Cybersecurity & Forensics

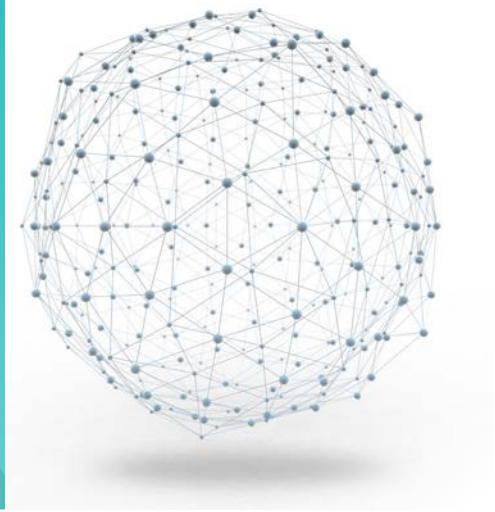
tcdi

www.tcdi.com

Table of Contents

Copyright © 2020 TCDI All Rights Reserved.

Our Story



For 30 years, TCDI has been a pioneer in the technology industry by empowering organizations to secure, discover, analyze and defend critical data as part of our legal services practice. We learned early that data security, data privacy and compliance are critical in our business, so we invested heavily on it, spending early and often. Investment in our own privacy and security led us to realize other small to medium size businesses could benefit from what we've learned over the years so we formed our Cyber division.

We take an innovative approach to data security services by combining "best of breed" technology with our proprietary cybersecurity assessment application. Our staff of trusted advisors, comprised of security experts and industry thought leaders, create custom tailored solutions to meet our client's unique needs.

We understand the importance of data security and privacy, and apply advanced security techniques as a standard throughout our organization. Our specialized cybersecurity team perform penetration testing, cybersecurity assessments, and other vital services to protect the confidentiality, integrity and availability of client data and critical systems.

Trusted with more than 1.7 petabytes of data in our on-site Tier 3 datacenter, 500 leading corporations and law firms rely on TCDI's services and solutions on a daily basis. Lean Six Sigma certified process experts account for over 70% of our team and allow us to help our clients through a unique focus on innovation, quality, and continuous process improvement.

Next Page
General Overview

General Overview

TCDI's services and solutions reflect our best practice approach from design through execution, and we have a 30-year proven record of efficiently working hand in hand with our clients.

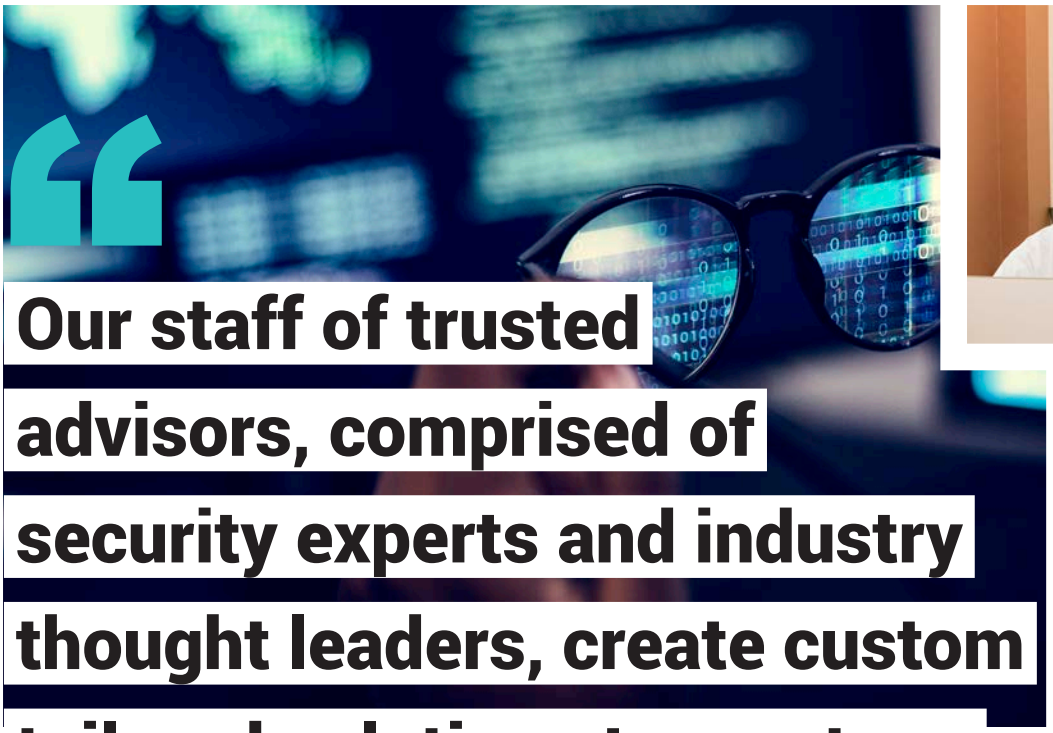
Our Philosophy

Our client driven culture is a result of our philosophy to grow alongside with our client's initiatives.

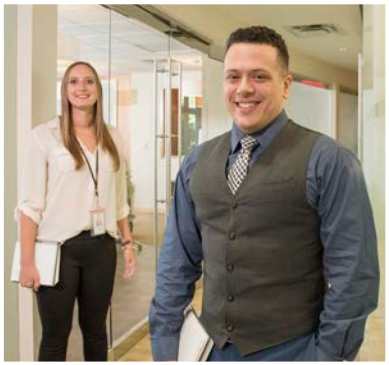
TCDI has unparalleled experience in cybersecurity and computer forensics. Our service offerings are the result of our commitment to providing cutting edge technology that is administered by industry leading experts. As a result, clients receive the best possible service from their trusted advisor.

In addition to our technical expertise, we are dedicated to superior project management and unparalleled customer service. Our team includes professionals with extensive subject matter expertise and thought leadership who operate with a clear understanding of the client's voice in everything we do. It's the experience our team brings that reinforces our client's sentiment that we are not only working in sync with them, but are an extension of their team. We know that if we take care of our clients, everything else will take care of itself.

That is the TCDI way.



Our staff of trusted advisors, comprised of security experts and industry thought leaders, create custom tailored solutions to meet our client's unique needs.



Next Page
Our Services

Our Services

Penetration Testing

Discover internal and external vulnerabilities through a simulated cyber-attack by highly-skilled experts using "best of breed" tools and technology.

Cybersecurity Assessment

Evaluate your company's security and privacy against a set of globally recognized standards and best practices.

CyberPulse 365

Implement a comprehensive security monitoring and management platform utilizing industry leading technology administered by cybersecurity experts.

Virtual CISO

Gain access to a team of certified and highly skilled cybersecurity experts on an "as-needed" basis for a fraction of the cost of a full-time resource.

SecureManagement 365

SecureManagement 365 offers a simplified, cost-effective cybersecurity program for small to mid-size firms to evolve and improve their data privacy.

Data Breach & Investigative Services

Bring in a team experienced in digital forensics and incident response to investigate, contain and remediate a data breach.

Computer Forensics

Whether relevant data is contained on a laptop, server, cell phone or other device, our certified forensic analysts follow forensic methodologies and procedures to collect electronic evidence.

Our Team

Expertise

In-depth knowledge and continuing education are important, especially in the rapidly changing field of cybersecurity and computer forensics. Our industry leading certifications such as Certified Information Systems Security Professional (CISSP) and Certified Forensic Analyst (GCFA) reflect our dedication to providing high quality service.

Collaborative Approach

Cybersecurity, computer forensics, and eDiscovery projects require effective planning and communication. Our team is dedicated to working closely with clients to identify their specific needs and deliver customized results.

Experience

TCDI has the optimal blend of legal, technical, and compliance professionals who have helped hundreds of clients navigate through security audits, incident response matters, and other projects involving electronically stored information.

Responsive Service

When responding to a data breach or assisting clients with legal matters involving electronically stored information, time is of the essence. Our team of experts are responsive to even the most urgent requests.

Testimony

Validation of digital evidence is an integral part of our services and we are adept at providing expert testimony to verify authenticity.

Next Page
Why Cybersecurity?

Why Cybersecurity?

There are risks and costs to a program of action - but they are far less than the long range cost of comfortable inaction.

- John F. Kennedy

$3,100,000

The average cost to small and medium-sized businesses due to cyber-attacks in 2019[1].

The most expensive component of a cyber-attack is information loss, which represents 43% of costs[2].

- **7,125,940** records lost or stolen **every day**
- **296,914** records **every hour**
- **4,949** records **every minute**
- **82** records **every second**[4]

[1] Ponemon Institute (2019). 2019 State of Cybersecurity in Small & Medium-Sized Businesses (SMB). Ponemon Institute LLC.
[2] Ponemon Institute (2017). 2017 Cost of Cyber Crime Study. Traverse City, MI. Ponemon Institute LLC.
[3] Verizon (2017). 2017 Data Breach Investigations Report. Verizon.
[4] Gemalto. "Data Breach Statistics by Year, Industry, More." Breach Level Index, breachlevelindex.com/.

“An investment in knowledge always pays the best interest.”
– Benjamin Franklin

Penetration Testing

Discover internal and external vulnerabilities through a simulated cyber-attack by highly-skilled experts using “best of breed” tools and technology.

Penetration testing helps answer the question, “how effective are my computers, network, people, and physical security at deterring a highly motivated and skilled hacker?”

A pen test is a simulated cyber attack that offers unparalleled insight into an organization’s data security effectiveness. During the test, security vulnerabilities are identified and attempts are made to compromise systems and gain unauthorized access to data. At the conclusion of the test, TCDI provides a written report summarizing the vulnerabilities identified, threat level, and suggested remediation steps.

Our goal is to identify systems that exhibit known vulnerabilities, weak configurations, or out-of-date software, and to measure the impact of those vulnerabilities on the network as a whole. Our engineers routinely write custom attack programs, or modify existing techniques to take advantage of security conditions that are unique to a given customer environment.

Penetration tests offer unparalleled insight into an organization’s security effectiveness as well as a road map for enhancing security. By hiring experts to simulate a cyber attack, vulnerabilities can be identified and corrected before they are exploited by a hacker or malicious insider.

External Pen Test
Addresses the ability of a hacker to gain access to the internal network from outside the firewall by exploiting internet-facing systems.

Internal Pen Test
Analyzes an attack from inside the firewall by an authorized user or hacker who has gained access to the network.

Wireless Pen Test
Reveals vulnerabilities on wireless networks that may allow unauthorized access to data and systems.

Social Engineering
Tests how well your “human network” defends against attacks such as phishing emails.

Next Page
Cybersecurity Assessment

Cybersecurity Assessment

Evaluate your company's security and privacy against a set of globally recognized standards and best practices. Areas covered include access controls, security governance, business continuity, application security, and more.

The Problem:

Companies are faced with ever confusing and complex regulatory requirements, security certifications and other standards that are simply not reasonable when applied to small or medium sized companies.

The Solution:

The TCDI Cybersecurity Assessment is a proportional and reasonable assessment that evaluates a company's security and privacy against a set of globally recognized standards and best practices. Recommendations and requirements from standards are mapped into a single set of objectives, avoiding the cost, complexity, and redundancy of multiple independent assessments.

The Cybersecurity Assessment matches the objectives of:

+ **NIST SP800-53**
+ **NIST SP800-171**
+ **ISO/IEC 27001**
+ **COBIT**
+ **AICPA Trust Service Criteria used in SOC Audits**

As well as regulatory objectives from:

+ **HIPAA/HITECH Omnibus Rule**
+ **PCI DSS**
+ **GDPR**
+ **FISMA, FERPA, and ITAR**

FIRST
Access Controls

+ Do you know everyone who has access to your systems?
+ How would you know if an unauthorized person accessed sensitive data?

SECOND
Business Continuity

+ Are you certain that you can recover from an unexpected loss?

THIRD
Application Security

+ Have your applications been tested from a security viewpoint?

FOURTH
Security Governance

+ How does your management team make and implement decisions about information security?

A cybersecurity assessment can be used to validate adherence to relevant standards and provides an easy to understand, prioritized road map for enhancing data privacy and security.

Next Page
CyberPulse 365
Managed Security Services

- Ken Poirot

CyberPulse 365
Managed Security Services

CyberPulse 365 helps companies proactively detect and defend against cyber threats with best of breed technology administered by TCDI's team of security experts.

The managed service combines security information and event management (SIEM), vulnerability scanning, endpoint protection, and data loss prevention technologies to provide a holistic threat management and monitoring solution.

CyberPulse provides organizations access to cybersecurity experts and cutting edge technology for a fraction of the cost of an in-house solution.

CyberPulse 365 is powered by SecureOwl, a cutting-edge security appliance that is installed onsite and administered remotely by the engineers in TCDI's Security Operations Center (SOC).

1

Cybersecurity Monitoring

The SecureOwl appliance collects log files from devices on your network including servers, workstations, switches, routers, firewalls, and storage devices. It then encrypts and sends the information to TCDI for analysis.

SECUREOWL

SecureOwl delivers multiple security functions including monitoring, detection, control, and protection.

2

Threat Detection

Events are analyzed in real-time and suspicious activity generates alerts that TCDI's CyberOps team reviews to determine if action is necessary and, if so, clients are contacted with remediation advice.

4

Vulnerability Management

TCDI will scan client networks monthly and deliver a list of vulnerabilities and prioritized remediation actions. Vulnerability scanning can be performed externally to test internet facing servers or internally to test workstations and servers within the organization.

3

Malware Protection

CyberPulse 365's advanced malware protection combines endpoint protection, centralized monitoring, rapid virus definition deployment, and access to incident response and malware sandboxing services to provide a powerful defense against an attack.

5

Data Loss Prevention (DLP)

Data loss prevention (DLP) policies are enforced across devices to control how data is used, stored, and transmitted. Some actions may trigger an alert while others are prevented, thus stopping data from traversing to unauthorized cloud services, external devices, or unknown email recipients.

Next Page
Chief Information Security Officer On-Demand

Chief Information Security Officer On-Demand

Benefits Include:

- + Data security peace of mind
- + Lower cost than a full- time employee
- + Readily available on demand
- + Access to sophisticated tools and subject matter expertise
- + Knowledge of the latest threats, laws, and guidelines
- + Objective third-party advice

Security is important for every organization but not every organization can afford to recruit, hire, and retain a cybersecurity expert. Our team is available "on-demand" to serve as trusted advisors who can fulfill your organization's data security needs.

Although everyone in an organization has at least some level of responsibility for data security, it is important to have someone in charge of and responsible for data security at your organization. This person should steward a secure information culture embedded in the organization's strategy, with a focus on continuous improvement. Hiring a full-time employee for this role, however, may not make sense.

A full-time Chief Security & Privacy Officer can be expensive, difficult to recruit, and hard to retain. The On-Demand Chief Information Security Officer does the same job as a traditional employee but with one difference: they are a part-time resource. As a result, you can secure your organization for a fraction of the cost.

3.5 Million cybersecurity positions will go unfilled in 2021[5]

70% of organizations say their security risk increased significantly in 2017[6]

2 out of 3 organizations do not believe they have adequate resources to manage security effectively[7]

[5] Morgan, Steve. "Cybersecurity Jobs Report 2018-2021." Cybersecurity Ventures, https://cybersecurityventures.com/jobs/.
[6] Ponemon Institute (2017). 2017 Cost of Data Breach Study: Global Overview. Traverse City, MI. Ponemon Institute LLC.
[7] Ponemon Institute (2017). The 2017 State of Endpoint Security Risk. Ponemon Institute LLC.

SecureManagement 365

Companies in every industry are entrusted with their clients' most sensitive information and have an ethical obligation to protect it. In today's digital world, that means ensuring technical and procedural safeguards are in place to prevent data breaches. Failure to do so can result in catastrophic damage to a firm's reputation and bottom line.

SecureManagement 365 from TCDI is a service that helps small and medium sized firms take reasonable steps to safeguard confidential information. SecureManagement 365 evaluates a firm's current state of cybersecurity from a variety of angles, including people, processes, and technology, in order to develop an action plan for improving data privacy.

Why TCDI?
TCDI has a deep understanding of a the strict data privacy obligations of a business because we too must adhere to them. As a trusted partner for large and complex litigation matters, our clients require the highest security standards.

Value

+ Gain access to cybersecurity thought leaders and industry-leading tools at an affordable price.
+ Get a holistic view of your current security posture and understand your exposure.
+ Develop a prioritized action plan for enhancing data privacy practices.
+ Work side-by-side with our experts on implementing your cybersecurity action plan.
+ Simplify the process of responding to vendor risk assessment questionnaires.
+ Verify to external stakeholders that your firm is proactively safeguarding confidential information.

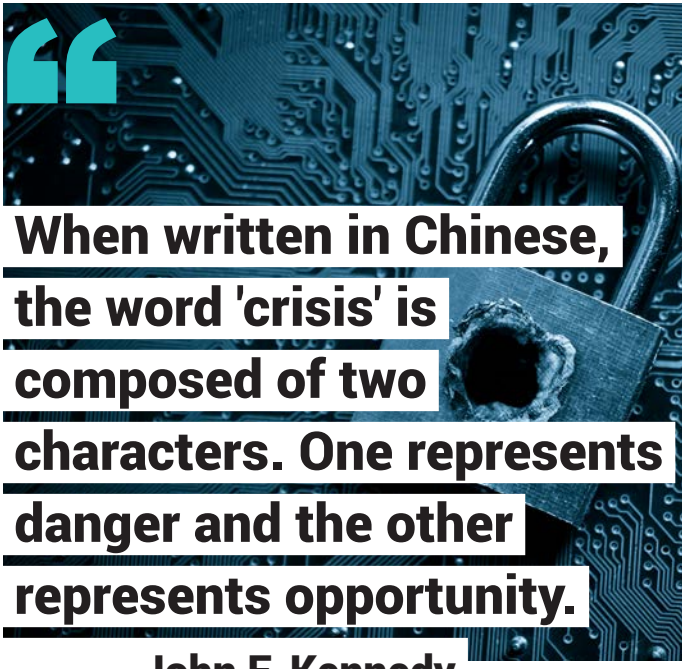
Service Description
SecureManagement 365 is comprised of the following bundled services:

+ Cybersecurity assessment
+ Penetration testing and/or vulnerability scanning
+ Managed social engineering (email phishing) tests
+ Automated security awareness program
+ Chief Information Security Officer On-Demand

Next Page
Data Breach Response and Investigative Services

Data Breach Response and Investigative Services

Bring in a team experienced in computer forensics and incident response to investigate, contain and remediate a data breach. Ready at a moment's notice, our experts will forensically preserve evidence and perform an analysis in our secure sandbox environment to uncover important facts regarding the incident.



Responding to a Data Breach

Time is of the essence when responding to a data breach, because every second counts when systems are compromised and a company's reputation is on the line.

How an organization responds to a data breach will speak volumes. Depending on the severity, it will be analyzed and scrutinized by many parties including regulators, lawyers, management, customers, and other stakeholders. They will not only want to know how and why the breach occurred, but also the steps that were taken to gather evidence, determine the scope, secure compromised systems, and notify those who were affected.

Organizations in the midst of a data breach may be well-advised to seek the assistance of a trusted partner who has the tools, expertise, and responsiveness to investigate and contain the breach and implement safeguards to defend against another attack.

Computer Forensics

In today's world, evidence is rarely preserved on paper. Security isn't compromised at the back door but at the firewall. The good news is electronic data often leaves a deeper trail than paper. You just have to know how to collect digital evidence and recover data. And we do. In fact, we specialize in computer forensics.

Computer forensics is useful in a variety of litigation matters, corporate investigations, and incident response.

Whether relevant data is contained on a laptop, server, cell phone or other device, our certified forensic analysts are trained to collect and analyze electronic evidence following forensic methodologies and procedures. Computer forensics can prove invaluable in numerous situations, including:

+ Theft of intellectual property
+ Preservation orders
+ Employment issues
+ Fraud or embezzlement
+ Divorce
+ Loss of data
+ Inappropriate computer usage
+ Data breaches

Cell Phone Forensics

Text messages, voicemail, call logs, device location, and internet browsing history

Social Media Discovery

Supported platforms include, but are not limited to, Facebook, Twitter, Instagram and YouTube

Employee Data Theft Investigations

Occurs most frequently just prior to, or immediately after, an individual's termination or resignation from an organization

The best time to plant a tree was 20 years ago.
The second best time is now.
-Chinese Proverb

Maybe you don’t know where to start with a cyber strategy or maybe you've had one all along.

Either way, we’d love to talk.

tcdi

4508 Weybridge Lane | Greensboro, NC 27407 | 336.232.5800
1375 Euclid Avenue - Ste 400 | Cleveland, OH 44115 | 216.664.1100