CYBERGATE

Whitepaper

Document’s Security

WE HAVE THE IN-HOUSE DEPTH AND BREATH OF
INFORMATION AND CYBER SECURIT

About Us

CyberGate Defense (CGD) is a solution provider for the full spectrum of Cyber Security Defenses including Identify, Protect, Detect, Respond and Recover. Our objective is to provide cyber security services that would improve the overarching cyber security posture of the nation especially how Government departments offer its IT services and improving the cyber maturity of the critical infrastructure industries.

We also provide an outline approach for developing a Cyber Security Strategy in collaboration with the Government by clearly presenting goals and vision and detailing how that vision can be achieved.

Our Vision

Building UAE’s cyber security resilience through effective use of technology, processes and the local people.

Our commitment

We believe that a cyber security provider can be about more than just the profits it makes, that by doing things the right way we can be a powerful force for good and safe environment where people and business communicate in cyber space with harmony.

By developing your strengths and enabling you to participate securely online, we'll help you to fulfil your security posture and getting the most from your IT investment.

What is Cyber Security?

According to the ITU, the United Nations specialized agency for information and communication technologies; Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, trainings, best practices, assurance and technologies that can be used to protect the cyber environment, organization and user’s assets.

Cyber Security Challenges

There is a growing concern of cyber-attacks on individuals, businesses, governments and the heavy industry which our modern lives depend on. There is a tangible risk of these systems being vulnerable and targeted. Governments are targeted by Advanced Persistent Threats (APT), by groups or nation state that are willing to employ time and resources to attack a specific system. For these kinds of attacks, there is a strong likelihood that a compromise will have national security implications.

Why we are different

Beyond our significant local presence, we have the in-house depth and breadth of information and cyber security expertise required to respond to the most technical information security challenges related to both Information and Operational Technology.

The principal reasons why CyberGate Defense is the right partner to assist you with any cyber security undertaking are:

Geographical:

Emirati Owned Company, headquartered in the UAE since 1987. Over the years Cyber Gate provided the UAE Government with high intelligent services and solutions. Today the scope of our services has been extended to include cyber security solutions aimed to strengthen the nation from cyber-attacks.

Sector Experience:

We currently operate in the Government sector providing value-added services and built solutions across the entire spectrum of cyber defense.

Security Expertise:

Our multidisciplinary team of information and cyber security professionals includes internationally renowned experts in the fields of protecting the critical infrastructure, industrial control systems, information systems and networks.

Document Risks

Cyber Security experts have reported an increase in cyber and network based attacks like denial of service and website defacement. In the effort of protection against such attacks, it is easy to oversee attacks on documents, as attacks against them are growing in sophistication. Documents can hold valuable and classified information, securing documents and their environments are equally important as network boundaries protection.
The Japan Network Security Association argues that failure to adequately protecting paper account for up to 50% of organizational information leakage. This suggests, organizations should invest more to protect documents.
Private memos, letters, diplomatic communications, strategic plans and roadmaps, are some of the many official documents found insecure in various organizations while computer hacking, data leaks, and other security breaches are on the rise worldwide. Many oblivious governmental departments continue to be trapped in the way they manage documents and then are suddenly hit by a security incident, concluding to data loss and data integrity issues.

Hard Copy Devices

Devices that process documents are referred to as Hard Copy Devices (HCD). They are capable of processing both paper-based documents and electronic documents. Faxes, photocopiers, scanners, and printers are some of the HCDs.

IEEE introduced a security standard with the aim to regulate HCD. Through this standard, HCD can be evaluated and certified under the common criteria evaluation process. *2600-2008 - IEEE Standard for Information Technology: Hardcopy Device and System Security.*

To date, end users rarely take advantage of the security features introduced by vendors to HCD and when it is applied by the end user, it is rarely configured correctly, resulting in poor data security.

HCD Challenges

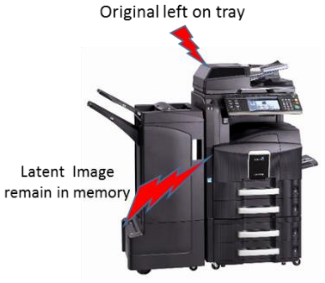
HCD are equipped with advanced computer based components such as processors, memory, communication ports; all of which are managed by an operating system or firmware which means they are capable of storing processed data, address book data and copies of documents. Without effective security measures, these devices can present a potential weakness to data security. For example, the latent image which is an invisible image produced by the exposure to light during faxing, copying, scanning and printing of documents remain in memory and can be retrieved and reconstructed.

Some of the challenges associated with specific devices are:

Fax

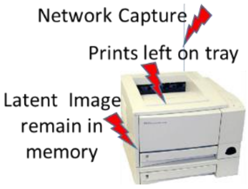
- Latent image of faxed documents remain in memory. If someone has access to the fax's HDD, a copy of the sent or received fax documents can be retrieved.
- Original document left unattended. It is easy for someone passing by to view or make copies of the document.
- Dialing attack from the phone line. Fax machines are equipped with modems and an attacker can maliciously access a remote fax and potentially leverage themselves onto the entire network through the HCD.

Photocopier



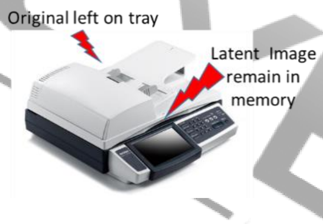
- Latent image of copied documents remain in memory. If someone has access to the copiers Hard Disk Drive (HDD), a digital copy of the copied document can be retrieved.
- Original document left unattended. It is easy for someone passing by to view or make copies of the document.

- **Printer**



- Latent image of printed documents remain in memory. If someone has access to the printer HDD, a copy of printed documents can be retrieved.
- Print data can be captured while in transit and then reconstructed.
- Original document left unattended. It is easy for someone passing by to view or make copies of the document.

- **Scanner**



- Latent image of scanned documents remain in memory. If someone has access to the scanners HDD, a copy of scanned documents can be retrieved.
- Scan data can be captured while in transit and reconstructed.
- Original document left unattended. It is easy for someone passing by to view or make copies of the document.

Document Management Server

Access Control
Theft of data

- Unauthorized access to documents.
- Capturing and stealing data

HCD Operating Systems

In addition to the common vulnerabilities detailed in the HCD challenges section, serious security holes have been found in there operating systems and firmware.

Different types of operating systems are used to operate different HCDs, some are cut down versions of popular operating systems such as UNIX, Windows and Window Embedded, and others make use of full versions. In both cases, HCD operating systems cannot be easily updated in the same way as conventional computer operating systems. Implementation of security patches on HCD operating systems are usually highly complex procedures produced by vendors.

The lack of updates is an obvious issue but the real danger lies when a modified operating system or firmware has been installed on a target HCD, thus allowing the attacker full control of the device and potentially leveraging access to the entire network.

A recent research has proved that a processed document such as print can be sent via the printers email subsystem to a desired email address. Furthermore, these devices normally are protected with a default password which anyone can find on the internet.

Optimize state of security

Information can be an invaluable asset, especially to government organisations. Since much information is held on paper and electronic documents, it is vital that these information assets are protected.

We appreciate that every government department is different, and hence developing and implementing a solution that is specific to that environment is important to protect documents from threats and enable organisations to share information quickly and flexibly.

HCD Security Solution

EGCD HCD Security service adds value to your organisation by protecting your sensitive information.

Our consultants will perform a systematic audits of your HCD security risks, by understanding the threats and vulnerabilities to your information assets. HCD Security audit will allow our consultants to analyse and optimise the state of security in your document management system.

The end result is an optimised document infrastructure harmonised for your work environment and security needs.

Consultancy service

We provide recommendations to ensure there is no danger of information falling into the wrong hands. A full data review service will ensure that data is permanently removed from any area of devices where information can be stored. With our document security consultancy service, your business is equipped with a reassuring combination of confidence and confidentiality.

CG Approach

We focus on protecting document flow. We can help you enhance information flow of paper-based and electronic documents at each stage of their lifecycle from creation through to distribution and deletion. We create a document management environment where only the right people have access to the information they need and develop an information management strategy to ensure long lasting protection.

We start by creating a comprehensive inventory of all HCD, details include but not limited to:

- Make
- Model
- Firmware level
- Applied security configurations (Data overwrite, HDD encryption, removable media, network ports, protocols, digital certificates and their strength and location),
- Access control information
- Auditing capabilities
- Remote configurations

Each HCD will be assessed from a security standpoint taking into consideration device features, current configurations, associated risks and type of documents processed on the device.

We will also provide a change management program to help smooth the transition of process changes and provide end user training.

CG Recommendations

Gathered from experience our recommendations will be one of the following:

A device that has some security capabilities but requires either all or some of the following:

- System updates (hardware and software)
- Implementation of additional security options such as data overwrite module, HDD encryption, removable media, network ports, protocols and digital certificates
- Configuration of built in security features.

A device that does not have security capabilities, we recommend replacing it with one that is fit-for-purpose. For example, a fax machine that does not support G3 technology and processes confidential documents should be replaced by a model that supports G3 technology. G3 fax capable machines do not accept standard modem commands which can be used by anyone who has a modem and knows the fax number.

A photocopier, printer or fax machine that does not support HDD encryption, data overwrite, or make use of digital signatures for demonstrating authenticity and integrity, should be replaced with a model that does support the required protective measure.

We will risk assess the Work environment, and based on the results, we may propose a new architecture. For example, if there is a risk of data being intercepted during transit and requirements dictate an end to end encryption solution, then a new architecture will be proposed as a suitable solution.

Our work environment assessments also examine how documents flow and are processed. Locked print maybe required to mitigate documents from being left unattended.

We will conduct a detailed analysis of the backend systems and evaluate its security capabilities and current settings. Any tactical security shortfalls will be highlighted and a best practice approach will be recommended and applied.

Document storage for both electronic and paper-based will be analyzed and any risks will be highlighted.

As a defense-in-depth approach, especially for highly classified documents, a PKI environment design maybe necessary, which uses digital signatures to provide document confidentiality and integrity. This technology of using digital signatures for document security is currently used by the US army.

EGCD will recommend the development of a document classification system, if it is deemed that the classification system is not fit-for-purpose. We can build a document classification system similar to the one used by the UK Government.

Value to the Business

- Protect the confidentiality and integrity of classified data.
- Prevent documents from being leaked.
- Protects organizations from security breaches, heavy fines, loss of revenue and negative reputation.
- Increase the confidence of your organizations security levels.
- Provides accountability and awareness of where your company's confidential data is stored, where it is being sent and who is accessing it.
- Protection of classified data against theft and accidental disclosure.

OUR SECURITY INTELLIGENCE SERVICES INCLUDES

- 24 x 7 x 365 security monitoring and analysis.
- Detect & mitigate against any reconnaissance process, credential theft, and lateral movement.
- User Behavior Analytica
- Incident management.
- Platform management.
- Custom data source integration and custom parser development.
- Vulnerability Management.
- Profiling of security controls.
- ADSIC or FEDNet Reporting.

DISCLAIMER

THIS DOCUMENT CONTAINS INFORMATION THAT IS PROPRIETARY TO CYBER GATE DEFENSE LLC. NO PART OF THIS PREREQUISITE MAY BE DUPLICATED OR USED FOR TECHNICAL OR COMMERCIAL PURPOSES WITHOUT THE PRIOR CONSENT OF CYBER GATE DEFENSE LLC.

TELEPHONE & FAX

+971 (0) 2 6655 855
+971 (0) 2 6712 211

ADDRESS

Al Bostan Tower (Office 103), Abu Dhabi,
UAE. PO BOX 43123

WEB

soc@cybergate.tech
www.cybergate.tech