
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

STP308

How to manage risk with minimal disruption

Tina Williams-Koroma (she/her)

Founder/CEO
CyDeploy

Ritik Khatwani (he/him)

Sr. Startup Solutions Architect
AWS

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

Speaker introductions

Balancing the risk of disruption

Common security, patch, and configuration testing approaches (pros and cons)

Recommendations

Resources

Q&A and contact information

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Ritik Khatwani

Senior Startup Solutions Architect

Ritik is Sr. Startup Solutions Architect at AWS based in New York City

He provides technical and strategic guidance to startups at various stages, helping them build and scale on AWS

He has over 13 years of experience building products as an engineer, architect, and founder

Away from work, he’s usually immersed in a book, blog, podcast, or video, chasing down myriad random facts he’ll never need



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Tina Williams-Koroma

CISSP, PMP, Esq.

Serial entrepreneur within the cybersecurity industry, with consulting and product experience

Over 20 years of technology experience ranging from software development to computer forensics, security engineering, risk assessments, and management

Seasoned leader and speaker, addressing the challenges and opportunities related to cybersecurity and privacy matters

Hands-on board of directors experience with various public and private institutions



aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Balancing the risk of disruption

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is risk?

LIKELIHOOD X IMPACT = RISK

Likelihood	Risk level				
Very likely	Low	Medium	High	Critical	Critical
Likely	Low	Medium	Medium	High	Critical
Possible	Low	Low	Medium	Medium	High
Unlikely	Low	Low	Low	Medium	High
Very unlikely	Low	Low	Low	Medium	High
Impact	Minimal	Low	Medium	High	Severe

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

> A deviation from or interruption of normal activities or operations that results in a loss of data, system availability, system reliability, or control of systems, or indicates unauthorized access to, or malicious software present on, critical information technology systems.[1]

Operational disruption, defined

1. NIST, CIO.com
2. https://www.lawinsider.com/dictionary/operational-disruption

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Balancing the risk of disruption

DUE TO A SECURITY EVENT

Cyber incident/cyber breach, defined:

"An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or that constitutes a violation or imminent threat of violating security policies, security procedures, or acceptable use policies."[1]

Common patterns found in security events[2]

- Social engineering
- Basic web application unauthorized access
- System intrusion
- Miscellaneous errors
- Privilege misuse
- Lost and stolen assets
- Denial of service
- Other (everything else)

1. Glossary | NIST (https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary)
2. Verizon 2021 DBIR

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Balancing the risk of disruption

DUE TO A SECURITY EVENT

The cost of disruption – The top 6 most expensive events[1]

6 – Sony PlayStation (2011): $171 million

5 – Hannaford Bros (2007): $252 million

4 – Veterans Administration (2006): $500 million

3 – Mafiaboy Attack (2000): $1 billion

2 – Epsilon (2011): $4 billion

1 – ExPetr/NotPetya (2017): $10 billion

1. https://tcecure.com/2021/10/06/the-top-6-most-expensive-cyber-attacks-in-history/

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Balancing the risk of disruption

DUE TO TIMELY (BUT UNTESTED) PATCHING AND CONFIGURATIONS

Security testing

- Vulnerability scans, depending upon the timing and tool settings, can adversely impact system and account access
- Penetration tests, depending upon the rules of engagement, and timing, can adversely affect system performance

Security configuration updates

- Army Gold Disk example
- Hardening systems according to security benchmarks like DISA STIGs or CIS

Patching

- Vendors release updates to their technologies to address security issues
- These updates are intended to plug holes, known vulnerabilities

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Common security, patch, and configuration testing approaches

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Common approaches

PROS AND CONS

Vulnerability and configuration scanning

- During work hours – A benefit to those doing the testing, but higher likelihood of adverse impact on operations
- During after hours – Time to recover from any adverse impact, but is taxing on an already stretched pool of workers

Functional testing

- Spray and pray – No testing, least resource intensive upfront, but high likelihood of adverse functional impact
- Limited deployment to production – Provides some advance insight into any issues, but difficult to stay on schedule and re-create issues should they be reported by a user
- Test environment with manual testing – Provides additional insight into any issues, but is very resource intensive

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Recommendations

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Recommendations

- Identify – The vulnerabilities and security compliance and best practice configuration gaps
- Test – The functional impact of fixing the vulnerabilities and gaps in a nonproduction environment
- Deploy – The security updates to the production environment

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resources

- National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence (NCCoE) – Practice Guide, “Improving Enterprise Patching for General IT Systems: Utilizing Existing Tools and Performing Processes in Better Ways”
  csrc.nist.gov/publications/detail/sp/1800-31/final
- Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) – Free cybersecurity tools
  cisa.gov/free-cybersecurity-services-and-tools
- Center for Internet Security (CIS) – Security benchmarks for numerous technologies
  cisecurity.org/cis-benchmarks
- CyDeploy – Remote, cloud-based SaaS environment for security and functional testing
  cydeploy.com

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Tina Williams-Koroma

tina.williams@cydeploy.com

cydeploy.com

linkedin.com/in/tcwk

Ritik Khatwani

ritikkh@amazon.com

@ritikkhatwani

linkedin.com/in/ritikkhatwani

CyDEPLOY



Please complete the session survey in the **mobile app**

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.