

tescometering.com

# CYBER SECURITY

## Standards and Securing Your Data

*TESCO's Meter School*

**TESCOOL** ▶▶

*July 24, 2024*

11AM – 12 PM

Alex Kobrenko

## Top 10 biggest breaches in the USA

	Organization name	Sector	Known number of records breached	Month
1	Discord (via Spy.pet)	IT services and software	4,186,879,104	April 2024
2	Real Estate Wealth Network	Construction and real estate	1,523,776,691	December 2023
3	Zenlayer	Telecoms	384,658,212	February 2024
4	Pure Incubation Ventures	Professional services	183,754,481	February 2024
5	916 Google Firebase websites	Multiple	124,605,664	March 2024
6	Comcast Cable Communications, LLC (Xfinity)	Telecoms	35,879,455	December 2023
7	VF Corporation	Retail	35,500,000	December 2023
8	iSharingSoft	IT services and software	>35,000,000	April 2024
9	loanDepot	Finance	16,924,071	January 2024
10	Trello	IT services and software	15,115,516	January 2024



tescometering.com

# CYBER SECURITY

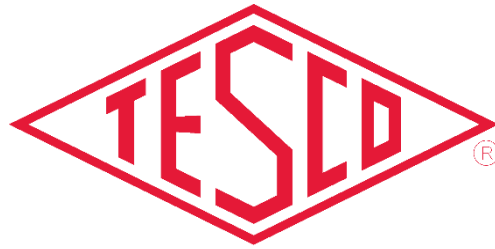
---

- Cyber standards : ISO 27001, NIST 800-53r3, SOC 2
- Knowing your organizations risks
- Backup and Recovery
- Reducing cyber risk with tools
- Identifying attack vectors for your organization
- Patch Management
- Securing IOT and SCADA
- Security first mindset
- Staying informed with latest threats

# CYBER SECURITY STANDARDS

---

- NIST 800-53r3
- ISO 27001
- SOC 1 – 3
- PCI
- GDPR
- UL 2900
- NIST CSF
- CISA Mandates
  - - Coop And Cyber Insurance
- CIRCIA – Passed 2022, requires CISA to develop and publish rules for companies that provide critical infrastructure.



tescometering.com

# PROTECTING YOUR DATA

Knowing what kind  
of data you store,  
how its collected and  
accessed.

- Definition: Protecting digital data from unauthorized access, corruption or theft
- Needed to safeguard sensitive information, maintaining privacy, and ensuring regulatory compliance

# BACKUP AND RECOVERY

---

- How often can you take backups
- Local backups
- Off-Site backups
- Type of Backups
- Off-Line Backups
- Encryption
- How long can we afford to be down
- How long will it take to recover your data
- Where will you recover to

# KNOWING YOUR RISKS

---

- What kind of data is stored
- Who is accessing your data
- What methods are used to secure access to data or resources
- Open incoming firewall ports
- Web / SFTP / public facing servers
- Data Exchange



# IDENTIFYING ATTACK VECTORS

---

- Pen Testing
- Email
- Endpoint Scanners
- End User
- Vendors
- Endpoints
- Exposed SCADA

- Get a baseline of devices
- Assign Responsibilities
- Patch Testing
- Maintain Update Schedule
- Software Standardization
- CVE – Critical Vulnerability and Exposure

- Firewalls
- Anti-Virus , EDR , XDR
- RMM
- 2fa whenever possible
- Pen Testing
- Nessus Scanner
- [cisa.gov](https://cisa.gov)
- [haveibeenpwned.com](https://haveibeenpwned.com)