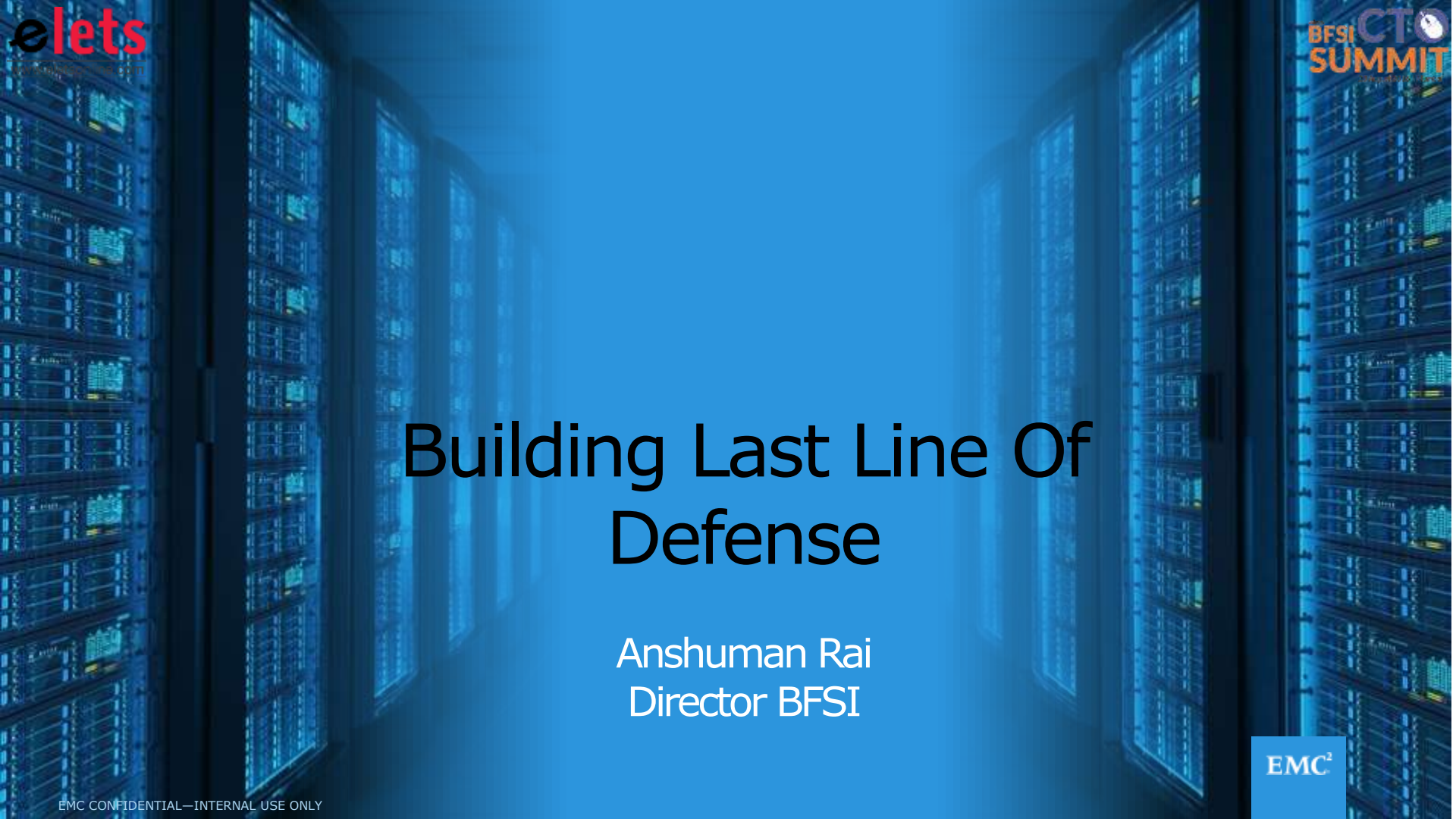


Building Last Line Of Defense

Anshuman Rai
Director BFSI

CYBER CRIME GETS SOPHISTICATED

ARE YOU STAYING AHEAD OF THE CRIMINAL EVOLUTION?

Traditional Threats

Cyber **Theft**

Denial of Service Attacks

Emerging Threats

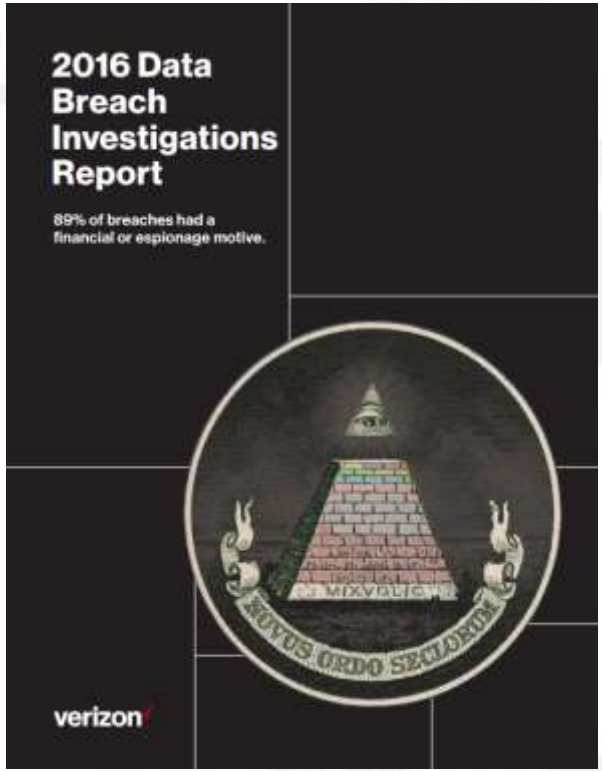
Cyber **Extortion**

Cyber **Destruction**

Isolated Recovery Solutions Protect Against these Classes of Attacks

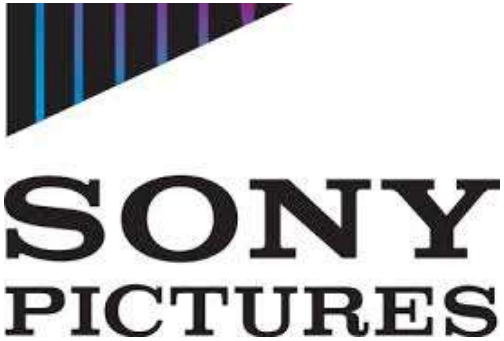
NATURE OF THE CHALLENGE

2016 DATA BREACH INVESTIGATIONS REPORT



- Breach Count Growing Exponentially Led By Hacking And Malware
- Attackers are able to compromise an organization within 6 minutes in 60% of cases.
- Likelihood To Discover The Breach Within Days Still Under 25%
- 58% of all data leaked in 2011 was owing to the actions of "ideologically motivated hacktivists."

THREAT EVENTS: A DIFFERENT CHALLENGE



"It erased everything stored on 3,262 of the company's 6,797 personal computers and 837 of its 1,555 servers. The studio was reduced to using fax machines, communicating through posted messages, and paying its 7,000 employees with paper checks."

- Fortune, July 2015

"The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key. In the best interest of restoring normal operations, we did this."

- Letter from CEO, Feb 17, 2016

THREAT EVENTS: UNPRECEDENTED RESPONSE

FBI releases flash memo titled "#A-000044-mw" within 6 days of the Sony event.

The report provided advice on how to respond to the malware and asked businesses to contact the FBI if they identified similar malware.

From the report:
"The overwriting of the data files will make it extremely difficult and costly, if not impossible, to recover the data using standard forensic methods."

- FBI Flash Report
  Dec 2nd 2014

FFIEC
FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL

"Data replication, however, may also be susceptible to simultaneous cyber attacks, and using this replication strategy may inadvertently result in backup or replicated data being destroyed or corrupted along with the production data.

The financial institution should take steps to ensure that replicated backup data cannot be destroyed or corrupted in an attack on production data.

...air-gapped data backup architecture limits exposure to a cyber attack and allows for restoration of data to a point in time before the attack began."

- FFIEC, Appendix J
  February 6, 2015

CYBER SECURITY FRAMEWORK - RBI

RBI/2015-16/418 DBS.CO/CSITE/BC.11/33.01.001/2015-16

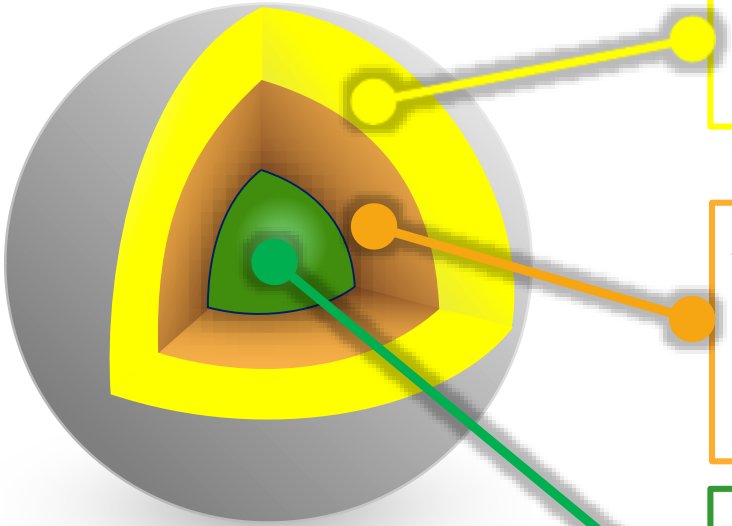
Banks **should immediately** put in place a cyber-security policy elucidating the strategy containing an appropriate approach to combat cyber threats given the level of complexity of business and acceptable levels of risk, **duly approved by their Board**.

Banks should **proactively initiate the process of setting up** of and operationalizing a **Security Operations Centre (SOC**) to monitor and manage cyber risks in real time.

CCMP should address the following four aspects: **Detection, Response, Recovery, Containment**

Considering the fact that cyber-risk is different from many other risks, **the traditional BCP/DR** arrangements may **not be adequate** and hence needs to be revisited keeping in view the nuances of the cyber-risk.

LAYERED CYBER SECURITY



Traditional Data Protection Best Practices

- Deploy a layered data protection approach ("the continuum") for more business critical systems but always include a point in time off array independent backup with DR Replication (N+1)

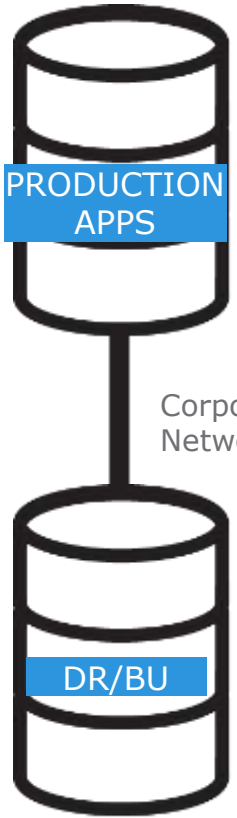
Additional Hardening & Protection Features

- DPS Product Specific Hardening Guides
- Encryption in Flight and/or at Rest
- Retention Lock w/Separate Security officer credentials

Advanced Protection Services

- Isolated Recovery Solution
- EMC Service Offerings
  - (Assess, Plan, Implement, & Validate)
- Use of Evolving Security Analytics
  - RSA Security Analytics

ISOLATED RECOVERY SOLUTION – OVERVIEW



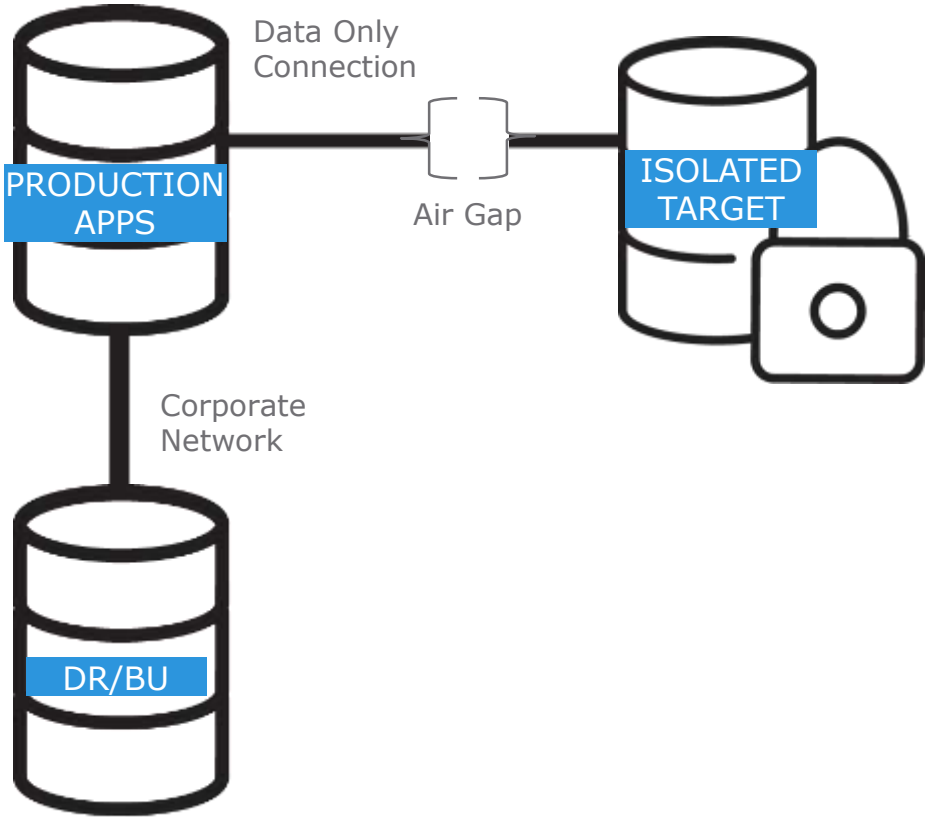
1

Planning and Design:

- Business Critical Applications
- Recovery Requirements
- Dependencies

Product Security / Hardening Procedures: support.emc.com

ISOLATED RECOVERY SOLUTION – OVERVIEW



1 **Planning and Design:**

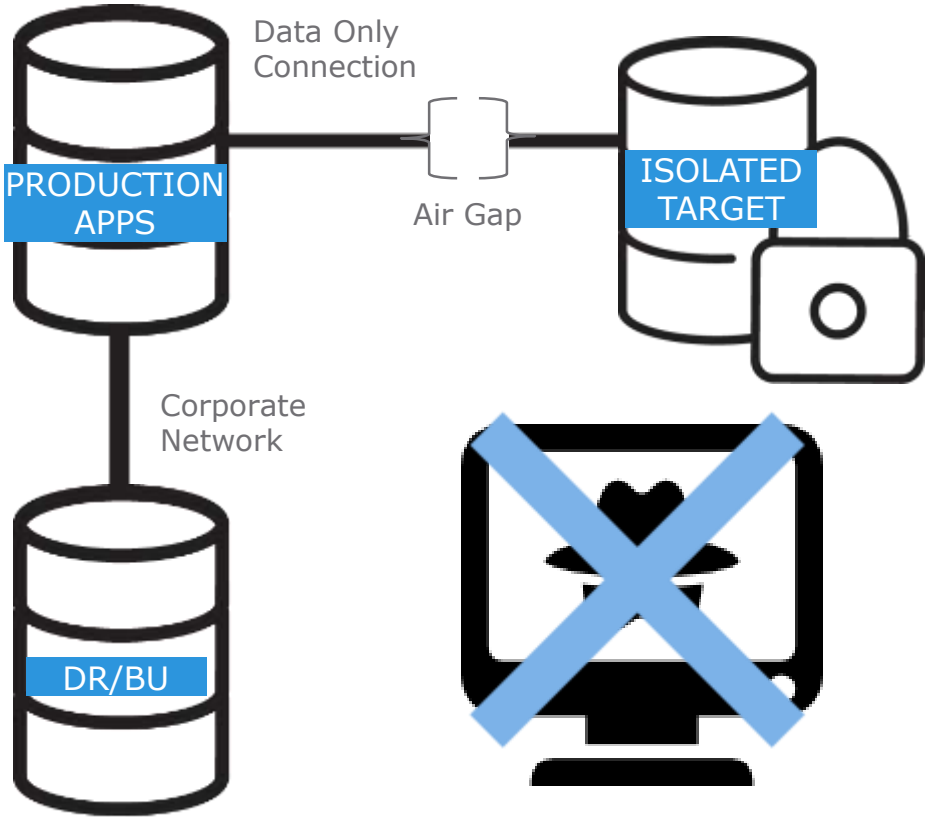
- Business Critical Applications
- Recovery Requirements
- Dependencies

2 **Isolation - Replication:**

- Network Isolation/Air Gap
- Dedicated Network Link
- Enable-replicate-disable link
- Automated and Scripted

Product Security / Hardening Procedures: support.emc.com

ISOLATED RECOVERY SOLUTION – OVERVIEW



1 **Planning and Design:**

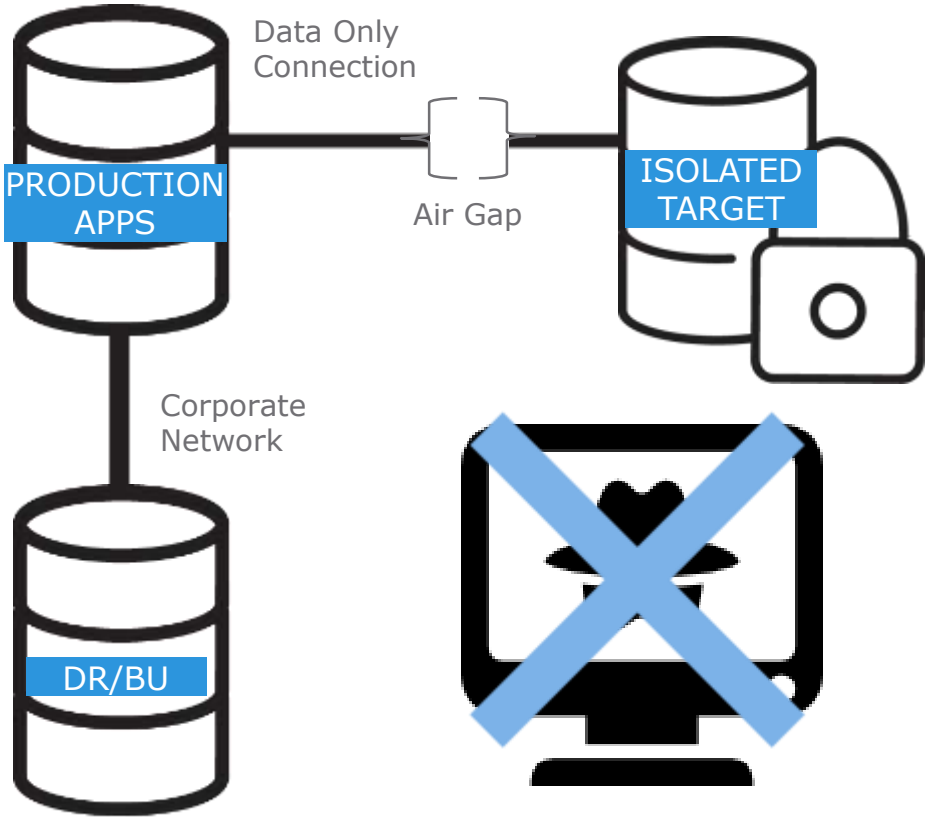
- Business Critical Applications
- Recovery Requirements
- Dependencies

2 **Isolation - Replication:**

- Network Isolation/Air Gap
- Dedicated Network Link
- Enable-replicate-disable link
- Automated and Scripted

Product Security / Hardening Procedures: support.emc.com

ISOLATED RECOVERY SOLUTION – OVERVIEW



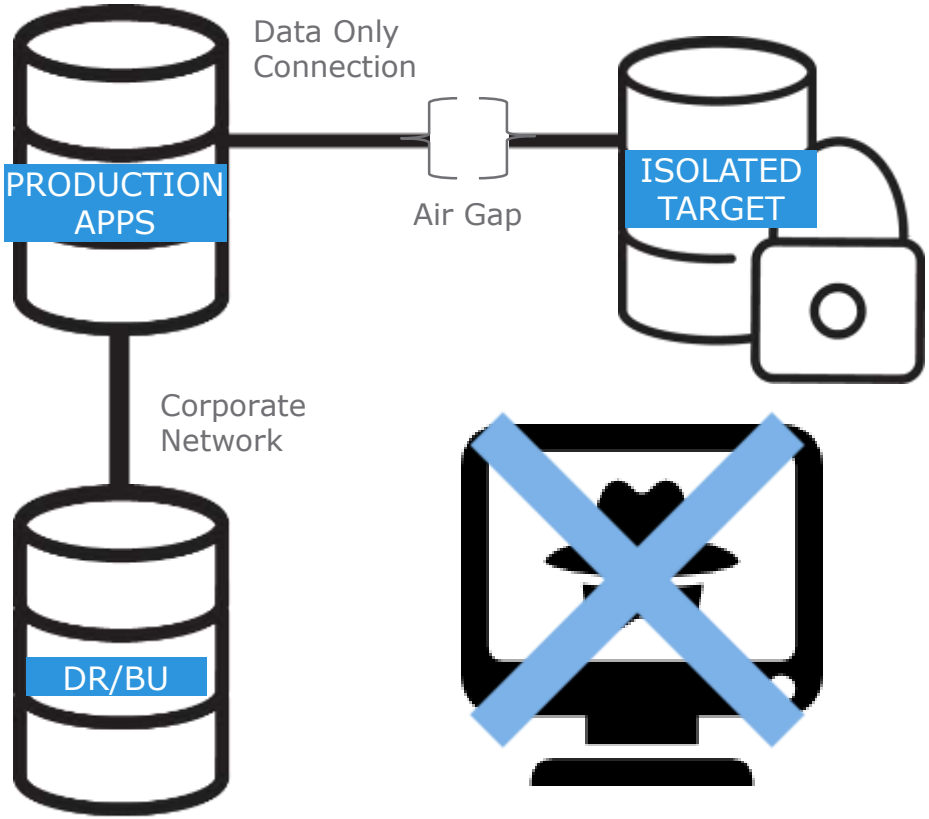
1 Planning and Design:
- Business Critical Applications
- Recovery Requirements
- Dependencies

2 Isolation - Replication:
- Network Isolation/Air Gap
- Dedicated Network Link
- Enable-replicate-disable link
- Automated and Scripted

3 Validation of Data:
- Trusted Copies and Versioning
- Validate Copy After Replication
- Tools and methods application dependent

Product Security / Hardening Procedures: support.emc.com

ISOLATED RECOVERY SOLUTION – OVERVIEW



1 Planning and Design:
- Business Critical Applications
- Recovery Requirements
- Dependencies

2 Isolation - Replication:
- Network Isolation/Air Gap
- Dedicated Network Link
- Enable-replicate-disable link
- Automated and Scripted

3 Validation of Data:
- Trusted Copies and Versioning
- Validate Copy After Replication
- Tools and methods application dependent

4 Restore and Recovery:
- Standard Restore Processes
- Additional validation recommended
- Ability to restore to dedicated restore host

Product Security / Hardening Procedures: support.emc.com

EMC'S IR SERVICES & NIST FRAMEWORK

Full Advisory Service Scope

NIST CYBERSECURITY FRAMEWORK

Identify	Protect	Detect	Respond	Recover
• Asset Management • Business Environment • Governance • Risk Assessment • Risk Management Strategy	• Access Control • Awareness and Training • Data Security • Information Protection Processes and Procedures • Maintenance • Protective Technology	• Anomalies and Events • Security Continuous Monitoring • Detection Processes	• Response Planning • Communications • Analysis • Mitigation • Improvements	• Recovery Planning • Improvements • Communications • Validation
EMC IR Services for Risk Management, Governance Model, & Operating Model	Isolated Recovery Solution Protective Technology, Processes & Procedures	Isolated Recovery Solution Validation Servers. RSA Security Behavior Analytics	EMC IR Services for Response Framework for Cyber Incident Management	Isolated Recovery Solution with Recovery Servers

EMC ISOLATED RECOVERY SERVICES & SOLUTION FRAMEWORK

HOW CAN EMC HELP: TWO APPROACHES

ADVISORY & IMPLEMENTATION SERVICES – OVERVIEW

Educate & Assess

Assess

- Business Application Protection Requirements
- Compliance Policies Requirements
- Application Readiness & Requirements
- Application Dependencies

Plan

- IRS Architecture & High-Level Design
- Technology Recommendations
- Implementation Plan & Timeline
- IRS Validation Test Design

Workshop Format

Advisory Service

Design & Build

Implement

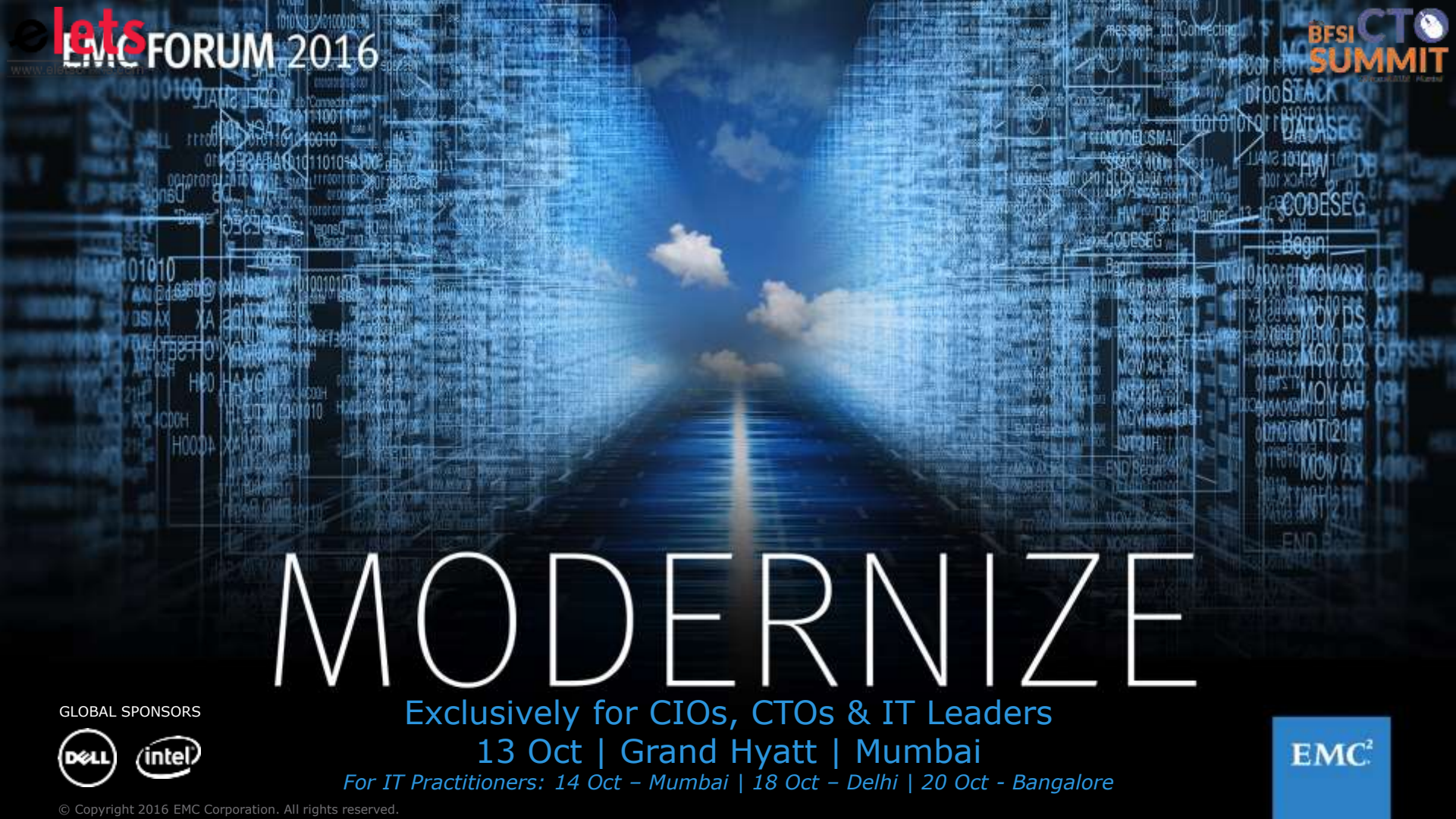
- Program Managed Implementation
- Technology Deployment & Hardening
- IRS Processes & Procedures
- IRS Run Books

Validate

- Compliance Ready Test Reports
- Facilitated IRS Table Top Exercises
- IRS Process Training
- Proctored IRS Test

Various Delivery Models

Implementation Service




EMC²