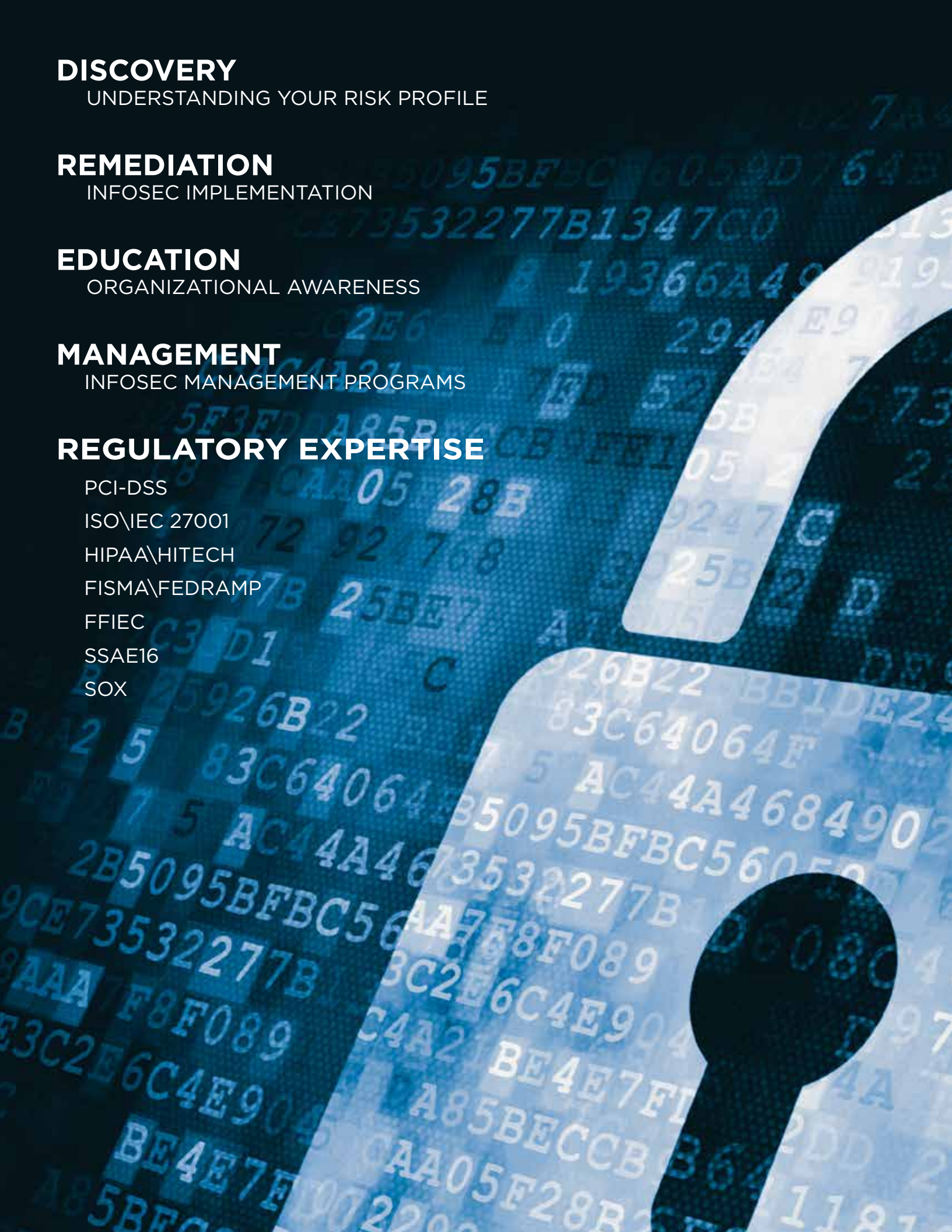
DISCOVERY
UNDERSTANDING YOUR RISK PROFILE

REMEDIATION
INFOSEC IMPLEMENTATION

EDUCATION
ORGANIZATIONAL AWARENESS

MANAGEMENT
INFOSEC MANAGEMENT PROGRAMS

REGULATORY EXPERTISE
PCI-DSS
ISO\IEC 27001
HIPAA\HITECH
FISMA\FEDRAMP
FFIEC
SSAE16
SOX



TROFI SECURITY®

INTELLIGENT INFORMATION SECURITY

"All organizations need some level of strategic support with their security programs, regardless of their program's maturity level, to combat the evolving threat landscape. **Our seasoned team of security professionals are uniquely qualified to provide our proven methodology and the essential hands-on know-how that security leaders need to successfully create and execute strategies aligned to their company's business objectives."**

- Mike Trofi | Co-Founder - Trofi Security

About TROFI SECURITY

Trofi Security was originally formed as Trofi Systems Solutions in Colorado in 1999, providing Information Technology and Information Security services to organizations in both the public and private sectors. Since then, Trofi Systems has expanded its employee ranks, its partner network, its services, and its footprint. By 2010, Trofi Systems maintained offices in Los Angeles, Denver, Rhode Island, and Ottawa. In 2014, Trofi Systems acquired Fury Mobile, greatly expanding its services in the areas of mobile security architecture mobile penetration testing, and Apple/IOS development services. This was followed soon after in early 2015 with the acquisition of CST Strategic Advisors, which provided executive-level information security management consulting. It was at this same time that Trofi Systems Solutions restructured itself, re-launching under the brand: **Trofi Security.**

During its 15+ year history, Trofi Security has maintained a commitment to its clients of ensuring they receive the very best guidance and service the market has to offer. Part of its mission has been to forgo quantity of business for quality of execution, and as a result, Trofi Security has remained a boutique Information Security firm utilizing only senior level practitioners on its engagements.

This commitment to quality has given Trofi Security a reputation within the industry, not only with clients, but with industry professionals and competitors, alike. This same reputation has allowed Trofi Security to attract some of the best talent in the industry, across virtually every security discipline. Every one of Trofi Security's consultant resources have a minimum of 15 years of experience in Information Security, and a number have over 20 years. In addition, every consultant maintains industry certifications within their respective areas of focus.

Company Leadership

MICHAEL **TROFI**

The original founder of Trofi Systems Solutions in 1999, Michael has over 27 years of experience serving as an Information Security Architect and Executive for organizations within both the Private and Public Sectors. Michael currently oversees the company's Security Architecture, Regulatory Compliance, and Penetration Testing operations.

ROD **SAUNDERS**

Formerly the Managing Partner for CST Strategic Advisors, Rod has over 25 years of experience serving as an Enterprise Architect, Information Technology Executive, and Information Security Advisor for organizations from Startups to the Fortune 500. Rod currently oversees the company's Virtual CISO & CTO consulting practices.

844 GO TROFI (844 468 7634)
info@trofisecurity.com
@trofisecurity

www.trofisecurity.com

These certifications include:

- **Certified Information Systems Security Professional (CISSP)**
- **Certified Encryption Specialist (E|CES)**
- **Certified Cyber Forensics Professional (CCFP)**
- **Certified Ethical Hacker (CEH)**
- **IACRB Certified Penetration Tester (CPT)**
- **GIAC Penetration Tester (GPEN)**
- **GIAC Web Application Penetration Tester (GWAPT)**
- **Certified Information Security Manager (CISM)**
- **Certified in the Governance of Enterprise IT (CGEIT)**
- **Certified in Risk and Information Systems Control (CRISC)**

The combination of commitment and reputation has allowed Trofi Security resources the opportunity to engage with some of the world's most notable brands and organizations. In the past 6 years alone, Trofi Security resources have been retained to provide Information Security Architecture, Management, and Testing services to organizations such as:

- **British Telecom**
- **Bureau of Communication and Technology**
- **Chanel**
- **Cohen & Steers**
- **Department of the Interior**
- **General Motors**
- **Kaiser Permanente**
- **Massachusetts Department of Transportation**
- **Mayo Clinic**
- **NCR / NCR-Retalix**
- **National Amusements**
- **Private Wealth Systems**
- **TicketMaster USA**
- **Time Warner Cable**
- **US Holocaust Museum**
- **Vail Resorts International**
- **VeriFone**
- **WealthTouch**

These organizations retained Trofi Security resources because they needed top-notch talent to ensure their brands and organizations had the best possible chance of securing their systems for their customers. We're proud to have had the opportunity to work with these organizations, and to know we've had a hand in assisting these organizations to secure their futures.

Trofi Security has grown to become one of the premier Information Security Advisory firms in the industry, and we're confident we can bring that depth and breadth of experience to bear for your organization as well. That's our commitment to you.

Michael Trofi | Founder/Partner

Rod Saunders | Founder/Partner

TROFI SECURITY®
INTELLIGENT INFORMATION SECURITY

844 GO TROFI (844 468 7634)
info@trofisecurity.com
@trofisecurity

www.trofisecurity.com

vCISO Services

Evolution of the Chief Information Security Officer

From small- and medium-sized businesses (SMB) to Fortune 500 enterprises, the need to address risks to information assets has long been understood; however, the manner and focus of that effort by organizations has steadily changed over time. Driven by a combination of factors from awareness, to growth in e-commerce channels, to increasing exposure to both internal and external threats, organizations have had to find better solutions for their information security strategies.

The following depicts 4 major steps in that evolution:

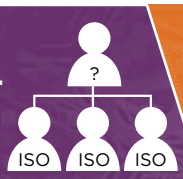
SPLIT ROLE

In the beginning (and still true for many smaller organizations) a CIO or CTO often played a dual role in order to fill in for the lack of a dedicated resource. Whether by lack of awareness or limited financial resources, this model failed to provide the focus necessary to properly address information security risk.

DEDICATED ROLE

As awareness and budgets grew, organizations hired dedicated resources to provide necessary focus on information security risk. While this worked for very small or low-complexity organizations, the increased focus brought awareness to executives that individual resources often lacked the breadth of expertise necessary to properly address risk in larger or more complex organizations.

DIVISIONAL ISO(S)



To address the breadth and complexity of information security risks, organizations began hiring divisional security officers, with specific expertise, to focus on a more narrow aspect of an organization. The idea was to network these individuals together to provide a more comprehensive information security strategy. To be effective, it came at a very high resource cost, and often meant organizations over-spent to get the expertise needed.

vCISO SERVICES

The "virtual" CISO model solves for the shortcomings of prior models. A vCISO resource is, in fact, a team of experts, fractionally applied by a primary CISO resource, working as an integrated partner to your organization. Leveraging highly-experienced, industry-certified, security experts in this manner ensures an organization is getting the very best information security guidance, across all aspects of their business, in the most cost-effective manner possible.

vCISO Services from Trofi Security make this model a reality for SMB organizations. Each of our senior-level consultants have over 25 years of experience across a number of industries including financial services, medical services, state and federal government, wholesale/retail, and more. Our consultants can help your organization in the areas of:

- **Cybersecurity Strategy**
- **Network & Application Security**
- **Intellectual Property Security**
- **User Security Awareness**
- **Regulatory Audit & Compliance**
- **Information Security Governance**
- **Information Security Risk Management**
- **Incident Management**

In today's digital world, your organization needs a comprehensive information security strategy. By leveraging the vCISO service model, you can be certain that strategy will be the most sound and cost effective way of protecting your business.

SSAE16 | Service Organization Control (SOC)

Audit and Readiness Services

More and more companies are outsourcing certain functions to service organizations. As a result, service organizations are being asked to provide assurances to their customers that their controls over financial reporting, IT security, availability, processing integrity, confidentiality, and privacy are adequate. Service Organization Controls (SOC) 1, 2, and 3 audit reports can meet these demands, as well as be an effective marketing tool to differentiate a service organization from competitors, attract new clients, and strengthen existing client relationships.

Depending on an organization's specific needs, a Type I or Type II report may be most appropriate.

See the chart below to determine which report and report type is right for your organization.

SOC 1

A ***proprietary, non-public*** report focusing on the controls specific to the integrity of financial reporting processes. This is the successor to the original SAS70 report.

The SOC I is required by many clients and service organizations for their ***financial reporting*** needs.

SOC 2

A ***proprietary, non-public*** report focusing on the controls related to the security, availability, processing integrity, confidentiality, and privacy of client data.

The SOC II is required by many clients and service organizations to maintain ***regulatory compliance.***

SOC 3

Similar to SOC2 Type I report, but less detailed.

A ***public statement of certification*** by an authorized CPA auditor, without divulging otherwise proprietary or sensitive system information.

Allows the display of an ***approved seal*** in marketing material and on websites.

No Type I or Type II report designation is available.

Type I	Focuses on a description of a service organization's system and on the ***suitability of the design*** of its controls to achieve the related control objectives.
Type II	In addition to Type I attestations, a Type II report include the auditor's opinion on the ***operating effectiveness*** of the controls, as well as a description of the tests used by the auditor to verify that effectiveness.

Trofi Security provides both readiness and audit services for all of the reports and report types above. Whether your organization is preparing for an audit and needs the expertise of experienced SSAE16 practitioners, or needs to complete the audit process to deliver certifications to clients, Trofi Security has both the information security experts and the authorized Certified Public Accountants on staff to assist.

The SSAE16 SOC reports are quickly becoming a contractual requirement for doing business across virtually every industry.

PCI-DSS Compliance

Readiness and Remediation Services

Uncertain whether your organization meets the new PCIv3 requirements? Struggling to even meet the PCIv2 requirements? Or perhaps your organization is one of the 80% of Level 1 Merchants who failed their initial audit last year, and incurred significant remediation and retesting costs. The Qualified Security Assessor (QSA) audit process can be costly even under the best of circumstances, much less when a company is out of compliance or simply unprepared. If this sounds familiar, **it's time to give Trofi Security a call.**

Trofi Security provides PCI-DSS Compliance Readiness Assessment and Remediation Services to help clients assess their true compliance posture, address gaps in their cardholder data protection capabilities, and prepare for QSA audits. Our regulatory experts will help ensure your successful audit by taking your team through the execution of 3 key processes: Assessment, Strategy, and Remediation.

ASSESSMENT

- CDE Scope and Segmentation
- Internal / External Penetration Testing
- Policy and Procedure Analysis
- Standards Testing
- Team Interviews
- Mock Audits

STRATEGY

- Remediation Roadmap Development
- Policy and Procedure Guidance
- Technology, Standards, and Resource Selection
- Timeline and Budget Forecasting

REMEDIATION

- Security Program Development
- Security Awareness Development
- Technology implementation:
  - >Web Application Firewalls
  - > Multifactor Authentication
  - > File Integrity Monitoring (FIM)
  - >Anti-virus
  - >Vulnerability Scanning
  - >Event Logging and SEIM

Challenges remain for many organizations in meeting and maintaining their PCI-DSS Compliance obligations; especially with the release of version 3.1 requirements only six months after version 3 requirements went into effect. Many organizations may not be prepared for their next round of compliance assessments, despite successfully meeting previous PCI-DSS requirements. Now more than ever, achieving and maintaining PCI-DSS Compliance requires a comprehensive strategy and expert help, in order to avoid the costly mistakes that come without it.

"We needed a trusted advisor, who would be there for us with a deep bench of resources when we needed them. With Trofi Security, I'm not worried about anyone going on vacation and not having the right people in place for support. **They've always been there for us, and I'd recommend them instantly to anyone."**

—Jason R. | CTO, Financial Services Technology Leader

ISO 27001 Certification

Readiness and Remediation Services

Information is one of the most important and valuable assets to any organization. In today's globally connected business environment, the confidentiality, integrity, and availability of that information faces an ever growing list of threats from both internal and external sources. Organizations that pursue an **ISO 27001 certification** and registration path, have made the choice to protect their information assets by constructing an Information Security Management System (ISMS) based on internationally-accepted, industry best-practices.

ISO 27001 Certification Benefits

- Demonstrates that your organization's infrastructure, applications and processes have passed rigorous, independent third-party testing.
- Provides clients with the assurances that your organization has tight and effective control over its operations; and that the likelihood of financial loss, operational failure or corruption of data is mitigated.
- Serves as a broad regulatory foundation, applying to numerous legislative and industry compliance requirements, both domestically and internationally.
- Provides a framework for improving both the maturity and efficiency of all organizational processes, while ensuring those processes evolve in the most secure manner possible.

Trofi Security assists organizations in preparing for ISO 27001 certification audits by assessing an organization's current information security infrastructure and practices, developing a gap analysis against ISO 27002 guidance, and formulating a roadmap for organizations to reach compliance.

Trofi Security ISO Readiness and Remediation Service Benefits

- ISO 27001/27002 Compliance Gap Analysis
- ISO 27001/27002 Risk Profile Assessment
- ISO 27001 Compliance Roadmap
- Collaboration with ISO Compliance Experts

Building an Information Security Management System (ISMS) capable of achieving ISO 27001 certification is one of the most valuable steps an organization can take to ensure critical information assets are protected. For many organizations, this is the first step toward achieving compliance with more complex compliance standards, such as PCI-DSS and NIST, or those being developed by larger corporate organizations, because it serves as a solid information security foundation. Taking that step, however, represents a big investment in both time and resources. Let Trofi Security use its years of experience helping international companies achieve and maintain their ISO 27001/27002 programs to ensure your time and resources are invested wisely.

HIPAA Compliance

Meaningful Use Risk Assessment Services

Trofi Security's comprehensive HIPAA Risk Assessment Program was developed in direct response to the need for medical practices to have a security advocate to help them achieve **HIPAA Part 15** of the required **Meaningful Use Core Objectives and Measures.**

The Meaningful Use Risk Assessment Process must be conducted at least once prior to the beginning of each electronic health record (EHR) reporting period. While it is not impossible for a medical practice to conduct their own Risk Assessment, it is not always feasible or recommended, and should not be taken lightly. Most medical practices simply do not have the time, expertise and resources available to conduct a comprehensive assessment. By leveraging our expertise, you will have more time to focus on your patients, while Trofi Security ensures your practice's compliance through an evaluation of the following security control areas, as defined by the HIPAA Security Rule:

ADMINISTRATIVE SAFEGUARDS

Administrative Safeguards are a special subset of the HIPAA Security Rule that focus on internal organization, policies, procedures, and maintenance of security measures that protect patient health information.

PHYSICAL SAFEGUARDS

The physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

TECHNICAL SAFEGUARDS

The technology, and the policies and procedures for its use, that protect electronic health information and its access. This is typically firewalls, intrusion prevention, antivirus, and other technologies.

Our consultants will work with your team to address these control areas by performing the following key steps during the assessment and, optionally, beyond the assessment:

DURING THE ASSESSMENT:

- Identify the scope of the assessment
- Identify and document potential threats and vulnerabilities
- Assess current security measures
- Determine the likelihood of threat occurrence
- Determine the potential impact of threat occurrence
- Determine overall level of risk
- Identify security measures and finalize assessment documentation

BEYOND THE ASSESSMENT: *(OPTIONAL)*

- Develop and Implement a risk management plan
- Implement security measures
- Evaluate and maintain security measures

Upon conclusion of the Assessment, Trofi Security will deliver a comprehensive report, which can be used to fulfill core requirement 15 of Meaningful Use, necessary to receive government funding and incentive bonuses from Medicare and Medicaid programs. In addition, this report can be used as a basis for the adoption and implementation of the proper PHI security measures, to ensure your organization can successfully pass an audit by the Department of Health & Human Services.

Penetration Testing

Black-box, White-box, and Red Team Services

Penetration testing uncovers critical issues and demonstrates how well your network and information assets are protected. Combined with a comprehensive security program, penetration testing can help you reduce your risk of a data breach and become proactive about threat management.

Trofi Security performs testing from an attacker's point of view. We don't just run a couple of scanning applications and give you the canned report from these tools. We use real-world attacks on your organization's infrastructure, based upon all available information about your organization, its technologies, and its people. We then combine those results with observations about your environment by our team of security experts, in order to give you a detailed view of your organization's actual risk exposure.

Trofi Security employs a number of proven methodologies as part of its testing services, depending on how comprehensively an organization wants to test its environment. These methodologies are categorized into 3 service types:

BLACK-BOX TESTING (LEVEL 1)

- External penetration tests simulating a "no previous knowledge" scenario of the systems being attacked
- Explores most likely attack scenarios posed by external and unrelated actors.
- Tests are crafted based on information collected during discovery.

WHITE-BOX TESTING (LEVEL 2)

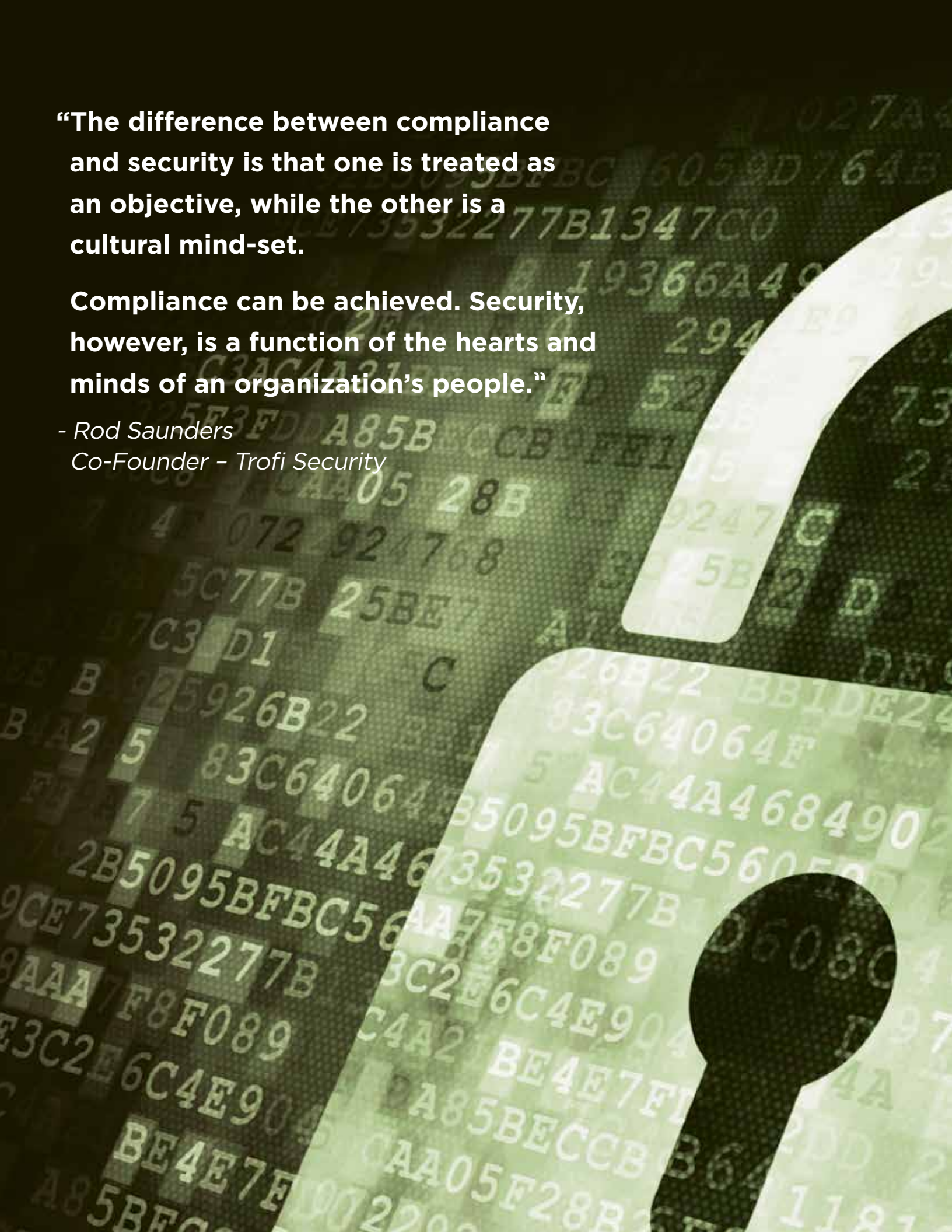
- Internal & External penetration tests based upon "prior knowledge" of the systems being attacked
- Additionally explores risk exposure to internal employees and vendors, with intimate knowledge of systems.
- Tests are crafted based on specific, known technologies and system configurations.

"RED TEAM" TESTING (LEVEL 3)

- Combines aspects of Level 1 and Level 2 testing, while also employing various social engineering attacks.
- Simulates a determined actor making a very direct and specific attack against your organization, with local, physical access to your locations and people.
- Tests are crafted based on Level 1 discovery, and Level 2 knowledge of locations and people.

Each form of testing reveals things that the other might not. We recommend that our customers have us perform all 3 forms of testing to give them a truly accurate representation of their attack risks. By engaging Trofi Security to emulate your adversary, you can discover critical exploitable vulnerabilities and remediate them before they are exploited.

Our team is highly experienced and trained in the latest tools and techniques used by individuals that commonly compromise **wired & wireless networks, web applications, mobile applications,** and more. The results of every penetration test presented by Trofi Security include complete details on the systems, applications and networks identified, exploitation results, as well both tactical and strategic recommendations to remediate your environment.



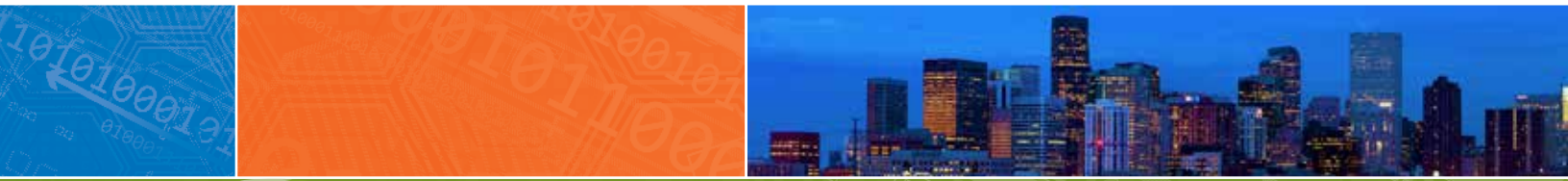
“The difference between compliance and security is that one is treated as an objective, while the other is a cultural mind-set.

Compliance can be achieved. Security, however, is a function of the hearts and minds of an organization’s people.“

- Rod Saunders
Co-Founder – Trofi Security

TROFI SECURITY®

INTELLIGENT INFORMATION SECURITY



www.**TrofiSecurity**.com

844 GO TROFI (844 468 7634)

info@trofisecurity.com

@trofisecurity

About Trofi Security

Trofi Security, originally Trofi Systems Solutions, was founded in 1999 to provide IT security advisory and compliance services to client organizations, as well as to serve as a security-community contributor in the development of cross-industry security best practices. Trofi Security's methodologies and expertise have been used successfully on more than 1000 projects, nationally, during its 15 year history.

Trofi Security has built a comprehensive set of tools and practices aimed at providing full lifecycle information security services to its clients, through engagement within multiple levels of an organization's strategic and tactical initiatives. These services include:

- **Virtual C/ISO**
- **Enterprise Risk Assessments**
- **Information Security Program Development**
- **Business Continuity Planning**
- **Penetration Testing**
- **Vulnerability Assessments**
- **Computer Forensics**
- **Secure Development Lifecycle**
- **Security Awareness Training**