

# Reducing Cyberattack Risk During Uncertain Times



***Sean Deuby***

*Director of Services, Semperis*

# Active Directory at the Core

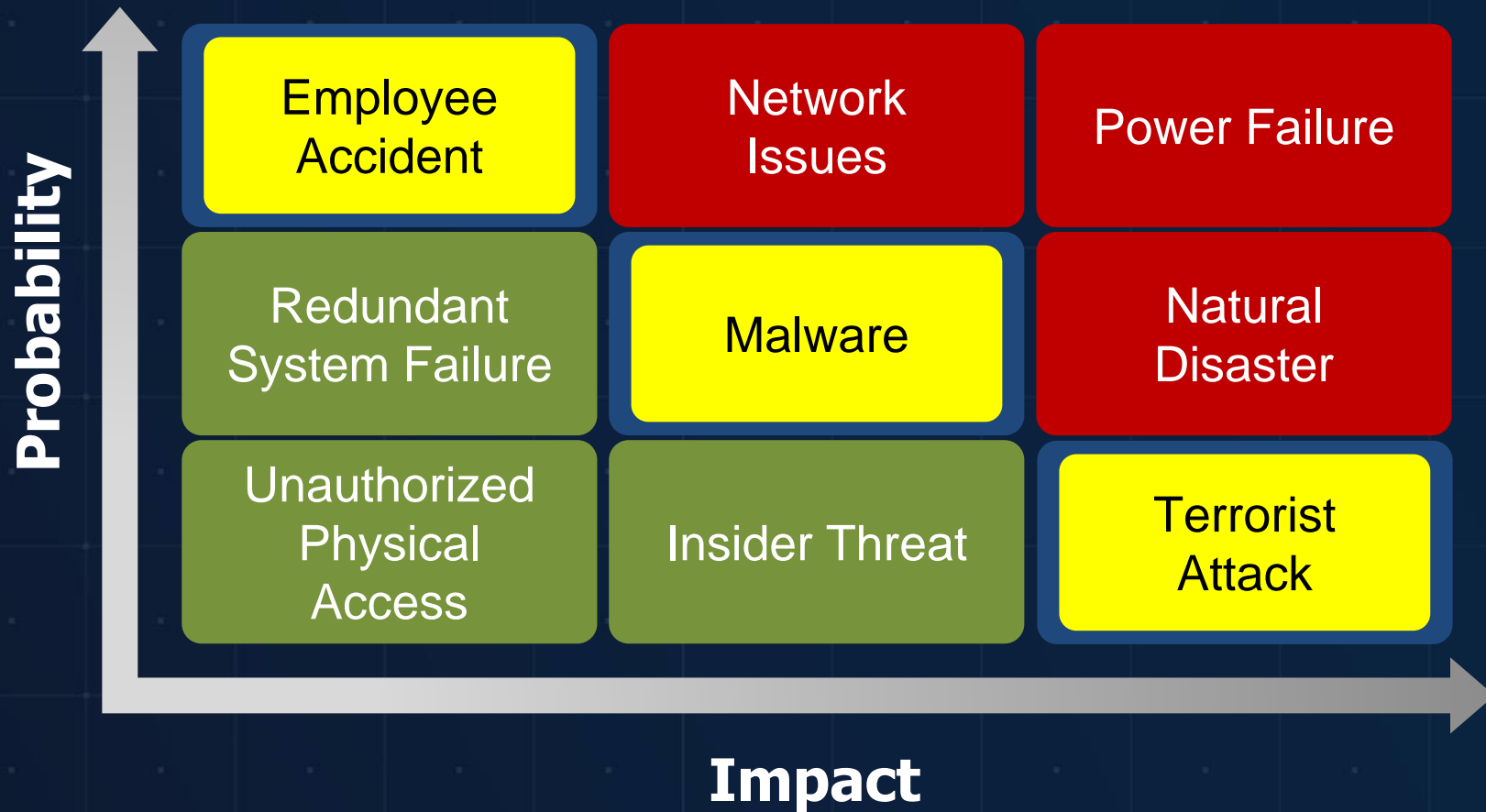
Active Directory is at the heart  
of your hybrid enterprise

If you haven't fully protected it,  
your organization remains  
vulnerable to catastrophic  
malware attacks

...and it's not as protected as  
you think it is



# Classic Disaster Recovery Risk Matrix







# What's Changed in the Threat Landscape?

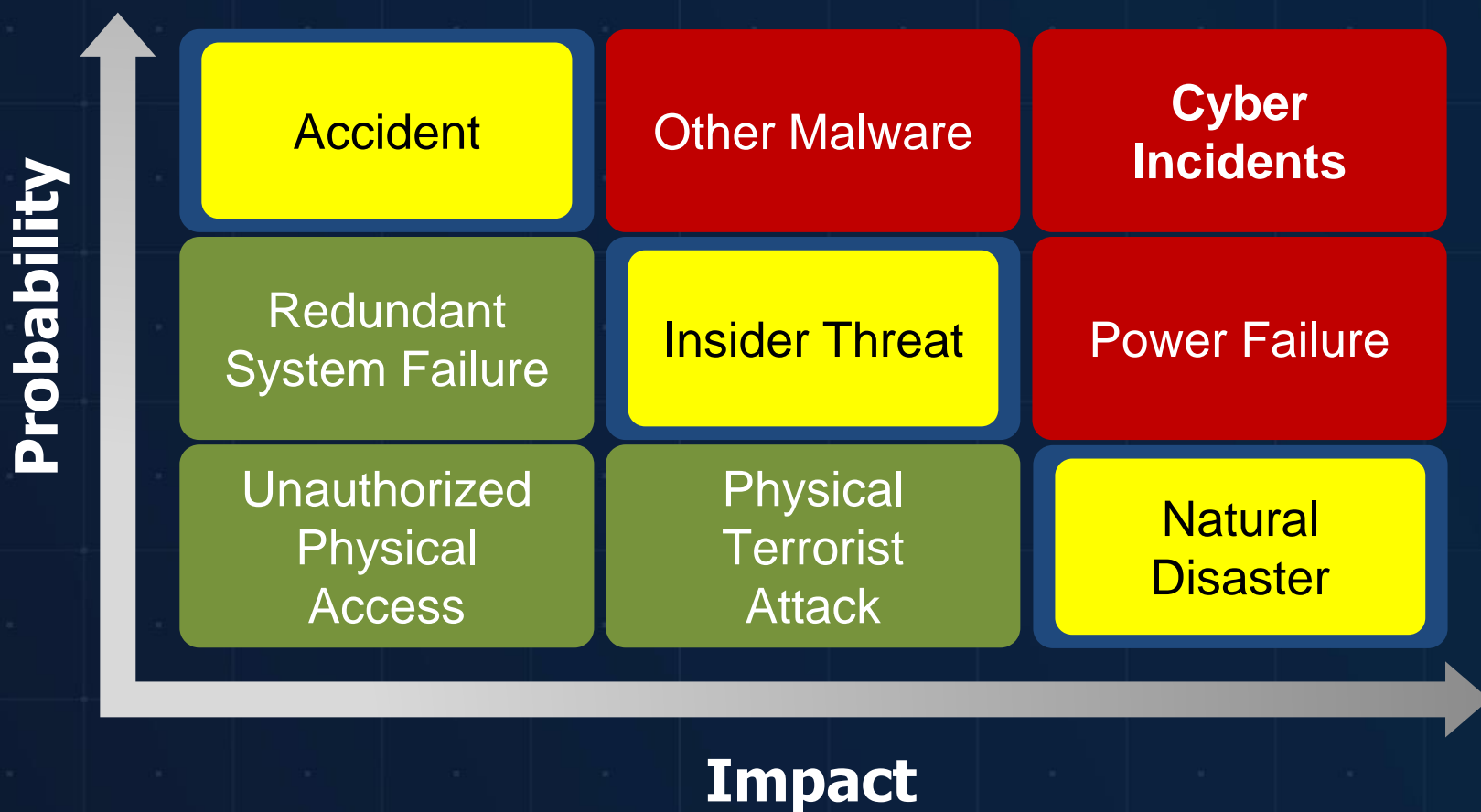
- In a word: **cyber**
- Classic threats are largely **geocentric**
  - Floods, power, wildfires, typhoons, etc.
  - That's why we have multiple data centers
- Cyber threats are **network centric**
  - Organization location is largely irrelevant
    - If you're on the internet, you're a target
  - Data center location is largely irrelevant
    - It's all the corporate network

# It's All About Identity – and It Will Happen

- **84%** of organizations worldwide suffered an identity-related breach in the last year<sup>1</sup>
- **78%** experienced direct business impacts such as recovery costs and reputational damage
- **96%** reported that they could have prevented or minimized the breach by implementing identity-focused security outcomes



# Cyber-First Disaster Recovery Risk Matrix



**How does Active Directory  
fit into this?**

---

# Active Directory in the Market

---

- Officially released in spring 2000
  - Most widely deployed Windows Server workload in Microsoft's history
  - 90% of organizations > 500 seats worldwide have it, and depend upon it
  - Hundreds of millions of AD users worldwide
- 





## KEYS TO THE KINGDOM

# 1: On-Premises Identity = Active Directory

Active Directory is the ubiquitous *glue* that empowers everyday activities.

The loss of Active Directory can put a halt to common, yet critical, operational activities.

It's easy to forget how dependent an organization has become on Active Directory.



## 2: Identity Is Central to Modern Security

"Identity is the **new control plane**."

—*Microsoft*

"Identity is **central** to providing appropriate, accurate and secure access to data, services and systems"

— *Gartner*

"Identity is a **core building block** of a robust Zero Trust security ecosystem and infrastructure."

- *Forrester*



### 3: Hybrid is the Dominant Identity Architecture

Most organization's identity systems are on premises

But SaaS apps (e.g. Microsoft 365) are extremely popular

Hybrid identity *projects* on-premises identities into cloud services to

- Use corporate identities for SaaS apps
- Provide secure single sign on

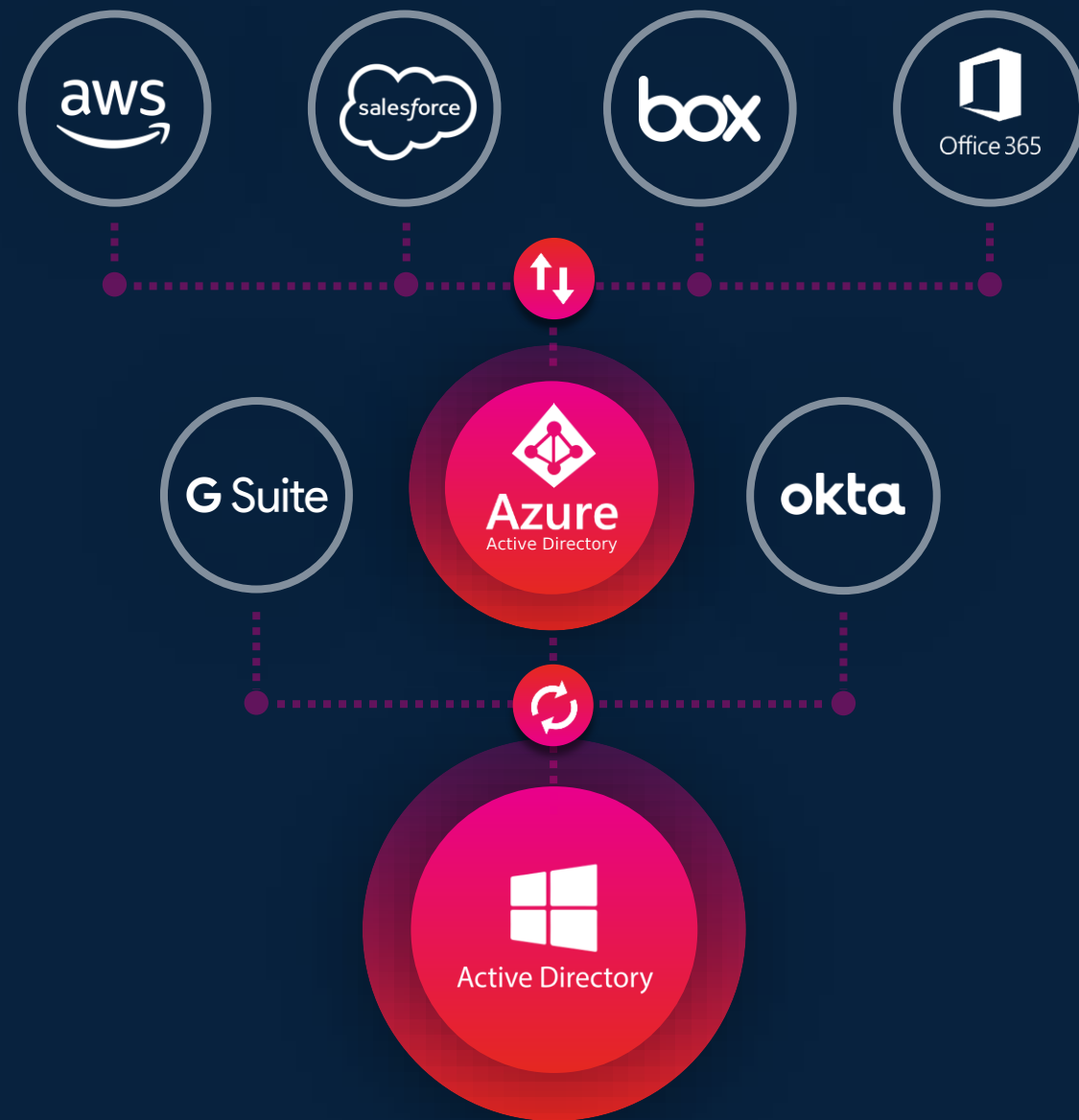


## KEYS TO THE KINGDOM

# 4: Active Directory is Central to Hybrid Identity

- Cloud identity extends from AD
- Zero trust model assumes hybrid AD integrity

➡ For 90% of enterprises, security starts with AD





## WIDESPREAD ATTACKS

# AD in the attackers' crosshairs

- 97% of organizations surveyed say that AD is mission critical
- The keys to the kingdom
- The treasure map to the data
- The pathway to spread the malware
- 57% say an AD outage would have “severe” or “catastrophic” impact



**NTT  
COMMUNICATIONS**  
2020



**BALTIMORE**  
2019



**NORSK HYDRO**  
2019



**SINGHEALTH**  
2018



**MAERSK**  
2017



**MONDELEZ**  
2017

**SONY**

**SONY**  
2014



**TARGET**  
2013

**aramco**

**SAUDI ARAMCO**  
2012



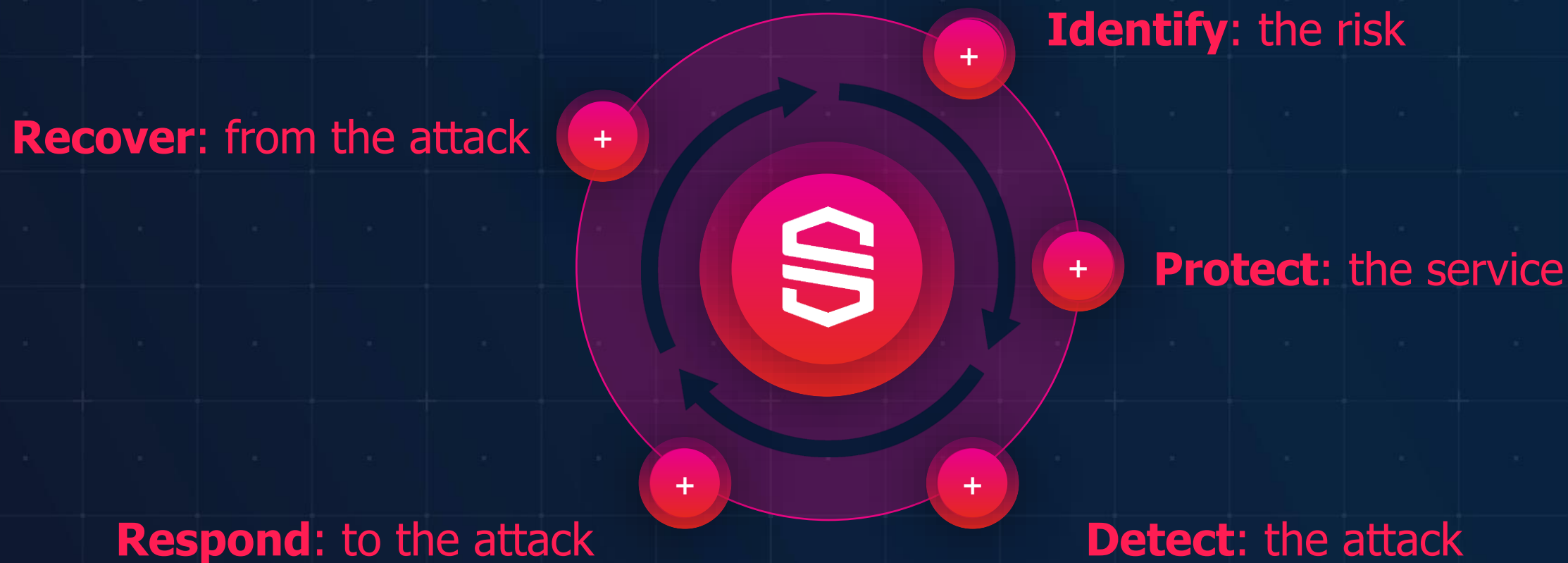
Many others

# Why is Active Directory So Vulnerable?

- AD security design is from another era
- “Your AD environment is a 22-year-old history of bad choices”
- Conventional recovery solutions can recover malware along with recovering AD
- Sophisticated attack tools
- Declining AD skillsets



# NIST Cybersecurity Framework



Before an attack

During an attack

After an attack







## MEET PURPLE KNIGHT

# Quickly evaluate the security of AD

**Purple Knight** is an Active Directory security assessment tool built and managed by an elite group of Microsoft identity experts. (5,000+ downloads)



**2021 GLOBEE® Winner**  
Risk Management Solution Innovation |  
Purple Knight

Learn more at [purple-knight.com](https://purple-knight.com) →

## SECURITY POSTURE OVERVIEW

This report summarizes the security assessment results performed in your hybrid identity environment on 07/12/22 by Semperis' Active Directory security assessment tool, Purple Knight. Depending on the environments selected for evaluation, the report includes the assessment results for an Active Directory forest, an Azure AD tenant, or both.

Active Directory forest: Purple Knight queried the Active Directory environment and ran a series of security indicator scripts against domains within the selected forest (see Appendix 1 – Domains list for a full list of the domains included in the assessment).

Azure AD tenant: Purple Knight queried the selected Azure AD tenant focusing on some of the most common attack vectors that threat actors use to gain access to the Azure AD environment.

The report provides an overall security risk score as well as detailed results about each Indicator of Exposure (IOE) found. By uncovering Active Directory and Azure AD security weaknesses, this assessment report provides valuable insight into the overall security posture across your hybrid identity environment and presents opportunities to minimize the attack surface and stay ahead of the ever-changing threat landscape.

[View Appendix 1 - Domains list](#)



▲ ACTIVE DIRECTORY



◆ AZURE AD

▲ Forest	f4.lab
📊 No. of Domains	1
🕒 Duration	00:00:24.9367601
👤 Run by	F4\Administrator

### Indicators

Evaluated	97
Not selected	1
🔴 IOEs found	39
✅ Passed	58
❌ Failed to run	0
ℹ Not Relevant	1
⏸ Canceled	0

◆ Tenant	Semperis F4 Hybrid
📋 Application ID	de0a18cd-cb2d-4ff3-95ce-8ee909df8e13
🕒 Duration	00:00:04.4430073
👤 Run by	F4\Administrator

### Indicators

Evaluated	10
Not selected	0
🔴 IOEs found	6
✅ Passed	4
❌ Failed to run	0
ℹ Not Relevant	0
⏸ Canceled	0

Before an attack

During an attack

After an attack



Before an attack

During an attack

After an attack

Recover



# NotPetya: Russian Cyber Weapon

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address:

1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWx

2. Send your Bitcoin wallet ID and personal installation key to e-mail [wowsmith123456@posteo.net](mailto:wowsmith123456@posteo.net). Your personal installation key:

sVC7Ff-MnXB05-Df1kXY-QHqef5-LCsHwN-G1F8bf-t9dgTM-eXsTVN-LTFMwM-VFXo1G

If you already purchased your key, please enter the key:

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address:

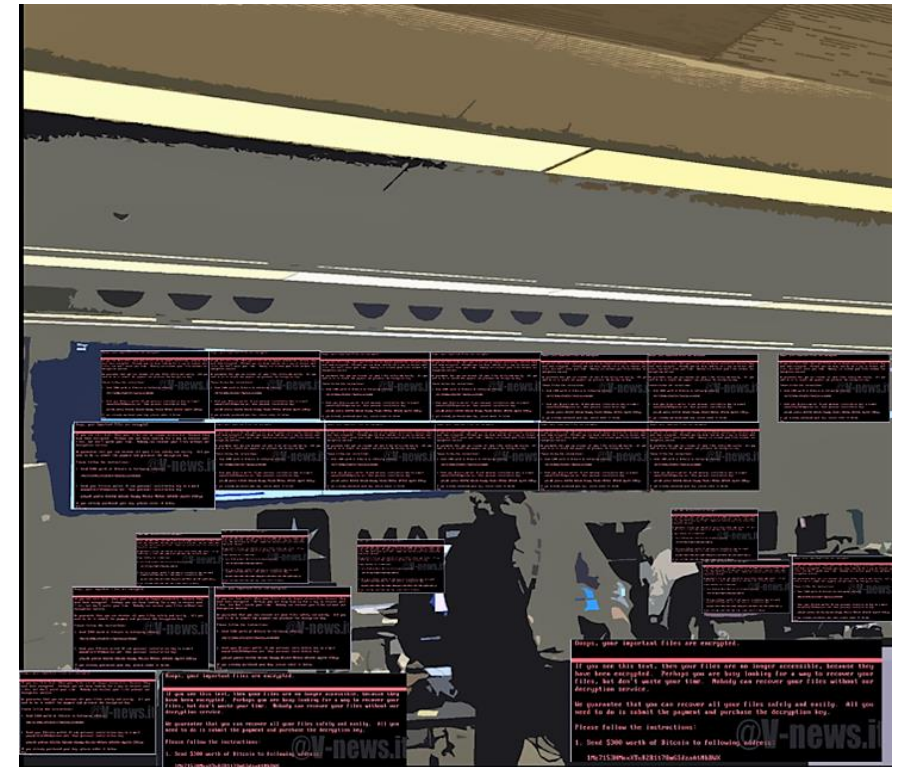
1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWx

2. Send your Bitcoin wallet ID and personal installation key to e-mail [wowsmith123456@posteo.net](mailto:wowsmith123456@posteo.net). Your personal installation key:



# Maersk and NotPetya


- World's largest shipping company
- First Russian supply-chain attack (e.g. SolarWinds)
- Collateral damage from Russia – Ukraine conflict
- Infected through a branch office PC
- 7 minutes later:
  - 55,000 devices destroyed
  - 146 of 147 AD domain controllers down
  - All 1200 critical applications offline
- CIO slept at the office for 70 days
- Estimated NotPetya losses worldwide: **\$10B**
- “(NotPetya) is what havoc looks like.”  
- Brad Smith, Microsoft President



## Few Can Recover AD Quickly After a cyberattack

- Only 37% of organizations understand the complexity of forest recovery
- >50% of survey responders have never tested their AD disaster recovery process – *or don't even have one*





**What steps should I take to reduce  
Active Directory cyber risk?**

## Action Plan: Identify & Protect

- **Evaluate your Active Directory risk profile**
  - Download and run Purple Knight
    - [Purple-knight.com](https://purple-knight.com)
  - Follow its guidelines to improve your score



## Action Plan: Detect & Respond

### ➤ Review your ability to protect and remediate Active Directory

- Monitor and track all activity
- Activity review (e.g. backdoor creation)
- Roll back unauthorized changes

## Action Plan: Recovery

### Mitigate the risk of a cyber-triggered corporate AD outage

- **Ensure** your AD and DR teams have a cyber-focused AD recovery plan
  - Understand the complexity of forest recovery
  - Don't recover malware with the recovered AD server
- **Build** your own recovery processes based on the Microsoft forest recovery doc
  - You *cannot* successfully perform a forest recovery without this pre-work
- **Consider** an automated recovery solution

“

***Nine days for an Active Directory recovery isn't good enough. You should aspire to 24 hours. If you can't, then you can't repair anything else.***

ANDY POWELL, MAERSK CISO

