How Do You Assess Risks & Prevent Data Loss?

TRANSFORM CYBER CONFIDENTIALITY, AVAILABILITY & PRIVACY WITH SGS SOLUTIONS

CYBER & DATA PROTECTION

BE THE BENCHMARK

WHEN YOU NEED TO BE SURE

SGS

Security Threats Facing Top Industries

Organizations regularly face digital security threats, regardless of size or sector. As technology evolves and consumer needs shift, modern businesses are under increased pressure to ensure that their data is safe, while continuing to provide an optimal customer experience.

While the security of business and customer data is a top priority, many organizations find themselves lacking the technical expertise and resources to develop, implement and monitor effective data protection measures. This often results in large fines, loss of stakeholder trust and a tarnished brand image.

As business continue to become digital they will require more comprehensive solutions that help maintain the safety of their data, across all aspects of their operations. Taking this into account, SGS provides a suite of digital security services designed to meet these needs. We partner with our clients to assess, execute and optimize various areas of their digital processes to help mitigate any potential disruption caused by digital security threats.

PREPARING FOR THE FUTURE

Digital systems have become an integral part of business operation. For this reason, ensuring the safety and efficiency of these systems is critical to reducing disruption. As companies try to keep up with current trends in data protection, new and unpredictable risks continue to occur. Threats need to be regularly evaluated with a combination of technology and human efforts from all aspects of the company, not just IT.

Increasingly, the general public is demanding heightened security measures for their data. Governments across the globe are working on implementing various regulations in order to establish a base line, resulting in large fines for businesses if they are found to be noncompliant.

TOP AFFECTED INDUSTRIES

HEALTHCARE

41.4 million patient records breached in 2019, fueled by a 49% increase in hacking, according to Protenus Breach Barometer.

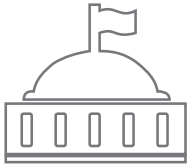
MANUFACTURING

50% of manufactures experienced data breaches, and 11% said they had experienced "major" breaches, according to a Sikich report.

FINANCIAL SERVICES

Financial firms are hit with approximately 300 times more cyber attacks than businesses in other industries, according to a report from Boston Consulting Group.

GOVERNMENT AGENCIES



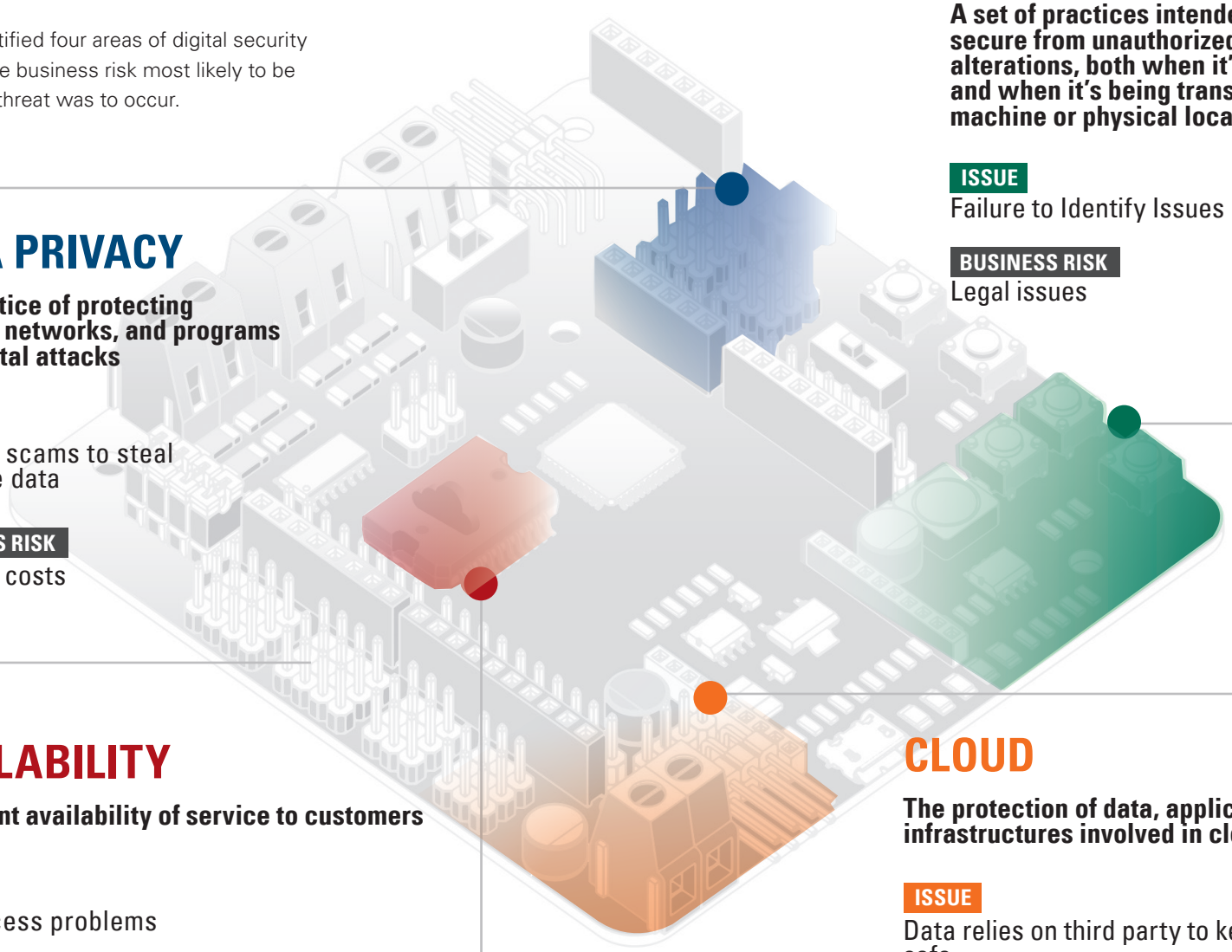
160 Million Government Records Exposed in Data Breaches from 2014-2019, according to reports by the Identity Theft Resource Center.

EDUCATION

Education districts and agencies had 3 times the reports in 2019 as they did in 2018, according to a report from the K-12 Cybersecurity Resource Center.

At Risk Areas for Data Threats

We have identified four areas of digital security threats and the business risk most likely to be impacted if a threat was to occur.



DATA PRIVACY

The practice of protecting systems, networks, and programs from digital attacks

ISSUE
Phishing scams to steal sensitive data

BUSINESS RISK
Financial costs

INFORMATION SECURITY

A set of practices intended to keep data secure from unauthorized access or alterations, both when it's being stored and when it's being transmitted from one machine or physical location to another

ISSUE
Failure to Identify Issues

BUSINESS RISK
Legal issues

AVAILABILITY

Consistent availability of service to customers

ISSUE
Data access problems

BUSINESS RISK
Disruptions to customers

CLOUD

The protection of data, applications, and infrastructures involved in cloud computing

ISSUE
Data relies on third party to keep information safe

BUSINESS RISK
Loss of client data & customer trust

Linking Industry Pain Points to Business Impact

To gain a holistic understanding of the potential security risks to businesses, SGS has developed a methodology that utilizes our compliance data to identify the overall top pain points and business impact events. This data was collected from the top certification standards. This analysis was based on the data collected from ISO 27001, the top standard on how to manage information security.

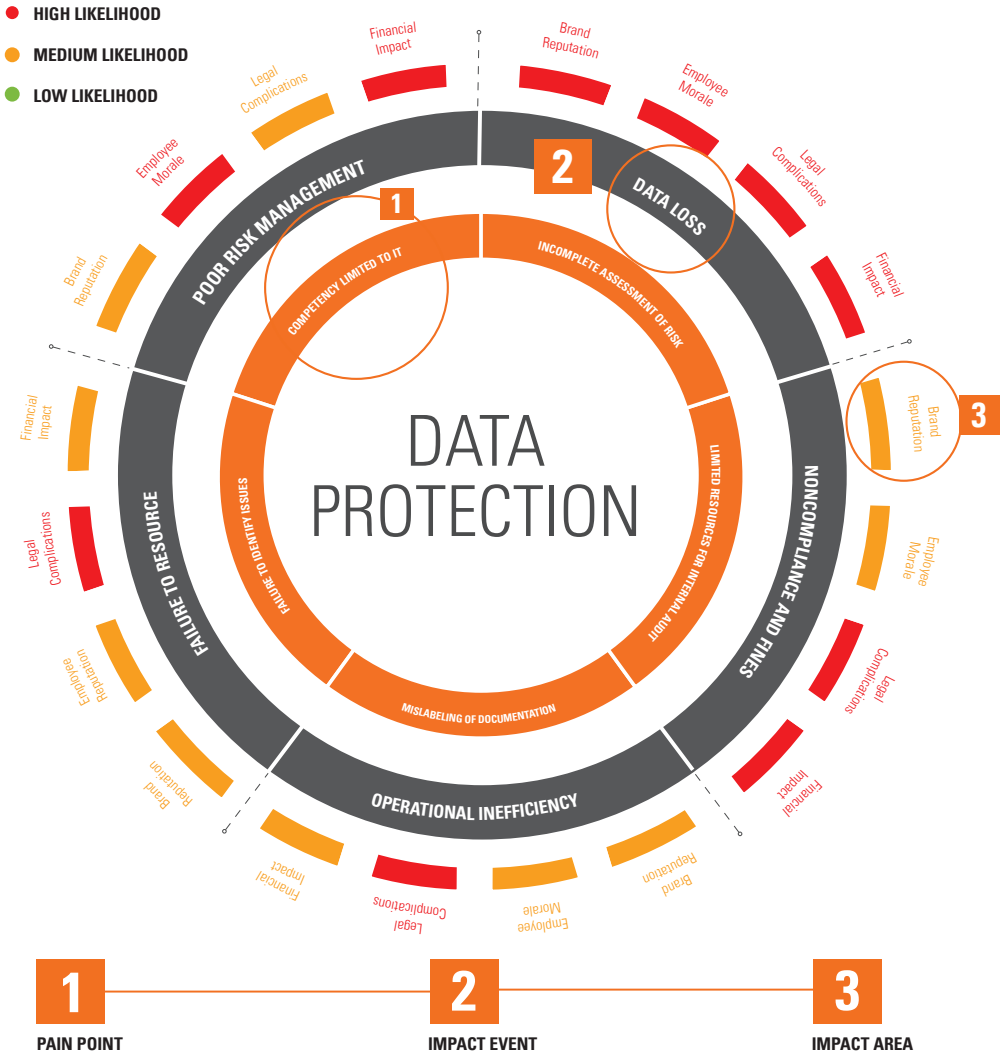
The graphic on the right highlights this process by identifying:

- Top industry pain points
- Impact events most likely to occur
- Impact areas with the highest business risk

KEY INDUSTRY FINDINGS

Our analysis indicates that the events with the highest risk revolved are:

- Data Loss
- Noncompliance and Fines
- Operational Inefficiency
- Failure to Resource
- Poor Risk Management



DATA SPECIFICATIONS

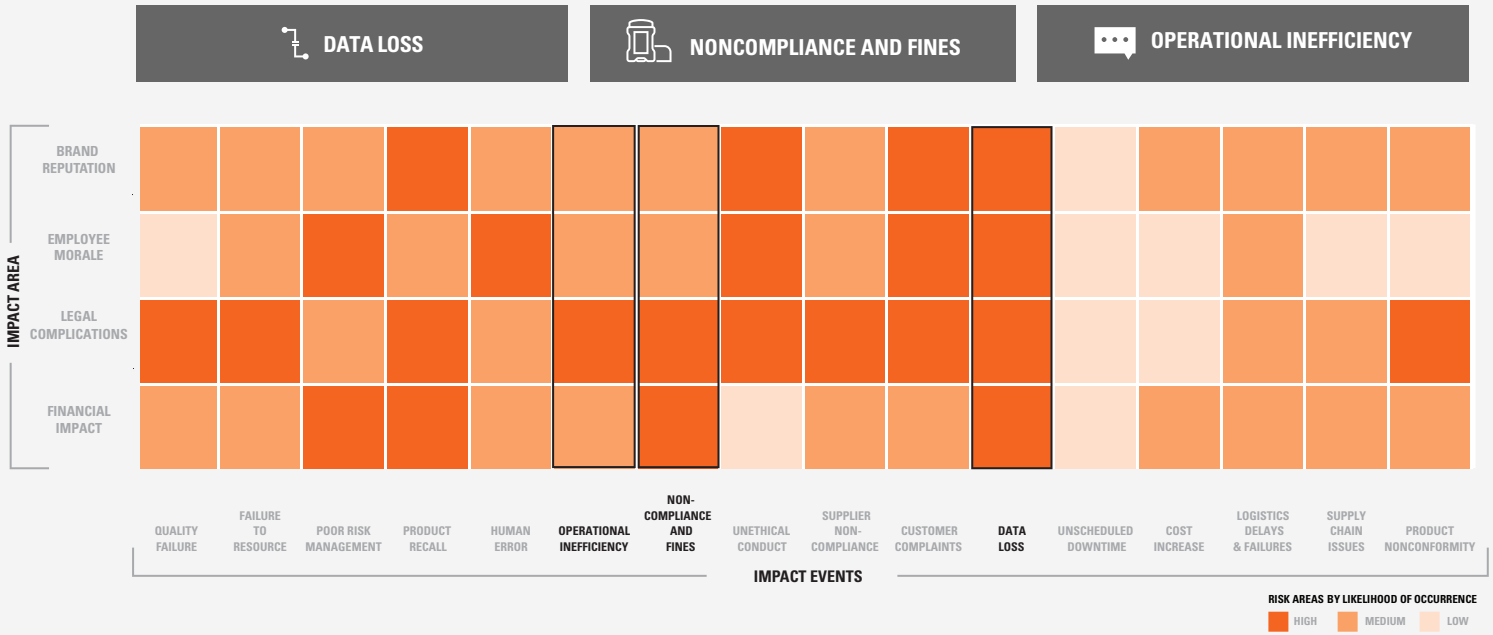
5,000 DATA POINTS

2,000 CERTIFICATES ISSUED

Linking Impact Events to Business Risk

Our analysis has identified operational inefficiency, noncompliance and fines, and data loss as the impact events most likely to occur. The heat map below highlights these three events and allows us to see how they all impact each of the four impact areas. Financiel Impact and Legal Complications are most at risk if these three impact events occur.

EVENTS WITH HIGHEST RISK IMPACT:



1. Understand the industry landscape by seeing how key areas of your business are impacted by the identified events.
2. Identify the top three events based on # of occurrences and see how they rate (low, medium, high) against the 4 impact areas.
3. The dark orange boxes showcase the area most likely to be affected by these events.

SGS Solutions

SGS provides a variety of services to help mitigate data protection risks. We offer certification and training services addressing issues in Cloud Security, Information Security, Data Privacy and Availability.

OUR SERVICES

ISO 20000: Information technology — Service management
Part 1: Service management system requirements

ISO 22301: Societal security — Business continuity management systems — Requirements

ISO 27001: Information technology - Security Techniques - Information security management systems — Requirements

ISO 27017: Code of practice for information security controls based on ISO/IEC 27002 for cloud services

ISO 27018: Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

ISO 27701: Information technology - Security Techniques - Information security management systems —
Privacy Information Management System

WLA-SCS-2020: The standard for WLA members give assurance to all their stakeholders that security is one of their highest priorities

GDPR Certification: delivers gap analysis and certification of compliance

Penetrative Testing: provides a picture of cybersecurity resilience and the weak points in infrastructure and processes.

Supply Chain Audits: a vendor audit program to independently assess compliance across the supply chain

RISK AREAS

SERVICE OFFERING	CLOUD	INFORMATION SECURITY	DATA PRIVACY	AVAILABILITY
ISO 20000				✓
ISO 22301	✓			✓
ISO 27001		✓	✓	
ISO 27017	✓	✓		✓
ISO 27018	✓		✓	
ISO 27701		✓	✓	
WLA-SCS-2020	✓	✓		
GDPR Certification			✓	
Penetrative Testing		✓	✓	
Supply Chain Audits	✓			

SGS Academy Training Courses

SGS has the capabilities in place to deliver consistent, effective and high-quality training for Cloud Security, Information Security, Data Privacy and Availability.

ISO/IEC 27001:2013 – INFORMATION SECURITY MANAGEMENT SYSTEMS – AUDITOR/LEAD AUDITOR TRAINING

This training course is designed to give you the relevant skills and knowledge to carry out audits of Information Security Management Systems (ISMS) against ISO 27001 standards.

ISO/IEC 27001:2013 – INFORMATION SECURITY MANAGEMENT SYSTEMS – INTERNAL AUDITOR TRAINING

This course has been designed to equip participants with the knowledge and skills needed to assess and report on the conformance and effective implementation of an information security management systems (ISMS) to protect organizations from risk.

ISO/IEC 27001:2013 – INFORMATION SECURITY MANAGEMENT SYSTEMS – AWARENESS TRAINING

The objective of this training is to introduce participants to the purpose and requirements of ISO/IEC 27001 Information Security Management Systems (ISMS) as a tool for business improvement.

IMPLEMENTATION COURSE - BUSINESS CONTINUITY MANAGEMENT SYSTEMS

This training provides a framework to help in implementing Business Continuity Management (BCM). The training is based on the Business Continuity Management Systems standard ISO 22301.

LEARNING MANAGEMENT SYSTEM

SGS Academy has a customized Learning Management System (LMS), fully integrated with our global training schedule. It provides management and employees with direct online access to relevant training programs and continuous professional development. SGS Academy LMS makes learning easier to organize, record and undertake. It has several advantages for learners and management.

FOR LEARNERS

- **Intuitive:** uses recognizable online methods to enhance the training experience
- **Effective:** uses client data to target relevant courses, promoting continuous professional development
- **Transparency:** all training is recorded and can be accessed at any time

FOR MANAGERS

- **Reports:** has a relevant number of reports available. Managers can access the data they need in a suitable format
- **Invoicing:** complete control over invoicing, allowing budget supervision
- **Resource management:** provides complete command over all aspects of staff training

PLEASE VIEW THE WORLDWIDE COURSE SCHEDULE AT WWW.SGS.COM/TRAINING

CONTACT SGS


www.sgs.com


www.sgs.com/facebook


www.sgs.com/twitter


www.sgs.com/linkedin


certification@sgs.com

WWW.SGS.COM

WHEN YOU NEED TO BE SURE

SGS