
# ERMProtect

Cybersecurity Solutions

www.ermprotect.com

ERMProtect
Cybersecurity Solutions

# ERMPROTECT: YOUR TRUSTED IT PARTNER

ERMProtect helps organizations fight back against cyberthreats and cryptocurrency fraud with a powerful arsenal of solutions to mitigate legal, regulatory and reputational risk.

We rigorously test the security of IT systems, as if we were hackers ourselves. We ensure compliance with data privacy laws and standards to reduce regulatory risk. We help fix what's broken and, if trouble comes, deploy powerful forensics.

We even tackle the human side of IT security, by training employees to recognize when they are being targeted through our proprietary ERMProtect e-learning platform.

## WHY 400+ COMPANIES HAVE PICKED US

### Experience

Our company has been in the field fighting and remediating cyber threats for more than 20 years, since the company's founding in 1998. We have a 90 percent client retention rate, which we think says it all.

### Expertise

We employ top-in-field professionals who have overseen IT security at major enterprises, such as Assurant Solutions, Diageo and General Growth Partners. Our executives are all former professionals at the Big 4 or top-tier consulting firms.

### Certifications

We don't just say we're good: We back it up. Our firm has earned coveted industry certifications, such as PCI QSA and PCI PFI. Our professionals are required to maintain high-level certifications in relevant fields.

### Trusted by Big Brands

Our clients include multiple Fortune 500 companies. We started small with them to prove ourselves, and they keep coming back. We've proven again and again that a boutique can deliver top quality at a reasonable rate.

### Compliance Expertise

We're not just an IT security company, we're an IT security company that knows data regulatory requirements inside and out. We identify gaps in IT security compliance and help clients shore up defenses.

| 35+ | 5,000+ | 4,000+ | 24 |
|---|---|---|---|
| **Industries Served** | **Pen Tests Performed** | **Security Assessments Performed** | **Years in Business** |

*"Our integrity is our No. 1 value. That, and client loyalty, drive everything we do."*

**— Silka Gonzalez**, Founder and President, ERMProtect



305-447-6750 | info@ermprotect.com | **https://ermprotect.com**

ERMProtect
Cybersecurity Solutions

# VULNERABILITY AND PENETRATION TESTING

## What We Do

**Our team of ethical hackers identifies whether your organization's sensitive information is vulnerable and details how to fix gaps. We also conduct tests required to demonstrate compliance with data laws, regulations and standards.**

## SERVICES

### Network Penetration Tests

The External Network Penetration Test simulates real-life hacker attacks at a network level, in a scenario where the hacker is located outside the organization and its internal network. The Internal Network Penetration Test simulates real-life hacker attacks at a network level, in a scenario where the hacker is located inside the organization, connected to its internal network.

### Web / Mobile Application Tests

Online portals, mobile applications and websites enable a significant number of critical data exchanges and transactions. Penetration tests reveal security gaps and whether hackers could successfully penetrate an application's defenses.

### Wireless Network Penetration Tests

A Wireless Network Penetration Test simulates attacks on an organization's wireless network, in a scenario where the hacker is within the range of the wireless network. The test provides insights into how well-protected the organization's wireless networks are from hackers and malicious individuals.

### Regulatory Compliance Penetration Testing

Organizations that maintain sensitive data are regulated by data laws and standards that require periodic and ongoing penetration tests. Our team helps organizations achieve compliance objectives by performing penetration tests completely tailored to the specific requirements of applicable laws, regulations and standards.

### Social Engineering Tests

An organization's technical cybersecurity mechanisms can be rendered useless by just one employee clicking on the wrong link. These tests simulate hacker attacks aimed at people so that organizations can evaluate the security awareness levels of their employees and understand how well they are able to protect organizational information and resources.


305-447-6750 | info@ermprotect.com | https://ermprotect.com

## Cloud Infrastructure Penetration Testing

Tests of Cloud Infrastructure identify vulnerabilities, misconfigurations, and implementation flaws. We test both publicly available and privately held systems which are hosted within a cloud environment.

## ICS/SCADA Penetration Testing

ICS/SCADA Penetration Tests target the Industrial Control Systems (ICS) or the Supervisory Control and Data Acquisition (SCADA) systems within an organization. Our tests are fully aligned with the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) requirements.

## Physical Site Penetration Testing

Sensitive data can be compromised by physical break-ins and theft. Testing an organization's physical defenses and security helps ensure data can't be exploited through these means.

## IoT Penetration Testing

The Internet of Things is the network of devices, such as vehicles and home appliances, that can connect, interact and exchange data. Our ethical hackers identify vulnerabilities within IoT infrastructures that could lead to a data breach or malicious attack.

## Network Scanning

External Network Scans are automated, tool-based probes of an organization's network from an external perspective. Internal Network Scans are automated, tool-based probes of an organization's network from an internal perspective.

ERMProtect
Cybersecurity Solutions

# PCI COMPLIANCE SERVICES

## What We Do

**Entities that store, process or transmit credit card data must comply with the Payment Card Industry Data Security Standard, and conduct forensic investigations of data breaches. Our certified PCI QSA experts help ensure compliance. Our certified PCI PFI investigators conduct PCI-compliant investigations of data breaches.**


## SERVICES

### PCI DSS Network Scans

We provide PCI DSS required quarterly network vulnerability scans to help organizations maintain compliance.

### PCI DSS Penetration Tests

We perform highly technical and detailed penetration tests mandated by the PCI DSS.

### PCI QSA Security Audits

As a certified Qualified Security Assessor (QSA), ERMProtect audits for compliance with PCI DSS and awards a Report on Compliance (ROC) and an Attestation of Compliance (AOC) to organizations who fully comply.

### PCI DSS Gap Analysis

A PCI DSS gap analysis is a crucial step toward achieving compliance. ERMProtect's gap analysis involves a meticulous review of the organization's cardholder data environment in scope, which is then mapped against PCI DSS requirements to identify gaps.

### PCI DSS Remediation

ERMProtect provides remediation support and guidance to help organizations implement a fully-compliant cardholder data environment and infrastructure.

### PCI SAQ Assistance

Many merchants and service providers are required by PCI DSS to complete a Self-Assessment Questionnaire (SAQ). We identify the type of SAQ that applies to organizations and help them complete it accurately in order to maintain PCI DSS compliance.

### PCI Digital Forensics

Following a cyberattack, PCI DSS requires an investigation by a PCI-certified Forensic Investigator. Our experts perform these complex, challenging and highly specialized digital forensic investigations.


305-447-6750 | info@ermprotect.com | https://ermprotect.com

# DATA BREACH INVESTIGATIONS & DIGITAL FORENSICS

## What We Do

**In the event of a breach, our seasoned security experts respond quickly to contain, investigate and recover from the breach. In cases of misconduct, fraud and litigation, our forensic specialists find critical information, analyze it and report back with actionable findings.**

## SERVICES

### Data Breach Investigations & Remediation

The ERMProtect team provides on-demand incident response to cyberattacks. Our digital forensic experts help organizations to contain, investigate and recover from breaches. All digital evidence is acquired and preserved in a manner that is admissible in a court of law. Post-breach, our cyber experts spell out specific steps to shore up defenses.

### Digital Forensics

A treasure trove of evidence resides on computers, digital and mobile devices. Our forensic team is trained and certified to use the latest tools to find and preserve evidence within the appropriate legal frameworks. Our team includes veteran investigators who have managed complex, franchise-stakes investigations.

### PCI PFI Data Breach Investigations

As a certified PCI PFI company, ERMProtect is one of a handful of firms certified globally to conduct PCI-compliant investigations of credit card data breaches. We investigate, help contain the breach and report findings to the Payment Card brands and PCI Council.

### Data Breach Response Plans

The success or failure of an attack depends heavily on the organization's incident response capabilities. We help organizations develop an Incident Response Plan that defines roles and responsibilities, spells out specific actions and establishes protocols for periodic tests and updates of the plan.

### Data Breach Vulnerability Testing

An organization's incident response capabilities must be tested periodically to ensure they address evolving threats. We perform live, simulated attacks, then work alongside the client to improve and update capabilities using table-top exercises and other techniques.


305-447-6750 | info@ermprotect.com | https://ermprotect.com

ERMProtect
Cybersecurity Solutions

# CRYPTO INVESTIGATIONS & COMPLIANCE

## What We Do

**We trace and analyze cryptocurrency transactions to investigate fraud, cyberattacks, theft, and other scams, frequently working alongside law enforcement or legal counsel. We also use our expertise to help financial institutions and businesses comply with blockchain-related regulations and laws.**

## SERVICES

### Crypto Forensic Investigations

We track, trace, and analyze crypto transactions to help law enforcement, regulators, lawyers, financial institutions, and businesses identify legitimate and illicit transactions.

### Ransomware Investigations

With expertise in both computer security and crypto forensics, we help organizations investigate ransomware attacks, identify attackers, and collaborate with legal counsel or law enforcement for prosecution and possible recovery of funds.

### Compliance

We help financial institutions implement Chainalysis, a proprietary crypto analysis software, to identify possibly illicit transactions and manage AML compliance issues. Our forensic investigators can also help financial institutions investigate fraud and other financial crimes.

### Government Agency Investigations

Our analysts help law enforcement, regulators, and government agencies identify entities behind nefarious crypto transactions so they can combat serious crimes, prosecute bad actors, and possibly recover funds.

### Chainalysis Product Sales

ERMProtect is an official reseller of Chainalysis Reactor, an investigation software that connects cryptocurrency transactions to real-world entities, so that organizations can understand their exposure to crypto, monitor transactions, combat crypto crime, and comply with regulatory guidance.

Chainalysis

Official Partners of Chainalysis, the world's most comprehensive cryptocurrency investigation and transaction monitoring solution.



305-447-6750 | info@ermprotect.com | https://ermprotect.com

ERMProtect
Cybersecurity Solutions

# CRYPTO INVESTIGATIONS & COMPLIANCE

# Chainalysis

## The Data Protection Platform that Lifts the Veil on Crypto Transactions

## FREQUENTLY ASKED QUESTIONS

### What is Chainalysis?

Chainalysis is the world's most comprehensive cryptocurrency investigation and transaction monitoring solution.

### How is Chainalysis used?

Chainalysis maps blockchain transactions to real- world entities so that financial institutions, government agencies, and cryptocurrency businesses can detect and investigate suspicious cryptocurrency activity.

Chainalysis also helps financial institutions understand their exposure to crypto, monitor ongoing customer activity, and comply with regulatory guidance.

### How does Chainalysis work?

Blockchain transactions are public. They can be mapped, analyzed, and clustered to link them to terrorist groups, sanctioned entities, darknet markets, ransomware actors, other illicit groups.

### What are the benefits?

- Uses the same compliance solutions trusted by the world's largest cryptocurrency businesses and banks.
- Uses the same technology trusted by U.S. federal law enforcement.
- Relies on the industry's largest and best data.
- Produces fully auditable findings that stand up in court.

### Can I get a demo?

ERMProtect is a Chainalysis investigative partner and product re-seller. Schedule a free demo of the product.

**REQUEST A DEMO**



305-447-6750 | info@ermprotect.com | https://ermprotect.com

ERMProtect
Cybersecurity Solutions

# SOC AUDITS AND READINESS

## What We Do

**Our team of CPAs and Information Security experts conduct SOC audits to identify whether an organization's IT security controls comply with a framework developed by The American Institute of Certified Public Accountants ("System and Organization Controls"). Organizations that achieve SOC compliance elevate client confidence and their position in the marketplace by demonstrating that they are effectively managing cyber risk.**

## SERVICES

### SOC 1 Assessments

These reports evaluate controls at service organizations and their impact on the financial statements of entities they serve. A Type 1 examination identifies if service providers have fairly described their controls. A Type 2 examination incorporates Type 1, plus examines whether the controls are operating effectively.

### SOC 2 Assessments

These reports provide detailed assurance about controls relevant to security, availability, and integrity of systems used to process users' data and the confidentiality of the information. These reports play an important role in supply chain risk management by identifying whether vendors are adequately protecting an organization's sensitive data. A Type 1 report examines management's description of systems and the suitability of the design of controls. A Type 2 examines incorporates Type 1 and provides an opinion on the operating effectiveness of controls.

### SOC 2 Readiness Assessments

We assess the security posture of organization's that store, process or manage confidential customer data to identify gaps that could cause the organization to fail a compliance audit. The scope does not include an assessment or opinion, as this is part of a SOC 2 examination, but gets organizations ready for an audit.

### SOC 3 Assessments

Like a SOC 2, these reports provide detailed assurance about controls relevant to security, availability, processing, integrity, confidentiality and privacy of systems that host confidential data. The main difference is that the SOC 3 report is stripped of details intended only for stakeholders and certain audiences. As such,

a SOC 3 can be made public and used to market products and services to the general public.

### SOC Plus + Assessments

A SOC Plus + examination modifies the scope of a SOC 2 examination to incorporate additional criteria of other regulations.

The scope, for example, could be expanded to include auditing for compliance with the Health Information Trust Alliance's (HITRUST) Common Security Framework (CSF) or the Cloud Security Alliance's (CSA's) Cloud Control Matrix (CCM). Additional regulations can also be defined.

### SOC for Cybersecurity

In a SOC for Cybersecurity examination, an assessment and an opinion are provided on the design and operating effectiveness of controls within a Cybersecurity Risk Management Program.

This Program is defined as the policies, procedures, and controls designed to protect information and systems from security events through the execution of timely detection, response, mitigation, and recovery activities.

Similar to a SOC 2 examination, a Type I or Type II can be performed, and one or more trust service principles and criteria can be included in scope. Also, similar to a SOC 2, a readiness assessment can be provided for the SOC Cybersecurity exam.

# GUIDE TO SOC

## What is SOC?

■ Many organizations and their third-party service providers are entrusted with sensitive and regulated data that, if breached, could compromise the security of customers.

■ A framework created by the American Institute of Certified Public Accountants (AICPA) enables CPAs and Information Security experts to review and formally comment on the adequacy of organizational controls pertaining to sensitive data.

■ This framework is known as "System and Organizational Controls" (SOC).

## Why is SOC Important?

■ Organizations that achieve SOC compliance elevate client confidence and their position in the marketplace by demonstrating that they are effectively managing cyber risk.

■ No matter what your business type or size, a SOC report can be a very powerful tool in establishing trust with current and prospective customers.

## Who needs a SOC?

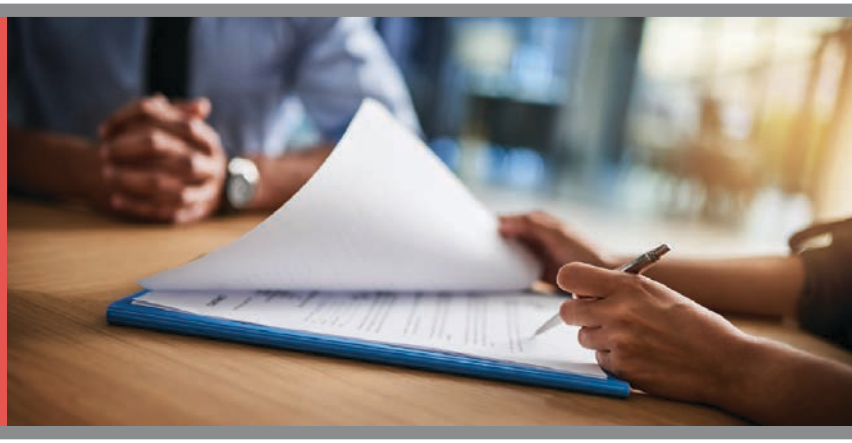
■ If your organization is collecting, processing, transmitting, or storing sensitive data, then your organization likely would benefit from a SOC.

ERMProtect
Cybersecurity Solutions

# REGULATORY COMPLIANCE SERVICES

## What We Do

**A host of local, state, federal and international laws regulate how organizations handle sensitive data. Our professionals perform a wide range of risk assessments and audit readiness assessments to help clients identify compliance gaps and close them.**



## SERVICES

### Privacy Laws Assessments & Strategy

We conduct gap analyses and remediation programs for compliance with laws including:

**CCPA -** The California Consumer Privacy Act (CCPA) enhances privacy rights and consumer protection for residents of California. The effective date is January 1, 2020, with a six-month delay in enforcement after that date.

**FACTA -** The Fair and Accurate Credit Transactions Act (FACTA) red flags rule requires financial institutions to demonstrate they have taken sufficient steps to protect consumers against identity theft.

**FERPA -** The Family Educational Rights and Privacy Act (FERPA) aims to protect the privacy of student education records and prevent unauthorized access to them. FERPA applies mainly to educational institutions.

**FISMA -** The Federal Information Security Management Act (FISMA) requires federal agencies to have a robust information protection plan in place. FISMA aims to help protect information held on federal information systems.

**GDPR -** The General Data Protection Regulation (GDPR) applies to all organizations that collect and process data that belongs to European Union (EU) citizens. The regulation has specific requirements related to privacy, security, data control, and governance.

**GLBA -** The Gramm-Leach Bliley Act (GLBA) is a U.S. federal regulation that requires financial institutions to ensure the confidentiality and integrity of the non-public personal information of their customers.

**HIPAA -** The Health Insurance Portability and Accountability Act (HIPAA) requires organizations dealing with Protected Health Information (PHI) and Electronic Protected Health Information (ePHI) to protect that data, and to require its business associates such as vendors to also comply.


305-447-6750 | info@ermprotect.com | https://ermprotect.com

**Sarbanes Oxley -** The Sarbanes Oxley Act of 2002 (SOX) has very specific stipulations and requirements related to information security and data governance that apply to all publicly held U.S. companies, international companies with SEC registered securities and to third-party firms that provide financial services to these companies such as CPAs.

**SEC Cybersecurity -** The Office of Compliance Inspections and Examinations (OCIE) and the U.S. Securities and Exchange Commission (SEC) conduct cybersecurity examinations that apply to financial institutions including investment advisors, investments companies, broker-dealers, transfer agents, and private fund advisors. We evaluate preparedness levels for the actual examinations and help organizations reach compliance-ready levels.

**State Cybersecurity Regulations -** All 50 states, the District of Columbia, Puerto Rico, Guam and the Virgin Islands have laws pertaining to data breaches and cybersecurity. Certain entities that operate in the state of New York must comply with that state›s latest cybersecurity regulation.

## Privacy Standards Assessments & Strategy

We conduct gap analyses and remediation programs for compliance with standards including:

**FFIEC -** Our experts perform an assessment and assist with remediation measures, so organizations meet cybersecurity standards set by The Federal Financial Institutions Examination Council.

**ISO27001 Gap Analysis -** We identify gaps in compliance with ISO27001, a framework for organizations to implement a standardized approach to information security.

**ISO27001 Certification -** We certify organizations that meet ISO27001 requirements, as demonstrated by detailed testing.

**NIST Gap Analysis -** We identify gaps in compliance with the National Institute of Standards and Technology (NIST).

**NIST Tests -** We perform highly specific NIST tests and assessments, followed by remediation.

**PCI QSA Gap Analysis -** We identify gaps in compliance with the Payment Card Industry Data Security Standard (PCI DSS).

**PCI QSA Security Audit -** A certified Quality Security Assessor (QSA), ERMProtect audits for compliance with requirements set by the PCI Council, and awards those who qualify with a Report of Compliance (ROC).

**PCI Network Scanning -** We provide quarterly network vulnerability scans required by PCI DSS.

**PCI Penetration Test –** We perform penetration tests required by PCI DSS.

ERMProtect
Cybersecurity Solutions

# COMPREHENSIVE ASSESSMENTS, REMEDIATION & IMPLEMENTATION

## What We Do

**Our team performs deep-dive assessments of the cybersecurity posture of organizations, their vendors and / or merger targets. We identify gaps, prioritize improvements and help implement solutions. These assessments can cover all aspects affecting data protection, including technical security, physical security and information-handling processes and procedures. Our suite of implementation and remediation solutions includes outsourcing and ongoing advisory services.**

## SERVICES

### Comprehensive Information Security Assessments

A Comprehensive Information Security Assessment is an in-depth technical examination of designs, configurations, documentation, processes and daily practices. The assessment covers all critical software and hardware, as well as physical and administrative procedures, implemented at your organization. This assessment is truly comprehensive and will provide an in-depth picture of the shape of your enterprise-wide cybersecurity and what you need to do to improve it.

### Security Risk Assessments

Security Risk Assessments analyze, identify and quantify an organization's risks, threats, and countermeasures related to its information assets. The goal is to initiate an ongoing process of identification, remediation, and prevention of cybersecurity issues. These assessments can help organizations with limited cybersecurity budgets prioritize where and how resources should be allocated to best protect information assets and infrastructure.

### Physical Security Assessments

Not all data breaches happen due to technical reasons. Old-fashioned theft and physical attacks can easily bypass sophisticated technical cybersecurity measures. Physical Security Assessments help evaluate your


305-447-6750 | info@ermprotect.com | https://ermprotect.com

organization's physical controls and security measures to provide insight into vulnerabilities.

## Vendor / Supply Chain Risk Assessments

Your vendors and supply chain providers present security risks that must be identified and managed. We help organizations implement a Cybersecurity Risk Management Program that identifies, classifies, monitors and manages vendor / supply chain risk on a consistent basis. Our periodic risk assessments use best-practice monitoring tools that align with ISO 27002, FFIEC, PCI, COBIT, the NIST Cybersecurity Framework HIPAA, GDPR and other regulations.

## Cybersecurity Advisory for Board Members

Board members charged with governance must make prudent decisions about an organization's cybersecurity posture. We work closely with board members to help them understand how to evaluate cybersecurity options within the context of budget, strategic plans and business impact.

## Information Security Implementation

We help organizations build cybersecurity from the ground up. We start from the very foundations of your organization's cybersecurity documentation and work up all the way to actual installation, configuration, and implementation of the principles of your cybersecurity program.

## Information Security Remediation

We help organizations with the often highly technical process of remediating issues identified during vulnerability testing. We assist the organization to implement changes and updates that improve IT security.

## CISO Outsourcing

For organizations that may be constrained by money or expertise, we offer a Chief Information Officer (CISO) level resource who designs, guides and supervises the in-house information security function in a results-oriented manner.

## Technical Audit Outsourcing

Organizations can outsource part or all of their internal technical audit function to our company.

ERMProtect
Cybersecurity Solutions

# EXPERIENCE BACKED BY TOP INDUSTRY CERTIFICATIONS

## Our Credentials

**Our firm and its professionals maintain top industry certifications in the fields of cybersecurity, payment card security, digital forensics, crypto forensics, data compliance, information strategy and investigations.**

### Firm Certifications

**PCI QSA –** Qualified Security Assessor (QSA) companies are independent security organizations that have been qualified by the Payment Card Industry Security Standards Council to validate an organization's compliance with PCI DSS.

**PCI PFI -** PCI Forensic Investigators (PFIs) identify the nature and scope of payment cardholder data breaches, verify containment, and document compliance gaps. ERMProtect is one of about 20 firms in the world with this certification.

**Chainanalysis -** The firm is an official investigative partner of Chainalysis, a comprehensive cryptocurrency investigation platform, and our professionals have earned advanced certifications to conduct crypto fraud investigations.

Chainalysis

PCI Security Standards Council™

### Staff Certifications

- Certified Chief Information Security Officer (C/CISO)
- Certified Business Continuity Professional (CBCP)
- Certified Business Manager (CBM)
- Certified Computer Forensics Examiner (CCFE)
- Certified Computing Professional (CCP)
- Certified Ethical Hacker (CEH)
- Certified Fraud Examiner (CFE)
- Certified Internal Auditor (CIA)


305-447-6750 | info@ermprotect.com | https://ermprotect.com

- Chainalysis Cryptocurrency Reactor Certification (CCRC)
- Certified Informational Privacy Professional (CIPP)
- Certified Information Privacy Manager (CIPM)
- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
- Certified Information Systems Security Professional (CISSP)
- Certified Information Technology Professional (CITP)
- Certified Network Defense Architect (CNDA)
- Certified Public Accountant (CPA)
- Certified in Risk and Information Systems Control (CRISC)
- Certified Software Manager (CSM)
- Certified Systems Professional (CSP)
- EnCase Certified Examiner (EnCE)
- Information Security Systems Management Professional (ISSMP)
- Information Systems Security Architecture Professional (ISSAP)
- Microsoft Certified Professional (MCP)
- Payment Card Industry Qualified Security Assessor (PCI QSA)
- Payment Card Industry Professional (PCIP)
- Payment Card Industry Forensic Investigator (PCI PFI)
- Project Management Professional (PMP)
- Payment Card Industry Approved Scanning Vendor (PCI-ASV)
- VMware Certified Associate (VCA)

## Degrees

We hire graduates of the top 10 security university programs in the nation.

# TRUSTED BY



305-447-6750 | info@ermprotect.com | https://ermprotect.com

ERMProtect
Cybersecurity Solutions

# TESTIMONIALS

GROVE BANK & TRUST

*"ERMProtect has been a great partner for our Bank for many years. I have always felt that the quality of service received from ERMProtect and staff have been excellent and unmatched by any other information security firm provider surrounding pen testing and threat intelligence relating specifically to our organization. "*

**— Frank Iglesias,** Grove Bank & Trust

Helm.

*"Their team of consultants has brought a level of expertise and professionalism that is unmatched. They help us operate in a more secure environment. I would recommend them to anyone."*

**— Rosa L. Ortiz,** Helm

TecniCard INC.

*"Throughout the years, ERMProtect has offered TecniCard excellent services and support, providing effective fraud-fighting solutions. Their tests of our Network and Applications to identify possible deficiencies are rigorous and highly effective. The expertise and professionalism of the staff is at the top of the industry."*

**— Oscar Gálvez,** TecniCard Inc.

PERRY ELLIS INTERNATIONAL

*""The team at ERMProtect has always been a valuable InfoSec resource to consult. Their services are thorough, insightful and quick."*

**— Perry Ellis International**

Paybox
AN OSG COMPANY

*"For 8 years, ERMProtect has provided Paybox with effective cybersecurity services covering all of our PCI DSS needs and ongoing penetration testing requirements. As a thought partner in our compliance initiatives, their professional team is highly trained and regarded as a trusted advisor in our information assurance process."*

**— Jorge Ferrer,** Paybox

XAVIER UNIVERSITY

*"All faculty, staff and students at Xavier University found ERMProtect's Information Security training modules comprehensive, creative and helpful for every type of learner. Our community is now well-informed and knows how to identify scams and phishing very quickly!"*

**— Jeff Edwards,** Xavier University

ERMProtect
Cybersecurity Solutions

800 S. Douglas Road, North Tower, Suite 940
Coral Gables, FL 33134
Phone 305.447.6750
info@ermprotect.com