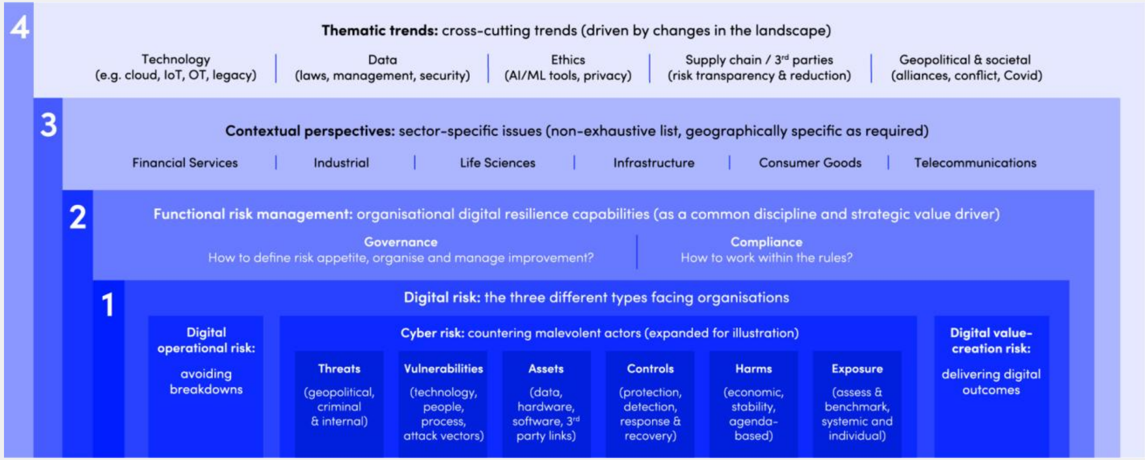
ICAI Brisbane Chapter

Exploring digital risks and key controls

Speaker: Vineet Arora
20 September 2022, 5.30pm

Key Points

- Consumers are increasingly swapping traditional channels for digital ones, and many executives are trying to turn operational necessities into competitive advantages.
- Digital risks are becoming more pronounced in three distinct categories: resilience, cyber, and customer value and experience.
- During the session, we will try provide high level insights on risks at functional and industry levels.



4 **Thematic trends:** cross-cutting trends (driven by changes in the landscape)

Technology (e.g. cloud, IoT, OT, legacy) | Data (laws, management, security) | Ethics (AI/ML tools, privacy) | Supply chain / 3rd parties (risk transparency & reduction) | Geopolitical & societal (alliances, conflict, Covid)

3 **Contextual perspectives:** sector-specific issues (non-exhaustive list, geographically specific as required)

Financial Services | Industrial | Life Sciences | Infrastructure | Consumer Goods | Telecommunications

2 **Functional risk management:** organisational digital resilience capabilities (as a common discipline and strategic value driver)

Governance How to define risk appetite, organise and manage improvement? | **Compliance** How to work within the rules?

1 **Digital risk:** the three different types facing organisations

Digital operational risk: avoiding breakdowns

Cyber risk: countering malevolent actors (expanded for illustration)

Threats (geopolitical, criminal & internal)

Vulnerabilities (technology, people, process, attack vectors)

Assets (data, hardware, software, 3rd party links)

Controls (protection, detection, response & recovery)

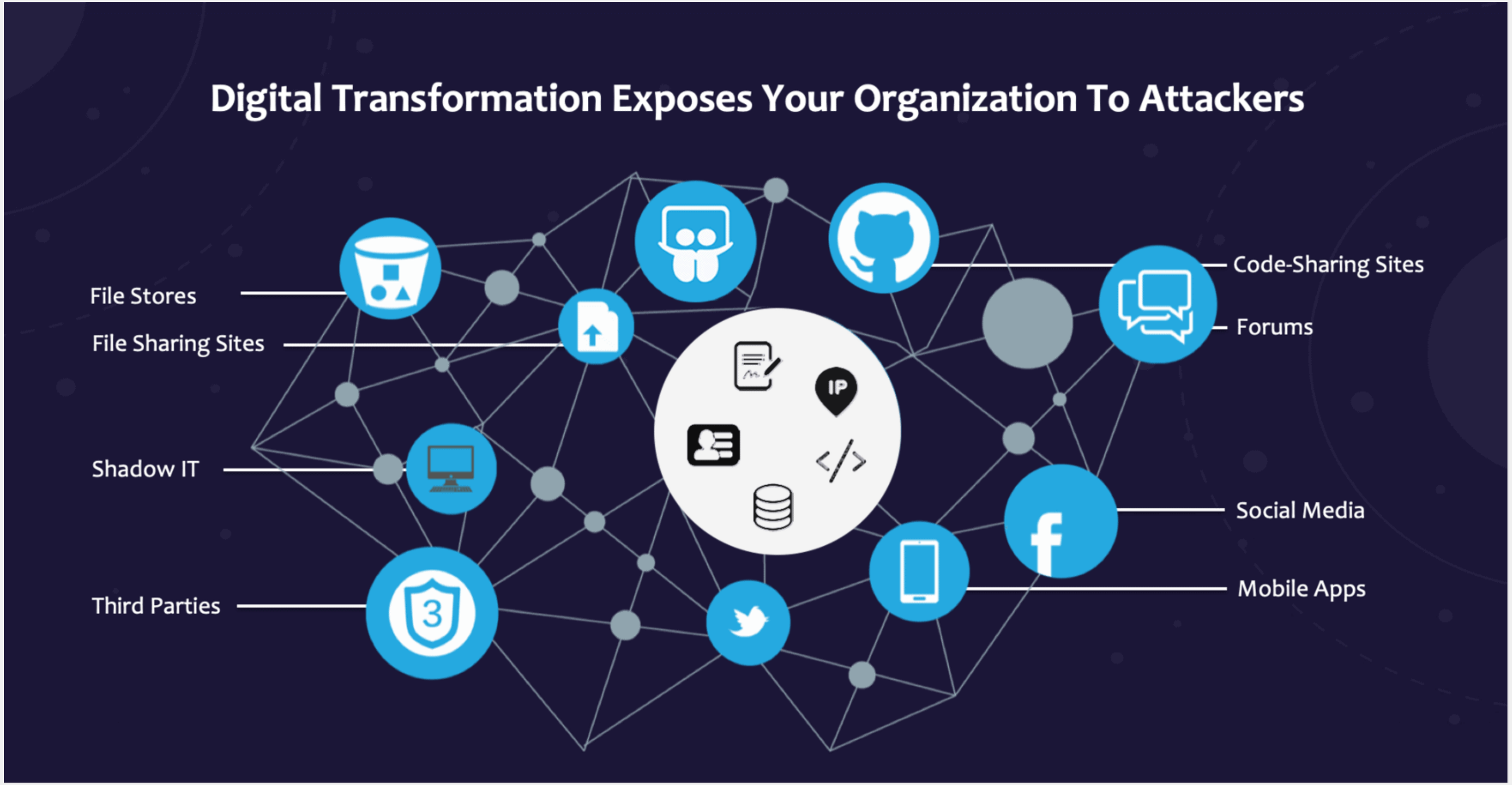
Harms (economic, stability, agenda-based)

Exposure (assess & benchmark, systemic and individual)

Digital value-creation risk: delivering digital outcomes

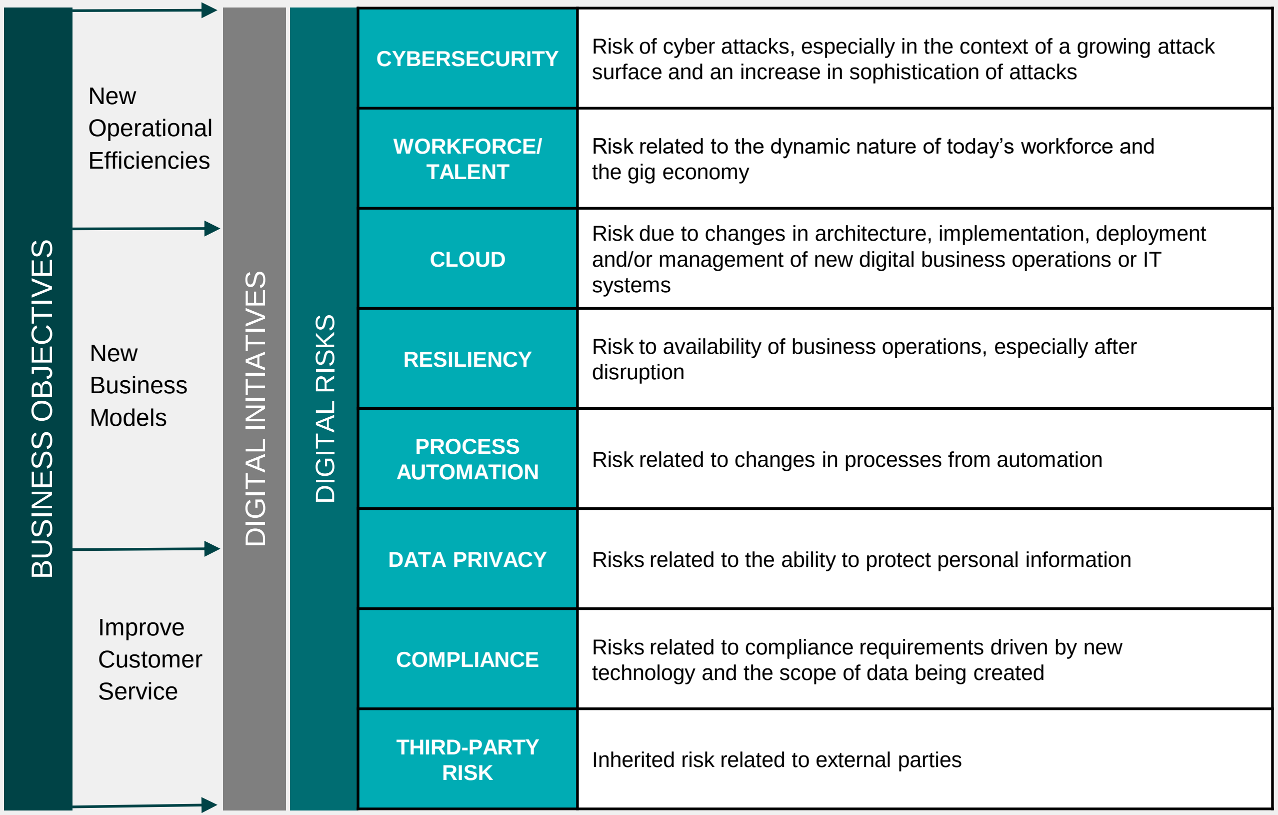
Source: Istari Global, https://istari-global.com/insights/navigate-your-digital-risk-landscape/

It is evident that any type of “Digital Transformation” exposes any organisation to a wide variety of risks



https://www.digitalshadows.com/blog-and-research/managing-digital-risk-4-steps-to-take/

Summary



BUSINESS OBJECTIVES

- New Operational Efficiencies
- New Business Models
- Improve Customer Service

DIGITAL INITIATIVES

DIGITAL RISKS

CYBERSECURITY	Risk of cyber attacks, especially in the context of a growing attack surface and an increase in sophistication of attacks
WORKFORCE/ TALENT	Risk related to the dynamic nature of today's workforce and the gig economy
CLOUD	Risk due to changes in architecture, implementation, deployment and/or management of new digital business operations or IT systems
RESILIENCY	Risk to availability of business operations, especially after disruption
PROCESS AUTOMATION	Risk related to changes in processes from automation
DATA PRIVACY	Risks related to the ability to protect personal information
COMPLIANCE	Risks related to compliance requirements driven by new technology and the scope of data being created
THIRD-PARTY RISK	Inherited risk related to external parties

Source: RSA.com, https://www.rsa.com/content/dam/en/e-book/how-to-manage-eight-types-of-digital-risk.pdf

Cyber risks (Following slides are not exhaustive lists, they show areas of immediate interest to a risk professional)

Key risks to consider

Data loss due to poor physical controls

Data loss due to poorly designed digital security (platforms with poor configuration or vulnerabilities)

Data that is not protected consistently across the whole lifecycle (we will expand on third party risk later)

Not being ready for specific types of attacks – DDOS, Ransomware etc

Key controls to assess and prioritise

Clearly defined physical security controls

Patching and vulnerability management

Continuous monitoring of config changes and vulnerability scans

Scanning for malware and suspicious activity across multiple layers – specifically protecting against DDOS, Ransomware

Layered security (no more hard shell, soft interior) – segmentation and compartmentalisation

Data loss prevention – knowing what is leaving the ecosystem, stopping it from happening

Transparency and reporting - accountability

Security education and awareness

Talent management and workforce planning

Key risks to consider

“The Great Resignation” – the impact of the COVID-19 pandemic on the workforce

Thinner leadership bench

Low retention in critical areas – direct disruption impact

Increasing turnover rates

Larger capability gaps

Reduced productivity

Lack of clarity on business critical systems

Failure to deliver workforce planning and organisation design programmes

Key controls to assess and prioritise

Talent growth and retention programmes

More pronounced succession planning and talent programmes

Remuneration reviews / market benchmarks

Technical training programmes

Improved tooling for productivity and automation

Focus on asset management including tiering

Higher visibility of talent management and workforce planning projects and programs

Cloud & XaaS environments

Key risks to consider

Financial risks – cost overruns or bill shock

Privacy related risks

Dependencies on 3rd parties

Non-compliance with regulations

Platform related risks

Performance risks

Great overview here: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/best-practices-to-manage-risks-in-the-cloud

Key controls to assess and prioritise

Due diligence – including external security reviews and certifications

Secure development lifecycles and safe configuration practices – heading toward continuous control monitoring

Ensuring that experts are involved across contractual, legal and regulatory approval steps

Identity and access management

System monitoring and incident management

Cloud Access Security Broker - CASB

Resilience

Key risks to consider

Failure to accurately consider “crown jewels” – leading to larger disruptions

Complicated service resilience picture – dependency on many parts

Failure to understand and monitor “service resilience”

Increased resilience requirements due to regulatory changes and higher compliance burden

Failing to meet customer expectations regarding digital channels

Interesting article by ISACA CEO here: https://www.csoonline.com/article/3234689/measuring-cyber-resilience-a-rising-tide-raises-all-ships.html

Key controls to assess and prioritise

Service mapping

Asset registration, classification and tiering

Clearly defined resilience criteria

Resilience reporting including RAS metrics

Assessment against existing and evolving regulatory requirements – proactive regulatory impact assessment

Making multiple digital channels independently available to combat unexpected disruption

Process Automation

Risks

Development and acceptance practices are not mature

Automation tools are not fit-for-purpose

Lack of automation skills

Organisational resistance to large scale automation

Inadequate monitoring of automation

Controls

Well-defined development lifecycle with acceptance checkpoints

Training

Partnering

Incident management and disaster recovery

Central Monitoring Center

Data Privacy

Risks

Increased regulatory focus

Cyber-crime and data breaches

Low Privacy skillset in the market

Business and technology awareness

Controls

Asset Governance and Management

Privacy Policy and Framework

Response and Recovery mechanism

Upskill existing workforce

Training and awareness

Compliance

Risks

Regulator pressure to report and comply
Financial Accountability Regime
Cyber Resilience Legislation
Resilience

Compliance to existing policies

Controls

Compliance Management Framework

Policies and Procedures

Incident and Service Management

1LOD teams

Third-party risk

Risks	Controls
Pandemic impact on logistics	Selecting the right partners
Supply chain vulnerabilities	Supplier contingencies
Visibility of Technology processes at third-party	Third party assurances