XLN SYSTEMS

Shadow IT Group

# Cyber Protection & Defense
for
# Small & Medium Business

**Adhering to the Ohio Data Protection Act of 2018**

Goal:

To strengthen cyber security for your business &
to achieve a legal "affirmative defense" in a potential tort case against your business.

Process:

Become cyber compliant by implementing a recognized Industry Security Standard
that best relates to the size, nature and complexity of your business.

Have XLN SYSTEMS perform a Cyber Security Review of your business.
This will result in a report detailing your cyber defenses weaknesses, strengths and needs.

Based upon the type of security defense pinpointed for remedy,
XLN SYSTEMS and Shadow IT Group
will bring any cyber deficiency into compliance.

Costs:

Cyber Security Review costs
are based upon the number of employees your business has:

| | |
|---|---|
| 10 employees or less | $545 |
| Up to 25 employees | $1,275 |
| Up to 40 employees | $1,875 |
| Up to 70 employees | $2,895 |
| Up to 100 employees | $3,495 |

Follow up Cyber Security consulting ranges from
$95 to $145 per consulting hour

## Follow-up services by XLN SYSTEMS

**Secure & Configure Wired Network Switch –** Set-up and configure firewall access and MAC security rule-sets for all wired devices. If necessary, additional network hardware installation can also be provided.

**Secure & Configure Wireless Network –** Remove and change any SSID's and passwords that are automatically configured by the device (which can be looked up online), segregate production networks from guest accessible networks which ensures a much greater level of data security**.**

**Classroom instruction on Cyber Security to employees –** Instruct employees on cyber awareness including, but not limited to, phishing attacks, strong passwords, email attachments and ransomware.

**Writing and/or updating Employee Manuals –** Assist HR and management on official written instruction to employees as it pertains to Cyber Security and Physical Security.

**Writing and/or updating your Cyber Response and Incident Plan –** Assist management with creating or modifying this strategic and essential plan. Included in this plan are details to execute if a ransomware attack has taken place.

**Disaster Recovery Planning and Implementation –** Assist management with creating or modifying this strategic and essential plan as it relates to business recovery and business resumption in case of an unforeseen emergency.

**PC cyber checklist –** Ensure that antivirus, antimalware, and software firewalls are enabled, scan for any malicious software signatures or keyloggers, and verify that all software is up to date**.**

## Follow-up services by Shadow IT Group

**Penetration Testing** - Performing an authorized attack on company to determine strength of cyber defenses to withstand cyber attacks both internal and external.

**Vulnerability Assessment** - Scan of company assets to determine risk exposure due to outdated software and firmware that expose company to vulnerabilities that can be used to breach company

**Mobile Device Management** - Management of devices that have access to company data by ensuring they adhere to the policies set forth by the business.

**Host/Network Intrusion Detection / Prevention Systems** - Install and Managed intrusion services to detect anomalies and security related events within company network

**Web Content Filtering** - Employing filtering in your business to monitor and ensure employees are able to access sites allowed to perform their job duties as well as restrict access to sites prohibited by the company and/or prevent access to sites determined to be malicious.

**DLP and IRM** - Data Leak Protection and Information Rights Management ensures access to sensitive information is controlled and audited.

**Data Forensics** - Forensic investigation & E-Discovery of data and events for legal and criminal matters.