

ults

An IT Initiative of ULCCS LTD.

SECURING THE FUTURE OF COOPERATIVES

ULTS Cybersecurity
Center of Excellence

CONTENTS

<i>1. Preface</i>	<i>3</i>
<i>2. Co-Creating a better world</i>	<i>4</i>
<i>3. Information security management</i>	<i>5</i>
<i>4. Security Flaws</i>	<i>6</i>
<i>5. Our recommendations for securing cooperatives</i>	<i>7</i>
<i>6. Our offerings</i>	<i>8</i>
<i>7. Managed Services platform for Cooperatives.</i>	<i>10</i>
<i>8. Why ULCCS?</i>	<i>12</i>

PREFACE

For over 160 years, cooperative societies in India have been an effective way for people to exercise control over their economic livelihood and to provide a unique tool for achieving one or more economic goals. The performance of cooperative movement in India is remarkable and has contributed largely to the socio-economic development of the country. The digital transformation has revolutionised the cooperative sector and helps it to remain competitive and simplify the services offered to the society. The fast paced transition from the legacy systems to IT based technologies, smart devices and the multi-cloud environment has increased the risk manifold. This reinforces the importance of cybersecurity for the cooperative societies today. The transactions over the Internet are becoming high risk as the malicious actors are becoming smarter with advanced technologies and hacking tools available on the dark web.

It is in the above context we wish to draw your attention to the relevance of the Uralungal Labour Contract Cooperative Society (ULCCS). To meet the challenges in the fast and continuously changing digital environment, ULCCS has developed capability in the information technology and information security domains. Thus being the first to setup a state-of-the-art Special Economic Zone (SEZ) Cyber Park with 2000+ working IT professionals at Kozhikode, Kerala. The UL Cyber Park is also the first green IT Park with a LEED rated IGBC GOLD certified campus in the cooperative sector.

ULTS the IT initiative of ULCCS has a proven track record in the field of Information Technology, Emerging Technologies (Block Chain, IoT, AI), GIS based solutions and securing the Cyber space with cybersecurity, and wishes to offer our expertise and facilities for the benefit of the entire cooperative institutions.

In the recent times, Covid-19 pandemic has devastated the cooperative institutions. The cooperative societies now are forced to respond in all the possible ways so as to provide relief its members, workers and the society they serve. Hence, It is time to integrate cooperatives, and digitally empower them to meet the challenges faced in the new normal. The current crisis does not seem to have a definite end and has impacted all spheres of life. These effects are directly going to determine how business will be done in future. The rapid increase in involvement of technology and lesser use of human resources in various business decisions. Thus it is imperative for the cooperatives to identify the gaps in their digitisation process while getting adjusted to the new normal to remain productive and sustainable.

CO-CREATING A BETTER WORLD

Cybersecurity should be the top priority for cooperative institutions today. Cooperative institutions, have got to deal with newer security challenges. The transactions over the internet are becoming riskier as the malicious actors are becoming smarter with advanced technologies and availability of the automated hacking tools in the dark web. The vulnerabilities could mean that the cooperative institutions have to fight it out on a daily basis to protect their critical assets.

Interestingly, not all security breaches are caused by break down in technology. Many security breaches are caused because of the absence of security postures in the network or by the breakdown in the overall security posture of the organisation. This being so, any dynamically changing network infrastructure can be properly managed only by forming intelligent information security policy and posture.

All these mean that all digital transformation initiatives have to be necessarily complemented by comprehensive cyber (or digital) security programs. Cybersecurity refers to policies, technologies, techniques, procedures and methods used to protect digital data and information from being stolen or compromised.

Cybersecurity landscape looming cooperative sector:

Data is the most critical asset. From lost business, reputation, regulatory fines, remediation costs, A data breaches have far-reaching consequences to the business. According to an IBM sponsored report, between July 2018 - April 2019, in India an average of 35,636 records were compromised.

The breakup of the breach are as follows;

- 51% from malicious or criminal attacks,
- 27% from system glitches and
- 22% due to human error.

Inherently Insecure Services

Even the most vigilant organisation that does their job well and keep up with their daily responsibilities, can fall victim to vulnerabilities if the services they choose for their network are inherently insecure. There are certain services that were developed under the assumption that they will be used over trusted networks; however, this assumption falls short as soon as the service becomes available over the Internet.

Some examples of inherently insecure services include under or over designed network architecture, insecure third party applications, pirated softwares, poor access management and authentication process, unmonitored remote access by third party through untrusted applications. The services noted above can more easily fall prey to what the security industry terms as a cyber attack.

In order to support the cooperative societies in India, NCUI (National Cooperative Union of India) the national apex body of Indian cooperative societies, has signed a MOU with ULCCS to help prevent the cooperative sector from cyber attacks and aid digitisation through specialised training programs and professional services.

ULCCS, known for its experience in integrating IT and security services with complex, large-scale IT programs is recognized by NCDC (National Cooperative Development Corporation) as well by inducting it as a member to the NCDC led Cooperative Institutions Cybersecurity Advisory Forum (CICAF).

INFORMATION SECURITY MANAGEMENT

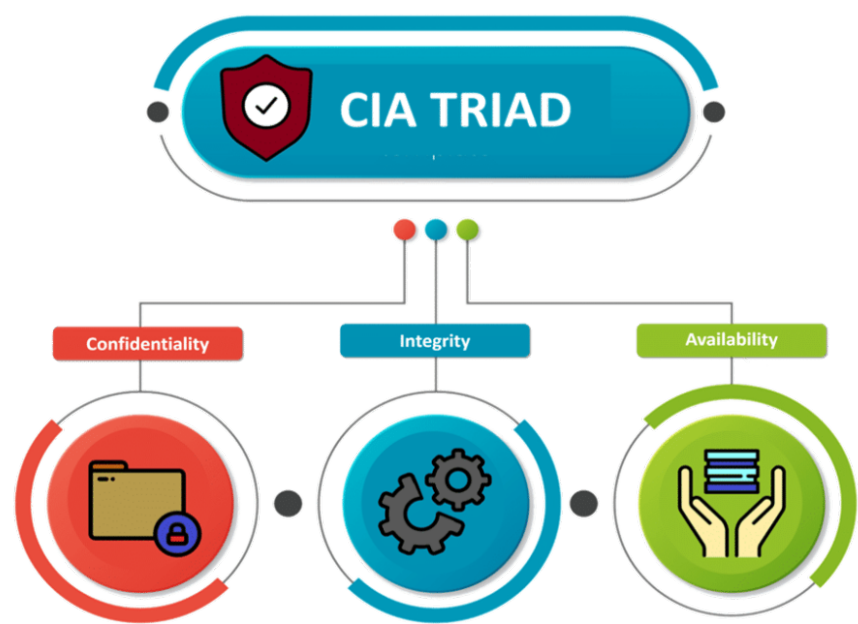
In today's highly digitised world there is data getting generated and captured at every instance. Data is the most valuable asset. Data is simply facts or figures, once processed reveals a lot of information and insights. Hence this has to be protected right from its source, process, transfer and storage. Unregulated data-mining or hacking causes a whole different set of problems – privacy issues. Hence there should be a strong security foundation in place to protect.

There are broadly three types of information assets in any cooperative society:

- 1) Information in the physical form,
- 2) Information in the digital form and
- 3) Information in the biological form.

Information security effectively addresses the ever-growing challenges providing adequate protection for these information assets. Information security deals with the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorised access, use, misuse, disclosure, destruction, modification, or disruption.

The basic components of information security are the CIA triad: confidentiality, integrity, and availability.



Information Security Management System describes and demonstrates the organisation's approach to secure its critical assets. This includes assessment on people, policies, controls and systems to identify the gaps, then address the opportunities and threats revolving around valuable information and related assets.

On the other side, Cybersecurity is about all the processes and practices we implement to protect networks, computers, applications and data from attacks on the confidentiality, integrity and availability.

Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

Cybersecurity Practice	
InfoSec Policy	Incident Response
Network Hardening	Security Operations Centre
Network Security	Cloud Security
Vulnerability Assessment	Awareness training



SECURITY FLAWS

Risk = Threat x Vulnerabilities

Cybersecurity risk is the probability of exposure or loss resulting from a cyber attack or data breach on the organisation. Risk is where threat and vulnerability overlap.

Vulnerability is a weakness which can be exploited by a threat actor to perform unauthorised actions within an IT infrastructure. The vulnerability gets exploited by malicious actor to damage data, steal data, or disrupt digital life in general. Threat include organised crime like implanting spyware, malware, adware, and using the disgruntled internal employees to leak information or gain backdoor access to the organisation’s digital infrastructure.

Some of the commonly found issues in the cooperative eco system are:

1. Vulnerability related to Network Infrastructure:

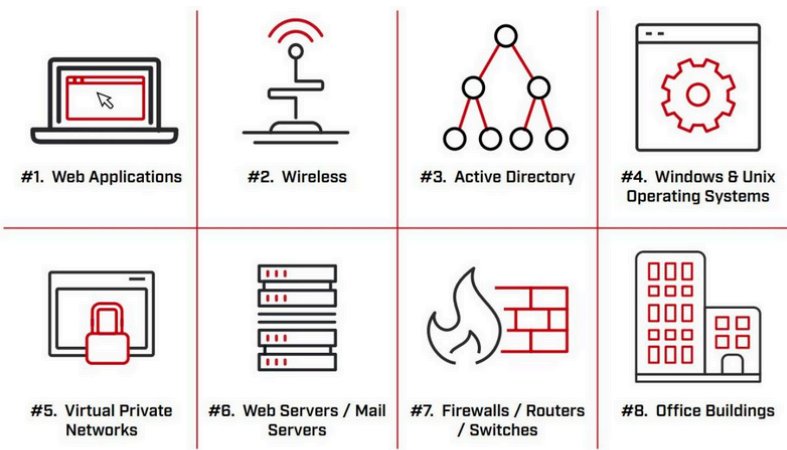


Fig:Risk and vulnerabilities related to Hardware and network

Routers, switches and firewalls, collectively known as network infrastructure devices, are the most important elements of any network. In terms of security, they should be the most hardened devices, however, administrators are seen ignoring to keep them updated to ensure they do not inadvertently turn a threat which could be exploited by an attacker. Under designed and expansion of networks using unsecured devices are primarily a reason of concern.

2. Unused Services and Open Ports:

A common occurrence among system administrators is to install an operating system without knowing what is actually being installed. This can be troublesome, as most operating systems will not only install the applications, but also setup a base configuration and turn services on. This can cause unwanted services, such as telnet, DHCP, or DNS to be running on a server or workstation without the administrator realising it, leading to unwanted traffic to the server or even a path into the system for crackers.

3. Unpatched Services:

There is no such thing as perfect software, and there is always room for further refinement. Many of the server applications have been in use in production environments for many years, and their code has been thoroughly refined and many of the bugs have been found and fixed. It is up to system administrators to patch and fix these bugs and unpatched systems wherever an update is released.

4. Inattentive Administration:

Administrators often fail to patch their systems or are too ignorant to do so. It is observed that administrators fail to patch their servers and workstations or fail to watch log messages from their system kernel or from network traffic. The primary cause of computer security vulnerability is assigning untrained people to maintain security.

5. Lack of Information security Policy:

In many cases we observe that there isn’t a information security policy in place. Cybersecurity culture at the workplace amounts to the promotion of safe cybersecurity practices that integrate seamlessly with work. Starting from the top management and then cascading to all the employees, through awareness sessions, Trainings & Workshops can help to create a security culture.

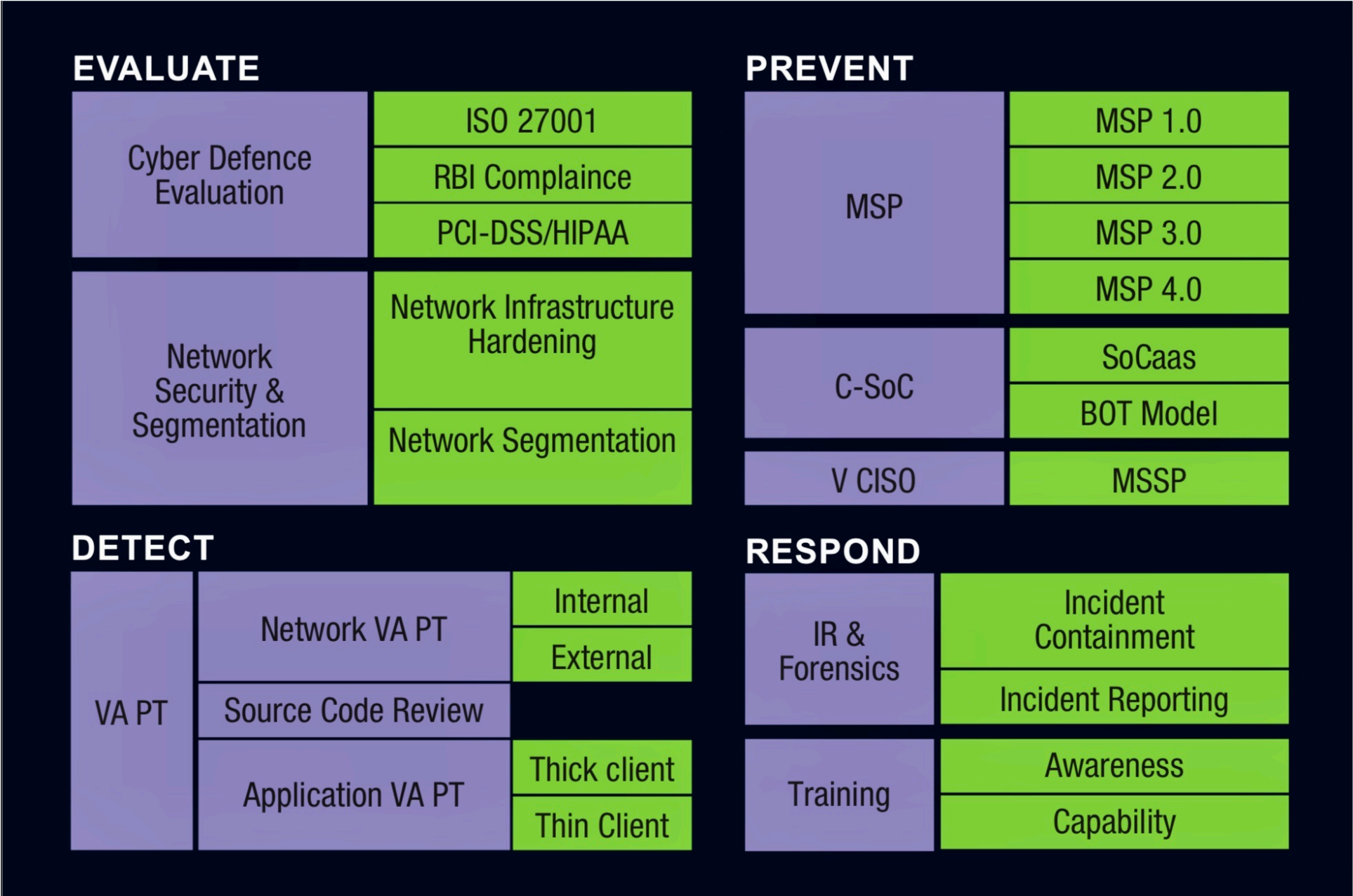
OUR RECOMMENDATIONS FOR COOPERATIVES

The recommendations stated below ideally suits for all cooperative to strengthen their security posture and successfully defend against a cyber attack. The actual security program will depend on the amount of the exposure and the critical assets the organisation wants to protect.

Defense- in-depth techniques can be adopted for those which has a larger exposure surface.

Security Baseline	Controls	Description
Security Foundation	Create an Information Security Policy for Cooperative societies.	Information security policy is required to provide relevant direction and values to individuals within the organisation with regards to security. It will make employees aware of cybersecurity threats and making them amend their behaviour accordingly, in order to mitigate potential threats. This has to be in line with the standards like ISO 27001:2013, RBI Cybersecurity guidelines, PCI-DSS, HIPAA etc.
	Develop an end-to-end cybersecurity strategy	<div>1. Identify the critical assets, the crown jewels.</div> <div>2. Devise a strategy to protect them</div> <div>3. Implement prevention security controls</div> <div>4. Comply to information security standards</div>
Prevention	Secure the network infrastructure	<div>Assess the network infrastructure</div> <div>1. Network environment - Firewalls, IDS/IPS, Routers</div> <div>2. Computing environment - Servers, Cloud</div> <div>3. Endpoint environment - Laptops, Desktops, Mobile devices.</div>
	Network Architecture Security Review (CIS Standard)	The Network Architecture Review will evaluate organisations network in line with CIS standard and identify the weakness and gaps
Protection	Security Controls	<div>Some security controls</div> <div>1. DLP - Data loss prevention</div> <div>2. Encryption of data</div> <div>3. Protection from DDoS attacks</div> <div>4. Identity Access Management</div> <div>5. Patch management</div> <div>6. User access control, Least privilege</div> <div>7. Third party environment - Third party apps, Remote access</div>
Detection	Vulnerability Assessment and Penetration Test	The network & App security audit will help to determine the effectiveness of security and to resolve underlying security issues. VA PT audits are critical to understanding how well the organization is protected against security threats - internal or external.
Defense	Surveillance & Incident response	<div>1. Managed security services</div> <div>2. MSP - UL Managed Security Platform</div> <div>3. Digital surveillance - Cyber Security Operations Center</div> <div>4. Periodical VA PT - Quarterly remote test and Half yearly remote and onsite</div> <div>5. Incident response</div> <div>6. Cyber Forensics services</div>

OUR OFFERINGS:



An overall cybersecurity posture assessment will help to get a view of the cooperative organisations internal and external security posture. We help to diagnose your digital stack and the complex digital environment across computing, network and endpoints and provide comprehensive, adaptive and collaborative security solutions to your cybersecurity concerns.

Our practitioners consists of cybersecurity domain experts, specialised consultants / advisors with extensive expertise in both offensive and defensive security domains and are committed to share their expertise with the clients in securing informations.

1. Cyber Defence Evaluation (Compliance Audit):

Our approach for cyber defence evaluation will be based on the information security policy of the organisation and the standards applicable to the industry concerned. The assessment of the information security policy shall be based on Information Security Management System (ISMS) readiness and compliance review in line with ISO 27001, PCI-DSS, HIPAA, NIST etc.

2. Network Architecture review & Hardening:

We shall conduct network architecture review to analyze relevant network artifacts (e.g. network segmentation, security requirements, technology inventory, DMZ) to identify how the network architecture and controls protect critical assets, sensitive data stores and business-critical interconnections in accordance with organisations business and security objectives.

- It will provide a high-level of design assurance by looking at the network and related security controls in a comprehensive and holistic manner
- Identify security exposures
- Provide feedback on your patch management and change management programs
- Provide prioritized recommendations to mitigate the identified operational risks, including improvements to topology, protocols, policy, device configurations, and network & security management tools.

3. Vulnerability Assessment and Penetration Testing:

Our Vulnerability Assessment and Penetration testing of the internal, external network and web / Mobile applications. The objectives of the testing are to comprehend the susceptibility of infrastructure components to unauthorised access from malicious insiders and outsiders and to help establish the effectiveness of your threat and vulnerability management program. The services will conclude with the development of recommendations to mitigate identified risks to an acceptable level and improve the organisation's information security posture.

4. Managed Security Services:

Our managed security services shall act as the trusted go-to partner bringing advanced expertise in the current threat landscape. We will be an extension of your security team, whether seeking assistance with dedicated and qualified engineers on FTE services, IT consultancy services and Virtual CISO Services. These services are delivered as a part of continuous engagement to provide fully customisable, industry aligned managed security solutions including advanced security event monitoring, threat analytics, cyber threat management, and incident response for businesses to meet the increasing market demand in cybersecurity services.

5. Incident Response / Cyber Forensics:

In case of an Incident gets reported, it will be addressed and managed so as to minimize the damage, reduce the disaster discovery time and mitigate the breach related expenses. Major phases in incident response include detection, analysis, information gathering, containment, education and recovery. Our team is capable to investigate, collect evidence, analyse and preserve evidence in a way that is suitable for presentation in a court of law.

6. C-SoC as a Service:

ULTS's managed Cybersecurity SOC services is a reliable and efficient solution with reasonable cost benefit of the high level expertise. Our security operations centre is a state of the art threat intelligence monitoring station that houses information security team responsible for 24x7 monitoring and analysing the security posture. SOC will monitor and analyse activity on networks, servers, endpoints, databases, applications, websites, and other systems, looking for anomalous activity that could be indicative of a security incident or compromise.

7. Awareness Sessions:

People often form the weakest link in the chain. Educating and creating awareness is needed to identify, report and avoid social engineering vulnerabilities.

The awareness program is divided into three disciplines in order to cater to the needs of the entire spectrum;

- Senior leadership & Governance team:
- IT / Network Engineers
- Employees and stakeholders

8. IT Infrastructure Management & Consultancy Services:

We build the infrastructure with all the components, provide technical support to the clients and maintain the already existing infrastructure. Everything including servicing requests, resolving incidents, applying patches/ upgrades, security remediation and recovering from crashes.

We have the expertise to advise and recommend IT solutions and OEM validation.

MANAGED SERVICES PLATFORM FOR COOPERATIVES





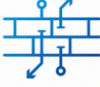








The Managed service platform is designed as a hybrid security assessment and Risk management services through automated and manual intervention as per a prescribed frequency.

The benefits of this platform will be to

1. Reduce cost, 2. Continuously improve security posture, 3. Lower Risk

The cybersecurity landscape is in a constant state of change. The integration and reliance on technology to enable growth is increasing, which poses serious risks to organisations without proper security measures. Managed services platform for cooperatives is designed to provide security-as-a-service to the wholistic information security requirement and as a continuous engagement model.

The areas covered at large are as mentioned below:

 Surveillance Information Security / Compliance Audit	Framework: RBI Cybersecurity Framework ISO 27001:2013 Framework UL Cybersecurity Framework (Any one of the above)  Once in a year
 Backbox Security Assessment	Broad sweep scan Network Application  Once in a quarter
 SMART scan (Systematic Manual And Remote Testing)	Sweep scan on critical elements Network VA PT Application VA PT  Once in a year
 Assess baseline secure configurations	Secure Configuration Endpoint devices OS Network devices Audit Log  Once in a year
 General awareness on cyber threats	Securing the front line  Twice in a year
 Alerts & Advisories	Updates on cyberthreat landscape  Fortnightly
 Assistance to respond to RBI compliance	

ULTS expert team shall assist you with the technical contents related to cybersecurity to enable you to respond to RBI notices and circulars.

The platform consists of pick and choose options for

- A) Small cooperatives (5-25 users)
- B) Medium sized cooperatives (26- 100 Users)
- C) Large cooperatives (Above 100 users)

The pricing for the platform will be based on security as a service based on no: of users / devices and chargeable on a monthly basis, thus avoiding a upfront investment to improve and mania a good security posture. Further, once enrolled, your are in the safe hands of cybersecurity experts at ULCCS.

Activities	Small Cooperatives (5-25 Devices)			Medium Cooperatives (26-100) Devices)			Large Cooperatives (>100) Devices)		
	Silver	Gold	Platinum	Silver	Gold	Platinum	Silver	Gold	Platinum
Compliance and Security Based on Specific Frameworks									
UL Cyber Security Framework	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
RBI Cyber Security Framework	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ISO 27000 Family, HIPAA, PCI or Others	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Security Archecture									
NIST Framework,CIS Controls,SABSA,TOGAF, O-ESA & OSA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Black Box Security Assessment									
Automated Application vulnerability Scans	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Automated Network vulnerability Scans	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
UL SMART									
Application VA PT	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Network VA PT	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Server Security Review	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Firewall Security Review	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Wireless PT	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Mobile Application VA PT	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Source Code Review	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IoT VA PT	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SCADA/ICS Security Testing	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Identity and Access Management									
UL Access Managment Solution	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Third Party Solution*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Endpoint Detection and Response									
UL ITDR	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Third Party Solution*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Digital Forensics and Incident Response	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Cyber Security Operation Centre as a Service	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Virtual CISO Service	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Threat Hunting	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Insurance Assistance	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Information Security Consultancy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
General awareness session , Silver Plan -1 Session ,Gold and Platinum-2 Sessions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Alerts & Advisory intelligence from the cyber threat landscape - Fortnightly	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**Cybersecurity is a journey,
Not a destination.**

PARTNER WITH US FOR YOUR SECURED JOURNEY

WHY ULCCS?

ULCCS through its IT initiative ULTS has unmatched expertise in cybersecurity strategic advisory, consulting, incident response, defence evaluation, detection and managed security services to prepare your businesses against cyber adversaries and reduce your threat and vulnerability exposure.

We provide a holistic digital risk management approach to prevent and protect organisations from cyber threats.

Our expertise is backed by:

- Each senior member of our consulting practice has at least 15 years' experience in information security audit cybersecurity, Cyber Forensics.
- The CoE team maintains prestigious professional certifications and licenses, such as **LA ISO 27001, PCI-DSS imp, CISA, CEH, CCNA, CCNP, MCSE, ITIL V2, CSM, CISSP, PCNSE, SCRUM** and more.
- State-of-the-art cross-spectrum security services based on leading security solutions that are independent of the hardware layer.
- Deep experience in integrating security services with complex, large-scale IT programmes.
- Readiness to intervene and contain any sort of cyberattack in real-time with **UL CERT (Cyber Emergency Response Team)**
- A strong commitment to innovation through emerging technologies like AI, Big Data, Blockchain and IoT.
- Member of the NCDC led **Cooperative Institutions Cybersecurity Advisory Forum (CICAF)**.



For enquiries :

Anoop Sivan
Account Manager

Email: anoop.sivan@ulcs.in

Cell:+91 9962060811

ULTS,
(An IT Initiative of ULCCS Ltd)
UL Cyber park, Nellikode Village, Nellikode (P.O)
Kozhikode- 673 016, India

www.ulcs.in

© 2020 ULTS, All Rights Reserved.

ULTSbelieves the information in this document is accurate as of its publication date; such information is subject to change without notice. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior permission of ULTS.

ulcs



ULCCS Ltd.