Know Your Network:
Tips to Fortify Your Cybersecurity

With cyber technology and threat actors in a race to see who can outsmart whom, protecting your business can seem like a complicated undertaking. With all the patches, antivirus software, and cyber awareness training, you may wonder where to start. The answer? Your network.

Understanding the intricacies of your network, from its architecture to its endpoints, is a foundational principle of effective cybersecurity. Lacking this knowledge leaves critical vulnerabilities unaddressed, making it imperative to grasp the complexities of your network's inner workings to safeguard against ever-evolving cyber threats.

Here are some tips to ignite your cybersecurity fortification journey:

- **Network Mapping and Inventory:**
  Begin with an extensive mapping of your network and create an inventory of hardware and software assets. Knowing what exists in your network is the first step toward securing it effectively. Maintain an updated list of all devices, software, and their configurations.

- **Access Control:**
  Implement stringent access controls and limit access to sensitive data and systems only to those who need it. Regularly review and update access permissions as personnel change and ensure every team member understands their security responsibilities.

- **Incident Response Plan:**
  Knowing what to do in a crisis can minimize damage and downtime. Develop a well-defined incident response plan that outlines the steps to take in the event of a cyberattack. An incident response plan should identify key internal and external stakeholders, as well as cover incident investigation, forensic evidence collection, remediation, return to normal operations, and post-incident analysis for continuous improvement.

- **Regular Vulnerability Scanning:**
  Understanding where vulnerabilities exist allows you to prioritize and address them proactively. Conduct regular vulnerability assessments and penetration tests to identify weak points in your network's security.

- **Security Patch Management:**
  Unpatched systems are often entry points for cyberattacks. Stay vigilant about applying security patches and updates to all network components, including operating systems, applications, and network devices.

- **Monitor and Detect:**
  Proactively spotting potential threats allows for rapid response. Employ network monitoring tools and intrusion detection systems to detect suspicious activities in real-time, enhancing your ability to thwart cyber threats in their tracks.

- **Data Backup and Recovery:**
  Regularly back up your critical data and ensure that backups are stored securely and independently from the primary network. In the event of a ransomware attack, having accessible and uncorrupted backups can help prevent you from falling victim to extortion.

- **Expert Collaboration:**
  Utilizing resources such as an attorney, data breach coach, or cyber insurance advisor can help you devise strategies to fortify your network's security posture. An experienced cyber insurance advisor can partner with you in this continual cybersecurity process by helping you identify potential exposures, offer resources, such as incident response teams, and create customized risk mitigation solutions that align with your unique profile.

The more knowledge you possess, the more power you have to protect your organization's network. We leverage industry-leading technology and relationships with top insurance companies to cultivate solutions to fortify your business for whatever tomorrow holds.

Partner with us to join you on your cybersecurity journey.

INSGROUP
A BALDWIN RISK PARTNER

BRP
CYBER CENTER OF EXCELLENCE