CHARITY
IT LEADERS

# Diversity Cyber Security: The Actionable Manifesto

Many thanks to everyone who took part in last year's hackathon on Diversity in Cyber Security. During the event it was clear that sector may have some bigger issues than diversity in Cyber Security and there was evidence of a lack of connection between technology leadership and the cyber security world. In a subsequent conversation with the leaders of Charity Security Forum, they reported that many of the Security Managers refer to themselves as isolated or disconnected from the CIO / Leader.

## Top Three things technology leaders should be doing….

1. Engaging with others in the organisation who may have a role to play e.g. HR and others.
2. Cost and value of cyber security underestimated and therefore securing funding very difficult. Work with finance professionals to investigate this issue, together.
3. Soft skills of cyber security professionals are more important than we currently give credence to. Hardware / Infrastructure is not always a good starting point for future security professionals. Consider your job descriptions and profiles, are you looking for the right skills?

## What the event discovered …

1. There is a lack of a clear career profession path for security specialists in the sector and we are concerned that security professionals tend to be infrastructure professionals.
2. There was concern that organisations may believe having a cyber security specialist in place is the end of the worry.
3. Diversity is not just about gender
4. Diversity gap is in technology not just cyber security
5. The image of cyber security is a problem too (too nerdy and infrastructure centric, see above).
6. Cyber Security professionals and technologists are not always looking beyond their own teams for the support and engagement and can be isolated.
7. Most members are struggling to secure the funding for even the basics in security – awareness is still too low and the costs / value consistently underestimated.
8. We are tending to see the responsibility as falling on the shoulders of a few within the Technology or Security field and not engaging with others in the organisation who could and should be getting involved and taking an active part (this will help with diversity).
9. We need good ways of measuring investment and threat e.g. Key Risk Indicators (KRIs).

# Charity IT Leaders Cyber Security Manifesto

The final outcome of the event was to pull together possible actions that we can all take either individually or with Charity IT Leaders. The following are the suggested actions that may just start to nudge the peanut forward.

## Actions for Individuals

- Attend CITL meeting on
  - Writing for inclusivity (job adverts)
  - Are we funding this the right way
- Audit your environment – how male dominated / white / middle class is it – knowledge is power
- Get the CIO/Dir of IT talking to the leader in HR about joint responsibility for the people side of security. Arrange a meeting and have a conversation.
- Talk to your local schools about a career in STEM
- Understand the benefits your charity offers to employees and make more of them (not just the money) in your recruitment
- Always run your advertisements through a diversity decoder - [http://gender-decoder.katmatfield.com/](http://gender-decoder.katmatfield.com/)

## Actions / Support from Charity IT Leaders

Getting the following onto the Agenda for Quarterly Meetings or other events: -

- Re-engage with Charity Security Forum and other NFP groups (e.g. Universities)
- Advert writing to attract different groups
- How to measuring inclusivity
- Build a library of job descriptions people can share
- Pull together ideas for the discussion with HR on security responsibility
- Getting the funding ask right for this – storytelling and measuring
- Discussing the role of Cyber Security – bring in the three lines of defence model.

**Three lines of defence**

| Lines | Role of CIO | Role of all Business Units | Role of the Security Leader |
|---|---|---|---|
| First Line *"The Operation"* | Risk Management of the Operation<br>Apply Internal Controls<br>Monitoring and reporting<br>Incident Management<br>Business Case for Investment in Security Technology | Risk Management of their part of the Operation including technology supporting their function<br>Apply Internal Controls<br>Monitoring and reporting<br>Incident Management | Review threat external landscape and vectors<br>Support incident management with expert investigation |
| Second Line *"Risk & Compliance"* | Provide organisational context to Security Leader<br>Support the recommendations of Security Leader<br>Sponsor the Security Leader<br>Advocate and guide other C-Level execs on their role and the standards they maintain | Feedback and contribute to policy setting<br>Set risk appetite<br>Take part in and sponsor awareness and education initiatives | Oversee and Challenge cyber security response and risk management<br>Provide guidance and direction<br>Develop policy and frameworks (based on context)<br>Awareness campaigns and education |
| Third Line *"Audit"* | Provide clear, actionable management response to audit reports<br>Guide other business units on the importance and value of audit reports | Provide clear, actionable management response to audit reports | Review 1st and 2nd Lines for compliance with policy<br>Provide an independent perspective<br>Challenge<br>Objective and offer assurance to executive leadership |

- Agree core messages for government and other charity groups to drive a consistent message.
- Asking to include diversity in reports on Cyber Security arising from government
- Writing articles in CIO, Civil Society and Computer Weekly on this issue.
- Bringing CIO's from Corporate World Together to share ideas and gain a consistent view.