North Risk Partners®

XIGENT
Result Driven IT

CYBER RANSOMWARE ATTACKS: THE ROLE OF DISASTER RECOVERY & BACKUP PLANS

DECEMBER 2024

PRESENTER

Amos Aesoph

Chief Information Security Officer

Xigent

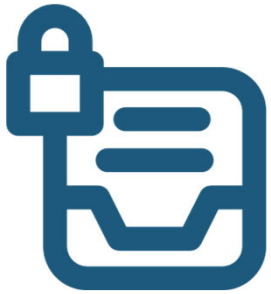
NORTH RISK PARTNERS®

XIGENT Result Driven IT

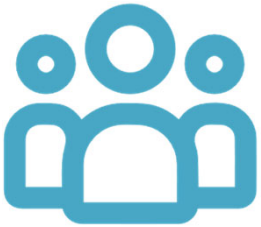
UNDERSTANDING THE THREAT OF RANSOMWARE

- Ransomware is a rapidly growing threat that encrypts data or locks systems, causing severe disruptions to businesses of all sizes.
- In 2023, ransomware attacks increased by 65%, with average ransom demands exceeding $1 million.
- Small businesses are particularly vulnerable, as 43% admit they lack a comprehensive recovery plan. Addressing this threat requires layered defenses and a proactive approach.

UNDERSTANDING THE THREAT OF RANSOMWARE



Encrypts Data or Locks Systems



Targets Organizations of All Sizes

Causes Financial, Operational, & Reputational Damage

POLLING QUESTION

NORTH RISK WEBINARS | 2024

STARBUCKS/BLUE YONDER

Blue Yonder Group, Inc.

American supply chain management company

Provides:

- Customer traffic on 30-minute intervals
- Automated planning for cleaning, admin time, deliveries
- Forecasted labor hours, staff availability, PTO, timecards, payroll
- Staff access for schedule viewing, time off requests

STARBUCKS/BLUE YONDER

November 2024, Blue Yonder suffered a ransomware attack that disrupted its managed services

Impact on Starbucks

Experienced significant operational challenges:

- Inability to manage employee schedules and payroll electronically
- Resorted to manual processes, such as using pen and paper, to track hours and pay employees

STARBUCKS/BLUE YONDER

December 3:

"We are making good progress; several of our impacted customers have been brought back online, and we are actively working directly with others to return them to normal business operations"

"We are recovering quickly and our back up system is working well"

HOW DISASTER RECOVERY MITIGATES RANSOMWARE RISKS

DR plans ensure systems and data can be restored.

Key Benefits:

- Reduced downtime
- Maintained business continuity
- Minimized damage

NORTH RISK PARTNERS®

XIGENT Result Driven IT

BACKUPS VS DISASTER RECOVER

1) Data Retention Requirements

Backup
Typically creates copies *on a daily basis* to ensure data retention at a single location

Disaster Recovery
Uses *recovery time objective* to determine the maximum length of time the business can withstand without its systems, typically requiring a duplicate data center location

2) Ability to Recover

Backup
Does *not* account for the physical resources to bring data online

Disaster Recovery
Makes provision for an *alternate environment* capable of sustaining your business until your primary environment is back up and running

3) Resource Needs

Backup
Requires *additional storage* to make copies of your data so you can restore it back to the original source

Disaster Recovery
Requires an alternative production environment where the data can live and run as it would in your primary environment – including *physical resources, software, connectivity and security*

4) Orchestration

Backup
Does *not* include a recovery plan or orchestration technology

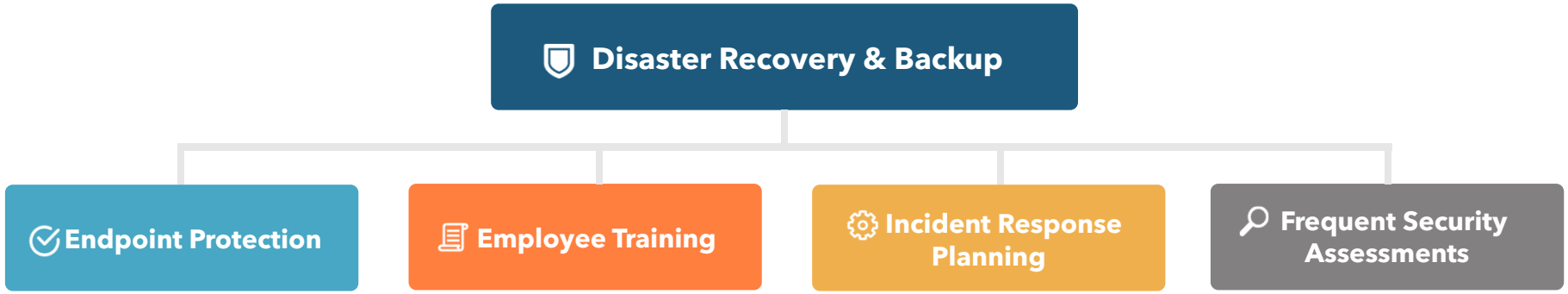
Disaster Recovery
Requires *planning and a comprehensive runbook* identifying which systems are considered mission critical, a recovery order, communication process and a way to *perform a valid test*

POLLING QUESTION

NORTH RISK WEBINARS | 2024

CREATING A MULTI-LAYERED DEFENSE

Disaster Recovery & Backup complement other measures:



LEARNING FROM REAL-WORLD EXAMPLES

MONDAY 05/23/2022 | **THE DAILY DISASTER** | PAGE #1

YOUR DAILY SOURCE FOR ANYTHING DISASTER RELATED

"Some data centers take their chances with floods"
Climate change is causing some IT leaders to consider relocating, or at least hardening, their facilities

"A tornado hit Nashville"
It wiped out the transportation company's headquarters, including the data center hosting crucial systems

"New York City's Law Department Got Hacked"
https://www.nytimes.com › nyc-law-department-hack

"John's Regional Medical Center building"
Stands in unusable condition and the 1,200-sq-ft data center is a "total loss"

"Linux Variant of HelloKitty Ransomware"
Targets VMware ESXi Servers

BLACK HILLS FEDERAL CREDIT UNION

Established in 1941: BHFCU has been a trusted financial partner for its members for over 80 years, offering a wide range of personal, business, and agriculture banking services.

- BHFCU serves more than 80,000 members through 15-member service centers across South Dakota
- Provides loans, savings, investment services, insurance, credit cards, and protection products to meet the diverse needs of its members
- Prioritizes improving service to its members in every decision and meeting, ensuring a seamless and reliable banking experience

NORTH RISK PARTNERS®

XIGENT
Result Driven IT

THE CHALLENGE

- BHFCU faced gaps in its self-managed backup and recovery systems
- Critical data and applications were not being replicated
- Limited testing reduced confidence in recovery capabilities

THE CHALLENGE

BHFCU Objectives	✕Before Implementation
Reduce risk of downtime and data loss	Some essential data was not backed up and there was no confidence in platform recoverability
Maintain recovery system with a known monthly cost	BHFCU expended both staff and equipment budget maintaining both production and DR sites
Test and document recovery for confidence about capabilities	No assurance that the recovery system works as planned
Gain a relationship with a trusted tech partner/advisor	BHFCU staff manage all IT functions
Build recovery into cyber security plan	No confidence of business continuity after disruption
Get long-term data protection and recovery for less critical systems	Identified recovery gaps in tier 2 and 3 systems

THE SOLUTION

- BHFCU implemented a customized Disaster Recovery as a Service (DRaaS) and Backup as a Service (BaaS) plan
- Regular testing and documentation of failover and recovery capabilities

Black Hills FEDERAL CREDIT UNION℠

+

XIGENT Result Driven IT

THE CHALLENGE

BHFCU Objectives	✓After Implementation
Reduce risk of downtime and data loss	All critical components run on-premise with continuous data protection
Maintain recovery system with a known monthly cost	BHFCU has known monthly costs, along with less personnel expense, as Xigent maintains systems
Test and document recovery for confidence about capabilities	Bi-annual scheduled failover testing by running production from a remote secondary site, including documentation that can be used for compliance audits
Gain a relationship with a trusted tech partner/advisor	Xigent provides ongoing consulting on right-fit technology and IT strategy
Build recovery into cyber security plan	A multi-layered cyber security approach that includes the ability to recover data and systems
Get long-term data protection and recovery for less critical systems	Complete Backup as a Service (BaaS) and recovery for tier 2 and 3 systems, including Microsoft 365

BENEFITS & RESULTS

Benefits of DRaaS

- Continuous data protection and replication of all critical systems
- Scheduled failover testing ensures recoverability and compliance
- Reduced risk of downtime and data loss

Overall Results

- BHFCU now has a well-managed recovery system.
- Proven recoverability through annual testing.
- Enhanced confidence in IT capabilities and member service

POLLING QUESTION

NORTH RISK WEBINARS | 2024

TAKEAWAYS FROM TODAY

- The essential role of disaster recovery (DR) and backup in minimizing the impact of ransomware attacks and enabling rapid data restoration and business continuity
- Effective backup strategies and best practices—such as immutable backups, offsite storage, and regular testing—that enhance resilience and improve recovery outcomes after a ransomware incident
- How to integrate DR and backup plans into a comprehensive cybersecurity strategy, ensuring a proactive, multi-layered defense that aligns with compliance and insurance requirements

BE PREPARED, STAY RESILENT

- DR and backup are vital tools against ransomware.
- Regularly review and test your strategies.
- Invest in a comprehensive plan to ensure resilience

QUESTIONS & DISCUSSION