Entrepreneur & Family BUSINESS COUNCIL

Module 5

Technology Adoption

Jon Pisani

PSM Partners

jpisani@psmpartners.com

Presenter Intro

Jon Pisani is a Solution Architect at PSM Partners with close to Two (2) decades of cybersecurity experience. Jon focuses his efforts on helping organizations and business owners identify gaps within their infrastructure and design roadmaps to allow businesses to smoothly and efficiently upgrade.

Technology Debt

- **Asset Identification** – Take inventory of all hardware, software, and cloud services. Knowing what exists prevents security blind spots.
- **Assess Requirements** – Compare current tools to what the business needs. Are licenses underused? Are old systems still running?
- **Identify Criticality** – Rank assets by how essential they are to daily operations. This helps decide what to upgrade or secure first.
- **Build Roadmap** – Create a step-by-step plan to modernize or retire outdated systems to reduce long-term risk.

Systematic Improvement

- **Design Solution** – Develop solutions that fit the business (e.g., upgrading email security, implementing MFA, automating backups).
- **Plan Implementation** – Map out resources, time, and budget needed. Ensure business disruption is minimized.
- **Execute Change** – Roll out improvements in phases to reduce risk and gain user adoption.
- **Rinse & Repeat** – Cybersecurity is never “done.” Review regularly to adapt to new threats and technology shifts.

Plan Cyber Security Approach

Category	High Security (High Friction)	Balanced Approach (Security + Usability)
Authentication	Complex passwords, frequent mandatory changes, MFA on every login	Single Sign-On (SSO), passwordless login (biometrics, hardware keys), adaptive MFA only when risk is detected
Access Control	Strict manual approvals for every resource request	Role-Based Access Control (RBAC) with pre-defined access, automated access reviews
Device Security	Users required to install patches manually, strict lockdowns preventing software use	Automated patching, endpoint protection that runs in background, secure containers on personal devices (MDM)
Network Security	Always-on full VPN for all traffic	Zero Trust Network Access (ZTNA) with application-level secure tunnels, split tunneling where appropriate
Application Use	Blocking many external services and cloud tools outright	Allowing approved SaaS apps with CASB (Cloud Access Security Broker) monitoring and data loss prevention controls
Monitoring & Alerts	Constant pop-ups, frequent security prompts	Silent background monitoring with alerts only when anomalies are detected
Incident Response	Users must call IT for every password reset or phishing report	Self-service password reset, one-click phishing report button, automated response playbooks
User Awareness	Long, infrequent training sessions	Micro-learning, phishing simulations, just-in-time security nudges

What’s Availble?

- **Consolidate vs. Separate** – One vendor suite (simpler, often cheaper) vs. best-of-breed tools (more complex but specialized).
- **Licensing Bundles** – Many platforms (like Microsoft 365 or Google Workspace) include security features businesses don’t fully use.
- **App Rationalization** – Eliminate redundant apps (e.g., multiple chat tools) to reduce risk and cost.

Data Protection

- **Manage Identities** – Ensure only the right people have the right access (identity and access management).
- **Control Devices** – Secure laptops, phones, and tablets with endpoint protection. Generate Conditional Access Policies
- **Govern Access** – Set permissions based on role (least-privilege model).
- **Protect Data** – Encrypt sensitive data and back it up securely to prevent breaches and ransomware damage.

Policy Governance

- **Business Continuity** – Plan to keep operations running during disruptions.
- **Disaster Recovery** – Ensure systems and data can be restored after cyber or physical disasters.
- **Incident Response** – Pre-plan who does what in the event of a security incident. Speed matters. Perform a table-top exercise.
- **IT Security Policies** – Written rules for employees (e.g., password management, phishing awareness). Determine compliance framework if applicable.

Data Transformation

- **Audit Business Processes** – Map workflows to understand where inefficiencies or risks exist.
- **Identify Integrations** – Look for opportunities to connect systems (e.g., CRM + accounting) for better efficiency.
- **Consolidate Data** – Reduce silos to improve decision-making and reduce duplicate information.
- **Integrate Visualization Tools** – Use dashboards (like Power BI, Tableau) to turn raw data into actionable insights.

Presenter Contact Info

Jon Pisani
PSM Partners
jpisani@psmpartners.com