IP Risk Assessment & Loss Prevention

By Priya Kanduri
Happiest Minds, Security Services Practice

happiest minds
The Mindful IT Company
Born Digital . Born Agile

IP Risk Assessment & Loss Prevention

Often when organizations are expanding rapidly, they do not give sufficient and necessary focus on information security aspects and guidelines, specifically IP protection. The focus has always been on BAU, market growth and business expansions. However, the security of an enterprise's IP assets is increasingly important in today's world of cyber threats and data leaks. This is especially critical for manufacturing and healthcare enterprises, as IP protection is the crux of its business.

Recently, there has been an alarming rise in incidents of data loss from IT departments as revealed by a January 2012 survey conducted by iStorage. The survey exposed a double-digit rise in the percentage of IT professionals losing portable devices containing corporate and personal data between. The kinds of data targeted in these kinds of incidents always are IP - 1) customer data, 2) corporate plans, 3) financials, and 4) R&D material.

If there are no measures to identify, record and track IP assets, usually IP attacks and data losses can even go undetected. There are also other implications such as:

- Increased unintentional data loss incidents from internal employees
- The authorised supplier/partner could be a malicious hacker and steal IP assets and thereby cause risks to business
- Any loss of PII data may lead to fines and irretrievably damage corporate image. Recent data loss surveys reported a loss of billions in proprietary information and intellectual property.

These implications may lead to significant business losses in the long run as loss of sensitive information may cause another enterprise to launch competing products or an insider to misuse proprietary knowledge or a hacker to publish private business details.

DEALING WITH ISSUES OF IP RISK

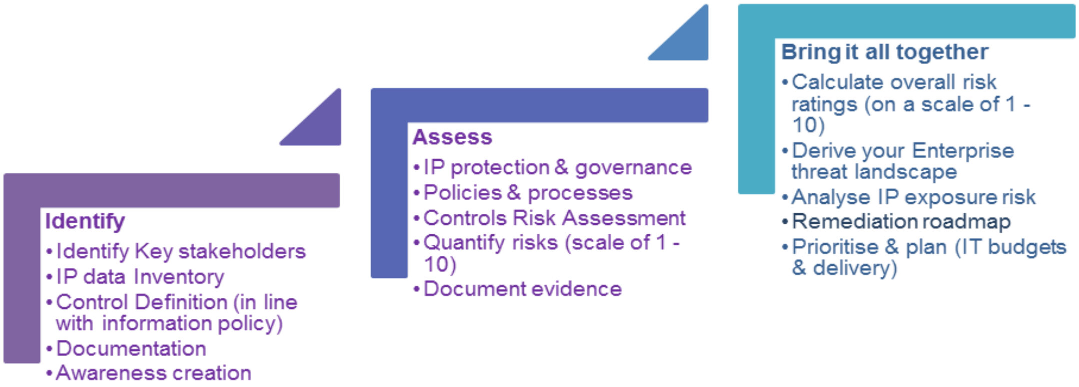
Any enterprise that has IP assets at the core of its business, needs to answer and validate several key questions:

> "Do you have documented visibility of your IP data?"
>
> "Are you sure that your IP data is safe enough?"
>
> "When was the last time you formally verified data security?"

If an enterprise fails to answer these questions satisfactorily,then its IP assets could be vulnerable to attacks. The best way to address the situation is to conduct a quick risk assessment around IP asset protection.

The next question to arise will be how to execute IP risk assessment, in a short span of time, with minimal interruption to the day to day operations of an enterprise.

Here's the answer - break down the problem into manageable pieces as shown below:



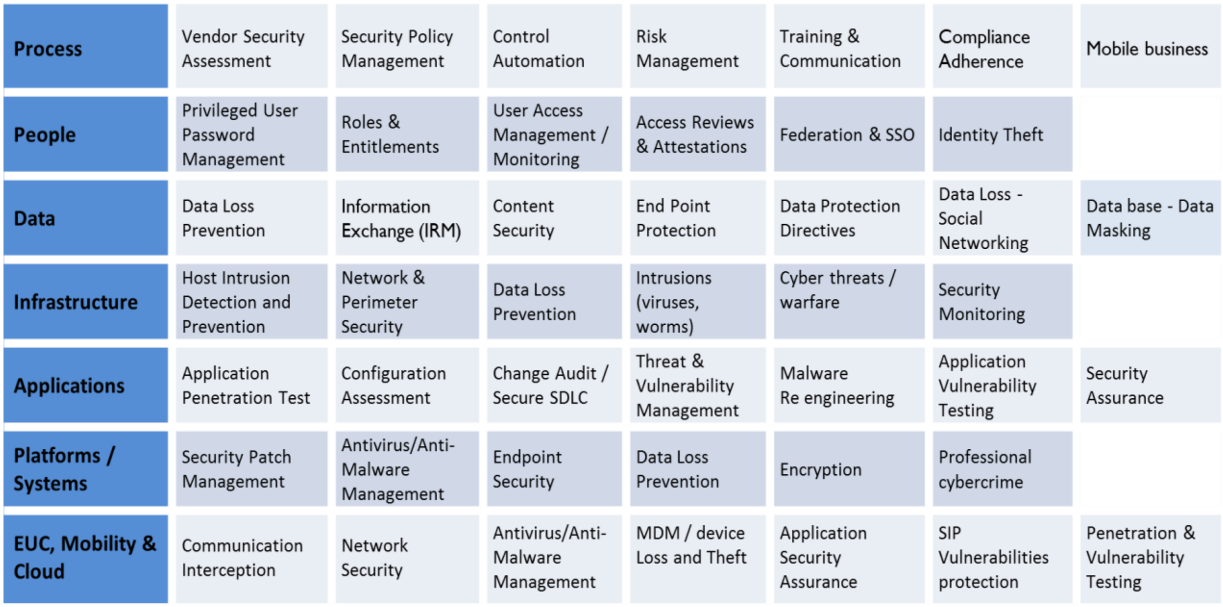
Identify
- Identify Key stakeholders
- IP data Inventory
- Control Definition (in line with information policy)
- Documentation
- Awareness creation

Assess
- IP protection & governance
- Policies & processes
- Controls Risk Assessment
- Quantify risks (scale of 1 - 10)
- Document evidence

Bring it all together
- Calculate overall risk ratings (on a scale of 1 - 10)
- Derive your Enterprise threat landscape
- Analyse IP exposure risk
- Remediation roadmap
- Prioritise & plan (IT budgets & delivery)

Thus the entire task can be achieved in a duration of 4 – 6 weeks for medium sized business with around 5000 employees, less than four data centres and a presence in 3 -5 locations or countries.

Enterprises should assess IP risks pertaining to key enterprise segments – People, Process, Data, Infrastructure, Applications and Next Generation Initiatives. For detailed assessment under each segment, the following chart may be used as a guideline. However, the fact that not all areas may hold the same priority for an enterprise's IP assets should be taken into consideration while assigning risk scores to each segment.

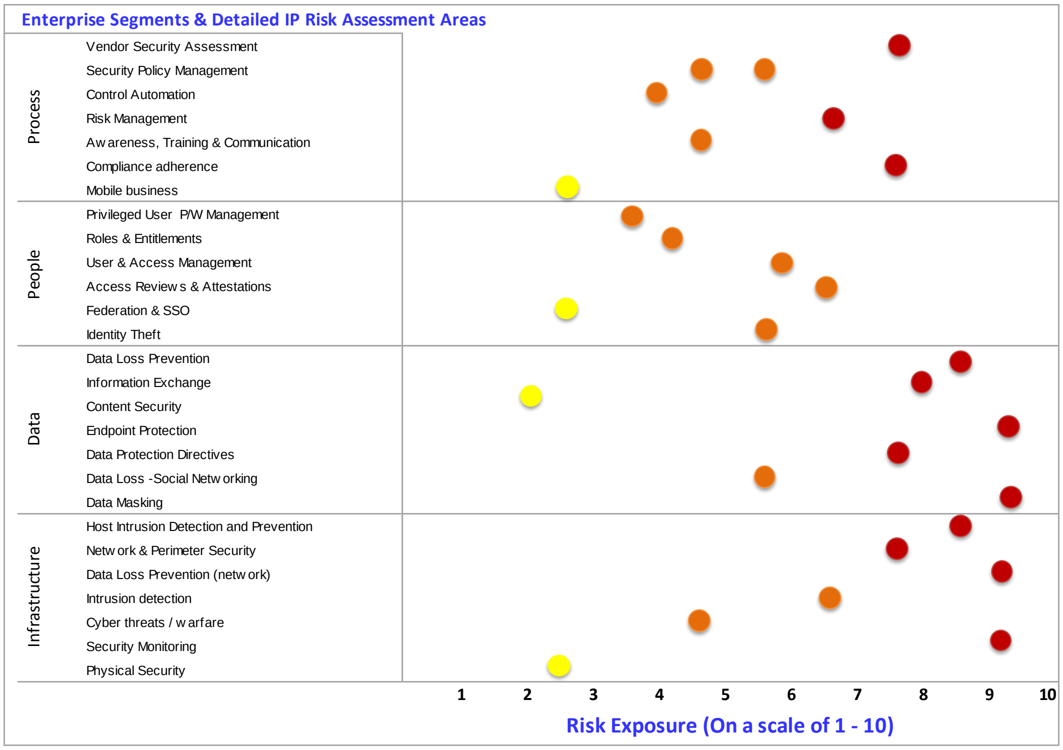


Process	Vendor Security Assessment	Security Policy Management	Control Automation	Risk Management	Training & Communication	Compliance Adherence	Mobile business
People	Privileged User Password Management	Roles & Entitlements	User Access Management / Monitoring	Access Reviews & Attestations	Federation & SSO	Identity Theft	
Data	Data Loss Prevention	Information Exchange (IRM)	Content Security	End Point Protection	Data Protection Directives	Data Loss - Social Networking	Data base - Data Masking
Infrastructure	Host Intrusion Detection and Prevention	Network & Perimeter Security	Data Loss Prevention	Intrusions (viruses, worms)	Cyber threats / warfare	Security Monitoring	
Applications	Application Penetration Test	Configuration Assessment	Change Audit / Secure SDLC	Threat & Vulnerability Management	Malware Re engineering	Application Vulnerability Testing	Security Assurance
Platforms / Systems	Security Patch Management	Antivirus/Anti-Malware Management	Endpoint Security	Data Loss Prevention	Encryption	Professional cybercrime	
EUC, Mobility & Cloud	Communication Interception	Network Security	Antivirus/Anti-Malware Management	MDM / device Loss and Theft	Application Security Assurance	SIP Vulnerabilities protection	Penetration & Vulnerability Testing

Risk assessment shouldbe conducted only for a sample of targets, audience, teams, applications, platforms or systems. However, it should cover all aspects of IP loss risks that apply to each enterprise segment for the chosen targets.

WHAT’S THE OUTCOME?

The following image reveals how an enterprise’s IP threat landscape will look towards the end of risk assessment:



This view provides answers to the earlier questions and thus helps an enterprise better plan its IT budgets, make informed decisions or choose to accept risks. There are also added benefits such as:

- ✓ IP risks and threats are – proved, quantified and presented with evidence.
- ✓ Knowledge of where the quick wins are for IP protection and how quickly the difference can be brought in
- ✓ Helps an enterprise (re)align budgets as per the IP threat landscape
- ✓ User awareness – this is key for any information security initiative and as part of risk assessment significant progress is made in this area
- ✓ IP asset inventory - data loss incidents primarily occur whenIP assets are not tracked in corporate accounting systems. The assessment exercise results in an IP asset registry or inventory that can be tracked on an on-going basis for any incidents.

SUMMARY

With the emerging cyber threats and malwares, risks to an enterprise's IP assets are always lurking in the background. From time to time it is important to assess the overall risk exposure and enterprise threat landscape. Surveys have proved that companies that had made IP protection a high priority indicated no loss incidents.

This article presents a quantifiable approach to deal with IP risk assessments & loss prevention. The key is to remember that IP risks can have catastrophic consequences for an enterprise, if ignored for too long.

Business Contact: **business@happiestminds.com** **Media Contact:** **media@happiestminds.com**

About Happiest Minds Technologies:

Happiest Minds, the Mindful IT Company, applies agile methodologies to enable digital transformation for enterprises and technology providers by delivering seamless customer experience, business efficiency and actionable insights. We leverage a spectrum of disruptive technologies such as: Big Data Analytics, AI & Cognitive Computing, Internet of Things, Cloud, Security, SDN-NFV, RPA, Blockchain, etc. Positioned as "Born Digital . Born Agile", our capabilities spans across product engineering, digital business solutions, infrastructure management and security services. We deliver these services across industry sectors such as retail, consumer packaged goods, edutech, e-commerce, banking, insurance, hi-tech, engineering R&D, manufacturing, automotive and travel/transportation/hospitality.Headquartered in Bangalore, India; Happiest Minds has operations in USA, UK, The Netherlands, Australia and Middle East.

To know more about our offerings. Please write to us at business@happiestminds.com

About the author

Priya Kanduri (Priya.kanduri@happiestminds.com) Priya Kanduri heads the security consulting practice at Happiest Minds Technologies Pvt. Limited. She brings over 13 years of experience in designing & implementing identiy access management, access governance, PKI & Key Management solutions. She was also associated with various enterprises in UK and Europe over the past 10 years focusing on the information security aspects of data protection, loss prevention, risk and compliance. She has also been a presenter in various IDAM internal conferences. Her recent work has included conducting IP risk assessments, IP loss prevention and executing short and long term remediation programs.

happiest minds
The Mindful IT Company
Born **Digital** . Born **Agile**