Background

Cyber Care (Pvt) Ltd is a company of enthusiastic information security experts that offer comprehensive, professional advice and education in the IT security field. An idea of quality and excellence conceived through passion and experience to address the needs of the ICT world as a whole and to specifically offer specialized services to ICT companies within our reach.

Cyber Care is a group of innovative and experienced young Zimbabwean professionals from the information security sector. The group has diversified technical experience in information technology audit and security implementation and maintenance.

Cyber Care is set to provide information technology security consultancy services that will enable service providers and consumers to compute securely.

Vision
Proactively protect all Zimbabwean systems and become the paramount security "solution" provider by 2018

Mission
To empower ICT professionals and institutions who use information technology about information security.

Values
- Confidentiality
- Integrity
- Authenticity

Security solution for proactive businesses
Think you're too small to be hacked?

Think again.

A common myth is that “we’re too small for anyone to be interested in hacking us.” Actually, small and medium-sized enterprises make the most enticing targets for cyber attacks. Why? Because the bad guys assume these organizations pay less attention to cybersecurity and have fewer resources to put toward the problem. Grabbing relatively modest assets from dozens of small businesses can be easier and more rewarding than the effort involved in making a major haul from a large enterprise.

This is one test you may want to fail.

Professional & Ethical Standards

- Serve & protect the client & uphold the security profession.
- Never take personal copies of the client’s data
- Never perform unauthorized testing
- Do not discuss any findings with unauthorized people
- Do not publish vulnerabilities without permission
- Test everything in scope and never go outside
- Observe all legal requirements
- Act with integrity
- Avoid conflicts of interest
- Avoid FUD (Fear, Uncertainty, Doubt)
- Avoid hubris
- Protect the client’s data
- Do not associate with black-hat hackers
- To understand the level of risk for your organization compared to similar companies.
- To complement your automated scanning appliance to better identify and validate all security vulnerabilities associated with your internet-facing environment as well as internal systems

Cyber Care also tests externally-facing network systems and services for vulnerabilities attributable to:
- Software flaws
- System configuration settings
- Network-layer password weaknesses

The devices tested include those that are accessible via public IP addresses, such as:
- Firewalls
- Routers
- DNS & other external services including servers on your DMZ
- Remote access services such as dial-up modems and IPSec endpoint.

All externally-reachable services will be identified and documented. Disruption to operations will be minimized.

Let Cyber Care discover your vulnerabilities before someone else does.

Consultancy Services

Penetration Testing

Our penetration tests utilize a risk-based approach to manually identify critical infrastructure vulnerabilities that exist on all internet-accessible services and internal systems within scope.

The primary goals of this assessment are to:
- Provide recommendation and details to facilitate a cost-effective and targeted mitigation approach.
- Create a basis for future decisions regarding information security strategy, requirements & resource allocation.

Why perform penetration testing
- To execute a real-world attack on critical infrastructure & understanding of the level of risk that exists as a single moment in time
Personnel who are trustworthy, cleared, credentialed, & trained. Because you're asking us to break into the inner-most recesses of your IT systems, you need the assurance that our personnel can be trusted and won't make mistakes. Many of our personnel are certified ethical hackers (CEHs) or have other certification such as Computer Hacking Forensic Investigation (CHFI). We have a strong commitment to cross-training our personnel so they can handle the full scope of cyber-related tasks including white-hat hacking, vulnerability analysis, assessment and authorization (A&A), and others.

Wireless Penetration Testing
Large corporation usually prefer wireless networks because of the increased convenience. This convenience comes at a price, however - if these networks are poorly secured, the entire network is at risk.

In addition to the protection of the official network, employees often establish their own hot-spots in the infrastructure to grant themselves or other easier access to the network. We here at Cyber Care do an analysis of all the active nodes in your facility.

### External Breaches Are Your Greatest Threat

<table>
<thead>
<tr>
<th>Percentage of all intrusions resulting from:</th>
<th>2009</th>
<th>2010</th>
<th>2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Agents</td>
<td>70%</td>
<td>92%</td>
<td>98%</td>
</tr>
<tr>
<td>Successful Hacks</td>
<td>40%</td>
<td>50%</td>
<td>81%</td>
</tr>
</tbody>
</table>

Source: Verizon Data Breach Investigations Report

Don't think that your worst security threats are only from disgruntled employees or failing to follow established security policies. The vast majority of attacks come from sources outside your organization or utilize some form of hacking. Telos can help you uncover these threats and effectively deal with them.

Our wireless investigations include but not limited to:-
- Encryption methods in use
- Central point for authentication
- Range of wireless networks
- Injection attacks on wireless networks
- Threat of break-ins
- Adequate protection of clients
- Unprotected areas of the network
- Access to network via inadequately secure elements
- Network naming convention
- Key / certificate change / rotation

### Tool usage and development

Tool usage and development has been a part of our assessment and authorization practice. Tools that we are proficient in and have successfully used during our penetration test efforts include:

- AppDetective™
- AppScan®
- Burp Suite
- CORE Impact®
- Metasploit® Framework
- Nessus®
- Nikto
- Nmap
- Retina
- w3af
- WebInspect
- WebScarab
  (or similar proxy technology)
All testing begins with limited knowledge and no credentials provided and is designed to simulate a real-world attack on your wireless infrastructure. This will help the client learn what vulnerabilities exist and the overall information security risk the wireless infrastructure introduces to your IT environment.

If desire, testing can also be performed with provided user credentials to associate to the wireless network and determine if access controls to connected networks are sufficient and systems located on the wireless network are sufficient and systems located on the wireless network are hardened.

Social Engineering
This is a sub-class of penetration testing that focuses on identifying and validating vulnerabilities associated with a client's employees ability to follow documented policies & procedures & security best practices. Types of social engineering will be remote & on-site.

SIEM Log Collection & Correlation
Each device in today's computer environment has a capability to write the events to a log file, these files need to be monitored on a daily basis. They show the administrator that an attack is underway. But we are all human, it is impossible today to monitor your logs and to perform your day-to-day work that is required from you. Cyber Care poses these three crucial questions.
1. Do you read through all the events in your log file on a daily basis?
2. Do you investigate all the event ID’s that are found in the log files?
3. Do you keep your log files for forensic investigation IN A CENTRAL LOCATION?

In the event that you answered NO to any of the above questions, you have to look at a "Log Management" solution. Cyber Care offers System Information Event Management (SIEM) solutions. These solutions provide you to real time monitoring of logs, incident detection, unified collection, aggregation and analysis etc. Contact us for this service.

Computer Forensics
Cyber Care offers this service so as to detect hacking attacks and properly extracting evidence to report the crime and conduct audits to prevent future attacks. We gather evidence from a wide range of computer crimes or misuse, including but not limited to theft of trade secrets, theft or destruction of intellectual property, and fraud. Our consultants draw on an array of methods for discovering data that resides in a computer systems, or recovering deleted, encrypted, or damaged file information, intruder's footprints and to properly gather the necessary evidence to prosecute.

Information Security Gap Analysis
Consultants will help you determine the present state of information security within your enterprise and its ideal or optimum state. With its experience Cyber Care will assist in bridging the space.
It does this by highlighting which requirements are being met and which are not. This analysis will provide a foundation for measuring the investment of time, money and human resources that is required to achieve a particular outcome.

Our gap analysis maybe aligned to different information security standards or best practices or the organizations already setup security policy.
Incidence Response Plan

This is an organized approach to addressing and managing the aftermath of a security breach or attack (incident). The goal is to handle the situation in a way that limits damage and reduces recovery time and costs. Our incidence response plan will include a policy that will define, in specific terms, what constitutes an incidence and provides a step-by-step process that should be followed when and incident occurs.

Cyber Care (Pvt) Ltd will assist clients in drafting a response procedure that will help them to reduce downtime as well as increase productivity. Basic steps to come up with this plan include preparation, identification, contamination, eradication, recovery and lessons learned.

Security Awareness Training

One of the greatest threats to information security could come from within a company or organization. Inside 'attacks' have been noted to be some of the most dangerous since these people are already quite familiar with the infrastructure. It is not always disgruntled workers and corporate spies who are a threat. Often, it is the non-malicious, uninformed employee.

Security awareness training will focus on uninformed users who can do harm to your network by visiting websites infected with malware, responding to phishing e-mails, storing their login information in an unsecure location, or even giving out sensitive information over the phone when exposed to social engineering.

Data Loss Prevention

This is an aim to protect an organization's critical information & access to it whether that information may exist.

DLP is a mechanism that identifies sensitive information by content-regardless of whether it is data in the process of being transmitted over the network (data in motion [DIM]), data on a server (data at rest [DAR]), or data at the end-point like a PC (data in use [DIU]) – and prevents it from leaking outside the company.
Some of the more important items to cover in the security awareness training will include the organizations security policy, data classification and handling, workspace and desktop security, wireless networks, password security, phishing, hoaxes, malware, file sharing and copyright.

Compliance Training

These are refresher courses that are based on the organizations already setup security policy or futuristic security policy. Other compliance training's include ISO 27001/27002 and PCI DSS for the purposes of being compliant with international standards.

NOTE: All consulting work is kept strictly confidential. Non-disclosure agreements are signing and rules of engagement stated before carry out any tasks. A detailed report(s) are submitted of every method used and result at the end of a milestone or task.

Information Security Audit

Consultants will carry out an evaluation of the security of your organizations information system by measuring how well it conforms to a set of established criteria. The audit will conduct a series of tests that guarantee that information security meets all expectations and requirements within the organization. It also ensures that data and assets related to information security i.e. phones, network, email, access cards, passwords, tokens are protected.