THE POWER OF BEING UNDERSTOOD

INCIDENT RESPONSE SERVICES

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

The increasing complexity and number of cybersecurity incidents occurring globally can significantly affect your organization. Regardless of the level of planning and preparation, no organization is completely safe against cyberattacks.

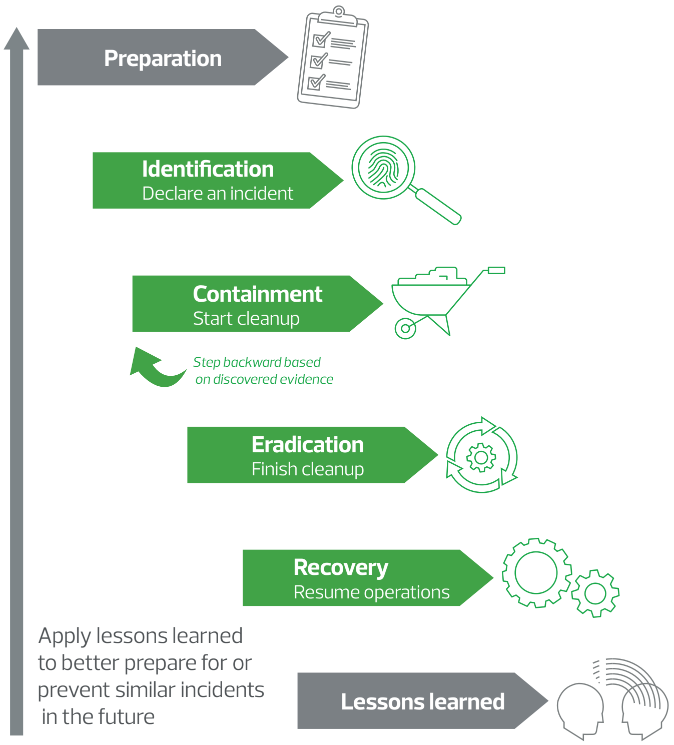
Today, cyberattacks come from fully formed criminal organizations seeking to monetize an attack in the quickest and easiest manner. Gone are the days of individuals attacking organizations largely for entertainment.

RSM Canada's experienced team is frequently called upon to respond to active cyberattacks and incidents that plague our clients, including:

- Ransomware
- Business email compromise
- Web application compromises
- Data theft and data loss

When an organization experiences a cyberattack, we respond quickly to identify and confirm the issue, providing assistance to contain and prevent further risk of harm. We also help identify and preserve information that can be used in an investigation or later proceedings.

Incident response is a cyclic process. Identifying an incident early is critical in mitigating risk. This takes preparation, planning and practice to ensure that you have an effective strategy and plan when you need it. If you are not experiencing an active incident today, your organization should be taking the time to process lessons learned from prior cyber events and to implement improvements to ensure that you are better prepared for future problems.



Ransomware

Ransomware attacks are designed to deny you access to a computer system or data until a ransom has been paid. We can help your organization perform an investigation to better understand the scale, nature, impact and risks associated with an attack.

In addition, organizations frequently need assistance in recovering from a ransomware attack. We leverage industry–leading endpoint detection and response tools that are robust and scalable to help with the recovery effort. In addition, you may need additional or specialized resources to ensure a swift and safe recovery. We can deploy these remediation and recovery solutions at a moment's notice.

Business email compromise

Cybercriminals regularly attack organizations in an attempt to gain access to their email systems, then leverage their access to facilitate financial fraud. Quickly identifying and taking back control of a hijacked email account is critical in mitigating risk; however, the response should not stop there. We have developed a workflow to acquire and review forensic artifacts from a variety of email platforms to determine how the cyber criminals were able to take over affected account(s), what the attackers may have done while they had access to the account, and whether they attempted to expand their attack to additional accounts or systems.

Web application

Vulnerable web applications are one of the leading causes of major breaches. Web applications have large attack surfaces not only because they are inherently accessible from untrusted networks and individuals, but also because they support and provide a large number of services, data sets, user-interaction and business functionality.

Our web application incident response approach is modeled on the same approach used by our web application penetration testers and is not limited to running an automated tool set. The combination of planning, discovery, analysis and attack techniques is correlated to ensure that a complete web application analysis is performed.

Our investigation uses elements and inputs from The SANS Institute, MITRE and Open Web Application Security Project, as these standards are currently considered to be among the best in the industry for application security, design and approach. These elements help build the foundation for our investigative approach and provide our incident responders a method to peel back the application and incident to help identify the attack surface, authentication and authorization impacts, server and logging configuration impacts, and malware and persistent capabilities; this approach also helps us determine if the compromise facilitated data staging or data theft through the vulnerability.

Data theft or loss

Data theft and data loss can come in many forms, such as unauthorized access by an attacker, system misconfigurations leading to vulnerabilities that expose data, employee error or an insider threat. We work collaboratively with your organization to learn as much as we can about the event and the affected systems and the scope of the incident. We use this information to develop an approach and methodology for identifying and investigating various evidence sources. Throughout the process, we will define indicators of compromise that we will use to correlate events and evidence sources that will be reviewed to determine if evidence data was accessed, viewed, acquired or exfiltrated in an unauthorized manner.

The RSM advantage

RSM Canada is a leading national provider of industry-focused professional services that can offer you a customized forensic approach based on your needs. The RSM professionals who work with you have wide-ranging experience within the forensics and response fields, including in law enforcement, military, intelligence and corporate investigations.

Cybercriminals continue to develop new attack approaches and methods; your organization needs to continually develop its cybersecurity program with the same persistence.

Whether you are looking to mature your security program or are looking to better understand the impacts of regulation, RSM's risk consultants combine industry and technical experience to tailor our approach to your unique business. This allows us to identify your highest risks and help plan for protection and compliance, both now and in the long term.

We work with you to:

- Assess physical, cyber and personnel vulnerabilities from various attack scenarios
- Design, implement and manage your enterprise security program
- Develop a program to proactively comply with evolving data privacy regulations
- Build a compliance program that aligns to various regulations such as GDPR, PCI, NIST, HIPAA and PIPEDA
- Develop an agile governance structure across all facets of security that aligns with your business strategy
- Build a culture and awareness around key cybersecurity considerations

+1 855 420 8473
rsmcanada.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 Canada LLP, RSM Alberta LLP and RSM Canada Consulting LP, and their affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person. This communication is being sent to individuals who have subscribed to receive it or who we believe would have an interest in the topics discussed.

RSM Canada LLP is a limited liability partnership that provides public accounting services and is the Canadian member firm of RSM International, a global network of independent audit, tax and consulting firms. RSM Alberta LLP is a limited liability partnership and independent legal entity that provides public accounting services. RSM Canada Consulting LP is a limited partnership that provides consulting services and is an affiliate of RSM US LLP, a member firm of RSM International. The firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmcanada.com/aboutus for more information regarding RSM Canada and RSM International.