



Transportation Security

10.31.23














James Makil

vCISO | Nth Generation



- Senior Security Consultant and vCISO
- 17+ years of IT and cybersecurity experience
- 280+ security assessments
- Cybersecurity experience in the following business verticals:
 - Entertainment
 - Finance
 - Healthcare
 - Transportation
 - Utility
 - Gaming
 - Educational
 - Retail
- Former Benedictine monk

16 Critical Infrastructure Sectors & Corresponding Sector-Specific Agencies

 CHEMICAL	DHS (CISA)	 FINANCIAL	Treasury
 COMMERCIAL FACILITIES	DHS (CISA)	 FOOD & AGRICULTURE	USDA & HHS
 COMMUNICATIONS	DHS (CISA)	 GOVERNMENT FACILITIES	GSA & DHS (FPS)
 CRITICAL MANUFACTURING	DHS (CISA)	 HEALTHCARE & PUBLIC HEALTH	HHS
 DAMS	DHS (CISA)	 INFORMATION TECHNOLOGY	DHS (CISA)
 DEFENSE INDUSTRIAL BASE	DOD	 NUCLEAR REACTORS, MATERIALS AND WASTE	DHS (CISA)
 EMERGENCY SERVICES	DHS (CISA)	 TRANSPORTATIONS SYSTEMS	DOT & DHS
 ENERGY	DOE	 WATER	EPA



CISA
CYBER+INFRASTRUCTURE

Michael A. Dailey

July 16, 2019

U.S. Transportation Sector and Its Subsectors



TRANSPORTATIONS
SYSTEMS

DOT & DHS

- **Aviation**
- **Highway Infrastructure and Motor Carrier**
- **Maritime Transportation Systems**
- **Mass Transit and Passenger Rail**
- **Pipeline Systems**
- **Freight Rail**
- **Postal and shipping**



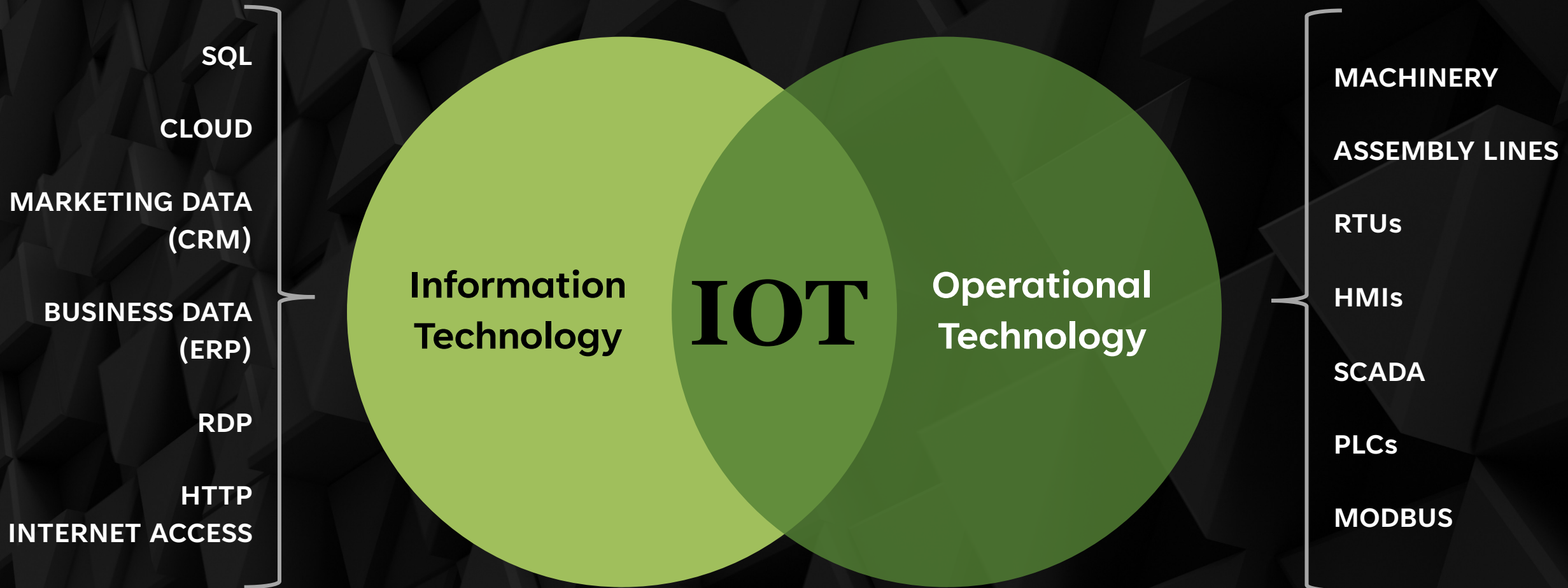
Analog vs Semi-Digital vs Digital



Odometers accurately count miles through a system of gears. STEPHANHOEROLD / GETTY IMAGES



The Ever-Evolving World of Technology



Evolving Risks and Threats

- Ransomware attacks **38%**
- Data-related threats **30%**
- Malware **17%**

- Denial-of-Service **DoS**
- Phishing / spear phishing **10%**
- Supply-chain attacks **10%**

Cybersecurity – Major Incidents

AVIATION

September 2022 | Breached American Airlines email accounts were abused for phishing purposes

MARITIME

June 2021 | Massachusetts Steamship Authority targeted in a cyberattack

September 2021 | Port Houston was targeted by a suspected nation-state actor in cyberattack

RAILWAY

January 2021 | A ransomware attack hit the short line rail operator OmniTRAX

April 2021 | Suspected Chinese hackers breached the New York City Transit Authority's computers

Cybersecurity – Major Incidents (Continued)

ROAD

June 2021 | Cape Cod Regional Transit Authority was hit by ransomware attack

September 2021 | Elon Musk's top-secret "full self-driving" AI car software was leaked to hackers

December 2021 | Kia Motors America was hit by a DoppelPaymer ransomware attack

June 2022 | American subsidiary of automotive hose maker Nichirin was hit by a ransomware attack

TRANSPORT SECTOR AS A WHOLE ("All transport")

September 2021 | Attackers impersonated the US Department of Transportation in a two-day phishing scam

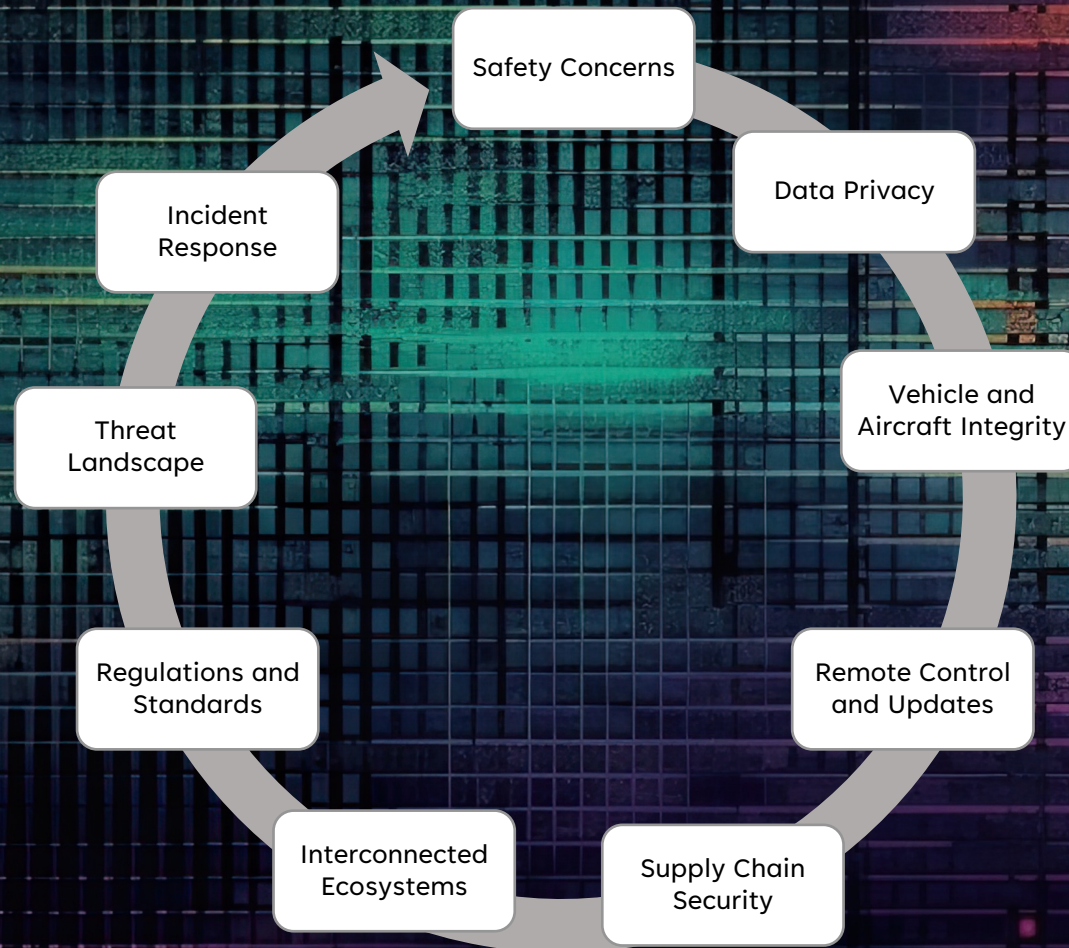
September 2022 | Microsoft365 phishing attacks impersonate US government agencies, including the Department of Transportation

Cybersecurity – Major Incidents (Organization)

Industry	Incidents				Breaches			
	Total	Small (1–1,000)	Large (1,000+)	Unknown	Total	Small (1–1,000)	Large (1,000+)	Unknown
Total	16,312	694	489	15,129	5,199	376	223	4,600
Accommodation (72)	254	4	2	248	68	4	1	63
Administrative (56)	38	8	14	16	32	8	11	13
Agriculture (11)	66	1	5	60	33	0	3	30
Construction (23)	87	7	1	79	66	4	1	61
Education (61)	496	63	15	418	238	28	8	202
Entertainment (71)	432	13	3	416	93	10	1	82
Finance (52)	1,829	70	30	1,729	477	38	18	421
Healthcare (62)	522	28	15	479	433	23	15	395
Information (51)	2,105	45	110	1,950	380	23	19	338
Management (55)	9	1	0	8	9	1	0	8
Manufacturing (31–33)	1,814	37	24	1,753	259	18	15	226
Mining (21)	25	2	0	23	13	2	0	11
Other Services (81)	143	7	2	134	100	6	1	93
Professional (54)	1,396	176	54	1,166	421	85	32	304
Public Administration (92)	3,270	87	110	3,073	582	48	39	495
Real Estate (53)	83	15	5	63	59	10	2	47
Retail (44–45)	404	62	44	298	191	33	28	130
Transportation (48–49)	349	13	25	311	106	8	13	85
Utilities (22)	117	12	6	99	33	3	3	27
Wholesale Trade (42)	96	42	22	32	53	23	11	19
Unknown	2,777	1	2	2,774	1,553	1	2	1,550
Total	16,312	694	489	15,129	5,199	376	223	4,600

Table 2. Number of security incidents and breaches by victim industry and organization size

Cybersecurity – A Critical Linchpin



Human Factor



**Training and
Education**



User Awareness



**Behavioral
Aspects**



Security Culture



**Adaptation to
New
Technologies**

What is the NIST Cybersecurity Framework (CSF)?

A highly detailed and structured framework of standards, guidelines, and best practices that provides a way to identify, protect, detect, respond, and recover from vulnerabilities cyberthreats or breaches.





Roadmap to Resiliency

Assessment & Awareness

Implementation & Protection

Education & Culture

Incident Response Testing



Q&A

Nth is Here to Help!

Request a Deep Dive, POC/POV,
Assessment, or Demo:

- ✓ Scan the QR code with your camera
- ✓ Check the box with the Nth
Evaluation that will best assist you

