ITMG™

ENSURING A TRUSTED WORKFORCE

2018

CORPORATE SERVICES GUIDE

INSIDER RISK MANAGEMENT

PREVENT. DETECT. MITIGATE

www.itmg.co

1200 19th St. NW
Washington, DC 20036

info@itmg.co

Welcome to

ITMG

What We Do

Client Profiles

Articles

Amateurs hack systems, professionals hack people.

Bruce Schneier

About ITMG

The proven leader and premier provider of insider risk management consulting, training, and staffing services. Trusted by leading Fortune 100, 500, and 1000 companies.

Founder and President

Mr. Thompson is the Founder of ITMG, the leading insider risk management firm providing expert consulting, assessment, training, and staffing services to corporations. He is an accomplished corporate executive with over 20 years' experience managing insider risk, including senior positions with FBI, DOJ, and NSA as a federal prosecutor, special agent, and senior risk management executive. He is a pioneer in the field of insider risk management and the author of the book "Insider Threat Program – Your 90-Day Plan." He is a member of the Maryland Bar.

> An opinion is only worth the experience that supports it.

ITMG, LLC is a consulting consortium formed in 2014 to focus solely on helping organizations ensure a trusted workforce by providing a range of insider risk management services including – strategic advising, insider risk assessments, program development, training, and staffing. ITMG's insider threat experts comprise the largest network of insider risk management practitioners in the world and include dozens of former Intelligence Community senior cyber security and insider risk management professionals. Our experts are pioneers in insider risk management and have served with numerous agencies including the FBI, DoD, DNI as well as several large corporations. Our vast network of bona fide insider threat professionals is located throughout the country, with an extended network in several countries including the UK, Australia, and Singapore. Our network includes experts in all insider threat disciplines including program development, governance, data management, user monitoring, data governance, identity and access management, training, investigation, privacy, incident response, compliance, behavioral psychology, and law.

Our Insiders

VAL LETELLIER
Principal Consultant

Mr. LeTellier has 30 years' risk management experience in the public and private sector. He ran security operations as a State Department Diplomatic Security Special Agent and then intelligence operations as a CIA operations officer and station chief. For twenty years he recruited sources and penetrated foreign organizations, providing him unparalleled experience and understanding of insider threat tactics, techniques, and procedures. He holds an MBA, MS, CISSP and PMP. He leads the ASIS Defense & Intelligence Insider Threat Working Group and is a member of the INSA Insider Threat Subcommittee.

SEAN WALSH
Attorney Advisor

Mr. Walsh is a former Assistant General Counsel of the FBI with over 30 years' experience on complex civil litigation and technology matters. He has extensive experience in cyber investigations and national security cases and served as the national security counsel to the FBI Cyber division. He has lectured extensively on computer security matters including at the European Union computer crime conference at The Hague. Mr. Walsh is an adjunct faculty member at the New Jersey Institute of Technology where he teaches a course on Cyber Investigations, Security, and the Law.

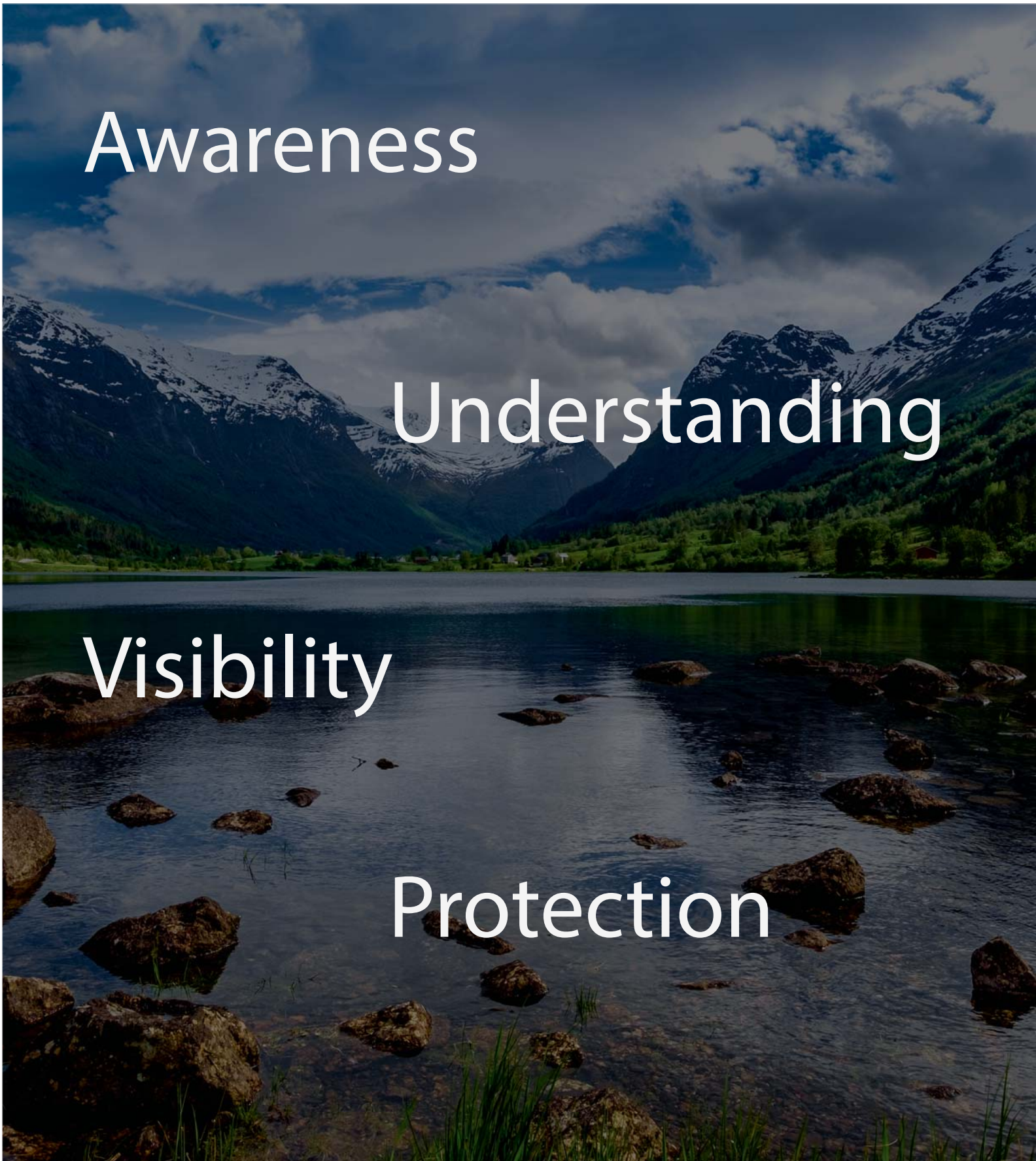
JUDY PHILIPSON
Behavioral Scientist

Judy Philipson, Ph.D. is a senior behavioral scientist and analyst specializing in threat detection, assessment, influence operations, and research methodology. Dr. Philipson has provided direct support to the Intelligence Community, DoD, and DHS on a broad range of operational, investigative, research and training activities. She served as Social Influence Advisor to the Counterterrorism Center at the CIA. She has a Ph.D. in clinical psychology from Drexel University where she focused on forensic populations and issues relating to deception and risk assessment.

JIM LIGHTBURN
Senior Solution Architect

Mr. Lightburn has over 30 years of management and operational technical experience with the US Intelligence Community and industry. He is a pioneer in the development of the Information-Centric Security model and he has extensive experience in developing data protection solutions for insider threat with Fortune 500 companies and classified US customers. He is an expert in implementing insider risk management technical solutions, including end-to-end encryption, DLP, UAM, SIEM, UEBA. He was nationally recognized by SINET for his innovative concept for protecting data at the object level and creating persistent data protection. He subsequently commercialized this technology into his patented Need2Know® data protection tool platform.

Our Value



What we do?

ITMG provides comprehensive insider risk management services. From baselining your current capabilities, to assessing risk, or selecting a tool, we've got you covered. We help corporations develop, implement, and manage formal insider risk management programs - from strategy to staffing.

BASELINE ASSESSMENTS

Review of functional component processes, technology, and people. Assess organizational insider risk management posture.

RISK ASSESSMENTS

Analyze critical asset impacts, vulnerabilities and threats. Assess risk of compromise to individual asset groups.

RED TEAM ASSESSMENTS

Evaluate insider risk prevention, detection, and mitigation processes. Assess capabilities against specific personas and events.

PROGRAM DEVELOPMENT

Create an Insider Risk Management Program strategy and framework. Define policies and a clear implementation roadmap.

STRATEGIC ADVISING

Provide expert guidance on implementing and integrating insider risk management strategies and solutions.

TECHNICAL CONSULTING

Provide expert guidance on insider threat tool selection, integration, and policy and rule development.

LEGAL & PRIVACY

Provide expert legal and privacy consulting. Foster a proper balance of privacy and security equities.

STAFFING

Provide uniquely qualified personnel to support program objectives. Including: analysts, investigators, behavioral psychologists, and SMEs.

TRAINING

Provide awareness training to employees and insider risk management operational training to program personnel.

INSIDER RISK

The Problem

The biggest threat to corporate assets are individuals to whom you grant authorized access. Managing the resultant risk requires a paradigm shift towards a new model that formally addresses insider risk.

Insiders are the greatest risk to your corporate assets

While insiders pose the greatest risk, traditional security risk management models focus nearly exclusively on external threats. Consequently, insider threats, although accounting for the great majority of incidents, receive only a fraction of security resources. The impact and harm caused by insider compromises can be as damaging, if not more so, than those caused by purely external attackers.

Who's the Bigger Threat:

Insiders or Outsiders?

Both surveys and actual data studies confirm the existence of a formidable and sizable insider threat problem. The exact scope and size of which is difficult to assess. Educated assessments, however, strongly suggest that insiders are responsible for the majority of security events.

Growing Problem

Insider threat is a growing problem, yet most still do not have controls (technical and programmatic) in place to manage insider threats. Most companies have experienced an increase in insider threat incidents with most organizations experiencing more incidents within the last year. Surveys also suggest that organizations are not prepared to prevent, detect, or manage insider threats. This is compounded by the willingness of insiders to engage in threatening activity. According to Symantec, 50% of employees retain confidential data in violation of policy and 90% intend to use the data to advance their career in a new job.

Actual Data Studies

According to IBM, the percentage of "attacks" carried out by insiders is 60%. This initially seems straightforward, however, IBM defines an "attack" as a "security event that has been identified by network tools as 'malicious' and sourced to an IP address." This definition ignores unintentional insider threat events as well as any insider threat event that cannot be sourced to an IP address. Thus, the true number of insider threat events is likely much greater than 60%.

According to most research, 90% of external attacks are facilitated by insiders . . . so even traditional "external" attacks have a large insider component!

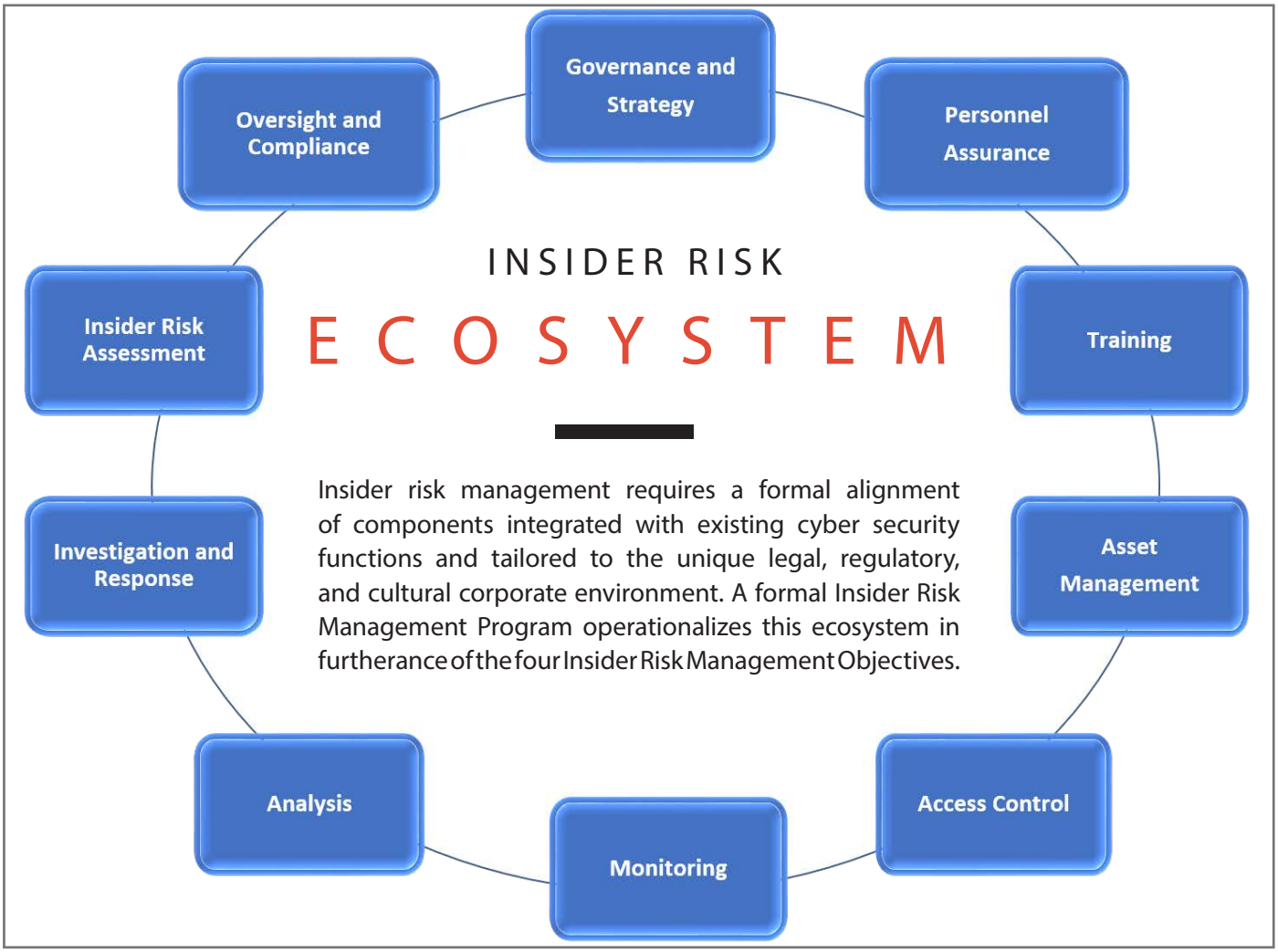
According to a study by the Ponemon Institute of 54 companies and nearly 900 security incidents, the percentage of insider threat incidents is 90%, of which 75% are attributed to Careless Insiders.

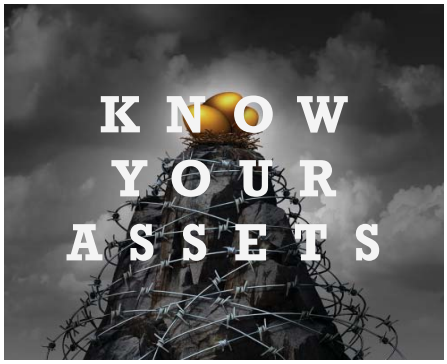
Insider Fraud

By comparison, during roughly the same time frame as the Verizon study, the Association of Computer Fraud Examiners in their 2016 report collected and analyzed 2,410 actual cases of fraud, which they defined as: Corruption, Asset Misappropriation, and Financial Statement Fraud. This figure is larger than the total number of "breaches" reviewed by Verizon and further supports that 1) insider involvement is much more than network activity and 2) is likely much higher than the IBM figure of 60%, since they limited their definition to "network based attacks" and the great majority of the ACFE cases fall outside of this scope.

Breaches as Proxies?

Data breach studies are like comparing apples and oranges when using them as proxies for insider threat events. For example, according to Verizon's study, only 20% of "breaches" are carried out by insiders. This is misleading, however, as a breach is defined by Verizon as a "confirmed" disclosure of data to an unauthorized party. A breach is thus much more easily ascribed to an outsider since, by definition, they are an unauthorized individual. Whereas an insider has some level of authorized access resulting in much more difficulty in proving a breach. When one looks at "security incidents," however, the level of insider involvement rises to 69%, according to Verizon. An incident is defined as a security event that compromises an information asset. The incident metric is thus more reliable in determining the true level of insider threat.





Insider Risk Management Objectives

Knowing Your People requires an understanding of the backgrounds of those to whom access is granted and ensuring that employees understand organizational policies and rules of behavior.

Knowing Your Assets involves understanding 1) what assets you have 2) where they are located 3) who can access them and 4) how they can be accessed. This includes understanding how assets move within an organization as well as controlling access to them.

Obtaining Visibility requires monitoring insiders interactions with assets: 1) Who has access 2) How they interact 3) When they access and 4) Why they are accessing them.

Responding to Actions requires access to relevant information and the ability to analyze, investigate, and mitigate threat events.

Consulting

Effective insider risk management requires a comprehensive strategy that aligns cost-effective security solutions with business objectives.

Program Development

So what is an "insider threat program?" Many practitioners claim that they will "build you an insider threat program," but most fail to understand what this means. This lack of understanding is largely the cause of the continuing and costly insider breaches that impact businesses everywhere. At ITMG, we believe an insider threat program (or "insider risk program") consists of and requires synergy between an ecosystem of ten interrelated functional components. Whether you're seeking to build a complete program, build an initial operating capability, or enhance existing components, we can help you every step of the way.

Technical Consulting

Effective risk management requires obtaining the necessary visibility of assets, user behaviors, and most importantly - user *interactions* with assets. This requires the use and leveraging of various toolsets including both network and endpoint monitoring solutions. Our team of technical experts have decades of hands-on experience implementing DLP, UAM, SIEM, and UEBA solutions. We can assist with tool selection, implementation, integration, and policy tuning and development.

Strategic Advising

You are undoubtedly aware of the harm that insiders can cause your business. In fact, they cause 90% of all security incidents. Unfortunately, today's piecemeal and ad hoc approach is simply not working. You need a holistic Insider Risk Management Program to effectively manage these threats and reduce the risk to your corporate assets. To that end, we will help you accomplish the four primary objectives – Know Your People, Know Your Assets, Obtain Visibility, and Respond to Actions.

Legal and Privacy

Implementing an insider threat program raises myriad privacy, regulatory compliance, operational liabilities, criminal and civil enforcement, and employment considerations. Each can have disastrous economic impacts on your business if not properly managed. As an experienced legal and operational practitioner in the area of compliance, employment, security, and criminal law, Mr. Thompson is uniquely positioned to advise your insider threat stakeholders on the parameters and best practices of implementing an insider threat program.

Client Profile

> ITMG developed a robust insider risk management program that allows us to protect our IP while continuing to enable innovation.
>
> Chief Security Officer

FORTUNE 100 RETAILER

Enabling innovation through insider risk management.

Client is an industry and market leader. Innovation drives all aspects of Client's business operations. As a market leader, Client is also the target of competitors who seek to leverage Client's technical innovations and human capital for their own corporate advancement. Consequently, protecting Client's intellectual property and human capital is a primary business objective. Client's relationship with its employees and partner networks are integral in securing IP and other critical assets. To properly manage these relationships, Client turned to ITMG to assess, develop, and implement a robust insider risk management program. ITMG created a program that protects Client's critical assets, respects employee privacy, and enables and enhances corporate innovation.

ITMG completed a complete review of Client's entire organization and assessed Client's insider risk management maturity level based on *ITMG's Insider Risk Maturity Model*. ITMG's assessment provided Client immediate return on investment by identifying gaps and providing recommendations and a roadmap for improving insider risk management capabilities.

Balancing privacy and security while fostering and enabling a culture of innovation.

WE ARE ITMG

1

The leading provider of insider risk management services and solutions.

40

Over 40 large scale assessments of corporate insider risk management capabilities, including over two dozen Fortune 100, 500, and 1000 companies.

500

Over 500 companies trained on insider risk management strategies, tactics, procedures, and best practices.

INSIDER RISK MANAGEMENT

Incentives

Risk management best practices notwithstanding, there are numerous legal entanglements and regulatory compliance requirements that justify and incentivize the formal management of insider risk.

COMPLIANCE

GRAMM-LEACH BLILEY
BANK SECRECY ACT
FACTA
HIPAA
SOX
PCI-DSS
NISPOM

LEGAL ENTANGLEMENTS

DUTY OF CARE
NEGLIGENT HIRING
RETALIATION
DISCLOSURE OF INFORMATION
HOSTILE WORK ENVIRONMENT
DATA BREACH

Legal Incentives

Employee Monitoring

The decision to monitor employees must be made within the context of current regulatory and legal frameworks that often incentivize employee monitoring. In many cases, monitoring employee behavior might be the only regulatory shield or legal defense available to an organization.

Employee monitoring requires consideration of several factors – cost, culture, privacy, perception, etc. The challenge is to balance the security needs of the corporation with the privacy concerns of employees. Sound security reasons notwithstanding, there are legal reasons to monitor employees.

Insider Threat Compliance

There are five general categories of government regulations that impose affirmative obligations to monitor employee behaviors.

Financial - Gramm-Leach-Bliley Act and Bank Secrecy Act: *Monitor user behavior to ensure proper access and use of customer records to prevent money-laundering by monitoring employee transactions.*

Healthcare - Health Insurance Portability and Accountability Act: *Monitor access rights to PHI information, detect behavior deviations, monitor accesses, and monitor file attribute changes.*

Public Companies - Sarbanes-Oxley Act: *Monitor to ensure access is limited to authorized users, perform risk assessments, and monitor for unauthorized access to corporate confidential financial information.*

Retail - Payment Card Industry Data Security Standard: *Monitor access of cardholder data to uncover unusual trends, monitor and uncover the sharing of credentials, and baseline user behavior and monitor for deviations.*

National Security - National Industrial Security Program Operating Manual: *Requires covered entities to establish a formal insider threat program, a key component of which is to implement user activity monitoring to detect insider threat activity.*

Legal Entanglements

Beyond regulatory incentives to monitor employees, there are several legal entanglements or risks that can often be mitigated through proper employee monitoring.

Duty of Care - A duty of care is a legal obligation imposed on individuals and corporations when performing acts that could foreseeably harm others. Courts have created a liability regime where monitoring employee behavior has become a matter of corporate self-interest. Employers now possess "affirmative obligations" to prevent and eliminate harassment in the workplace, prevent retaliation, prevent workplace violence, and prevent the disclosure of protected information (i.e. manage insider threats). Since knowledge of employees' behavior is required to address such behavior and avoid liability, monitoring is critical to meeting these burdens of proof.

Negligent Hiring and Retention - These claims generally arise in the context of a workplace violence incident when facts exist that show that the employee had a violent history and that the employer could have reasonably learned of this behavior. Here, monitoring can help the employer prevent, detect, and mitigate such behaviors and provide adequate proof to meet legal obligations, and limit liability, as described above.

Retaliation - Retaliation claims arise when an employee alleges that they have participated in a "protected activity" and, as a result, were subsequently subject to an "adverse employment decision." Defending such claims can be difficult for employers since courts have created a framework that tends to require an omniscient employer who possess knowledge of all activities and relationships within their organization. Employee monitoring represents the only logical approach to attempt to meet this standard and to properly defend against a claim of retaliation.

Disclosure of Sensitive Information - Businesses may be liable for the unauthorized disclosure of sensitive personal information of its employees and customers, as well as the sensitive business information of its partners. Employers can be vicariously liable for the actions of their employees, so monitoring employee behavior may be the only way to adequately prevent, detect, and mitigate this behavior.

Hostile Work Environment - These claims arise when an employee alleges that an employer has created a workplace that a "reasonable person would consider intimidating, hostile, or abusive." Logically, monitoring employee behavior may be the only way to detect and mitigate such actions.

The key is to balance security and employee privacy.

Client Profile

ITMG developed a data protection and risk management program that provided greater visibility and protection of critical assets.

FORTUNE 100
ELECTRONICS MANUFACTURING SERVICES

Creating insider visibility through Data Loss Prevention strategies.

Client has over 140,000 employees worldwide but lacked a clear strategic vision for protecting data. Client had a DLP MSP contract that was not well aligned with their business objectives, resulting in several implementation issues. DLP agents were deployed on 75,000 devices, but the limited internal staff lacked the technical skills and procedures to properly manage the alerts and were entirely reliant upon the DLP vendor for support.

ITMG provided strategic guidance on aligning the DLP program with an Insider Risk Management strategy. ITMG defined a new DLP strategy, developed goals, conducted data collection interviews to identify technical and operational gaps then developed a new data protection roadmap. ITMG realigned Client's existing DLP vendor relationship and negotiated a new contract, on behalf of the Global CISO. ITMG then managed the first 90 days of the implementation which included onsite technical support to develop DLP policies and responses, weekly vendor and client team meetings, and the deployment of over 70,000 registered secure USB drives for automated data encryption. The new MSP contract provided the Client with significant cost savings.

Effective risk management through greater visibility.

Assessments

Tailored assessments provide understanding of risk management capabilities, awareness of risk levels, and knowledge of exploitable weaknesses.

Baseline Assessments

A baseline review will provide you an objective programmatic and operational insight into your current insider risk management capabilities. The findings will allow you to fully understand your current strengths, any shortfalls, and areas for improvement. You will not only obtain an objective review of your current components, but also recommendations and strategies for building out additional components to augment your current operating capability. The results can serve as talking points with senior executives and provide a basis for subsequent business cases pursuing specific component improvements or buildouts.

Red Team Assessments

Our Red Team models how real-world insiders might compromise and exfiltrate sensitive corporate information. In addition to evaluating the compromise methods of insiders, we also test your insider threat incident response procedures. After a red teaming exercise, you'll have a better understanding of your organization's security posture as it relates to specific insider threat personas and events and you'll know where to focus your future efforts for improvement.

Return on Investment

Increase client confidence
Reduce risk of compromise
Increase employee productivity
Increase investor confidence
Protect reputation
Create asset protection culture
More efficient decision-making
Early threat detection
Lower remediation costs
Reduce impact of compromise
Halt loss of intellectual property
Bolster existing security measures
Reduce time to resolve incidents
Reduce liability exposure

Risk Assessments

Our assessment is the only methodology that provides you with a clear and granular understanding of:

- Insider risk security posture based on our proprietary *Key Risk Factors*
- Critical assets based on our proprietary *Key Impact Factors*
- Insider threats posed to your organization based on our proprietary *Key Threat Factors*
- Vulnerabilities to your assets based on our proprietary *Key Vulnerability Factors*

Client Profile

> ITMG created a tremendous insider risk management program for us, ensuring compliance with our myriad regulatory and legal requirements. ITMG consultants are extremely knowledgeable and I look forward to engaging their services in the future.
>
> SVP, General Counsel

LexisNexis®

New York, New York
10,000 employees
www.lexisnexis.com

Ensuring effective compliance through insider risk management.

LexisNexis Legal & Professional is a leading global provider of legal, regulatory and business information and analytics that help customers increase productivity, improve decision-making and outcomes, and advance the rule of law around the world. To enhance these services, LexisNexis turned to ITMG to develop and implement a robust insider risk management program. ITMG created a program that protects LexisNexis's intellectual property and business processes while complying with applicable legal and regulatory requirements.

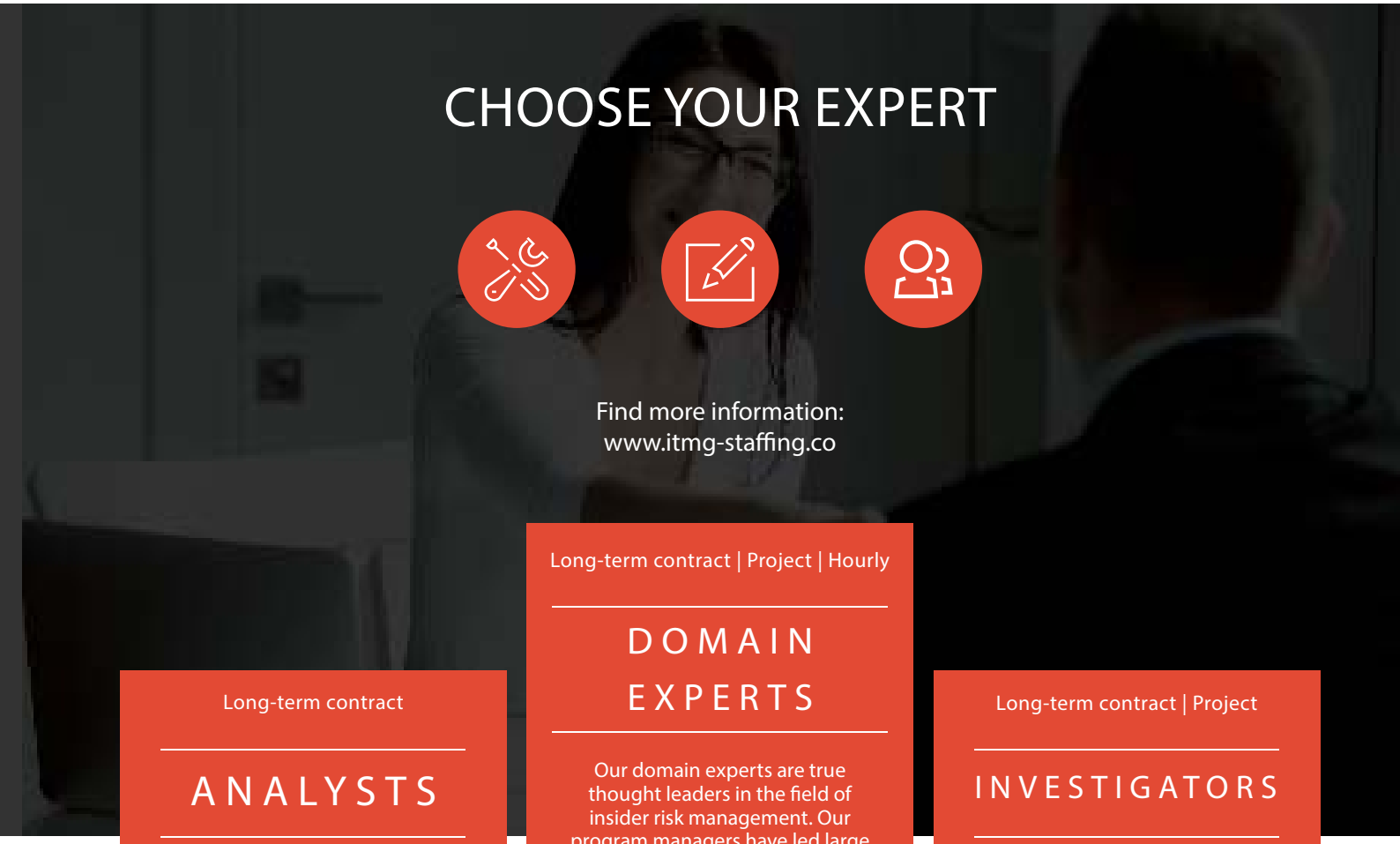
ITMG completed a complete review of LexisNexis's entire organization and assessed current HR and security policy and procedures. ITMG developed an insider risk management strategy and provided LexisNexis immediate return on investment by developing and drafting new strategic and operational policies and procedures. ITMG then advised executives on developing an effective employee communication and implementation plan .

Insider risk management supports effective and compliant business processes.

Insider Risk Management

Staffing

Effective insider risk management requires a unique and diversified skillset. ITMG is uniquely positioned to provide qualified personnel to support your insider risk management program. We have access to the largest network of bona fide insider threat experts in the world, most with over 15 years' experience.



CHOOSE YOUR EXPERT

Find more information:
www.itmg-staffing.co

Long-term contract

ANALYSTS

Our insider risk analysts have experience collecting and aggregating information from multiple data sources, including developing and refining policies for DLP, UAM , and other common toolsets. Most importantly, our analysts have real-world experience supporting insider risk management programs in the corporate sector.

Long-term contract | Project | Hourly

DOMAIN EXPERTS

Our domain experts are true thought leaders in the field of insider risk management. Our program managers have led large scale corporate engagements, our Tool SMEs have operational knowledge of leading solutions, and our Behavioral Psychologists are pioneers in developing threat indicators and ontologies.

Insider Risk Program Managers

Insider Threat Tool SMEs

Behavioral Psychologists

Long-term contract | Project

INVESTIGATORS

Our investigators have decades of experience managing large scale government and corporate insider threat investigations, including IP theft, misconduct, and corporate espionage. We can augment the operation of your existing insider risk management program or conduct case or project specific investigations.

We provide real

Return on Investment

ITMG leverages decades of real-world experience to provide creative risk management solutions that are tailored to the unique corporate environments of our clients.

Consulting and Staffing

Fortune 100 retailer - "*More effective capabilities*" - Conducted full insider risk assessment of entire organization. Worked with all levels of organization from C-suite to operational staff. Assessed organization's current insider risk operating capability against ITMG's ten components. Designed a "future state" Insider Risk Program and a roadmap for development and implementation. Provide ongoing managed services: strategic advising, management consulting, analyst support, and training.

Assessments

Fortune 100 financial - "*More efficient resource allocation*" - Developed insider threat program, incorporated an assessment, drafted policies and procedures, and developed compliance protocols. The assessment provided the client with an understanding of gaps, critical assets, current capabilities, and which controls will produce the greatest security benefit at the lowest cost. ITMG's assessment allowed client to efficient allocate current resources and to plan for future fiscal year budgetary requirements.

The true value of an insider risk program is the overall improvement of business processes and the enhanced collaboration of functional components.

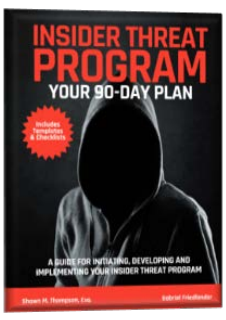
Training

Fortune 500 technology firm - "*Promoting security through applied learning*" - ITMG developed a comprehensive insider risk management training program to aid client in the development and implementation of their business objectives. Training included general awareness modules designed for client's employees. Both training components fostered greater understanding of insider threat personas, tactics, and procedures. Client has observed a considerable reduction in policy violations and greater employee acceptance and participation in security programs.

Legal and Privacy

Fortune 1000 financial - "*Obtained greater risk visibility through proper balancing of privacy and security*" - ITMG worked closely with the General Counsel and Chief Privacy Officer to develop a legally defensible and culturally acceptable employee monitoring program. ITMG provided consulting regarding tool selection and implementation as well as policy development. Procedures and messaging were created to inform the workforce and to align the monitoring program with client's insider risk management strategy, while ensuring compliance with laws and regulations.

Recognized Expertise and Thought Leadership



WIRED

BALTIMORE BUSINESS JOURNAL

the cyberwire

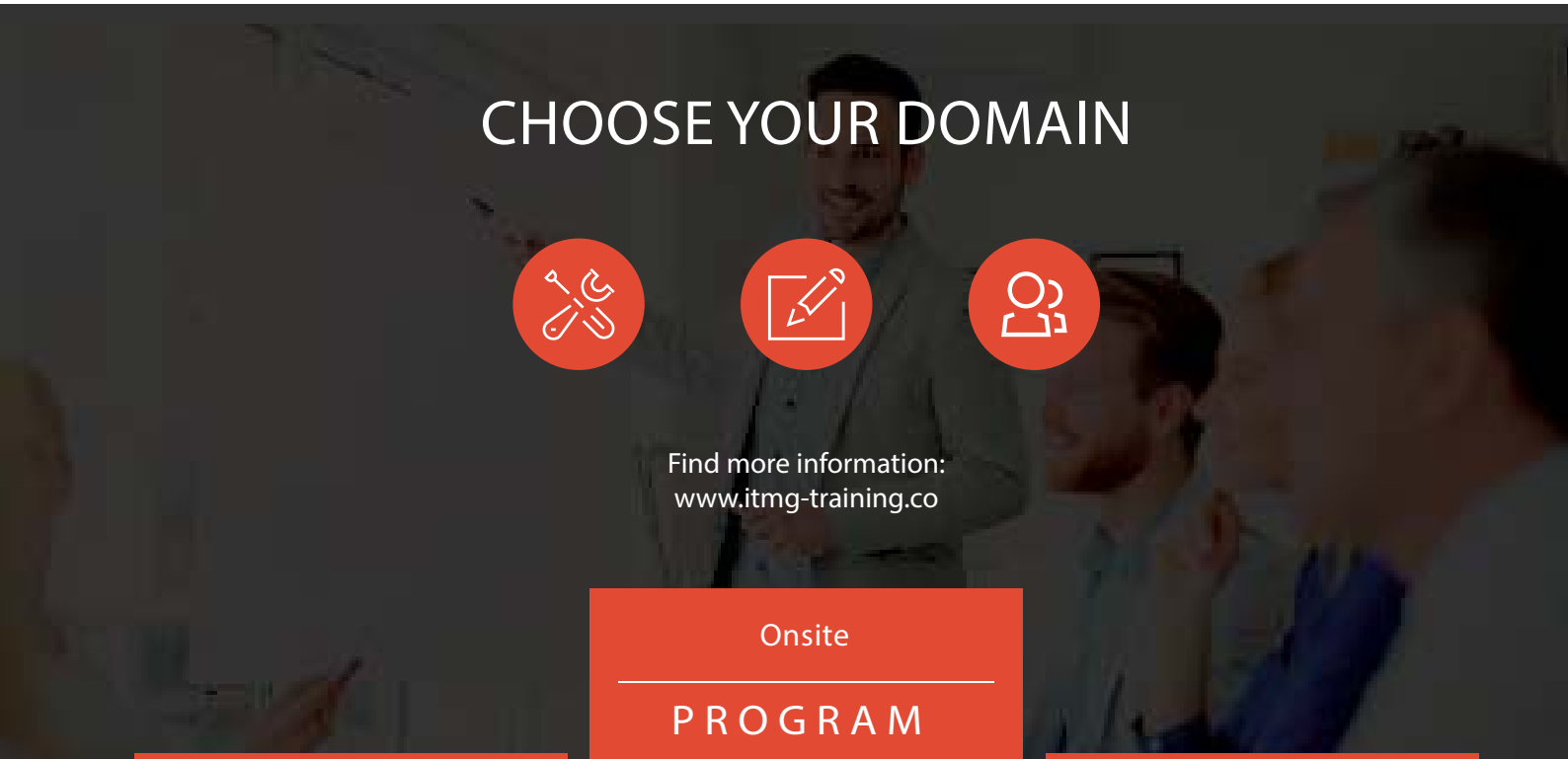
CIO FROM IDG

CSO FROM IDG

Insider Risk Management

Training Programs

Our training programs are the most comprehensive in the industry and taught by bona fide insider risk management practitioners. Each program is designed to develop practical insider risk management skills and awareness for both employees and insider risk management program personnel.



CHOOSE YOUR DOMAIN

Find more information:
www.itmg-training.co

Web-based | LMS | Onsite

AWARENESS

Our awareness programs are specifically designed to provide your employees a comprehensive understanding of the threats posed by insiders and the common tactics, techniques, and methods used to compromise corporate assets. Our programs are fully compliant with regulatory training requirements including SOX, HIPAA, FISMA, NISPOM, among others.

Onsite

PROGRAM DEVELOPMENT

Our program development courses are two-day courses designed for insider risk management operations and executive personnel. Each course covers the fully panoply of insider risk domains including program strategy, development, and implementation. In addition, legal and regulatory parameters are fully explored and delivered by a licensed attorney and experienced insider risk practitioner.

Insider Risk Program Manager Certification

Web-based | LMS | Onsite

OPERATIONS

Our operations training programs provide your insider risk management personnel with the knowledge and skills necessary to function in analytic or investigative roles. Program topics include: Behavioral Indicators, Insider Threat Tools, Data Sources, Interviewing, Insider Threat Law, among others.

Insider Risk Analyst
Insider Threat Investigator
Certification

Client Profile

> ITMG's training provided our staff with a comprehensive understanding of insider risk management. The training modules easily integrated into our Learning Management System. ITMG's domain expertise and unique instructional methods are best in class!
>
> Global Training Director

Lexmark™

Lexington, Kentucky
14,000 employees
www.lexmark.com

Fostering business objectives through insider risk management.

Lexmark International, Inc. is a leading developer, manufacturer, and supplier of printing, imaging, device management, managed print services (MPS), document workflow, and business process and content management solutions worldwide. Lexmark partnered with a leading insider threat tool provider and began to bundle this offering with their existing print and document security solutions. To foster greater awareness and understanding of insider threat and insider risk management, Lexmark turned to ITMG to develop a robust training program for its executives and staff across their business development, marketing, and sales divisions. ITMG created a modular program that is compatible with and delivered via Lexmark's Learning Management System.

ITMG developed a complete training program on insider risk management - problems, context, incentives, and solutions. ITMG's training provided Lexmark immediate return on investment by educating their personnel on the insider threat problem, identifying solution buyer personas, discussing decision points, and understanding tool capabilities and differentiators.

Expanding new business lines through insider risk management training and awareness.

Insider Risk Management

Question and Answer

We've collected some common questions about our strategy and services and provided some brief descriptions below. We encourage you to visit our website, give us a call, or schedule a no obligation scoping session where we can drill down on your particular risk management concerns.

01 What is the difference between insider threat and insider risk ?

An insider threat is an identified threat actor that is in position to harm your corporation. Risk is the degree of harm to a given asset and is represented by a combination of asset impact, vulnerability, and threat. Therefore, insider risk is the level of harm that an insider can cause to corporate assets, based on an examination of the insiders access, asset controls, and harm that would result if the asset were compromised.

02 Should the Insider Risk Program fall under the CISO or CSO?

An Insider Risk Program is by definition a cross-functional program requiring collaboration of multiple business units. While each corporate structure is unique, in our experience the CSO is in the best position to facilitate the required collaboration. The CSO can more efficiently integrate the program components with the assistance of the CISO and other functional leaders.

03 What is the difference between a Baseline Assessment and a Risk Assessment?

The purpose of the Baseline Assessment is to understand the current insider risk management operating capabilities. The focus is on the ten functional components of the ecosystem. By contrast, the purpose of the Risk Assessment is to understand the risk levels of specific asset groups (i.e. how likely they are to be compromised). The focus is on identified assets and an insider's ability to take advantage of asset vulnerabilities to effect a compromise.

Find more information:
www.itmg.co

> Well done is better than well said.
>
> Benjamin Franklin

04 What are the delivery options for insider threat training?

We offer three delivery options and each can be tailored for your unique corporate needs and requirements. The first option is delivered via ITMG's web-based learning management platform. The second option is to tailor the training for your corporate LMS. The third option is to deliver the training live and in person. We hold regular training sessions throughout the country and also can deliver at your corporate offices.

05 My company has a CISO and CSO, why do I need to create an Insider Risk Program?

An Insider Risk Program requires formal integration and collaboration of multiple functions, including the CISO and CSO, but also HR, Legal, Privacy, Risk, and business units. A formal program will require the necessary collaboration and remove stovepipes that inhibit effective insider risk management.

06 What makes someone an insider threat expert?

Expertise is a process and something that is earned through experience, not learned in a classroom. At ITMG, our domain experts have a minimum of 15 years' of real-world insider risk management experience, and many have more than two decades. Insider threat expertise also requires experience across multiple domains - network security, personnel security, employee management, investigations, and legal.

410-874-3712
info@itmg.co

Contact person:
Jennifer Bray


AN OPINION IS ONLY WORTH THE EXPERIENCE THAT SUPPORTS IT.
ITMG consultants are bona fide risk management experts. They provide creative solutions tailored to our unique corporate needs and requirements. I highly recommend ITMG for any corporate risk management project.
GLEN KAZERMAN
CEO, VENTURE CAPITALIST

ITMG™

RISE ABOVE THE RISK

www.itmg.co
info@itmg.co
410-874-3712