Cyber Resilience

“In the last week of the quarter we were hit by a cyber attack. Business volumes were negatively affected for a couple of weeks in July and, as a consequence, our Q3 results will be impacted. We expect that the cyber attack will impact results negatively by $200-300M” [1]


CYBER RESILIENCE DEFINED

Cyber Resilience is the ability of an organization to minimize the operational impact of a cybersecurity incident. While organizations continue to focus much attention on security controls for preventing breaches and meeting regulatory requirements, cyber threats are increasing in sophistication and the consequences for system downtime have grown exponentially. Cyber Resilience is comprised of technology solutions and processes that support security, availability and regulatory requirements.

System downtime can have both immediate and long term adverse effects. Today, organizations are finding that customer or third-party applications that interact with their systems are not being reset nightly as had typically been performed in the past. If the system these applications are attempting to connect with is not available, they will roll over to an alternate system, which can often be a competitor’s system. These applications will not return to the default setting (your organization’s system) until they are reset, which, in today’s ‘zero-downtime’ landscape, may not occur for an extended period of time due to increased availability of applications.

Organizations are also increasingly seeking to leverage new technology capabilities like autonomous devices and empowered edge computing, which increase the importance of system availability, and simultaneously evaluating technologies to minimize the impact to operations when a security incident occurs. Some of these solutions may already be in place, but often need to be enabled.

HOW CAN ORACLE ASSIST

Many thousands of organizations run their mission critical systems on Oracle technologies. That said, every organization’s environment is unique, and it can prove difficult to ascertain exactly how to optimize the environment to minimize the impact to operations if an incident does occur. Oracle now offers a complimentary Cyber Resilience Assessment for customers who are utilizing Oracle technologies in mission critical systems and who might experience significant adverse business impacts if unplanned downtime occurs.

[1] CNBC “Shipping company Maersk says June cyberattack could cost it up to $300 million” (8/17/2017)
ORACLE CYBER RESILIENCE ASSESSMENT

- Running prepared scripts to assess the security posture of a selected Oracle database. The scripts evaluate existing configurations and security controls for the database with guidance from respected authorities like the Center for Internet Security (CIS) and the Defense Information Systems Agency (DISA) to assist in identifying potential misconfigurations and gaps.

- Answering a questionnaire about the specific database instance being analyzed, plus the organization’s cyber resilience maturity based on the Cyber Resilience Review (CRR) process published by the United States Department of Homeland Security.

- Prioritized recommendations for enhancing availability, security and regulatory compliance for the critical system. The assessment and resulting recommendations can be adjusted to prioritize availability, security or regulatory requirements, based on the organization’s desired focus.

Key Features

- PEOPLE – Oracle expert advisors certified in industry security standards and enterprise architecture methods

- PROCESS – Practical and proven security architecture development process focused on business enablement

- PORTFOLIO – Trusted artifacts including business models, reference architectures, Oracle best practices and business cases

Key Business Benefits

The Oracle Cyber Resilience Assessment will assist your organization with:

- Minimizing the financial impact from a cyber attack

- Focusing on your most important Cyber Resilience challenges

- Prioritizing actions leading to a strengthened Cyber Resilience posture

- Facilitating cooperation on Cyber Resilience initiatives

Cyber Resilience Deliverables

The Oracle Cyber Resilience Assessment will produce:

- Key Findings

- Recommended Priorities

- Business Benefits

Figure 1. Cyber Resilience Assessment process.

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com. Outside North America, find your local office at oracle.com/contact.

blogs.oracle.com/oracle facebook.com/oracle twitter.com/oracle

integrated Cloud Applications & Platform Services

Copyright © 2019, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 1019