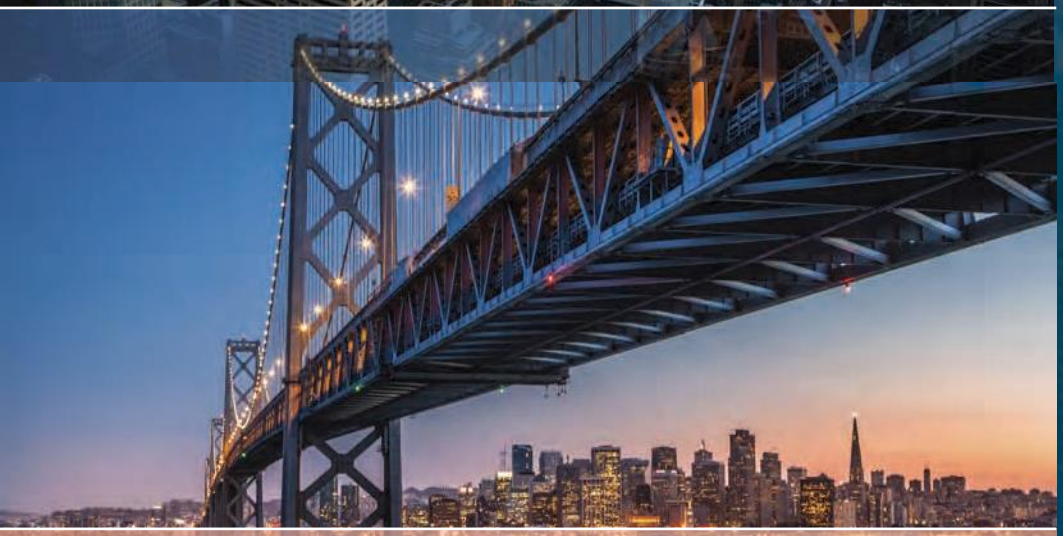
PROTECTION | INSURANCE | EDUCATION | RESPONSE



RIDGE™
CANADA

RANSOMWARE

RISK MANAGEMENT

RANSOMWARE - CYBER SECURITY "DO's & DON'TS"

As more organizations digitize their operations and employees use technology and work remotely, the potential number of entry points for attackers increases significantly. More ransomware variants are leveraging vulnerabilities in remote desktop protocols to enter the network and are taking advantage of unpatched systems and zero-day exploits.

Below are some practical tips that can be implemented to reduce the probability of an incident and reduce the severity of an incident in the event that systems do become compromised.

PREVENTION:

1. ***Maintain strong backups, which are encrypted, segregated and tested:***
    a. Encryption of sensitive data at rest should be applied. If unencrypted data is accessed in a ransomware incident, there is higher potential of the requirement to report the incident to regulators.
    b. Periodically test backups to ensure they are working properly and can be restored.
    c. Maintain backups offline or on a separate back up network to prevent attackers from moving laterally through the network.

2. ***Employ endpoint threat detection on each agent within the network:***
    a. Machine learning based software should be able to identify known threat signatures, or at minimum, sandbox unknown processes that are running on each agent.
    b. Implement processes to generate alerts and log cybersecurity events in response to anomalous activity. Review the logs and respond to alerts in a timely manner.
    c. Ensure that endpoint threat protection is installed on all endpoints **including** personal mobile devices if a "Bring Your Own Device" policy is in place.

3. ***Staff Training:***
    a. Phishing awareness training for employees can increase the probability of employees recognizing and reporting phishing emails. Provide security awareness briefings to staff and consider implementing an email-threat filter.
    b. Organizations should have policies that describe security training requirements and include training in the following:
        - Security Awareness
        - Security Incident Recognition
        - Reporting procedures for personnel & contractors
    c. Provide security training, and include incident response-training, to personnel-assigned security duties upon hiring and thereafter.

4. ***Patch Management:***
    a. Ensure that your organization has a plan in place to manage regular and timely deployment of updates and patches and ensure critical patches are updated in a timely manner.
    b. Disable unnecessary and vulnerable services.
    c. Do not use software or firmware that is no longer supported by the developer, such as Windows 7. If you absolutely must, ensure this software is being run on air-gapped networks that are not connected to the internet.

RESILIENCE:

1. ***Business Continuity Plans and Incident Response Plans:***
    a. Have a chain of command internally & externally and assign tasks with multiple individuals having authority if the first designated individual cannot be reached during a time of crisis.
    b. As speed of response to an incident is critical, ensure a copy of the incident response plan is easily accessible for everyone involved. This could mean having a physical copy or having the contact information of all parties stored in a personal phone that is not connected to corporate networks.
    c. Identify external stakeholders and build them into the response plan. Make sure that all parties understand when to escalate issues to designated external parties.

2. ***Log Management and Forensic Tool Deployment:***
    a. Deploy in conjunction with Security Incident and Event Management Technology
    b. Attackers commonly install other malware and exploit kits on endpoints and networked systems. The risk of follow-on attacks from lingering software can be mitigated by forensic specialists.
    c. Performing root cause analysis to understand what happened then modifying policies and processes to prevent similar incidents from recurring is necessary.

3. ***Cyber Insurance and Notification:***
    a. Cyber Insurance exists to supplement the in-force risk management procedures as a backstop
    b. Understanding how and when to notice the policy will prevent using the policy incorrectly which could limit the amount of recoverable costs and expenses
    c. Noticing as soon as possible will provide you access to specialists who have expertise in responding to cyber incidents.

Ridge Canada Cyber Solutions Inc.
1628-401 Bay Street
Toronto, ON M5H 2Y4

T +1 (647) 643 4737
E contact@ridgecanada.com
www.ridgecanada.insure