BCREA and AXIS Cybersecurity Presentation Summary and Actionable Steps

Thank you for attending our recent cybersecurity presentation at the Community of Practice.

This document summarizes the key points discussed during the presentation and provides actionable steps to manage your cyber risks effectively.

Types of Attacks:

1. Denial of Service (DoS) Attack:
    - Definition: A DoS attack disrupts the normal functioning of a network, system, or website by overwhelming it with excessive traffic or requests.
    - Impact: The target cannot respond to legitimate users or access the systems, causing a denial of service.
2. Credit Card and Password Theft:
    - Definition: Unauthorized acquisition of credit card information and passwords by cybercriminals using hacking, phishing, or malware techniques.
    - Impact: Stolen credit card information can be used for fraudulent transactions, while stolen passwords can lead to unauthorized access to personal or financial accounts.
3. Phishing Attacks:
    - Definition: Fraudulent attempts to trick individuals into sharing sensitive information through deceptive emails, messages, or fake websites.
    - Impact: Personal information like passwords, credit card details, or social security numbers can be compromised.
4. Ransomware and Viruses:
    - Definition: Ransomware encrypts files, making them inaccessible until a ransom is paid. Viruses replicate and infect files or systems, causing various damages.

- Impact: Ransomware leads to data encryption and demands payment, while viruses cause data loss or system malfunction.

5. Social Engineering:
    - Definition: Manipulating individuals to gain unauthorized access or obtain sensitive information using psychological tactics.
    - Impact: Cybercriminals exploit human vulnerabilities to deceive people into revealing confidential data.

Actions to Manage Your Cyber Risks:

1. Discuss this with your IT provider.
2. Always backup your data:
    - Regularly backup critical data.
    - Ensure restore tests are conducted.
    - Follow the 3-2-1 backup strategy:
        - Keep three copies of your data.
        - Store two copies on different media.
        - Keep at least one copy offsite.
3. Protect from Viruses:
    - Install a good antivirus software.
    - Keep antivirus software up-to-date.
    - Scan external USB drives before opening.

Recommended Antivirus Software:

- Paid:
    - Norton: https://ca.norton.com/
    - McAfee: www.mcafee.com
    - BitDefender: www.bitdefender.com

- Free:
    - BitDefender Free Edition: https://www.bitdefender.com/solutions/free.html
    - Avast: https://www.avast.com/en-ca
    - Windows Defender: www.microsoft.com/en-ca/windows/comprehensive-security

4. Account Protection:
    - Use long, complicated passwords.
    - Consider using a password manager.
    - Avoid using the same password for multiple accounts.
    - Enable MFA or 2FA for accounts that offer this feature.
    - Use a VPN when connecting to public Wi-Fi, like NordVPN, SurfShark or ExpressVPN.
    - Keep your systems updated.
    - Avoid clicking on links from unknown or suspicious sources.

5. Protect from Phishing:
    - Look at the email address, not just the sender.
    - Pay attention to poor spelling and grammar.
    - Be cautious of messages that create a sense of urgency.

6. Enroll yourself and your staff in Cyber Security Awareness training. Recommended Cyber Security Awareness Training:

- NINJIO: https://ninjio.com/
- KnowBe4: www.knowbe4.com

7. Contract a Cyber Security Insurance

Axis Insurance Contact Information:

- Website: https://realtor.axisinsurance.ca/
- E-mail: rob.mcleod@axisinsurance.com
- Phone: 604-629-2680

What to Do if You Suspect a Breach:

1. Talk to your IT provider.
2. Activate your Cyber Insurance coverage.

By implementing these actionable steps, you can effectively manage your cyber risks and protect your business from potential threats. If you have any further questions or concerns, please reach out to our team or your IT provider.

Thank you for your attention,

Mairon