THE POWER
OF BEING
UNDERSTOOD

CYBERSECURITY READINESS AND INCIDENT RESPONSE SERVICES

Strategies to effectively remediate risks and thoroughly investigate and combat information security incidents.

No organization is completely safe against cyberattacks; unfortunately, it is not a matter of if you will experience an incident, but when. RSM can help you understand your information security risks, develop a readiness strategy and effectively respond to an incident, thereby limiting your exposure.

The complexity and number of cybersecurity incidents are steadily rising, as is your organization's financial and reputational risk of harm. Businesses are generally not properly prepared; controls aren't scalable as technology grows, and data collection and storage become daunting. Government and regulatory agencies are also taking a proactive approach to challenge your security posture.

RSM's global cybersecurity advisors provide a wide range of solutions to help you identify and mitigate risks. We work closely with data privacy attorneys and cyberinsurance carriers to protect your enterprise value, understand legal and regulatory requirements and effectively respond to and investigate cyber-related incidents.

Information security threats are extremely diverse and constantly evolving. Cyberattacks may come in the form of malicious software, skilled cybercriminals and rogue employees. A data breach will significantly impact your organization, both in the near- and long-term, and the methodical tasks associated with responding to such incidents can be complicated. You need an experienced team that understands the magnitude of the challenges you face and will help you navigate the path to readiness.

Readiness: The first line of defense

Information security requires your entire organization's awareness to help protect sensitive data and intellectual property. RSM's experienced advisors help you proactively recognize your risks and vulnerabilities by identifying personal and sensitive data you possess, closely evaluating your existing administrative and technical controls and developing a remediation road map for a stronger cybersecurity posture.

IT risk assessment: We evaluate your infrastructure or third-party vendors using a chosen framework (ISO 27001, NIST, HIPAA, FISMA) to identify gaps, including legal or regulatory requirements. Our advisors also perform a high-level evaluation of your overall information technology (IT) organization and application environment for overall fit, as well as coverage and controls. In addition, we identify and inventory electronically stored information containing sensitive data.

Network vulnerability testing: Our team identifies IT security weaknesses within your networks and Web application environment utilizing secure, flexible remote assessment solutions driven by experienced staff. We will identify vulnerabilities and develop recommendations to protect your infrastructure.

Incident response planning: Organizations should build and maintain an incident response plan that addresses a variety of incidents. Our team assists your organization to identify gaps in your written plan, and conducts tabletop and simulation exercise drills to assess the effectiveness of your response team and plan.

Security awareness training: Technology is not the only approach to securing your IT infrastructure. Organizations need to "secure the human" through employee education and awareness. RSM offers live and online training customized to your industry with all materials provided for future use.

Red team exercises (ethical hacking): Security testing serves as a vital quality assurance function of your security strategy and controls to protect critical data. A red team is a group made up of various specialists in different aspects of offensive security. RSM deploys red teams to perform blended methods of testing, including physical, social engineering, as well as application, network and wireless hacking.

Payment Card Industry (PCI) compliance: Named by the PCI Security Standards Council (PCI SSC) as a Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV), RSM has an experienced team of information security consultants who help your organization maintain compliance with PCI Data Security Standards (DSS) version 3.0.

Incident response services

With a situation as critical as a cybersecurity incident, you need someone in your corner who understands the magnitude of the threat and how to limit your exposure. When it happens, we will assist you through the dynamic and elaborate process of determining the scope of the incident and helping you mitigate the further risk of harm. The RSM professionals who will work with you have wide-ranging experience within the forensics and response fields, including law enforcement, military, intelligence and corporate investigations.

Incident response: In the event of a cybersecurity incident, we respond quickly to identify and confirm the issue, providing assistance to contain and prevent further risk of harm. Whether you suffer from malware expanding across your network, unauthorized access or a denial of service attack, our experienced team is ready to respond. We also help identify and preserve information that can be used in an investigation or later proceedings.

We also offer the ability to deploy industry-leading incident response tools through our strategic partnerships with FireEye™ and Bit9 + Carbon Black. These tools offer a robust solution for incident response investigation and remediation support.

Digital forensics: Unlike paper evidence, computer evidence is extremely volatile and requires specialized knowledge and experience for identification and analysis. Our on-site and remote solutions are effective for conducting analysis and recovery of computer systems and networks.

Our team uses an approach designed to:

- Protect your computer systems and evidence from any possible alteration, damage, data corruption or virus introduction
- Perform malware analysis and remediation tasks
- Identify deletion of files and use of wiping utilities
- Detect and recover deleted files
- Identify user habits, such as Internet activity, file transfers, email addresses and timeline analysis
- Provide expert consultation and testimony as required

After we determine the sources of the data at risk, we perform an analysis to identify protected information elements, such as personally identifiable information (PII) and protected health information (PHI).

The RSM difference

RSM is a leading national provider of industry-focused professional services. We have a team of over 50 dedicated security and privacy professionals in the United States, with deep hands-on experience covering a wide range of industries. We hold numerous industry certifications including Certified Ethical Hacker (CEH), GIAC Penetration Tester (GPEN), GIAC Reverse Engineer of Malware (GREM); GIAC Certified Forensic Examiner (GCFE); GCIA Certified Information Security System Professional (CISSP); Certified Information Systems Auditor/Manager (CISA/CISM); and Certified Information Privacy Professional (CIPP).

Our depth of experience enables us to understand your cybersecurity threats, no matter how complex or where they originate. Whether you need an experienced team to provide incident response services on short notice, or assistance in developing your internal forensic and response capabilities, we're ready to help.

+1 800 274 3978
www.rsmus.com

This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute audit, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person. RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International. RSM® and the RSM logo are registered trademarks of RSM International Association. *The power of being understood®* is a registered trademark of RSM US LLP.