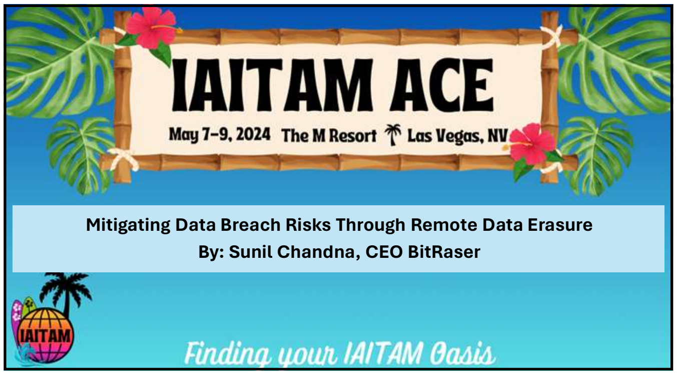
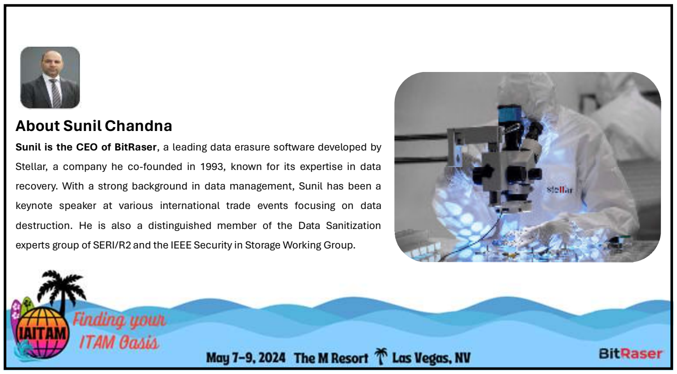


IAITAM ACE

May 7–9, 2024 The M Resort Las Vegas, NV

Mitigating Data Breach Risks Through Remote Data Erasure
By: Sunil Chandna, CEO BitRaser

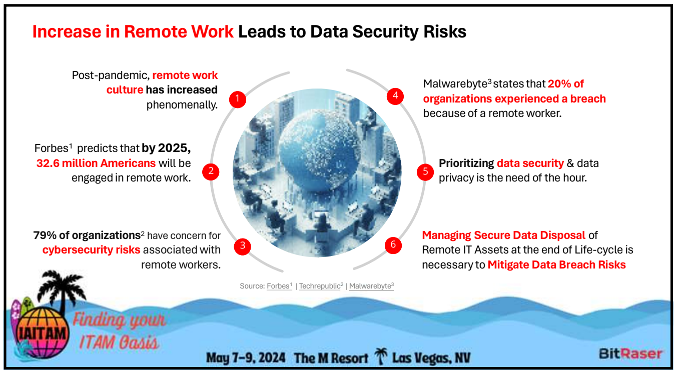
1



About Sunil Chandna

Sunil is the CEO of BitRaser, a leading data erasure software developed by Stellar, a company he co-founded in 1993, known for its expertise in data recovery. With a strong background in data management, Sunil has been a keynote speaker at various international trade events focusing on data destruction. He is also a distinguished member of the Data Sanitization experts group of SERI/R2 and the IEEE Security in Storage Working Group.

2

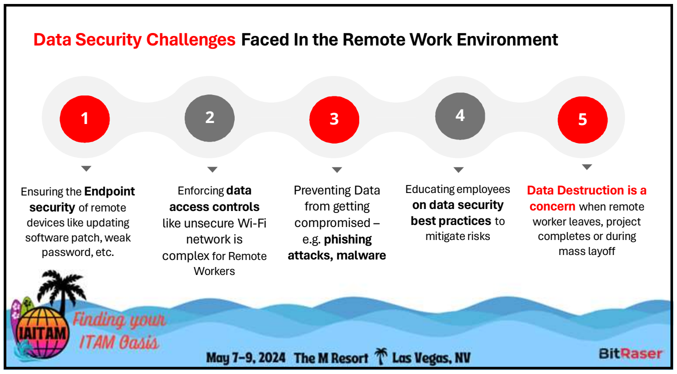


Increase in Remote Work Leads to Data Security Risks

1. Post-pandemic, **remote work culture has increased** phenomenally.
2. Forbes[1] predicts that **by 2025, 32.6 million Americans** will be engaged in remote work.
3. **79% of organizations**[2] have concern for **cybersecurity risks** associated with remote workers.
4. Malwarebyte[3] states that **20% of organizations experienced a breach** because of a remote worker.
5. **Prioritizing data security** & data privacy is the need of the hour.
6. **Managing Secure Data Disposal** of Remote IT Assets at the end of Life-cycle is necessary to **Mitigate Data Breach Risks**

Source: Forbes[1] | Techrepublic[2] | Malwarebyte[3]

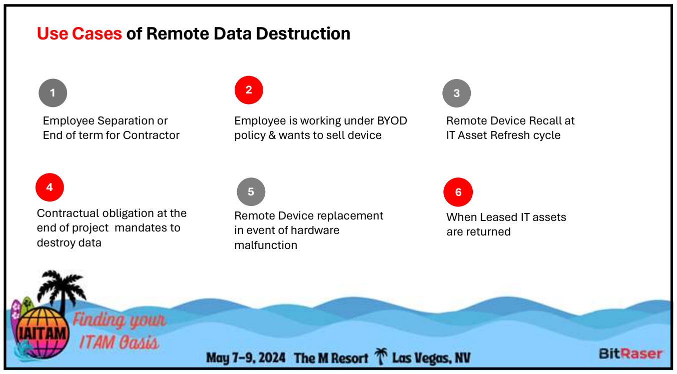
3



Data Security Challenges Faced In the Remote Work Environment

1. Ensuring the **Endpoint security** of remote devices like updating software patch, weak password, etc.
2. Enforcing **data access controls** like unsecure Wi-Fi network is complex for Remote Workers
3. Preventing Data from getting compromised – e.g. **phishing attacks, malware**
4. Educating employees **on data security best practices** to mitigate risks
5. **Data Destruction is a concern** when remote worker leaves, project completes or during mass layoff

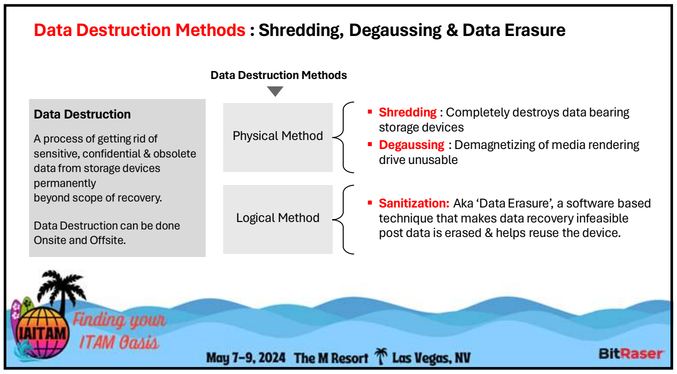
4



Use Cases of Remote Data Destruction

1. Employee Separation or End of term for Contractor
2. Employee is working under BYOD policy & wants to sell device
3. Remote Device Recall at IT Asset Refresh cycle
4. Contractual obligation at the end of project mandates to destroy data
5. Remote Device replacement in event of hardware malfunction
6. When Leased IT assets are returned

5



Data Destruction Methods : Shredding, Degaussing & Data Erasure

Data Destruction

A process of getting rid of sensitive, confidential & obsolete data from storage devices permanently
beyond scope of recovery.

Data Destruction can be done Onsite and Offsite.

Data Destruction Methods

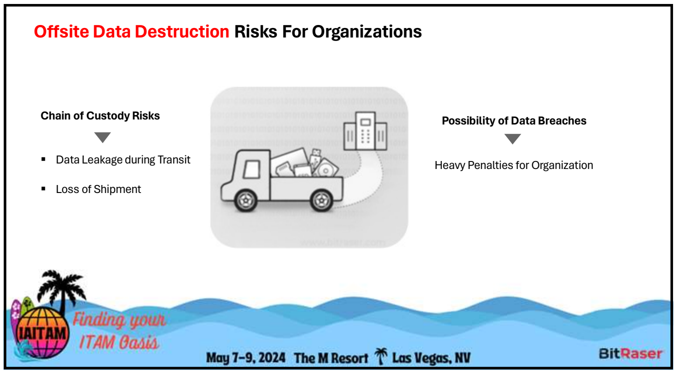
Physical Method

- **Shredding** : Completely destroys data bearing storage devices
- **Degaussing** : Demagnetizing of media rendering drive unusable

Logical Method

- **Sanitization:** Aka 'Data Erasure', a software based technique that makes data recovery infeasible post data is erased & helps reuse the device.

6



Offsite Data Destruction Risks For Organizations

Chain of Custody Risks

- Data Leakage during Transit
- Loss of Shipment

Possibility of Data Breaches

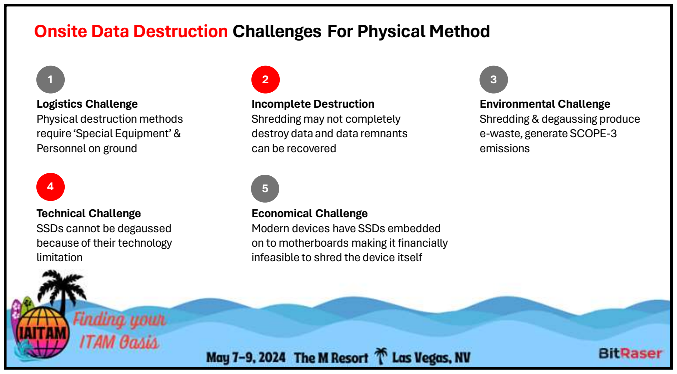
Heavy Penalties for Organization

IAITAM Finding your ITAM Oasis

May 7–9, 2024 The M Resort Las Vegas, NV

BitRaser

7



Onsite Data Destruction Challenges For Physical Method

1 **Logistics Challenge**
Physical destruction methods require 'Special Equipment' & Personnel on ground

2 **Incomplete Destruction**
Shredding may not completely destroy data and data remnants can be recovered

3 **Environmental Challenge**
Shredding & degaussing produce e-waste, generate SCOPE-3 emissions

4 **Technical Challenge**
SSDs cannot be degaussed because of their technology limitation

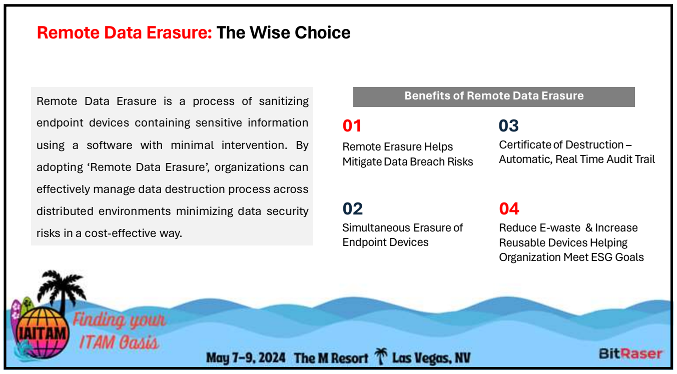
5 **Economical Challenge**
Modern devices have SSDs embedded on to motherboards making it financially infeasible to shred the device itself

IAITAM Finding your ITAM Oasis

May 7–9, 2024 The M Resort Las Vegas, NV

BitRaser

8



Remote Data Erasure: The Wise Choice

Remote Data Erasure is a process of sanitizing endpoint devices containing sensitive information using a software with minimal intervention. By adopting 'Remote Data Erasure', organizations can effectively manage data destruction process across distributed environments minimizing data security risks in a cost-effective way.

Benefits of Remote Data Erasure

01 Remote Erasure Helps Mitigate Data Breach Risks

02 Simultaneous Erasure of Endpoint Devices

03 Certificate of Destruction – Automatic, Real Time Audit Trail

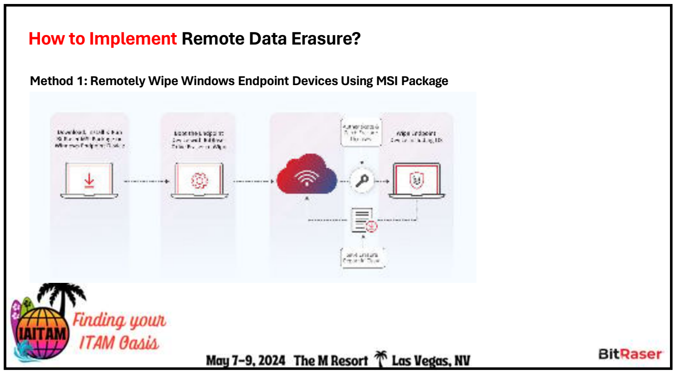
04 Reduce E-waste & Increase Reusable Devices Helping Organization Meet ESG Goals

IAITAM Finding your ITAM Oasis

May 7–9, 2024 The M Resort Las Vegas, NV

BitRaser

9



How to Implement Remote Data Erasure?

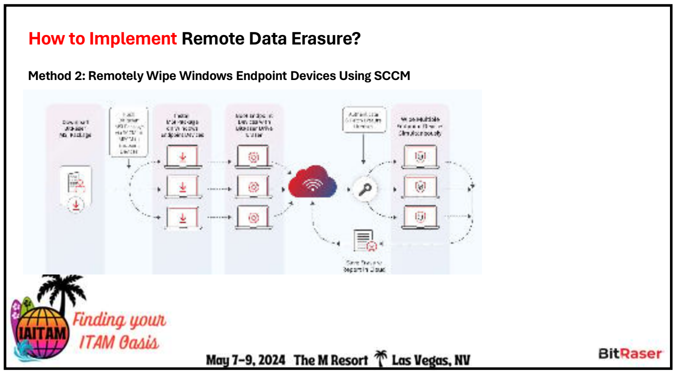
Method 1: Remotely Wipe Windows Endpoint Devices Using MSI Package

Finding your ITAM Oasis

May 7–9, 2024 The M Resort Las Vegas, NV

BitRaser

10



How to Implement Remote Data Erasure?

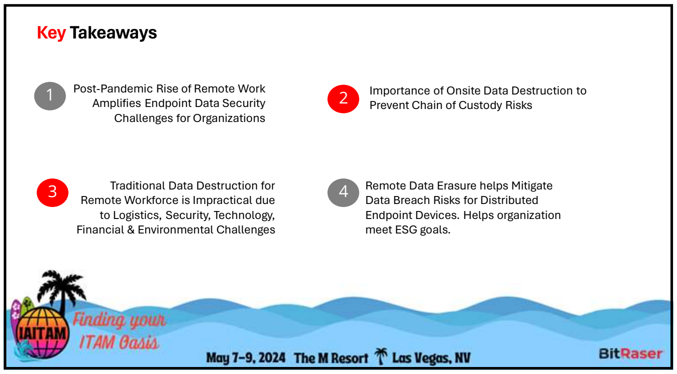
Method 2: Remotely Wipe Windows Endpoint Devices Using SCCM

Finding your ITAM Oasis

May 7–9, 2024 The M Resort Las Vegas, NV

BitRaser

11



Key Takeaways

1 Post-Pandemic Rise of Remote Work Amplifies Endpoint Data Security Challenges for Organizations

2 Importance of Onsite Data Destruction to Prevent Chain of Custody Risks

3 Traditional Data Destruction for Remote Workforce is Impractical due to Logistics, Security, Technology, Financial & Environmental Challenges

4 Remote Data Erasure helps Mitigate Data Breach Risks for Distributed Endpoint Devices. Helps organization meet ESG goals.

Finding your ITAM Oasis

May 7–9, 2024 The M Resort Las Vegas, NV

BitRaser

12