



Introduction to SensCy™

April 2023

SensCy Inc.

info@senscy.com

734.276-9891

455 E. Eisenhower Pkwy

Suite 300

Ann Arbor, MI 48108

www.senscy.com



SensCy Introduction

SensCy Leadership Team



Rick Snyder

Chief Executive Officer
PwC, Gateway, Avalon,
Ardesta, State of
Michigan



David Behen

Chief Client Success Officer
Washtenaw County, InfoReady,
State of Michigan, La-Z-Boy



Bhushan Kulkarni

Chief Operating Officer
GDI, InfoReady



Dave Kelly

Chief Technology Officer
Michigan State Police Cyber
Command, ibi, TIBCO



Raj Patel

Chief Growth Officer
KPMG, Plante Moran

Vision

To be the Trusted Guide for Sensible
Cybersecurity for small and medium
organizations

Mission

To improve our clients' cyberhealth by
providing a high value, easy to understand
solution through continuous personal
interactions, technology, unbiased
referrals, and education.



Recent Cyber Attacks



March 17 2023: Michigan-based Lansing Community College was compromised by a cyberattack on March 17, resulting in the closing the college for three days, national media coverage and investigation is ongoing.



Feb 1, 2023: Russian hackers take down at least 17 U.S. Health System Websites, including Michigan Medicine. Hackers have been targeting countries that support or send resources to Ukraine.



Nov 2022: Jackson & Hillsdale County schools closed for multiple days following a ransomware attack. Hope College in Holland, MI faces a \$5 million lawsuit by former student.



Feb 15, 2023: Grand Rapids, MI based equipment supplier of wood products detected a cyberattack and shut down their systems to investigate. As Feb 28th, their website says their systems are still offline.



Feb 8, 2023: Benefit fund administrator from Indiana experienced a ransomware attack in March 2022. TIC waited 6 months before they notified 187,341 fund participants that their names, addresses, social security numbers and protected health information was compromised from the cyberattack. Class Action Lawsuit was filed in Feb 2023. A fund participant & plaintiff from Michigan experienced credit card fraud with Best Buy gift card and had an unknown person ship an auto part to his address after the breach occurred.



TEIJIN AUTOMOTIVE TECHNOLOGIES

Feb 3, 2023: Reported ransomware attack on December 13, 2022. On February 3, 2023, the automotive parts supplier headquartered in Auburn Hills, MI revealed that cybercriminals stole current and former employee's PII data. On Feb 9th, a class action lawsuit was filed against Teijin for failing to exercise reasonable care in safeguarding employee's personal information.



City of WHITEHALL

Dec 2022: Ohio City sent out 37,000 notifications to people in 11 states alerting them that their personal information may have been compromised from ransomware attack. It took them 6 months to notify from date of breach.



Nov 2022: Class action lawsuit alleges Michigan prosthetics & orthotics manufacturer failed to adequately safeguard Protected Health Information (PHI) of 877,584 patients.



Nov 11, 2022: 2nd lawsuit filed against Troy, MI based bank, stemming from a data breach in Dec 2021 that was reported in June 2022. Data was compromised for 1.5 million customers. Earlier, in March 2021, the bank faced a breach from the hacking of Accellion, a file sharing technology third-party vendor. Accellion reached a \$8.1 million settlement for a class-action law suite.



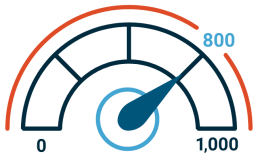
SensCy Subscription: Great Protection and Price



Cyber Advocate

A cyber professional that will be a trusted guide and will have regular checkpoints with you to ensure you are on track with your cyberhealth plan.

CYBERHEALTH EVALUATION



Generates your **SensCy Score™** like a credit score for your cyberhealth



CYBERHEALTH PLAN

A client customized plan to improve your cyberhealth score



CYBER TRAINING

Employee awareness & policy training help your employees become a first line of defense



EXTERNAL SCANS

Vulnerability and dark web scanning help keep you protected



INCIDENT RESPONSE PLAN

Help your team respond to an attack and minimize the impact



EXECUTIVE BRIEFING

Cyber briefings to your leadership team, key stakeholders or board members



CYBER POLICY LIBRARY

A policy library to ensure you are following best practices



PHISHING

Friendly phishing tests to keep your employees vigilant against phishing attacks



CYBER ALERTS

Proactive outreach for emerging threats – tailored to your systems



CYBER INSURANCE

Assist with properly completing cyber insurance forms



CLIENT DASHBOARD

Visibility into your cyberhealth & regular touchpoints to ensure your cyberhealth plan is on track

Monthly Subscription Pricing

\$750

1 – 20 active online users

\$1,000

21 – 100 active online users

\$1,500

101 – 250 active online users

(Contact us for pricing for over 250 active online users)

- Evangelize cybersecurity in your community
- Discuss with your IT team or MSP that SensCy complements them vs replacing them. We only provide dedicated cybersecurity expertise and tools.
- Sign up for a free no-obligation SensCy Score for your government organization.


SCHEDULE C
(Form 800)

Cybersecurity Best Practices for Tax Returns
visit to www.senscy.com for your trusted guide to sensible cybersecurity

2022

Caution: Protecting your tax return and documentation is protecting your identity and financial security

	YES	NO
<p>Social Security Number</p> <ol style="list-style-type: none"> 1. Are you monitoring your social security number on the dark web? 2. Are you monitoring your family (including children's) social security number on the dark web? 3. Have you put a credit freeze on your children's social security number so no one can open a line of credit in their name? 	<input type="checkbox"/>	<input type="checkbox"/>
<p>Passwords</p> <ol style="list-style-type: none"> 1. Do you use a strong password for IRS website? 2. Do you use a strong password for accessing your tax preparer software? 3. Did you change these passwords in the last 90 days? 4. Do you multi-factor authentication to access these sites? 	<input type="checkbox"/>	<input type="checkbox"/>
<p>Document Storage</p> <ol style="list-style-type: none"> 1. Do you store your prior tax returns and documentation in a secure location? (Storing them on your home computer is not a secure. Hackers can access your home computer when it is connected to the Internet. They can lock your data down and hold you for ransom. They can also steal your personal information.) 2. Do you store your tax returns and documentation in an encrypted hard drive that is disconnected from the Internet or a computer connect to the Internet when not in use? 3. Does your CPA store your tax documents in a secure portal? 4. Do you remove your tax returns from any online portals after the returns are filed? (Once the tax returns are filed, you should go and remove the tax returns and supporting documents from all on-line storage sites. This also applies when you provide tax returns to banks for loan applications.) 	<input type="checkbox"/>	<input type="checkbox"/>
<p>Access</p> <ol style="list-style-type: none"> 1. Do you restrict who can access your electronic or paper tax returns in your household? (This could be your spouse, it can be your children, the nanny, cleaning person, contractor, etc.) 2. Do you trust the staff at your CPA to handle your tax information securely? 	<input type="checkbox"/>	<input type="checkbox"/>
<p>Phishing</p> <ol style="list-style-type: none"> 1. Are you extra vigilant for phishing and smishing scams during the tax season? 2. Do you know what to look for in a phishing email? 3. Do you know that IRS will never call you at home, office or your mobile phone? 4. Do you know what to do, if you clicked a suspicious link in an email or text message? 	<input type="checkbox"/>	<input type="checkbox"/>
<p>Backup</p> <ol style="list-style-type: none"> 1. Do you have a secure backup storage to save your current and prior year tax returns? (Remember, there are federal and state retention requirements.) 	<input type="checkbox"/>	<input type="checkbox"/>
<p>Other</p> <ol style="list-style-type: none"> 1. Do you have a credit monitoring service? 2. Do you use free-public wi-fi while handling your tax data or using a computer that has your tax data? 3. Do you use a malware monitoring software on your computers? 	<input type="checkbox"/>	<input type="checkbox"/>

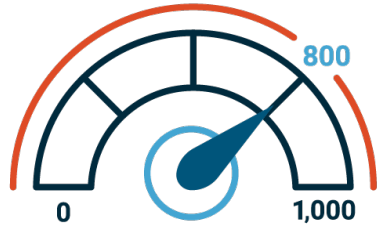


SENSCY™
Your Trusted Guide to Sensible Cyber



SensCy Score: Find out your Cyberhealth

Help mitigate your risk of a cyberattack – uncover your **SensCy Score™**



A great tool to help determine your overall cyberhealth is the SensCy Score™. It's akin to a credit score in the sense that it gives you a broad estimation of your organization's cybersecurity. The score is a good indication of your organization's cyber hygiene and how prepared your organization is against cyber threats. The score considers information from your system, including preparedness, defenses, detection, response, and recovery. The score is on a scale from 0 to 1000. An organization should strive for a score of 800 or more.



To schedule your SensCy Score™ please scan the QR code or visit our website at senscy.com/senscy-score.



The Trusted Guide to Sensible Cyber For Small and Medium size Organizations