
Play your favorite music
Order pizza from Domino's
Voice control your home
Request rides from Uber
Find local businesses
Hacker story : Amazon Alexa

RISK

$$\text{Risk} = \frac{\text{Assets(A)* Threat(T)*Vulnerability(V)}}{\text{Security measures (SM)}}$$

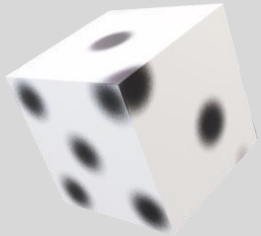
Where Impact (I) is hidden in the assets

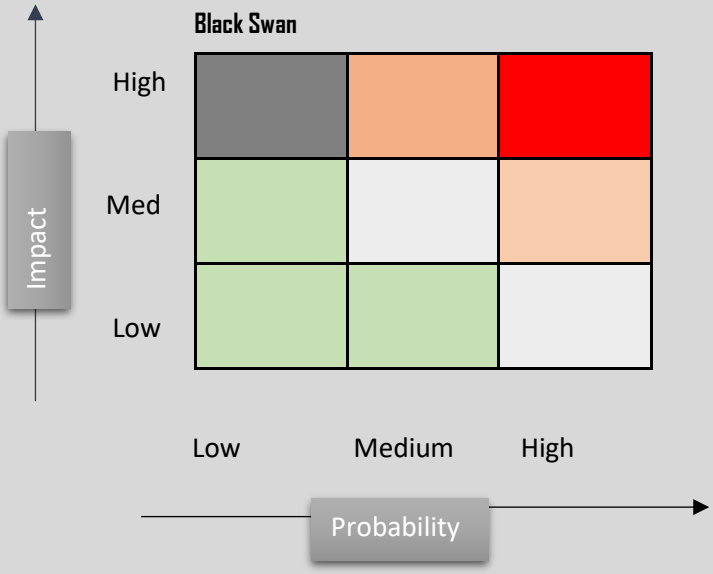
Probability(P) is hidden behind the Threats

Both I and P are execlusively related.

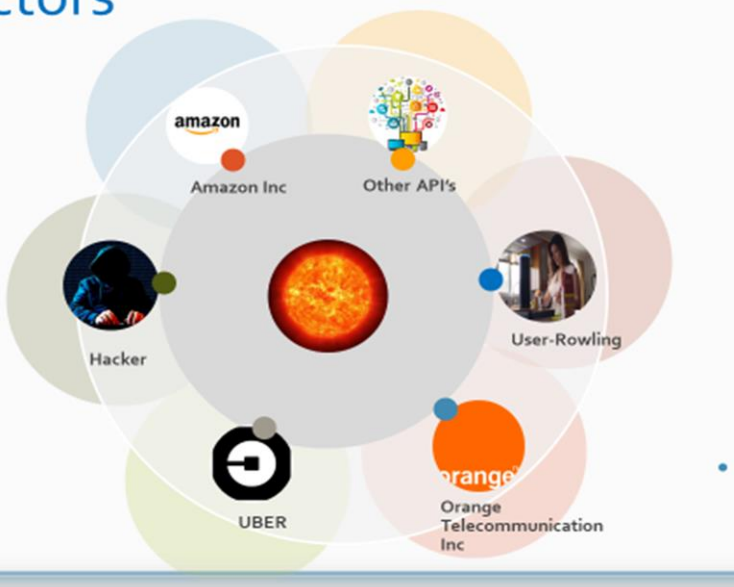
P = F (E,I,S,R)

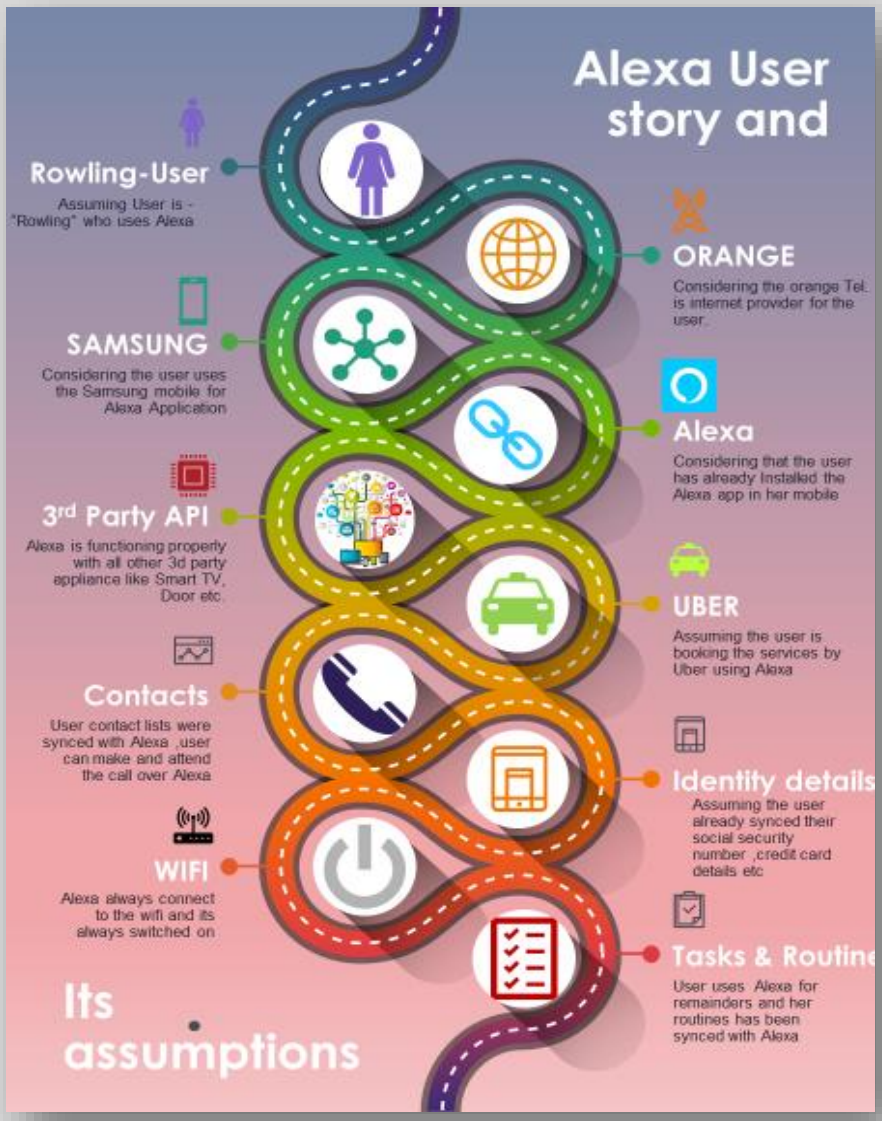
Where E-Existence, I-Intentions-Skills-Recourse





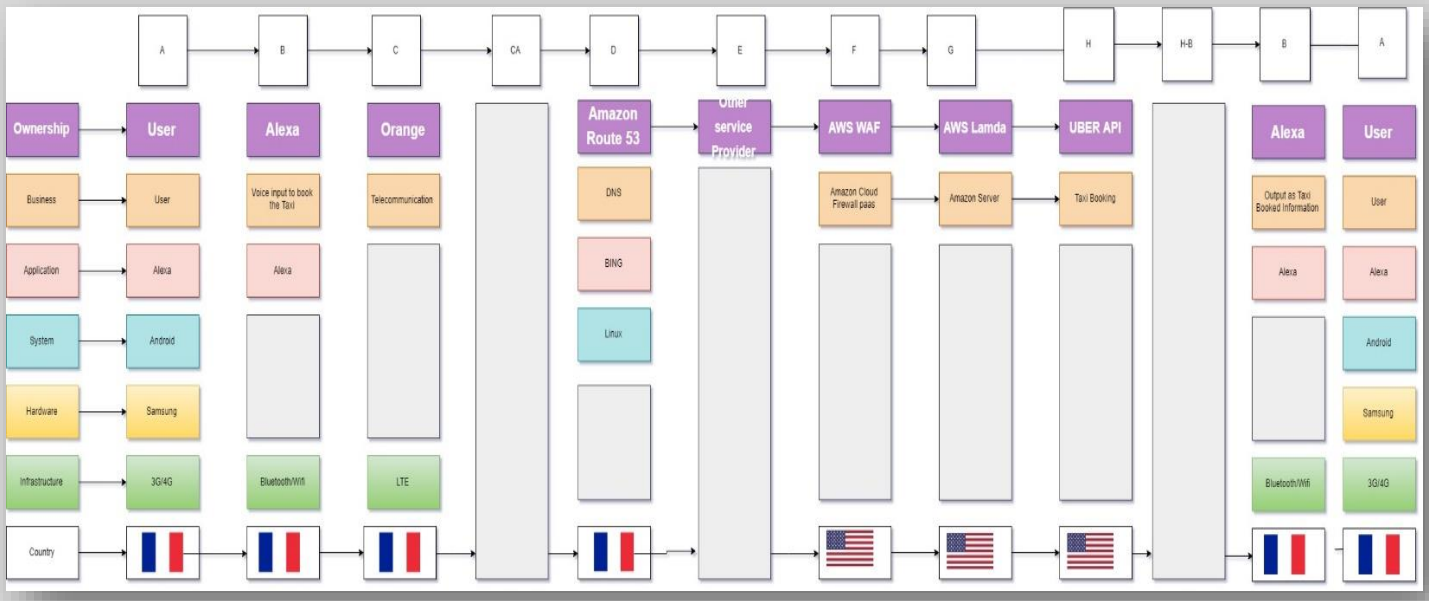
Sun of actors





OBASHI FLOW:

For Alexa User



Hacker story for Amazon Alexa User:

1. As a self-Employed hacker, I want to use Rowling's Alexa device data by injecting a sequence of inaudible voice commands by exploiting the audio hardware vulnerability (the dolphin attack), in order to sniffing the Rowling activities.

2. As a State sponsored hacker, I want to hack the Rowling host country's-Alexa cloud server data, in order to mass surveillance of the people activities and behavioural pattern.

3. As a hacker employed by the potential future competitor, I want to bypass the amazon infrastructure to access the top employees' device, in order to access the Alexa's future R&D project details (Intellectual proprietary theft)

4. As a hacker driven by fun or curiosity, I want to successfully take down the amazon services by commands and controls the botnet to launch a DDoS attack for a while, in order to feel better about my selves

5. As a hacker (previous employee of amazon with malicious intent), I want to inject the malicious software in the amazon cloud infrastructure by privilege misuse, in order to make the services down to give back my revenge.

6. As a hacker employed by neighbour of Rowling, I want to hack the Rowling Wi-Fi and compromise the Alexa, in order to disturbing the Rowling by unlocking of doors, making unauthorized purchases, controlling sensitive home appliances (e.g., security cameras and thermostats),

and transmitting sensitive information.

7. .As a hacker employed by the competitor, I want to hack the amazon Alexa cloud user details and expose it to public, in order to make Amazon's brand erosion.

8. As a hacker employed by the politician, I want to hack the amazon Alexa data, in order to know the behaviour and opinion of the user

9. As a self-employed hacker, I want to spread the Ransomware in the Alexa user, inorder to get the funds as a ransom to the user.

10. As a hacker employed by health Insurance corporation, I want to hack the amazon Alexa user's data, in pattern to introduce the insurance policy accordingly.

11. As a hacker paid by direct competitor, I want to make the services down by DDOS attack, in order to promote by product among the Voice controlled service users

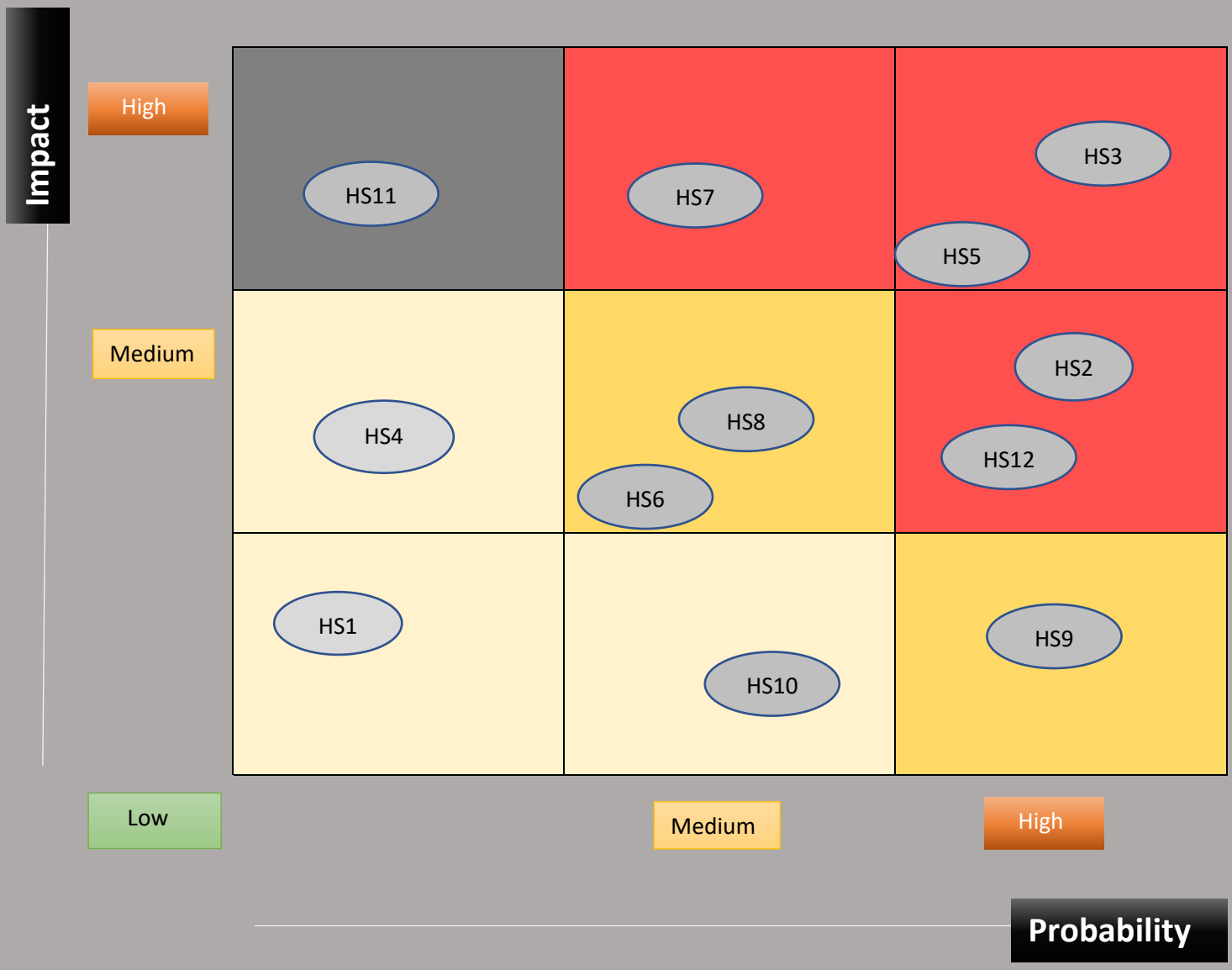
12. As a Grudged insider hacker, I want to steal the intellectual propriety and sell to competitor, in order to endure financial loss of the Alexa.

13. As a self-employed hacker, I want to steal Rowling Identity by physical theft of Phone /Alexa, in order to steal social security number, credit card details etc.

14. As a hacker recruited by the detective agency, I want to hack by hijack the traffic from the user inorder to investigate the data

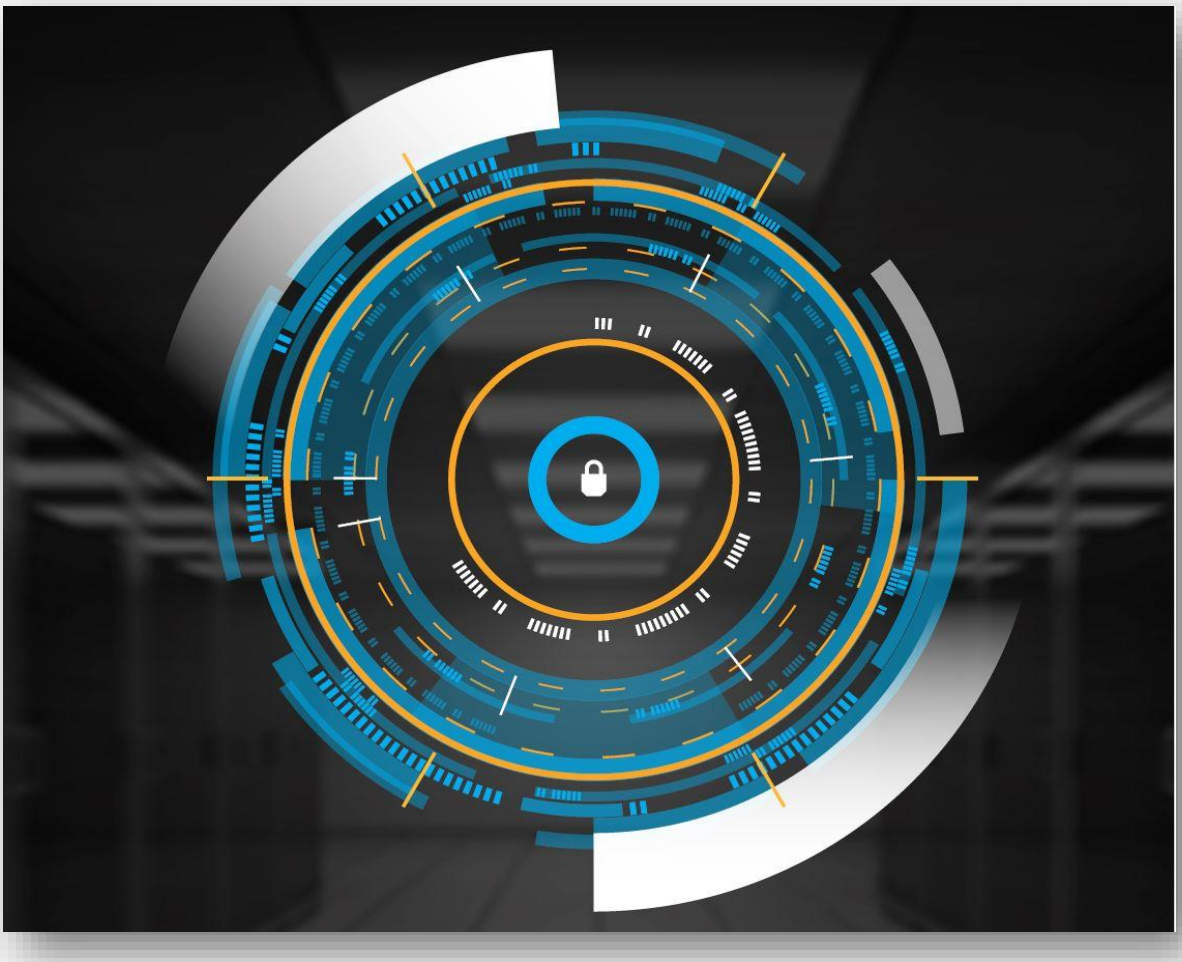
15. As a thrill wanted hacker, I want to hack the amazon's data by exploiting the zero-day vulnerability, in order to gain the access in the cloud server

RISK ANALYSIS:

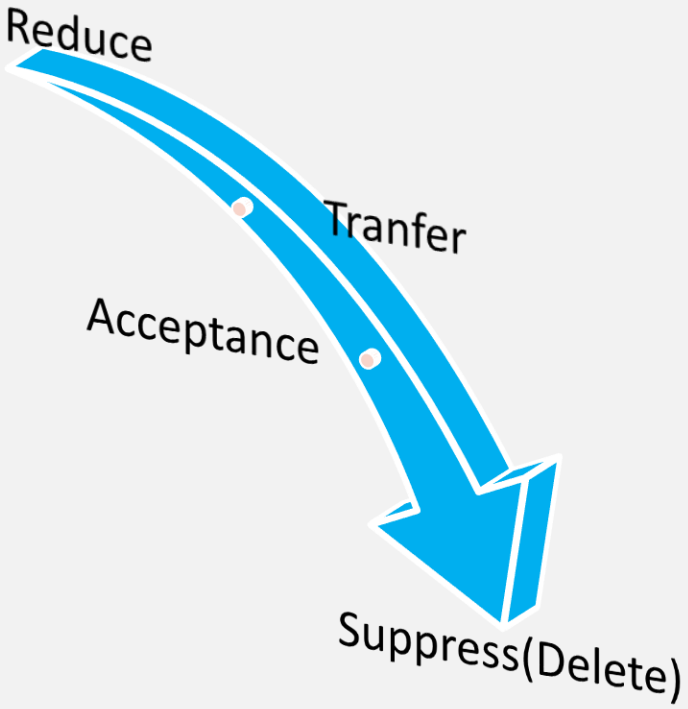


The occurrences for H11 is the low probability and high impact, it is called black swan because the chance is low, but the impact is serious. The H3 and H5 are similar and hence placed in the High-high, as the probability of this is high and the impact is high. Hacker stories H6 and H8 share the same space on medium-medium, as this can be really carried out and can impact the business. This needs to be brought down to the low-low. The occurrences of H3, H5, H12,H2 and H7 are similar and are placed in the low-low section of the graph as the chances of this to happen is low and results in either a low impact or can be taken care of pretty easily once the high and mediums are taken care of. The stories H7 is placed in the medium high, this needs to be brought to the low-low. We could have listeners that listen to activities such as payment failures and drop the transaction numbers to a high priority queue and mitigate similar issues

RISK MITIGATION



The risk can be mitigated by the following four actions:



1.As per the ANSSI 34 and 35 the suggestion- Following of Define an update policy for the components of the information system. Since, it is the new hardware vulnerabilities, the amazon should do proper research on their third-party hardware vulnerability and do the possible qualification of corrective measure can reduce this type of risks.

2.As per the ANSSI 3rd,18th -Following of Only allow controlled devices to connect to the network of the organization and Encrypting sensitive data sent
through the Internet and maintain the proper incident management and monitoring tools like SIEM in their infrastructure can able to mitigate this risk

3.As per the ANSSI 19th and 24th suggestion, Segmenting the network and
implement a partitioning and Protect your professional email between these areas can reduce this kind of data loss risks.

4. Implementing a secure access gateway to the Internet and proper Disaster recovery system in the system can transfer this kind of service down risks.

5. As per the ANSII 5th suggestion, Having an exhaustive inventory of
privileged accounts and keep it updated and implementing the User Behaviours Analytics (UBA) can able to mitigate this kind of data misuse attacks by insiders.

6. As per the ANSII 11th Suggestion, protecting passwords stored on systems ,12th Change the default authentication settings on devices and services, and Encrypt sensitive data sent through the Internet can able to mitigate this kind of tampering the data attacks

7. Activate and configure the firewall and Securing the network connection
of devices used in a mobile working situation and implement the proper incident management tools can able to reduce this kind of data theft risks.

8.As per the ANSSI 23 rd. Suggestion, Segregating the services visible from the Internet from the rest of the information system can able to reduce this kind of data loss attacks

9As per the ANSSI 30th Suggestion Using a dedicated and separated
network for information system administration can reduce the illegal footprint tracing of outsiders

10 As per the ANSSI 25th, Allocating the appropriate rights to the information system's sensitive resources and Define and apply a backup policy for critical components can reduce this king of the attacks.

Conclusion:

As following the proper risk assessment of the information system and applying the appropriate risk mitigation strategies can mitigate the risk underlying in the systems.we can reduce the risk from right to left as shown in the below P-I Risk matrix.