MāKINSIGHTS

Accomplish together

FINANCIAL SERVICES

Contents

- Introduction
- Third-party management – TPM
- Resiliency & recovery
- Offensive security
- PCI – DSS compliance
- SWIFT advisory & audit
- Privacy program definition

Background

MAKINSIGHTS was founded in **2013 in Detroit, MI** and expanded to **Lima, Peru in 2018.** Our competitive edge is combining a global "Big-4" mindset with local talent and expertise through our worldwide footprint of partners and industry veterans possessing unique **INSIGHTS**

MAKINSIGHTS has successfully established programs and delivered innovative projects across **IT Risk Management, Privacy, Information Security, Cybersecurity,** and **IT Governance** in the US, Europe, Asia-Pacific, and South American countries

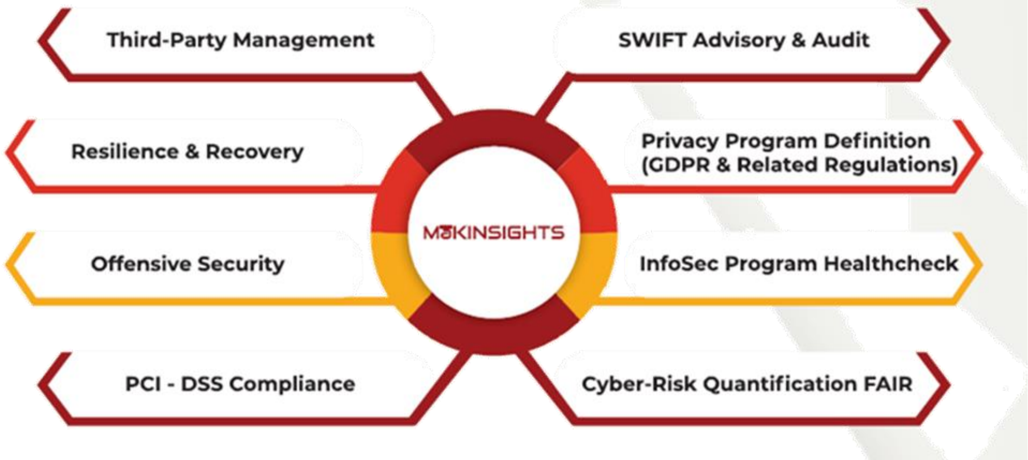
MAKINSIGHTS actively supports global organizations and those with other levels of scale in the following verticals:

- Manufacturing
- Financial Services
- Healthcare
- Internet/Technology
- Telecommunications & Utilities

FS-industry Services Overview

Global Financial Services firms are subject to more cyber-attacks than ever with threat actors using new, aggressive and sophisticated methods of attack that target people, technology, and processes

MAKINSIGHTS strives to ensure our clients are better prepared to prevent, detect, and respond to these types of threats and have identified a set of services relevant to the financial services sector that are designed to effectively support their Information Security & Information Privacy strategies



Third-party Management - TPM

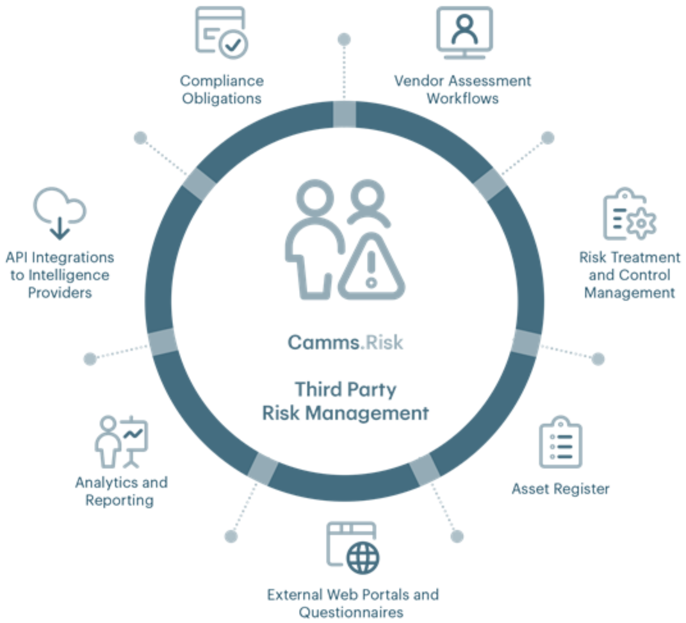
Improve the health of your supplier environment and ensure your organization is abreast of regulatory demands placed on the supply-chain through proactive management of third-party risk

Benefits

- Enhance the organization's capabilities to manage vendors
- Identify gaps in vendor Information Security capabilities and accelerate remediation
- Establish acceptable standards for managing vendors and contracts
- Implement an on-going monitoring capability that anticipates and assesses unforeseen risks
- Increased efficiency and cost savings across the vendor ecosystem

Typical activities

- Specifying acceptable contractual terms and conditions to protect your business
- Creating a governance program based on ITIL management principles
- Identifying essential and "risky" suppliers and classifying services by levels of criticality
- Designing, implementing, and maintaining governance programs for service providers
- Training of contract owners on third-party management expectations
- Providing ongoing support of "outsourced" vendor management programs


Compliance Obligations
Vendor Assessment Workflows
API Integrations to Intelligence Providers
Risk Treatment and Control Management
Camms.Risk
Third Party Risk Management
Analytics and Reporting
Asset Register
External Web Portals and Questionnaires

Resiliency & Recovery

Ensure your organization is well-prepared for significant operational challenges and disaster scenarios in close alignment with the resiliency demands of your key business processes

Objectives

- Identify the key assets and processes of the organization
- Understand primary risk factors to health and human safety and other business objectives
- Consider different methods of ensuring availability during disruption
- Establish principles and expectations for resiliency
- Develop guidance and raise awareness of expectations; meet cultural and regulatory expectations
- Be prepared in the event of a disruption and reduce the potential negative impact on the organization

Typical activities

- Identifying crown jewels and key processes of the organization
- Conducting a BIA (Business Impact Analysis) and risk analysis across people, process, and technology
- Developing the BCM (Business Continuity Management) strategy
- Creating enterprise guidance in the form of policies and standards
- Designing and establishing the business continuity plan and supporting procedures
- Testing the BCM plan using table-tops, simulations, and real exercises
- Providing feedback, training, and coaching to the internal team

Offensive Security

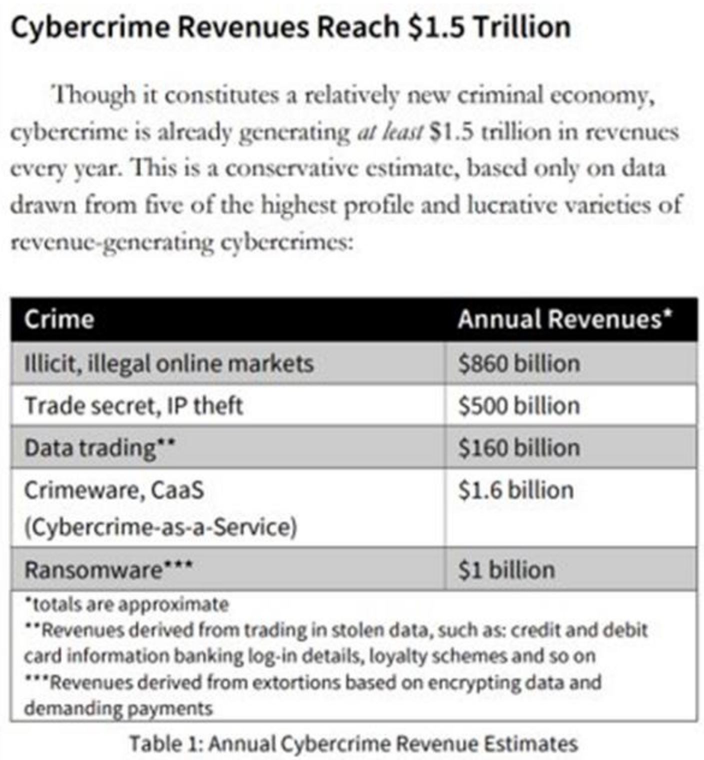
Proactively identify and address weaknesses while being prepared to prevent, detect, and respond in a timely manner to the most common threats that can impact the lifeblood of your business

Benefits

- Build muscle memory by leveraging our skilled resources to simulate real campaigns
- Allow quick identification and correction of weaknesses
- Improve the detection and response capabilities of your team
- Ensure you are able to focus on protecting the right assets with the right set of controls

Typical activities

- Immediate Threat Analysis / Breach and Attack Simulation (BAAS)
- Infrastructure / Network penetration testing
- Web & mobile penetration testing
- Security Incident Table-Top exercises
- Ethical Hacking
- Rogue/Trusted Insider Analysis
- Red/Purple Teaming
- Employee Awareness Campaigns



Cybercrime Revenues Reach $1.5 Trillion

Though it constitutes a relatively new criminal economy, cybercrime is already generating *at least* $1.5 trillion in revenues every year. This is a conservative estimate, based only on data drawn from five of the highest profile and lucrative varieties of revenue-generating cybercrimes:

Crime	Annual Revenues*
Illicit, illegal online markets	$860 billion
Trade secret, IP theft	$500 billion
Data trading**	$160 billion
Crimeware, CaaS (Cybercrime-as-a-Service)	$1.6 billion
Ransomware***	$1 billion

*totals are approximate
**Revenues derived from trading in stolen data, such as: credit and debit card information banking log-in details, loyalty schemes and so on
***Revenues derived from extortions based on encrypting data and demanding payments

Table 1: Annual Cybercrime Revenue Estimates

PCI-DSS Compliance

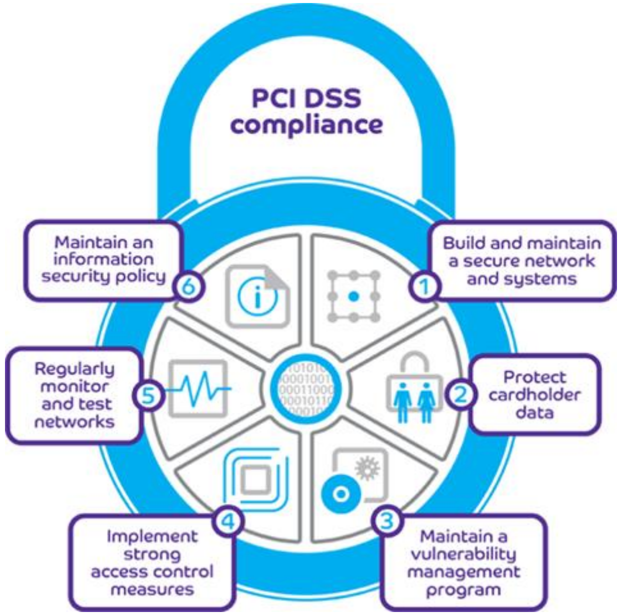
Validate that your organization has adopted practices and controls that meet the recently enhanced requirements of the PCI council while ensuring a suitable level of compliance at an appropriate level of investment

Benefits

- Improve our information security posture and achieve compliance with the Payment Card Industry Data Security Standard (PCI-DSS) mandated by card processors (i.e. Visa, Mastercard, American Express, etc.).
- Develop and reach broad consensus on a cross-functional strategy, solution roadmap, and implementation plan leading to stronger information security controls and eventual compliance with PCI-DSS
- Understand your most critical information risks and ensure there are adequate treatment plans
- Prioritize the most critical treatment options and make better investment decisions using limited funds\
- Simplify understanding of complex situations and develop messaging that resonates with the board and executive management

Typical activities

- Performing stakeholder orientation & executing a comprehensive PCI gap analysis
- Analyzing current systems against the PCI categories and controls in the areas of Network Security, Data in transmission, Data at rest, Systems Security, Application Security, Vulnerability Management Program, Access Control, Monitoring and periodic Testing, and Security Policies/Procedures
- Developing and reviewing alternative options, discussing implications and reaching decisions with stakeholders
- Developing potential “target state” solutions for key applications, systems, and platforms
- Creating a multi-year roadmap to attain PCI Compliant computing environment by leveraging stakeholder preferences gathered during workshops and interviews



PCI DSS compliance

1 Build and maintain a secure network and systems

2 Protect cardholder data

3 Maintain a vulnerability management program

4 Implement strong access control measures

5 Regularly monitor and test networks

6 Maintain an information security policy

SWIFT Advisory & Audit

Obtain a 360-degree view of your SWIFT Information Security program based on SWIFT's compliance requirements

Benefits

- Understanding and articulating how information security must be established according to SWIFT's requirements
- Clearly align the Information Security decisions required with the organization's commercial strategy
- Establish a clear multi-year strategy backed by an investment route to comply with changes and improved compliance in SWIFT
- Simplifying the understanding of complex situations and developing messages that result with the board of directors and the executive management on the requirements that SWIFT demands

Typical activities

- Conducting 360-degree meetings with LOB heads and executive management
- Review governance decisions in the context of your business model aligned with the changes and updates to controls required by SWIFT
- Evaluate the convergence of the information security strategy based on SWIFT with that of the organization in general
- Carrying out a maturity assessment against key standards such as ISO 20022

Privacy Program Definition

Confirm your data protection strategy provides customer value and is in compliance with different regulatory frameworks related to state, country, and industry-specific privacy legislation

Benefits

- Reduce the probability of fines or lawsuits
- Establish corporate expectations for dealing with sensitive personal information
- Understand your most critical privacy risks and ensure there are adequate treatment plans
- Prioritize the most critical treatment options and make better investment decisions using limited funds
- Simplify complex privacy requirements and develop messaging that resonates with the board and executive management

Typical activities

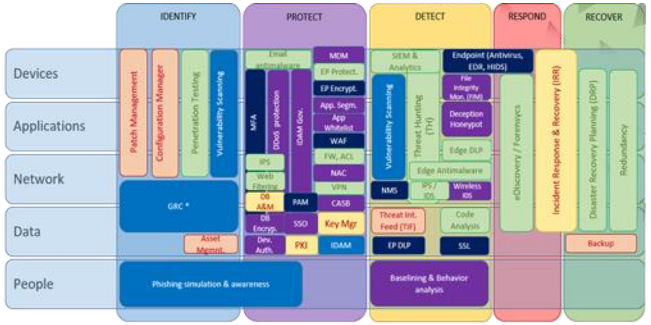
- Identifying key PII data types that are processed across critical business applications & IT systems
- Performing a data inventory/mapping exercise
- Interviewing IT/Biz stakeholders to understand data usage and controls
- Gathering evidence of data/controls in place using a customized privacy questionnaire (DPIA)
- Documenting the data life cycle by mapping key business/data processing flows including how data is collected/stored/transferred through the organization and 3rd party vendors
- Performing a gap analysis by data type against the specific element controls required versus the controls that are currently in place
- Identifying and prioritizing control gaps as per applicable compliance requirements
- Creating and seeking funding for a prioritized roadmap to address the identified gaps

InfoSec Program HealthCheck

Obtain a 360-degree view of your Information Security, Risk, and Governance functions to understand your specific risks, strengths and weaknesses, while setting program priorities and the underlying investment roadmap

Benefits

- Understand your top risks and articulate how Information Security can best provide value to business partners
- Clearly align Information Security decisions with the Core Values and business strategy of the organization
- Establish a clear multi-year strategy supported by an investment roadmap
- Integrate internationally recognized principles and frameworks within the context of your program
- Simplify understanding of complex situations and develop messaging that resonates with the board and executive management



Typical activities

- Performing 360-degree meetings with LOB heads and executive management
- Reviewing governance decisions in the context of your business model
- Comparing your risk management approach against the 3-lines of defense paradigm
- Evaluating the convergence of the Information Security strategy with that of the broader organization
- Conducting a top risks workshop against Crown Jewels to better understand the potential financial impacts
- Conducting a maturity assessment against key standards such as ISO and NIST-CSF
- Tuning the Information Security strategy and investment roadmap to address key risks

RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
CYBERSECURITY FRAMEWORK VERSION 1.1

Cyber Risk Quantification (based on FAIR)

Quantify the financial implications of your organization’s most important Information Security risks and develop messages that resonate with the BOD and Executive Management

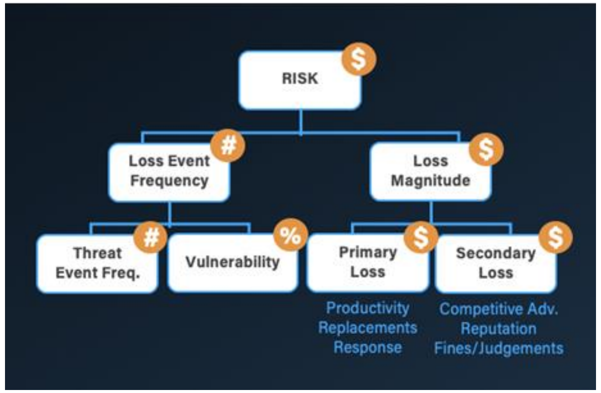
Benefits

- Understand your most critical information risks and ensure there are adequate treatment plans
- Effectively communicate information risks in financial terms with key decision makers such as the BOD, management team, senior executives, and other governance bodies
- Build a robust knowledge base that facilitates understanding the impact of critical risks on the business and improves investment decision-making overall
- Prioritize the most critical risk treatment options and make better investment decisions using limited funds
- Understand how different investments reduce your exposure to loss in financial terms and develop an optimal investment roadmap focused on management of information risk

Typical activities

- Training of personnel on the FAIR methodology
- Facilitating workshops and conducting interviews to understand key business processes and critical systems
- Collaboratively leading cross-functional working sessions to identify and quantify key risks
- Evaluating the impact of different controls on specific scenarios and in aggregate
- Adjusting and enhancing the Information Security strategy to drive financial reduction in risk
- Developing an optimized initiative roadmap to address risks
- Creation of materials for communicating to the BOD and Executive management
- Regular reporting of progress against plan and demonstrating how risk is being addressed in financial terms

FAIR INSTITUTE



Questions?

Management Team

Our team of seasoned professionals has led projects around the world for many of the largest and most recognized organizations, providing **MAKINSIGHTS** with deep domain expertise in **IT Strategy, Governance, Risk Management, Compliance, Privacy and Cybersecurity**

MARC KREVINGHAUS
MANAGING PRINCIPAL
President ISC2 - Peru

FELIPE CASTRO
Consulting Director

ANDRÉS AYBAR
Consulting Director

ANGEL LAY
Commercial Director

Contact Us

MāKINSIGHTS
Accomplish together

✉ ideas@makinsights.com

🌐 MAKINSIGHTS.com