entire network that ensure there is no way for data to easily leave the network that is supposed to be confidential. There should be limits put in place so that there is no way for employees to access data outside of the data that they need to do their jobs.

The hardware and software that should be used include firewalls and antivirus/antimalware software. There should also be an IDS/IPS to scan the network for traffic from outside the network that does not belong. This could help stop attacks much earlier and would benefit the organization financially. One policy that needs to be put in place is to encrypt data that is at rest and keep it encrypted as it leaves the network sending it over encrypted channels to other networks that are known to be safe.

Each department of the organization should be given their own private network. Each network should have firewall rules to limit access between each department. This will help limit proprietary information from escaping the network again. This also helps ensure confidentiality is followed in the organization.

After making these changes to the organizational structure the McCumber cube will be more closely followed. On the Goals side, Confidentiality, Integrity, and Availability will be better as the organization becomes more secure and policies are put in place by the CISO to keep the organization safe. The states side will be better followed after data at rest and data in transit is encrypted so it cannot be deciphered by a bad guy that might get access to it unless they have the encryption key which will be kept secure. The safeguards side of the McCumber cube will be properly followed as policies are put into place and enforced by the CISO and the IT department. The technology will be patched regularly, and policies and practices will be clearly stated for when to do things like patching devices or limiting the things that a user is allowed to do.

There will also be more clear points where the Cyber Kill Chain is broken and the actions that will be taken if someone is trying to intrude on the Implements of Honor network to steal their data. Delivery methods could be limited with clear policies so that users cannot go to some websites or open links in emails for example. If that does not work, there should be software and hardware in place to help detect suspicious activity on the systems and policies for what to do to stop the activity and figure out where it is coming from. The cyber kill chain should be stopped before command and control help the attacker get information about Implements of Honor and their designs and data.

Risk Assessment Introduction

A risk assessment needs to be conducted on database servers used by Implements of Honor. Implements of Honor uses database servers to store their data. There are five servers that are running Microsoft SQL server 2016. The database servers meet the minimum requirements for Windows Server 2016. There is a firewall that protects the database servers. The databases do not have strong password requirements, which could be a risk. There is also no encryption or backups so data could outside sources can access data or data is lost if it gets destroyed.

Threat Sources

NIST SP 900-30 has tables that can be used to conduct a risk assessment. The first tables that will be used are found in Appendix D and they describe threat sources. The sources are described as adversarial, accidental, structural, or environmental. The tables also describe the adversary's capability and intent among other things (Joint Task Force Transformation Initiative, 2012, pp. 65-68).

One potential threat source found in these systems is a structural threat and it is a lack of an edge-of-network firewall. This is a failure of environmental controls. Without an edge-of-network firewall an attacker could get themselves into the network where they can learn more about the network and give themselves more privileges that allow attacks to happen. The privileges the attacker gives themselves might allow the attacker to get past the firewall that protects the databases and then cause harm to the databases by being able to log into the database and then do damage. For example, the attacker could steal data, change data, or install malicious software that destroys the database server.

Another adversarial threat source is the competition to Implements of Honor. The competition could want to steal design data from Implements of Honor and use the designs to give themselves a competitive advantage in the market and steal the clients of Implements of Honor for themselves. We know that designs have been found on the internet and it is possible these designs were put there by competitors or the competitors have found designs and used them for themselves in their designs.

Another potential threat source is structural and focuses on the IT equipment used for the database servers. One risk is the databases have the minimum specs required to run Windows Server 2016 which is the OS that the servers run on. The minimum specs are not the best idea to use because if the servers have usage that is above what is expected it could be too much for the hardware to handle and this could cause the servers to fail. The minimum requirements for the size of RAM that Windows Server 2016 needs are 512 mb (dknappettmsft & Jenks, 2021). The minimum requirements for Microsoft SQL Server 2016 include 1 GB (Ray et al., 2023). This will lead to problems with SQL server being able to run on the Windows Servers when the RAM the servers have is not enough to run the SQL servers. This could lead to problems with storing and accessing data that is saved on the servers.

Another problem with the equipment is they lack encryption. Data at rest should be encrypted to keep the data safe. If someone gets into the servers, they could be able to read and transfer design data, or personally identifiable information (PII) of the employees. They do not even need an encryption key to read the data or take it off the database and still be able to read it. Also, a lack of backups means the data is not safe in the event of a failure and would be costly to rebuild. According to a source found at fortinet.com fault tolerance is designed to allow systems to operate when problems occur. ("What is Fault Tolerance?," n.d.) This includes diversity, redundancy, and replication. Diversity involves using multiple systems or having devices in separate locations, or use of multiple power sources. Redundancy and replication would involve the use of backups of an OS and data to ensure that if data is lost, it can be recovered.

Appendix D also has tables to describe the threat levels of different threat sources. One potential adversary is a competing company trying to gain a competitive edge in the market. A potential adversary has moderate resources or a in terms of impact. The adversary, if they are a competing company, has high intent. The adversary has strong motivation to target Implements of Honor to gain data for themselves. Another potential adversary is an insider threat. Insiders are very capable of causing harm to systems or data protection. They could accidentally cause harm to the company, or they could be purposely bringing harm to the company by leaking design data for their own personal gain.

Threat Events

Appendix E of NIST SP 800-30 describes threat events. Both adversarial and non-adversarial threats are discussed. There is also a table to describe the relevance of the events (Joint Task Force Transformation Initiative, 2012, pp. 69-76).

One non-adversarial event that is anticipated is the mishandling of critical or sensitive information by authorized users. This is an example of an insider threat event that could happen. This could be on purpose or accidental. The users could put data out in the open by sharing it on the internet with or without meaning to or they could leave it out in the open where someone unauthorized could read the data. This is a possible or predicted threat event. Design data is on the black market, and it could have been put there by employees.

Another non-adversarial threat event to anticipate is incorrectly applied privilege settings. One example of this is the SA having administrator privileges without having an account that is properly configured. Other ways this could happen include users having more access than they need or using an account with high level access as their normal work account. This is a confirmed event because the SA does not have a properly configured password.

One adversarial event that should be anticipated is attackers giving themselves access that they should not have. They could do this by creating their own account that they escalate the privileges on, or they could use already existing accounts that have high privileges for their own gain. Attackers could also hide what they are doing on the systems if they can get logs and change them or if they look like a user that belongs to the systems. This is a threat event. Attackers could have gained unauthorized access and used that to put the design data on the internet that Implements of Honor has found.

Vulnerabilities

Appendix F in NIST SP 800-30 describes vulnerabilities that an organization could face. The severity of vulnerabilities is described in both quantitative and qualitative terms. Predisposing conditions are also described. (Joint Task Force Transformation Initiative, 2012, pp. 77-80)

One vulnerability that an organization could face is insecure passwords. Implements of Honor currently has this vulnerability, and it could have a very high impact on the organization. Very high impact on predisposing conditions. This vulnerability puts the entire organization at risk of losing data that is supposed to be secure. This relates to the information-related and technical predisposing conditions. The predisposing conditions have a very high impact in relation to the database servers. The use of insecure passwords being exploited will put the database servers at risk.

Another vulnerability that Implements of Honor faces is a lack of backups. This vulnerability has a very high impact. No backups mean there will be lost data if there is a failure or threat event of some kind. An attacker could exploit this by causing malware to be installed that corrupts the data saved to the database. There could also be a failure that comes from hardware failing. This could cause financial problems for the organization if data is lost and depending on what data is lost. The predisposing conditions this applies to are information-related and technical. This has a very high impact on predisposing conditions.

Likelihood of Occurrence

In Appendix G of NIST SP 800-30 there are tables that describe the likelihood that threats and vulnerabilities will occur. These tables are used to estimate the likelihood that an attack will happen and how much damage it could cause. (Joint Task Force Transformation Initiative, 2012, pp. 81-82)

A non-adversarial threat event that could occur is mishandling of critical information or sensitive information by users who are authorized to access data. There is a very high likelihood that users will mishandle data. When this does occur, there is a high likelihood that this will have an adverse impact on the company.

Another non-adversarial threat event that Implements of Honor could face is incorrect privilege settings. There is a very high likelihood that this will occur. Implements of Honor have already seen this occur and should expect to see this happen again. There is also a high likelihood of adverse effects to the company because of this threat.

Another threat event that could occur is an attacker or employee gains unauthorized access to the systems or data. There is a very high likelihood of this occurring. When this does occur, there will be major damage to Implements of Honor.

One vulnerability that exists is the improper use of strong passwords on IT systems owned by Implements of Honor. There is a very high likelihood of this occurring. Implements of Honor currently does not require strong passwords meaning this already occurs and will continue to occur. Brute forcing could find the passwords easily because they are not secure. When this does occur the chance of impact is very high.

A second vulnerability that is occurring already, so the likelihood is very high is no backups. If the storage or server fails and there is no way to access the data saved to the servers, the impact will be very high due to the fact large amounts of important data could be lost.

Impact

NIST SP 800-30 uses Appendix H to describe the impact of exercised threats and vulnerabilities. It describes the categories that could face harm. These categories include individuals, assets, operations, other organizations, and the nation. (Joint Task Force Transformation Initiative, 2012, pp. 83-85)

One threat that could occur is the mishandling of critical or sensitive information by authorized individuals. This could bring harm to assets or individuals. The assets could be harmed by unauthorized users getting knowledge of internal systems and finding ways to exploit them which could also cause harm to assets. Individuals are hurt by their PII getting exposed or attackers finding information that they could use to hurt the employees of Implements of Honor. Mishandling of data could result in a loss of money for the company. This has the potential to have a high impact. This could have a financially adverse effect on the company because competition could use the designs of Implements of Honor to gain advantage over Implements of Honor in the market causing Implements of Honor to lose money.

Another threat that could cause harm is the improper use of privilege settings. This could harm assets or operations. Without proper policies in place there are no clear guidelines on what privileges an employee should have. This leads to accounts having too many privileges. This brings potential harm to assets, operations, and individuals. Assets could be harmed by losing intellectual property that is saved on the systems. Someone could get in the database and delete or change important data that the company needs to operate properly. This leads to the potential in the loss of operations. If design data is no longer on the servers, then the company cannot build their products or improve on existing designs. This should have a high impact on the company.

Another threat event that could occur is a user gaining unauthorized access. If someone gains unauthorized access, they can bring grave damage by stealing data or destroying data. This brings harm to individuals, assets, and operations. An attacker could gain access to PII of employees and use that to harm the employees, the attacker could potentially get information that could be used for identity theft. The assets and operations can be harmed because the data could be destroyed, or systems could be damaged. An attacker could get access to the servers and potentially add malware or ransomware that makes the servers function incorrectly. They could also change or steal data. This threat has a very high impact.

One vulnerability that exists in the organization is there are no strong password policies. The use of weak passwords could cause harm to assets, individuals, or the operations of the company. Attackers could use this vulnerability to exploit the database servers and cause substantial amounts of impact. For example, they could steal PII or design data from the company. If they gain access to PII they could use the information to harm employees of the company. The attackers could also gain administrator access and lock employees out of the systems which will harm the assets and operations of Implements of Honor. This vulnerability has a very high impact with the potential to cause substantial amounts of financial damage to the company.

Another vulnerability that exists is a lack of backups of the servers that are storing company data. This will bring harm to assets and operations. The company is relying on the servers to remain functional and not have any failures or malware that makes the stored data inaccessible. The loss of information is also a loss of assets because assets include intellectual property which is what Implements of Honor's design data is. This has a very high impact on the company.

Risk of Operating

At this time, according to the table found at Appendix I-2 in NIST SP 800-30 the likelihood is very high and so is the potential impact meaning the risk level is very high. (Joint Task Force Transformation Initiative, 2012, p. 86). Adversaries could get in and cause severe damage to the organization or the databases could fail, and the resulting data also causes severe impact to the organization. Table I-3 describes very high risk as having multiple severe or catastrophic adverse effects on organization operations, assets, individuals, other organizations, or the Nation. (Joint Task Force Transformation Initiative, 2012, p. 87).

The current problems that Implements of Honor have in their database systems could fail in multiple ways and cause catastrophic damage to the assets and operations of Implements of Honor. There is also a risk of harm to individuals who work for Implements of Honor because they could have their personal information compromised.

Incident Response Plan Introduction

Incident response plans need to be created by the organization. Implements of Honor faces many threats to plan for. One threat that could bring a lot of harm to Implements of Honor is an insider threat. An insider threat is an employee or someone else who has access to the internal systems of Implements of Honor. They can harm a lot of systems including: Active Directory, PII databases, and design databases. An Incident Response Plan (IRP) needs to be created for each of these systems. Incident response examples from NIST, Michigan and California, and NIST SP 800-61 revision 2 have been used to create the incident response plans for Implements of Honor.

Some ways that an insider could bring harm and is a threat to the organization are either accidental or purposeful. An insider could click on a malicious link that downloads malware onto the device, this could be made worse if the user has elevated privileges. The malware could lock up systems, spy on systems, or take data from systems for example. A user could purposely install malware on systems if they are unhappy with the organization. An insider could also purposely steal company data and sell it for their personal gain.

NIST SP 800-61 describes incident response teams and plans. Implements of Honor is small so a central incident response team will be used in the organization. If needed, some of the incident responses may be outsourced. Due to the size of the company some members of the incident response teams will have other jobs but be asked to put those aside when an incident they need to respond to occurs.

The teams will need to be trained in how to respond before an incident occurs. There will be various methods of training on the various incidents that need responding to. This includes tabletop discussions, simulations, and complete walkthroughs of the plan with simulated incidents. Teams need training on what to look for, and who to contact about incidents. The company also needs to establish contacts with external sources like law enforcement, or customers to ensure there is compliance with laws and the plan works effectively.

Active Directory

One area to plan for is active directory. Active Directory (AD) is used to log into computer systems inside the company. AD tracks what employees can access, and what files exist in the system on the databases. An insider could stop AD from working by changing permissions, or locking accounts out, or changing group policy settings, or gain higher privileges than they should have and delete accounts. There are also accidental things an insider could do like opening attachments that have malware while logged in as a high privilege user, or an insecure password could be used. According to an article written by Forbes a study found that 80% of breaches stemmed from the misuse of privileged accounts. (Nayyar, 2021)

If AD went down, this could prevent the company from operating. This brings serious harm to the company's ability to function. If AD fails, it will need to be restored as soon as possible, or when the company starts losing money from AD being down.

Members of the Incident Response Team (IRT) for this incident include the CISO, members of the HR and IT departments. The CISO will be responsible for leading the incident response and they will make sure that the plan is followed correctly. The HR department will make sure that an employee gets the proper punishment if it was an insider, and they will help facilitate any future training that may be needed. The IT department will help restore the AD services, resetting passwords companywide, and making sure AD functions correctly without any issues.

Steps to the Incident Response Plan for Active Directory

1) Prepare for the incident. The CISO will be designated as the single point of contact for the team. They are the only source of truth for anything related to an incident. A primary and secondary method of communication needs to be established.

The databases will be backed up, allowing recovery of data that could be lost or corrupted when an incident occurs. Train employees of Implements of Honor on what an incident related to AD looks like. Tell them who to contact if something looks suspicious. Employees should contact the IT department who will look at AD and report to the CISO if there is suspicious activity. Teach about attack vectors including external media, email, improper usage, etc.

Employees need to understand how Active Directory normally functions and what they will see when Active Directory is used for their jobs. Active directory is used to sign in and grant users access to files and systems. Employees need to know who to contact if they cannot access things that they should be able to or if they cannot sign in. Employees who have access to the AD database should also know what it looks like if something looks wrong when they are working on AD. Also, there should be monitoring of AD so if changes are made, the company can be assured that those changes were meant to happen and investigate the event if they were not supposed to happen.

Take steps to ensure that the cause of an incident will be able to be found and systems can be recovered in a timely manner. One step to take is to regularly backup the AD databases. Take full systems backups once a week and incremental backups at the end of every day. Also, collect log files for activity on the AD databases. This will be helpful evidence when conducting a root cause analysis after an incident has occurred.

2) If an incident is detected or reported by an employee, the CISO will oversee contacting the appropriate members of the incident response team (IRT) and bringing them together to go to the next steps.

3) The IRT will examine the reported incident and see if it occurred. If it occurs, they will analyze how severe it is, and determine the next steps. When a response is started the IRT documentation should begin to ensure that all steps are taken, and everything is recorded for legal reasons and to improve the response plan. Document time of incident reported, what has happened, what has been affected, snapshots of the PII databases. Establish a chain of custody and document every step of the chain including: time of collection, who collected, storage location, what was collected, employees that have had the evidence and why. The incident should then be communicated to the proper internal and external parties. including employees, regulators, and customers.

4) The IRT will then follow steps to limit the damage done. The incident containment depends on many factors. These include potential damage, evidence preservation, service availability, and time to restore, if the AD server still works and is not putting other areas at risk then the company should not completely remove the AD server from the systems as that will prevent employees from working and prevent the company from making money. If other systems are at risk, or the incident is too severe to contain without completing taking AD offline then AD should be taken offline. If the time to restore costs the company more money than the incident could cost the company, then the company should not take AD offline if possible. Appropriate containment measures should be taken based on the severity of the incident.

5) After the cause has been identified, the IRT will take steps to eradicate the incident from AD databases and recover, bringing the AD databases back to an operational state. A root cause analysis will be conducted to determine the cause. This analysis determines if the cause was an insider, firewall controls, utility damage, firewall failure, etc. Find and remove artifacts that were left by the attacker in the incident. Ensure that all applications have the most recent update applied. If external IP addresses were involved in the incident null route those addresses so they no longer have access to the company network and can no longer do any harm,

6) After eradication comes recovery. Reimage the AD databases and other systems that were affected by the incident where possible. This will ensure that the system is clean and does not keep the cause of the incident on the systems. Restore data from their backups to ensure no data is lost and all systems function correctly. Test backups before restoring them to ensure the cause of the incident is not present on the backups as well. There will be changes made to the systems to prevent the incident from happening again. The IRT will document the changes that they made so the company can work better in future incidents or make changes to the baseline settings that they are using.

7) After the incident, a lessons learned meeting will be held and it will go over many things including what the incident was, if the procedures were adequate and followed in a timely manner, information that was needed, steps that didn't work or need to be added, actions to take to prevent this incident from happening again, resources that would improve response to the next incidents.

A gap analysis should be conducted to compare where the company stands to where they should be in their baseline settings of AD systems and user privileges. If it is found that they are not where they should be the company should make changes to improve review of settings and ensure that everything works correctly. There may be a need to improve what the expected settings and access privileges are on systems.

A root cause analysis will be conducted to determine what the actual cause of the incident was. This can happen throughout the response, but it should happen after the incident is resolved. Take documentation from the incident and review that to see if anything stands out. Look at the AD databases and related systems to identify the problem and ask questions about who was involved, what happened, where did the incident start, when did the incident happen, why did the incident happen. Use log files to help answer these questions. Analyzing these questions will be helpful in finding what caused the incident and steps to take to ensure this does not happen again.

8) After the incident is resolved and review is complete, communicate with everyone who has a stake in the company about the incident and lessons that the company learned and steps that will be taken to improve going forward.

Personally Identifiable Information Databases

Another area of the company that is important to have a plan for is databases that hold personally identifiable information (PII). An insider could gain access to databases that store PII and exfiltrate the data for their own personal gain, or they could cause the database to become unsecure, or have the database lose PII records that they hold.

If the databases that store potentially identifiable information (PII) have an incident this could bring harm to employees. Employees could have their identity stolen, their lives be put at risk, their home address could be taken which could harm the employees, or if PII is lost the employees could lose trust with the company and its ability to store and protect the personal information of employees, or potential customers.

Members of the Incident Response Team (IRT) for this incident include the CISO, members of the HR and IT departments. The CISO will oversee the incident response and make sure that the plan is followed correctly. The IT departments will help restore and secure the databases that hold PII. The HR department will have to be involved in dealing with employees who potentially had their data lost by the company. The HR department will also ensure that the functions they use on the PII databases are working correctly again. The company will need to consult someone for legal issues that could come from the PII databases having an incident.

Steps to the Incident Response Plan for Personally Identifiable Information Databases

1) Prepare for the incident. The CISO will be designated as the single point of contact for the team. They are the only source of truth for anything related to an incident. A primary and secondary method of communication needs to be established.

Train employees of Implements of Honor on what an incident related to the PII databases looks like. They will need to know to report if any employee is doing suspicious things with the PII databases. The PII databases will be monitored closely for unusual activity to detect an incident as soon as possible. If something is suspicious an employee will report to the proper employees that something seems suspicious on the PII databases. The databases will be backed up, allowing recovery of data that could be lost or corrupted when an incident occurs.

Employees need to know about the PII databases and what they look like when functioning normally and what to do if something goes wrong. The PII databases store information about the employees that the company needs and will not be accessible by most employees in the company. HR is the main department that will be using the PII databases. They will need to ensure that employees' data is entered correctly and make updates as needed. There should be settings on the database to detect suspicious activity and report to the correct members of the IRT. If employees are not able to do something on the databases, they should also be able to notify the proper members of the IRT.

Take steps to ensure that the cause of an incident will be able to be found and systems can be recovered in a timely manner. One step to take is to regularly backup the PII databases. Take full systems backups once a week and incremental backups at the end of every day. Also, collect log files for activity on the PII databases. This will be helpful evidence when conducting a root cause analysis after an incident has occurred.

2) If an incident is detected or reported by an employee, the CISO will oversee contacting the appropriate members of the incident response team (IRT) and bringing them together to go to the next steps.

3) The IRT will examine the reported incident and see if it occurred. If it occurred, they will analyze how severe it is and determine the next steps. When a response to a PII incident is started the IRT should begin to document everything relevant to the incident. This includes time of incident reported, what has happened, what has been affected, snapshots of the PII databases. Establish a chain of custody documenting every step of the chain including: time of collection, who collected, storage location, what was collected, employees that have had the evidence and why. After an incident is found and documentation started, communicate the occurrence of the incident to the proper internal and external parties including employees, regulators, and customers.

4) The IRT will then follow steps to contain the incident to limit the damage done. The first thing to do will be determine the level of containment which depends on multiple factors. These include potential damage, evidence preservation, service availability, and restoration time.

Containment also includes the other things the incident puts at risk, and how much time it will take to restore, or how much money the business will lose. The PII server should not affect normal operations so the business should be able to function as normal if the PII server goes offline. If the PII server puts other systems on the network at risk, it should be taken offline. If the PII server is potentially exposing customer or employee data to external parties, then the system should be taken offline. There could be legal problems with loss or exposure of PII so the company should quickly contain the incident to limit how much PII could be exposed if that is happening.

5) After the cause has been identified, the IRT will take steps to eradicate the incident from PII databases and recover, bringing the PII databases back to an operational state. A root cause analysis will be conducted to determine the cause. This analysis determines if the cause was an insider, firewall controls, utility damage, firewall failure, etc. Find and remove artifacts that were left by the attacker in the incident. Ensure that all applications have the most recent update applied. If external IP addresses were involved in the incident, null route those addresses so they no longer have access to the company network and can no longer do any harm.

6) After eradication comes recovery. Reimage the databases if possible, to remove any artifacts or chance of leaving the cause of the incident on the databases. The backups of PII will be used to restore the database systems to an operational state. Before applying the backups, use a test environment to check that the cause of the incident does not exist on the backups. If it does exist, then restoring the backups will cause the incident to come back. The IRT will document the changes that they made so the company can work better in future incidents or make changes to the baseline settings that they are using.

7) After the incident, a lessons learned meeting will be held and it will go over many things including what the incident was, if the procedures were adequate and followed in a timely manner, information that was needed, steps that didn't work or need to be added, actions to take to prevent this incident from happening again, resources that would improve response to the next incidents.

A gap analysis should be conducted to compare where the company stands to where they should be in their baseline settings of systems and user privileges. If it is found that the PII databases are not where they should be, then the company should make changes to improve review of settings and ensure that everything works correctly. There may be a need to improve what the expected settings and access privileges are on systems.

A root cause analysis will be conducted to determine what the actual cause of the incident was. This can happen throughout the response, but it should happen after the incident is resolved. Take documentation from the incident and review that to see if anything stands out. Look at the PII databases to identify the problem and ask questions about who was involved, what happened, where did the incident start, when did the incident happen, why did the incident happen. Analyzing these questions will be helpful in finding what caused the incident and steps to take to ensure this does not happen again. Use log files to find the cause to ensure the cause is resolved and will not happen again.

8) After the incident is resolved and review is complete, communicate with everyone who has a stake in the company about the incident and lessons that the company learned and steps that will be taken to improve going forward.

Design Databases

Design databases are another area that Implements of Honor needs to have a plan for. Databases are used to hold design information. If these get hacked the company's ability to make money is at risk. An insider could get into these databases and make copies of the designs to give to other companies or use for other personal gains, destroy, or change the design data to make it unusable for the company, or leak them onto the internet where they can be picked up by competitors.

This could bring financial harm to the company if the company loses customers to competition or is unable to complete the manufacturing of their product because the design data is unusable, so the employees have no good designs to manufacture their designs. This could also hurt the company's ability to improve existing products when they have no copies of designs that are reliably accurate.

Members of the IRT include the CISO, members of the manufacturing department, and members of the design department, and HR. The CISO will lead the incident response and bring members from different teams together. The design team will help ensure that backups are restored correctly. The manufacturing department will ensure that things are restored to where they are able to manufacture products again. HR will be responsible for ensuring that the company follows policies in punishing employees for the harm they might have caused.

Steps to the Incident Response Plan for Design Databases

1) Prepare for the incident. The CISO will be designated as the single point of contact for the team. They are the only source of truth for anything related to an incident. A primary and secondary method of communication needs to be established.

Train employees of Implements of Honor on what an incident related to the design databases looks like. They will need to know to report if any employee is doing suspicious things with the design databases or the designs themselves. The design databases will be monitored closely for unusual activities including exfiltration of data from the databases to an external device, or who is modifying data in the databases to detect an incident as soon as possible. Prepare systems by putting monitoring on the databases to notify of activity and detect suspicious activity. The databases will be backed up, allowing recovery of data that could be lost or corrupted when an incident occurs.

Teach employees how to recognize when the design databases are not working correctly or recognize if designs are modified or missing unexpectedly. Tell employees who to contact when suspicious activity is found on the databases, or if something is suspicious about the designs.

Take steps to ensure that the cause of an incident will be able to be found and systems can be recovered in a timely manner. One step to take is to regularly backup the design databases. Take full systems backups one a week and incremental backups at the end of every day. Also, collect log files for activity on the design databases. This will be helpful evidence when conducting a root cause analysis after an incident has occurred.

2) If an incident is detected or reported by an employee, report to the proper departments, including the CISO. The CISO will oversee contacting the appropriate members of the incident response team (IRT) and bringing them together to go to the next steps.

3) The IRT will examine the reported incident and see if it occurred. If it occurred, they will analyze how severe it is and determine the next steps. Before analyzing documentation of the incident will begin. Documentation includes: time incident was reported, what the incident is, what the incident affects, and snapshots taken of design databases. A chain of custody needs to be established documenting every step of the chain including: time of collection, who collected, storage location, what was collected, employees that have had the evidence and why. Communicate incidents to proper parties, both external and internal.

4) The IRT will then follow steps to contain the incident to limit the damage done. The next step that will occur is containing the incident. Full or partial containment depends on factors including: potential damage, evidence preservation, service availability, and restoration time.

Containment also depends on factors including: if the company can operate without the design databases, time to restore, risk to company to keep databases running, cost to go without databases. If the design data is being exfiltrated to other companies, the database should be taken offline which might prevent the company from operating but the cost of allowing data to continue to escape is bad. If design data has been changed the company could keep the database up, just isolate the design data that has been affected, so the company can still make some money and have employees completing their work.

5) After the cause has been identified and contained, the IRT will take steps to remove the cause from the design databases and recover the databases to their normal operational state. A root cause analysis will be conducted to determine the cause. This analysis determines if the cause was an insider, firewall controls, utility damage, firewall failure, etc. Find and remove artifacts that were left by the attacker in the incident. Ensure that all applications have the most recent update applied. If external IP addresses were involved in the incident null route those addresses so they no longer have access to the company network and can no longer do any harm,

6) After eradication comes recovery. The design databases will get a fresh image on them, if possible, to ensure the incident cause no longer exists. After testing the backups to ensure the cause of the incident is not on the backups the IRT will restore backups to ensure data integrity on the design database is followed and they will make changes to the database to prevent the incident from reoccurring. Changes that are made to prevent a future incident will be documented.

7) After the incident, a lessons learned meeting will be held and it will go over many things including what the incident was, if the procedures were adequate and followed in a timely manner, information that was needed, steps that didn’t work or need to be added, actions to take to prevent this incident from happening again, resources that would improve response to the next incidents.

A gap analysis should be conducted to compare where the company stands to where they should be in their baseline settings of design database systems and user privileges. If it is found that they are not where they should be the company should make changes to improve review of settings and ensure that everything works correctly. There may be a need to improve what the expected settings and access privileges are on systems.

A root cause analysis will be conducted to determine what the actual cause of the incident was. This can happen throughout the response, but it should happen after the incident is resolved. Take documentation from the incident and review that to see if anything stands out. Look at the design databases to identify the problem and ask questions about who was involved, what happened, where did the incident start, when did the incident happen, why did the incident happen. Analyzing these questions will be helpful in finding what caused the incident and steps to take to ensure this does not happen again. Use log files to answer these questions and find the root cause of the incident.

8) After the incident is resolved and review is complete, communicate with everyone who has a stake in the company about the incident and lessons that the company learned and steps that will be taken to improve going forward.

References

CA Dept of Technology. (n.d.). Incident Response Plan Example. https://cdt.ca.gov/wp-content/uploads/2017/03/templates_incident_response_plan.doc

Cichonski , P., Millar , T., Grance, T., & Scarfone, K. (2012, August 6). Computer Security Incident Handling Guide - NIST. COMPUTER SECURITY RESOURCE CENTER. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

Cyber Kill Chain®. Lockheed Martin. (2011). https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Cynet. (2023, November 7). *NIST Incident Response*. Cynet. https://www.cynet.com/incident-response/nist-incident-response/#:~:text=Incident%20response%20is%20a%20structured,%3B%20and%20post%2Dincident%20activity.

dknappettmsft, & Jenks, A. (2021, December 12). *Hardware requirements for windows server*. Hardware requirements for Windows Server. https://learn.microsoft.com/en-us/windows-server/get-started/hardware-requirements

Golovatenko, I. (2018, December 13). *The Three Dimensions of the Cybersecurity Cube*. Swan Software Solutions. https://new.swansoftwaresolutions.com/the-three-dimensions-of-the-cybersecurity-cube/

JOINT TASK FORCE TRANSFORMATION INITIATIVE. (2012, September). Guide for Conducting Risk Assessments - NIST. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Michigan State Police Criminal Justice Information Center . (n.d.). Example incident response plan - state of Michigan. Example Incident Response Plan .

https://www.michigan.gov/-/media/Project/Websites/msp/cjic/pdfs6/Example_Incident_Response_Policy.pdf?rev=4bf335b6d1344226a92a0947bc8688ec

Nayyar, S. (2021, August 4). Council post: How to stop risky activity on privileged accounts. Forbes. https://www.forbes.com/sites/forbestechcouncil/2021/08/04/how-to-stop-risky-activity-on-privileged-accounts/?sh=69ed8e6d50fa

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017, June). *Michael Nieles Kelley Dempsey Victoria Yan Pillitteri - NIST*. NIST. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

Ray, M., West, R., McClister, C., Roth, J., Jenks, A., Konidena, R., HaiyingYu, Assaf, W., cawrites, Coulter, D., Sabotta, Guyer, C., Lopes, P., Agarwal, S., Schonning, N., Mabee, D., Ersan, E., Lahoud, P., Wells, J., … Kirsch, J. (2023, August 24). *SQL Server 2016 & 2017: Hardware & Software Requirements - SQL server*. SQL Server 2016 & 2017: Hardware & software requirements - SQL Server | Microsoft Learn. https://learn.microsoft.com/en-us/sql/sql-server/install/hardware-and-software-requirements-for-installing-sql-server?view=sql-server-ver16

What is fault tolerance?: Creating a fault-tolerant system. Fortinet. (n.d.). https://www.fortinet.com/resources/cyberglossary/fault-tolerance#:~:text=Fault%20tolerance%20is%20a%20process,operating%20despite%20failures%20or%20malfunctions.