



SensCy Inc.

info@senscy.com

734.276.9891

455 East Eisenhower Parkway

Suite 300

Ann Arbor, MI 48108

www.senscy.com

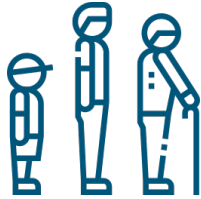
Adapting to the New Norm:

Managing Cybersecurity Threats in the Age of Advanced Technology & Geopolitics

David Behen, SensCy
July 25, 2023



Large Macro Challenges



Demographics

Aging population
Shrinking talent supply



Cybersecurity

Increasing threats
Escalating arms race



Climate Change

Increasing volatility



Lack of Civility

Attack
Blame
Destroy



Artificial Intelligence

Faster analysis
Good and bad



Geopolitical Risk

Government intervention
& actions



Supply Chain

Shutdown risk



Pandemic / Unknowns

They will happen



Introduction

- **Are you worried about Cyber Threats?**
- **What are you worried about?**





Oakland, California (Feb 2023 - ongoing)

OAKLAND -- A ransomware attack plaguing City of Oakland computer systems has worsened with a new trove of personal data of employees and residents released onto the so-called dark web, city officials acknowledged.

The ransomware attack began in February and resulted in network outages to the city's systems, prompting the city administrator to declare a state of emergency to fast-track the restoration process. Ransomware attacks involve hackers encrypting files and demanding ransom to decrypt them. The release of data indicates no ransom has been paid and hackers are following through on their threats.

On Tuesday, city officials confirmed the same hacker group which released sensitive personal information in February was also responsible for a data dump of some 600 gigabytes of information, about 60 times larger than the previous data release. The data is accessible by anyone with custom software created for darknet websites.

The data is compiled of information such as social security numbers, home addresses, and medical data from thousands of current and former city workers. Confidential information from some of the city's residents who have filed claims against the city or applied for programs through City of Oakland websites has also been included in the data dump.

Mayor Sheng Thao said Wednesday during a press event promoting downtown businesses that the city was still working with local and federal law enforcement to resolve the ongoing attack.

The Ramifications of a Breach

The impact of the security breach went beyond the disruption of city services, affecting both Oakland residents and city employees on a personal level. From July 2010 to January 2022, city employees were notified that their personal information may have been compromised. Additionally, certain Oakland residents, such as those filing a claim against the city or applying for federal programs through the city, may have also been affected.

As expected, this ongoing situation is a nightmare for both IT services and city administration, and it is also a public relations nightmare. Many concerned citizens continue to question how they are impacted and how to protect themselves against identity theft.

Last week, the Oakland police officers' union filed a claim against the city for damages suffered because of the ransomware attack. The claim from the Oakland Police Officers' Association seeks monetary damages as well as credit monitoring services, bank monitoring services, credit restoration services and identity theft insurance.

Attorneys for the police union said the city was repeatedly warned in the past and recently of "significant deficiencies in the security of its information technology systems," according to the claim.



BankInfoSecurity


<https://www.bankinfosecurity.com> › after-ransomware... ⋮

After Ransomware Attack, Oakland Faces Data Breach ...

Jun 1, 2023 — A flurry of legal complaints and a lawsuit have been filed against **Oakland, California**, in the wake of a ransomware attack that disrupted ...



Recent Attacks

 July 11, 2023

Cyber attack on a city government in North Carolina, USA

Town of Cornelius - Cornelius, North Carolina, USA (Mecklenburg County)

 July 9, 2023


Ransomware at a city government in California, USA

Hayward, California, USA (Alameda County)

 July 8, 2023


Cyber attack on a county government in Delaware, USA

Kent County - Dover, Delaware, USA (Kent County)

 June 28, 2023


Cyber attack on the judicial branch of Nebraska, USA

Judicial Branch - Lincoln, Nebraska, USA (Lancaster County)

 June 23, 2023


Website of a city in Texas, USA hacked

Fort Worth, Texas, USA (Tarrant County and others)

 June 2023


Cyber attack on a township in New Jersey

Montclair Township - Montclair, New Jersey, USA (Essex County)

 June 2023


Cyber attack on a city government in Utah, USA

City of West Jordan - West Jordan, Utah, USA (Salt Lake County)

 June 8, 2023


Cyber attack on a city government in Arkansas

City of Fayetteville - Fayetteville, Arkansas, USA (Washington County)

 May 31, 2023

Agency in Rhode Island, USA affected by cyber attack

Rhode Island Government - Providence, Rhode Island, USA (Providence County)

 May 31, 2023

County government in Florida, USA affected by cyber attack

Hillsborough County - Tampa, Florida, USA (Hillsborough County)



3rd Party Cyber Risks

SecurityIntelligence

Home / News

Cyberattacks Rise Sharply Against Governments and Schools



News | March 6, 2023

By Jonathan Reed | 4 min read

Third-Party Cyber Victims Affect the Public Sector

In many instances, attacks on third parties can affect entire sectors, including the public sector. For example, in a notification shared with New York's [Rockland County](#), cloud-based solutions provider Cott Systems informed its customers that it had been hit by an "organized cyberattack" on its servers on December 26. In response to the intrusion, the company disconnected its servers to contain the breach.

Cott Systems helps manage government data for public records, land records and court cases. The company serves over 400 local governments across 21 states and has established relationships with several national and international organizations. The server outage caused hundreds of local governments to rely on manual processes. This led to delays in the processing of birth certificates, marriage licenses and real estate transactions, as per [ISMG](#).

"Everything is at a much slower pace," Scott Rogers, assistant manager of Nash County, told [WRAL-TV](#). At least six counties in North Carolina couldn't access their vital records systems and had to revert to manual record-keeping.

A worker in Livingston Parish, Louisiana, where Cott provides e-services, told [WAFB9](#) news agency that "the workaround has been to use pens to timestamp new filings and search through piles of physical copies to find valuable records." County clerks from Connecticut and Mississippi also reported similar slowdowns in the past week as services remained offline.



Discussion Topics

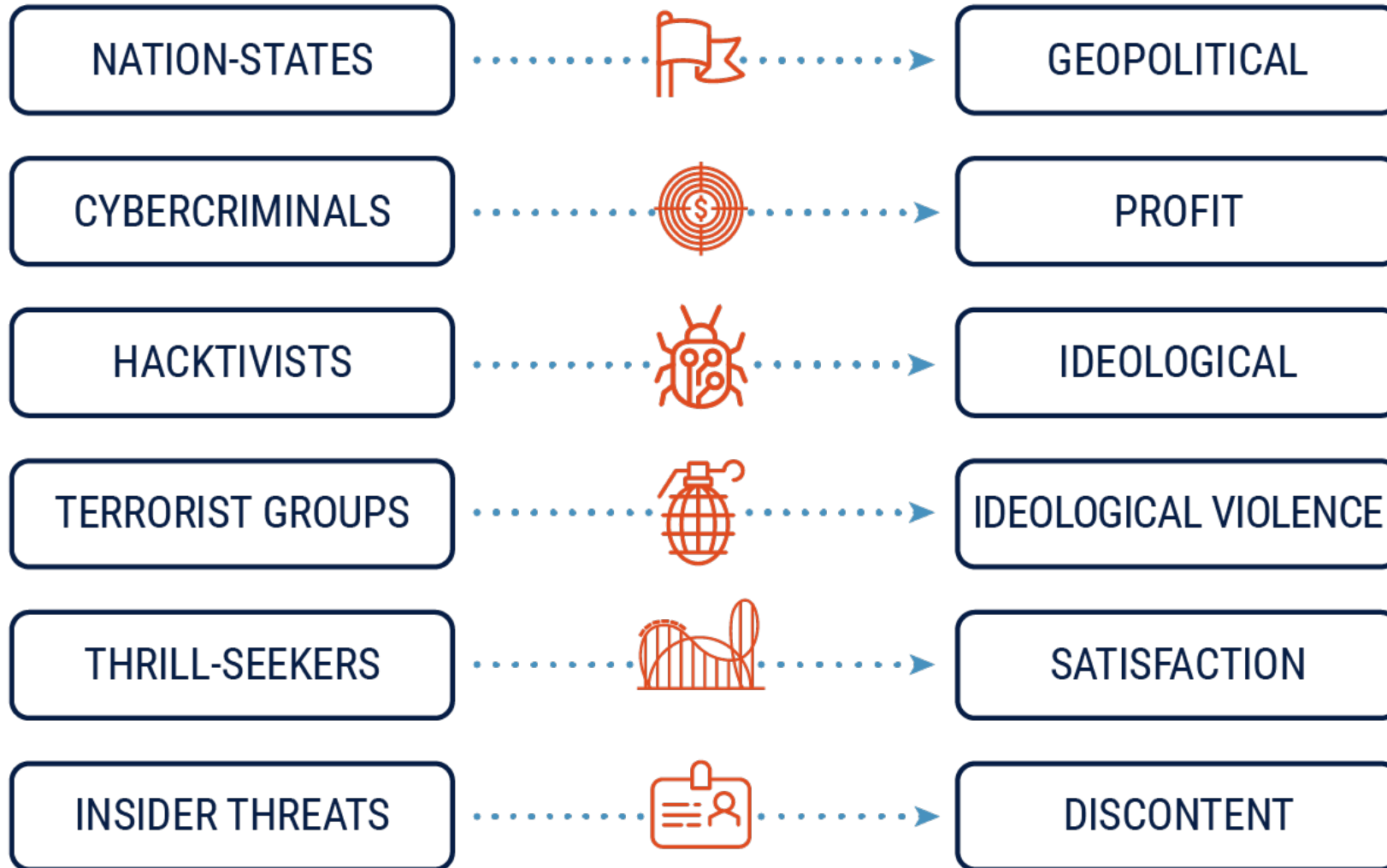
- Who are these threat actors?
- The threats your organizations face
- Your responsibilities
- Protecting your organizations



THREAT ACTORS

CYBER THREAT ACTOR

MOTIVATION





COMMON CYBER ATTACKS

- Ransomware
- Phishing
- Malware
- Zero-Day
- Insider





WHAT IS THIS?



Wana Decrypt0r 2.0 English



Payment will be raised on
5/15/2017 16:32:52

Time Left
02: 23: 59: 49

Your files will be lost on
5/19/2017 16:32:52

Time Left
06: 23: 59: 49

[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

What Happened to My Computer?

Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am CMT from Monday to Friday.

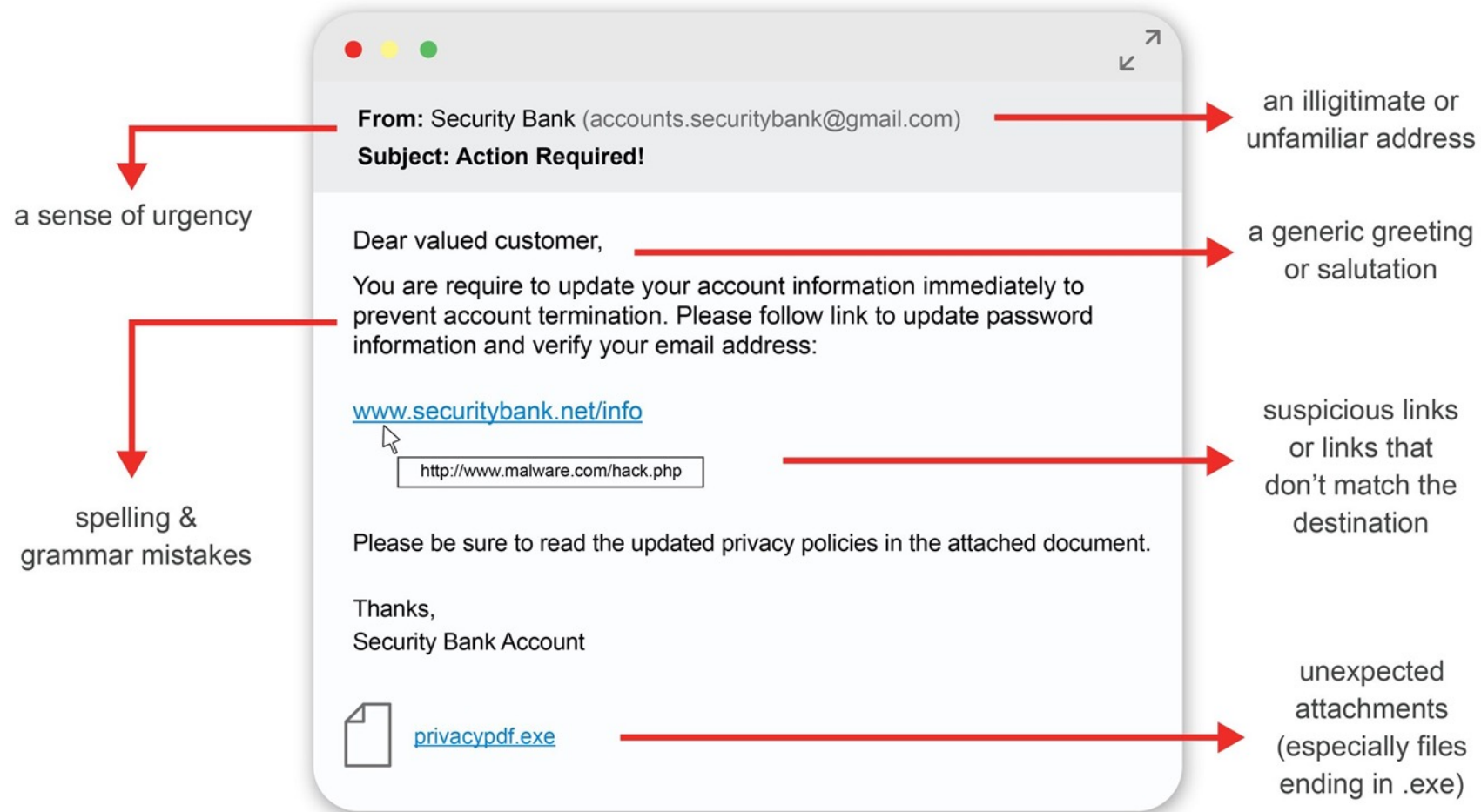
Send \$300 worth of bitcoin to this address:

 **bitcoin**
ACCEPTED HERE

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw Copy



Phishing





Zero Day

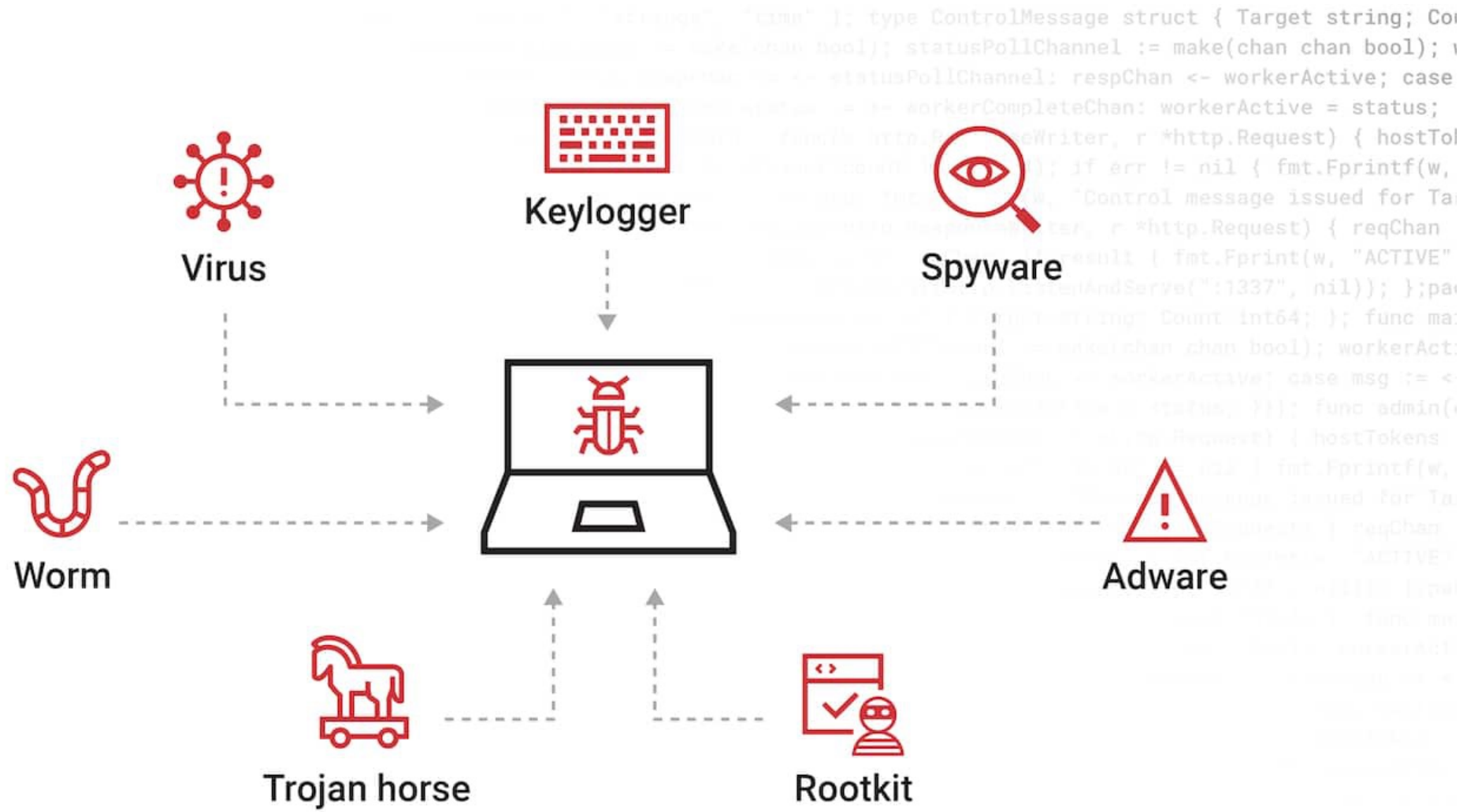


By not updating your systems, you are extending the risk-timeline for zero-day attacks

- 1. Vulnerability introduced.** You have software with a bug. It might be a coding mistake, missing encryption, or anything else that lets unauthorized people access the system.
- 2. Exploit released in the wild.** Cybercriminals find the bug, release an exploit code or malicious payload, and use it to conduct attacks.
- 3. The vendor finds the vulnerability.** Vendors or parties responsible for fixing the software discover the bug, either by their continuous testing or via third-party researchers. They start working on a patch.
- 4. Vulnerability disclosed in public.** The vendor or affected parties publicly disclose information about the bug. The bug gets a **common vulnerabilities and exposures (CVE)** number for easy identification. Some vulnerabilities remain private and get patched quietly.
- 5. Anti-virus signatures released.** Once the involved parties know about the vulnerability, cybersecurity vendors detect signatures of attacks and exploit the **hackers** made using the flaw. They then update their scanning and detection systems.
- 6. Patch released.** Meanwhile, the software vendor releases patches for the vulnerability. Anyone who updates their systems with patches is no longer susceptible to attacks.
- 7. Patch deployment complete.** Once patch deployment is complete, the vulnerability can no longer be exploited in any way.



Malware





Insider Threats



Negligent



Fast Worker



Disgruntled



Impact of Artificial Intelligence

Advantages

- User Access & Actions
- Threat Detection & Response
- Risk Management
- Enhance Compliance



Disadvantages

- Users putting confidential information in public AI tools
- Phishing attacks difficult to detect
- False positives
- Identifying bad code faster
- Identifying vulnerable organizations faster



What is your responsibility?



- Confidentiality
- Integrity
- Availability
- Compliance



PROTECT YOURSELF TODAY



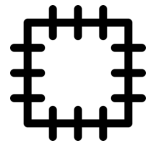
Start with basic cyber hygiene

- Professionally and personally
- 88% of cyber incidents can be avoided with basic cyber hygiene



Strong passwords

- Weak: password, Password, Password1, P@ssword1
- Strong: Cl1mbTh3Mount@!n (Climb The Mountain "passphrase")



Patch your systems

- Accept automatic updates or develop a process to accept updates 1 week after release



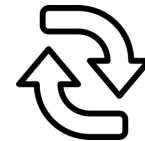
Regular backups

- Back up to portable drives or subscribe to a service for cloud storage



Multifactor authentication

- Enroll whenever available



Password Reuse

- Never reuse passwords across systems (e.g. bank and Netflix)



MORE WAYS TO PROTECT YOURSELF



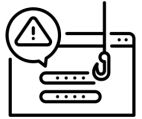
Use anti-malware / anti-virus software

- Keep subscriptions and definitions up-to-date



User security awareness training

- SensCy
- CyberSafe
- Security Mentor



Do not click links in email from people you don't know

- Hover over email address, links, and attachments to display actual address



Contact organizations directly when asked to change financial data or provide personal data



PROTECT YOURSELF & YOUR FAMILY



Purchase a credit protection service

- Experian, LifeLock, etc.
- I use Experian - \$19.99 per month

Purchase a password manager

- Password Keeper – family plan is \$79.99 per year

Install multi-factor authentication wherever possible

Secure home Wi-Fi

Upgrade devices regularly (auto update)

Use biometrics whenever possible

Back up to the cloud daily

- Such as iCloud
- Back up often to a secure portable device



RESOURCES

- **Subscribe to SensCy Cyber Briefs** – www.senscy.com
- **StaySafeOnline** – <https://staysafeonline.org/>
- **US-CERT** – <https://www.us-cert.gov/ncas/tips/ST06-003>
- **Children Safety** – <https://www.us-cert.gov/ncas/tips/ST05-002>
- **DHS** – <https://www.dhs.gov/how-do-i/protect-myself-cyber-attacks>
- **SANS Tip of the Day** – www.sans.org/tip-of-the-day
- **Federal Trade Commission** – <https://www.consumer.ftc.gov/features/feature-0038-onguardonline>
- **NetSmartZ** – <https://www.netsmartz.org/Home>
- **State of Michigan** – https://www.michigan.gov/som/0,4669,7-192-78403_78404---,00.html



Cybersecurity is a Chronic Condition

PREVENTION



CURE



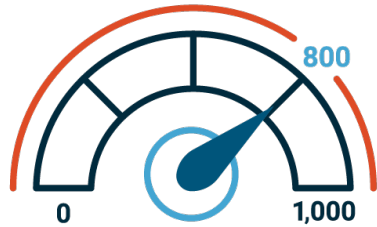
Prevention is better than the cure

- If your township/city lost 10,000 customer records, it would cost you **\$1,640,000**
- Preventative measures would cost a lot less



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 sency.com/sency-score.



Sensible Cyber Solution

Monthly Subscription Pricing

\$750

1 – 20 active online users

\$1,000

21 – 100 active online users

\$1,500

101 – 250 active online users



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 POLICY LIBRARY

A policy library to ensure you are following best practices



CYBER TRAINING

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



PHISHING

Friendly phishing tests to keep your employees vigilant against phishing attacks



EXTERNAL SCANS

Vulnerability and dark web scanning help keep you protected



CYBER ALERTS

Proactive outreach for emerging threats – tailored to your systems



INCIDENT RESPONSE PLAN

Help your team respond to an attack and minimize the impact



CYBER INSURANCE

Assist with properly completing cyber insurance forms



EXECUTIVE BRIEFING

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



CLIENT DASHBOARD

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

Buying equivalent services on an ad hoc basis would be much more expensive. Our comprehensive, wrap around solution in plain language has great value.



QUESTIONS





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