Protect Yourself

Governments throughout the world are increasingly mandating institutions rigorously protect the PRIVACY of those individuals they serve. This is especially true for the DATA PROTECTION of personal data stored by these institutions. Failure to comply can lead to catastrophic economic and social repercussions.

If your organization is storing data about people, privacy should be a big deal to you

The Federal Government has developed a tool to assist in identifying and managing Privacy Risk. Created by NIST (National Institute of Standards and Technology), the program contains five (5) basic components to any secure framework. Taken directly from its website these are…

IDENTIFY	The Identify Function assists in developing an organizational understanding to managing cybersecurity risk to systems, people, assets, data, and capabilities. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.
PROTECT	The Protect Function outlines appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event.
DETECT	The Detect Function defines the appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events.
RESPOND	The Respond Function includes appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident.
RECOVER	The Recover Function identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident.

Important concepts include the following…

Data Protection is about securing data against unauthorized access. This is a TECHNICAL issue

Data Privacy is about authorized access — who has it and who defines it. This is a LEGAL issue

Both are unfailingly linked and need to be incorporated throughout any IT framework

To be secure AND compliant the entire process from data collection, its maintenance and its ultimate destruction needs to be impervious to threat

Triantan CCC is part of only 10% of all IT Service Providers that specialize in Compliancy and Risk Assessment, Implementation and Management.

So what can TCCC do for you?

TCCC provides organizations with a granular look into their technology environment through a comprehensive Security and Risk Assessment. Our certified engineers perform an on-site assessment of all existing hardware, software and network configurations. Upon completion you will be provided a documented inventory of your technology environment, results of an array of industry standard testing, and any recommendations to optimize and protect your environment now and in the future. The 52 items of the assessment follow the five NIST components…

Triantan CCC, LLC
"The Convergence Company"

Your Trusted, One-Stop Source for IT Compliancy, Privacy and Security Management

Triantan CCC, LLC
230 Spring Lake Drive
Itasca, Illinois 60143
877.282.9227
www.ccctechnologies.com

IDENTIFY	***Asset Management***	NIST CSF Identify Worksheet
		NIST Asset Inventory Worksheet
		NIST Application Inventory Worksheet
		NIST Full Detail Excel Export
	Business Environment	NIST CSF Identify Worksheet
		PCI Compliance Report
		HIPPA Compliance Report
		Cyber Insurance Report
		Other Compliance Report :
	Risk Assessment	NIST CSF Identify Worksheet
		NIST Risk Analysis
		Patch Assurance Report
		NIST External Vulnerability Scan
		Internal Vulnerability Scan
		NIST User Access Review Worksheet
	Risk Management Strategy	NIST CSF Identify Worksheet
	Supply Chain Management	NIST CSF Identify Worksheet
		Vendor Security Assessment Form
PROTECT	***ID Management Authentication and Access Control***	NIST CSF Protect Worksheet
		Remote Access
		BYOD/MOM Policy
	Security Awareness	NIST CSF Protect Worksheet
		Awareness Training Program
	Data Security	NIST CSF Protect Worksheet
		Data Classification Policy
		System Development Life Cycle
	Policies & Procedures	NIST CSF Protect Worksheet
		Acceptable Use Policy
		Change Control Managment
		Change Control Log
		Data Destruction Policy
DETECT	***Maintenance Procedures***	NIST CSF Protect Worksheet
		Workstation Patching, Maintenance, and AV Scan Policy
		Server Patching, Maintenance and AV Scan Policy
		Application Patching
		Network Infrastructure Patching
		3rd Party Networked Device Patch (UPS, Scanne rs, Printers, IOT)
	Detection Procedures	NIST CSF Detect Worksheet
	Internal Access Detection	Report from Customer System
	Anti-Virus/ End-Point Security	Report from Customer System
	SIEM for Network Devices or MSSP Services	Report from Customer System
	User Security Monitoring in Office365	Report from Customer System
	Dark Web Monitoring	Report from Customer System
RESPOND	***Respond Procedures***	NIST CSF Respond Worksheet
	Security Incident Policy	Security Incident Policy
	Security Incident Log	Security Incident Log
	Response Plan	Response Plan Template
RECOVER	***Recovery Procedures***	NIST CSF Recover Worksheet
	BC/DR Plan	BC/DR Plan