How a data breach happens *and how to stop it*

Step 1: **Initial compromise**

Attack vector: Phishing email or malicious link.

Statistic: 95% of data breaches are linked to human error.

Quick fix: Plan regular employee cybersecurity training to recognize and avoid phishing attempts.

Step 2: **Exploitation of vulnerabilities**

Attack vector: Exploiting unpatched software or outdated systems.

Statistic: Outdated technology costs companies in lost productivity, security vulnerabilities, compatibility issues, and high maintenance costs.

Quick fix: Regularly update and patch all software and systems to fix known vulnerabilities.

Step 3: **Credential theft**

Attack vector: Using stolen or weak passwords to gain unauthorized access.

Statistic: 86% of data breaches involve the use of stolen credentials.

Quick fix: Enforce strong password policies and set up multi-factor authentication (MFA).

Step 4: **Data exfiltration**

Attack vector: Transferring sensitive data outside the organization.

Statistic: Nearly half (46%) of all breaches involve customer personal identifiable information (PII).

Quick fix: Monitor data transfers and use encryption to protect sensitive information.

Step 5: **Detection and response**

Challenge: Delayed detection and response can exacerbate the breach impact.

Quick Fix: Implement intrusion detection systems and create an incident response plan to quickly address breaches.

Need help? We can help you stay vigilant and proactive to safeguard your business against data breaches.

Get in touch.

INLAND productivity SOLUTIONS
Your Business Technology Partner
www.inland-prod.com