SHARP®

Checklist to Mitigate Threats at the MFP

Today's headlines are filled with news of cyber-attacks, designed to leverage any vulnerability, whether they be human or technical. Today's intelligent MFPs and printers have evolved to touch various types of business communications, network and data storage services. Failing to protect MFPs and printers may result in serious damage to a company. The following checklist is designed to help achieve optimum security around your Sharp MFP:

Checklist to ensure optimal threat mitigation at the MFP:

- ✓ **Access Control & Password Management**
  - ▸ Implement secure user access control (Active Directory® or LDAP user authentication).
  - ▸ Ensure that users are assigned to properly configured authority groups.
  - ▸ Disable unused device functions.
  - ▸ Limit users who have administrator's rights.
  - ▸ Apply more complex administrator password rules.
- ✓ **Network & Communication**
  - ▸ Close unused ports and disable unneeded network services and protocols.
  - ▸ Use IP and MAC address filtering to limit MFP access to only necessary PCs.
  - ▸ Enable the TLS protocol to secure all communications.
  - ▸ Enable S/MIME, POP3 and SMTP authentication if possible.
  - ▸ Change the MFP's SNMP community name from its default "public."
  - ▸ Do not "publish" an MFP's IP address outside your organization's firewall.
  - ▸ Ensure Wifi and mobile security are properly configured.
- ✓ **Data Encryption & Overwrite**
  - ▸ Install a Data Security Kit (DSK) or configure built-in data security features for data protection (in transition and at rest).
- ✓ **Perform Periodic Audits**
  - ▸ Periodically review job and audit logs for suspicious activity – import syslog/audit logs to IT's core monitoring systems.

Checklist to Mitigate Threats at the MFP

Threat Mitigation

Corporations and organizations are under constant threats that put sensitive information and business continuity at risk. Information security can be compromised through ignorance and lack of training, or through malicious actions. In addition, adoption of new technology such as mobile and cloud, extends security challenges although they are essentials to keep up the speed of business communications.

Threat Types

Insider Security Breach

- Wrongful distribution or viewing of confidential information
- Improper routing of sensitive information
- Unauthorized access to data stored on the MFPs, folders and other services
- Lost laptops and mobile devices

Cyber Attacks

- Email containing malware and bots
- Email Phishing DDoS attacks
- Password hacks
- Malware and ransomware by attacking network and system vulnerability

New Risks – Third Platform

Mobile Adoption

- Data and network security vulnerability through BYOD
- Mobile OS vulnerability
- Malicious apps
- Infect mobile devices for monetization
- Misplaced mobile devices

Cloud Services

- Uncontrolled use of cloud services
- Business continuity and vulnerability challenges
- DoS attacks
- Cloud service hijack for ransom

Business Impact

- Loss of productivity
- Large fines due to regulatory non-compliance
- Loss of access to data and network
- Loss of competitiveness due to stolen information
- Lawsuits
- Loss of business continuity

Sharp Security Suite

Sharp continues to help keep our data and network safe through the **Sharp Security Suite,** which consist of a mix of MFP functionality complemented by software services:

- Standard MFP Security Features
- Data Security Kit (DSK) Features
- Print Driver
- Sharp Remote Device Manager (SRDM) and other Sharp Applications
- Sharp OSA® Applications

SHARP®

SHARP ELECTRONICS CORPORATION
100 Paragon Drive, Montvale, NJ 07645
1-800-BE-SHARP • www.sharpusa.com