

IT GlobalSecure, Inc.  
PROPRIETARY DATA ENCLOSED



Email: [info@ITGlobalSecure.com](mailto:info@ITGlobalSecure.com) Web: <http://www.ITGlobalSecure.com/>

## Security Assessment Proposal

For East Coast Credit Union

This is a Sample Proposal for Assessment Services for a Mid-Sized Business Entity.

East Cost Credit Union is a fictitious name.

**Prepared by: IT GlobalSecure Inc.**

1837 16th Street NW

Washington, D.C. 20009 USA

+1 . 202. 332. 5878 (tel) +1. 202. 478. 1743 (fax)

**July 6, 2001**

## Table of Contents

|  |    |
|--|----|
| INTRODUCTION .....   | 3  |
| RESPONSE TO ECCU REQUIREMENTS.....   | 4  |
| Scope .....  | 4  |
| How We Differ .....  | 4  |
| IT from a Business Perspective .....   | 5  |
| The Security Assessment Approach.....  | 7  |
| Step 1. Component Identification.....  | 7  |
| ECCU Specific Questions (for Step 1) .....   | 9  |
| Step 2. Business Process Identification.....                                       | 10 |
| Step 3. Resource Planning – Determining a Workable Business Model.....             | 11 |
| Step 4. Business Information Technology Security Assessment .....                  | 12 |
| Step 5. Security Engineering – Implementation and Remediation (Option).....        | 13 |
| Step 6. Business Information Technology Security Engineering Support (Option)..... | 13 |
| Pricing.....   | 15 |
| ABOUT THE COMPANY .....  | 15 |
| Contact Information.....   | 15 |
| Success Stories.....   | 17 |
| Clients.....   | 19 |
| Quality Approach.....  | 20 |
| Global IT Security Exchange.....   | 21 |
| REFERENCES .....   | 22 |
| SERVICES.....  | 23 |
| PRODUCTS .....   | 25 |
| RESUMES OF KEY PERSONNEL .....   | 27 |

## INTRODUCTION

IT GlobalSecure, Inc. is pleased to respond to East Coast Credit Union's (ECCU) request for security assessment and vulnerability services. This response recommends a course of action based on June phone conversations and a network diagram delivered June 20, 2001. Pricing information is contained in the final section of this response.

Security awareness and improvements continue long after initial assessments and upgrades. We will work with your management team to ensure that any steps taken to improve or enhance your IT security can be sustained by your IT staff over time. For this reason, we are fully committed to addressing important issues such as knowledge transfer between technical staff, or working with other contractors or in-house staff as part of a team-based project schedule. We can also assist you with identifying local staff to provide "hands-on" security support in conjunction with your local IT maintenance and operations staff. In so doing, we can – should you desire – become a valuable source for on-going independent review, testing, or other validation/auditing services.

The next section contains a detailed description of the approach recommended by IT GlobalSecure for proceeding with a security assessment for ECCU.

IT GlobalSecure is a systems integration firm with a specialty in providing secure computer and network solutions for business and government. We are a multi-disciplinary services company dedicated to helping our clients select, purchase, and implement robust cost-effective IT solutions. We are partnered with manufacturers of IT products and IT service providers. Our solutions span hardware and software for networks, enterprises, servers, desktop platforms, mobile platforms, and handheld devices.

Our solutions have supported the global trade, claims processing, telecommunications, and finance industries, numerous government agencies – all of which have demanding requirements for performance, feature expansion, privacy, distributed access, reliability, and –of course– security.

Given that our staff and work experience are not well known by ECCU, we have taken the opportunity to provide you with more information about IT GlobalSecure. This information is in the "About the Company" portion of this response. We hope it will be of use to you as you proceed with your selection of contractors. We would welcome an opportunity to work with ECCU and enhance its services in the financial sector.

## **RESPONSE TO ECCU REQUIREMENTS**

### **Scope**

Security surveys repeatedly report that most security incidents are caused by insiders (numbers ranging from 60 to 80 percent) and that the monetary damages are significant (often millions of dollars). The question should be – where are these vulnerabilities and what is driving the costs?

The purpose of a security assessment should be to identify these vulnerabilities to a company's information infrastructure as well as appropriate countermeasures and remediation steps. Often, however, security assessments deliver scathing indictments of company's IT departments practices without ever actually addressing the source of the loss – quantifying how it did (or could) occur, the potential for system or data compromise, the business loss (which can be in dollars, reputation, productivity, or continuity in operations), and how such losses can be prevented.

### **How We Differ**

We believe our security assessments provide better value to the business manager and the IT department. By understanding the business loss potential, pragmatic decisions can be made about “how to invest” in making security improvements or fixes.

In contrast, most of these assessments provide reports on poor passwords for operating systems, network configuration problems, and server configuration problems. The resulting report typically consists of lists of denial of service attacks or misuse of resources via broken passwords and the actions system and network administrators need to take to fix them. Some security assessments include penetration tests with comparable results – bad passwords, operating system patches, and network holes. Occasionally, these reports will provide information on misconfigured applications (mail servers, web servers, and occasionally database servers). While all of this information is useful and important, the question remains – is this where the losses come from?

IT GlobalSecure's motto “The Business of Security is Business”™ captures the essence of our IT security strategy for our customers. IT GlobalSecure uses its Business Information Technology Security Assessment methodology to help its customers identify where security vulnerabilities are, what is their business impact, and what should be done. Our Business Information Technology Security Engineering and Implementation solutions consist of more than simply selling products or services, but rather helping our customers to integrate IT security into their business operations – protecting current revenues and opening new opportunities.

IT GlobalSecure is uniquely positioned to provide security support for the full range of business IT security needs through our wide range of vendor products, access to numerous service providers, and unique ability to assess and secure custom, high-end enterprise and operations applications.

## **IT from a Business Perspective**

The complex network infrastructure of ECCU, as provided to us on June 25th, is shown in Figure 1. It is anticipated that ECCU employees spend their days writing, communicating, analyzing, building, buying, selling, and reporting with computers, laptops, cell phones, PDAs, servers, mainframes and special purpose devices.

In our discussion, it was mentioned that Reflections Software was used for communication with HP3000 hosts. We assume this was the Reflections for HP (with SOCKS proxy server support), but we would also seek clarification on what other terminal emulation or mainframe interfaces (interface software and connection protocols) would be in use. With this profusion of platforms, and adoption of enterprise software (most commonly used for messaging, project planning, billing, information sharing and reporting), the key corporate data and business processes have moved from file cabinets and locked up data centers onto every desktop in a company.

# HISD Wide Area Network

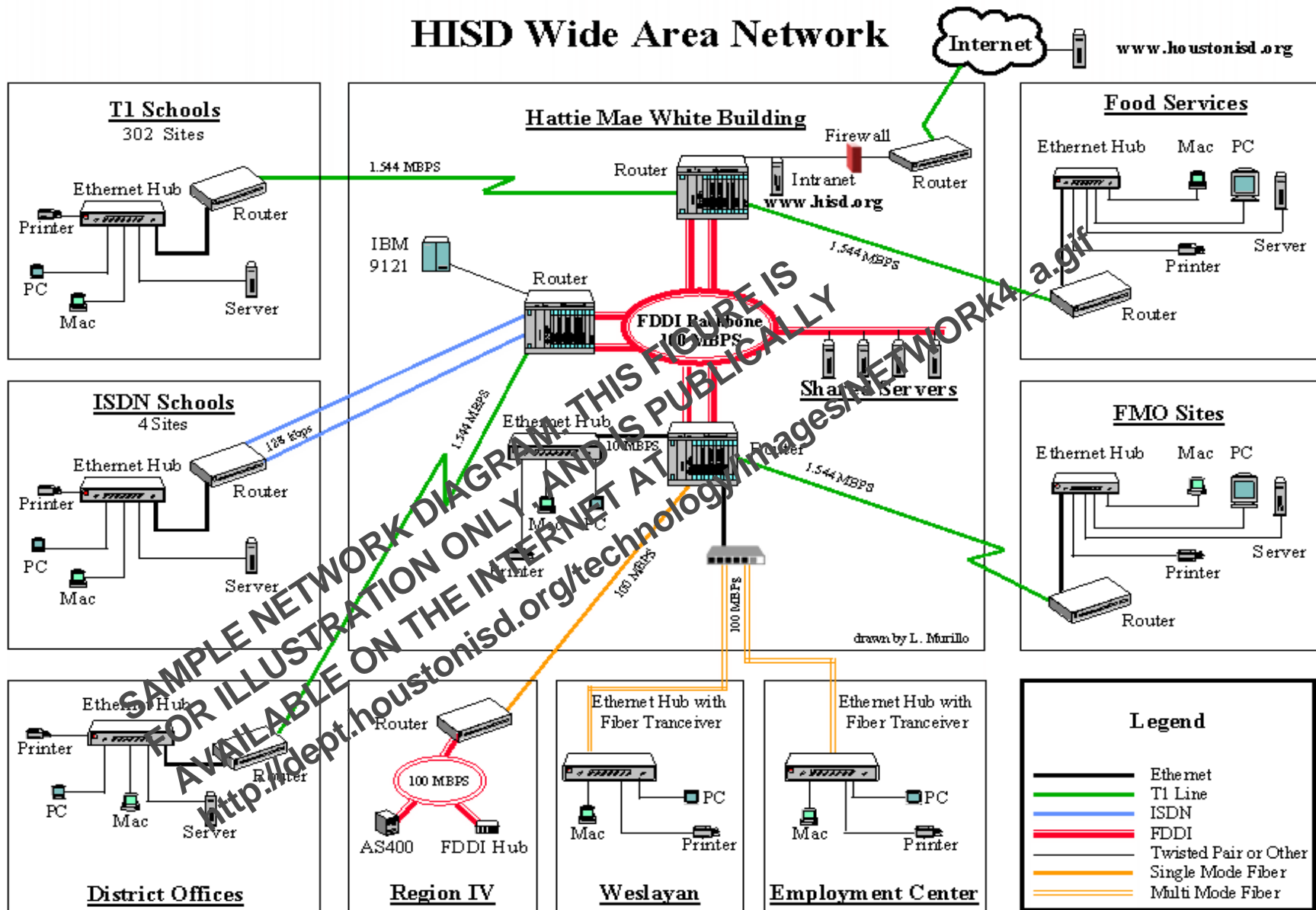


Figure 1. ECCU Network Diagram

## The Security Assessment Approach

Security assessment must be tied to the business value of the IT components. During the assessment, the vulnerabilities will be individually identified and evaluated. Just as companies have separate insurance coverage for fire vs. theft vs. liability, so a security assessment should keep separate track of Internet vandalism, denial of service, loss of business, and compromise of sensitive information. In order to carry out this assessment, the IT components of a business must be assessed in terms of their business function.

### Step 1. Component Identification

Step One of our response, is therefore, an identification of IT components to be considered within the scope of the assessment. This will be conducted during a visit to your central site or facility. We recommend that a “kick-off” meeting with senior management occur at this time. We have priced this effort assuming that your IT staff can provide most of this information, and that a full-fledged configuration audit with site survey at all facilities is not required.

The component list and supporting documentation, to be assembled by your staff prior to our arrival (as best as possible) and discussed during our visit, should include items as listed below. We recognize that not all information will have pre-existing documentation, and that IT GlobalSecure staff will assemble notes and pictures from discussions during our visit to the central facility. The quality of the assessment report is contingent upon receiving as much documentation as possible regarding items in the list below.

- a. **Systems & Network Components** – the hardware and software that forms the basic IT foundation. This includes platforms and operating systems.
  - o Computers (O/S, manufacturer, physical location, quantity, placement in LAN/WAN topology, access and authentication controls, policies and other administrative procedures)
    - Desktops
    - Servers
    - Mobile Platforms
    - Terminal Access Points
    - Mainframes
    - Dedicated Appliance Devices
  - o Physical Data Stores (Repositories of information containing information of importance to the business)
    - Databases
    - File Archives
    - Messaging Servers
    - Reporting/Logging Systems
    - Archival/Backup/Configuration Management Systems

## Other Media Storage Systems

### Web Servers

- Connectivity Devices (O/S, manufacturer, physical location, placement in LAN/WAN topology, supported protocols, permitted modes/ports; access methods; authentication techniques, administrative procedures)
  - Routers/Switches/Hubs
  - Gateways
  - Proxy Servers
  - VPN Gateways
  - RADIUS/TACACS/Other Remote Access Devices
  - Voice Systems/Modem Banks/PBX Devices
  - Communication Servers
  - Firewalls
  - Other Encryption Units
- LAN/WAN Specifications (To include maintenance and service procedures)
  - Physical Topology
  - Logical Topology
  - Network Management Tools/Techniques
  - Network Protocols/ Routing Protocols

b. **Infrastructure IT Services** – these are the basic, commodity IT applications that are shared across a company (mail, web servers, file servers, etc.). Most security assessments only review the security of Infrastructure IT Services and Systems and Network Components.

c. **IT Applications**

- **Desktop IT Applications** – these are the commercial, typically commodity, IT applications such as word processing, spreadsheets, etc.
- **Desktop Business Applications** – these are business specific desktop applications, typically commercial commodity applications, but that are inherently tied to business processes and whose data is critical to the day-to-day operation of a business - desktop accounting packages, contact management tools, etc.
- **Enterprise Business Applications** – these are backbone core business applications, typically found in larger enterprises. They are often medium to high-end commercial applications that require extensive tailoring and support to implement standard business processes such as Enterprise Resource Planning (ERP), human resource systems, procurement systems, billing, large scale accounting packages, etc.
- **Operations Applications** – these are applications, often custom, that implement core portions of a companies business activities and directly provide revenue. E-commerce and the Internet are making these applications much more common in

businesses. Embedded applications in factory systems would also qualify as operations applications.

### ECCU Specific Questions (for Step 1)

There are some questions that are of particular interest for ECCU components, given a preliminary review of the ECCU diagram. This diagram contained a mixture of high-level functional detail combined with network identification and component information, prompting the questions below:

**Note: These questions would be different for EVERY PROPOSAL, and tailored to the system architecture and unique concerns of each customer.**

#### Internet-Related

Please describe the firewall architecture in place for Internet access protection?

This diagram does not show a web server. Are you using a hosted external service?

#### Server(s)

What if any Demilitarized Zones (DMZs) are in use for application or database servers?

What, if any, multi-tiered security architectures are employed?

Is the mail server outside or inside the firewall?

What access control do you use to the HP 3000? How is this approach supported within the Reflections software, or outside of it? Are there other security tools on the HP3000 (please describe all access and authentication methods)?

Is there virus scanning in place on the mail server?

What commercial or custom applications exist? Are there legacy banking applications? How are they documented? Please define all database applications in use. How does one gain access? Where do users reside?

#### Other Gateways/ Connectivity Issues

What information comes over the [NAME DELETED] Home Banking network, and how is that protected? Likewise, how is information protected for the [CREDIT CARD 1] and [CREDIT CARD 2] Gateways?

There is a [NAME DELIVERED] LAN shown relative to the HP3000; is the HP3000 being timeshared? Is there a dedicated use by [OTHER COMPANY]? Are there more complex organizational relationships between ECCU and [OTHER COMPANY] (or other credit unions)?

Please describe the interfaces with other regional offices and branches. What aspects are shared (infrastructure, data, voice, staff)? What "Service Center" aspects do you provide on their behalf?

What dial-up modems exist? What secondary connections for the routers exist as a backup?

Is the frame relay backbone commercially provisioned, or do you control and own the frame relay devices? Is this a public frame relay cloud, or is this a VPN Frame Relay cloud (or some combination thereof).

How do your electronic banking (hosted) applications connect to your back-end applications?

You show the closed branch at the [THIRD COMPANY]. Is the branch closed and the connection still alive?

Do you support a remote or mobile workforce for employees or administrators, either through the Internet or through modems? If so, what is the procedure for connection and gaining access?

#### Platforms

Are the devices that hook-up to the network special purpose terminals or PCs or both?

Do any of the devices that connect to the network also have modems?

#### Voice

What is the voice infrastructure – is ECCU concerned about toll fraud? What management systems or monitoring exists on the PBX?

Do you multiplex your voice and data on the frame relay cloud?

#### Other Issues

This diagram (Figure 1) appears to be a depiction of an operational network. Is there a separate corporate IT network? Is there a separate diagram? If not, where do the “ordinary” office systems fit into this infrastructure?

Please provide existing administrative policy and policy documents.

Do administrators have access to all the machines (common passwords and password lists). A similar question exists for routers.

What procedures exist for adding or removing users from the business and essential business applications? How do you revoke access and privileges when people leave or change positions?

What other intrusion detection systems, commercial tools for sniffing the network, tamper detection tools, and network management tools are in use?

Are there specific legal, insurance, or management-directed requirements for protecting your IT that you are supposed to formally meet?

We would like to receive an organizational chart, and where IT management relates to the overall management hierarchy

### Step 2. Business Process Identification

A security assessment that is not done in the context of the business will not provide meaningful information for business executives to allocate or reallocate resources to address security

problems. To assist in resource allocation – whether of people or money – a security questionnaire will be performed with ECCU staff to answer the questions shown below. This, in turn, will allow the IT components to be mapped to business processes which make use of them, and to determine which business processes – if compromised – pose greatest risk to ECCU:

- Where is the business value in the IT infrastructure?
- What are the business consequences of an IT security vulnerability?
- What are the available immediate remedies?
- What is the lifecycle cost of the remedies?
- What is the expected cost of an incident?

### Step 3. Resource Planning – Determining a Workable Business Model

Security expertise is a scarce commodity and is often not necessary or supportably for a company to meet its security needs. IT GlobalSecure will work with ECCU to determine the appropriate model for Business IT security. As part of this effort, IT GlobalSecure will require information on the existing ECCU workforce (staff skills and quantity), and outside resources (in use or planned).

- **In House Expertise** – by maintaining security expertise completely within the business, a company has complete control over access to vulnerability information. This requires a substantial investment in acquiring and maintaining expertise as well as careful integration of security into the management hierarchy to ensure independence of operations and IT development.
- **Regular Outside Assessments** – regular outside review of a company’s security status to complement internal security resources allows an independent view. Just as with financial audits, companies must develop a close and enduring relationship with their auditors to ensure that the assessment accurately reflects an understanding of the company’s security requirements. The largest risk for this approach is that a company may change its business and IT strategy quickly and the outside assessment may get dangerously out of step with the company.
- **Consulting** – this allows companies to bring in specialty skills on a short term basis to address specific security needs. Identifying quality security consultants is always a challenge and, as with all consultants, a company must provide this outsider with extensive business information and manage the deliverables and knowledge transfer portions of the engagement closely.
- **Contracted Security Services** – critical security services can be “contracted in” so that the delivered solution is owned and controlled by the company. This maintains control of critical business assets by the company while allowing outside experts to carry out the development and integration with the remainder of the corporate infrastructure. A company may even consider using an outside contractor to operate the resulting solution. The risk to a company is that the relationship is likely to become long term and will be

difficult to transition in-house or to another contractor. This type of solution is typically applicable for Operations Applications, as part of support for Enterprise Business Applications, or during the development phases of establishing security for Infrastructure IT Services and Systems and Network Components.

- **Outsourced Security Services** – some aspects of security, such as basic firewall and intrusion detection, can be outsourced. Businesses must consider carefully the service level agreements and reliability and stability of the provider. Companies must also be aware that outsourcing security services typically do not address business specific security requirements and that outsourcing specific security services does not outsource security requirements.

IT GlobalSecure works with our customers to identify the proper model for IT security within a company. Our commitment to vendor neutral product and service solutions will ensure that we develop the best-value security approach for our clients.

#### Step 4. Business Information Technology Security Assessment

An IT GlobalSecure Business Information Technology Security (BITS) Assessment encompasses ECCU's operations as well as its computers. By looking at the objectives of the firm as well as its information technology resources, IT GlobalSecure can identify where the bottom line value lies with a ECCU's IT assets. IT GlobalSecure will work with IT and business managers to determine the firm's business security strategy. By combining deep expertise in security with a wide range of business experience, the IT GlobalSecure team delivers security solutions that deliver on the company's bottom line. The BITS assessment methodology will identify whether key corporate resources are held in a spreadsheet, database, or in a custom application – and concentrate security measures to protect those assets.

- The BITS assessment will determine what combination of outsourcing, internal expertise development, or other staffing strategy is needed to ensure the ongoing security of business operations.
- The BITS assessment will provide the financial trades necessary for senior corporate leaders to make intelligent decisions about the impact of security on their business.
- A BITS assessment delivers a Information Technology Security Business Strategy and a business case for change
- The BITS assessment contains the corresponding technical solution(s) with selection criteria, accompanying diagrams and tables with notations marking changes, upgrades, or points requiring remediation, and a proposed schedule for implementation.

This effort does not include port scans or other active testing being performed on site. IT GlobalSecure will review any logs or reports from such scans, but we believe that the on-going vulnerability tests (port scans, version or configuration testing, password checking tools) should be an on-going activity of the ECCU IT department.

The assessment report will be delivered in hardcopy volume and electronically. It will be followed by a wrap-up meeting with your senior management.

The pricing information within this proposal concludes with Step 4. Steps 5 and 6 are mentioned as steps that logically follow a BITS assessment, which IT GlobalSecure can support, in accordance with the resource business model discussed in Step 3.

#### Step 5. Security Engineering – Implementation and Remediation (Option)

Once the Information Technology Security Business strategy is in place as a result of the BITS Assessment, IT GlobalSecure and ECCU can move forward to design and implementation. IT GlobalSecure can take the role that best meets your requirements – from program management, engineering advice, and independent validation and verification to hands on implementation, integration, and development.

IT GlobalSecure's depth of security expertise allows us to do more than simply install commercial products. Our team can design and build an entirely custom solution, if necessary. With detailed knowledge of cryptography, security protocols, and system engineering, we have the skills to implement virtually any needed security solution.

Our extensive set of partners gives us a base for rapidly delivering off-the-shelf solutions, but we will buy, partner, or otherwise acquire the right IT security products and services that our clients need to implement their IT security strategy. We will also use third party outsourced security services or explore other innovative solutions – whatever is necessary for our clients.

#### Step 6. Business Information Technology Security Engineering Support (Option)

Secure operations are the essence of a successful IT security strategy. IT GlobalSecure can provide training and support to ensure that a business can be IT security self-sufficient. IT GlobalSecure can also provide auditing and retained security services for those clients that want or need ongoing external security