Monistax Risk and Compliance Assessment Report

By Darius Richardson

Contents

I. Risk Assessment

1. Operational Risk Scenarios

The table below lists 10 potential risks of the Software as a Service (SaaS) software solution.'Knowing' column explains how the attacker could search for information on the solution. 'Entering' column explains the techniques that the attacker could use to get in. 'Finding' column explains how the attacker could search for the information that interests them and 'Exploiting' explains how the attacker could use that information.

RISK NO.	KNOWING	ENTERING	FINDING	EXPLOITING
1	Social engineering via phishing emails	Password theft through phishing	Accessing confidential files	Data leakage
2	Cryptovirology malware via Ransomware software	Personal data breach through Ransomware	Accessing personal Information	Financial gain
3	Malware via Worm attack	PeoplePro Suite information system unavailable via Worm attack	Gain access to PeoplePro Suite information system	Service disruption
4	Supply chain via Trojan horse attack	A supplier access Employee self-service portal via Trojan horse	Gain access to payment statements	Financial fraud
5	Distributed Denial of Service (DDoS) via web server requests	Website tempered through malware	Gain access to PeoplePro Suite	Service disruption
6	Man-in-the-Middle via WiFi Eavesdropping on wireless networks	Employee's data modified through wireless networks	Accessing Employee's Payslip and pay details	banking information
7	Encryption via Encryption layer	Data encrypted by attacker through ransomware	Data accessed and converted into read-only format	Payment of a ransom
8	Drive-by attack via malicious scripts	Install Malware through website	Access sensitive information	Cyber espionage
9	Spoofing via email	Send an email using a false email address	Access login details	Obtain data from PeoplePro Suite Systems Solution
10	Structured Query Language (SQL) Injection	Database breached via SQL Injection	Accessing database	Modify database

2. Likelihood of Operational Scenarios

The table below shows the plausible attack path and the likelihood of success. The strategic attack path column explains the sequence of steps and techniques that the attacker would take to exploit the vulnerability and the overall likelihood column states the attacker's chance of success and their likelihood of going through the attack path.

Improbable (likelihood score 1) means risk never appear or unlikely to happen, conceivable (likelihood Score 2) means the risk is possible but not expected under normal circumstances, frequent (likelihood score 3) means has a fair chance of occurring and very frequent (likelihood score 4) means the risk is guaranteed to happen.

Scenario	Strategic attack path	Overall likelihood
1	The attacker used a botnet to perform a Distributed Denial-of-Service (DDoS) attack on the solution.	2 - Conceivable
2	The attacker would send an email to an Employee to download an antivirus software that is actually a Ransomware software on the solution.	1 - Improbable
3	The attacker uses Malware behind the scenes to make a Worm attack on Monistax's information system.	2 - Conceivable
4	The attacker gives Employee a downloadable file to access self-service portal.	1 - Improbable
5	The attacker uses Distributed Denial of Service via web server requests to make Monistax's Information system unavailable to use.	2 - Conceivable
6	The attacker listens to ongoing network communications to modify Employee's data.	2 - Conceivable
7	The attacker add an encryption layer by using an encryption key to encrypt data for ransom.	2 - Conceivable
8	The attacker creates compromised website from malicious code that the Employee visits.	1 - Improbable
9	The attacker sends an email to the Employee to ask to change the password to security reasons.	2 - Conceivable
10	An attacker uses SQL Injection admin' OR '1'='1 in login and enters a random password but still login as admin.	4 - Very frequent

3. Impact of Operational Scenarios

The table provides a description of each risk on how it would impact the company and the Impact scores for each risk scenario.

A minor impact (impact score 1) means the consequences are very minor which won't cause significant disruption, a moderate score (impact score 2) means the impact is noticeable but is manageable without big disruptions, a high impact (impact score 3) is significant and requires management without big disruptions and a severe Impact (impact score 4) can cause critical consequences.

Scenario	Impact description	Impact score
1	The impact would mean employee workload would increase and a condemnation or fine for the company.	4 - Severe impact
2	The impact would mean adaptation of work organisation needed.	1 - Minor impact
3	The impact would mean Employee's data is compromised from the system.	3 - High impact
4	The impact would be limited adaption of work organisation needed.	2 - Moderate Impact
5	The impact would be Civil condemnation of an Employee.	4 - Severe impact
6	The impact would cause a complaint from an Employee.	2 - Moderate Impact
7	The impact would mean data cannot be accessed and could potential cause loss of money unless action is taken.	2 - Moderate Impact
8	The impact would cause disruptions to an Employees work.	2 - Moderate Impact
9	The impact would mean attacker will be able to login to access private data such as bank details would could cause financial loss.	2 - Moderate Impact
10	The impact would mean attacker has access the database which would cause serious damage to the organisation.	4 - Severe impact

4. Risk Severity and Acceptance

The Risk Severity and Acceptance table shows the matrix scores and the risk acceptance levels for each risk scenario.

The matrix score between 1, 2 or 3 is a low matrix score which means it a harmless risk but still needs to be reported, 4,6,8 or 9 is medium-high impact which means to pay attention to risk and requires action and 12 or 16 is high impact which means likely to happen and requires prompt action. The matrix score is calculated using a risk matrix model. To calculate the matrix score is impact x likelihood.

The weak risk acceptance level means that little or no action needs to be taken, the average risk acceptance level means that the risk is noted but is not severe to take action straightaway and the high level risk acceptance level means action needs to be taken straightaway as it is urgent.

Scenario	Severity (matrix score)	Risk acceptance level
1	8	Average – Tolerable under control
2	1	Weak – Acceptable
3	6	Average – Tolerable under control
4	2	Weak – Acceptable
5	8	Average – Tolerable under control
6	4	Average – Tolerable under control
7	4	Average – Tolerable under control
8	2	Weak – Acceptable
9	4	Average – Tolerable under control
10	16	High – Unacceptable

5. Risk Prioritization

The table below is the order of risk scenarios but in order of priority from highest to lowest. The order of the risk scenarios are based on the matrix scores.

Scenarios in order of priority (highest -> lowest priority)
The attacker uses SQL Injection admin' OR '1'='1 in login and enters a random password but still login as admin.
The attacker used a botnet to perform a Distributed Denial-of-Service (DDoS) attack on the solution.
The attacker uses Distributed Denial of Service via web server requests to make Monistax's Information system unavailable to use.
The attacker uses Malware behind the scenes to make a Worm attack on Monistax's information system.
The attacker add an encryption layer by using an encryption key to encrypt data for ransom.
The attacker listens to ongoing network communications to modify Employee's data.
The attacker sends an email to the Employee to ask to change the password to security reasons.
The attacker gives Employee a downloadable file to access self-service portal.
The attacker creates compromised website from malicious code that the Employee visits.
The attacker would send an email to an Employee to download an antivirus software that is actually a Ransomware software on the solution.

6. Recommended Actions

For each of the risk scenario's, the table explains the security measures such as the actions to take, what risk it solves and who is responsible for monitoring and resolving those risks. As well as, explaining the difficulty of implementing the security measure, the cost and complexity of implementing, how soon to take action when a risk emerge despite the security measures put in place and the time frame to implement the security measures.

Risk scenario	Security measure	Difficulties for implementation	Timeframe
1	The action to take to minimise the Distributed Denial-of-Service (DDoS) attack is by modifying the Domain name server records which provide temporary relief. The person responsible for this is the DDoS specialist.	The level of difficulty implementing and modifying the Domain name system (DNS) records depends on the specific changes that are made. For example, changes that are made through the domain registrar's control panel is easy whereas setting up a DNS security extensions is difficult. Modifying the DNS records is not expensive and the complexity depends on what specific changes need to be made. The action should be taken straight-away to make sure that the risk doesn't escalate.	Mid-term
2	The organisation is responsible for making sure that phishing emails are not being received by employee. In case phishing emails get through its important the employee can detect phishing emails.	There is no cost and is not complex. The best way to recognise a phishing attack is to look at the public domain. In the emails themselves, phishing emails usually will not state the name of the Employee. What action needs to take place is Employee's need to undergo employee training so that they are aware of the risks of phishing. Make sure to delete the phishing email to prevent human error by accidentally clicking on the link from email.	Short-term

3	What actions to take when dealing with a worm attack is disconnect from the network, run a full system scan, update security software, delete infected files and patch vulnerabilities. This helps mitigate the spread of malware and prevent further worm attacks from happening.	What needs to be implemented to resolve the attack is to scan and clean all affected systems and strengthen the security measure to prevent future attacks. The cost of the impact of the worm attack can vary depending on the seriousness of the impact such as resulting in system repair and data recovery costs. The action needs to be taken as soon as possible. The Information Technology Security team within the company are primarily responsible for detecting, mitigating and containing worm attacks. Employee's need to take training regarding worm attacks to be prepared for one as they play a part in being responsible for dealing with a worm attack such as knowing who to report to when it happens.	Mid-term
4	When it comes to attacker giving an Employee a downloadable file, no action is required but to alert the Cybersecurity experts about it. It is important to make sure work contact details such as email addresses are kept private to prevent attackers from sending a harmful file to an Employee.	No implementation is required, as long as the file was not opened. No cost will be loss for the company. The complexity can be quite difficult because of the network architecture and trying to maintain the security. Employees would need training to be able to detect a file as whether it is save to download.	Short-term

5	To deal with a DDoS attack on a web server is to quickly use traffic analytics tools to confirm the attack and find unusual traffic patterns due to DDoS. These solves the risks of malicious traffic and keep the server running. The organisation is responsible for Distributed of Denial Service attacks but the Network or IT security team are primary responsible for monitoring and responding to those attacks. Those who are responsible are the Internet Service Providers but within the organisation the IT department owns the relationship with the Internet Service Providers and the IT Department would need to leap into action should an attack materialise.	The difficulty of implementing Distributed Denial of Service protection is difficulty due to the complexity of the attacks and the scalability of large volumes of traffic. The cost of implementing is expensive. This includes costs for hardware, software and services, as well as ongoing maintenance and updates. The action should be taken immediately.	Long-term
6	The action to take to solve the man in the middle via eavesdropping is to make sure that the operating system is up to date to eliminate vulnerabilities and in case it does happen, disconnect from network to prevent further data interception. Employee is responsible for making sure that the operating system is up to date in regards to disconnecting the network. The network administrator or IT manager would contact the Internet service providers (ISP) for further information on disconnecting the network. The IT team would be likely monitor the installation of the system and software updates to make sure that employees remain compliant.	Updating the operating system is not difficult to do and does not cost anything to so. It’s best to update the operating system as soon as possible.	Short-term

7	The action to make is to use network monitoring tools to find unusual encryption activities and isolate the systems affected from the network to prevent the attack from spreading further. The person responsible for dealing with this risk is the Incident Response Teams to handle the threats.	Isolating the systems affected from the network is challenging due to several factors such as complex network structures and maintaining they security. The cost to isolate the systems affected can vary depending on the size of the network. The action should be taken straight away to prevent further impact to the network.	Long-term
8	To fix the issue of suspicious websites is to run a full system scan and to reset the browser settings. The employee is responsible for making sure to check the website is real and safe.	Running a full system scan is straight forward but can be time consuming depending on the large number of files and can cause the system performance to be slow while scanning due to scan using a lot of system resources. The cost to running a full scan typically ranges from £995 to £2250. The action should be taken as soon as possible.	Long-term
9	Best action is to check email headers and report suspicious emails. This helps in identifying which emails are spoofing. Employee's are responsible for making sure that they do not click on any links from suspicious emails. It is best to implement email authentication protocols.	Implementing email authentication protocols can be challenging because of multiple DNS records and understanding the nuance of each protocol. It is critical to prevent spreading Employee's information where attackers can use them. No cost is required and there is no complexity. Actions should be taken very soon to prevent more emails from coming. Employees need to be educated when comes to spoofing so that they are aware of the risks that can be appear and what to do about it.	Long-term

10	What action needs to be taken is to implement input validation to restrict types of characters that are entered and use stored procedures instead of dynamic SQL. This will prevent attacker from using admin'OR'1'='1. The security team and database administration are responsible of resolving the risk of SQL injection.	A cost would be development costs when providing secure coding practices. The action should be taken straight away to prevent hackers from access sensitive data. There is no cost for making modifications to the Structured Query Language (SQL) and complexity is difficult depending on Development and maintenance. This can be done by using stored procedures, input validation and Object-Relational Mapping (ORM). The best way to prevent SQL injections is to filter the database by filtering any input from users so that it is clean before putting into the database. Make sure the database can be accessed only by authorised personal.	Mid-term

7. Conclusion

In conclusion, after careful consideration of the risks, impacts, likelihood of those risks and what action needs to be taken before or after the risks are happening, that the company should adopt the SaaS software solution. Despite, the significant damage that can be caused as a result of the risks for the solution as well as the long-term time frame it would take to implement most of the security measures by implementing the security solutions before any potential attacks it would prevent or minimise the significant damage and costs from happening to the company.

The actions that the company needs to take when implementing the solution assigning responsibilities to individuals on specific attributes of the solution so that when the possibility (despite implementing the security measures) that a risk has been made it's way through, it will help to quickly stop the risk before it escalates further. It is also best to do a full security scan on the SaaS software solution to evaluate the vulnerabilities and to make sure that the features work as intended.

II. Compliance Assessment

1. Discrepancies

A discrepancy that was found is the database can be easily be accessed by using the SQL Injection whereas in the policy it mentions the importance of keeping data secure and safe from unauthorised access.

Another Discrepancy is that in the solution and description documentation it does not mention two-factor authentication whereas In Article 7.3 – Identity and access management, the policy mentions two-factor authentication as an extra layer of security rather than just username and password to gain access.

A third discrepancy is that in the termination and refund policy in the termination and data disposal that it will be deactivated or deleted without delay whereas in the termination and refund policy in the terms and conditions the client retains access to their data for a specified period.

2. Source of Discrepancies

In the table below, are the discrepancies for the PeoplePro Suite solution and the company policy.

Discrepancy	Source: solution or policy?
Being able to connect as the admin user on database without knowing the password by using admin'OR'1'='1 as a SQL injection.	PeoplePro Suite solution.
Not including two-factor authentication is a risk as makes it more likely for hackers to access solution.	PeoplePro Suite solution.
By not giving an exact date and time of notice when the termination will happen to third parties, they will not know when to collect the data that third party might want to keep.	Monistax Third-Party Supplier Security Policy.

3. Recommendations: Solution

In the table below, are the discrepancies for the solution such as the flaw within the solution, the action to take to fix the flaw and to justify the decision to take that action.

Flaw	Action	Justification
SQL Injection.	Use parameterised queries to to stop attackers from using admin'OR'1'='1 SQL injection.	This will prevent attacker from accessing database.
No two-way authentication.	Implement a two-way authentication to the service portal.	This will help provide extra protection to the Service Login Portal to reduce hackers chance from getting access to personal information.

4. Recommendations: Updates or Corrections to Policy

In the table below, is the discrepancy for the company policy, what modification to make in policy document and to justify why it is necessary to do so.

Section of policy or document to be modified	Suggested Modification	Justification
In the Monistax Third-Party Supplier Security Policy.	Make modifications in the Termination and Data Disposal section by providing an exact date and time of termination of data.	This will let the third parties know when termination will happen to help better prepare them to save any personal data they may want to keep.

Glossary

Term	Definition
Breached	Someone’s security has been broken into.
Cryptovirology Malware	A harmful software that uses encryption to lock up data or to take control of a computer.
Cyber Espionage	When someone uses the internet to privately steal information from a company.
Data Leakage	When sensitive information unexpectedly gets out to people who shouldn’t have it.
Database	A collection of structured data that stores and organises information so it can be easily found and used later.
Distributed Denial-of a Service (DDoS)	It’s a type of cyberattack where computers work together to overwhelm an online service to cause much traffic causing slow down or crash.
Domain Name System (DNS)	It reaches websites by translating the easy-to-remember website into IP addresses.
Encryption	Locking information with a secret code so that only someone with the right key can read it.
Encryption Layer	Is an extra shield around information which adds a layer of protection by locking data with a secret code so people who have authorisation can access the data.
Financial Gain	When a hacker’s earns money when using someone's data that has been stolen.
Incident Response	The process of handling and managing unpredicted problems or attacks.
Information Technology Security Team	A group of experts who secure a company’s computer system and data from hackers.
Internet Service Providers (ISP)	Provide companies the connection that businesses need to access the internet.
Information Technology Department	Is a team in a company that takes care of all technology such as computers, networks and support to make sure everything runs correctly.
Malicious Scripts	Harmful scripts pieces of code written to damage or steal with a computer.
Malware	A harmful software made to damage computers and networks.
Man-in-the-Middle	It’s a type of attack where someone secretly intercepts and potentially alters the communication between two people or systems.
Network	Connected devices such as computers that can communicate with each other.

Object-Relational Mapping (ORM)	A way to connect with data within a database. This is used for save, retrieve and manage data by permitting developers to write code that represents data as objects.
Phishing Emails	A deceptive message that looks like it's from a real source like a bank but is really a trick to take personal information.
Ransomware	A type of malicious software that locks files making them inaccessible unless payments is made to unlock files.
Risks	Potential problem or dangers that could cause harm or loss.
Security Measures	Actions to take to protect something from harm.
Security Policy	A set of rules and guidelines that outlines how to protect a company's information and systems.
Service Disruption	When something goes wrong and stops a service from working correctly.
Software as a Service (SaaS)	A software over the internet that does not require installing it on a computer instead it is accesses through web browser.
Spoofing	When someone acts to be someone they're not to trick you.
Structured Query Language (SQL)	A language used to manage and work with databases. It creates, update, retrieve and delete data within a database.
Supply Chain	A network of companies involved in creating and sending technology products or services.
Systems	Groups related to parts that work together to complete a similar goal.
Third Party	Someone who is not directly involved in the business but stills affects the business such as someone using a business's service.
Trojan Horse Attack	Malicious software pretends to be something harmless or useful to trick a user into installing it.
Two-way Authentication	A security process where it requires two different methods to verify a user's identity.
Vulnerabilities	A weaknesses or flaws in a system or software that can be use by attackers to cause gain access.
Web Server Request	When a computer asks a website to show a page.
WiFi Eavesdropping	Someone secretly listens in on a Wi-Fi network to capture information.
Worm Attack	When a malicious software spreads itself across computers or networks without requiring assistance from users.