# Information Security

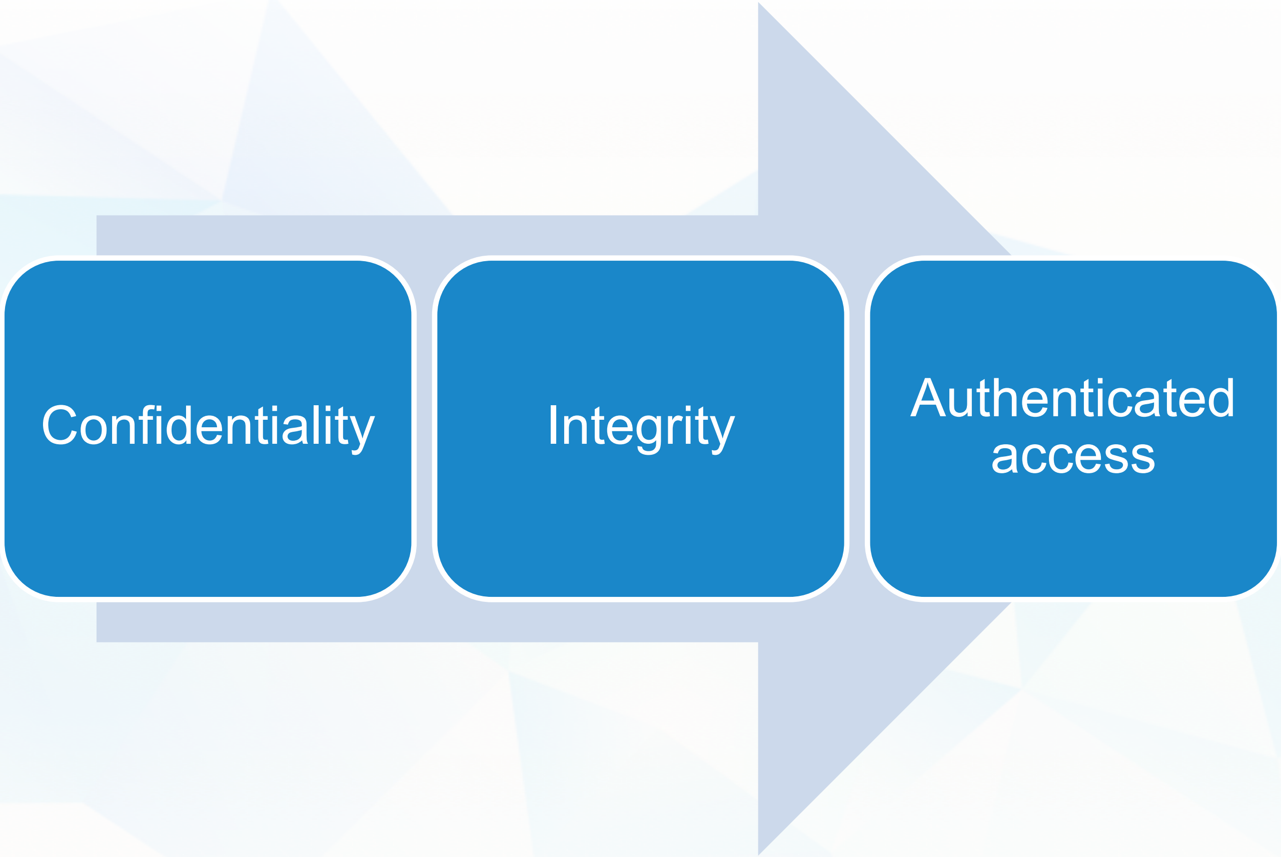
## At ICANN Org

Ashwin Rangan

Montreal 2019

ICANN

# A 3-step, holistic approach to InfoSec vulnerabilities



Confidentiality

Integrity

Authenticated access

**Drilling-in: Bad-actors have to be right just ONCE**
**We have to be right every day, all the time**

# Acute awareness of likely entry-points for bad-actors

- Hardware
  - Storage
  - Processing
  - Networking infrastructure

- Software
  - CLOUD
  - Operating Systems
  - Database management systems
  - Applications
  - Development and CI/CD environments

- 3$^{rd}$ parties – with whom ICANN Org has business relationships

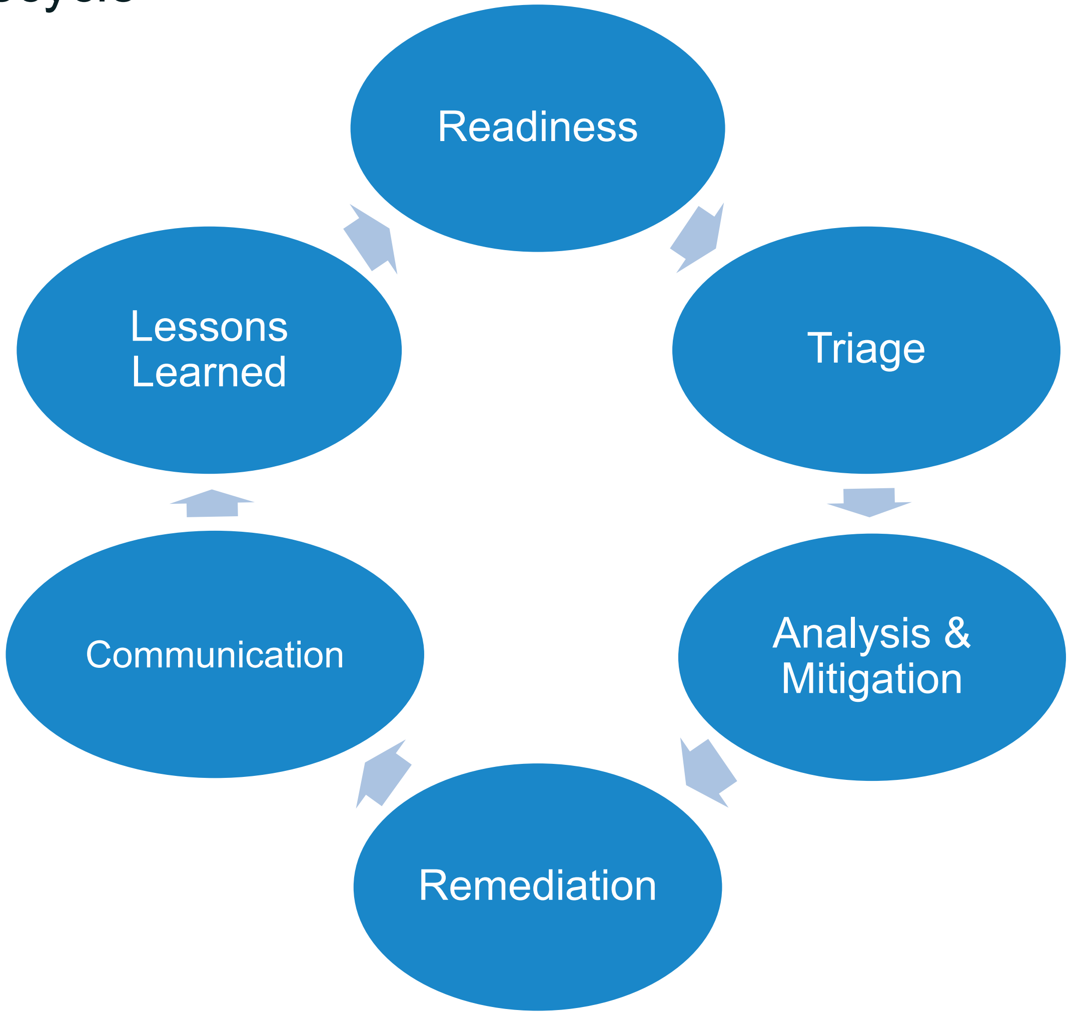
**On a path to address these holistically**

# ICANN Org InfoSec is on a good trend-line…

## Delivered in the last 6 months

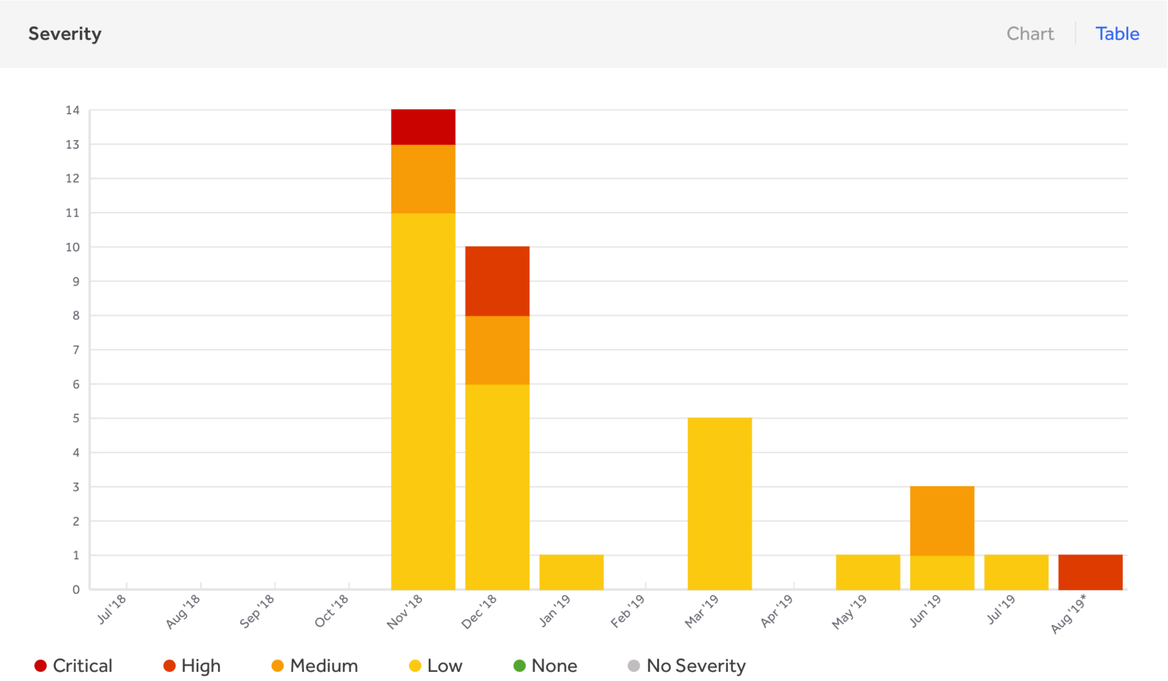
# ICANN InfoSec – Already Delivered

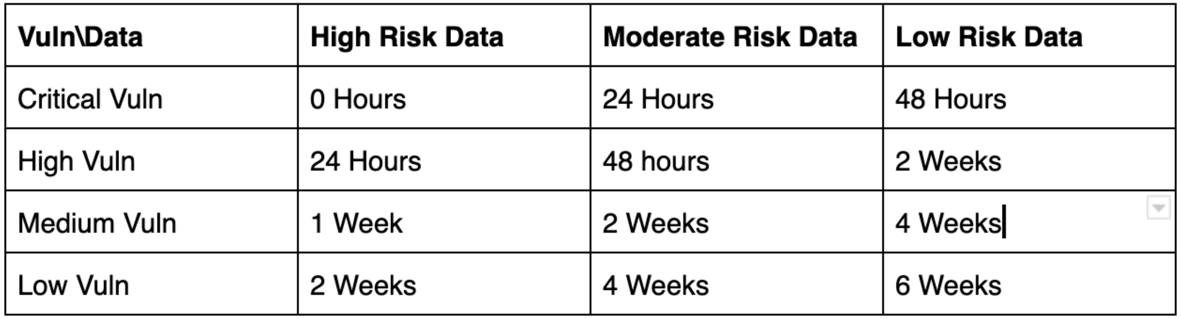
- Internal commitment to Computer Security Incident Response Team (CSIRT) Lifecycle



# ICANN InfoSec – Already Delivered

- HackerOne Program & Established Internal SLAs for Vulnerabilities





| Vuln\Data | High Risk Data | Moderate Risk Data | Low Risk Data |
|---|---|---|---|
| Critical Vuln | 0 Hours | 24 Hours | 48 Hours |
| High Vuln | 24 Hours | 48 hours | 2 Weeks |
| Medium Vuln | 1 Week | 2 Weeks | 4 Weeks |
| Low Vuln | 2 Weeks | 4 Weeks | 6 Weeks |

# ICANN InfoSec – Already Delivered

- Red Team exercise of ICANN meetings network in Kobe
  - 13 InfoSec recommendations presented to right actors for remediation
  - 11 recommendations adopted and either implemented or on improvement roadmap
  - 2 yet to be planned
    - Meeting with other Network Admins who run similar conference networks
    - On-site Intrusion Detection System (IDS) and Packet capture

# ICANN InfoSec – Already Delivered

- InfoSec Ambassador Program
  - Representatives from all significant Functions in ICANN
  - Much better Org engagement with InfoSec – culture shift
  - Regular positive and topical email discussions. Such as:

| | |
|---|---|
| Password Managers | ICANN Cloud Security |
| Phone Numbers as Identity | Five Recent industry InfoSec Compromises |
| Travel Security | Navex Training (mandatory staff InfoSec awareness training) |
| Have I Been Pwned | Passphrases |
| Digital Signatures (email) | … |

# ICANN InfoSec – Already Delivered

- Created ICANN Org's first-ever Configuration Management Database (CMDB)
- Secure coding training for developers
  - Checkmarx Codebashing
    - All programming languages used at ICANN
    - Security basics
    - HTTP Security Principles
    - OWASP top 10 for each language
  - 35 Team members enrolled
    - 33 from the development team
    - 2 from InfoSec

# The Next Two FY Quarters

# ICANN InfoSec – FY20Q1 & FY20Q2

- Automated vulnerability auditing of all ICANN owned assets
  - Using Nexpose
  - Reports to be sent directly to Service Owners and Executive Relationship Managers for action

- Automated Common Vulnerabilities and Exposures (CVE) assignment to service owners
  - VulDB
  - Based on our catalogue of services and Common Platform Enumeration (CPE) from the ICANN CMDB

# ICANN InfoSec – FY20Q1 & FY20Q2

- By country - matrix of InfoSec risk for ICANN Staff
  - Matched to InfoSec recommended controls for travelling staff

- Scoping and Profile Definition of NIST Cybersecurity Framework (CSF)
  - Focus of ICANN on secure processes
  - Maturing InfoSec in ICANN as an organization (compared to CIS20 style controls)

# ICANN InfoSec – FY20Q1 & FY20Q2

- Centralized log collection, indexing, alerting, and dashboarding
  - Splunk!!

- Expansion of traffic capture infrastructure
  - TAPs into all ICANN network segments
  - Sufficient storage
  - More processing power to more quickly search for event related information

# Forward Thinking

# ICANN InfoSec – Future Work

- Review of HackerOne
  - Consider financial rewards for discovered vulnerabilities
  - Consider back-of-office ability to meet SLAs
- Red Team exercise on all ICANN networks
  - Internal from within, potentially external 3rd party
  - Consider turning into an ongoing program
    - Checks and balances / costs / tradeoffs
- Browser Isolation Evaluation
  - In-hand with browser selection and trust anchor store & browser extension audits
- End User Device Security review
  - Are we doing the best we can?
  - Are there better/easier tech options for 2FA available?

# ICANN InfoSec – Future Work

- More NIST CSF! - assess, analyze gaps, action gaps, reassess, …
- InfoSec Strategy day (internal) with the InfoSec Ambassadors
  - Solid engagement with ICANN departments
  - Glibly; "bring out your dead!" ☺
    - What are those processes that are security naïve?
- SSR-RT2 Findings and Recommendations
  - I'm sure there will be a number of items!
  - Watch this space
- ICANN posture on third-party hosted platforms
  - Review what influence we have
  - What more would we like
  - Access to logs is "interesting"

# Thank You and Questions

Visit us at **icann.org**
Email: email

@icann

linkedin/company/icann

facebook.com/icannorg

slideshare/icannpresentations

youtube.com/icannnews

soundcloud/icann

flickr.com/icann

instagram.com/icannorg