CiO Espresso
Fueling your digital transformation, one sip at a time
#19
2024

TOP **5** CONSIDERATIONS *for CIOs*

How to...

ensure availability, maintainability and security of an IT estate

Business Continuity and Disaster Recovery Planning

Having a plan is great *in theory*

Testing and using it *is better*

Develop and maintain robust business continuity and disaster recovery plans to ensure the timely recovery and restoration of critical systems and services in the event of a disaster or outage.

Bottom line: First, use your BCPs in anger. Fire drills are important and reinforce mental toughness in a time of crisis. **Only 6% of companies without a disaster recovery plan survive a disaster** (Invenio IT). Second, in the immortal words of Mike Tyson: "Everyone has a plan until they get punched in the face."

Infrastructure Resilience and Redundancy

What happens *if I turn this off?*

Should be asked *against any part of your IT infrastructure*

Implement redundant systems, failover mechanisms, and disaster recovery capabilities to minimise single points of failure and ensure continuous availability of critical IT services.

Bottom line: If you can't answer the *what if?* question you've identified a resilience weak point in your transformation journey. Companies integrating SRE practices report 50% fewer critical incidents and 2.5 times faster incident recovery times.
If it is *resilient,* poking it shouldn't break it—theoretically!

Data Protection and Privacy Compliance

Too strict and they'll *circumvent it*

Too loose and you'll be front page news *Find the balance*

Implement robust security controls, encryption, access controls, and monitoring mechanisms to safeguard data from unauthorised access, breaches, and cyber threats.

Bottom line: Organisations with a good balance are 50% less likely to suffer a data breach compared to those with overly rigid or too loose data protection measures. This balance allows for effective compliance without stifling operational flexibility, ensuring both security and business agility. Humans will always follow a path of least resistance, so implement controls to elevate the work practices, not stifle them.

> *After 30+ years of experience...*
> Execute the simple things well. CIOs and their teams often get distracted by overseeing new changes, becoming unaware of rising technical debt or changing risk profiles.
> The answer? Nail the basics. Go slow to go fast!

Vendor and Third-Party Risk Management

You wouldn't *invite just anyone into your home*

So, qualify vendors *like family (at least you get to choose them)*

Conduct thorough due diligence and risk assessments of vendors to ensure they adhere to security best practices, compliance requirements, and contractual obligations.

Bottom line: Experienced vendors may tick all the boxes, but are they a fit for your business maturity, culture, and future partnering needs? Underdeveloped vendor partnerships may result in you paying to mature their operations. Overpaying for a highly mature vendor can lead to significant costs with minimal benefits.

Security Awareness and Training

We all want *to be secure to do what we want to do*

The whole team *must be on board and know their roles*

Assess your organisation's security awareness and training programs to educate employees about cybersecurity threats, best practices, and their role in maintaining IT security.

Bottom line: Providing regular training and awareness to employees at all levels can reduce human error, insider threats, and social engineering attacks. Generic security training casts a wide net but often misses the mark. *Targeted training, is a precision tool that addresses specific risks and user behaviours, leading to a 75% reduction in phishing susceptibility* (K. Mitnick).

Like to delve into, dissect or draw on my experience over a coffee—let's set up a time...

E L