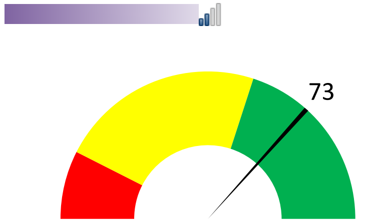
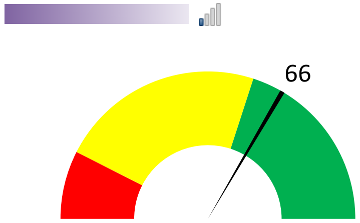
10 Steps to Cyber Security: Dashboard

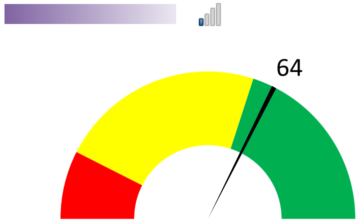
1. Information Risk Management



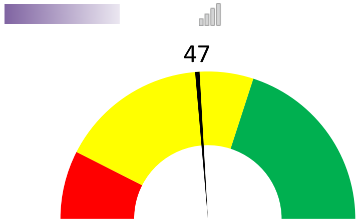
2. Network Security



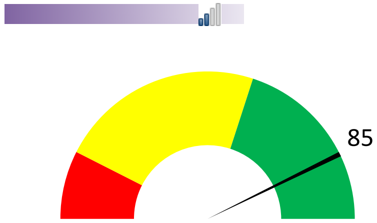
3. Malware Prevention



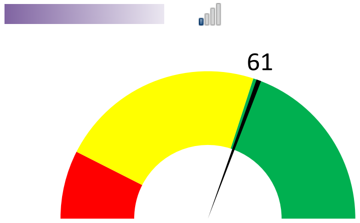
4. Monitoring



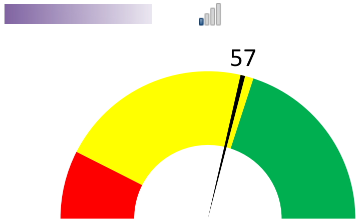
5. Incident Management



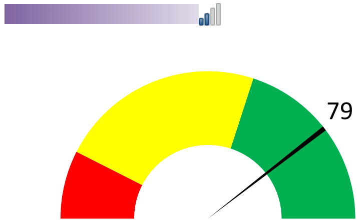
6. Managing User Privileges



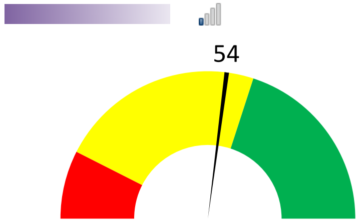
7. Removable Media Controls



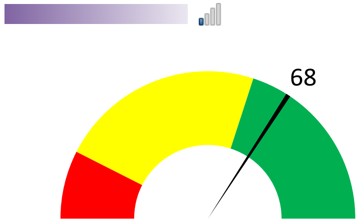
8. Secure Configuration



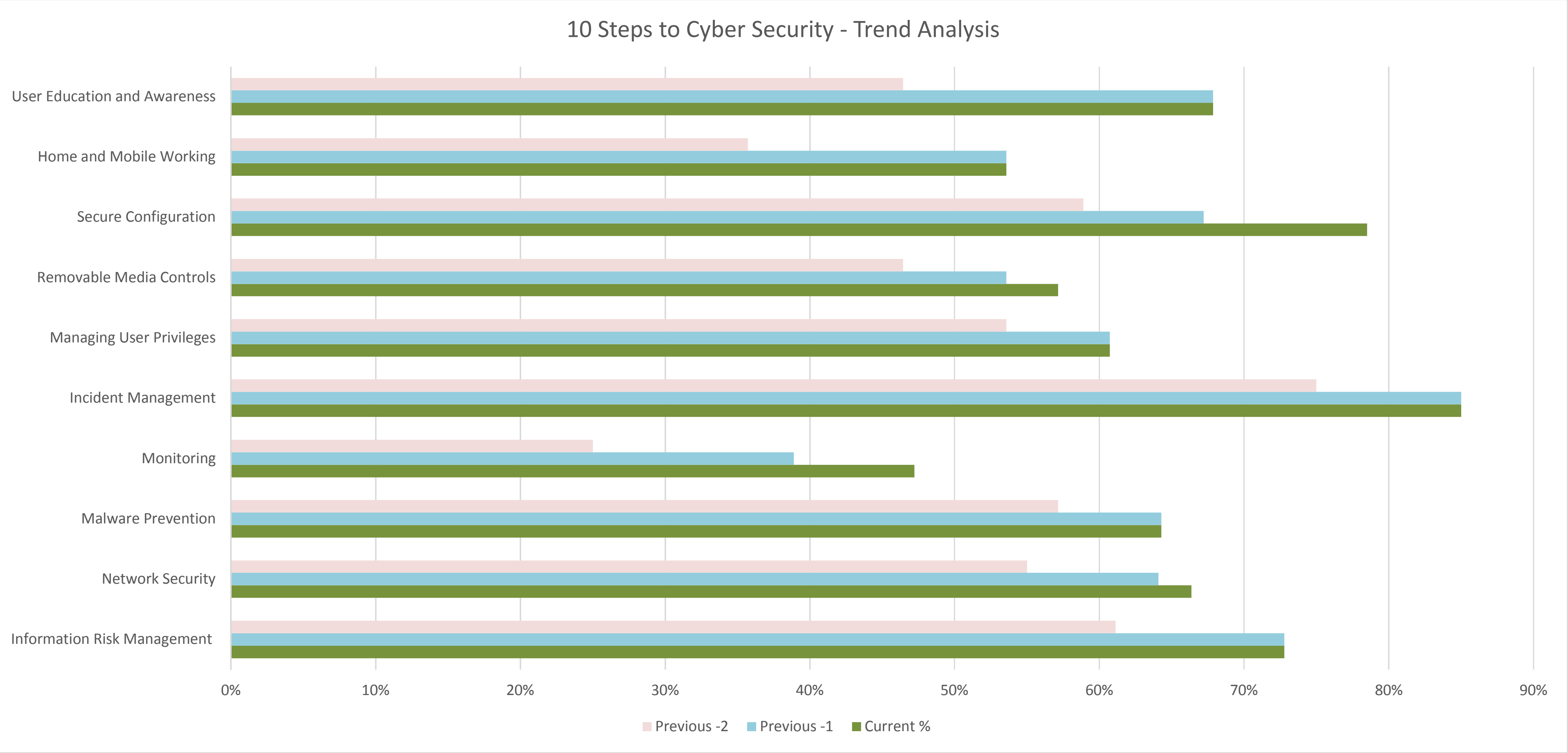
9. Home and Mobile Working



10. User Education and Awareness



City of London Corporation - Report of: Gary Brailsford-Hart, Director of Information & CISO - Assessment Date: 04 May 2018


10 Steps to Cyber Security - Trend Analysis
User Education and Awareness
Home and Mobile Working
Secure Configuration
Removable Media Controls
Managing User Privileges
Incident Management
Monitoring
Malware Prevention
Network Security
Information Risk Management
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
Previous -2
Previous -1
Current %

	% Complete	Target Score	Actual Score
Information Risk Management	**73%**	**4**	**3**
Establish a governance framework	100%	4	4
Determine the organisation's risk appetite	25%	4	2
Maintain the Board's engagement with information risk	100%	4	4
Produce supporting policies	100%	4	4
Adopt a lifecycle approach to information risk management	100%	4	4
Apply recognised standards	75%	4	3
Make use of endorsed assurance schemes	75%	4	3
Educate users and maintain their awareness	50%	4	2
Promote a risk management culture	30%	4	2

	% Complete	Target Score	Actual Score
Network Security	**66%**	**4**	**3**
Police the network perimeter	75%	4	3
Install firewalls	100%	4	4
Prevent malicious content	75%	4	3
Protect the internal network	80%	4	3
Segregate network as sets	25%	4	1
Secure wireless devices	100%	4	4
Protect internal IP addresses	25%	4	1
Enable secure administration	25%	4	2
Configure the exception handling process	100%	4	4
Monitor the network	25%	4	1
Assurance process	100%	4	4

	% Complete	Target Score	Actual Score
Malware Prevention	**64%**	**4**	**3**
Develop and implement anti-malware policies	50%	4	2
Manage all data import and export	75%	4	3
Blacklist malicious web sites	100%	4	4
Provide detailed media scanning machines	25%	4	1
Establish malware defences	75%	4	3
End user device protection	50%	4	2
User education and awareness	75%	4	3

Monitoring	**47%**	**4**	**2**
Establish a monitoring strategy and supporting policies	25%	4	1
Monitor all ICT systems	50%	4	2
Monitor network traffic	50%	4	2
Monitor all user activity	50%	4	2
Fine-tune monitoring systems	50%	4	2
Establish a centralised collection and analysis capability	50%	4	2
Provide resilient and synchronised timing	100%	4	4
Align the incident management policies	25%	4	1
Conduct a lessons learned review	25%	4	1

Incident Management	**85%**	**4**	**3**
Obtain senior management approval	100%	4	4
Provide specialist training	100%	4	4
Define the required roles and responsibilities	75%	4	3
Establish a data recovery capability	100%	4	4
Test the incident management plan	100%	4	4
Decide what information will be shared and with whom	25%	4	1
Collect and analyse post-incident evidence	75%	4	3
Conduct a lessons learned review	100%	4	4
Educate users and maintain their awareness	75%	4	3
Report criminal incidents to law enforcement	100%	4	4

Managing User Privileges	**61%**	**4**	**2**
Establish effective account management processes	100%	4	4
Establish policy and standards for user identification and access control	75%	4	3
Limit user privileges	75%	4	3
Limit the number and use of privileged accounts	50%	4	2
Monitor	50%	4	2
Limit access to the audit system and the system activity logs	25%	4	1
Educate users and maintain their awareness	50%	4	2

Removable Media Controls	**57%**	**4**	**2**
Produce corporate policies	50%	4	2
Limit the use of removable media	50%	4	2
Scan all media for malware	75%	4	3
Formally issue media to users	75%	4	3
Encrypt the information held on media	25%	4	1
Actively manage the reuse and disposal of removable media	50%	4	2
Educate users and maintain their awareness	75%	4	3

Secure Configuration	**79%**	**4**	**3**
Use supported software	80%	4	3
Develop and implement corporate policies to update and patch systems	100%	4	4
Create and maintain hardware and software inventories	80%	4	3
Manage your operating systems and software	75%	4	3
Conduct regular vulnerability scans	75%	4	3
Establish configuration control and management	75%	4	3
Disable unnecessary peripheral devices and removable media access	75%	4	3
Implement white-listing and execution control	100%	4	4
Limit user ability to change configuration	100%	4	4
Limit privileged user function	25%	4	1

Home and Mobile Working	**54%**	**4**	**3**
Asses the risks and create a mobile working security policy	50%	4	2
Educate users and maintain their awareness	50%	4	2
Apply the security baseline	75%	4	3
Protect data at rest	75%	4	3
Protect data in transit	75%	4	3
Review the corporate incident management plans	50%	4	2

User Education and Awareness	**68%**	**4**	**3**
Produce a user security policy	75%	4	3
Establish a staff induction process	50%	4	2
Maintain user awareness of the cyber risks faced by the organisation	75%	4	3
Support the formal assessment of Information Assurance (IA) skills	75%	4	3
Monitor the effectiveness of security training	50%	4	2
Promote an incident reporting culture	50%	4	2
Establish a formal disciplinary process	100%	4	4

Current status of 10 Step control areas across organisation.

ASSESSMENT DATE: 04 May 2018

Control Area	% Complete	Target Score	Actual Score
Information Risk Management	73%	4	3
Network Security	66%	4	3
Malware Prevention	64%	4	3
Monitoring	47%	4	2
Incident Management	85%	4	3
Managing User Privileges	61%	4	2
Removable Media Controls	57%	4	2
Secure Configuration	79%	4	3
Home and Mobile Working	54%	4	3
User Education and Awareness	68%	4	3

City of London Corporation - Report of: Gary Brailsford-Hart, Director of Information & CISO - Assessment Date: 04 May 2018