IT RISKS:

BACKUP AND RECOVERY BLUEPRINT

UNITRENDS
A Kaseya COMPANY

Introduction

Modern enterprises are reimagining the traditional work models and transitioning to the hybrid model — the workplace of the future — due to the various benefits it puts forth. Both employers and employees are increasingly embracing this futuristic model.

However, in the quest to address this growing hybrid workforce and fuel digital transformation, organizations have been undergoing radical changes, both from an IT and business perspective. For instance, organizations' data footprints are increasingly expanding beyond the conventional on-premise infrastructure to hybrid and multicloud environments. As a result, business-critical data now lives in more places than ever before, from on-premise data centers and multiple clouds to SaaS applications and remote endpoints. A widely dispersed workforce and data footprint also mean that businesses now heavily rely on their information and communication technology (ICT) infrastructure. With the advent of remote and cloud workloads, ICT systems have become the backbone of modern businesses that ensures collaboration and operational continuity.

While this transition offers many advantages, it's not all sunshine and roses for modern enterprises. As the amount of data created and stored across these multiple environments continues to grow, monitoring mission-critical data and its protection has become a Herculean task. More than 40% of cloud engineering and security professionals revealed that cloud-native services increase complexity and further complicate security efforts. The rapidly expanding data footprint and the growing reliance on new ICT systems — or cutting-edge technology — have introduced novel threat vectors and galvanized some others, which are waiting to leap at the opportunity to wreak havoc in your IT landscape.

© 2023 UNITRENDS // ALL RIGHTS RESERVED // WWW.UNITRENDS.COM

The latest reports from the cybersecurity landscape underscore these growing risks. According to **IBM Cost of a Data Breach Report 2022**, over 80% of the surveyed organizations have suffered more than one data breach. What's more alarming is the cost of remediating a data loss incident, which averaged an all-time high of $4.35 million in 2022. **Another survey by Statista** reports that around 70% of businesses were victimized by ransomware in 2022 — a record high. This ever-increasing and ever-evolving threat landscape can be a death knell for businesses if not tackled properly.

Over 80% of the surveyed organizations have suffered more than one data breach. What's more alarming is the cost of remediating a data loss incident, which averaged an all-time high of $4.35 million in 2022.

Failure of ICT systems due to security issues, such as systems intrusion or malware infection, will impact business continuity because the critical functions that ensure business continuity are usually dependent upon ICT systems. So, how can modern businesses protect their business-critical data and ICT systems from these rising security threats and keep them readily available? Organizations must weave together plans to create a holistic strategy, which includes:

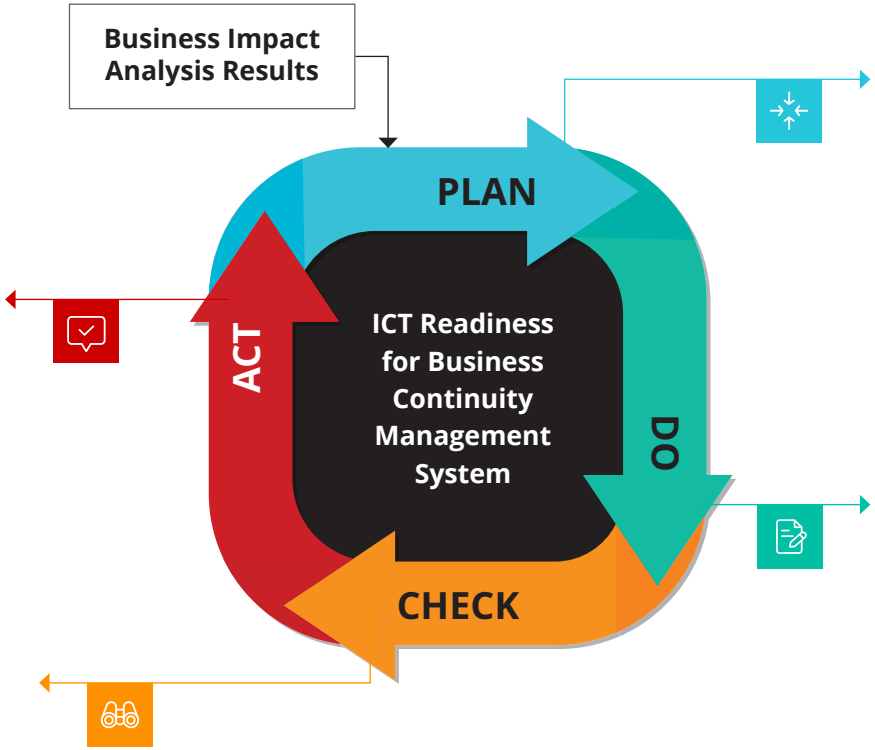
- A **risk mitigation plan** that reduces the impact of potential security risks.
- An **incident response plan** that gives clear guidance on what to do during an adverse incident.
- A **business continuity plan** that details how operations will be maintained during the event.
- A **disaster recovery plan** that restores operations to normalcy after the disaster.

This eBook aims to describe in detail how organizations can develop a comprehensive approach and achieve ICT Readiness for Business Continuity (IRBC) so that they continue to operate and meet their business objectives during times of disruptions. IRBC defines the capability of an organization to continue its business operations by preventing, detecting and responding to disruption of ICT services. Aligning with the ISO/IEC 27031:2011 standard that describes the concepts and principles of IRBC, we aim to provide you with a blueprint for ensuring your business continuity plan deals with any security incident and aid you in developing a consistent and confident approach to planning and implementing a disaster recovery (DR) plan.

© 2023 UNITRENDS // ALL RIGHTS RESERVED // WWW.UNITRENDS.COM

Backup and recovery blueprint

ISO 27031 provides a framework of methods and processes to guide organizations in identifying and specifying all aspects — such as performance criteria, design and implementation — to improve their IRBC. It guides IT pros on how to effectively plan for business continuity and disaster recovery (BCDR) by helping them recognize, respond to and recover from disruptions to ICT services.



PLAN

- Develop business requirements based on BIA results
- Understand critical ICT services
- Develop/update IRBC Policy
- Identify performance gaps
- Develop strategy options

DO

- Document IRBC processes
- Implement IRBC Strategies
- Implement/update ICT response and recovery plans
- Execute training and awareness activities

CHECK

Ongoing

- Monitor, detect and analyse threats
- Measure IRBC performance

Annual Review

- Test and exercise IRBC strategies
- Review and audit by internal and external groups

ACT

- Management reviews IRBC program
- Management directs IRBC improvement measures

© 2023 UNITRENDS // ALL RIGHTS RESERVED // WWW.UNITRENDS.COM

Organizations need to implement a systematic process to prevent, predict and manage disruptions and incidents that can potentially disrupt ICT services, which is best achieved by employing a Plan-Do-Check-Act (PDCA) cycle. The goal of the PDCA cycle is to put into action measures that can improve preparedness and response in the event of an interruption in ICT services. By doing so, you can ensure both information security management (ISM) and business continuity management (BCM) are effectively carried out. Ensuring the continuity of ICT services helps in monitoring, access control, safe transmission and secure storage of confidential information, thereby aiding in ISM. At the same time, by assuring that the ICT services are resilient and recoverable within a pre-determined period, the PDCA cycle also helps support BCM.

PLAN

Planning is the first stage in the PDCA cycle, where the overarching governance structure of the IRBC management system is established and maintained. During the planning stage, an IRBC policy is formulated, which defines the best practices to be followed so the business can continue its operations amid an IT disaster and determines the potential IT strategy solutions that will help meet those requirements. The goal here is to minimize the disruptions and losses caused by the incident while also enabling the business to meet its time-bound commitments. Establishing an incident response (IR) plan is critical; businesses without an IR plan incurred, on average, **data breach remediation costs $2.66 million higher** than those with an IR plan.

To realize operational continuity amid a disaster and swift recovery from it afterward, an organization must have an effective **BCDR plan** in place. A BCDR plan mitigates the damage and ensures the continuity of vital business processes during a disruptive event. It also includes steps to quickly restore ICT systems and data to resume business as usual after the event.

A major thing to consider here is the creation of a failback site to replicate/relocate the mission-critical data and ICT systems so that the business can continue its operation without disruption. It would be best if you also considered geographical and infrastructure risk factors, such as the need for multiple sites or backups in the cloud.

The planning stage must include a risk assessment and business impact analysis and establish the recovery objectives — **recovery time objective (RTO) and recovery point objective (RPO)** — accordingly. This stage can also be used to delegate roles and responsibilities, determine communication channels and document all the relevant processes and procedures.

© 2023 UNITRENDS // ALL RIGHTS RESERVED // WWW.UNITRENDS.COM

DO

The “Do” stage focuses on performing activities and implementing solutions that were established in the first stage so that the organization can keep an eye out and get back up and running in the event of an ICT services interruption. The key outputs for this phase are the implementation of determined strategies, the generation of appropriate plans and the execution of training and awareness activities to realize IT resilience and support the continuity of ICT services.

Tabletop exercises are an excellent practice on that front. When an unpredictable incident like a natural disaster or a cyberattack occurs, the more you are prepared, the better the results will be. Such exercises help teams experience firsthand the challenges that may arise and take on the roles they would need to during a real crisis. It also allows them to pinpoint areas that require improvement and prepare a step-by-step plan guideline.

CHECK

Imagine discovering that your recovery strategies and plans do not work in the midst of an IT disaster. That’s why it’s critical to have the “Check” phase, where the review and evaluation of your backup and recovery plan and the performance of the IRBC management system take place. The key outcome of this phase includes continuous monitoring of ICT systems for disruptions and periodic reviews of ICT responsiveness and recoverability.

Organizations need to have a comprehensive DR plan and conduct regular testing, failing which they could face devastating consequences while attempting a recovery during an emergency. However, DR testing can eat up your valuable resources and time and drastically impact your productivity if your organization lacks automated testing capabilities. You must be able to automatically test and certify your RTO, RPO and SLAs ahead of time without affecting your production servers.

© 2023 UNITRENDS // ALL RIGHTS RESERVED // WWW.UNITRENDS.COM

ACT

In the final phase, the leadership should assess how effectively the whole IRBC strategy is working and consider implementing remedial measures to improve the effectiveness of the initiatives and lessen the likelihood of interruptions to ICT services. This stage ensures the continuous improvement of IRBC and, thereby, the organization's readiness to handle unforeseeable events that could jeopardize business operations.

More than 40% of cloud engineering and security professionals revealed that cloud-native services increase complexity and further complicate security efforts.

© 2023 UNITRENDS // ALL RIGHTS RESERVED // WWW.UNITRENDS.COM

Backup and recovery with Unitrends Unified Backup

As organizations become increasingly reliant on reliable, safe and secure ICT infrastructures, it has become critical for them to effectively thwart the ever-burgeoning threat landscape. A natural disaster, a cyberattack or even a small human error can put your mission-critical systems and data at risk, bringing your business to a standstill.

That's where Unitrends Unified Backup saves the day. No matter where your data resides — be it on-premise data centers, various clouds, SaaS applications or remote endpoints — Unitrends Unified Backup can ensure your business-critical systems and data stay safe, secure and readily available all the time, at a price that best suits your budgets and needs.

Whether you have one virtualization platform with a handful of virtual machines (VMs) or a complete data center environment with physical servers and thousands of VMs, Unitrends Unified Backup can protect them all.

Do you not have the money, time and resources required to research, implement and test DR plans?
No problem, Unitrends DRaaS will help you protect your critical workloads at a cost significantly lower than what you would have to bear when you build and manage your own off-site DR.

Does your business-critical data reside on SaaS applications?
Unified Backup can get the job done.
Our platform offers native, cloud-to-cloud backup and recovery for critical SaaS data living in Microsoft 365, Google Workspace and Salesforce. All modules are managed from a central interface, providing users with a single pane-of-glass for all your backup and recovery needs.

© 2023 UNITRENDS // ALL RIGHTS RESERVED // WWW.UNITRENDS.COM

There are "bad days" in IT. Then there are the "really bad days," which can put the whole business at risk. These are just some examples where Unitrends has helped organizations like yours get past their worst days unscathed.

Anatomy of a DRaaS event

Founded in 1968, Safety Products Inc. (SPI) is a manufacturing company in Florida that produces safety apparel, signs and safety equipment, and fire extinguishers. SPI onboarded Unitrends to leverage both local backup and recovery and off-site DR from the same vendor. "We are not a large company, but data loss to us is really critical. It could result in the loss of the entire company," says Dennis Hershey, CTO of SPI. When the company learned that Hurricane Irma was scheduled to hit Florida in five days, they contacted Unitrends support to declare a disaster event and initiate failover. As Hershey recalls, "DRaaS spin-up began immediately." Unitrends spun up SPI's critical applications in the cloud and ensured they were able to maintain operations as usual.

Following the event, Unitrends also helped SPI enhance their DR plan and switched them to Unitrends Cloud, saving them an enormous amount of time and money. Shortly after the Hurricane Irma DR event, SPI faced another unfortunate security incident when they were hit with a Crypto Locker ransomware attack. Using the same Unitrends components that enabled DRaaS, SPI was able to recover in less than one hour. "We were fully restored in under an hour," states Hershey. He further adds, "Our previous product would take 20 minutes just to locate the files that required restoration."

> "We are looking to expand our DR capabilities now that we have seen how the process works with Unitrends. We know there are many other capabilities that their solutions provide and we want to see what else we can add to our DR strategy. — Dennis Hershey

© 2023 UNITRENDS // ALL RIGHTS RESERVED // WWW.UNITRENDS.COM

An IT pro's worst nightmare

Dualite Sales and Services, Inc. is a company headquartered in Ohio that creates signage, architectural awnings, fabrications and custom designs for brands such as Kawasaki, Sherwin Williams and Michelin. Dualite upgraded their backup system from tapes to Unitrends Recovery Series appliance, saving them plenty of time and giving them 100% backup and recovery confidence. Chris Rolke, IT director of Dualite, notes, "I have the confidence that all the data is there. Before Unitrends, I had to guess if a backup was complete."

Rolke's confidence was put to the test in June 2020 when he experienced an IT administrator's worst nightmare — a network-wide ransomware attack. In the middle of the night, he discovered that his entire network was compromised due to a massive ransomware attack. "I drove to the office and was in the door by 3 am," says Rolke. He started doing restores in the Unitrends user interface. "It just started happening. As far as Hyper-V restores, it was just like, 'Boom, they're back!' I'm like, wow, this is really cool," enthuses Rolke. After discovering the attack at 2 am, Rolke was able to restore to the point in time before the attack with minimal data loss.

> "I was able to remote access back in from home and verify and see Oracle data. I felt like someone gave me a billion dollars at that point.
>
> — Chris Rolke

© 2023 UNITRENDS // ALL RIGHTS RESERVED // WWW.UNITRENDS.COM

UNITRENDS
A Kaseya COMPANY

More than 30,000 businesses like SPI and Dualite have put their faith in Unitrends and reaped the benefits — and your business could be next.

Get a backup and recovery solution that best suits your budget and needs and gain 100% confidence in your recovery capability.

Get a demo today!

PART # WP-2125-ENG-A