IT Security Stance of Public Sector Units
The Economic Times' initiative on consumer research, which over time has grown into a full service consumer research entity.

ET-RICS now provides customized research solutions across almost all key sectors.

ET-RICS is committed towards arming its clients with superior insights while ensuring quick turnaround and high ROI.

Exploratory studies / Consumer Purchase analysis

Campaign Evaluations / Brand tracks / Awareness studies

Hypothesis testing / Dipsticks / Event specific surveys

Concept / Product tests*
Objective & Methodology

- The objective behind this study was to understand the status and perception of Indian PSUs regarding IT security in their respective organizations.

- The interview questionnaire was prepared with information security experts from Microsoft.

- Responses were collected through Face-to-Face interviews with 12 PSU IT leaders.

- Survey participants: BHEL, BPCL, BSNL, HPCL, IFFCO Tokio, IFFCO, IOCL, NSE, NTPC Petronet LNG, RCF and SCI
Overview

The PSU sector has played a critical role in India’s growth. The state-owned enterprises have enabled capital formation, employment generation, balanced regional development, and promotion of research and development.

However, to continue their stellar work, PSUs would have to take into account the fast-changing business environment. One of the biggest threats for businesses today is that of information security.

As technology is changing at scorching speed, hackers are becoming more persistent, turning the response to cyber security incidents an increasingly complex challenge.

Against such a scenario, Economic Times CIO and Economic Times RICS, in association with Microsoft, decided that it would be pertinent to explore and understand the thoughts and opinions of IT decision makers from India’s top PSU on the crucial subject of information security.

The Economic Times CIO, therefore, caught up with India’s top 12 PSU IT decision makers, and interviewed them one-on-one on diverse information security areas.

The outcome of the comprehensive discussions has been captured in this insightful report, which provides an accurate and deep understanding of the information security stance of some of India’s top PSUs.
Digital Transformation Imperatives
Business need, and drive to increase efficiency are key forces driving PSUs towards digitization.

Key reasons for going Digital:

- 64% Business Requirement
- 64% Business process improvement
- 18% Better customer service
Shortage of right skill set and mindset of internal stakeholders seem to be the biggest hurdles faced by PSUs while going digital.

Key challenges in going Digital:

- **73%**: Finding right skill set
- **64%**: Mindset issues
- **36%**: Rapid change in technology
- **18%**: Unable to show clear business value
Most PSUs are planning to go for complete digitization, which would change their internal processes as well as customer interface.
Majority of PSUs dealing in sensitive customer transaction & customer interaction data which makes it imperative for them to focus on data security.

Customer data being collected:

- 60% Customer purchase/Transaction data
- 50% Customer interaction/CRM data
- 40% Web analytics
- 30% Customer survey data
- 20% Social data
Applications & payment interfaces emerge as biggest concern for PSUs regarding data security

Channelwise risk perception

- Third party applications: 58%
- Payment interfaces: 58%
- Cloud applications: 58%
- Mobile channel: 25%
- Social media: 25%

Total respondents = 12
11 out of 12 PSUs pointed outsourced service providers as a potential risk source

Source of threat:

- Outsourced service provider: 92%
- Unconnected: 58%
- Internal: 50%
- Customer network: 33%
- Former employees: 8%

Total respondents = 12
Phishing, Virus & Spyware/adware attacks lead the threat pack
PSUs anticipate biggest risk emerging from Botnets, Phishing and Malware attacks

**Biggest risk in near future**

- **Phishing**: 64%
- **Malware**: 64%
- **Botnets**: 64%
- **Viruses**: 55%
- **Denial of service**: 45%
- **Identity theft**: 36%
- **External Unconnected**: 27%
- **Internal sources**: 18%
- **Spyware & Adware**: 10%
- **Corporate account takeover**: 9%
- **Service provider network**: 9%
- **Mobile interfaces**: 9%

Total respondents = 10
Majority of PSUs lack a detailed process to recognize and prioritize new threat sources

Presence of process to identify & prioritize new threat sources

- 58% have some process
- 25% have a detailed process
- 8% have a state-of-the-art process
- 8% have no comment

Total respondents = 12
Organizational security & Risk Awareness
9 out of 11 PSUs reported having a board approved policy to manage cyber security

Presence of board approved Cyber Security Policy

- **YES**: 82%
- **NO**: 9%
- **Do not wish to state**: 9%

Total respondents = 11
10 out of 11 PSUs conveyed having adequate funding towards their IT security setup

Current funding status for IT security setup

- Sufficient funding: 91%
- Funds are constrained: 9%

Total respondents = 11
A large number of PSUs seem to rely on random updates for making internal stakeholders cognizant of security threats.

Process to spread awareness of security threats among employees/associates:

- Regular updates: 55%
- Occasional updates: 45%

Total respondents = 11
Data classification & Governance
5 out of 11 PSUs do not have any data governance tool to manage data handling

Presence of data governance tools for data handling

- Yes: 55%
- No: 45%

Total respondents = 11
9 out of 10 PSUs lack advanced e-discovery tools that leverage machine learning and help reduce the cost/time for compliance audits.

Presence of advanced e-discovery tools

- Yes: 10%
- No: 90%

Total respondents = 10
Information protection
Majority of PSUs are confident of using the correct tool for protection of sensitive data.

Use of right management tool to protect sensitive data across all sources with option to apply policy automatically.

Yes: 73%
No: 27%

Total respondents = 11
Majority of PSUs still not using data loss prevention tools

Use of data loss prevention tool to prevent sensitive data leak across mail and content repositories

Yes: 45%
No: 55%

Total respondents = 11
4 out of 11 PSUs still do not apply compliance policies to laptops and handheld devices

Have tools to apply security and compliance policy to devices in the user's hands

Yes: 64%
No: 36%

Total respondents = 11
Of the total PSUs analysed, more than half admitted of having no knowledge of the file storage & sharing apps used by their employees.

Do you know which SaaS apps your employees are using for file storage & sharing?

Yes: 45%
No: 55%

Total respondents = 11
Use of single sign on seems to be gaining traction as 6 out of 10 PSUs reported using it.

Implementation of single sign on?

Yes: 60%
No: 40%

Total respondents = 10
Real-time anomaly detection still has a long way to go among PSUs as currently 6 out of 10 have not deployed it.

Tools to detect anomalies based on location or user behaviour and taking action for protecting data.

Yes: 40%  
No: 60%

Total respondents = 10
5 out of 9 units reported presence of a strong threat intelligence framework

Robust framework for threat intelligence

Yes: 56%
No: 44%

Total respondents = 9
Most PSUs gearing up to handle and protect from zero day virus/spam attacks

Behavioural detection in Antivirus/Antispam engine

- Yes: 75%
- No: 25%

Total respondents = 12
IT security at most PSUs has not evolved to the level of deploying machine learning to monitor and analyze past events & triggers to predict future security events.

Use of machine learning to predict future security events

- Yes: 20%
- No: 80%

Total respondents = 10
6 out of 11 PSUs currently do not use Big Data and Predictive Modelling for real time fraud analysis & risk analysis.

Total respondents = 11
Leveraging Cloud
9 out of 12 PSUs have either planned to transition to cloud computing or have begun evaluating the same.
Reason behind the transition towards cloud computing seems multi faceted

Key reasons behind going for cloud computing

- 38% Business continuity
- 38% Cost reduction & efficiency
- 38% Security analysis
- 25% Business expansion
PSU Security Stance Survey Findings

Digital Transformation
Indian Public Sector Units (PSUs) are undoubtedly going digital. They realize that digital transformation is a critical business need and is imperative to drive efficiency and productivity. Hence, they are aggressively digitizing their customer-facing as well as internal processes. However, there are impediments in this journey. Shortage skilled manpower and legacy mind-set issues come across as key challenges in the PSUs quest to digitization.

Risk Perception
Digitization and information security go hand-in-hand as the former opens up PSUs to external threats. PSUs feel third party applications and payment interfaces are the biggest areas of concern, while outsourced service providers are overwhelmingly believed to be the biggest potential risk source. Amongst future threats, Botnets, phishing and malware are feared the most.

Organization security & Risk Awareness
Most PSUs have a board-approved cybersecurity policy in place backed with adequate budgets.

Data Classification & Governance; Information Protection
PSUs fall woefully short when it comes to Data Classification & Governance; Information Protection. Few use e-discovery tools and almost half of them still don't leverage data governance tools and data loss prevention tools. Most PSUs also lack visibility into file storage and sharing apps being used by employees.

Threat Intelligence
While a majority of PSUs have a strong threat intelligence framework and are gearing up to counter zero day attacks, they are far from implementing next-gen technologies such as machine learning and predictive solutions for pre-empting threats.