Why health check your Vulnerability Management Program?

WHY DO WE NEED TO RUN A CYBER SECURITY HEALTH CHECK?

- Your organization will face a cybersecurity threat this year. It's an unfortunate reality in this day and age.
- Data is valuable no matter the size of your business and, more and more, cyber-criminals will attack a smaller business to try and get access to their supplier and customer data.
- It can be scary to know that some experienced cyber-criminals actually have the ability to target thousands of smaller and larger businesses at once with the right code or ransomware.

SO, HOW DO WE COUNTER THESE THREATS AND ENSURE CYBER ATTACK PROTECTION FOR W-OF-G BUSINESS?

- A properly governed cyber security health check goes beyond keeping your antivirus software up to date and avoiding dodgy links.
- By evaluating every area of your business with a cyber security health check - a process that involves more than basic internet security hygiene - a health check on your areas and applications can improve your organisations defences and put you in good stead with ever evolving regulations.
- It covers all layers of your essential business operations to put you in a better, more secure position.
- The CSU Unit is here to partner with you, and to help your entity to drive your security maturity. We are here to assist where we can, and security health checks can be a really useful way to stop, check and gauge where you may need to course correct.

WHAT DO YOU LOOK AT, HOW DO YOU DO IT?

- We focus on existential security risks first and review and analyse areas and apps to understand whether your security controls are consistent, adequate, reasonable and effective.
- We help to identify security initiatives vs business outcomes and relay that information in a way that you can utilise the information to drive the business need discussions and help you to underpin the story, that "Cyber is not just about ICT!'.
- We help to determine actionable results which can be used to lead to an improved security posture.

WHAT DO WE GET OUT OF IT?

- A good understanding of what your 'crown jewels' are, (and what state they are in!) – a Health Check helps you identify current security strengths and weaknesses and ensure that you are protecting your most important business assets.
- An understanding of your maturity level in accordance with Essential 8 requirements (including patch management) - You can read more about the Essential 8 recommended by the Australian Government if you're keen to know more.
- A suggested roadmap to mature your vulnerability management program in the future.
- Understanding where you need to prioritise your cyber hygiene – especially addressing critical vulnerabilities.

RIOT VULNERABILITY MANAGEMENT HEALTH CHECK – PLAN ON A PAGE

PRE-MOBILISATION → REVIEW → ANALYSIS → COMPLETE FINDINGS → RECOMMENDATIONS

ACTIVITIES

1 – 2 WEEKS PRIOR TO START

Pre-work

- **Data** Gathering
- **Plan** for workshops/interviews/meetings
- **Co-ordinate** access to key resources on Customer side, and plan for interviews and workshops

You need to:

- **Assign** a Sponsor (i.e. CIO or ED level)
- **Assign** a contact to work with RIOT
- **Allocate** resources to assist information flow
- **Attend** key governance meetings
- Openly discuss issues and needs

- **Allow** RIOT access to the entity console and environment
- Confirm dates of access to entity console and environment

- **Please** note that the program is contractually covered by a data privacy NDA, however if you require further confirmation from the RIOT Team these will need to be actioned at entity level.

Stage 1

- **Identify** prioritised applications/areas where RIOT is able to:
  - Identify Governance Maturity
  - Identify Asset Management Maturity
  - Identify Automated Scanning Maturity
  - Identify Manual Scanning Maturity
  - Identify External Scanning Maturity
- **Identify** asset fleet (i.e. 'Crown Jewels')
- **Undertake** meetings and workshops with relevant app owners, IT Team and Business Stakeholders

Stage 2

- **Analyse** prioritised applications/areas where RIOT is able to:
  - Analyse Vulnerability Prioritisation Maturity
  - Analyse Vulnerability Analysis Maturity
- **Communicate** prioritised applications/areas where RIOT is able to:
  - Analyse metrics and reporting maturity
  - Analyse vulnerability alerting maturity
- **Remediate** prioritised applications/areas where RIOT is able to:
  - Analyse change management maturity
  - Patch management maturity

Stage 3

- **Gather** final information
- Confirm application/area-specific risk areas and workloads
- **Identify** areas and applications which need further assessment
- **Review** current plans to identify gaps, risks/issues
- **Identify** opportunities to optimise and improve existing plans
- **Prepare** for summary of diagnoses findings
- Jointly discuss recommendations
- **Status** update to business and IT stakeholders

Stage 4+ **

- **Executive** presentation on findings and recommendations
- **Jointly** workshop the models that are informed by analysis
- Provide path way towards E8 patch and change management maturity uplift
- **You decide a path forward!**

Resources & Effort Required:

- Access to interview key staff supporting the initiative, including key future state decision makers, e.g. Architects and Technology Planners etc
- Access to key staff providing the services around Service Management/DevOps etc and permission to interview key staff
- Details regarding current infrastructure and future state and access to interview key resources involved in the current RIOT arrangements
- Participation in workshops and interviews during the engagement (low to medium effort)

** NB: We outline a health check will last for 3 days, however the complexity of your entity may require an adjustment to the time required.
- The RIOT Team will discuss this with you -