TurnKey Solutions
We make technology work for you!

Cyber Security

Essential Resources Guide

2023

Critical Starting Resources Every Business Leader Needs to Prevent Unnecessary Cyber Security Disasters

Foreward:

Why Did We Create This Guide?

Turn Key Solutions is a service organization.   We believe it is imperative that we focus our, and our clients' attention and efforts' on preparing for success in the event of the inevitable business destroying forces ravaging our community, our country, and our world.

From our home towns here in the Gulf South of the United States we're all very familiar with what hurricanes can do to a business and a community.

What we've discovered in the last 24+ years of protecting our clients from cyber criminals is that the destruction caused by a cyber-attack event can be worse than a hurricane.   Unlike a hurricane, though, cyber-attacks occur with little "direct" warning.

What I mean by "direct" warning is that there's no mass-alert early warning system quite like a TV channel (yet) that has 24x7 coverage telling us when a specific part of the country will get hit by a cyber-attack.   These attacks are occurring everywhere, non-stop, and with little preference for industry, size of company, or location.

Turn Key Solutions believes that it is imperative that you prepare yourself and your organization for the onslaught of attacks that appear to only be getting more frequent, more devastating to their victims, and more random in their attack patterns.

As your partner in this, we look forward to being there with you every step of the way, but some of the most important steps in preparation need to be directly influenced by you, the business owner, IT director, or manager.

To that end, we've prepared this ***short list*** of essential documents, guides, policies, and procedures that we believe to be extremely helpful if not essential in every business' preparation for the inevitable attack.

We hope you will find it useful, and if you need help working through these resources for your business, or if you would like us to work more closely with you in their implementation, please reach out to us any time.

-Henry Overton, President and Co-Founder,
Turn Key Solutions, LLC

FIRST: Protect Yourself

Cybercriminals are attacking business leaders more often, and more effectively, every day. They want your identity, your privileges, and your authority, so that they can steal your resources and those of your company, your employees, and your clients.

This is why we have prepared this guide: to equip you, as a leader in your company, to keep yourself secure.   In doing so, you will be protecting your company, your customers, and your community.

1: Know how to recognize a phish

3 Types of Phishing:

1. “Regular” phishing casts a wide net and is easier to detect.
2. Spear Phishing is focused, personalized, and harder to detect
3. Executive Whaling is highly targeted, using multiple attack fronts, using detailed knowledge of the target, and is often very hard to recognize.

Protect yourself by

1. Slowing down & examining all requests closely *(contact us for help with detailed analysis!*
2. Never call the phone numbers in request emails you receive

2: How to protect your passwords

Start with:

1. Do not **reuse passwords**
2. Do not **use patterns**
3. Avoid **insecure password storage, like** Outlook, Word Documents or Excel Files
4. Get a password manager program, secure it with MFA.
5. Enable Multifactor Authentication (MFA) on everything possible

3: Keeping your Microsoft 365 account safe

1. Do not log onto M365 from non-work computers or public networks
2. Do not be a “global admin” with your daily use account
3. Know your M365 “Security Score” number and make a plan to improve it

FIRST: Protect Yourself (cont'd)

4: Avoiding **smishing**

Don't respond to texts or open links!
Never share sensitive information, especially by text
Numbers can be spoofed – even friends & family!

5: Avoiding multifactor authentication bypass

Never approve an **unexpected push notification**
Do not give your **MFA codes** to anyone

6: Protecting personal information

Encrypt your drives
Store sensitive information in encrypted vaults, only unlock when needed

7: Knowing if you've **been hacked**

5 Simple Signs you've been hacked:

1. Your password gets **randomly reset**
2. Your **email signature** gets updated
3. New phone number, business name, or title
4. You start getting **TONS of spam**
5. Your computer starts getting tons of **popup messages**
6. You notice **emails you didn't send** in your sent items

UP NEXT: Protect Your Company

SECOND: Protect Your Company

No Security Stack Is One-Size-Fits-All

BUT all companies fit into one of these three categories: Basic Needs, Security Conscious, or Compliance Driven. Use the following model to find yourself and build out your security stack to fit your company's unique wants and needs.

HUMAN LAYER 6

Prevent

Basic Needs	Security Conscious	Compliance Driven	
◐	●	●	User Account 2FA
○	◐	●	Change Management
○	◐	●	Least Privilege
○	◐	●	Ops Training
○	◐	◐	Policy Mgmt Service
○	◐	●	Password Policy
○	◐	◐	Password Vault
○	◐	●	Enforced Password Change / Complexity
◐	●	●	Phishing Training
◐	●	●	Security Training
○	◐	●	System Use Warning
○	◐	◐	Last Login Notification

Guard

Basic Needs	Security Conscious	Compliance Driven	
○	◐	◐	Phone Recording
○	◐	●	Data Loss Protection
○	◐	◐	Email Encryption
●	●	●	Admin Account 2FA

Detect

Basic Needs	Security Conscious	Compliance Driven	
○	◐	●	3rd Party Audit
○	◐	◐	Dark Web Monitoring
○	◐	●	IT Compliance (Audit)
○	◐	●	Change Mgmt
○	●	●	Vulnerability Analysis
○	◐	●	Risk Analysis
○	◐	◐	User Activity Monitoring
○	◐	◐	Penetration Testing

Mitigate

Basic Needs	Security Conscious	Compliance Driven	
○	●	●	Breach Response Procedure

PERIMETER LAYER 5

Prevent

Basic Needs	Security Conscious	Compliance Driven	
●	●	●	Anti-spam
○	◐	●	DMZ
●	●	●	Firewall Patching
●	●	●	Firewall - Filtering
◐	●	●	Firewall - IPS
●	●	●	Firewall - Stateful

Guard

Basic Needs	Security Conscious	Compliance Driven	
◐	●	●	Firewall - Antivirus
○	◐	●	Firewall - DLP
○	◐	◐	Internet Fail Over
○	◐	◐	Video Surveillance
◐	●	●	VPN

Detect

Basic Needs	Security Conscious	Compliance Driven	
◐	●	●	Firewall - IDS
○	◐	●	Firewall - Log Collection

APPLICATION LAYER 2

Prevent

Basic Needs	Security Conscious	Compliance Driven	
◐	◐	◐	Line of Business Software Mgmt
●	●	●	Patch Mgmt
●	●	●	Server Maintenance
○	◐	◐	Application Whitelist

Guard

Basic Needs	Security Conscious	Compliance Driven	
●	●	●	Server Monitoring

Detect

Basic Needs	Security Conscious	Compliance Driven	
○	◐	●	App Monitoring
○	◐	◐	Honey Pots

Mitigate

Basic Needs	Security Conscious	Compliance Driven	
○	◐	◐	Compute Redundancy
○	◐	●	HyperVisor Maintenance

NETWORK LAYER 4

Prevent

Basic Needs	Security Conscious	Compliance Driven	
○	◐	◐	DNS Sanitation
○	◐	●	Network Segmentation
◐	●	●	Router Patching
◐	●	●	Switch Patching
●	●	●	Switch Standard
○	◐	◐	Wireless RADIUS Authentication
●	●	●	Wireless Standard

Detect

Basic Needs	Security Conscious	Compliance Driven	
◐	●	●	Log Collection
○	◐	●	Log Forensics
○	◐	●	Network Scanner
○	◐	◐	SIEM

Mitigate

Basic Needs	Security Conscious	Compliance Driven	
○	◐	◐	Security Operations Center

DATA LAYER 1

Prevent

Basic Needs	Security Conscious	Compliance Driven	
○	◐	●	Data Asset Mgmt
●	●	●	Data Destruction
○	◐	●	Email Legal Hold
○	●	●	Email Archiving
○	◐	●	Drive Encryption
○	◐	●	File Encryption
○	◐	●	Full Drive Encryption

Guard

Basic Needs	Security Conscious	Compliance Driven	
◐	◐	●	Backup - Archival
◐	◐	●	Backup - Near Line
●	●	●	Backup - Offline
◐	●	●	Backup - Offsite
○	◐	●	Collaboration Mgmt

Detect

Basic Needs	Security Conscious	Compliance Driven	
○	◐	●	Batch Monitoring

Mitigate

Basic Needs	Security Conscious	Compliance Driven	
○	●	●	Storage Redundancy

ENDPOINT LAYER 3

Prevent

Basic Needs	Security Conscious	Compliance Driven	
○	◐	◐	Application Whitelist
○	◐	◐	Ring Fencing
○	●	●	Stop Malicious Downloads
○	◐	◐	Browser Isolation
◐	●	●	Anti-Tampering
●	●	●	Disk Space Monitoring

Guard

Basic Needs	Security Conscious	Compliance Driven	
○	●	●	Heuristic Antivirus
●	●	●	Signature Antivirus
○	◐	●	USB Lockdown

Detect

Basic Needs	Security Conscious	Compliance Driven	
○	◐	●	Behavioral Monitoring
○	◐	●	Advanced Machine Learning

ASSETS

Protect vulnerable assets such as:

- CRM Database
- Document Mgmt System
- File System Data
- GL Software
- HR System
- Payroll Data
- ERP, HIS, EMR Solutions
- Remote Control
- RMM Tools
- Software Images

ARE YOUR LAYERS ACTUALLY WORKING?

FIND OUT AT:

turnkeysol.com/stack

LEGEND

○ **Low Perceived Value:** Valuable as they are, most companies will not perceive value from these items.

◐ **Recommended:** With education, most companies will invest in these these protections.

● **Mandatory: Table stakes items, if you skip these, you are being negligent.**

SECOND: Protect Your Company (cont'd)

Complete This Worksheet:

What are you doing to protect each layer of your business' assets & systems?

List the program, protection system and/or processes / policies you have in place for each item below.

1: Data..

....

....

2: Applications..

....

....

3. Endpoint Computers..

....

....

4. Network (including home if applicable)..

....

....

5. Perimeter..

....

....

6. Human..

....

....

7. Business Liability..

....

THIRD: Learn More

INVESTIGATE & USE THESE RESOURCES

LEGAL RESOURCES

- Link to the Cyber Incident Reporting for Critical Infrastructure Act of 2022: https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia

- Link to review of 2020 IOT CyberSecurity Improvement Act of 2020 https://www.gibsondunn.com/new-federal-law-for-iot-cybersecurity-requires-thedevelopment-of-standards-and-guidelines-throughout-2021/

- FBI Resource on when & how to report a cyber incident: https://www.fbi.gov/file-repository/cyber-incident-reporting-united-message-final.pdf/view

- National Conference of State Legislatures guide to local state Security Breach Notification Laws https://www.ncsl.org/research/telecommunications-and-information-technology/securitybreach-notification-laws.aspx

EDUCATIONAL RESOURCES

Follow our Facebook & other social media resources for 3-7 weekly updates, training resources & industry newsflashes, as well as helpful videos about a variety of security, business, and productivity subjects.

- https://www.facebook.com/TKSLA
- https://twitter.com/tksllc
- https://www.Linkedin.com/company/turnkey-solutions-llc

Krebbs on Security –
This is one of the industry's best-known analysts of cyber news & events.

https://krebsonsecurity.com/

Verizon Data Breach Report –

This report is compiled annually; is a great executive-level review of what trends their researchers have found and has become a mainstay in the industry for "where to go" for what's happening. If nothing else, read the first few pages for the executive summary.
https://enterprise.verizon.com/resources/reports/dbir/

THIRD: Learn More (Continued)

PICK A PLAN – YOUR CYBER SECURITY FRAMEWORK

We believe that it is essential that every organization first selects the framework, or underlying plan, that they will use as their outline for designing their security practice. Here are some common, very well-thought-out, and highly recommended frameworks.

18 CIS Controls – from the Center for Internet Security
This is our favorite plan for almost every organization, of any industry.   Though not always referred to a full "framework," these 18 CIS Controls outline the best time tested, proven effective "things to do" aka "Controls" that are useful and applicable in every other framework.   These recommendations "map to" and overlap with almost any compliance mandate or other framework.

https://www.cisecurity.org/controls/cis-controls-list/

NIST Cybersecurity Framework - https://www.nist.gov/cyberframework

HIPAA – HIPAA references the NIST framework, but here's great resources if you work in a HIPAA – regulated organization

https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html

ISO 27001 and ISO 27002 https://www.iso.org/isoiec-27001-information-security.html

GLBA, SOC2, FISMA, and GDPR are other examples of frameworks and cyber security mandates.

POLICY & PROCEDURE RESOURCES

RISK MANAGEMENT FRAMEWORK:
National Institute of Standards and Technology Risk Management Framework Guidance
https://csrc.nist.gov/projects/risk-management/about-rmf

CYBER INCIDENT RESPONSE PLAN: https://us-cert.cisa.gov/ncirp

SANS POLICY TEMPLATES
In collaboration with information security subject-matter experts and leaders who volunteered their security policy know-how and time, SANS has developed and posted here a set of security policy templates for your use.   We recommend you start with, at a minimum, these: Acceptable Use policy, Password creation & protection policy
https://www.sans.org/information-security-policy/

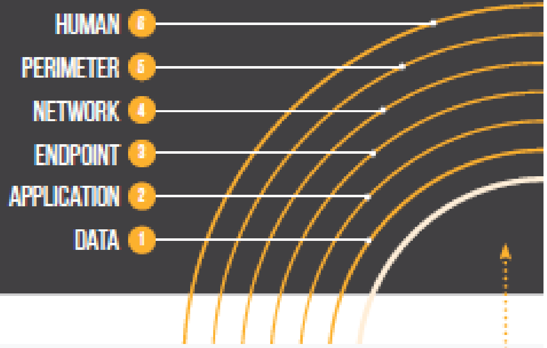
CENTER FOR INTERNET SECURITY Policy Template Guide:
https://www.cisecurity.org/wp-content/uploads/2020/07/NIST-CSF-Policy-Template-Guide-2020-0720-1.pdf

21-MINUTE CYBER STACK STRATEGY CONSULTATION

CAN YOUR CYBER STACK WITHSTAND HACKERS, THE PANDEMIC AND A RECESSION?

DOES IT ACTUALLY PROTECT YOU AND YOUR CLIENTS FROM RANSOMWARE ATTACKS?

We've analyzed over 100 security solutions in the last year.
We have the data on what works and what doesn't.
We will expose where your plan falls short.



WE'RE OFFERING YOU A

FREE 21-MINUTE CYBER STACK STRATEGY CONSULTATION

YOU'LL DISCOVER:

The inside track so you don't make the same mistakes others have made.

Up to the minute information on which tools are working in the field *(and which are a waste of money).*

Answers to your biggest security questions.

Peace of mind that you're not over-investing in one layer while completely missing something critical in another.

A plan to **secure your engineers** while they are working from home.

WE'LL DIVE INTO THE MAJOR COMPONENTS OF YOUR STACK

How confident are you about:

- Passwords Control and Management?
- Event Tracking?
- Network Security?
- Endpoint Protection?
- Antivirus?
- O365 Security?
- Firewall Security?
- Encryption?
- Documentation and Liability?
- Cyber Insurance?
- Simplifying Policy and Procedure Management?
- Developing/Growing Your Cybersecurity Stack?
- Backups Working?
- Data Continuity?
- Disaster Recovery Planning?

GET YOUR LIMITED TIME OFFER:

FREE 21-MINUTE NO OBLIGATION CYBERSECURITY STACK CONSULT

SPACES ARE LIMITED!

FOR MORE INFORMATION, VISIT turnkeysol.com/stack