How Important is an Annual Risk Assessment?

WHAT IS A RISK ASSESSMENT?

ONEcon

Agenda

- Introductions
- The Foundation
- What is a Risk Assessment?
- What to Measure
- SMB Cyber Concerns
- Risk & Responsibility
- Q&A

ONEcon

Speaker Intro

Natalie Suarez

Principal Solutions Advisor

CONNECTWISE

- 2023 CRN® Channel Chief
- 25+ years in IT and Cybersecurity
- Began career as a software developer
- Supported Department of Defense Intelligence analysts
- IT Nation Certify Instructor
- Speaker at Industry Events
- Co-chair, CompTIA ISAO Executive Steering Committee
- Launched the IT Nation Evolve™ Cybersecurity Peer Group
- Passionate about my family, threat intelligence, and LEGO™
- Bachelor of Science, Computer Engineering, magna cum laude

ONEcon

The Foundation

What is Cybersecurity?

You keep using that word. I do not think it means what you think it means.

- Inigo Montoya (Mandy Patinkin, Actor), The Princess Bride

Cybersecurity is about managing risk. For most businesses, security is a cost center, so security only makes sense to the extent that it reduces business risk or saves money.

What is Risk?

- Risk - Combination of the probability of an event occurring and the consequences
- Inherent Risk - The risk level without considering any actions taken to mitigate the threat
- Residual Risk – The risk level after safeguards has been put in place

Definitions

- Threat – Anything that can act against an asset to be able to cause harm
- Asset – Something that is worth protecting
- Vulnerability – Weakness in the design, implementation, operation or control that could expose a system to threats
- Control - Controls are activities that mitigate or eliminate certain risks or threats

What is a Risk Assessment?

Frameworks

Starts with a Framework

- Establish a common language
- Cybersecurity frameworks are a system of standards, guidelines and best practices to manage risks (that arise in a digital world)
- A cybersecurity framework prioritizes a flexible, repeatable and cost-effective approach to promote the protection and resilience of your business
- This includes improving communications, awareness and understanding between and among IT planning and operations as well as senior executives of organizations

Protect your “House”

ONEcon

'The Right' Cybersecurity

Identify	Protect	Detect	Respond	Recover
Family / Pets	Doors Windows	Alarm	Dog	Cyber Incident Response Plan
Collectibles	Locks	Motion Sensor	Flee	Business Continuity/ Disaster Recovery Plan
Documents / Valuables	Education	Doorbell Camera	Police	Insurance
Electronics / Computers	Yard Signs	Neighborhood Watch	Baseball Bat	Emergency Equipment/ Incident Responders

ONEcon

Risk Assessment

A cybersecurity risk assessment refers to the process of identifying, estimating, and prioritizing information security risks. These assessments cover everything from policies, processes, employee training, and technologies used to protect an organization's users and data.

ONEcon

Network Assessment

- *Internal Systems*
- *Backup Recovery Plans*
- *Employee Roles*
- *System Stability*
- *Use Policies*

ONEcon

Security Assessment

- *Attack Surfaces*
- *Points of Entry*
- *User Habits*
- *Security Policies*
- *HR Procedures*
- *Legal Impact*

ONEcon

Vulnerability Assessment

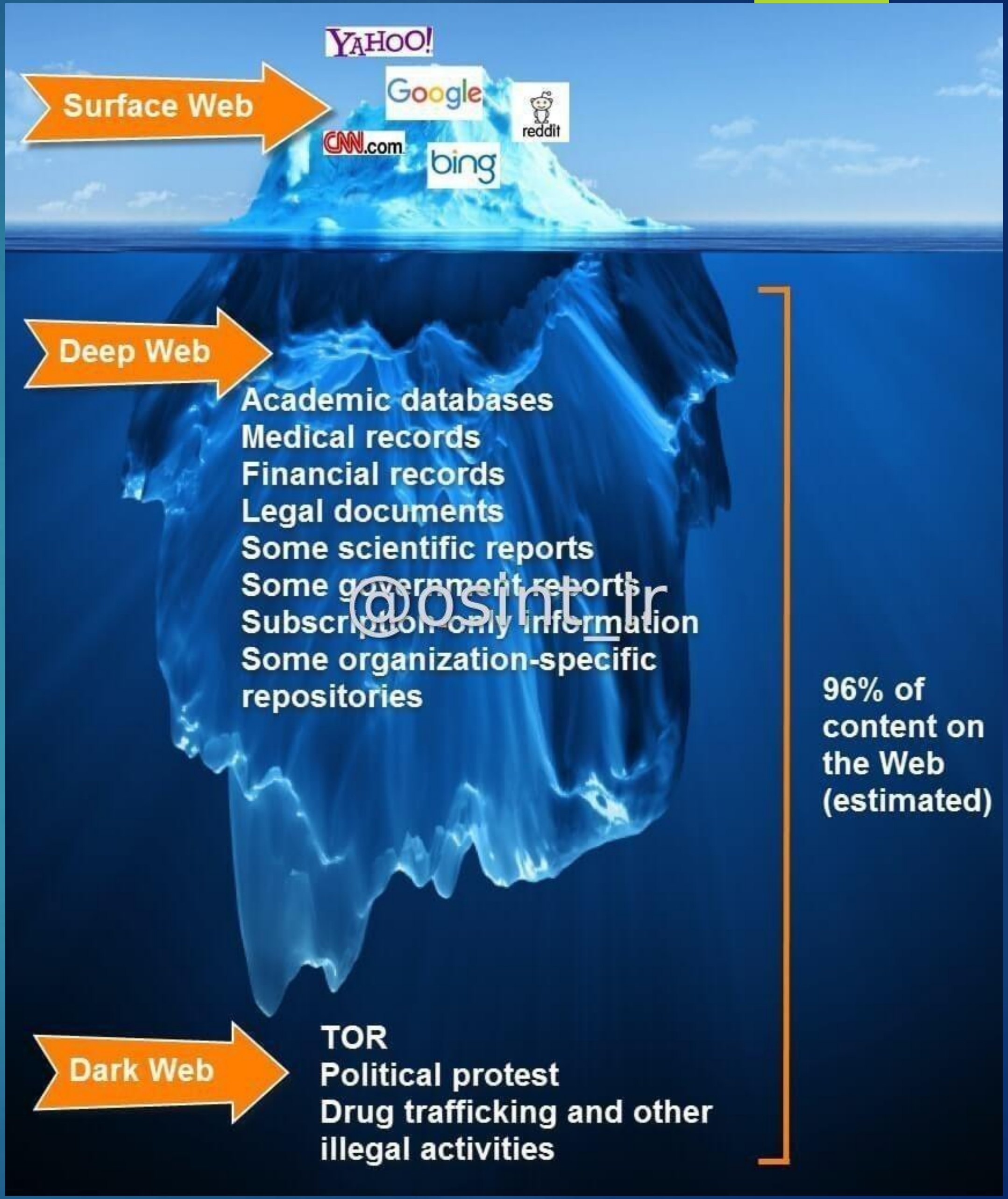
- *Application Flaws*
- *Operating System Flaws*
- *Computer System Flaws*
- *Enabled Ports, Processes and Services*
- *Database*
- *Human Error*

Dark Web Assessment

Surface Web – Publicly available information; Crawled by search engines

Deep Web – Majority of online content, (90-96%), e.g., online shopping, banking, medical records, etc.

Dark Web – Anonymous, accessed by law enforcement, criminals, and the curious; Not accessible by commercial search engines



Surface Web

Deep Web

Academic databases
Medical records
Financial records
Legal documents
Some scientific reports
Some government reports
Subscription-only information
Some organization-specific repositories

96% of content on the Web (estimated)

Dark Web

TOR
Political protest
Drug trafficking and other illegal activities

What is my data worth? Match the values.

1. Online Banking Information:
2. Access to Corporate Network
3. Full Credit Card Details
4. Healthcare Data
5. Social Security Number

A. $10 - $100
B. $1,000
C. $1
D. $100
E. $2,000 – $4,000

What is my data worth? Answers

1.	Online Banking Information	D.	$100
2.	Access to Corporate Network	E.	$2,000 - $4,000
3.	Full Credit Card Details	A.	$10 - $100
4.	Healthcare Data	B.	$1,000
5.	Social Security Number	C.	$1

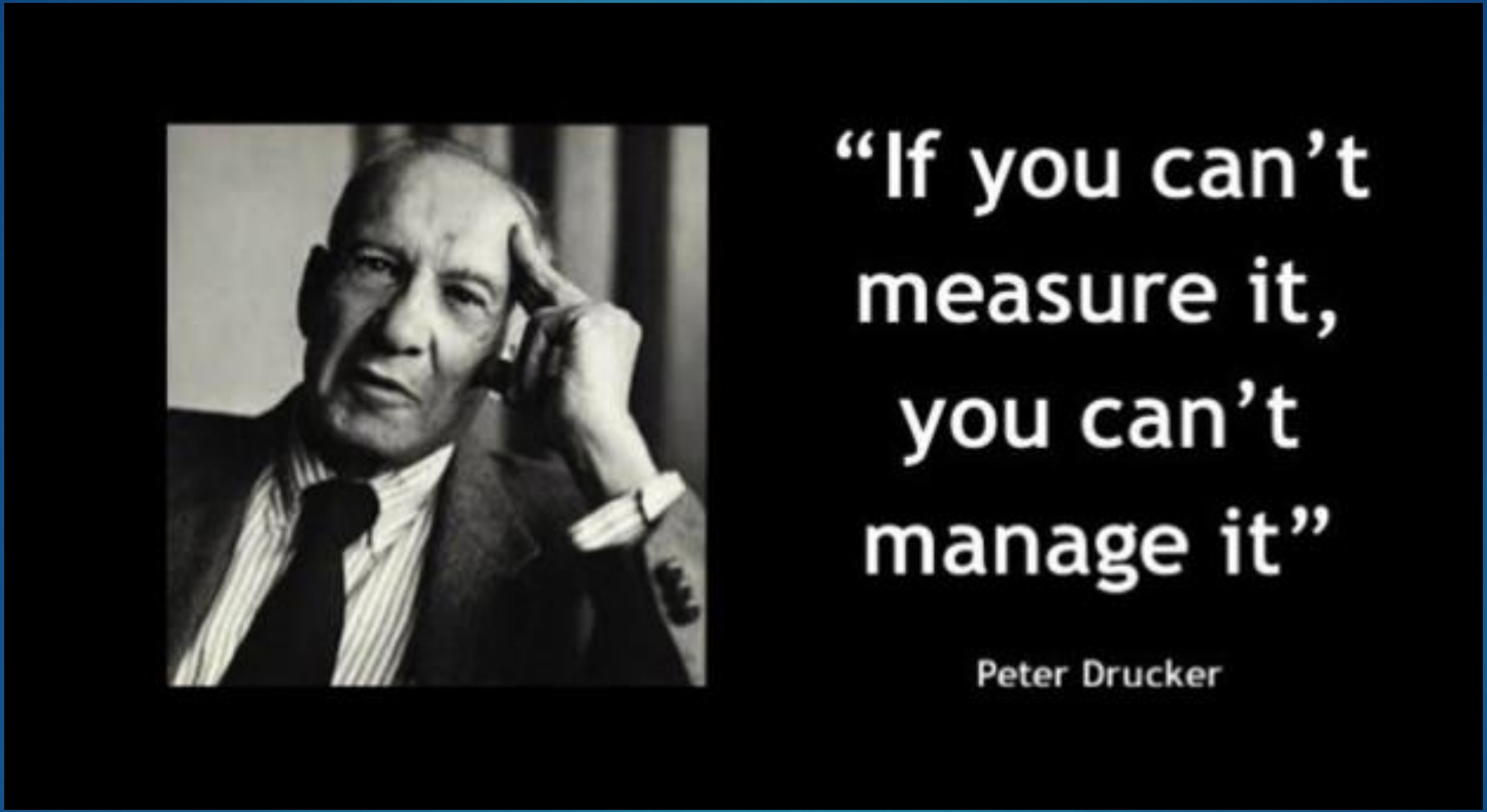
Sources:
Healthcare Data: The Perfect Storm (forbes.com)
BTC/USD 36,809.20 (▼0.75%) | Google Finance
Infant Social Security numbers are for sale on the dark web (cnn.com)
Revealed – how much is personal data worth on the dark web? | Insurance Business Canada (insurancebusinessmag.com)

Risk Assessment Purpose

- Identify Threat Sources
- Identify Threat Events
- Identify Vulnerabilities
- Determine the Likelihood of Exploitation
- Determine Probably Impact
- Calculate Risk as a Combination of Likelihood and Impact

What to Measure?

HOW DO YOU KNOW WHERE YOU ARE?



“If you can’t measure it, you can’t manage it”

Peter Drucker

People, Process & Technology

People

Process

Technology

ONEcon

PEOPLE	PROCESS	TECHNOLOGY		CAPACITY OUTCOMES
○	○	○	→	No Defense
●	○	○	→	No ability to execute
○	●	○	→	Wasted effort
○	○	●	→	Shelf-ware
●	●	○	→	Burden to scale
●	○	●	→	Inconsistent operation
○	●	●	→	Poor adoption
🟢	🟢	🟢	→	**Success**

ONEon

What is Cybersecurity Culture

The Cybersecurity Culture of an organization

refers to the:

- **Knowledge**
- **Beliefs**
- **Perceptions**
- **Attitudes**
- **Assumptions**
- **Norms**
- **Values**

… of people regarding cybersecurity and how they manifest in people's behavior with information technologies.

It must be an integral part of an employee's job, habits and conduct, embedding them in their day-to-day actions.

Policies

- Acceptable Use Policy
- Anti-Virus and Malware Policy
- Data Access and Password Policy
- Data Back-Up Policy
- Facility Security Policy
- Perimeter Security and Administration Policy
- System Configuration Policy
- Telecommuting / Remote Work Policy
- Vulnerability Identification & System Updates Policy
- Asset Management Policy
- Change Management Policy
- Code of Ethics Policy
- Encryption Policy
- Information Security (InfoSec) Risk Assessment Policy
- Logging and Monitoring Policy
- Incident Response Policy
- Internal Privacy Policy (Data Protection)
- Service Provider Security Policy
- Social Networks Policy
- Artificial Intelligence Policy

Components of a Well-Designed Cybersecurity Solution for your Business

- Security Assessment
- Security Awareness
- Passwords
- DNS Protection
- Mobile Device Security
- Advanced Endpoint Detection & Response
- SIEM / Log Management
- Dark Web Research
- Business Continuity/ Disaster Recovery
- Computer Updates
- Spam Email
- Multi-Factor Authentication
- Encryption
- Firewall
- Cyber Insurance

ONEon

Risk Assessment Outcomes

- Roadmap that aligns your business objectives with the likelihood and impact of risks.
- Gives your business the tools and understanding to protect against threats
- O good, now we’re done…

Why do I need to do this again?

- Ever evolving **Cyber Threat Landscape**
- Change in **Business Objectives or Business Model**
- Changes in **infrastructure**
- Changes in **Resources**
- Improvements and course corrections in the **Cyber Roadmap**

SMB Cyber Concerns

WHY MY BUSINESS SHOULD CONDUCT AN ANNUAL RISK ASSESSMENT

Everyday Challenges for SMBs

- Cybersecurity confusion (IT challenge vs. Business Challenge)
- Difficult to manage cybersecurity with competing priorities
- Complexity of shifting to a remote workforce
- Limited cybersecurity resources within the organization
- Ad hoc business continuity & disaster recovery (BCDR) efforts
- Increased costs to respond & recover from an incident
- Global legislation
- Cyber warfare
- Reputation Damage

ONEcon

SMBs Are Targets

The gap between the number of breaches seen by small and large organizations has become much less pronounced.

All organizations are being targeted by

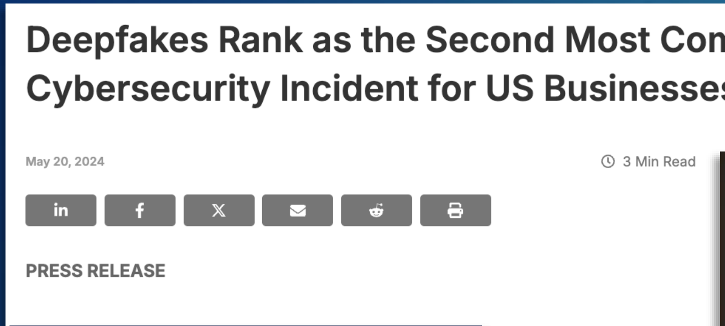
financially motivated organized crime actors !!

82% of Ransomware Attacks Target SMBs

Articles (umaryland.edu)

ONEcon

Current Threat Landscape

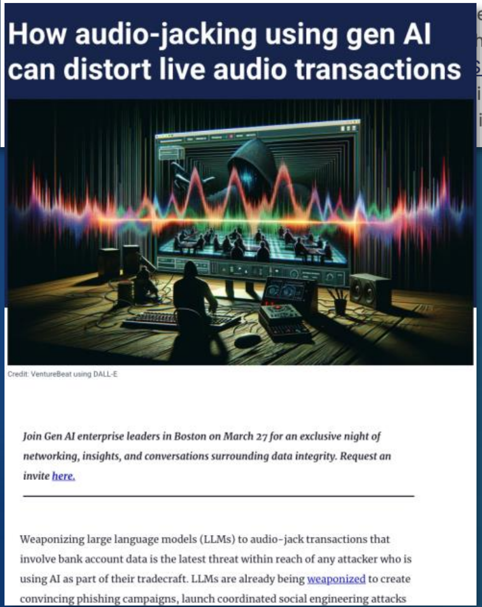


Deepfakes Rank as the Second Most Common Cybersecurity Incident for US Businesses

May 20, 2024 — 3 Min Read

PRESS RELEASE

e second most common he past year, trailing only SMS.online, the auditor ird of businesses across in the last 12 months.

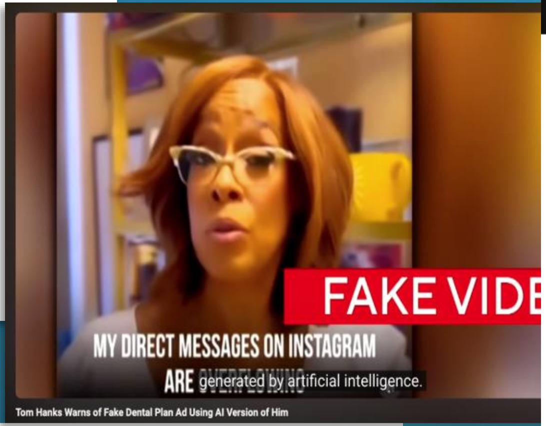


How audio-jacking using gen AI can distort live audio transactions

Credit: VentureBeat using DALL-E

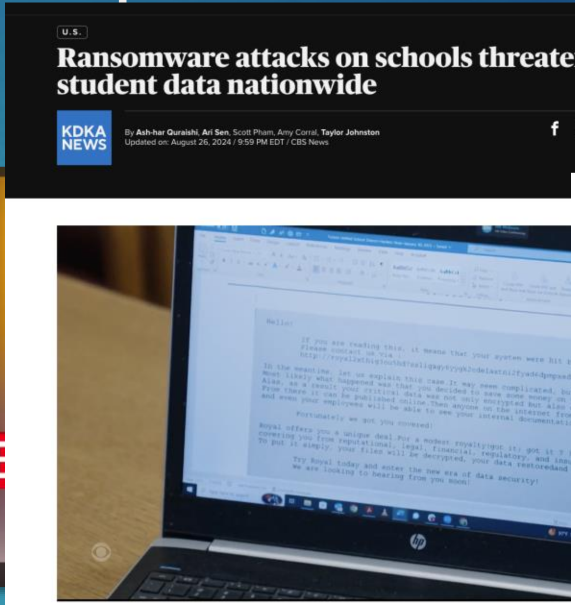
Join Gen AI enterprise leaders in Boston on March 27 for an exclusive night of networking, insights, and conversations surrounding data integrity. Request an invite here.

Weaponizing large language models (LLMs) to audio-jack transactions that involve bank account data is the latest threat within reach of any attacker who is using AI as part of their tradecraft. LLMs are already being weaponized to create convincing phishing campaigns, launch coordinated social engineering attacks



FAKE VIDE
MY DIRECT MESSAGES ON INSTAGRAM
ARE generated by artificial intelligence.

Tom Hanks Warns of Fake Dental Plan Ad Using AI Version of Him



U.S.

Ransomware attacks on schools threaten student data nationwide

KDKA NEWS

By Ash-har Quraishi, Ari Sen, Scott Pham, Amy Corral, Taylor Johnston
Updated on: August 26, 2024 / 9:59 PM EDT / CBS News

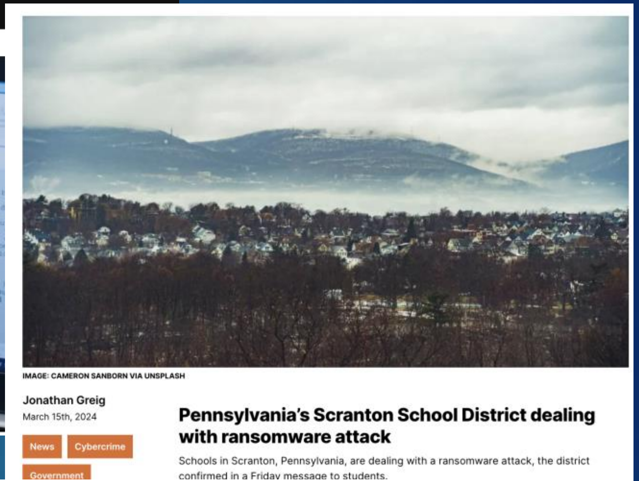


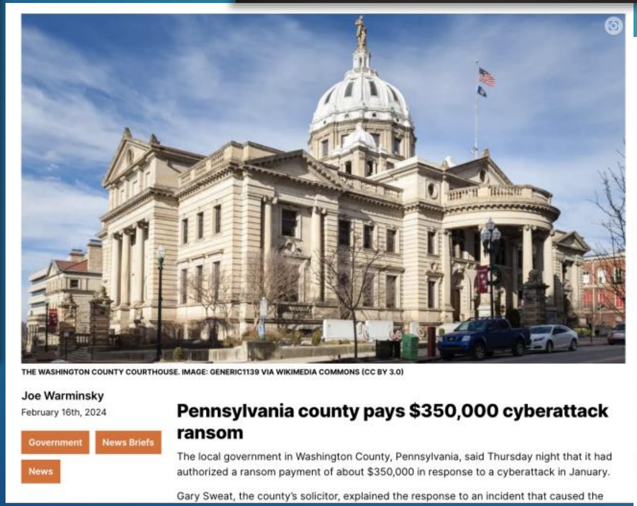
IMAGE: CAMERON SANBORN VIA UNSPLASH

Jonathan Greig
March 15th, 2024

News | Cybercrime | Government

Pennsylvania's Scranton School District dealing with ransomware attack

Schools in Scranton, Pennsylvania, are dealing with a ransomware attack, the district confirmed in a Friday message to students.



THE WASHINGTON COUNTY COURTHOUSE. IMAGE: GENERIC1139 VIA WIKIMEDIA COMMONS (CC BY 3.0)

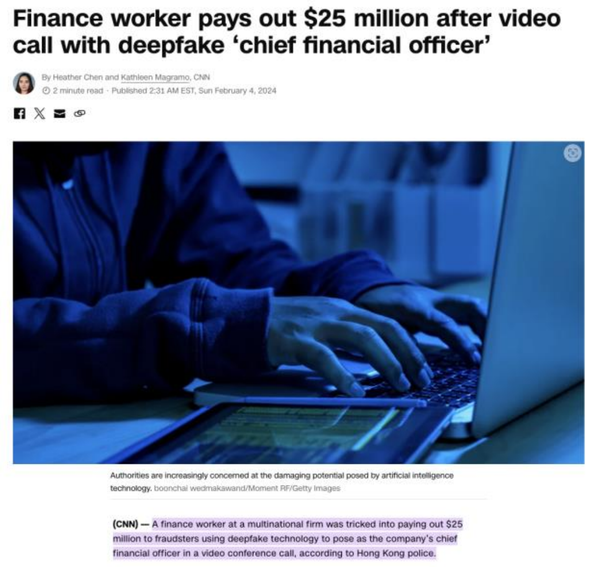
Joe Warminsky
February 16th, 2024

Government | News Briefs | News

Pennsylvania county pays $350,000 cyberattack ransom

The local government in Washington County, Pennsylvania, said Thursday night that it had authorized a ransom payment of about $350,000 in response to a cyberattack in January.

Gary Sweat, the county's solicitor, explained the response to an incident that caused the

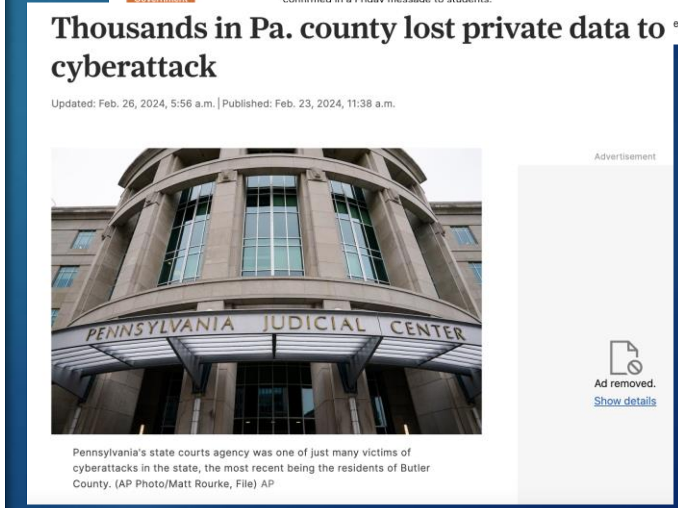


Finance worker pays out $25 million after video call with deepfake 'chief financial officer'

By Heather Chen and Kathleen Magramo, CNN
2 minute read · Published 2:31 AM EST, Sun February 4, 2024

Authorities are increasingly concerned at the damaging potential posed by artificial intelligence technology. boonchai wedmakawand/Moment RF/Getty Images

(CNN) — A finance worker at a multinational firm was tricked into paying out $25 million to fraudsters using deepfake technology to pose as the company's chief financial officer in a video conference call, according to Hong Kong police.



Thousands in Pa. county lost private data to cyberattack

ead

Updated: Feb. 26, 2024, 5:56 a.m. | Published: Feb. 23, 2024, 11:38 a.m.

Pennsylvania's state courts agency was one of just many victims of cyberattacks in the state, the most recent being the residents of Butler County. (AP Photo/Matt Rourke, File) AP

ONEon

Verizon 2024 DBIR

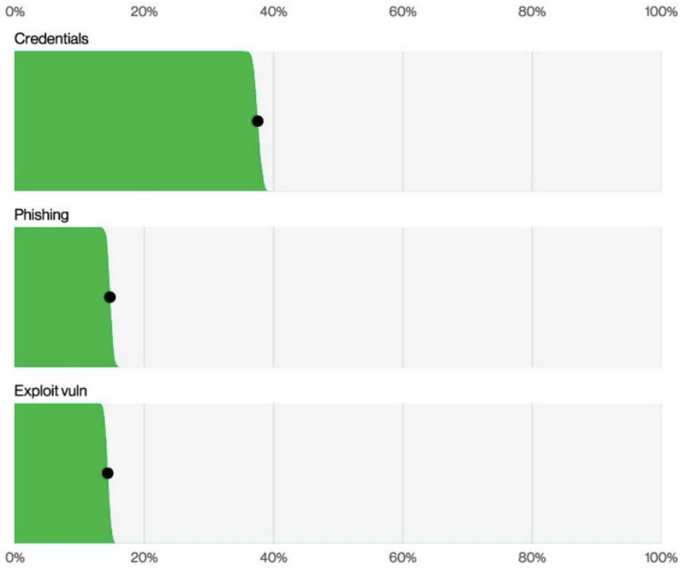
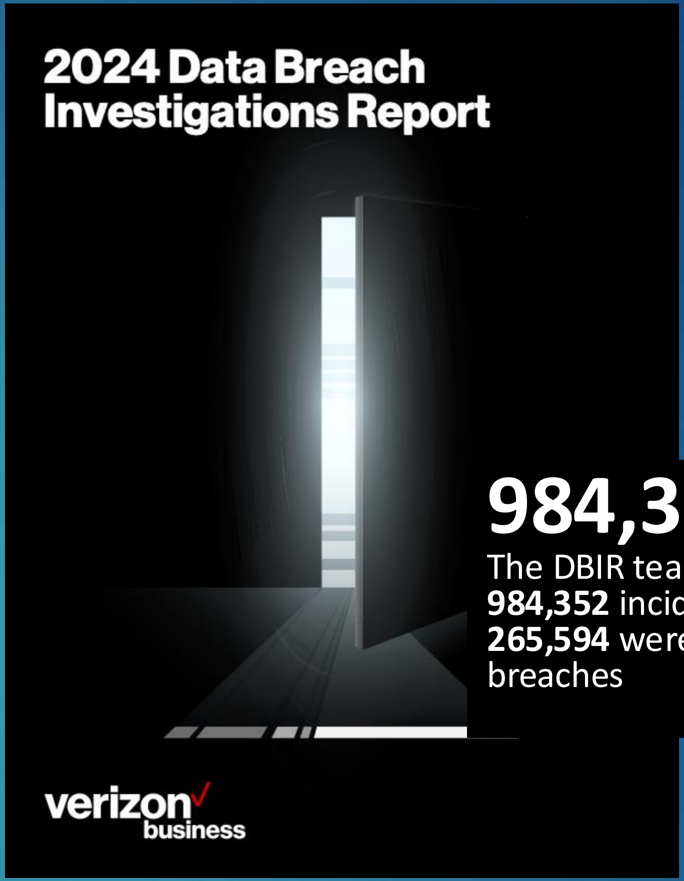


Figure 1. Select ways-in enumerations in non-Error, non-Misuse breaches (n=6,963)



984,352

The DBIR team has analyzed **984,352** incidents, of which **265,594** were confirmed breaches

There are three key paths leading to the compromise of your estate:

- Credentials
- Phishing
- Exploit vulnerabilities – 180% growth since 2023

Verizon 2024 Data Breach Investigations Report

ONEcon

No organization is safe without a plan to handle them all.

Artificial Intelligence

AI will fundamentally change the way we consume technology.

Automation efficiency and ease of use will be augmented by AI.

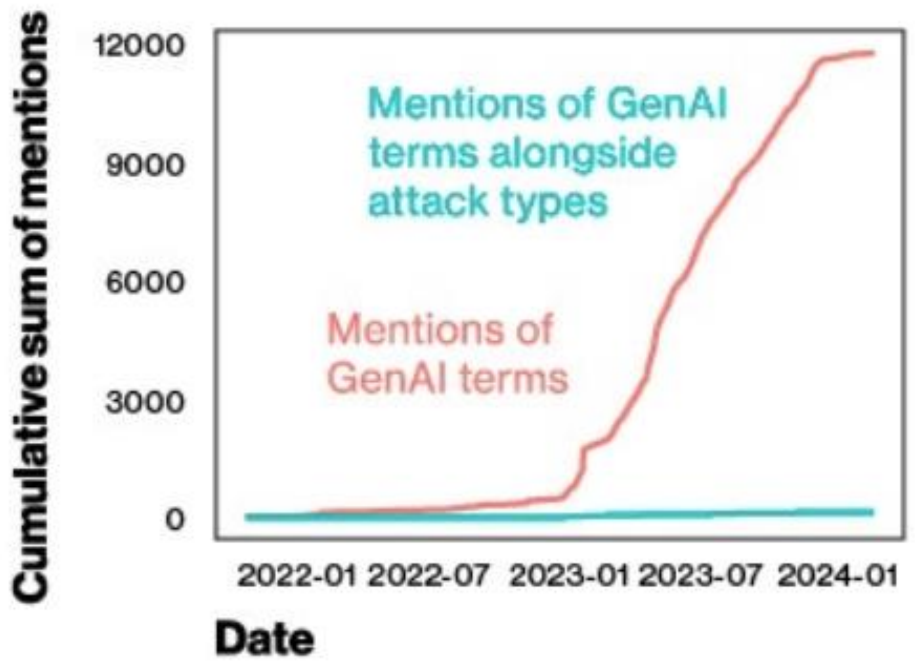


Figure 14. Cumulative sum of GenAI in criminal forums

Verizon 2024 Data Breach Investigations Report

The Human Factor

What %age of breaches involve the Human Element?

A. **20%**

B. **74%**

C. **51%**

D. **82%**

E. **35%**

ONEcon

The Human Factor - Answer

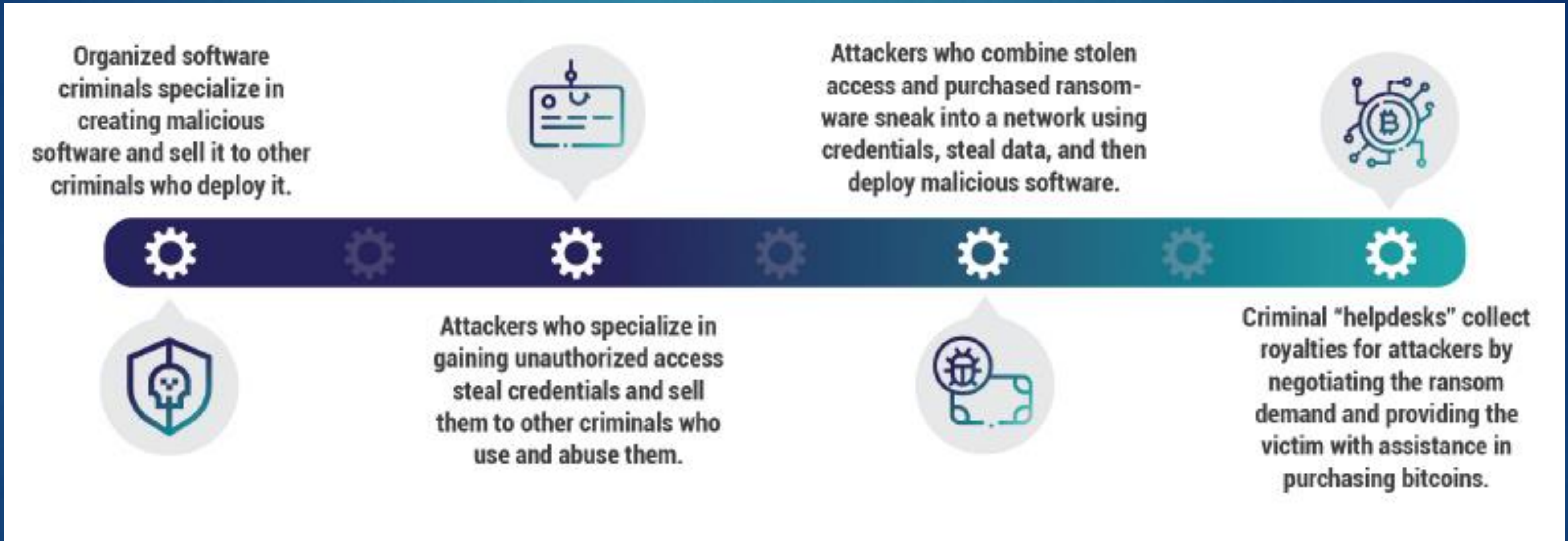
74% of all breaches include the human element, with people being involved either via Error, Privilege Misuse, Use of stolen credentials or Social Engineering.

73% of breaches involved External actors, and the primary motivation for attacks continues to be overwhelmingly financially driven, at 97% of breaches.

ONEcon

Verizon 2024 Data Breach Investigations Report

Ransomware-as-a-Service:
A production line of organized crime



Organized software criminals specialize in creating malicious software and sell it to other criminals who deploy it.

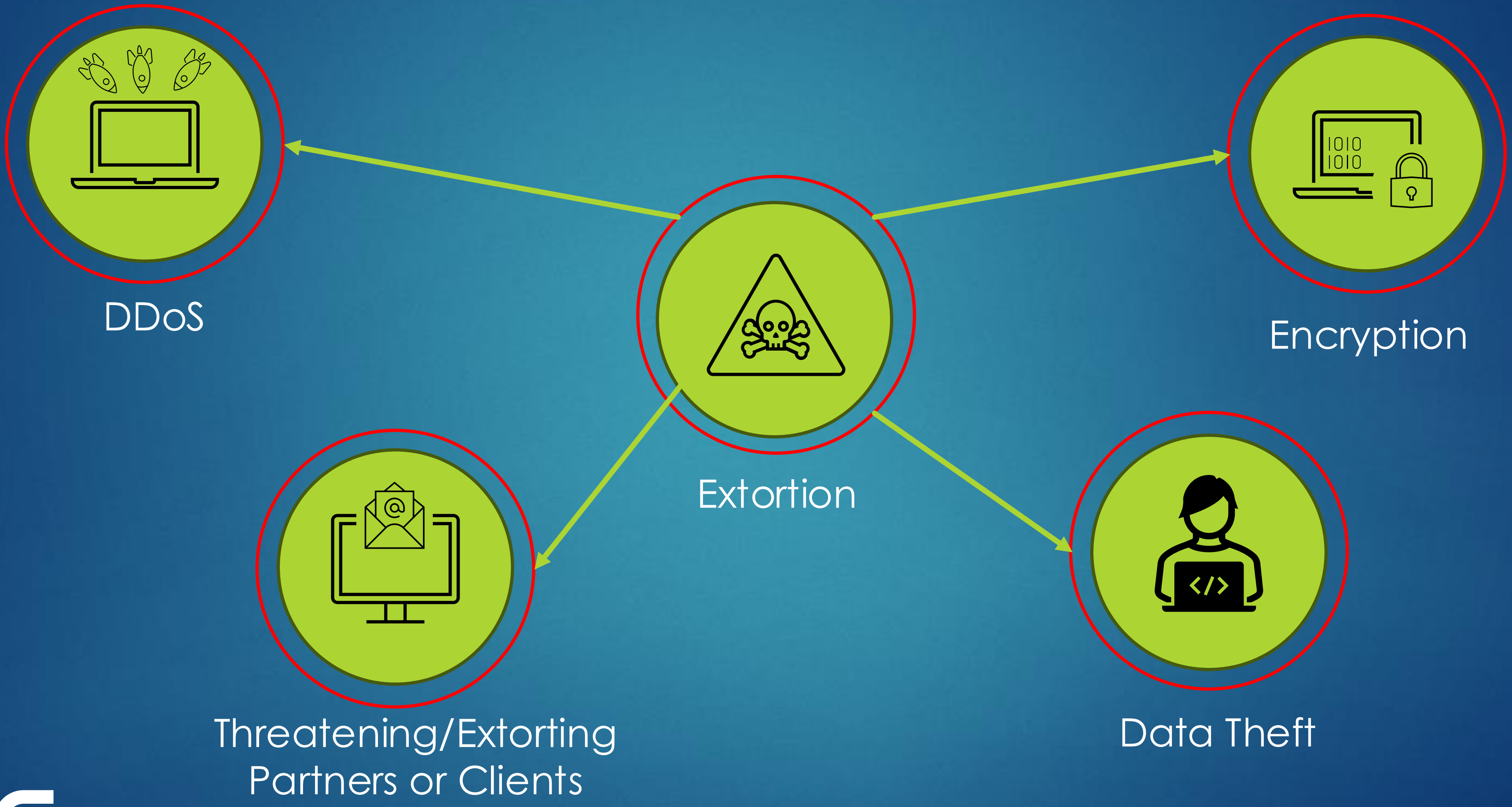
Attackers who specialize in gaining unauthorized access steal credentials and sell them to other criminals who use and abuse them.

Attackers who combine stolen access and purchased ransomware sneak into a network using credentials, steal data, and then deploy malicious software.

Criminal "helpdesks" collect royalties for attackers by negotiating the ransom demand and providing the victim with assistance in purchasing bitcoins.

Source: https://delinea.com/blog/ransomware-as-a-service-new-ransomware-model

Quadruple Extortion Tactics



Canadian Centre for Cyber Security: National Cyber Threat Assessment (2023/2024)

More Than Ransom

- Downtime
- Staff Time
- Device Cost
- Network Cost
- Lost Opportunity Cost
- Reputation

ONEcon

Paying Ransom Rarely Works

On average:

- **66%** - of data is restored after paying the ransom
- **57%** - of the encrypted data is recovered
- Very few companies recover 100% of their data.

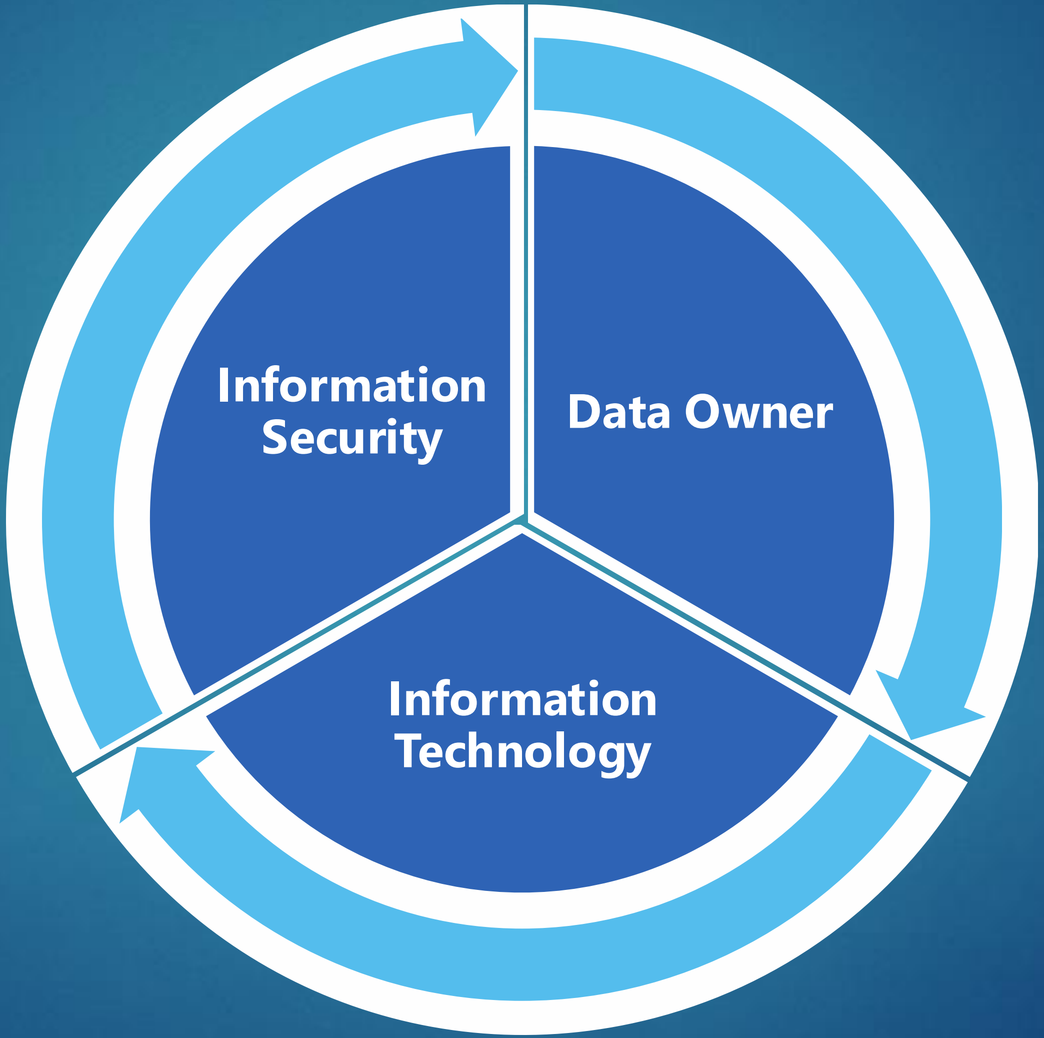
ONEcon

Risk & Responsibility

WHY MY BUSINESS SHOULD CONDUCT AN ANNUAL RISK ASSESSMENT

Understand Data Responsibility

Information Security
Provides risk insight and mitigation information for the Data Owner



Data Owner
Owns the liability and establishes the budget for protecting data

Information Technology Team
Implements solutions and are the custodians of data

ONEcon

What risk level are you willing to accept to protect your most valuable assets?

The Perfect is the Enemy of Good.

- Voltaire

The only way to stay ahead in the cybersecurity game is to conduct an annual risk assessment!

Please complete the survey!

Questions?

Thank You!

ONEcon