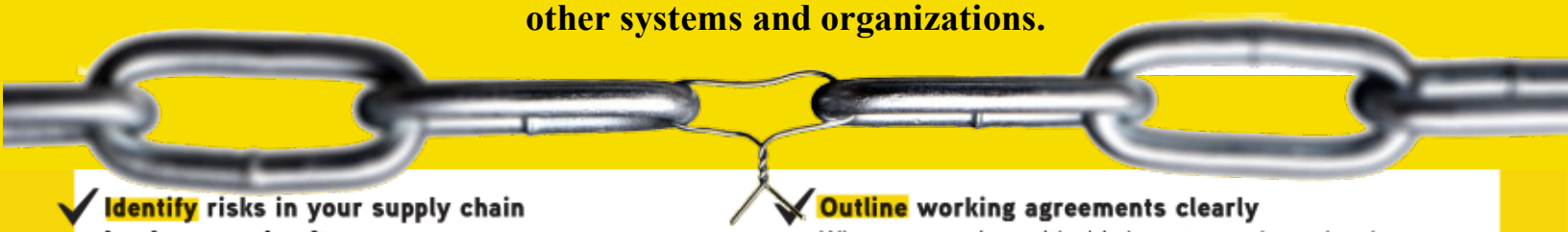
ITNS Consulting
Cybersecurity - Compliance - Managed Services

STRATEGIES TO MANAGE YOUR SUPPLY CHAIN RISKS

Although your relationships with your suppliers and vendors are important to ensure business growth, they can leave you vulnerable to supply chain attacks. These attacks exploit weaknesses within the supply chain to infiltrate systems and cause harm. With the increased prevalence and widespread impact of supply chain attacks, businesses of all sizes and industries must take steps to address gaps within their suppliers' and vendors' environments, as well as their own environment, to avoid becoming superspreader to the other systems and organizations.



✓ **Identify risks in your supply chain hardware and software**
Suffering an attack through your hardware or software can have a devastating effect on your organization. Since purchasing hardware and software from third-party providers carries significant risks, ensure all hardware and software are scanned and tracked to find potential threats.

✓ **Screen external vendors carefully**
It's critical that external and third-party providers go through a rigorous vetting procedure before you choose anyone to partner with. You may even need to expand your verification further if they have additional partners. It's crucial to plan out your vetting procedure before you initiate a partnership with any vendor.

✓ **Restrict access and permission for third-party programs**
Segmenting your network will allow you to separate and limit access to specific vendors within specific departments. Even if your network is compromised, the risks can be contained within a specific segment instead of affecting the entire network.

✓ **Implement a comprehensive cyber defense strategy**
Cyberattacks are becoming more sophisticated every day, and no business is immune. Just taking a proactive approach to preventing suppy chain risks is not enough. You also need a robust incident response plan.

✓ **Outline working agreements clearly**
When partnering with third-party vendors, develop a thorough agreement of their roles to protect the cybersecurity of your company. Both parties must be clear about their expectations and adhere to security best practices.

✓ **Review and audit vendors regularly**
Vendor screening shouldn't be limited to onboarding. They can pose risks to your supply chain at any time, with or without their knowledge. Auditing vendors can help mitigate any product quality or safety issues resulting from their quality control processes. An organization can also measure the performance of a vendor using this approach.

✓ **Create a supply chain incident response strategy**
It's important to develop a full-cycle incident response strategy that encompasses readiness, response and recovery — both from technical and business perspectives. Ensure that your response plan is organization-wide, addresses the actual and potential damage throughout the company, and is continually updated and reviewed.

✓ **Partner with an IT service provider**
Partner with an IT service provider who can offer you an integrated solution suite for vulnerability and patch management in real-time, minimize supply chain risks and build a strong cybersecurity posture for your organization.

ITNS Consulting
Cybersecurity - Compliance - Managed Services

Phone: 608-563-1975
Email: infosec@itnsconsulting.com
Website: https://itnsconsulting.com