Entrepreneur & Family BUSINESS COUNCIL

# Cybersecurity & Technology Adoption


**Jon Pisani**

**PSM Partners**

jpisani@psmpartners.com


# Presenter Intro

Jon Pisani is a Solution Architect at PSM Partners with close to two 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.

# Agenda

- Cybersecurity Misconceptions
- Technology Debt
- Systematic Improvement
- Data Protection
- Planning Your Cybersecurity Approach
- What’s Available?
- Integrations
- Policy Governance

PSM
TECHNOLOGY | TALENT

# Cybersecurity Misconceptions

**What do you think are some common misconceptions around cybersecurity?**

PSM
TECHNOLOGY | TALENT

# Cybersecurity Misconceptions

1. “I’m too small to be noticed.”
2. “I’ve got antivirus on my computer, so that’s enough.”
3. “We have a backup, so ransomware can’t hurt us.”
4. “Cyber threats are always external – there is no internal threat.”
5. “My devices are fine. I would know if I was compromised.”
6. “Cybersecurity is IT’s responsibility. They got this.”

**Cybersecurity is everyone’s responsibility.**

PSM
TECHNOLOGY | TALENT

# Technology Debt

- **Identify Assets:**
  - 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.

# Technology Debt

- **Build Roadmap:**
  - Create a step-by-step plan to modernize or retire outdated systems to reduce long-term risk.


Image from ACTE.in

PSM
TECHNOLOGY | TALENT

# Systematic Improvement

- **Design Solution:**
  - Develop solutions that fit the business.
  - Examples: upgrading email security, implementing MFA, automating backups

PSM
TECHNOLOGY | TALENT

# Design Solution: Passphrases Example

**Take a look at the following four passwords.**
**Which one is the strongest password (the hardest to hack)?**

1. W3lcome@
2. sunshine1
3. Cl*&n%X2
4. MyCatHatesMondays

PSM
TECHNOLOGY | TALENT

# Time it takes a hacker to brute force your password in 2025

| Number of Characters | Numbers Only | Lowercase Letters | Upper and Lowercase Letters | Numbers, Upper and Lowercase Letters | Numbers, Upper and Lowercase Letters, Symbols |
|---|---|---|---|---|---|
| 4 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 5 | Instantly | Instantly | 57 minutes | 2 hours | 4 hours |
| 6 | Instantly | 46 minutes | 2 days | 6 days | 2 weeks |
| 7 | Instantly | 20 hours | 4 months | 1 year | 2 years |
| 8 | Instantly | 3 weeks | 15 years | 62 years | 164 years |
| 9 | 2 hours | 2 years | 791 years | 3k years | 11k years |
| 10 | 1 day | 40 years | 41k years | 238k years | 803k years |
| 11 | 1 weeks | 1k years | 2m years | 14m years | 56m years |
| 12 | 3 months | 27k years | 111m years | 917m years | 3bn years |
| 13 | 3 years | 705k years | 5bn years | 56bn years | 275bn years |
| 14 | 28 years | 18m years | 300bn years | 3tn years | 19tn years |
| 15 | 284 years | 477m years | 15tn years | 218tn years | 1qd years |
| 16 | 2k years | 12bn years | 812tn years | 13qd years | 94qd years |
| 17 | 28k years | 322bn years | 42qd years | 840qd years | 6qn years |
| 18 | 284k years | 8tn years | 2qn years | 52qn years | 463qn years |

**Hardware: 12 x RTX 5090**
**Password hash: bcrypt (10)**

Hive Systems

**Read more and download at**
**hivesystems.com/password**

# Design Solution: Passphrase Scenario


PSM
TECHNOLOGY | TALENT

# Design Solution: Passphrase Practice

**Pick one of the prompts below and create your own passphrase:**

- **What's a meal you'll never forget? Where did you eat it?**
  - *tacos-in-Austin-2019*
- **Finish this sentence: "I would never eat…"**
  - *I-would-never-eat-ketchup-on-a-hot-dog!*
- **What's the most random thing you can picture right now?**
  - *purple-giraffe-on-skates*
- **Describe something in your daily routine in a weird way.**
  - *coffee-before-humans-please*
- **What would your pet say if it could talk?**
  - *take-me-out-on-a-walk*

PSM
TECHNOLOGY | TALENT

# Systematic Improvement cont.

- **Design Solution:**
  - Develop solutions that fit the business.

  - Examples: upgrading email security, implementing MFA, automating backups

- **Plan Implementation:**
  - Map out resources, time, and budget needed. Ensure business disruption is minimized.

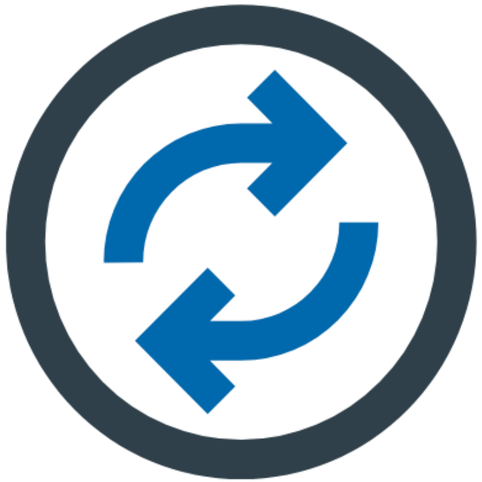
- **Execute Change:**
  - Roll out improvements in phases to reduce risk and gain user adoption.

PSM
TECHNOLOGY | TALENT

# Systematic Improvement cont.

- **Rinse & Repeat:**
  - Review regularly to adapt to new threats and technology shifts.

## Cybersecurity is never “done.”



PSM
TECHNOLOGY | TALENT

# 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.
    - Example: What criteria do people / devices need to meet? Location? Operating system? Device type?

- **Protect Data:**
  - Encrypt sensitive data and back it up securely to prevent breaches and ransomware damage.

PSM
TECHNOLOGY | TALENT

# Planning Your Cybersecurity Approach

**Categories to Think About:**

- Authentication
- Access Control
- Device Security
- Application Use
- Monitoring & Alerts
- Incident Response
- User Awareness

PSM
TECHNOLOGY | TALENT

# Planning Your Cybersecurity Approach

| Category | High Security (high friction) |
|---|---|
| **Authentication** | Complex passwords, frequent mandatory changes, MFA on every login |
| **Access Control** | Strict manual approvals for every resource request |
| **Device Security** | Users required to install patches manually, strict lockdowns preventing software use |
| **Application Use** | Blocking many external services and cloud tools outright |
| **Monitoring & Alerts** | Constant pop-ups, frequent security prompts |
| **Incident Response** | Users must call IT for every password reset or phishing report |
| **User Awareness** | Long, infrequent training sessions |

PSM
TECHNOLOGY | TALENT

# Planning Your Cybersecurity Approach

| Category | Balanced Approach (secure + usable) |
|---|---|
| **Authentication** | Single Sign-On (SSO), passwordless login (biometrics, hardware keys), adaptive MFA only when risk is detected |
| **Access Control** | Preapproved access based on the user's role within the organization |
| **Device Security** | Automated patching, endpoint protection that runs in background, containing application data within approved applications (MAM) |
| **Application Use** | Allowing approved SaaS apps with monitoring and data loss prevention controls |
| **Monitoring & Alerts** | Silent background monitoring with alerts only when anomalies are detected |
| **Incident Response** | Self-service password reset, one-click phishing report button, automated response playbooks |
| **User Awareness** | Micro-learning, phishing simulations, just-in-time security nudges |

PSM
TECHNOLOGY | TALENT

# What’s Available?

**One Vendor Suite vs. Best-of-Breed Tools**

Think about the various tools (applications, platforms, licenses, etc.) you use for work. Do you tend to use a “one vendor suite” (like Microsoft 365, Google Suite etc.), or do you use a mix of tools depending on your specific need?

**What are some pros and cons to each approach?**

PSM
TECHNOLOGY | TALENT

# What's Available?

**Key Considerations:**

What are your needs? What challenge(s) are you facing? Is there a solution that exists within your existing licenses/bundles, or do you need to look externally?

- **Consolidate vs. Separate:**
  - One Vendor Suite (simpler, often cheaper) **vs.**
  - Best-of-Breed Tools (more complex but specialized)

- **Licensing Bundles:**
  - What licenses do you already use? Do you use them to their fullest potential?
  - Many platforms (like Microsoft 365 or Google Workspace) include security features businesses don't fully use.

- **App Rationalization:**
  - Which apps do you use? What purpose(s) do they serve?
  - Eliminate redundant apps (e.g.: multiple chat tools) to reduce risk and cost.

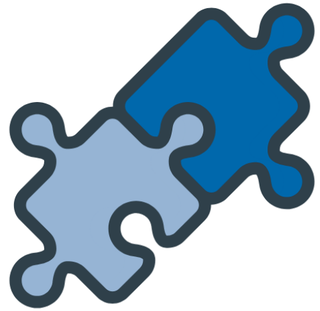
PSM
TECHNOLOGY | TALENT

# Integrations

- **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.



PSM
TECHNOLOGY | TALENT

# Policy Governance

**Why do we need policies around our technology use?**

**Can’t we just rely on IT to keep us safe?**

PSM
TECHNOLOGY | TALENT

# Policy Governance

## What happen when something goes wrong?

E.g.: your system goes down, your office building is inaccessible, your devices are compromised, your data is deleted, etc.

PSM
TECHNOLOGY | TALENT

# Policy Governance

**Key Considerations:**

How can you plan around disruptions before they happen?

- **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.

PSM
TECHNOLOGY | TALENT

# Summary

Nobody is immune to cyber attacks. We need to prepare in advance.

Cybersecurity is ALL of our responsibility. Keeping an organization safe is a team effort.

It’s not a light switch change. There is a tiered approach.

PSM
TECHNOLOGY | TALENT

# Presenter Contact Info

**Jon Pisani**

**PSM Partners**

jpisani@psmpartners.com