
February 2020

Cyber Resilience Strategies for Protecting your Data from Sophisticated Cyberattacks

sambath.narayanan@dataeverconsulting.com



Session Objectives

- Cyberattack Case study and Learnings
- Understand the Cost of a Data Breach
- What is Cyber Resilience ?
- We have Cyber Security, don't we ? What is the difference ?
- Why Cyber Resilience ?
- NIST Cyber Security Framework
- Cyberattack : Business Impact vs Timeline
- The 5 Key Cyber Resilience technologies
- Key Takeaways



Devastaing sophisticated Malware that raced to 130 countries in hours

- June 2017.
- Ground Zero - Server Room. Likosys Group, Ukraine
- M.E.Doc software- anyone does Biz in Ukraine must use it to file Taxes



- Hackers used update servers to get Backdoor entry to release NotPetya Malware into 1000s of systems around the world
- Hacker Tools used: Mimikatz and Eternal Blue

- Malware spread worldwide from Hospitals in US to Chocolate factory in Australia – Govt offices, Banks, Gas station, Nuclear plants wasn't spared

Learning : Sophisticated Cyber attacks used networked systems to spread globally with high velocity



In hours, entire network of 4000 servers and 45000 PCs crashed

- Global corporation HQd in an European country
- Computer Terminal room. To her horror the admin was seeing all the monitors turning from Green to Black. Black. Black.Black,...
- In hours, entire network of 4000 servers and 45000 PCs crashed Website down. IT Help desk unavailable




- None could find one critical layer of N/W domain controllers. Entire user access depends on this.
- No Domain controller. No recovery possible. Period.
- After frantic search ...

- Lone surviving domain controller in a remote office in Ghana could be found. Before the Cyber attack Ghana systems went out of the Network. Thanks to the Power Outage !!
- After 2 weeks company was back in operation !

Learning : Golden copy: Protect the backup of crucial data outside the network



The Cost of a Data Breach 2019 Report's Summary Findings

Global Averages 	Average size of a data breach	25,575 records
Average total cost of a data breach \$3.92M	Cost per lost record	Time to identify and contain a breach
	\$150	279 days
	Highest country average cost of \$8.19 million	Highest industry average cost of \$6.45 million
	United States	Healthcare

*The Business impact of Cyber outages and odds of occurrence are very high. The estimated **global cost of WannaCry ransomware attack alone is US\$ 4 billion.***



Business Impacts of a Cyberattack

- Not just financial loss, there would also be
 - **Lost customer data, damage to brand reputation, and non-compliance to security breach notification laws.**
- The adverse impact to the Business due to a breach at the large credit reporting agency¹.
 - **145 million customers**
 - **CEO had to resign**
 - **investigation from a financial conduct authority.**



What is Cyber Resilience ?

Cyber resilience is an organizational capability to prepare for, respond to and quickly recover from known and unknown types of cyber attacks with minimal Business Impact

Business Benefits of Cyber Resilience

- **Protects organizations and its assets against known and unknown Cyberattacks**
- **Ensures continuity of Business operations despite an attack.**
- **Minimizes the Business impact**

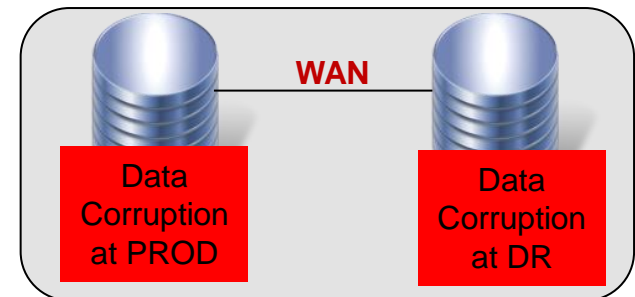
Traditional cyber security defence measures are not just enough. Organizations' ability to identify and rapidly respond to security breaches is now critical

Why a focused Cyber Resilience strategy required?

- **Business Risk:** Data corruptions, data theft, loss of personal information, paying ransom to decrypt systems that had been impacted, service outages and a combination of the above result in a significant Business impact.

To Speedup recoveries and to reduce Business impact Cyber Resilience strategy required

- **To contain corruption propagation.** Here, the WAN network is continuously exposed resulting in corruption propagation from production to the DR infrastructure, thereby making both primary and DR data unusable.



- **To handle new type of Cyberattacks** - traditional cyber security measures are no longer enough to protect organizations from the spate of persistent attacks(40% of all UK Business suffer a breach at least 1 per month)
- **To protect DR/Backup copies** which are vulnerable to corruption and can't be fully relied upon in the event of a cyber-attack. For example, the ransomware 'WannaCry Crypto Locker' targeted the shadow volume copies on Windows OS.

Cyber Resilience and Business Resilience are holistic organizational capabilities having a strong alignment

	Cyber Resilience	Business Resilience
Threat	Cyber Attacks	Natural or man-made disasters
Specific capability	Cyber Security	Business Continuity
Technology	Technical controls: End Point Defence, Authenticate, Authorize, Account, Cloud security, Encryption	IT-DR
Framework	NIST : Identify, Protect, Detect, Respond, Recover	Plan-Do-Check-Act (PDCA)
Alignment with Standard	ISO/IEC 27001:2013, ITF	ISO 22301
Compliance	GDPR, PCI-DSS	GDPR
Management System	ISMS	BCMS

NIST : Cyber Security Framework and Functions

Other available frameworks are more or less similar

Recover

- Recovery planning
- Recovery operation
- Communications
- Other Enhancements

Respond

- Incident management
- Communication
- Analysis
- Mitigation
- Other enhancements



Detect

- Anomalies, Events, incidents, breaches
- Continuous monitoring
- Detection processes

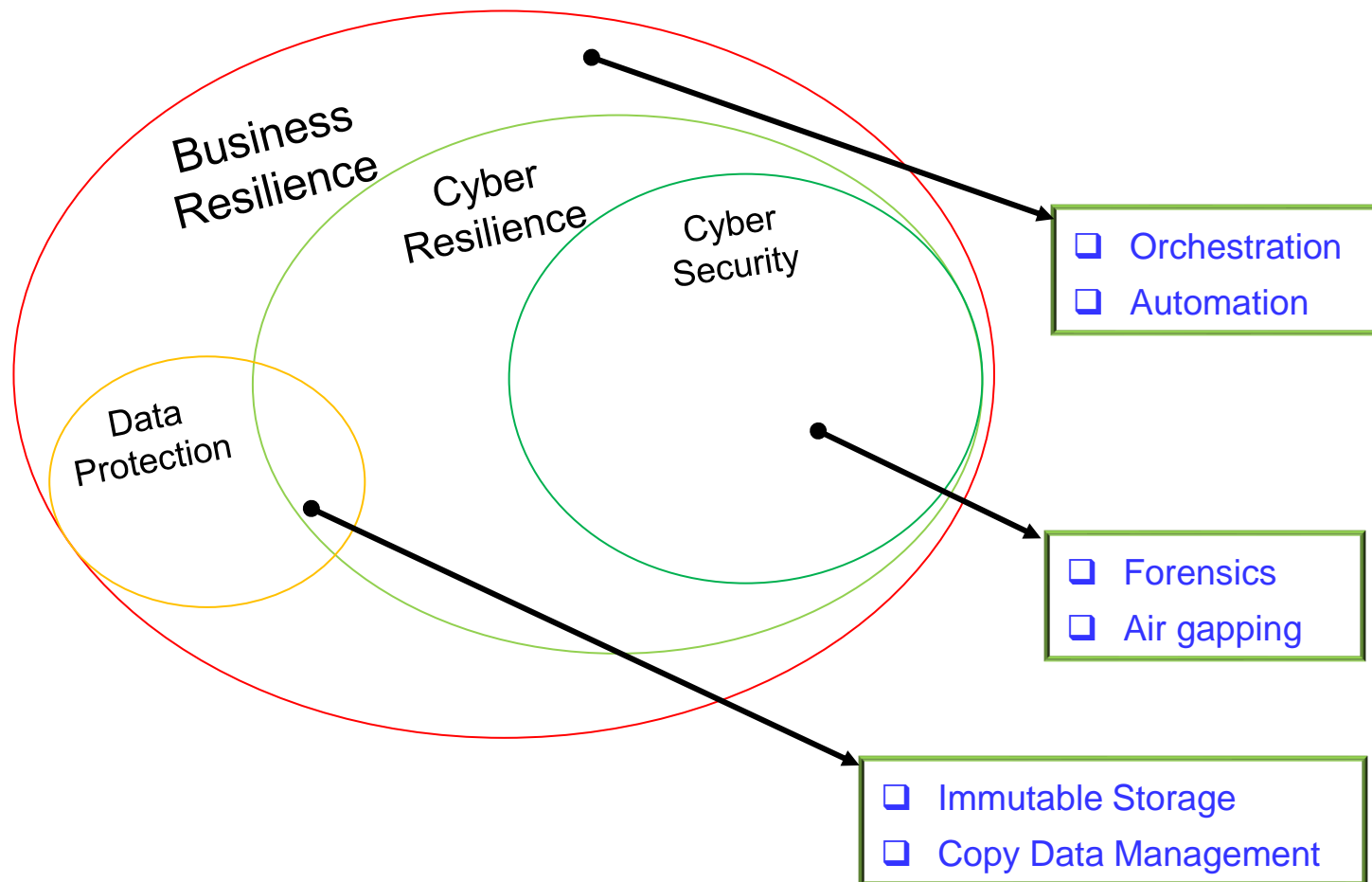
Identify

- Potential Threats
- Information Assets management
- Governance
- Risk assessment

Protect

- Access control
- Training
- Data security
- Information protection
- Maintenance
- Protection Technologies

Key Cyber Resilience capabilities are derived from Cyber Security, Business Continuity and Data Protection technologies



What are the top five technologies that form key part of Cyber Resilience ?



Air Gap protection

Means of isolating critical Data from networks to prevent unwanted access



Data integrity checking

Check the data integrity before it is used in production. Various techniques such as with data analytics, Forensics, DB/application tests can be used. Testing environment is very helpful for checking the data.



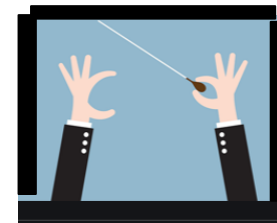
Immutable storage

Write Once Read Many times (WORM) storage. For a specified time duration, the data once written can't be deleted or modified



Copy Data management

CDM is a Lifecycle management of backups with ready to use point-in-time backup copies.



Orchestration and automation

Use of process workflows to automate the full cyber recovery

Strengthening the Cyber Resilience- benefits of technologies



Air Gap protection

Protects Data from Ransomware type of Cyberattacks



Immutable storage

Protects critical backups from Cyberattack induced deletion/corruption. **Helps in complying to Regulations.**



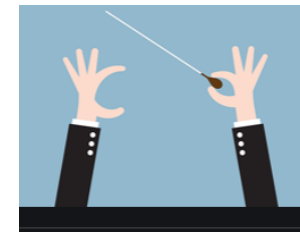
Data integrity checking

Prevents recurrence of Cyber threat from the protected Data



Copy Data management

Post Cyberattacks, CDM provides ability to **rapidly recover Business operations** from a specific time of the day. Streamlines Data protection.



Orchestration and automation

Minimizes insider threat and **reduces** recovery time objective

Key Takeaways ...

- It is not IF (cyberattack happens) but WHEN (cyberattack happens) ...
- Traditional cyber security measures alone are not enough to protect organizations from sophisticated attacks
- In order to move up from cyber security to cyber resilience, it is critical to evaluate and integrate new data protection technologies, airgap protection, immutable storage, forensics and orchestration
- Innovative technologies and solution strategies can effectively manage new types of threats – together they help to build a strong Cyber Resilience capability within an organization
- With a strong Cyber Resilience in place, the time to Respond and Recover can be reduced and thus reducing the adverse Business impact
- Thus safeguard Customer interests and be compliant to regulations

Additional Reference Material

- Data Breach Calculator

<https://bit.ly/33BaESy>

- **The Cost of a Data Breach Report is sponsored, analyzed and reported by IBM Security. Previous years' Cost of a Data Breach Reports are available at**

<https://ibm.co/2R7xwGL>

- ¹<https://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html>
- <https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/>
- IT Governance Green Paper : Implementing Cyber Resilience, Jan 2019
- IT Governance Green Paper : Cyber Resilience - Cyber Security and Business Resilience, Jan 2019

February 2020

Cyber Resilience Strategies for Protecting your Data from Sophisticated Cyberattacks

sambath.narayanan@dataeverconsulting.com