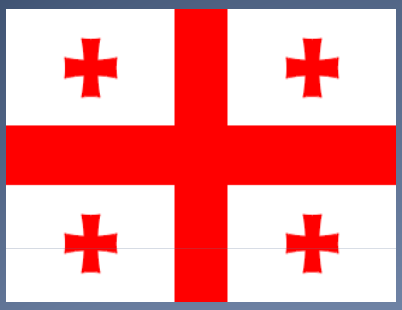
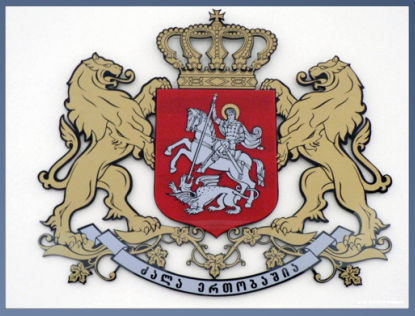
"Real-Time" Georgia!.....

.....Securing Government & Enterprise Operations



Dr David E Probert
VAZA International



1st Georgian IT Innovation Conference
Tbilisi, Georgia : 29th - 30th Oct , 2008

Download GITI Presentation On-Line @ www.valentina.net/vaza/eGe.pdf

Introduction

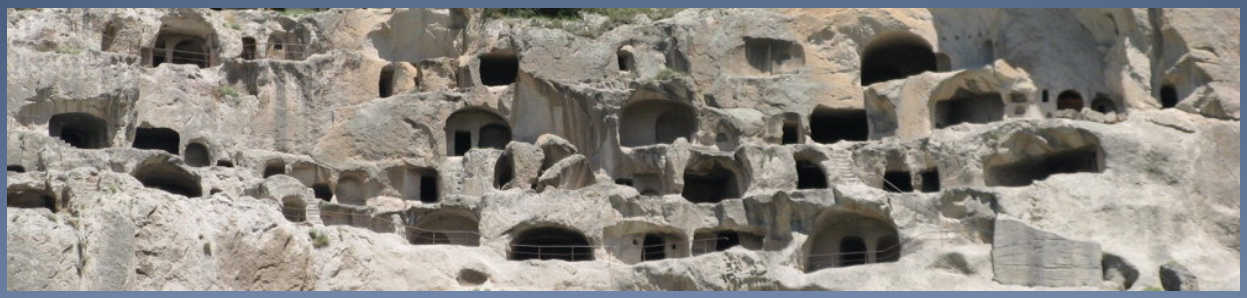
- IT Security is critical to Georgia's future economic growth
- EU Security Adviser to the Georgian Parliament – 2007
- Working with IT specialist Tbilisi-based Orient-Logic Team
- "Real-Time" Georgia requires distributed e-defence network
- Current networks are quite fragile, insecure & open to attack

Current Security Situation

- Too many single points of network & system failure
- Inadequate data back-up & storage procedures
- Often there is no real communicated security policy
- Networks open to Cyber Attacks and Cyber Crime
- Small skill base of specialist IT security personnel

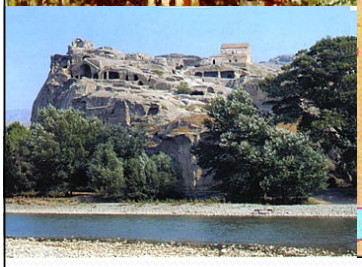
Project Vardzia - ვარძია

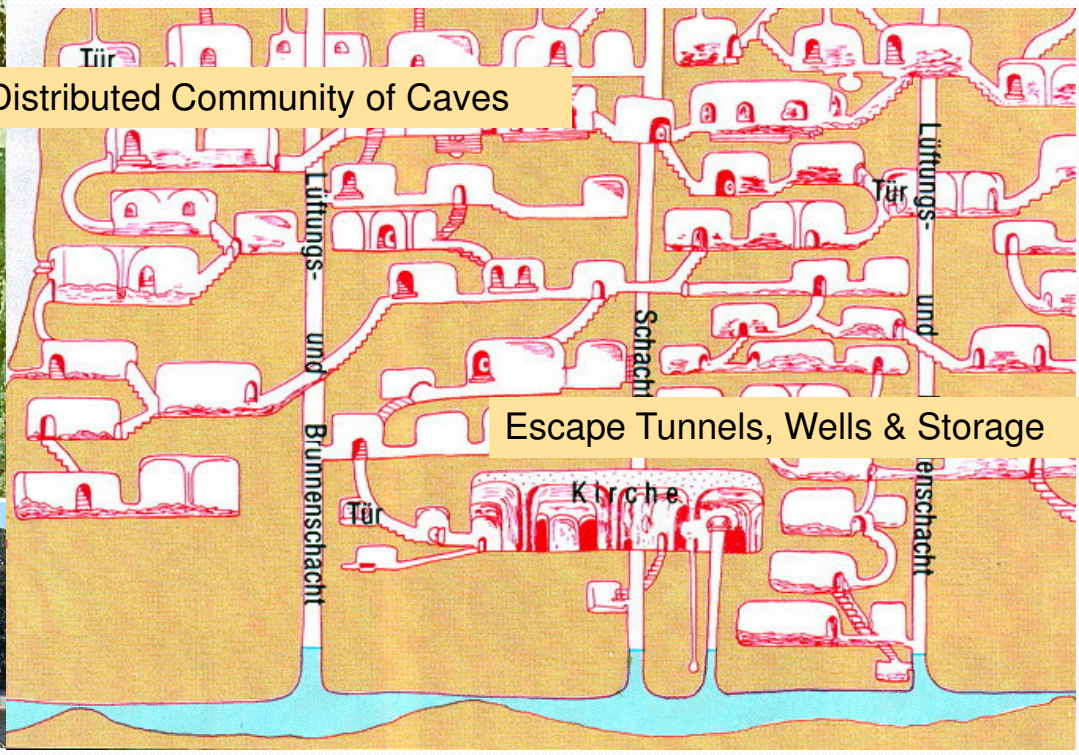
- 12thC Vardzia was a secure distributed networks of caves!
- Vardzia caves provided physical protection for 300+ years
- All resources were secured including water from River Kura
- Escape tunnels, wells & food storage protected against siege…



- …eGeorgia community requires distributed electronic security
- Security is not a "quick IT patch" but requires a multi-year programme based upon recognized ISO/IEC 27000 Standards

Vardzia: Secure 12thC Community





Distributed Community of Caves

Escape Tunnels, Wells & Storage

Major 21stC Security Threats

- Distributed Denial of Service (DDOS) through "Botnets"
- Targeted Trojan Horses (including dormant sleepers)
- Destructive Viruses (often by email & exe files & scripts)
- Theft of Information, Passwords, ID & Keys
- Fake Web Sites and IP Addresses
- Physical Destruction through fires, floods, earthquakes
- Planned Cyber Attacks and Cyber Crime
- Remote Agent interception & control of "secure" networks

The CyberCrime Business Model

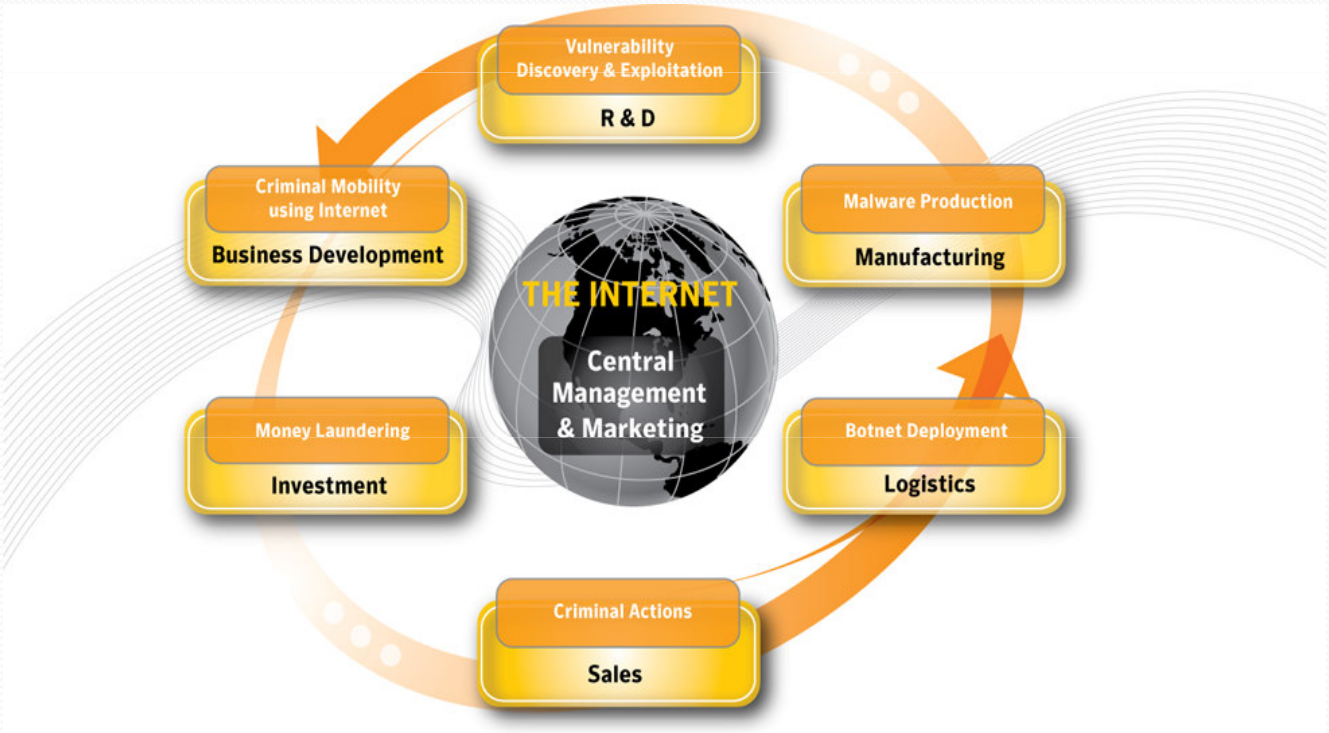


Diagram Courtesy of Symantec - UK

Technological Solutions

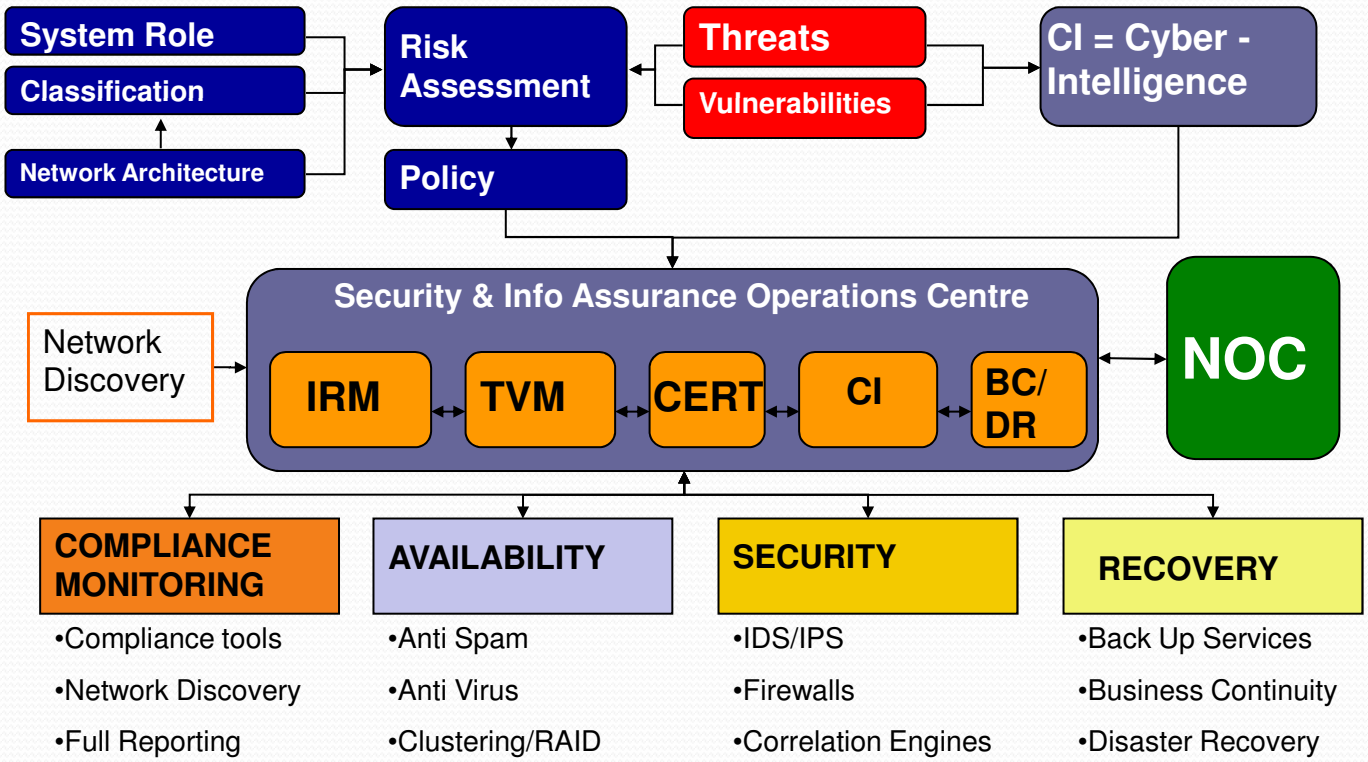
- Intrusion Detection & Protection Systems (IDS/IPS)
- Threat and Vulnerability Management (TVM)
- Real-Time Deep-Packet Inspection to detect DDOS Attack
- Web-Site & IP Address Assessment
- End-User Log-On Authentication & Certificates– IEEE802.1X
- Encryption both for secure networks as well as storage
- Digital Signatures to secure Data & Document Integrity
- Biometric access both for IT Devices as well as access security

Operational Solutions

- Business Continuity Programme (BCP)
- Disaster Recovery Planning & Training (DR)
- Electronic Asset Management (RFID Tagging)
- Physical Building Security (Networked IP CCTV)
- CERT (Computer Emergency Response Team)
- Professional Security Training to ISO Standards
- Communication of comprehensive security policy

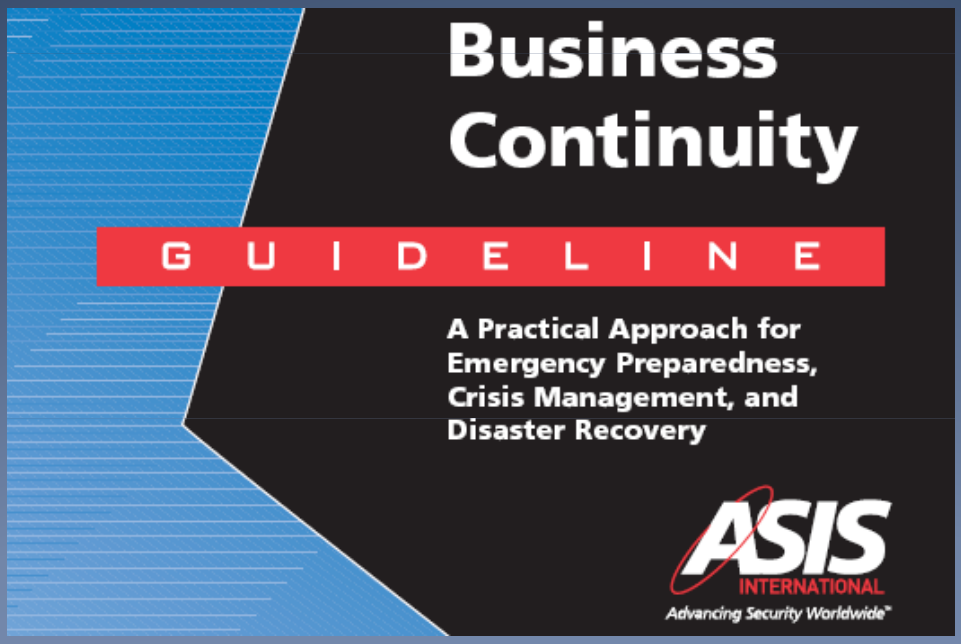
➢ *.....Integrated Tech & Op Solution = Cyber Defence Centre*

Integrated Cyber Defence Centre



Business Continuity Guidelines

- ASIS International Commission on Business Continuity & Disaster Recovery Guidelines- 2005



- ASIS Guidelines also include an excellent complete checklist for Business Continuity Planning

Security Standards - Matrix

- Framework for comprehensive security policy from Information Security Forum : ISF
- Security Standards includes the ISO/IEC – 27000 Series – 27001 and 27002 & 2700x
- European Countries such as UK and Germany have full-time security teams
- Georgian Government requires full-time Security Team to implement & monitor Policy

Information Security Forum (ISF) : "Top Themes"

Aspect	The Standard of Good Practice
Security Management	Keeping the business risks associated with information systems under control within an enterprise requires clear direction and commitment from the top, the allocation of adequate resources, effective arrangements for promoting good information security practice throughout the enterprise and the establishment of a secure environment.
Critical Business Applications	A critical business application requires a more stringent set of security controls than other applications. By understancing the business impact of a loss of confidentiality, integrity or availability of information, it is possible to establish the level of criticality of an application. This provides a sound basis for identifying business risks and determining the level of protection required to keep risks within acceptable limits.
Computer Installations	Computer installations typically support critical business applications and safeguarding them is, therefore, a key priority. Since the same information security principles apply to any computer installation - irrespective of where information is processed or on what scale or type of computer it takes place - a common standard of good practice for information security should be applied.
Networks	Computer networks convey information and provide a channel of access to information systems. By their nature, they are highly vulnerable to disruption and abuse. Safeguarding business communications requires robust network design, well-defined network services, and sound disciplines to be observed in running networks and managing security. These factors apply equally to local and wide area networks, and to data and voice communications.
Systems Development	Building security into systems during their development is more cost-effective and secure than grafting it on afterwards. It requires a coherent approach to systems development as a whole, and sound disciplines to be observed throughout the development cycle. Ensuring that information security is addressed at each stage of the cycle is of key importance.

Topic	SM	CB	CI	NW	SD
Access control		CB3.1 Access control	CI4.1 Access control arrangements CI4.3 Access privileges		
Acquisition					SD4.4 Acquisition
Application controls		CB2.2 Application controls			SD4.2 Application controls
Asset management	SM4.3 Asset management		CI1.3 Asset management		
Availability requirements		CB1.3 Availability requirements			SD3.4 Availability requirements
Back-up		CB4.4 Back-up	CI3.2 Back-up	NW3.5 Back-up	
Business continuity	SM4.5 Business continuity	CB2.5 Business continuity	CI6.1 Contingency plan CI6.2 Contingency arrangements CI6.3 Validation and maintenance	NW3.6 Service continuity	
Change management		CB2.3 Change management	CI3.3 Change management	NW3.2 Change management	
Confidentiality requirements		CB1.1 Confidentiality requirements			SD3.2 Confidentiality requirements
Configuring network devices				NW2.1 Configuring network devices	
Cryptography	SM6.1 Use of cryptography	CB6.2 Cryptographic key management			
Development methodologies and environment					SD1.2 Development methodology SD1.4 Development environments
E-mail	SM6.3 E-mail				
Electronic commerce	SM6.6 Electronic commerce				

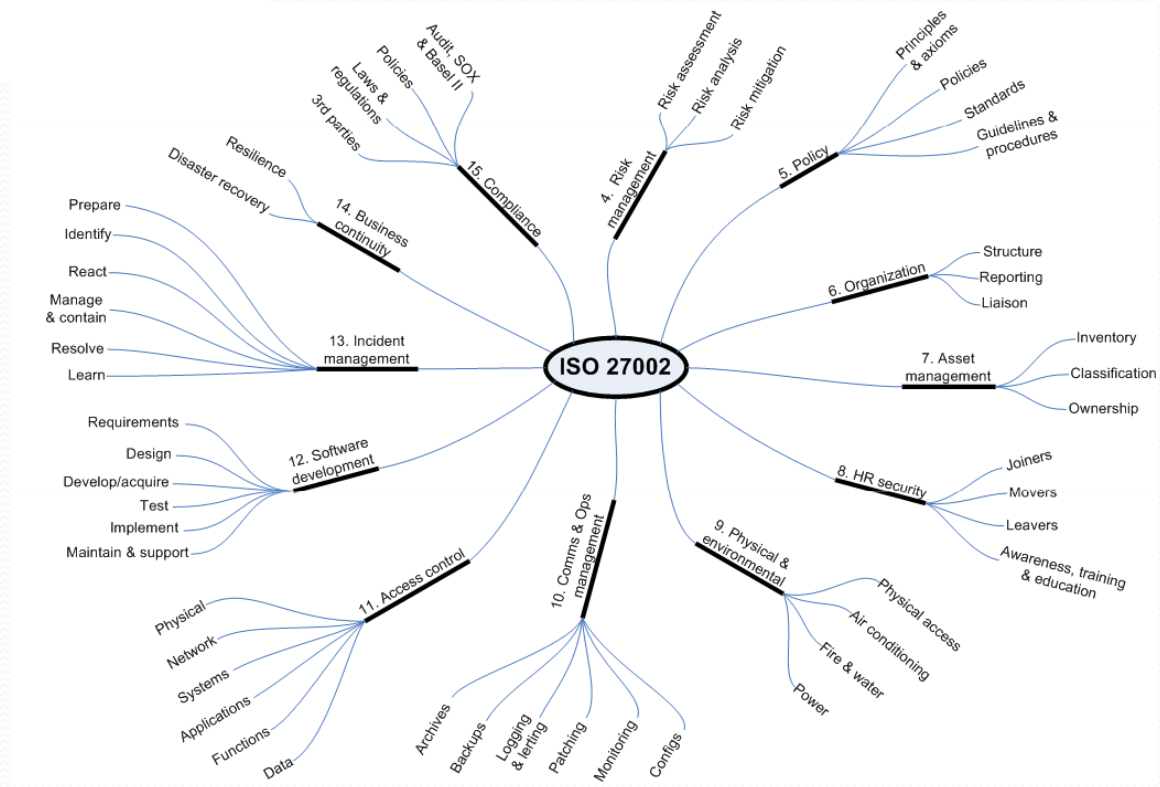
Topic	SM	CB	CI	NW	SD
Emergency fixes			CI3.5 Emergency fixes		
Event logging			CI2.2 Event logging		
External access/ connections		CB4.3 External connections		NW2.3 External access	
Firewalls				NW2.2 Firewalls	
Forensic investigations	SM5.5 Forensic investigations				
General security controls					SD4.3 General security controls
Handling information		CB2.6 Sensitive information	CI3.1 Handling computer media		
Hazard protection			CI2.6 Hazard protection		
Host system configuration			CI2.3 Host system configuration		
Incident management	SM5.4 Emergency response	CB2.4 Incident management	CI3.4 Incident management	NW3.3 Incident management	
Information privacy	SM4.2 Information privacy				
Information security function	SM2.2 Information security function				
Installation and network design			CI2.1 Installation design	NW1.2 Network design	
Instant Messaging	SM 6.8 Instant Messaging				
Installation process					SD6.2 Installation process
Integrity requirements		CB1.2 Integrity requirements			SD3.3 Integrity requirements
Intrusion detection	SM5.3 Intrusion detection				

Topic	SM	CB	CI	NW	SD
Local security co-ordination	SM2.3 Local security co-ordination	CB5.1 Local security co-ordination	CI5.1 Local security co-ordination	NW4.1 Local security co-ordination	SD2.1 Local security co-ordination
Management commitment	SM1.1 Management commitment SM2.1 High-level control				
Malicious mobile code protection	SM5.2 Malicious mobile code protection				
Network documentation				NW1.4 Network documentation NW5.1 Voice network documentation	
Outsourcing	SM6.7 Outsourcing				
Patch Management	SM 5.6 Patch management		CI3.6 Patch management		
Physical protection	SM4.4 Physical protection		CI2.8 Physical access	NW3.4 Physical security	
Post-implementation review					SD6.3 Post-implementation review
Power supplies			CI2.7 Power supplies		
Public key infrastructure	SM6.2 Public key infrastructure	CB6.3 Public key infrastructure			
Quality assurance					SD1.3 Quality assurance
Remote maintenance				NW3.7 Remote maintenance	
Remote working	SM6.4 Remote working				
Resilience		CB4.2 Resilience	CI2.5 Resilience	NW1.3 Network resilience NW5.2 Resilience of voice networks	
Risk analysis/assessment	SM3.3 Information risk analysis	CB5.3 Information risk analysis	CI5.4 Information risk analysis	NW4.4 Information risk analysis	SD3.5 Information risk assessment
Roles and responsibilities	SM3.2 Ownership	CB2.1 Roles and responsibilities	CI1.1 Roles and responsibilities	NW1.1 Roles and responsibilities	SD1.1 Roles and responsibilities

Topic	SM	CB	CI	NW	SD
Security architecture	SM4.1 Security architecture				
Security audit/review	SM7.1 Security audit/review	CB5.4 Security audit/review	CI5.5 Security audit/review	NW4.5 Security audit/review	SD2.3 Security audit/review
Security awareness	SM2.4 Security awareness	CB3.4 Security awareness	CI5.2 Security awareness	NW4.2 Security awareness	SD2.2 Security awareness
Security classification	SM3.1 Security classification	CB5.2 Security classification	CI5.3 Security classification	NW4.3 Security classification	
Security education	SM2.5 Security education				
Security monitoring	SM7.2 Security monitoring				
Security policy	SM1.2 Security policy				
Service providers		CB4.1 Service agreements	CI1.2 Service agreements	NW1.5 Service providers	
Sign-on process		CB3.2 Application sign-on process	CI4.4 Sign-on process		
Special controls				NW5.3 Special voice network controls	
Specifications of requirements					SD3.1 Specification of requirements
Staff agreements	SM1.3 Staff agreements				
System design/build					SD4.1 System design SD4.5 System build
System network monitoring			CI1.4 System monitoring	NW3.1 Network monitoring	
System promotion criteria					SD6.1 System promotion criteria
Testing					SD5.1 Testing process SD5.2 Acceptance testing
Third party access	SM6.5 Third party access	CB6.1 Third party agreements			

Topic	SM	CB	CI	NW	SD
User authentication			CI4.5 User authentication		
User authorisation			CI4.2 User authorisation		
Virus protection	SM5.1 Virus protection				
Web-enabled applications		CB6.4 Web-enabled applications			SD4.6 Web-enabled development
Wireless access				NW2.4 Wireless access	
Workstation configuration		CB3.3 Workstation configuration	CI2.4 Workstation configuration		

ISO27002: Security Standard - Scope



EU Country Model Review

- UK Developed e-Government Security Architecture, Data Interchange Format as well as framework for disaster recovery and management – 2002
- German Government published detailed IT Security Guidelines – 2004
- Also worthwhile researching other EU National Government Security Frameworks as input for Republic of Georgia – Government Security Policy

E-Government – UK Security Model

Office of the *e-Envoy*
Leading the drive to get the UK online
delivering UK online

Network Defence
e-Government Strategy Framework Policy and Guidelines

Version 2.0
September 2002

Office of the *e-Envoy*
Leading the drive to get the UK online
delivering UK online

Security Architecture
e-Government Strategy

Version 2.0
September 2002

Office of the *e-Envoy*
Leading the drive to get the UK online
delivering UK online

Registration and Authentication
e-Government Strategy Framework Policy and Guidelines

Version 3.0
September 2002

Office of the *e-Envoy*
Leading the drive to get the UK online
delivering UK online

Trust Services
e-Government Strategy Policy Framework and Guidelines

Version 3.0
September 2002

German Government Guidelines

IT Security Guidelines

IT Baseline Protection in brief

BSI

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189, 53175 Bonn • Postfach 20 03 63, 53133 Bonn
Tel.: + 49 (0) 1888 9582-0 • Fax: + 49 (0) 1888 9582-400 • Internet: www.bsi.bund.de

Short Term Programme…

…Next 12 Months – Up to 2010

- Establish Cyber Security Team
- Government Security Review & Audit
- Information, Database and Document Back-Up
- Upgrade Security Software & Systems
- Replicate Network & Wireless Connectivity
- Ensure Information and Database Integrity
- Work with NATO / EU to launch Cyber Defence Centre

Medium Term Programme…

…3 Years – Up to 2012

- Data Centre Storage, Virtualisation & Remote Back-Up
- Security for the Regional and Local Government Offices
- Professional Security Training with Government Certification
- Develop in-depth BCP and Disaster Recovery Programmes
- Implement Deep-Packet Inspection as early alert for DDOS
- Launch fully secure e-Business Ventures in target sectors
- Consider GRENA.Ge – Georgian Research & Academic Network
  - An excellent reference point & foundation for eGeorgia – eGe
  - Already includes a Computer Emergency Response Team - CERT.Ge

The primary mission of GRENA is creation of a unique information infrastructure connected to Internet for Georgian research and educational institutions, libraries, academic hospitals, international organizations and their programs working in education.
It was founded on 26 July 1999.

GRENA
Georgian Research and Educational Networking Association

ქართული English

Georgian Research and Educational Networking Association (GRENA)
10 Chovelidze St.,
0108 Tbilisi, Georgia
Tel: +995 32 250590
+995 32 250591
Fax: +995 32 912952
E-mail: contact@grena.ge
Web-site: www.grena.ge

- About GRENA
- News
- Service
- Cooperation
- Education

We offer guaranteed high speed internet service (ADSL) to the organizations working in scientific, educational and informational spheres using following telephone stations: 22, 23, 25, 29, 30, 33, 36, 37, 38, 39, 91, 92, 93, 94, 95, 96, 97, 98,

Guaranteed INTERNET

Dear Customers,

For the purposes of improving our service and its transparency, we have created an online system for monitoring internet speed used by you. You have an opportunity to control your internet speed during 24 hours.

As an example, please find below a statistical chart reflecting the speed of internet used by you. International and local traffic is recorded as a whole; statistics are renewed automatically in every 5 minutes.

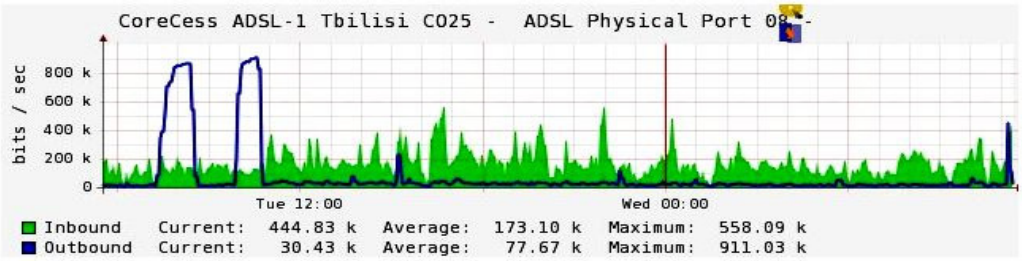
Chart reflects the speed of internet package received and sent by you.

www.cert.ge
www.grena.ge

Inbound - Speed K - Kb/sec, Speed M - Mb/Sec
Outbound - Speed K - Kb/sec, Speed M - Mb/Sec

Also, statistics demonstrate an average and maximum speed of internet used by you.

To find statistics of your internet traffic, please visit **http://netmrg.grena.ge** and enter your username and password.



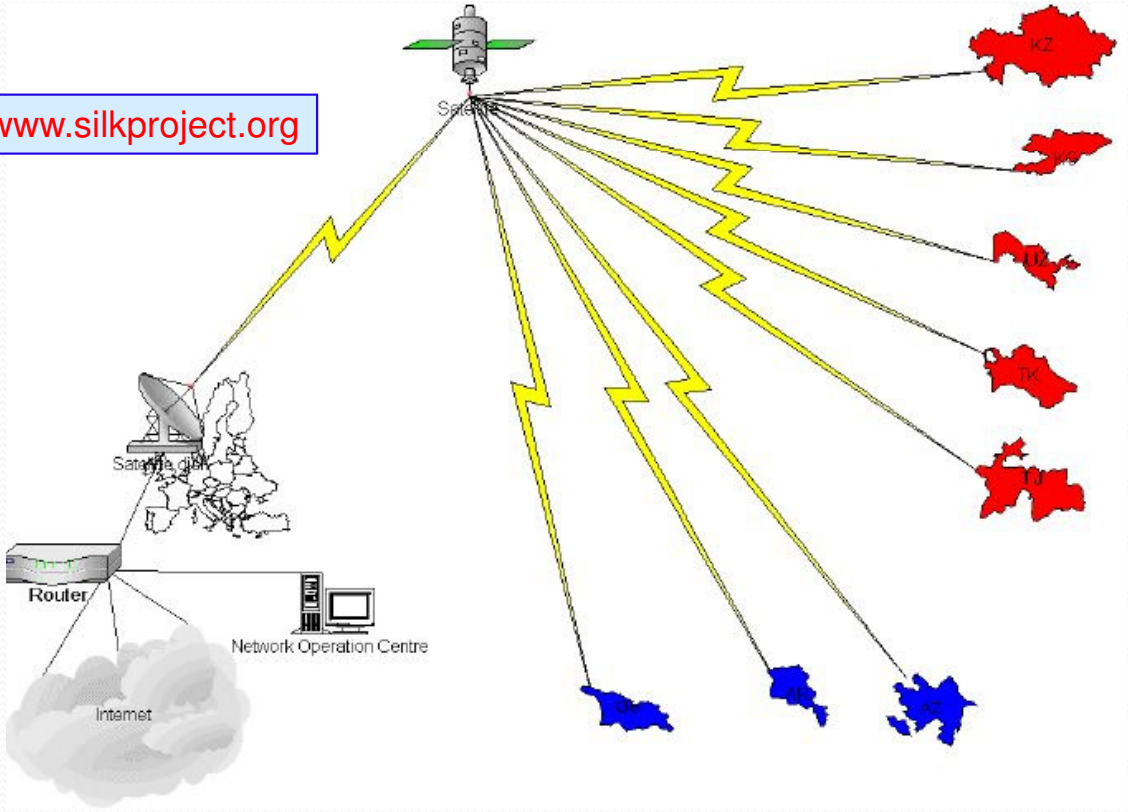
Longer Term Programme…

…5 Years – Up to 2014

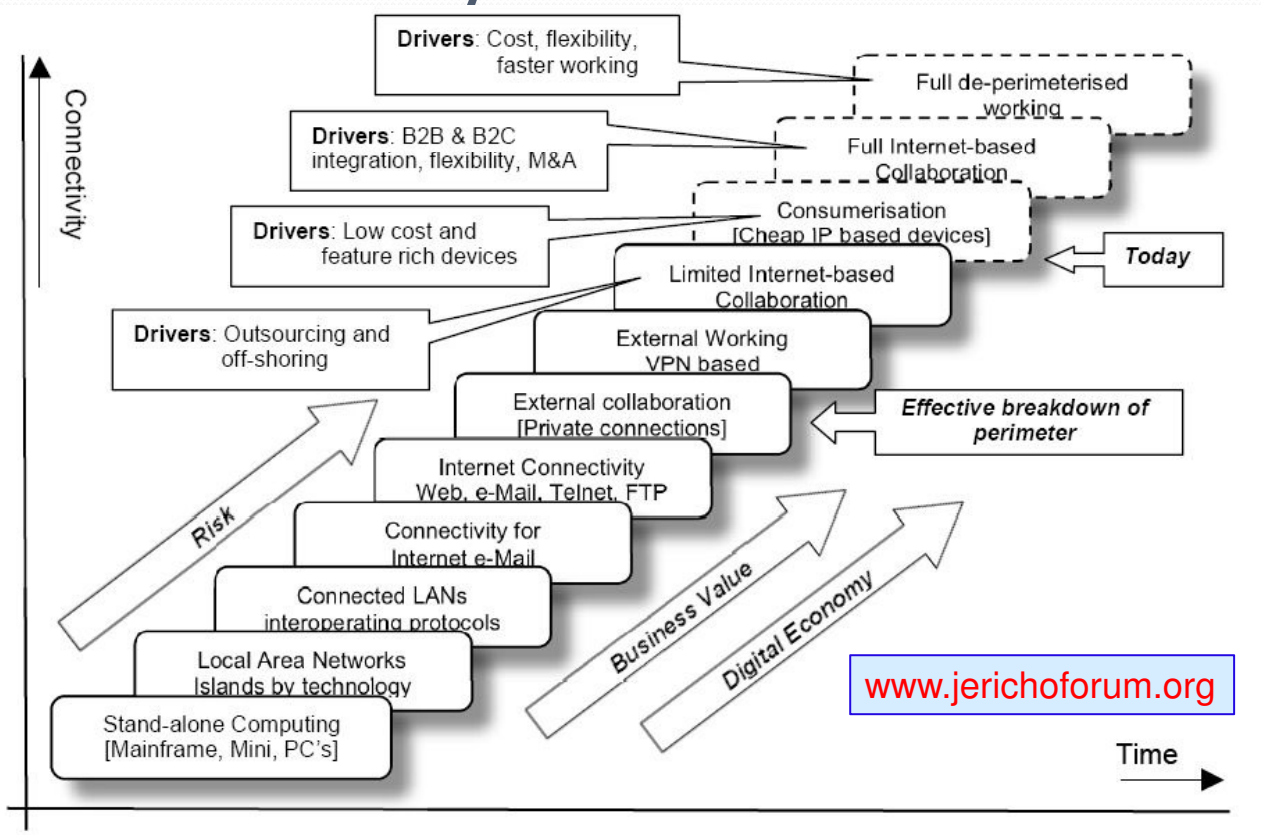
- Trans-Europe eGovernment Interoperability Framework – EIF
- Physical Access, CCTV and Electronic IP Security Integration
- Biometric ID and RFID Asset Management
- Security of End-User Devices and New Software Applications
- Georgia as an International e-Trading Economic Hub
- The NATO sponsored satellite based Virtual Silk Highway Project is an excellent reference project – SilkProject.org

NATO : Virtual Silk Highway Project

www.silkproject.org



New Security for 21stC Networks



www.jerichoforum.org

Biometric Security Solutions

- Latest Biometric Technologies include : Finger Print, Palm Print, Vein ID, Iris Scan, 3D Facial Recognition
- Personal ID Documents – Passports, Driving Licences
- Applications for Border Protection, Offices, Hospitals, Prisons, Transportation, Banks, IT Mobile Devices
- Easily integrated using the ISO BioAPI Specification, and IP networked as total physical security solution
- Extremely portable and robust security solution in difficult environmental locations – quickly installed

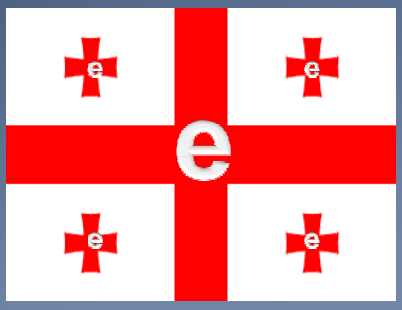
Next Practical Steps...

...6 Months - Nov 2008 to April 2009

- Appoint a full-time team of Government Security Professionals
- Undertake a comprehensive audit of all strategic government facilities, focusing upon potential single points of failure
- Based upon the security audit, develop detailed engineering plans with both approved international consultants & local IT vendors
- Take urgent measures to protect against further DDOS attacks
- Work with NATO & EU teams to establish a Cyber Defence Centre as focus for National Security Monitoring, Alerts & Training

eGeorgia: საქართველო : eGe

- Mission Critical Programme for the 21stC Georgian Economy
- In-Depth Security Project required to protect eGovernment and eBusiness against all future Cyber Attacks and Cyber Crime
- Start *Project Vardzia* as comprehensive 21stC Security Defence



e = *electronic*

G =Georgia

e = *economy*

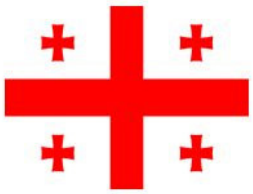
21stC

Download "White Paper" – "Real-Time Georgia" @ www.valentina.net/vaza/GITI.pdf

e-Security "White Paper"

"Real-Time Georgia"

Securing Government & Enterprise Operations



Dr David E Probert

VAZA International

Download @ www.valentina.net/vaza/GITI.pdf

1st Georgian IT Innovation Conference

Tbilisi : 29th & 30th October 2008

"Real-Time Georgia": *Securing Government & Enterprise Operations*

Dr David E Probert – *VAZA* International – www.*VAZA*.com

(1) Introduction: The security of Georgia will be critical to the future economic growth and development of this new democratic nation. Last year I was honoured to be invited by the European Union to review and to make recommendations with regard to improving and upgrading the security for the Georgian Parliament, working with its IT Director – Merab Gotsiridze. I was also invited by Dr Dimitri Kipiani (Orient-Logic Ltd) to present to a group of Enterprise CIOs & Government IT Specialists with regards to Business Continuity and Disaster Recovery, as well as IT Security, Denial of Service and protection against Cyberwarfare. Much has happened during the last 12 months, and it is a real pleasure to be back in Tbilisi, working with new friends and colleagues to further plan, and to upgrade the electronic security infrastructure as the basis of national resilience!

This Security White Paper focuses upon the practical project steps required to upgrade Georgia's IT, Computing & Communications Infrastructure to support a fully secure and resilient "Real-Time" 21stC e-Government, linked with electronically trading enterprises both in Georgia & Globally.

An underlying theme in this paper is that of securing distributed networked systems. In the past era of Web1.0, a dual firewall with DMZ (De-Militarised Zone), and Proxy Server was all that was necessary to secure your main servers, intranet, e-mail and documentation. Now in this new era of Web2.0, the secure perimeter is less well defined as well all carry a range of gadgets – 3G Mobile phones, iPod, Memory Sticks, Laptops, and other Wi-Fi, Bluetooth & Wireless Devices.

There are parallels with the historic position of Georgia in which the Caucasus provided a physical firewall against invasion from the North, whilst in the South, religious cave complexes such as Vardzia - ვარძია - were constructed in the 12thCentury to provide relatively secure life against invasion from the Southern Borders. In fact, this ancient Vardzia Architecture still provides a useful analogy since in the 21stC, instead of securing a 3D network of caves on a cliff-face, we are securing a highly complex multi-dimensional network of servers, databases, and end-user devices. Vardzia stands on the beautiful Kura River which flows through onward through Georgia to the capital Tbilisi, and then to Rustavi, close to another even older 6th Century cave complex of Davit Gareja. So now we're securing electronic caves (servers), full of valuable information resources, and I'll take the liberty of referring to the proposed programme to develop & fully secure "Real-Time" Electronic Georgia , e-GE - as Project Vardzia! A bridge between the 12thC and our current 21stC!

During my work with the Georgian Parliament last year, it quickly became clear that historically, there had been minimal investment in the IT infrastructure, particularly with regards to the security support, data back-up, duplication, and adherence to international ISO Security standards. The tragic events of the last 6 months will have demonstrated the urgent requirement for significant investment in both the Government & Enterprise IT & Security Infrastructure, since the current networks are extremely fragile, with minimal resilience to cyber attacks or other disasters.

Security References

- ISO/IEC – 27001/27002 Guidelines www.iso.org - 2005
- ISF - Information Security Forum: Security Guidelines – 2007
- OECD Security Guidelines for Information Systems & Networks
- US Congress – Security in the Information Age - 2002
- UK Government – Security Architecture - Version4.0
- German Government – IT Security Guidelines - 2004
- EIF – European Interoperability Framework – 2004
- ASIS International Guidelines for BCP/DPR - 2005

Profile – Dr David E Probert

- ***Computer Integrated Telephony (CIT)*** – Established and led British Telecom's £25M EIGER Project during the mid-1980s' to integrate computers with telephone switches (PABX's). This resulted in the successful development and launch of CIT software applications for telesales & telemarketing operations in a worldwide marketplace.
- ***Blueprint for Business Communities*** – Visionary Programme for Digital Equipment Corporation during late-1980's that included the creation of the "knowledge lens" and "community networks". The Blueprint provided the strategic framework for Digital's Value-Added Networks Business that secured significant contracts for enterprise networks.
- ***European Internet Business Group (EIBG)*** – Established and led Digital Equipment Corporation's European Internet Group for 5 years, from 1994 to 1999. Projects included support for the national Internet infrastructure for countries across EMEA as well as major enterprise, government & educational Intranet deployments. Dr David Probert was a sponsoring member of the European Board for Academic & Research Networking (EARN/TERENA) for 7 years (1991 ➔1998)
- ***Supersonic Car (ThrustSSC)*** – Worked with Richard Noble OBE, and the Mach One Club to set up and manage the 1st Multi-Media and e-Commerce Web-Site for the World's 1st Supersonic Car – ThrustSSC – for the World Speed Record.
- ***Secure Wireless Networking*** – Business Director & VP for Madge Networks to establish a portfolio of innovative secure wireless Wi-Fi IEEE802.11 networking products with technology partners from both UK and Taiwan.
- ***Networked Enterprise Security*** - Appointed as the New Products Director (CTO) to the Management Team of the Blick Group plc with overall responsibility for 55 professional engineers & a diverse portfolio of hi-tech security products.
- ***Republic of Georgia*** – Senior Security Adviser – Appointed by the European Union to investigate and then to make recommendations on *all* aspects of IT security, physical security and BCP/DR relating to the Georgian Parliament.
- *Dr David E. Probert is a Fellow of the Royal Statistical Society. He has a 1st Class Honours Degree in Mathematics (Bristol University) & PhD from Cambridge University in Self-Organising Systems (Evolution of Stochastic Automata) , and his full professional biography is featured in the Marquis International Directory of Who's Who in the World – 2007 / 2009 Editions.*