Top 10 Cybersecurity Best Practices

Welcome to the Human Side of Tech

When developing your cybersecurity strategy, determining where to start or what to do next is not always clear. Along with increasingly complex regulatory requirements, identifying an approach that is proportional to the needs of your organization is a common concern that we hear time and time again.

That is why we have compiled a list of the ten best practices that every organization, regardless of size or industry, should implement to ensure their network and data are protected. Whether you handle cybersecurity in-house or work with a trusted advisor, use this list to evalute your current cybersecurity program and identify gaps in your strategy.

Cybersecurity Checklist

- ☐ **Conduct a Cybersecurity Assessment**
  Create a baseline to measure your progress over time.
- ☐ **Perform Penetration Testing**
  Are the security controls you implemented working correctly?
- ☐ **Actively Monitor Your Networks**
  Identify suspicious activity on your devices in real time.
- ☐ **Have a Written Incident Response Plan (IRP)**
  Make decisions ahead of time rather than in the midst of a crisis.
- ☐ **Understand Your Compliance Requirements**
  This is determined by the types of data you hold and your industry.
- ☐ **Train Employees**
  Incorporate training during onboarding and throughout the year.
- ☐ **Perform a Data Audit**
  You can't protect what you don't know you have.
- ☐ **Perform an Account Audit**
  Identify unknown accounts or change in permissions more easily.
- ☐ **Initiate a Patch Management Program**
  Don't rely on employees to patch their computers individually.
- ☐ **Backup Data**
  Keep a copy offline and test your backups regularly.

Getting Started

As you review your cybersecurity strategy, check the boxes next to the items you are currently doing. Not sure what one of the items entails? Click on it to visit our blog for more details.

The TCDI Difference

TCDI has helped organizations gain peace of mind in our digital world for over three decades. As a trusted advisor, we pride ourselves on delivering holistic solutions to meet our client's needs.

TCDI's experts provide incident response and investigative services, penetration testing, threat detection and prevention, computer forensics, and other vital services to protect the confidentiality, integrity, and availability of client data and critical systems. TCDI is unique in that it is a hybrid organization: one division dedicated to cybersecurity and computer forensics, and the other on developing software focused on eDiscovery and litigation management with distinct data privacy and security concerns.