LOGICON

WORKBOOK 2025

Adapting IT & security for an AI-powered future.

Welcome to LogicON!

As the technology landscape continues to evolve, events like LogicON provide a critical space for collaboration, learning, and innovation. This workbook has been designed to be your guide throughout the sessions, offering practical exercises, insights, and frameworks that relate directly to the topics covered.

Each worksheet corresponds to a specific session, ensuring you can actively engage with the content and apply key takeaways in real time. Whether you're delving into advanced cybersecurity strategies, data management best practices, or new innovations in IT infrastructure, these tools will help you maximize your experience at LogicON.

We encourage you to use this workbook not just during the event but also as a resource to revisit and implement the strategies you'll learn over the next few days. Your participation and insights are essential in fostering a stronger community, and we hope this workbook will serve as a catalyst for the work you'll do moving forward.

Thank you for joining us. We look forward to the conversations and collaborations ahead.

Sincerely,

The LogicON Team

Thank You to Our Sponsors

We would like to extend our heartfelt thanks to the sponsors of LogicON, whose support and partnership have made this event possible.

Your commitment to innovation and dedication to advancing the fields of IT and cybersecurity have been instrumental in shaping the quality of this event. Your sponsorship enables us to create an environment where thought leaders, experts, and attendees can come together to share insights, build valuable connections, and drive progress within our industry.

We are incredibly grateful for your contribution and belief in the vision of LogicON. Together, we are fostering growth, collaboration, and cutting-edge solutions that will continue to shape the future of our sector.

Thank you for your continued support in making LogicON a success!

SONICWALL®

Extreme networks

seceon

TD SYNNEX

SentinelOne

Kaseya

Microsoft

osano

HUNTRESS

cysurance

GreatAmerica FINANCIAL SERVICES
HARD WORK • INTEGRITY • EXCELLENCE

FORTINET

TECHchieva

rewst

Contents

The AI Paradox – Innovation, Complexity & Hype

Joshua Skeens, Chief Executive Officer, Logically
https://www.linkedin.com/in/joshuaskeens/
Jennifer Ives, VP of Artificial Intelligence & Modernizing Government, Partnership for Public Service
https://www.linkedin.com/in/jennifersives/

Session Recording: https://vimeo.com/1133601984/ae7b367fb0?share=copy&fl=sv&fe=ci

Presentation Materials: https://go.logically.com/hubfs/LogicON25/Session-PDFs/The%20AI%20Paradox%20%E2%80%93%20Innovation%2c%20Complexity%20&%20Hype.pdf

AI is everywhere—but is it truly delivering impact? This session explores the tension between hype-fueled innovation and the practical realities of implementation. Many IT and InfoSec leaders are under pressure to integrate AI into strategy, yet face overwhelming complexity, unclear ROI, and growing scrutiny around risk and governance. This talk will explore how to cut through noise and build an AI program rooted in value, security, and long-term business alignment. It will offer perspective on how to harness AI without chasing vaporware or introducing unnecessary risk.

Learning Outcomes:

- Identify common organizational challenges that block AI momentum.
- Separate AI reality from hype and vendor exaggeration.
- Learn a strategic lens for evaluating and deploying AI solutions.

Notes:

AI Leadership Quick Start: 10-Day Action Plan

Use this worksheet as your launchpad for meaningful momentum in AI leadership. The following steps are designed to be implemented over the next 10 business days, helping you and your team lead with clarity, purpose, and visible results.

Monday Morning Checklist

1. **Identify (and name) an AI Sponsor:** Accountability is the foundation of progress. Assign a dedicated individual to champion your AI initiatives.
2. **Map the Shadow AI:** Take inventory of all AI tools currently in use within your organization, whether officially sanctioned or not.
3. **Define the First Win:** Select a business process that can be improved within 90 days. Start with a manageable project to build confidence and momentum.
4. **Set Guardrails, Not Roadblocks:** Establish three straightforward "rules of the road" to guide responsible AI experimentation without stifling innovation.
5. **Ask the Leadership Question:** Evaluate whether your AI efforts align with your organization's core values and mission.
6. **Track Cost of Inaction:** Quantify the opportunity cost of not acting. For example, saving one hour per day equals 240 hours per year for each employee.
7. **Pressure-Test Vendors:** Critically assess vendor claims by asking how proposed AI solutions will cut costs, reduce risk, or shorten cycle times within six months.
8. **Engage Your Skeptics:** Invite your most resistant leader to participate in the pilot phase to gain diverse perspectives and address concerns early.
9. **Invest in Fluency, Not Just Tools:** Educate leaders to ask increasingly strategic questions about AI, fostering a culture of informed decision-making.
10. **Set a 30-Day Review:** Schedule a review session now to reflect on what was attempted and what was learned within the first month.
11. **Define Your AI Boundaries:** Clearly document what data, processes, and decisions AI is allowed to impact today. This transparency builds trust and empowers teams to move forward with confidence.

Why eleven steps? In the era of AI, progress means pushing beyond the obvious—stopping at ten is no longer enough.

The Four Quadrants of AI Implementation

To visualize your organization's position in the AI landscape, plot it on a 2×2 matrix:

- X-axis: Value Realization (ranging from Pilots to measurable ROI)
- Y-axis: Governance Rigor (ranging from No guardrails to Clear ownership)

Consider where your current projects and initiatives fall along these axes. Are you running many pilots with little oversight (bottom-left quadrant), or have you established clear ownership and are now realizing tangible business value (top-right quadrant)? This diagnostic helps identify whether your focus should be on maturing your governance structure, accelerating value realization, or both. Use this as a tool to spark internal discussion and set priorities for your AI journey.

The Hype Zone – High talk, low governance

Organizations here are enthusiastic about AI, but lack structured oversight.
Next: Assign a sponsor for accountability and launch a focused pilot project to translate ideas into tangible outcomes.

The Wild West – Pilots, no guardrails

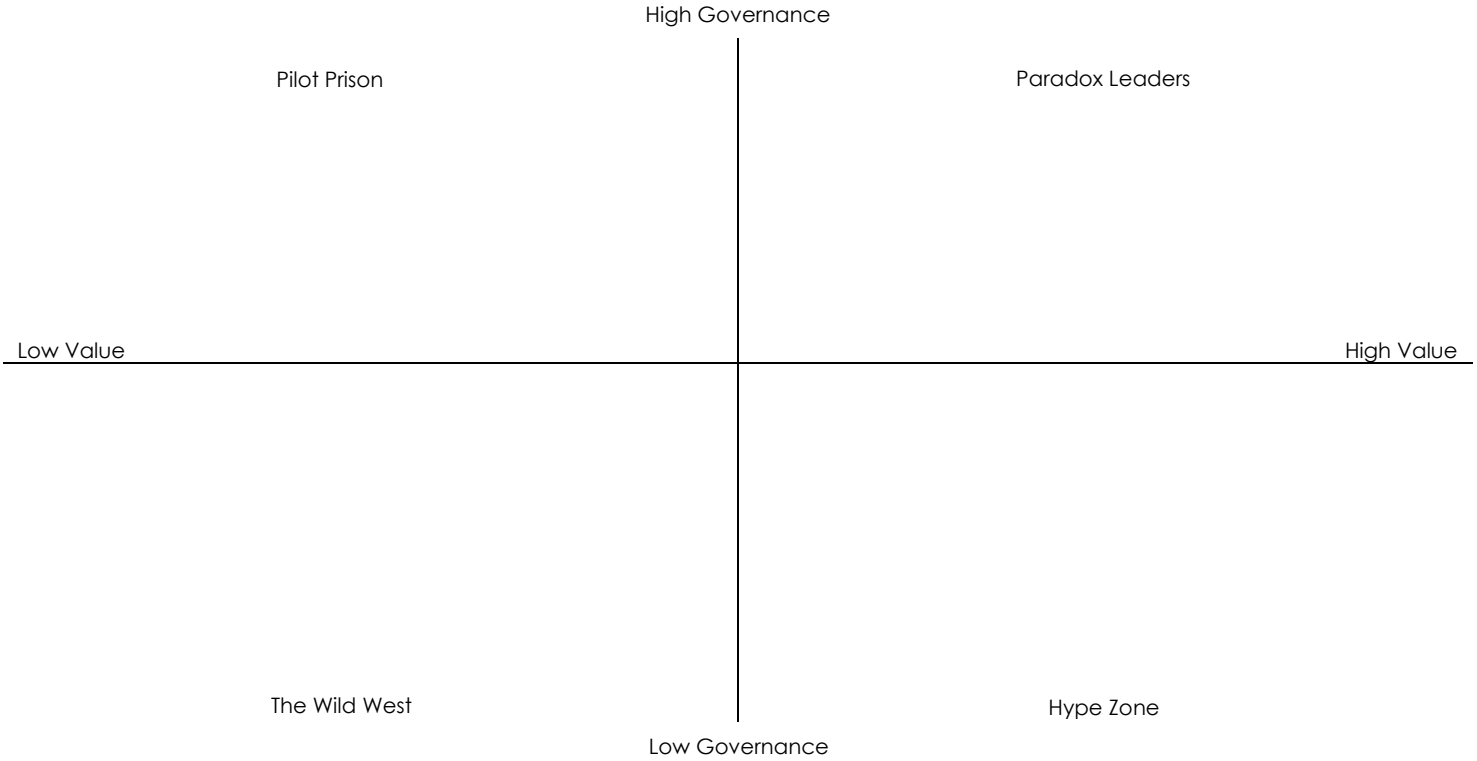
Many AI experiments are underway, but there's little control or risk management.
Next: Establish three core "rules of the road" to guide responsible experimentation and reduce potential risks.

Pilot Prison – Governance, no results

Strong governance exists, but progress has stalled.
Next: Select one promising process and move it into production to demonstrate real value and build momentum.

Paradox Leaders – Balanced value + governance

These teams are successfully blending measurable results with robust oversight.
Next: Scale up by initiating a 10-day sprint to rapidly expand proven solutions and maximize impact.



AI Decision Matrix in Detail

Use this worksheet to assess your organization's AI initiatives and determine where to focus your efforts. Plot each use case based on its perceived Value (Y-axis) and your organization's Readiness (X-axis). This tool helps identify whether you should build capabilities, invest, test cautiously, or avoid certain initiatives altogether.

HIGH VALUE + HIGH READINESS = INVEST NOW

Your organization has both the capability and the business case to succeed. The data foundation, governance, and executive alignment are in place — and the ROI potential is high.

Indicators:

- Data is clean, accessible, and integrated across systems.
- Teams understand how to use AI tools, and governance frameworks exist.
- The use case is tightly aligned to revenue, cost reduction, or risk mitigation.

Examples:

- Predictive maintenance in manufacturing with years of equipment data.
- AI-driven fraud detection in a financial institution with structured transaction data.
- Automated customer support using internal knowledge bases.

Outcome:

These are your early wins — they build momentum, credibility, and executive trust. Success here proves the AI strategy is tangible, measurable, and worth scaling.

HIGH VALUE + LOW READINESS = BUILD DATA FOUNDATIONS

You've identified a high-impact area for AI, but your infrastructure, data quality, or talent are not mature enough yet. Jumping too fast risks failure and "AI fatigue."

Indicators:

- Valuable business use cases exist, but data is siloed or inconsistent.
- There's no clear AI governance or model lifecycle management process.
- Employees lack understanding of AI tools or change management support.

Examples:

- A healthcare provider wanting to use AI for patient outcome predictions but with fragmented EHR systems.
- A retailer wanting demand forecasting but lacks integrated inventory and sales data.

Outcome:

The right move is foundational work — invest in data architecture, labeling, and upskilling teams. Otherwise, the initiative will fail not because the use case was wrong, but because the foundation wasn't ready.

Low Value + High Readiness = SANDBOX ONLY

The organization can execute AI projects (tools, data, and people are ready), but the use case doesn't drive significant business value. These are safe places to experiment, learn, and demonstrate capability — without large financial bets.

Indicators:

- Data and systems are mature, but the use case is peripheral.
- Outcomes won't materially impact key metrics like revenue or risk.
- Often "nice-to-have" rather than "need-to-have" initiatives.

Examples:

- Using AI to summarize internal emails.
- Chatbots for non-critical internal FAQs.
- Visual dashboards that "look intelligent" but don't drive action.

Outcome:

Use this quadrant for learning and innovation — to build internal fluency, test new tools, and refine governance before scaling to higher-value areas. But don't oversell the impact.

Low Value + Low Readiness = AVOID

Neither the organizational maturity nor the business case justify AI investment. These projects consume resources and create skepticism about AI's usefulness.

Indicators:

- Poor data hygiene and no clear owner for outcomes.
- No connection to core strategy or measurable KPIs.
- Initiatives driven by hype or "shiny object" enthusiasm.

Examples:

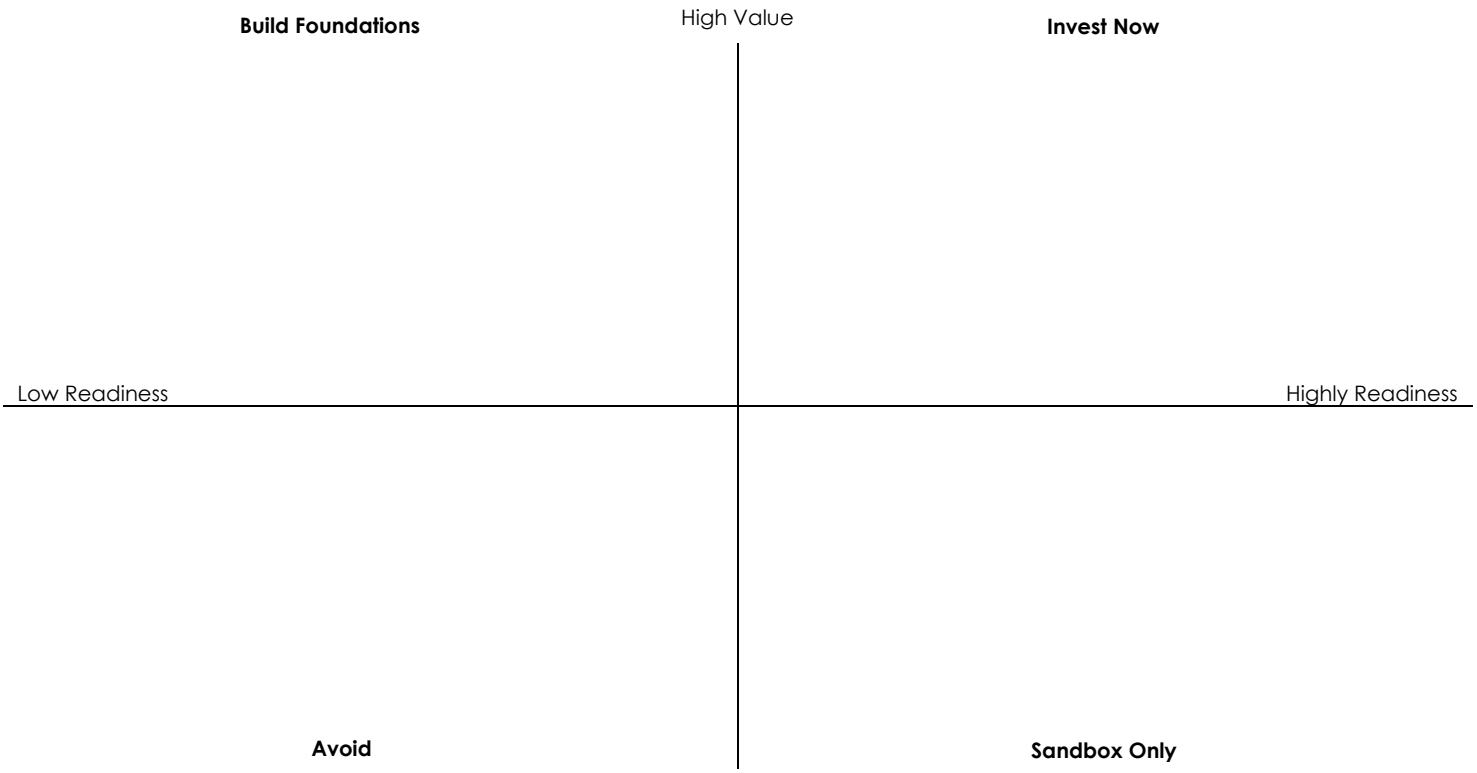
- Using generative AI to write internal memos when data security is poor.
- Piloting advanced AI models in an area with minimal business relevance.

Outcome:

Avoid until readiness and value both increase. These efforts are likely to become "AI theater" — activity without impact, which erodes trust and credibility.

Quadrant	Priority	Risk	ROI Potential	Recommended Action
High Value + High Readiness	Invest Now	Low	High	Scale aggressively
High Value + Low Readiness	Build Foundations	Medium	High (future)	Strengthen data + skills
Low Value + High Readiness	Sandbox	Low	Low	Experiment, learn
Low Value + Low Readiness	Avoid	High	Minimal	Defer investment

To visualize your organization's position in the AI landscape, plot it on a 2×2 matrix:



Pre-Launch Checklist for AI Pilot Projects

Before moving forward with any AI pilot initiative, it is essential to conduct a thorough readiness assessment by addressing three critical questions:

1. **Ownership:** Clearly identify and name the leader who will be held accountable for the pilot. This ensures that there is a designated individual responsible for overseeing the project and managing outcomes.
2. **Data Usage:** Specify the types of data the pilot will use. It is particularly important to flag any sensitive or restricted data involved, as this has implications for privacy, security, and compliance.
3. **Human Judgment:** Define the precise point in the process where human intervention or decision-making is required. This step clarifies the boundaries between automated operations and human oversight, reducing potential risks.

If you cannot confidently answer these three questions within a minute, the AI pilot is not sufficiently prepared for launch. Ensuring clarity on these points is crucial for responsible experimentation and risk mitigation.

Let's try it! Think of a current project that is underway and fill out the below.

What is the name of the pilot? _____

Who is accountable for the pilot? _____

What data is used?

_____

_____

_____

_____

Where does a human make the call?

_____

_____

_____

_____

Is the pilot ready (circle answer)? Yes No

Calculating the Cost of Inaction for Repetitive Tasks

Identify a repetitive task in your organization to assess the value of AI automation and guide technology investment priorities.

Step 1 – Identify the task

Repetitive task: _____

Step 2 – Estimate weekly time spent

Hours per week (per employee): _____

Number of employees: _____

a) Calculate total annual hours

Formula: hours per week × number of employees × 52 weeks = _____ Total Annual Hours

Step 3 – Apply labor cost

Fully loaded hourly cost: _____

b) Calculate annual labor cost of this task

Formula: total annual hours × hourly cost = _____ Annual Labor Cost

Step 4 – Estimate AI savings

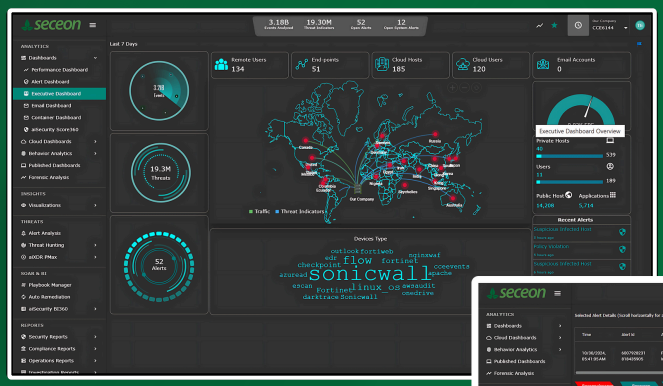
If AI reclaims 20%:

Formula: annual labor cost × 20%= _____ Potential AI Savings

seceon

SECURITY FOR EONS

All-In-One Security. One Powerful Platform.



Trusted by 9000+ Customers

SIEM | XDR | UEBA | SOAR | NDR | Threat Intel | AI/ML Driven |

Protect
Single Pane of Glass for Multi-Tenant Visibility

Defend
AI-Driven SOC Efficiency

Comply
Simplify Compliance & Risk Reporting

Scale
No Shelfware or Hidden Fees

850+ Integrations

SentinelOne · Kaseya · aws · CROWDSTRIKE · CISCO

SONICWALL · CONNECTWISE · zscaler · paloalto NETWORKS · servicenow

ThreatScape 2025: What Every Leader Needs to Know Now

Joe Evangelisto, CISO, NetSPI
https://www.linkedin.com/in/joe-evangelisto/

Session Recording: https://vimeo.com/1133605160/7b488227cf?share=copy&fl=sv&fe=ci

Presentation Materials: https://go.logically.com/hubfs/LogicON25/Session-PDFs/ThreatScape%202025%20-%20What%20Every%20Leader%20Needs%20to%20Know%20Now.pdf

Cyber adversaries aren't just evolving—they're accelerating. For mid-market organizations, the challenge is clear: you face the same threat actors as the enterprise, but with fewer resources to fight back. This opening keynote delivers an unfiltered look at the 2025 threatscape—ransomware-as-a-service, AI-powered phishing, supply chain infiltration, and the growing risk to OT systems. Pulling from the latest global threat intelligence, this session breaks down where attacks are headed, which sectors are being targeted, and what tactical moves you can make now to build resilience—without breaking the bank.

Learning Outcomes:

- Analyze emerging threat vectors that target mid-market organizations.
- Learn practical mitigation strategies based on industry trends.
- Understand how attackers are evolving their toolsets with AI.

Notes:

AI Deepfake Scam Case Study

A real-world example of a multi-million-dollar deepfake scam targeting a major company. Attackers used an AI-generated video call to impersonate a senior executive.

Questions for Reflection:

- What documented escalation and verification protocols are triggered when financial requests deviate from standard patterns or come from high-authority sources?

  _____
  _____
  _____
  _____

- Which verification processes are documented, tested, and enforced to prevent social engineering attacks targeting executive impersonation?

  _____
  _____
  _____
  _____

Exercise: Verification Process Maturity

Question	Answer
Rate your verification processes for unusual financial requests: (1 = non-existent, 5 = fully mature)	
Do you have documented, tested, and enforced verification protocols? (Yes/No)	
List the steps your team follows to verify identity during urgent financial requests:	
How often are these protocols reviewed and updated? (Monthly/Quarterly/Annually)	
Have you conducted a deepfake simulation exercise in the past 12 months? (Yes/No)	

Actions to Take:

- ❑ Review and document verification protocols for financial and executive-level requests.
- ❑ Train staff to identify signs of deepfake scenarios, including unusual video or voice behavior.
- ❑ Schedule and conduct a tabletop exercise simulating a deepfake attack targeting leadership.
- ❑ Implement voice authentication safeguards for sensitive communications.
- ❑ Audit financial approval workflows to identify and remediate vulnerabilities.

Phishing Defense

Phishing remains the top attack vector, with AI-generated emails dramatically increasing click-through rates—demanding stronger employee training and technical controls.

Key Points:

- Phishing remains the primary method used for delivering ransomware and other types of malware.
- SMBs receive one malicious email for every 323 messages.
- 92% of malware is delivered via email, making phishing the most common entry point for attacks.
- One-third of BEC attacks target small businesses, with an average cost of $50,000 per attack.
- AI-written phishing emails now achieve a 54% click-through rate.

Questions for Reflection:

- What is the cadence and format of phishing awareness campaigns, and how are reporting metrics tracked and reviewed at the leadership level?

  _____

  _____

- How is your organization adapting training and email filtering strategies to address the increased sophistication and success rate of AI-generated phishing attacks?

  _____

  _____

Exercise: Phishing Resilience

Question	Answer
Rate your phishing training frequency: (1 = rarely, 5 = regularly)	
Do you simulate phishing attacks for training? (Yes/No)	
Do you track employee reporting rates? (Yes/No)	
Do you use AI-based email filtering tools? (Yes/No)	
What percentage of employee's report phishing attempts?	

Actions to Take:

- ❑ Send a phishing awareness reminder to all staff, emphasizing recent trends and tactics.
- ❑ Launch a simulated phishing campaign to assess employee vigilance and response rates.
- ❑ Review phishing reporting metrics and trends to identify gaps in awareness or response.
- ❑ Update training materials to include examples of AI-generated phishing threats and how to spot them.
- ❑ Evaluate current email solutions and deploy tools capable of detecting AI-enhanced phishing attempts.

Ransomware Threats

Ransomware-as-a-Service has made attacks more accessible and devastating, with high rates of operational shutdowns and data leak threats among SMBs.

Key Points:

- Ransomware-as-a-Service (RaaS) is now behind more than 60% of ransomware campaigns, making these attacks more accessible for criminals.
- One in five SMBs hit by ransomware had to suspend operations temporarily.
- 60% of SMBs shut down within six months of a cyberattack.
- 72% of SMB ransomware incidents now include threats to leak stolen data.

Questions for Reflection:

- Which attack vector poses the greatest risk to your business continuity, and how is it prioritized in your current risk register or board-level reporting?

  _____

  _____

- How are threat vectors mapped to strategic initiatives, budget allocations, and board-level KPIs in your cybersecurity roadmap?

  _____

  _____

Exercise: Ransomware Readiness Scorecard

Question	Answer
Rate your backup strategy maturity: *(1 = poor, 5 = excellent)*	
Do you have a ransomware response plan? (Yes/No)	
Have you tested your incident response in the last 6 months? (Yes/No)	
Do you have offline backups? (Yes/No)	
Is your backup data encrypted and access-controlled? (Yes/No)	

Actions to Take:

- ❑ Audit backup systems to ensure they are complete, encrypted, and regularly tested for restoration.
- ❑ Run a ransomware tabletop exercise to simulate decision-making under pressure.
- ❑ Review and update the ransomware response plan to include communication protocols, legal steps, and recovery procedures.
- ❑ Implement EDR tools across all critical systems and validate their alerting capabilities.
- ❑ Train employees to recognize ransomware indicators such as suspicious file behavior, access denials, or ransom notes, and establish clear reporting channels.

AI-Powered Attacks

AI is transforming cyber threats through real-time, adaptive attacks and deepfake social engineering, requiring advanced detection and response capabilities.

KEY POINTS:

- AI is accelerating the speed and scale of cyberattacks.
- Attacks have surged by 47%, overwhelming many traditional defenses.
- Voice phishing (vishing) attacks are up 442%, highlighting the need for stronger protocols.

QUESTIONS FOR REFLECTION:

- What safeguards and training protocols are in place to detect and respond to AI-enhanced voice phishing, and how is their effectiveness measured?

  _____

  _____

- What investments or architectural changes are required to scale your defenses against adaptive, AI-driven threats, and how are these prioritized in your strategic planning?

  _____

  _____

EXERCISE: AI THREAT READINESS

Question	Answer
Rate your detection readiness for AI-powered threats: *(1 = non-existent, 5 = fully mature)*	
Do you have a tabletop exercise planned for AI threats? (Yes/No)	
List current tools used for AI threat detection:	
How do you monitor adaptive attack behaviors? (Yes/No)	
Do you have a response plan for voice phishing attacks? (Yes/No)	

ACTIONS TO TAKE:

- ❑ Brief your cybersecurity and IT teams on current AI threat trends, tactics, and real-world case studies.
- ❑ Develop AI-specific threat detection criteria and playbooks, including indicators of compromise and response protocols.
- ❑ Schedule and conduct a tabletop exercise focused on AI-powered attack scenarios to test team readiness.
- ❑ Evaluate AI-based threat monitoring solutions for integration into your existing security stack.
- ❑ Update your incident response plans to include AI-specific scenarios, such as adaptive malware and deepfake impersonation.

Emerging Threats

New risks like quantum computing, IoT exploitation, and AI misuse are reshaping the threat landscape, urging organizations to prepare for complex, evolving vulnerabilities.

Key Points:

- Ransomware uses AI for speed and precision, creating attacks that adapt in real time.
- Major supply chain disruptions are increasing; with 2–3 massive incidents predicted for 2025.
- With over 32 billion IoT devices projected, many lack proper security, making them prime targets.
- Employees may accidentally expose sensitive company data by interacting with AI platforms.
- Traditional encryption is at risk; preparation for post-quantum cryptography is now crucial.

Questions for Reflection:

- Which emerging threat has the highest likelihood of disrupting your operations, and what measurable steps have been taken to mitigate it?

  _____

  _____

- What guardrails, usage policies, and training programs are in place to prevent unintentional data exposure through employee interactions with AI platforms?

  _____

  _____

Exercise: Emerging Threat Prioritization

Rank each threat by Likelihood and Impact on a scale of 1–5. Risk Score: RS = (L x I)

- **Low Risk (Score: 1–5)** - Minimal likelihood and/or impact
- **Medium Risk (Score: 6–14)** - Moderate likelihood and/or impact
- **High Risk (Score: 15–25)** - High likelihood and/or severe impact

	Likelihood (L)	Impact (I)	Risk Score: RS = (L x I)
AI-Powered Attacks			
Deepfakes			
Supply Chain Attacks			
IoT Exploitation			
Quantum Threats			

Actions to Take:

- ❑ Review the Emerging Threat Prioritization Grid and identify the top 2 threats.
- ❑ Update your risk register to include the identified emerging threats with appropriate risk ratings.
- ❑ Develop mitigation plans for each top-ranked threat, including technical, procedural, and policy controls.
- ❑ Schedule and conduct awareness training sessions focused on recognizing and responding to emerging threats.
- ❑ Review vendor security practices and assess supply chain risks; ensure third-party risk management policies are up to date.

Surviving and Thriving Amid Cyber Regulation Overload

Michael O'Hara, Security Consultant, Logically
https://www.linkedin.com/in/michael-o-hara/

Session Recording: https://vimeo.com/1133607841/2a4e16fd5d?share=copy&fl=sv&fe=ci

Presentation Materials: https://go.logically.com/hubfs/LogicON25/Session-PDFs/Surviving%20and%20Thriving%20Amid%20Cyber%20Regulation%20Overload.pdf

With cybersecurity oversight expanding at federal and state levels, executives are facing mounting regulatory pressure. This session will unpack what the latest wave of compliance changes means for IT and InfoSec leaders—from the SEC's cybersecurity disclosure requirements to the increasing global reach of data protection laws. Attendees will learn how to position compliance not as a box-checking exercise, but as a business enabler that supports transparency, trust, and long-term resilience.

Learning Outcomes:

- Understand current and emerging cyber regulations impacting mid-market firms.
- Align compliance strategy with board expectations and legal obligations.
- Build processes that scale across controls, audits, and reporting.

Notes:

AI in Governance, Risk & Compliance (GRC)

Section 1: Oversight & Accountability

Key Concepts:

- SEC disclosure requirements (material incidents, 4-day window)
- CPRA data correction rights
- Cyber hygiene basics
- Board responsibilities

Notes:

_____
_____
_____
_____

Reflection Question: Who currently reports cybersecurity updates to your executive management, board, or ownership?

- ❑ IT/Security Team
- ❑ Compliance Officer
- ❑ Executive Leadership
- ❑ Other: _____

Section 2: Compliance Changes

Key Concepts:

- Proposed HIPAA/HITECH changes
- PCI DSS 4.0 requirements
- Global Data Protection (GDPR, CPRA, LGPD)
- Fiduciary duty claims
- EU AI Act — phased obligations: bans & AI literacy (Feb 2, 2025), governance & GPAI (Aug 2, 2025), broad applicability (Aug 2, 2026), high-risk embedded systems (until Aug 2, 2027).
- California (CPRA/CCPA) — CPPA finalized rules on ADMT, cybersecurity audits, risk assessments (July 24, 2025).
- Colorado AI Act (SB24-205) — duties for developers & deployers of high-risk AI, effective June 30, 2026.
- U.S. Federal (OMB M-24-10) — binding AI governance/risk requirements for federal agencies, spillover to vendors.
- ISO/IEC 42001:2023 — voluntary AI management system standard for structured governance and continuous improvement.

Notes:

_____
_____
_____
_____

Reflection Question: How well prepared is your organization to demonstrate active oversight of cyber risk?

- ❑ Very Prepared
- ❑ Somewhat Prepared
- ❑ Not Prepared

Section 3: Compliance as a Business Enabler

Key Concepts:

- Certifications (SOC 2, ISO 27001) as competitive advantage
- Insurance requirements
- Cyber hygiene essentials

Notes:

_____
_____
_____
_____

Reflection Question: What steps are you taking to ensure trust and transparency?

_____
_____

Section 4: AI in GRC

Key Concepts:

- When AI can help: automation, evidence collection, monitoring
- Where humans are non-negotiable: risk interpretation, ethical decisions, compliance sign-off

Notes:

_____
_____
_____
_____

Reflection Questions:

1. What tasks would you never trust AI to handle in compliance?

_____
_____

2. How could strong GRC + cyber hygiene help your business avoid an insurance denial post-event?

_____
_____

Section 5: Outcomes & Takeaways

Key Concepts:

- Emerging regulations (EU AI Act, CPRA, Colorado AI Act, OMB AI policies, ISO/IEC 42001)
- Importance of scalable processes and alignment with board expectations

Notes:

_____
_____
_____
_____

Action Item: What one action will you take back to your leadership team after today's session?

_____
_____

Glossary of Acronyms & Key Terms

- **AI –** Artificial Intelligence
- **ADMT –** Automated Decision-Making Technology (covered under CPRA/CCPA regulations)
- **CCPA –** California Consumer Privacy Act (baseline California privacy law before CPRA)
- **CPRA –** California Privacy Rights Act, expands CCPA with new rights and creates CPPA enforcement agency
- **CPPA –** California Privacy Protection Agency, established to enforce CPRA/CCPA rules
- **ePHI –** Electronic Protected Health Information (regulated under HIPAA)
- **GA –** General Applicability, denotes effective dates in regulations
- **GDPR –** General Data Protection Regulation (EU)
- **GLBA –** Gramm-Leach-Bliley Act (U.S. financial services data protection law)
- **GRC –** Governance, Risk, and Compliance
- **HIPAA –** Health Insurance Portability and Accountability Act (U.S. healthcare privacy & security law)
- **HITECH –** Health Information Technology for Economic and Clinical Health Act, strengthens HIPAA enforcement
- **IR –** Incident Response (plans, teams, processes for cyber events)
- **ISO/IEC 42001 –** International standard for AI Management Systems (AIMS)
- **MFA –** Multi-Factor Authentication
- **NPP –** Notice of Privacy Practices (required under HIPAA)
- **NPRM –** Notice of Proposed Rulemaking (used for HIPAA/HITECH changes)
- **OCR –** Office for Civil Rights (enforces HIPAA)
- **OMB –** U.S. Office of Management and Budget (issued M-24-10 on AI governance)
- **PCI DSS –** Payment Card Industry Data Security Standard
- **PHI –** Protected Health Information
- **RFP –** Request for Proposal
- **SRA –** Security Risk Assessment
- **SOC 2 –** Service Organization Control 2 auditing standard

Privacy on the Edge: Protecting Data in an AI-Driven World

Racheal Ormiston, Chief Privacy & Trust Officer, Osano
https://www.linkedin.com/in/rachael-ormiston/

Session Recording: https://vimeo.com/1133611617/e52287ff71?share=copy&fl=sv&fe=ci

Presentation Materials: https://go.logically.com/hubfs/LogicON25/Session-PDFs/Privacy%20on%20the%20Edge%20-%20Protecting%20Data%20in%20an%20AI-Driven%20World.pdf

Data privacy is becoming harder to manage as new tools, teams, and AI models interact with sensitive information. In this session, we'll explore the friction between digital innovation and data privacy requirements—especially as teams adopt GenAI tools without clear controls. You'll learn how to manage exposure risk, safeguard proprietary data, and meet privacy obligations while enabling productivity. This is a must-attend for anyone navigating a landscape where sensitive data lives in many places—and often travels without oversight.

Learning Outcomes:

- Identify common privacy pitfalls when deploying AI and SaaS.
- Implement protections for IP and sensitive data across tools.
- Build user policies that reinforce responsible data usage.

Notes:

Embedding Privacy in the AI Era

Privacy programs aren't just about avoiding fines. They're about **building trust, protecting people, and enabling growth**. A **Privacy Maturity Model** can help to track how well you're doing and prepare for the privacy risks AI can bring.

This worksheet is designed to help your team to:

- Benchmark your current privacy practices.
- Reflect on strengths, gaps, and risks.
- Capture actionable next steps.
- Learn how Osano approaches privacy maturity so you can adapt it to your own program.

The Privacy Maturity Ladder

The 5 Levels of Maturity:

1. **Reactive (Level 1)** – Respond only after an incident, regulator inquiry, or customer complaint.
2. **Provisional (Level 2)** – Some processes exist, but they are siloed and inconsistent.
3. **Formalized (Level 3)** – Documented policies and roles; improvements are ad hoc.
4. **Monitored (Level 4)** – Metrics tracked, regular reviews, leadership engagement.
5. **Proactive (Level 5)** – Privacy is embedded in strategy; risks are anticipated before they happen.

Tip: Don't aim to jump straight to "Proactive." Start with the areas where non-compliance or customer trust issues could hurt you most (e.g., vendor risk, subject rights).

For a more detailed dive into privacy program maturity, visit https://www.osano.com/guide/privacy-program-maturity-model

Reflection #1 – Where Are You Today?

Mark the level that best fits your company right now:

- ❑ Reactive
- ❑ Provisional
- ❑ Formalized
- ❑ Monitored
- ❑ Proactive

Notes / Next Steps:

Section 1: Transparency & Rights

Do people know and control how their data is used?

- ❑ Our **privacy notices** are clear, accessible, and regularly updated.
- ❑ We explain why we collect data in plain language.
- ❑ We request, store, and honor **consent choices**.
- ❑ We process **subject rights requests (DSARs)** accurately and within deadlines.
- ❑ Employees know how to escalate data rights questions.

💡 *Tip:* A simple DSAR intake form (web or email template) dramatically reduces errors and response time.

Notes / Next Steps:

Section 2: Data Lifecycle Management

Do we handle personal data responsibly from start to finish?

- ❑ We maintain a **data inventory / RoPA** that's updated at least annually.
- ❑ We know **where data flows** (systems, vendors, transfers).
- ❑ We practice **data minimization** — no unnecessary collection.
- ❑ We delete or anonymize data when no longer needed.
- ❑ Vendor contracts include **privacy & security clauses**.
- ❑ We test **security controls** regularly.

💡 *Tip:* Start by mapping your top 5 systems or highest-risk vendors. This builds momentum without overwhelming the team.

Notes / Next Steps:

Section 3: Risk & Incident Management

Can we identify and handle problems before they escalate?

- ❑ We run **Privacy Impact Assessments (PIAs/DPIAs)** for new products and processes.
- ❑ We have a documented **incident & breach response plan**.
- ❑ We conduct annual **tabletop exercises** to test our response.
- ❑ We log, track, and escalate privacy risks to leadership.

💡 *Tip:* Even a 1-hour tabletop exercise can surface gaps in communication, escalation, or decision-making.

Notes / Next Steps:

Section 4: Culture & Operations

Is privacy part of how people work every day?

- ❑ We have **dedicated budget and staff** for privacy.
- ❑ All employees receive **privacy training** at onboarding and annually.
- ❑ Leaders regularly **signal support for privacy** in meetings or communications.
- ❑ We use **Privacy by Design** checklists in projects.
- ❑ We revisit our privacy program and **update policies each year**.

Tip: Treat privacy like security: everyone is responsible, not just the privacy team.

Notes / Next Steps:

Reflection #2 – What's Most Urgent?

Looking at Sections 1–4, which gaps feel riskiest to your organization?

My priority areas are:

1. _____
2. _____
3. _____

Section 5: Continuous Improvement & Stakeholder Engagement

How do we adapt and build trust over time?

- ❑ We regularly **measure and report** on privacy KPIs.
- ❑ We **update policies** as laws and business practices change.
- ❑ We evaluate **vendor and third-party tools** for compliance.
- ❑ We involve employees, customers, or partners in feedback loops.
- ❑ We provide a way for stakeholders to **report issues or ask questions**.
- ❑ We share **privacy wins** to build culture and trust.

Tip: Even informal feedback sessions or surveys can strengthen trust and surface blind spots.

Notes / Next Steps:

Reflection #3 – My Top 3 Next Steps

After reviewing all sections, commit to three actions for the next quarter:

1.
2.
3.

Osano's Starter Actions (What Worked for Us)

- ❑ Document one undocumented data flow.
- ❑ Refresh your privacy notice in plain language.
- ❑ Run a mock DSAR or breach scenario.
- ❑ Add one privacy KPI to your team's dashboard.
- ❑ Host a 30-minute privacy Q&A for employees.

AI's Ripple Effect Across the Org Chart

Cara Parfitt, Vice President of Technology Alliances, Logically
https://www.linkedin.com/in/cara-parfitt-52373127/
Karl Noone, Chief Financial Officer, Logically
https://www.linkedin.com/in/karl-noone-435457/
Christopher A. Hudson, Senior Vice President of Global Business Performance, archTIS
https://www.linkedin.com/in/christopherhudsonhr/
Whitney Hausmann, Director of Marketing Excellence, The Riverside Company
https://www.linkedin.com/in/whitney-hausmann/

Session Recording: https://vimeo.com/1133840023/b74c7eb008?share=copy&fl=sv&fe=ci

Presentation Materials: https://go.logically.com/hubfs/LogicON25/Session-PDFs/AIs%20Ripple%20Effect%20Across%20the%20Org%20Chart.pdf

AI is not just an IT initiative—it's a cultural and operational shift touching every corner of the organization. This panel of leaders from marketing, HR, operations, and finance will share how AI impacts decision-making, workflows, risk tolerance, and hiring. For CIOs and CISOs, this is a rare opportunity to hear firsthand how other departments view AI adoption—and what they need from IT to make it work.

Learning Outcomes:

- Understand how AI is reshaping work outside the IT domain.
- Identify partnership opportunities between IT and business units.
- Anticipate the change management needs of non-technical teams.

Notes:

Generative AI Council Readiness Checklist

Use the checklist below to assess your organization's readiness to establish a Generative AI Council.

Alignment is the most critical step! The success and progress of all other steps depend on it.

Alignment

- ❑ Do you have executive alignment on AI adoption priorities?
- ❑ Have you defined what 'responsible use' of GenAI looks like in your company?
- ❑ Is there shared agreement that AI governance requires cross-functional input (not just IT)?
- ❑ Have business leaders identified key pain points or opportunities for AI?
- ❑ Do you have early adopters or 'champions' willing to test and iterate?

Structure & Council Formation

- ❑ Have you determined whether council members will be appointed or volunteer-based?
- ❑ Does your council include representation from all key departments (e.g., HR, Legal, Security, Ops, Revenue, Product)?
- ❑ Will you create a charter or purpose statement for the AI Council?
- ❑ Do you have a cadence for meetings (e.g., monthly, quarterly)?
- ❑ Has someone been selected as the lead or chair to ensure Council follow-through?

Governance, Risk & Guardrails

- ❑ Have you reviewed how GenAI may impact data privacy, ethics, and compliance?
- ❑ Have you defined what data sources should not be used with GenAI tools?
- ❑ Is there an intake process (e.g., a Use Case Request Form) to evaluate potential use cases?
- ❑ Do you have a mechanism to approve, reject, or sandbox AI use cases?
- ❑ Have you addressed whether AI tools will be centrally provisioned or department-led?

Adoption & Enablement

- ❑ Do you have a plan for educating employees on AI tools and use policies?
- ❑ Have you defined how success will be measured (e.g., time saved, errors reduced)?
- ❑ Is there a central knowledge base or communication channel for AI updates?
- ❑ Have you recognized or celebrated early wins to encourage adoption?
- ❑ Do you have feedback loops to revise policies as use of AI evolves?

Show Me the ROI – Budgeting for Real AI Outcomes

Kerry Nix, Vice President of Client Engagement & Strategic Services, Logically
https://www.linkedin.com/in/kerry-nix-015b2b72/

Session Recording: https://vimeo.com/1133823369/5fffa63635?share=copy&fl=sv&fe=ci

Presentation Materials: https://go.logically.com/hubfs/LogicON25/Session-PDFs/Show%20Me%20the%20ROI%20%E2%80%93%20Budgeting%20for%20Real%20AI%20Outcomes.pdf

Many AI pilots are stalled—not for lack of potential, but lack of business justification. In this session, finance, technology, and business leaders will unpack how to frame AI investments in terms of efficiency, automation, and value creation. From quantifying productivity boosts to avoiding hidden cost centers, attendees will learn how to fund AI with intention, track ROI with precision, and communicate results across stakeholders.

Learning Outcomes:

- Build business cases for AI investments aligned to outcomes.
- Understand cost modeling for GenAI and ML tools.
- Avoid common budget traps when scaling AI across teams.

Notes:

AI ROI Calculation

This worksheet is designed to help evaluate the financial impact and return on investment (ROI) of AI projects. By filling in the project details and applying the formulas provided, you can estimate total benefits, costs, net returns, and the payback period. This structured approach ensures decision-makers have a clear, data-driven view of potential outcomes before committing resources.

Download the template here:
https://go.logically.com/hubfs/Logically_AI_ROI_Calculator.xlsx

Input Metrics	Description
Estimated Annual Benefit	Monetary gains or cost savings per year from AI implementation
Initial Investment	One-time costs (software, data setup, consulting, etc.)
Annual Operating Cost	Ongoing costs (cloud usage, support, staff, maintenance, etc.)
Implementation Time	Time (in months) until AI system is live and delivering value
Time Horizon	Evaluation period in years (e.g., 1, 2, 3 years)
Discount Rate	The minimum required rate of return (or cost of capital) that you use to evaluate future cash flows

ROI Metrics	Formula
Total Benefits	Estimated Annual Benefit × Time Horizon
Total Costs	Initial Investment + (Annual Operating Cost × Time Horizon)
Net Benefit (Total ROI Value)	Total Benefits – Total Costs
ROI %	(Net Benefit ÷ Total Costs) × 100
Payback Period (Years)	Initial Investment ÷ Estimated Annual Benefit
Annual ROI %	(Estimated Annual Benefit – Annual Operating Cost) ÷ Initial Investment × 100
Breakeven Month	Payback Period (in years) × 12
Net Present Value (NPV)	Σ (Net Cash Flow ÷ (1+Discount Rate)^t) – Initial Investment
Internal Rate of Return (IRR)	Discount rate at which NPV = 0

Burnout, Balance & AI in the Human Workflow

Chris Cochran, Founder & CEO, Commandant AI
https://www.linkedin.com/in/chrishvm/

Session Recording: https://vimeo.com/1133828175/d5e4b98a29?share=copy&fl=sv&fe=ci

Presentation Materials: https://go.logically.com/hubfs/LogicON25/Session-PDFs/Burnout%20Balance%20&%20AI%20in%20the%20Human%20Workflow.pdf

Today's IT and InfoSec leaders are under unprecedented pressure—from defending against relentless cyberattacks and delivering AI initiatives at warp speed, to driving digital transformation with constrained budgets and shrinking teams. Compounding the stress is the looming uncertainty around AI's impact on job security, fueling anxiety at all levels. This session takes a candid look at how these forces are converging to create a burnout crisis among technology professionals. Attendees will explore how to manage these pressures through thoughtful leadership, strategic delegation to AI, and a renewed focus on human-centered workflows. We'll unpack how to strike a balance between automation and well-being, ensuring that teams stay productive, protected, and resilient in an AI-powered workplace.

Learning Outcomes:

- Identify systemic and psychological drivers of burnout in high-stakes IT and security roles.
- Implement AI in ways that alleviate, not amplify, staff pressure.
- Develop leadership strategies that prioritize well-being while meeting aggressive innovation goals.

Notes:

The Modern Pressure Cooker

We live and work in an era of unprecedented pressure. The relentless pace of technological change, coupled with ever-increasing demands, has created a perfect storm for burnout. This section explores the nature of burnout and how AI can either exacerbate the problem or become a powerful part of the solution.

The Three Pillars of Burnout

Burnout is more than just feeling tired; it's a state of chronic workplace stress characterized by three key dimensions:

Pillar	Description
Exhaustion	A state of physical and emotional depletion. It's the feeling of being completely drained, unable to recover even after a good night's sleep.
Cynicism	A negative, detached, or cynical attitude toward one's job, colleagues, and the organization. It's a loss of engagement and a feeling of disillusionment.
Performance Drop	A reduced sense of personal accomplishment and a decline in professional efficacy. It's the feeling that you're no longer effective at your job.

AI: Stress Multiplier vs. Ally

AI is not inherently good or bad; its impact on our well-being depends on how we implement and interact with it. The following table illustrates the two potential paths:

AI as a Stress Multiplier	AI as an Ally
Tool Overload: Multiple, disconnected AI platforms create confusion and frustration.	**Integrated Workflow:** AI tools are seamlessly integrated into existing workflows, simplifying tasks.
Job Security Anxiety: The fear of being replaced by AI creates a constant sense of unease.	**Partnership Mindset:** AI is viewed as a partner that handles repetitive tasks, freeing up humans for more strategic work.
Accelerated Expectations: The promise of faster delivery leads to an ever-increasing pace of work.	**Protective Layer:** AI absorbs mundane and repetitive tasks, creating a buffer against burnout.

Introspective Writing: Your Experience with Burnout

Take a few moments to reflect on your own experiences. Use the space below to answer the following questions:

- Which of the three pillars of burnout resonates most with you right now? Why?

  _____

  _____

- In what ways has technology, including AI, added to your feelings of stress or pressure at work?

  _____

  _____

- Can you think of a time when a tool or technology genuinely made your work life better? What was it, and why was it helpful?

  _____

  _____

Mastering the Craft: LLM Prompting Tips & Tricks

Effective prompting is the key to unlocking the true potential of AI. By learning how to communicate clearly and effectively with Large Language Models (LLMs), you can transform them from simple tools into powerful partners. This section introduces you to the core techniques and best practices of professional prompt engineering.

Core Prompting Techniques

Technique	Description	When to Use
Zero-Shot Prompting	Directly instructing the model to perform a task without providing any examples.	For simple, straightforward tasks where the model is likely to understand the request without additional context.
Few-Shot Prompting	Providing a few examples (1-5) in the prompt to demonstrate the desired output format and style.	For tasks that require a specific output format or when the model needs a bit of guidance to understand the task.
Chain-of-Thought (CoT) Prompting	Guiding the model to break down a complex problem into a series of intermediate reasoning steps before providing a final answer.	For complex tasks that require logical reasoning, such as math problems, strategic analysis, or multi-step instructions.

Professional Prompting Framework: RTFD (Role, Task, Format, Details)

The RTFD framework is a simple yet powerful way to structure your prompts for professional use. It ensures that you provide the AI with all the necessary information to generate a high-quality response.

- **Role:** Assign the AI a specific professional role (e.g., "Act as a data analyst," "You are a senior copywriter").
- **Task:** Clearly and concisely define what you want the AI to do.
- **Format:** Specify the desired output format (e.g., "in a bulleted list," "as a JSON object," "in a professional email format").
- **Details:** Provide any additional context, constraints, or information the AI needs to complete the task (e.g., "target audience is C-level executives," "the tone should be formal and persuasive").

Prompting Best Practices Checklist

- ❑ **Be Specific and Clear:** Avoid ambiguity. The more specific your instructions, the better the result.
- ❑ **Provide Context:** Give the AI the background information it needs to understand the task.
- ❑ **Define the Audience:** Tell the AI who the response is for.
- ❑ **Specify the Tone and Style:** Guide the AI on the desired tone and style of the response.
- ❑ **Use Examples:** When in doubt, provide a few examples of what you're looking for.
- ❑ **Iterate and Refine:** Don't expect the perfect response on the first try. Experiment with different prompts and refine your approach based on the results.

Your AI Toolkit: Prompt Templates for the Workplace

This section provides a collection of ready-to-use prompt templates for common workplace tasks. Use these as a starting point and customize them to fit your specific needs.

Email & Communication

1. Draft a Professional Email

Act as a [Your Role]. Draft a professional email to [Recipient Name] about [Topic]. The key points to include are:

* [Point 1]

* [Point 2]

* [Point 3]

The tone should be [Tone] and the desired outcome is [Outcome].

2. Summarize a Long Email Thread

Summarize the following email thread into three key takeaways. For each takeaway, provide a brief explanation of its importance.

[Paste Email Thread Here]

3. Rewrite an Email for Clarity and Impact

Rewrite the following email to be more concise, persuasive, and professional. The target audience is [Audience].

[Paste Email Draft Here]

Productivity & Time Management

1. Create a Meeting Agenda

Create a meeting agenda for a [Duration]-minute meeting about [Topic]. The attendees are [Attendee Names]. The key objectives of the meeting are:

* [Objective 1]

* [Objective 2]

The agenda should include time allocations for each topic and a list of any necessary pre-reading materials.

2. Plan Your Day

Act as a productivity coach. Based on the following list of tasks and priorities, create a time-blocked schedule for my day. I have meetings at [Meeting Times].

Tasks:

* [Task 1] (Priority: [High/Medium/Low])

* [Task 2] (Priority: [High/Medium/Low])

* [Task 3] (Priority: [High/Medium/Low])

Creative & Strategic Thinking

1. Brainstorm Ideas

Act as a [Role, e.g., marketing strategist, product manager]. Brainstorm [Number] creative ideas for [Topic]. For each idea, provide a brief description and a potential first step.

2. Solve a Problem

I am facing the following problem: [Describe the problem in detail]. Using the Chain-of-Thought technique, break down the problem into its root causes and propose three potential solutions. For each solution, list the pros, cons, and potential risks.

The Reflective Practitioner

This section provides a space for you to reflect on how you can apply the concepts from the talk to your own work. Use these prompts to think critically about your relationship with technology and to identify opportunities for positive change.

- **Automating the Drain, Not the Drive:** What are the top 3-5 tasks that drain your energy and could potentially be automated or delegated to AI? What are the core activities that give you a sense of purpose and fulfillment?

- **Keeping Humans in the Loop:** In what areas of your work is human oversight and judgment absolutely essential? How can you design workflows that leverage AI for efficiency while ensuring that you remain in control of the final output?

- **Measuring Wellness, Not Just Output:** What are some ways you could track your own well-being at work? What metrics, other than productivity, could you use to measure a "good" day?

Action & Accountability

This final section provides a set of checklists to help you put what you've learned into practice. Use these as a guide to integrate AI into your workflows in a way that promotes both productivity and well-being.

AI Implementation Checklist

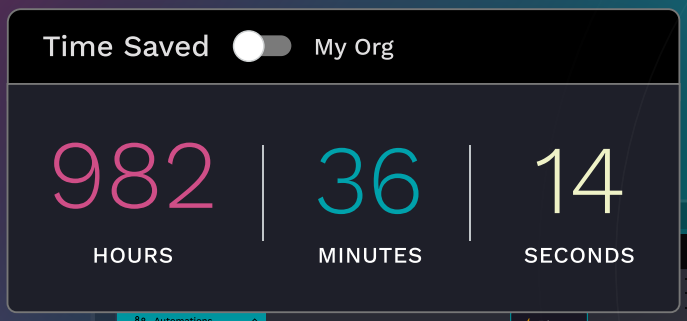
- ❑ **Identify a Low-Stakes Task:** Start with a simple, repetitive task that is not mission-critical.
- ❑ **Choose the Right Tool:** Select an AI tool that is well-suited for the task.
- ❑ **Craft Your Prompt:** Use the RTFD framework to create a clear and effective prompt.
- ❑ **Test and Refine:** Run the prompt and evaluate the output. Refine the prompt as needed.
- ❑ **Integrate into Your Workflow:** Once you are satisfied with the results, integrate the AI-powered task into your regular workflow.
- ❑ **Monitor and Adjust:** Periodically review the process and make adjustments as needed.

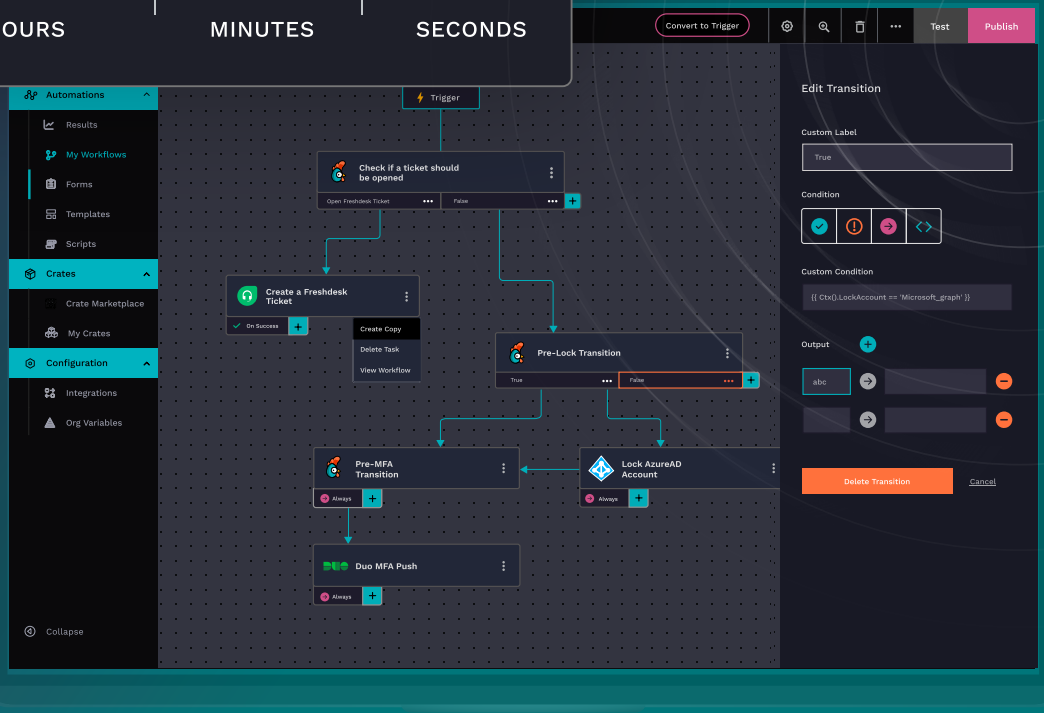
Wellness Checklist

- ❑ **Schedule Regular Breaks:** Step away from your computer for a few minutes every hour.
- ❑ **Set Boundaries:** Define clear start and end times for your workday.
- ❑ **Disconnect:** Avoid checking work email and messages outside of your working hours.
- ❑ **Move Your Body:** Incorporate physical activity into your daily routine.
- ❑ **Practice Mindfulness:** Take a few minutes each day to meditate or simply be present in the moment.
- ❑ **Connect with Colleagues:** Make time for social interaction with your coworkers.
- ❑ **Celebrate Small Wins:** Acknowledge and appreciate your accomplishments, no matter how small.

Unlock Scalable Growth with Automation

Discover 10 common use cases for MSPs





rewst

rewst.io

Fireside Chat with Logically's AI Team - Lessons Learned from the Trenches.

Chris Morton, Chief Information Officer, Logically
https://www.linkedin.com/in/christopher-morton-b10b4313/
Jake Tarrant, Security Operations Center Manager, Logically
https://www.linkedin.com/in/jake-tarrant-aba436188/
Jason Hall, Regional Director of Managed Services, Logically
https://www.linkedin.com/in/jason-hall-97ab59102/
Carl Gallicchio, Director of IT Operations & Governance, Logically
https://www.linkedin.com/in/cgallicchio/

Session Recording: https://vimeo.com/1133875090/9af04b05e0?share=copy&fl=sv&fe=ci

Presentation Materials: https://go.logically.com/hubfs/LogicON25/Session-PDFs/Fireside%20chat%20with%20Logicallys%20%20AI%20Team%20-%20Lessons%20learned%20from%20the%20trenches.pdf

AI adoption is rarely smooth, especially for mid-market teams balancing risk, culture, and integration challenges. In this candid conversation with Logically's AI leadership, we'll explore what it really takes to implement AI across departments. Hear real-world lessons about navigating internal resistance, aligning AI to business priorities, mitigating risks, and partnering with vendors like Copilot and Hatz.AI. It's a behind-the-scenes look at what worked, what didn't, and how Logically is designing a responsible AI culture for long-term success.

Learning Outcomes:

- Understand common pitfalls and breakthroughs in AI adoption.
- Learn strategies for cross-functional AI enablement.
- Gain insight into aligning technical rollouts with cultural change.

Notes:

Turning Problems into AI/RPA Solutions

Checkpoint 1: Define the Problem

Mission Objective: Identify a real problem AI/RPA can solve.

Every good mission starts with clarity. The more specific the problem, the easier it is to test and solve. Don't aim for "world peace" — think about pain points like wasted time, repetitive work, or delays in decision-making.

Problem Statement:

_____
_____
_____
_____
_____
_____

Checkpoint 2: Break the Problem into Chunks

Recon Report: Split the big problem into 3–5 smaller chunks.

Large challenges often feel overwhelming. By dividing the mission into manageable pieces, you make it easier to find quick wins and test solutions. Each chunk should be distinct but related to the bigger mission.

Chunk 1: _____

Chunk 2: _____

Chunk 3: _____

Chunk 4: _____

Chunk 5: _____

Checkpoint 3: Select Priority Target

Ascertain the Target: Choose the most testable chunk for your initial mission focus.

Not all problems are equal. Some are too big, some too vague, some too costly to tackle first. Select the chunk where AI/RPA can make an immediate impact and where testing is realistic within 30 days.

Priority Target: _____

Checkpoint 4: Tactical Options

Mission Directive: Brainstorm at least 3 solution ideas for your chosen chunk.

Creativity fuels progress. Don't stop at one idea — map out a baseline option, a realistic test idea, and a stretch idea that pushes the limits. Remember: the goal isn't to be perfect, it's to explore.

Idea 1 (Baseline): _____

Idea 2 (Test Idea): _____

Idea 3 (Stretch Idea): _____

Checkpoint 5: After-Action Notes

Debrief: Decide what you'll test first and what you hope to learn.

Action beats theory. The best AI/RPA strategies emerge from real-world tests. Identify one solution you can pilot within 30 days and capture what success (or failure) will teach you.

Solution to Test in 30 Days:

_____
_____
_____
_____
_____
_____

Expected Lesson Learned:

_____
_____
_____
_____
_____
_____

Field Note

The magic isn't in the tool.
It's in **learning fast, failing small, and scaling what works**.

Data or Bust: Building the Backbone for AI Success

Callen Sapien, CEO, Synthreo
https://www.linkedin.com/in/callensapien/

Session Recording: https://vimeo.com/1133964578/eebabb0ab4?share=copy&fl=sv&fe=ci

Presentation Materials: https://go.logically.com/hubfs/LogicON25/Session-PDFs/Data%20or%20Bust%20-%20Building%20the%20Backbone%20for%20AI%20Success.pdf

AI is only as good as the data behind it. This session dives into how to clean, structure, and govern data so it can be used safely and effectively in AI workflows. We'll explore how IT leaders can modernize legacy data environments, implement role-based access, and ensure data quality and security—while still enabling fast experimentation and decision-making. Learn the fundamentals that make or break enterprise AI readiness.

Learning Outcomes:

- Learn best practices for data hygiene, lineage, and governance.
- Build secure pipelines that prepare data for machine learning.
- Enable agile data use without compromising compliance.

Notes:

The Data-to-AI Readiness Playbook

AI initiatives are only as strong as the data they rely on. Poor data quality, fragmented ownership, and missing governance structures can derail even the best AI strategy—costing months of effort and substantial investment. Use this section to align leadership on **why** data readiness is non-negotiable before scaling AI.

Top 3 Risks of Ignoring Data Cleanup

- ❑ Loss of trust in AI outcomes due to incomplete, duplicated, or siloed data
- ❑ Delayed decision-making from unreliable or slow reporting
- ❑ Security and compliance exposure from uncontrolled data access

Top 3 Business Outcomes of Doing It Right

- ❑ Faster, more accurate decisions across departments
- ❑ Reduced operational waste and reporting inefficiencies
- ❑ Proven AI readiness — pilots that scale into production with ROI

Leadership Readiness: Data as a Strategic Asset

Before tools or technology, success starts with ownership. Leadership alignment ensures accountability and sustained investment in data quality initiatives.

Checklist — Executive Actions

- ❑ Sponsor a data ownership and governance program
- ❑ Secure cross-department executive buy-in
- ❑ Assign data owners and stewards; connect metrics to OKRs
- ❑ Require AI readiness checks before funding pilots
- ❑ Add data governance as a standing agenda item in leadership meetings

Notes / Decisions: _____

Setting the Baseline: Your "Before and After"

This helps visualize what transformation looks like — from messy, unreliable systems to data-driven outcomes that unlock AI potential. Fill in a few ideas of systems within your organization.

Current State (Before)	Future State (After)
CRM has 15% duplicates; reports take hours; no clear owner.	*Chatbot resolves 60% of tickets; reports refresh automatically; data ownership embedded.*

The Data-to-AI Journey

Every AI-ready organization follows this maturity path — from assessing foundations to automating governance. Use this map to locate where you are and define your next milestone.

Stage	Key Activities	Typical Timeline	Business Impact
Foundation	Audit sources, identify quick wins, assign data owners	1–2 months	Builds trust — AI learns from reliable data
Enablement	Cleanse, standardize, secure access, document lineage	2–3 months	Consistent data powers search & pilots
Implementation	Build pipelines, dashboards, and pilots	3–4 months	Improves accuracy, reduces AI hallucinations
Scaling	Automate monitoring, expand governance, roll out AI	Ongoing	Enables production-grade, trustworthy AI

Where are you now? □ Foundation □ Enablement □ Implementation □ Scaling

Prioritizing Data Work: The Heatmap

Not all problems are equal. This scoring tool helps you identify and sequence the most critical cleanup and governance actions.

Instructions:
Rate each area **1 (Low)** to **5 (Critical)** for *Impact* and *Urgency*. Multiply for total priority.
Focus on areas scoring **15 or higher** before starting any AI pilot.

Area	Best Practice Target	Impact (1–5)	Urgency (1–5)	Priority (I×U)	Notes / Actions
Inventory	100% of critical data sources cataloged with owner + refresh cadence				
Quality	≥98% accuracy; ≥95% completeness; <1% duplicates				
Ownership	One accountable owner per dataset, reviewed quarterly				
Access Control	Least privilege + MFA for production data				
Integration	Automated pipelines with lineage; <1-hour lag for ops data				

AI Readiness Gate: *Do not advance to AI pilots until Inventory & Quality ≥ 15.*

Executing Quick Wins

Start small, prove impact, and build momentum. Quick-win data projects deliver measurable improvements within weeks, not months. Here are some typical examples.

System	Top 3 Issues	Quick Win Action	Result / Benefit
CRM	15% duplicates; missing emails; inconsistent state abbreviations	Use built-in deduplication; standardize fields	Duplicates <1%; improved forecast accuracy
ERP	Duplicate vendors; missing tax IDs	Merge vendor records; validate IDs	Fewer AP errors; 2-day faster close
HRIS	Inconsistent job codes	Standardize codes; sync with payroll	Fewer onboarding errors; accurate headcount

Your Quick Win Project:
System: _____
Action: _____
Expected Outcome: _____

Building Governance that Scales

Governance ensures long-term sustainability — keeping data accurate, secure, and trusted as AI scales across functions.

Roles & Responsibilities

- *Executive Sponsor:* Ensures budget and organizational support
- *Data Owner:* Accountable for data quality, refresh, and access
- *Data Steward:* Executes ongoing monitoring and remediation

Governance Cadence

- *Monthly:* Run data quality checks and anomaly reports
- *Quarterly:* Conduct governance reviews and update scorecards

Sample RACI Matrix

Task	Exec Sponsor	Data Owner	Data Steward	IT / Security
Define standards	A	C	R	C
Run quality checks	C	C	R	I
Approve access	C	A	R	R
Report to leadership	A	R	C	I

(A = Accountable | R = Responsible | C = Consulted | I = Informed)

Your First 30 Days

Turn insights into immediate progress. Use this four-week plan to operationalize governance and start improving data quality fast.

Week	Action Step	Owner / Notes
Week 1	Run a 15-minute data audit; identify top 3 data pain points	
Weeks 2–3	Complete the Priority Heatmap; assign owners; choose a quick-win cleanup	
Week 4	Launch the quick-win; record baseline KPIs (accuracy %, duplicates %, report time)	

Tip: Share your Heatmap and KPIs with leadership to secure visibility and future investment.

Sustaining Momentum: Implementation & Scaling

Once foundations are solid, focus on process automation and measurable outcomes from AI pilots.

Implementation Checklist

- ❑ Design and build secure data pipelines
- ❑ Implement RBAC and access logging
- ❑ Deploy data quality and anomaly dashboards
- ❑ Select 1–2 AI pilot use cases; define success metrics (precision, recall, time saved)
- ❑ Run pilots only on datasets ≥95% quality
- ❑ Automate quality checks and anomaly alerts
- ❑ Publish quarterly data quality reports
- ❑ Create a model retraining / re-embedding cadence

Next Actions / Responsible Owner: _____

Reflection & Next Steps

Close the loop. Reflect on your progress, capture lessons, and identify the next opportunity for AI enablement.

- **Biggest data quality win:** _____
- **Blockers that remain:** _____
- **Next AI use case to explore:** _____
- **Date for next review session:** _____

Quick Reference: Data Glossary

Term	Definition
Database	Structured collection of stored data
Schema	Blueprint of a dataset (fields, data types)
Metadata	Descriptive info: owner, refresh time, sensitivity
Data Pipeline	Automated flow for moving and transforming data
RAG	Retrieval-Augmented Generation (search + AI model)
Embeddings	Numeric representations of text for semantic search
RBAC	Role-Based Access Control
Lineage	Documented flow from source to output
Deduplication	Removing duplicate records
KPI	Key Performance Indicator — tracks progress

Resource Guide

Open-Source Tools:

- dbt
- Great Expectations
- Airbyte
- Metabase

Low-Cost SMB Tools:

- Talend Cloud
- Fivetran Starter
- BigQuery Sandbox

Learning:

- *Coursera — Data Management for AI*
- *O'Reilly — Data Quality Handbook*

Shadow AI: The Invisible Threat Inside Your Organization

Zack Finstad, Vice President of Cybersecurity, Logically
https://www.linkedin.com/in/zacharyfinstad/

Session Recording: https://vimeo.com/1133960795/a0cba1c853?share=copy&fl=sv&fe=ci

Presentation Materials: https://go.logically.com/hubfs/LogicON25/Session-PDFs/Shadow%20AI%20-%20The%20Invisible%20Threat%20Inside%20Your%20Organization.pdf

AI use is exploding across teams—but much of it is happening without oversight. Shadow AI represents a growing threat vector where well-meaning employees introduce tools like ChatGPT or Gemini without security controls or compliance visibility. This session explores how to identify and rein in Shadow AI, develop policy frameworks, and foster a culture of responsible innovation before exposure leads to disaster.

Learning Outcomes:

- Define and detect Shadow AI within your organization.
- Develop governance models that enable transparency and safe experimentation.
- Prevent inadvertent IP leakage and regulatory violations.

Notes:

Shadow AI Discovery & Risk Audit

To identify, assess, and create a governance plan for unauthorized or unmanaged AI tools ("Shadow AI") being used within the organization.

What is Shadow AI?

Shadow AI refers to any AI tools, applications, or services used by employees without official approval, procurement, or oversight from the IT, Security, or Governance departments. While often adopted to improve productivity, they can introduce significant risks.

Section 1: Discovery & Inventory

Brainstorm with department heads (e.g., Marketing, Sales, R&D, HR) to identify tools employees might be using. Think about browser extensions, web apps, and APIs.

Department	Potential Use Case	Known or Suspected Tool(s)	What kind of data is being input? (e.g., PII, confidential, public)	Is there an official, company-approved alternative? (Y/N)
Example: Marketing	*Blog post drafting*	*Copy.ai, Jasper, ChatGPT Free*	*Internal strategy documents, public web data*	*N*

Download template:
https://go.logically.com/hubfs/logicon25/Downloadable%20Templates/shadowai-section-1-discovery-inventory.csv

Section 2: Risk Assessment

For each tool identified in Section 1, perform a risk assessment. Use the following scale:

- **Likelihood/Impact Scale:** 1 (Very Low) to 5 (Very High)
- **Risk Score = Likelihood × Impact**
- **Risk Level:** Low (1-8), Medium (9-16), High (17-25)

Tool Identified	Primary Risks (e.g., Data Leak, IP Loss, Compliance, Inaccuracy)	Data Sensitivity (Low/Med/High)	Likelihood of Risk Occurring (1-5)	Impact if Risk Occurs (1-5)	Risk Score	Risk Level
Example: ChatGPT Free	*Data Leak (conversations used for training), IP Loss*	*Medium*	*4*	*4*	*16*	*Medium*

Download template:
https://go.logically.com/hubfs/LogicON25/Downloadable%20Templates/shadowai-section-2-risk-assessment.csv

Section 3: Mitigation & Action Plan

Based on the risk levels identified in Section 2, define your response.

1. ***High-Risk Tools (Score 17-25):***
   - *Immediate Action:* _____
     (Example: Block access to the tool at the network level; communicate immediate cessation of use.)
   - *Long-Term Plan:* _____
     (Example: Procure an enterprise-grade, secure alternative that meets the business need.)
2. ***Medium-Risk Tools (Score 9-16):***
   - *Immediate Action:* _____
     (Example: Issue interim guidance on acceptable use; prohibit use with sensitive data.)
   - *Long-Term Plan:* _____
     (Example: Begin a formal vetting process to decide whether to approve, sanction, or block the tool.)
3. ***Low-Risk Tools (Score 1-8):***
   - *Action Plan:* _____
     (Example: Formally approve the tool for specific use cases; add it to an "Approved Tool List".)
4. ***Policy & Training:***
   - *Draft or update the company's "Acceptable Use Policy" to include AI tools.*
   - *Develop a clear process for employees to request new AI tools.*
   - *Plan a training session for all employees on the risks and responsible use of AI.*

AI Risk Tolerance & Strategy Alignment

Objective: To define the organization's appetite for various AI-related risks and ensure that current and future AI initiatives are aligned with this tolerance level.

What is Risk Tolerance? Risk tolerance is the specific, acceptable level of variation from your organization's overall risk appetite. It sets the threshold for when a risk becomes unacceptable and requires mitigation.

Define Your Risk Appetite

For each category, discuss and define your organization's general appetite for risk. This sets the strategic tone.

Risk Category	**Risk Appetite** (Low / Medium / High)	**Justification & Guiding Principle**
Example: *Ethical & Reputational* *(Bias, fairness, brand damage)*	*Low*	*"Our brand is built on trust. We will not deploy AI that could lead to public criticism or discriminatory outcomes."*
Ethical & Reputational *(Bias, fairness, brand damage)*		
Data Security & Privacy *(Data leaks, PII breaches)*		
Compliance & Legal *(GDPR, CCPA, industry regulations)*		
Model Performance & Accuracy *("Hallucinations," poor decisions)*		
Operational Reliance *(Disruption if AI fails)*		
Financial & ROI *(Project over-runs, failing to deliver value)*		

Download template:
https://go.logically.com/hubfs/LogicON25/Downloadable%20Templates/shadowai-section-1-define-your-risk-appetite.csv

Audit & Align Current AI Projects

List your organization's key AI projects (planned or in-progress). Audit them against the risk appetite defined above.

AI Project / Initiative	**Primary Risks Involved** (from Section 1 categories)	**Current Assessed Risk Level** (Low/Med/High)	**Aligned with Appetite? (Y/N)**	**Required Action for Alignment**	**Owner**	**Deadline**
Example: *AI for resume screening*	*Ethical & Reputational (bias), Compliance (hiring laws)*	*High*	*N (Appetite is Low)*	*Conduct bias audit; implement human-in-the-loop review.*	*HR Director*	*Next 30 days*

Download template:
https://go.logically.com/hubfs/LogicON25/Downloadable%20Templates/shadowai-section-2-audit-align-current-ai-projects.csv

Section 3: Governance & Review Cadence

A risk framework is only useful if it's maintained. Define how your organization will govern this.

1. Who is responsible for overseeing AI risk?
   - ❑ An existing committee (e.g., Risk & Compliance, IT Governance)
   - ❑ A new, dedicated AI Governance Board
   - ❑ A designated individual (e.g., Chief AI Officer, Head of Innovation)

2. How often will this AI Risk Tolerance framework be reviewed and updated?
   - ❑ Quarterly
   - ❑ Semi-Annually
   - ❑ Annually, or when a significant change occurs (e.g., new regulation, major new project)

3. How will project teams use this framework?
   - ❑ All new AI projects must complete a Risk Alignment assessment (from Section 2) before budget approval.
   - ❑ Project teams must report on their risk mitigation progress on a _____ basis.
   - ❑ The "Approved AI Tool List" will be managed by _____ and reviewed _____.

Artificial Intelligence Tool Policy Sample

Section: Security | **Policy No:** LGOV_101

Subject: Responsible use of AI Tools | **Issue Date:** 01/01/2025

Owner: Governance | **Version:** Original v1.0

Artificial Intelligence (AI) tools are transforming the way we work. They have the potential to automate tasks, improve decision-making, and provide valuable insights into our operations. **{Company Name}** 's AI tool usage policy outlines best practices for use of artificial intelligence tools in our company, especially as it pertains to using sensitive data and proprietary company and customer information in these tools.

Scope

This policy applies to all **{Company Name}** employees, contractors, and any other personnel who access and use AI tools in the course of their work for **{Company Name}** .

Purpose

The purpose of this policy is to ensure that all **{Company Name}** personnel use AI tools in a secure, responsible and confidential manner. Careless use of AI tools presents the possible risk of:

- Human bias: prospective employees, employees, clients, and other individuals experiencing unfair or discriminatory treatment based upon inaccurate AI results;
- Privacy and data security law violations: disclosure of personally identifiable information without consent.
- Copyright infringement: AI data output includes someone else's copyrighted materials used or disclosed by **{Company Name}** or its employees without authorization.
- Loss of important Company trade secrets: disclosure to a third party AI tool of Company's trade secrets results in the loss of trade secret ownership/protection.
- Unfair and deceptive law violations: incorporation of third party AI tools with **{Company Name}** products/services without an understanding of the AI tool ("blackbox effect") may cause substantial injury to consumers who rely upon the products/services and therefore violate state and federal consumer protection laws.

{Company Name} issues this Policy to provide you with (i) knowledge of the above AI risks and (ii) responsibilities to safeguard against those risks. This policy outlines the requirements that employees must follow when using AI tools, including the evaluation of security risks and the protection of confidential data.

Other Company Policies

{Company Name} 's Acceptable Use Policy governs overall use of Company information and equipment while this policy serves as supplemental guidance. Our organization recognizes that the use of AI tools can pose risks to our operations and clients. Therefore, we are committed to protecting the confidentiality, integrity, and availability of all company and client data consistent with Company Policies. This policy requires all personnel to use AI tools in a manner consistent with **{Company Name}** policy.

Your Responsibilities

All employees, contractors, or other personnel who access AI tools are expected to adhere to the following acceptable use and security best practices when using AI tools:

- Evaluation of AI tools: For individual use of publicly accessible tools, personnel must evaluate the security of the AI tool before using it. This includes reviewing the tool's security features, terms of service, and privacy policy. Personnel must also check the reputation of the tool developer and any third-party services used by the tool before any AI tool can be used with **{Company Name}** data or on **{Company Name}** systems. This ensures that periodic security review will occur, according to risks posed by the specific tools. AI tools may include incidental use of AI chatbots such as ChatGPT and others accessible on public web pages.
- Protection of confidential data: Personnel **are prohibited** from uploading or sharing any company data or other data made available to them as a result of their employment or contract with **{Company Name}** that is confidential, proprietary, or sensitive without written, prior approval from the Executive Leadership Team. This includes internal emails, texts, chats, client data and any other data related to products, services, vendors, employees, or partners.
- Review and Approval Process: Before any confidential or sensitive **{Company Name}** data can be used with or by an AI Tool, explicit written permission from the Executive Leadership Team must be obtained. Requests for approval should be directed to the Governance Team distribution group. The governance team will review all requests for business value and potential security risks and present the findings to the executive leadership team for approval.
- Access control: Personnel **are prohibited** from giving access to AI tools, licensed to the Company, to any other entity or person outside the company without prior approval from the Governance committee and subsequent processes as required to meet security and other legal and compliance requirements. This includes sharing login credentials or other sensitive information with third parties.
- Use of reputable AI tools: Personnel should use only enterprise version licenses (in lieu of general consumer licensed software) issued by reputable AI tools and be cautious
- when using tools developed by individuals or companies without established reputations. Any AI tool used by personnel must meet our security and data protection standards.
- Compliance with security policies: Personnel must apply the same security best practices we use for all company and customer data. This includes using strong passwords, keeping software up-to-date, and following our data retention and disposal policies and verifying AI license terms are consistent with these policies.
- Data privacy: Personnel must exercise discretion when sharing information publicly. As a first step, Personnel must ask themselves the question, "Would I be comfortable sharing this information outside of the Company? Would we be okay with this information being leaked publicly?" before uploading or sharing any data into AI tools. Second would be to follow the "Protection of confidential data" step above.

Monitoring

{Company Name} owns and operates company-issued communication systems and equipment and therefore monitors employee and contractor uses of these systems and equipment, whether accessed at work or elsewhere, through remote telecommunication. The purpose of this monitoring is to ensure protection of **{Company Name}** 's intellectual property and compliance with federal, state, and local laws and regulations, this policy, and other company policies and procedures.

Violations

Employees or contractors who violate this Policy are subject to discipline which can include termination. Failure to adhere to this policy may also constitute violations of other company policies of **{Company Name}** or governmental entities.

Employees can report actual or perceived violations to supervisors, or anonymously with Red Flag Reporting. Red Flag Reporting can be used by visiting RedFlagReporting.com (Code: **{Company Name}**) or calling 1-877-64-REDFLAG (1-877-647-3335).

Revision History

Version	Date	Editor	Approver	Description of Changes
1.0	11/28/2025	CIO	CEO	Final Approval by ELT and CEO.
.2	11/12/25	IS Team Project Manager	CIO	Consolidated revisions from CPO, CIO, and COO to make the policy {Company Name} specific, fix grammatical errors, and include several other AI-related notes.
.1		IT Ops Engineer Name		Addition of the policy overall and editing for specific **{Company Name}** content and language.

Download template:

https://go.logically.com/hubfs/LogicON25/Downloadable%20Templates/Logically-AI-Policy-Template.docx

Seeing Isn't Believing: Deepfakes and the Erosion of Digital Trust

Buddy Pitt, vCSO, Logically
https://www.linkedin.com/in/buddypitt/
Jake Tarrant, Security Operations Center Manager, Logically
https://www.linkedin.com/in/jake-tarrant-aba436188/

Session Recording: https://vimeo.com/1133848622/2778a1d856?share=copy&fl=sv&fe=ci

Presentation Materials: https://go.logically.com/hubfs/LogicON25/Session-PDFs/Seeing%20Isnt%20Believing%20-%20Deepfakes%20and%20the%20Erosion%20of%20Digital%20Trust.pdf

In a digital world shaped by generative AI, the ability to manipulate audio, video, and images with startling realism has sparked a new class of cybersecurity and reputational threats—deepfakes. While headlines often highlight political implications or celebrity hoaxes, the real risk to mid-market IT and security teams lies in business email compromise, executive impersonation, fraud, and social engineering attacks amplified by synthetic media.

This session will explore the rise of deepfake technology, including how it's created, why it's growing more accessible, and what it means for organizations that rely on trust and identity verification. From targeted phishing campaigns to synthetic voice fraud, we'll examine the evolving threat landscape and highlight real-world use cases that expose vulnerabilities in employee training, authentication systems, and crisis communication protocols.

You'll walk away with a clearer understanding of how to assess your organization's exposure to deepfake-enabled threats, build defensive frameworks that include awareness training and AI-powered detection tools, and protect your executive team and brand from manipulation.

Key Takeaways:

- Learn how deepfakes are created and where they pose the most risk to mid-sized businesses
- See examples of deepfake-enabled attacks in the wild and their operational consequences
- Understand how to detect, defend, and respond to identity-based threats using AI and layered security
- Get practical tools to train your teams, secure executive communications, and safeguard trust in an era where seeing—and hearing—is no longer believing

Notes:

Deepfake Orgnaizational Self-Assessment

In the presentation "Seeing Isn't Believing: Deepfakes and the Erosion of Digital Trust" – it was shown how easy it is to deepfake a person. Does your organization have the right controls in place?

Reflecting on Leadership & Authority

An organization's leaders are its most valuable asset and its most prominent target. Their public presence creates the raw material for impersonation.

Thought-Provoking Questions:

1. How much of your key executives' voice and likeness is publicly available (e.g., podcasts, conference talks, media interviews, social media videos)? Who has the most "training data" available online?

   _____
   _____
   _____
   _____
   _____

2. In your company, what is the cultural response to a request from the CEO or another senior leader? Is it "Yes, right away," or is there space for "Let me just verify that"? Be honest about the power dynamics at play.

   _____
   _____
   _____
   _____
   _____

3. Imagine you received an urgent voice message from your boss asking for a "quick favor" that was slightly unusual. What is your immediate, gut reaction? What feelings or pressures would influence your next action?

   _____
   _____
   _____
   _____
   _____

4. If a leader needed to prove their identity to you over the phone, what "secret" question or piece of shared knowledge would they use? Now, could an attacker find that information by researching their social media or your company's history?

   _____
   _____
   _____
   _____
   _____

Reflecting on Financial Processes & Pressure

Fraud follows the money. Deepfake attacks on financial processes are designed to create a sense of urgency that bypasses normal procedures.

Thought-Provoking Questions:

1. Describe the process for an urgent, out-of-cycle wire transfer. Who feels the most pressure to act quickly? Where are the points of friction that someone might be tempted to skip "just this once"?

2. What happens if an employee *challenges* a financial request from a senior executive? Is that employee praised for their diligence or subtly seen as "not a team player"? What does this tell you about your security culture?

3. Think of the last time a financial control was bypassed for a legitimate, urgent reason. Why was it bypassed? What does that incident reveal about the strength of your day-to-day processes when they are under pressure?

4. When your team receives a request for payment or information, what is their default method for verification? Is it hitting "reply" to the email? Is it calling a phone number that was provided *in the suspicious request itself*?

Reflecting on Company Culture & Awareness

Your culture can be your greatest defense or your biggest vulnerability. It dictates how your team responds to the unusual, the unexpected, and the urgent.

Thought-Provoking Questions:

1. How would you describe your company's "speed of business"? Are you a culture that values meticulous process, or one that rewards rapid, decisive action? How could an attacker leverage that pace against you?

2. Imagine a junior employee spots something "off" about a request from a senior leader. How confident are you, on a scale of 1-10, that they would feel psychologically safe enough to raise the alarm? What barriers might stop them?

3. When was the last time your team talked about a real-world security incident or scam (either at your company or one in the news)? Is security an ongoing conversation, or something only discussed during annual training?

4. If you had to tell a new hire the "unwritten rule" for handling a strange request from leadership, what would it be? Does that unwritten rule match your official policy?

From Reflection to Action

Now, let's turn these reflections into a commitment.

1. **My Single Biggest Realization:** After considering these questions, what is the most surprising or concerning vulnerability you've identified in your organization?

   _____
   _____
   _____
   _____
   _____

2. **The One Conversation to Start:** Based on your realization, what is the single most important conversation you need to have, and who do you need to have it with (e.g., your CFO, your leadership team, your entire staff)?

   _____
   _____
   _____
   _____
   _____

3. **The One Process to Fortify:** What is the one process (e.g., wire transfers, IT admin changes, executive communications) that you will commit to strengthening in the next 30 days? What is the first step?

   _____
   _____
   _____
   _____
   _____

SentinelOne

Evolve Beyond Legacy Security

Staying Ahead of Modern Threats Starts with Singularity™ Endpoint.

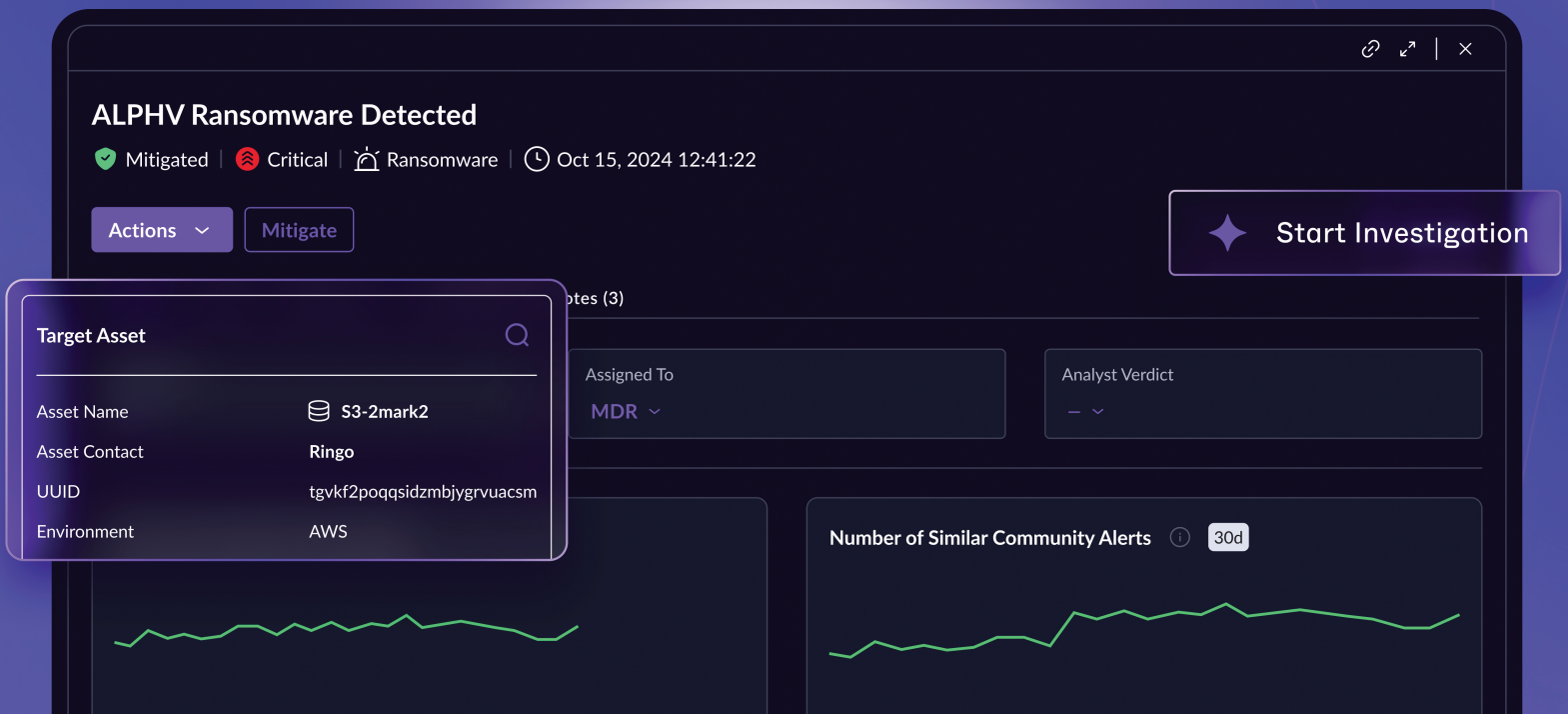
Enterprise-Wide Protection
One platform with AI-powered EPP, EDR, and XDR

Purple AI
The world's most advanced AI cybersecurity analyst

AI SIEM
Protect your organization with the industry's fastest open platform

AI-Powered CNAPP
Secure every aspect of your cloud in real time

Learn More at sentinelone.com



Change Smarter: Leading Through the Disruption of Change

Tony Chatman, Keynote Speaker, Author, Organizational Culture Expert
https://www.linkedin.com/in/tonychatman/

Session Recording: https://vimeo.com/1133844080/b4f7ed910d?share=copy&fl=sv&fe=ci

Presentation Materials: https://go.logically.com/hubfs/LogicON25/Session-PDFs/Change%20Smarter%20-%20Leading%20Through%20the%20Disruption%20of%20Change.pdf

We often plan for change but disruption comes without little or no warning. It's unsettling and disorienting. We lose our routines, our sense of stability. sense of community, and often even our confidence. Yet we still need to be able to function, keep our heads, and be productive before a sense of normalcy has emerged.

You don't just need more inspiration. You need traction. That's where this keynote comes in.

You have the unenviable task of needing to navigate change and lead it at the same time. You can't afford to just "manage change." You need to lead through it.

You Will Learn How To:

- Focus Where It Matters Most: Identify the people and pressure points that offer the highest return on effort and use them to spark real traction during times of change.
- Turn Resistance Into Resilience: Uncover the hidden drivers behind pushback and reframe challenges into opportunities for growth, buy-in, and stronger team dynamics.
- Communicate to Make Change Stick: Leverage the most underused leadership tool to build trust, inspire ownership, and ensure that change doesn't just happen it lasts.

Bottom Line

When you are navigating change, you don't need theory. You need traction. You need tools. You need leadership that lights the way forward. Because when you know where to focus, how to communicate, and how to turn resistance into resilience, change becomes a launchpad, not a landmine.

Notes:

Leading Through the Disruption of Change Takeaways

Most Change Efforts Fail!

- 70% of companies are unsuccessful in implementing reengineering programs
- 70 - 80% of companies do not obtain the expected return on quality improvement investments
- 75% of cultural change initiatives do not achieve the required change in the organization's culture
- 60 - 70% of companies do not realize expected benefits from implementing technology initiatives
- 50 - 60% of customer service programs do not result in benefit to the customer

1. It's All About Resistance—Expect It

COMMON RESISTANCE EMOTIONS:

Surprise	***Resentment***	***Loss***
Shock	***Sadness***	***Relief***
Denial	***Fear***	***Uncertainty***
Numbness	***Worry***	***Frustration***
Anger	***Confusion***	***Depression***
Stress	***Low Energy***	***Reservation***

Key Takeaways:

- Change Is Personal: Change isn't just organizational—it's emotional. What feels strategic to you may feel chaotic to someone else.
- Your Change = Their Disruption: What leaders see as purposeful and planned, others often experience as unexpected and unsettling.

GRIEF CYCLE – THE NATURAL EMOTIONAL RESPONSE TO LOSS

Emotion	Strategy
Denial	People deny that the loss will actually happen. It doesn't demand action on your part unless it goes on too long. If people stay in denial for more than a few days, then address it, such as saying, "A lot of you are acting as though X isn't for real. Well, it is. I'm concerned because I want all of us to get through this change with as little distress and disruption as possible. We'll never do that if we pretend it isn't happening."
Anger	Everything from grumbling to rage, often misdirected or undirected. It can lead to foot-dragging, mistakes, and even sabotage. Listen and acknowledge that the anger is understandable. Don't take on the blame if it is being misdirected toward you. Distinguish between the acceptable emotions and the unacceptable acting-out behavior: "I can appreciate how you feel, however I'm not going to allow this project to fail. Nor do I want to see you fail."
Bargaining	Bargaining appears as unrealistic attempts to get out of the situation, trying to strike a special deal, or making big promises if you'll only undo the change. Distinguish between bargaining efforts and real problem solving. Keep a realistic outlook and don't be swayed by desperate arguments or impossible promises.
Anxiety	Silent or expressed, it is a realistic fear of an unknown and probably difficult future. It can include catastrophic fantasies. Help people to not feel stupid for feeling it; anxiety is natural. Just keep feeding them the information as it comes, and commiserate with them when it doesn't.
Sadness	You see everything from silence to tears. Encourage people to say what they are feeling, and share your feelings too. Don't try to reassure people with unrealistic suggestions of hope. Sympathize. You can be sympathetic to the feelings, even as you continue to support the change.
Disorientation	Confusion, forgetfulness, and feelings of being lost and insecure are common. Give people extra support, such as opportunities to get things off their chests, and reassurances that disorientation is natural and common. Give them extra attention.
Depression	Feelings of being down, of hopelessness, and being tired all the time. You, and others on your team, will probably find it is hard to be around someone with depression. You can't make it go away. People have to go through it, not around it. Make it clear that you understand and even share the feeling yourself, but that work still needs to be done. Help restore people's sense of having some control over their situations.

Key Takeaways:

- When disruption hits, people go through the same stages as grieving a loss: Denial, Anger, Bargaining, Depression, before eventual acceptance.
- Don't trust your emotions during disruption—they are often poor indicators of reality.

The Stressor Scale

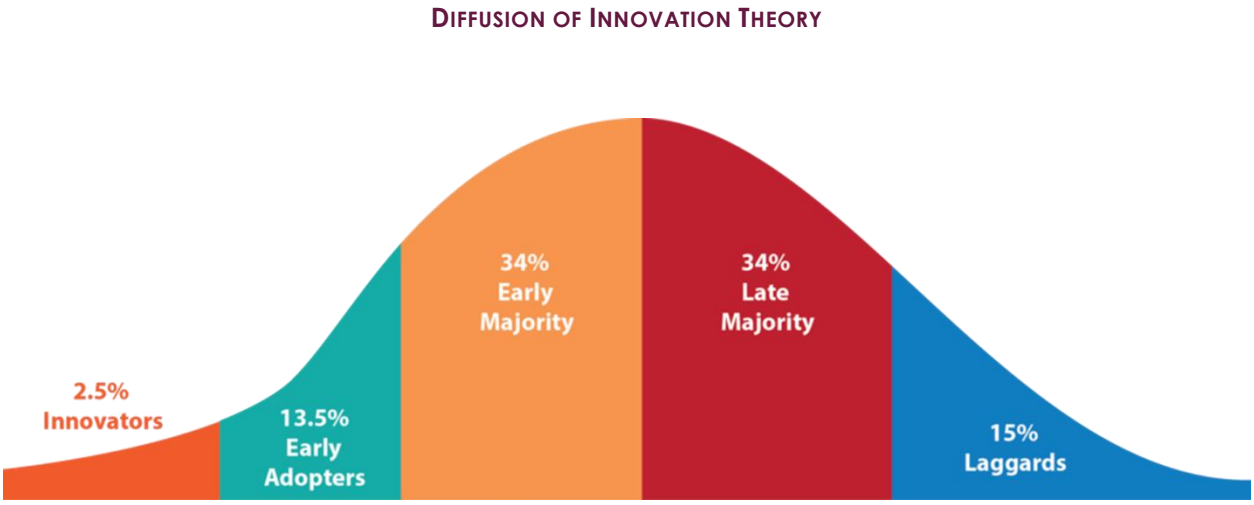
Death of spouse	100	Change in number of marital arguments	35
Divorce	73	Mortgage or loan over $10,000	31
Marital separation	65	Foreclosure of mortgage or loan	30
Jail term	63	Change in work responsibilities	29
Death of close family member	63	Son or daughter leaving home	29
Personal injury or illness	53	Trouble with in-laws	29
Marriage	50	Outstanding personal achievement	28
Fired from job	47	Spouse begins or ceases working	26
Marital reconciliation	45	Starting or finishing school	26
Retirement	45	Change in living conditions	25
Change in family member's health	44	Revision of personal habits	24
Pregnancy	40	Trouble with boss	23
Sexual difficulties	39	Change in work hours, conditions	20
Addition to family	39	Change in residence	20
Business readjustment	39	Change in schools	20
Change in financial status	38	Change in recreational habits	19
Death of close friend	37	Change in church activities	19
Career change	36	Change in social activities	18

2. Over-Communicate

Key Takeaways:

- Most organizations underestimate the volume of communication needed during disruption.
- Incomplete communication leaves space for fear and speculation. When people don't have answers, they fill in the blanks.
- A formal communication strategy is non-negotiable. Ad hoc updates aren't enough—your message needs structure, consistency, and intention.

3. Focus on The Right People



Don't focus on Innovators or Laggards—they're either already on board or unlikely to shift.

Who to focus on if you want change embedded in your organization?

Focus your efforts where they matter most: Top Leadership, Middle Managers, and especially Opinion Leaders.

Fortifying the Cloud Edge: Securing and Scaling AI-Driven Infrastructures

JT Fanning, Senior Manager of Strategic Partners and Cloud Security, SonicWall
https://www.linkedin.com/in/jtfanning/

Session Recording: https://vimeo.com/1133896814/6782ee3ecf?share=copy&fl=sv&fe=ci

Presentation Materials: https://go.logically.com/hubfs/LogicON25/Session-PDFs/Fortifying%20the%20Cloud%20Edge%20-%20Securing%20and%20Scaling%20AI-Driven%20Infrastructures.pdf

As organizations embrace AI to enhance operations, the expansion of cloud-based infrastructure introduces new security challenges at the network edge. This session explores the evolving landscape of cloud edge security, focusing on strategies to safeguard AI-driven workloads and ensure seamless scalability.

Attendees will learn about:

- the role of unified security frameworks (SASE),
- real-time threat detection,
- and adaptive access controls in protecting distributed environments.

Notes:

Fortifying the Cloud Edge Session Worksheet

Use this worksheet during the presentation to jot notes, answer prompts, and build your own action plan.

Section 1: The Reality Check – Physical vs. Digital Security

"If someone stole your office chair, you'd know exactly what it cost. But if someone stole your data…?"

1. List 3 types of physical security you currently have in place (locks, cameras, etc.):

   _____
   _____
   _____

2. List 3 types of digital security measures you have in place:

   _____
   _____
   _____

3. Takeaway: How does the cost of lost data compare to lost equipment for your organization?

   _____
   _____
   _____

Section 2: Why Businesses Stay Exposed

1. Which of these factors apply to your organization? (check all that apply)
   - ❑ Resistance to MFA
   - ❑ Legacy applications/workflows
   - ❑ Limited visibility into user/device access
   - ❑ No centralized policy enforcement
   - ❑ Other: _____
2. What's one "we've always done it this way" process you suspect is creating risk?

   _____
   _____
   _____

Section 3: Zero Trust + AI Complications

1. **Zero Trust Reality Check:** Rate your organization's maturity:
   - ❑ 1 - No Zero Trust practices
   - ❑ 2 - Some isolated policies
   - ❑ 3 - Partial rollout
   - ❑ 4 - Nearly complete
   - ❑ 5 - Fully implemented
2. List any AI tools or agents your staff are already using (officially or unofficially):

   _____
   _____
   _____

3. Where are the biggest unknowns about how those AI tools handle your data?

   _____
   _____

Section 4: Data & Stories That Stick

1. **Shadow AI Self-Audit:**
   Have you identified "Shadow AI" usage (employees using AI outside IT oversight)?
   ☐ Yes ☐ No ☐ Not Sure
2. If yes, how do you currently govern or restrict it?

   _____

   _____
3. **Incident Reflection:**
   If your organization suffered a breach/ransomware event tomorrow, what would be the *business impact* (lost revenue, regulatory fines, reputational damage)?

   _____

   _____

Section 5: From Fear to Action – Build Your Plan

Three Things You Can Do Today - Use the checklist below to mark your progress:

Action Item	Status	Notes
Define critical data and access (where it resides, who can touch it)	☐ Not Started ☐ In Progress ☐ Done	
Evaluate Zero Trust readiness and AI usage across your environment	☐ Not Started ☐ In Progress ☐ Done	
Ask your team key questions (data location, access controls, policies)	☐ Not Started ☐ In Progress ☐ Done	

Your Next 30 Days:
List one step you can commit to before the end of the month:

_____

_____

Section 6: Questions for Your Team After the Session

- Where is our most sensitive data located?
- Who has access, and under what conditions?
- What controls do we have to prevent "Shadow AI" risks?
- How quickly can we detect and respond to threats at the edge?

Use the below space for your notes:

_____

_____

Section 7: Call to Action

"Don't wait until your Fitbit logs a breach-induced marathon. Start today, with what's in the workbook."

- Schedule a security review or Zero Trust assessment: _____
- Meet with your IT/security partner to review AI-related policies: _____

Checklist for Zero Trust Evaluation

For each question, rate your organization from **1 (lowest maturity/risk awareness)** to **5 (highest maturity/best practice)**. Circle one number per question, then total your score at the bottom.

1. **How well do you know the value of your digital assets?**
   - ❑ 1 – I honestly don't know
   - ❑ 2 – I have a rough idea, but haven't measured
   - ❑ 3 – I know where they are, but not the true cost of loss
   - ❑ 4 – I have identified key data and partial cost estimates
   - ❑ 5 – I know exactly where they are and their business value
2. **How strong are your access practices (MFA, device trust, identity checks)?**
   - ❑ 1 – No MFA, users log in however they want
   - ❑ 2 – MFA only on a few critical systems
   - ❑ 3 – Partial rollout, user pushback common
   - ❑ 4 – MFA enforced on most systems with some exceptions
   - ❑ 5 – MFA enforced everywhere with strong identity policies
3. **How modern is your remote access approach?**
   - ❑ 1 – Legacy VPN/SSL, "make it work" mindset
   - ❑ 2 – Mostly VPN, no visibility into traffic
   - ❑ 3 – Hybrid of VPN and newer access tools
   - ❑ 4 – Majority Zero Trust or SASE adoption
   - ❑ 5 – Fully implemented Zero Trust framework
4. **How does your organization manage AI tool usage (ChatGPT, Copilot, etc.)?**
   - ❑ 1 – No awareness or rules, employees use freely
   - ❑ 2 – Aware but no policies in place
   - ❑ 3 – Discussed but rules not enforced
   - ❑ 4 – Policies exist, some monitoring in place
   - ❑ 5 – Clear policies, training, and monitoring for AI use
5. **How prepared are you for a cyberattack (backup, recovery, insurance)?**
   - ❑ 1 – No plan, would be in big trouble
   - ❑ 2 – Backups exist but no tested recovery
   - ❑ 3 – Plans exist but rarely tested
   - ❑ 4 – Plans tested occasionally, partial coverage
   - ❑ 5 – Full playbooks, backups, insurance, and tested recovery

Your Score: _____/25

21–25 → **Ahead of the curve.** Keep adapting for AI-driven risk.
16–20 → Solid progress, but gaps remain. Prioritize modernization.
11–15 → **High risk.** Outdated practices leave you exposed.
≤10 → **Critical risk.** You should urgently evaluate.

Bonus question: How comfortable are you deploying security solutions?

- ❑ 1 – I don't feel comfortable at all
- ❑ 2 – I rely on a trusted IT provider to handle it
- ❑ 3 – I have some in-house knowledge but need outside help
- ❑ 4 – I have an IT/security team that can manage most projects
- ❑ 5 – We have a fully equipped staff for end-to-end deployment

Note: Less than 16 on the above and 1-3 on the bonus should really consider outside guidance.

Traditional VPN Solutions Are Broken—It's Time to Modernize

Secure Remote Access Made Simple with CSE

Running a small- to medium-sized business (SMB) comes with enough challenges—managing customers, growing your team and keeping operations running smoothly—while also staying up to date with the latest technology. On top of all that, cyberattacks targeting SMBs are becoming more frequent at a rate that can no longer be ignored.

> **In fact, recent reports indicate that 43% of cyberattacks are aimed at small businesses, yet only 14% are adequately prepared to defend themselves.**

It's no surprise attackers frequently target smaller firms, assuming many SMBs are not equipped to handle security breaches.

One of the most critical areas where SMBs should focus their security investments is in upgrading their remote access strategy to a secure, modern solution. As your business—and the world—transitions to cloud-first applications and supports a modern workforce that values flexibility to work in the office, at home or even at a coffee shop, ensuring secure access is essential.

For an SMB, malware, ransomware and beyond aren't just annoying issues—they're costly and devastating. Leading analysts in the cybersecurity industry estimate the average cost of an attack on SMBs can range from $25,000 to as much as $3 million. The good news: proactively securing your business is far less expensive (and far less stressful) than dealing with the aftermath of a cyberattack. Investing in solutions that offer comprehensive protection can help you avoid the steep costs, downtime and recovery challenges that follow an attack.

Learn more at:
go.logically.com/spa-vpn-as-a-service

SONICWALL®

Essential AI Use Cases as an IT Manager

Dustin Greiner, Solutions Architect, Logically
https://www.linkedin.com/in/rdgreiner/
John McFarland, Service Delivery Manager, Logically
https://www.linkedin.com/in/john-mcfarland-83a96a10/
Alex Burton, Microsoft Partnership Manager, Logically
https://www.linkedin.com/in/davidalexanderburton/
Charles Brandt, Security Director, Rewst
https://www.linkedin.com/in/charlesbrandt/

Session Recording: https://vimeo.com/1133925477/79e6b5f0e0?share=copy&fl=sv&fe=ci

Presentation Materials: https://go.logically.com/hubfs/LogicON25/Session-PDFs/Essential%20AI%20use%20cases%20as%20an%20IT%20Manager.pdf

IT managers are often expected to deliver more with fewer resources—and AI can help, if applied thoughtfully. This session explores real-world use cases where AI is augmenting IT operations, from meeting transcription and analytics to advanced troubleshooting and reporting. You'll hear how frontline teams are using tools like CoPilot to drive productivity, assist with training, and enhance knowledge sharing—without compromising security or oversight.

Learning Outcomes:

- Discover tactical AI use cases relevant to day-to-day IT management.
- Learn how to enable secure access to generative tools for staff.
- Explore metrics for measuring the impact of AI in service and support workflows.

Notes:

Steps to a Successful Prompt

Step 1: Define the Objective Clearly

- **What to do:** State what you want the output to achieve.
- **Why it matters:** A clear goal helps the AI (or person) understand the purpose and direction.
- *Example:*
  - "Summarize this report for executive review."
  - "Generate ideas for a marketing campaign targeting Gen Z."

Step 2: Provide Relevant Context

- **What to do:** Include background info, constraints, or the situation.
- **Why it matters:** Context helps tailor the response to your needs.
- *Example:*
  - "This is for a retail company launching a new app."
  - "The audience is non-technical stakeholders."

Step 3: Specify Format and Style

- **What to do:** Indicate how you want the output delivered (e.g., list, summary, slide outline, code).
- **Why it matters:** Format guides structure and usability.
- *Example:*
  - "Give me a bullet-point list."
  - "Write in a persuasive tone, under 300 words."

Step 4: Add Constraints or Success Criteria

- **What to do:** Include limits, benchmarks, or what "good" looks like.
- **Why it matters:** Constraints keep the output focused and aligned.
- *Example:*
  - "Include 3 examples and avoid jargon."
  - "Make it suitable for a 5-minute presentation."

Step 5: Invite Clarifying Questions

- **What to do:** Encourage the AI (or team) to ask for more info if needed.
- **Why it matters:** Clarifying questions reduce ambiguity and improve quality.
- *Example:*
  - "Let me know if you need more details about the audience or use case."
  - "Ask me if anything is unclear before you start."

What's Most Important in a Prompt	
Element	Why it's important
Clarity	Prevents confusion and vague responses
Context	Ensures relevance and personalization
Format	Makes the output usable and actionable
Constraints	Keeps the response focused and high-quality
Feedback Loop	Allows refinement through clarifying questions

Prompt Examples for IT Business Leaders

Here's a deep dive into the top 5 most valuable prompt scenarios for a corporate IT business leader, each crafted to deliver maximum actionable output and include a feedback loop for refinement and iteration.

1. Digital Transformation Roadmap

Optimized Prompt: *"Act as a CIO for a mid-sized enterprise in [industry]. Build a 12-month digital transformation roadmap aligned with business goals such as [e.g., operational efficiency, customer experience, cost reduction]. Include:*

- *Strategic initiatives (e.g., cloud migration, automation, AI adoption)*
- *Quarterly milestones*
- *Required cross-functional collaboration*
- *KPIs to measure success*
- *Dependencies and risks*

After presenting the roadmap, ask: 'Which initiatives or timelines need adjustment based on current business constraints or leadership priorities?' Then refine accordingly."

Why It Works:
This prompt balances strategic vision with tactical execution, and the feedback loop ensures alignment with real-world constraints and stakeholder buy-in.

2. Hybrid Cloud Optimization Checklist

Optimized Prompt: *"Create a comprehensive checklist and action plan for optimizing hybrid cloud infrastructure in a corporate environment using both on-prem and Azure workloads. Include:*

- *Cost optimization strategies (e.g., reserved instances, rightsizing)*
- *Performance tuning (e.g., latency, load balancing)*
- *Security and compliance controls*
- *Governance and tagging policies*
- *Tooling recommendations (e.g., Azure Advisor, Defender for Cloud)*

After presenting, ask: 'Which area—cost, performance, or security—is currently the biggest pain point?' Then generate a deeper dive into that area."

Why It Works:
This prompt drives operational efficiency and cost savings while allowing the leader to focus on the most pressing infrastructure challenge.

3. Zero Trust Architecture Rollout Plan

Optimized Prompt: *"Design a phased rollout plan for implementing Zero Trust architecture in a corporate IT environment. Include:*

- *Identity and access management (e.g., MFA, conditional access)*
- *Device trust (e.g., endpoint protection, compliance policies)*
- *Network segmentation and micro-perimeters*

- *Application-level controls and monitoring*
- *User education and change management Present quick wins and long-term investments.*

Then ask: 'Which phase presents the biggest challenge in your current environment—identity, device, network, or application?' Refine the plan based on that input."

Why It Works:
Zero Trust is complex, and this prompt breaks it into digestible phases while allowing the leader to prioritize based on organizational maturity.

4. IT Performance Dashboard Design

Optimized Prompt: *"Design a dashboard layout to monitor IT service performance across the enterprise. Include:*

- *Key metrics (e.g., incident volume, resolution time, SLA compliance, user satisfaction)*
- *Visualization recommendations (e.g., Power BI, ServiceNow, Tableau)*
- *Segmentation by department or region*
- *Automated data sources and refresh cycles*

After presenting, ask: 'Which metrics are most critical to your leadership team's decision-making?' Then tailor the dashboard to emphasize those metrics."

Why It Works:
This prompt ensures visibility into IT operations and aligns reporting with executive priorities, making it a powerful tool for continuous improvement.

5. IT Budget Forecast Model

Optimized Prompt: *"Build a quarterly IT budget forecast model for a corporate IT department. Include:*

- *Historical spend analysis*
- *Upcoming initiatives and project costs*
- *Vendor contract timelines and renewal estimates*
- *Personnel and training costs*
- *Scenario modeling (best-case, worst-case, most likely)*

After presenting, ask: 'Do you want to model specific initiatives or adjust assumptions based on leadership feedback?' Then refine the forecast accordingly."

Why It Works:
Budgeting is both strategic and tactical. This prompt provides a flexible model that can be adapted to changing priorities or financial constraints.

Internal AI Poll

Here's the poll we gave the Logically team, drop it into your favorite Forms with your preferred setting and send it out! If anonymizing responses, we recommend separate polls for departments to aggregate data.

We also recommend that you add questions directly related to your organization's workflow and culture to find out details specific to your teams.

1. **How often do you use AI tools in your daily workflow?**
    a. Daily
    b. A few times a week
    c. Occasionally
    d. Rarely
    e. Never
2. **Which AI tools do you use most frequently? (*Multiple Choice)***
    ❑ CoPilot
    ❑ ChatGPT
    ❑ Gemini
    ❑ Claude
    ❑ Grok
    ❑ Perplexity
    ❑ Other (*If your Forms tool supports it, set to fill in the blank)*
3. **Do you have a preferred AI tool?**
    a. Yes
    b. No
4. **Which AI model do you prefer?**
    a. CoPilot
    b. ChatGPT
    c. Gemini
    d. Claude
    e. Grok
    f. Perplexity
    g. Other
    h. None
5. **Why do you prefer your chosen AI model or version for your tasks? (*Multiple Choice)***
    ❑ Better Accuracy
    ❑ Easier Interface
    ❑ Integration with Existing Tools
    ❑ Faster Response Times
    ❑ No Preference
    ❑ Other (*If your Forms tool supports it, set to fill in the blank)*
6. **What tasks do you use AI tools for? (*Multiple Choice)***
    ❑ Troubleshooting Issues
    ❑ Drafting Client Communications
    ❑ Summarize Meetings and Emails
    ❑ Learning New Tools
    ❑ Automation of Tasks
    ❑ Other (*If your Forms tool supports it, set to fill in the blank)*

7. **What challenges have you faced when using AI tools? (*Multiple Choice*)**
    - ❑ Lack of Training
    - ❑ Inaccurate Responses
    - ❑ Integration Issues with Tools
    - ❑ Security Concerns
    - ❑ Data Integrity Concerns
    - ❑ Other (*If your Forms tool supports it, set to fill in the blank)*
8. **What kind of support or resources would help you use AI tools more effectively? (*Multiple Choice*)**
    - ❑ Training Sessions
    - ❑ Use Case Examples
    - ❑ One on One Coaching
    - ❑ Other (*If your Forms tool supports it, set to fill in the blank)*
9. **What would encourage you to use AI tools more often? (*Multiple Choice*)**
    - ❑ More Training or Onboarding
    - ❑ Better Integration with Existing Systems
    - ❑ Clear Use Cases
    - ❑ Peer Recommendations
    - ❑ Other (*If your Forms tool supports it, set to fill in the blank)*
10. **How confident are you in the responses provided by AI tools?**
    a. Very Confident
    b. Somewhat Confident
    c. Neutral
    d. Not Very Confident
    e. Not Confident at All
11. **How do you stay updated on the latest developments in AI tools relevant to your role? (*Multiple Choice*)**
    - ❑ Company Training Sessions
    - ❑ Online Courses or Webinars
    - ❑ Industry Newsletters
    - ❑ Peer Recommendations
    - ❑ Social Media and Forums
    - ❑ Other (*If your Forms tool supports it, set to fill in the blank)*
12. **Please share any additional comments or suggestions about AI usage in your role.** *If your Forms tool supports it, set this question to 'long answer' or equivalent to allow teammates to answer in full.*
13. **What are two common or preferred prompts you use when using AI to get specific information you regularly need?** *If your Forms tool supports it, set this question to 'long answer' or equivalent to allow teammates to answer in full.*

From Telemetry to Triumph: Driving AI-Powered Performance with Sauber F1

Dan Dulac, Vice President of GTM Strategic Programs, Extreme Networks
https://www.linkedin.com/in/dan-dulac-6495926/

Session Recording: https://vimeo.com/1133893068/a951588e1c?share=copy&fl=sv&fe=ci

Presentation Materials: https://go.logically.com/hubfs/LogicON25/Session-PDFs/From%20Telemetry%20to%20Triumph%20-%20Driving%20AI-Powered%20Performance%20with%20Sauber%20F1.pdf

In the high-octane world of Formula 1, every millisecond counts—and every byte of data matters. Nowhere is the demand for speed, precision, and reliability greater than in the race to the podium. In this keynote, discover how the Sauber Formula 1 team leverages Extreme Networks cutting-edge technology to operate as one of the world's most data-driven enterprises. From capturing and transmitting real-time telemetry to harnessing AI for predictive analytics, Sauber transforms torrents of data into split-second insights that can make the difference between victory and a dreaded DNF. And just like Sauber, every business enterprise today faces the same challenge: turning massive amounts of real-time data into intelligence that drives agility, innovation, and competitive advantage. Join us for an inside look at how Extreme's next-generation networking fuels innovation, enhances reliability, and helps one of the sport's most storied teams stay ahead of the curve—both on and off the track.

Notes:

Modern Networking: From Legacy Complexity to Intelligent Connectivity

This worksheet helps you reflect on how Fabric Networking—the modern approach to secure, automated, and intelligent connectivity—addresses the limitations of legacy network architectures.

A Fabric connects your entire environment as a single, virtualized network. It simplifies provisioning, enhances visibility, and ensures that users and services connect securely—no matter where they are.

1. Quick Insight Check

1. What are the top **three frustrations** your team faces today in managing your network?
   - ❑ Manual configuration steps
   - ❑ Lack of end-to-end visibility
   - ❑ Complex VLAN structures
   - ❑ Long maintenance windows
   - ❑ Security segmentation challenges
   - ❑ Other: _____
2. **True or False:** Modern network architectures allow provisioning and changes to happen **at the edge**, not at the core.
   - ❑ True
   - ❑ False
3. **Fill in the blanks:** Modern networks are designed to be _____, _____, and _____, reducing operational risk and enabling faster change.

2. Apply It to Your Environment

1. When you think about your organization's current network, where do you see the biggest **manual effort or delay** today (e.g., provisioning, security policies, troubleshooting)? *Write a few examples:*

   _____
   _____
   _____
   _____

2. Imagine your network could self-adjust to traffic changes or add new sites automatically. What business outcomes would that unlock? How would it change your team's daily operations?

   _____
   _____
   _____
   _____

3. What's one step your organization could take this year to make your network more:

   - **Visible:** _____
   - **Automated:** _____
   - **Resilient:** _____

3. Action Planning

1. Based on today's session, identify one area where **network modernization** could deliver the most value:
   - ❑ Improved user experience
   - ❑ Reduced downtime
   - ❑ Faster cloud adoption
   - ❑ Simplified security
   - ❑ Cost optimization
   - ❑ Other: _____
2. What's one initiative you'll explore or accelerate after LogicON to modernize your network?

   _____
   _____
   _____
   _____

Tip: Modernization doesn't always mean replacement—it often starts with rethinking architecture, visibility, and automation.

Extreme networks

One Powerful, Unified Experience

Extreme Platform ONE™ radically simplifies complexity by unifying networking, security, and AI.

Learn More:
extremenetworks.com/platform-one

AI as a Cybersecurity Force Multiplier: Practical Use Cases from the Field

Kyle Sandy, Director of Cybersecurity, Logically
https://www.linkedin.com/in/kyle-sandy-cissp-cism-17a527152/
Rob Dunn, Senior Escalation Engineer, Logically
https://www.linkedin.com/in/rob-dunn0712/
Chandra Pandey, Founder and CEO, Seceon
https://www.linkedin.com/in/chandrashekharpandey/

Session Recording: https://vimeo.com/1133955624/64424f34ee?share=copy&fl=sv&fe=ci

Presentation Materials: https://go.logically.com/hubfs/LogicON25/Session-PDFs/AI%20as%20a%20Cybersecurity%20Force%20Multiplier%20-%20Practical%20Use%20Cases%20from%20the%20Field.pdf

This session moves beyond theory into practical application. Drawing from their own cybersecurity workflows, the team of experts will demonstrate how AI is transforming detection, triage, and even reporting. Whether it's breaking down complex vendor configs, speeding up ticketing, or translating technical speak into business language, this is a hands-on look at AI in action—from one security practitioner to another.

Learning Outcomes:

- See firsthand how AI is augmenting the cybersecurity toolkit.
- Explore specific time-saving and decision-support use cases.
- Understand best practices for adoption without over-reliance.

Notes:

AI as a Cybersecurity Force Multiplier: Field Application Worksheet

This worksheet helps you translate today's session insights into practical next steps for your organization. As you explore how AI is augmenting cybersecurity detection, triage, and reporting, use this guide to evaluate your current workflows, identify where AI can help, and capture actionable prompt ideas to experiment with back at your desk.

Use Cases in Action

The panelists will share specific, real-world examples of how AI is used in cybersecurity environments — from triaging alerts to creating leadership-ready reports. Use this section to document what stands out and assess which examples could be replicated or adapted within your own security operations.

Instructions: As each example is discussed, note the challenge it addressed, how AI helped solve it, and whether it's applicable to your team's environment.

Use Case Example	Challenge It Solved	How AI Helped	Could This Apply to My Org?
Vendor configuration breakdown	Complex, multi-vendor syntax	AI summarized configs and flagged misalignments	☐ Yes ☐ Maybe ☐ No
Alert triage and classification	Too many false positives	AI clustered events, summarized probable root cause	☐ Yes ☐ Maybe ☐ No
Executive report generation	Technical detail overwhelm	AI turned SOC notes into business-readable summaries	☐ Yes ☐ Maybe ☐ No
Threat intel correlation	Disparate data sources	AI identified emerging patterns and overlaps	☐ Yes ☐ Maybe ☐ No
			☐ Yes ☐ Maybe ☐ No
			☐ Yes ☐ Maybe ☐ No
			☐ Yes ☐ Maybe ☐ No
			☐ Yes ☐ Maybe ☐ No
			☐ Yes ☐ Maybe ☐ No
			☐ Yes ☐ Maybe ☐ No
			☐ Yes ☐ Maybe ☐ No

Operational Reality Check

Before adding new tools or AI workflows, it helps to understand where your current pain points lie. This section helps you quickly benchmark the maturity and speed of your existing processes.

Instructions:
Rate your organization's strength in each core area using a scale of 1–5 (1 = weak or manual, 5 = strong and efficient). Then identify where your team spends the most time or struggles the most.

Function	1 (Weak)	2	3	4	5 (Strong)
Detection accuracy	☐	☐	☐	☐	☐
Alert triage speed	☐	☐	☐	☐	☐
Root cause analysis	☐	☐	☐	☐	☐
Incident response efficiency	☐	☐	☐	☐	☐
Ticket documentation quality	☐	☐	☐	☐	☐
Knowledge base management	☐	☐	☐	☐	☐
Executive/Board reporting	☐	☐	☐	☐	☐
Threat communication clarity	☐	☐	☐	☐	☐

Biggest time drain: _____

AI Opportunity Mapping

AI can boost efficiency at multiple stages of the security lifecycle — but you'll get the best results when you target one area first. This section helps you focus where AI could deliver the greatest impact in your environment.

Instructions:
Based on the biggest time drain selected above, describe your current challenge, how AI could address it, and what a successful outcome would look like.

- **Biggest challenge today:** _____
- **AI could help by:** _____
- **What success would look like:** _____

PROMPT LIBRARY

- **Detection Accuracy**
  Goal: Improve precision and reduce false positives.
  - *Structured prompt (for automation):*
    - "You are an AI security assistant analyzing SIEM logs from the past 24 hours. Identify anomalies that deviate from baseline behavior and summarize them by source, frequency, and potential severity. Exclude known false positives and provide a short confidence rating for each detection."
  - *Analyst prompt (for insight generation):*
    - "Compare today's detection alerts against the previous 7-day trend. Highlight any new or unusual event patterns, explain why they might be significant, and suggest one correlation or rule refinement to improve accuracy."
- **Alert Triage Speed**
  Goal: Accelerate sorting, clustering, and prioritization of alerts.
  - *Structured prompt:*
    - "You are assisting with SOC triage. Categorize these alerts into 'Critical,' 'High,' 'Medium,' and 'Low' based on context indicators, repetition, and source IP reputation. Provide a one-line justification for each categorization."
  - *Analyst prompt:*
    - "Summarize this batch of alerts by probable root cause and urgency. Identify duplicates, known benign events, and any alerts requiring immediate analyst attention. Recommend what to escalate versus close."
- **Root Cause Analysis**
  Goal: Trace incidents back to their origin quickly and consistently.
  - *Structured prompt:*
    - "Given this incident log, identify the most likely root cause based on event sequence, process lineage, and prior alert correlations. Present your reasoning in a 3-step cause chain (trigger → compromise → outcome)."
  - *Analyst prompt:*
    - "Explain the chain of events that led to this security incident in plain language. What underlying misconfiguration, user behavior, or system weakness contributed most to the issue?"
- **Incident Response Efficiency**
  Goal: Speed containment and streamline remediation actions.
  - *Structured prompt:*
    - "Analyze this incident ticket and generate a prioritized response plan including immediate containment steps, verification checks, and suggested remediation actions. Output in checklist format."
  - *Analyst prompt:*
    - "Review this incident timeline and identify where response could have been faster or automated. Suggest one AI-assisted improvement (e.g., auto ticket creation, alert correlation, or playbook triggering)."

- **Ticket Documentation Quality**
  Goal: Improve clarity, consistency, and reporting speed.
  - *Structured prompt:*
    - "Summarize this closed incident ticket in 3 sentences for SOC records. Include incident type, duration, impact, and resolution steps. Use consistent terminology and omit redundant details."
  - *Analyst prompt:*
    - "Generate a concise summary of this ticket suitable for executive review. Include the what, when, impact, and resolution, then recommend how this case could improve future detection or triage."
- **Knowledge Base Management**
  Goal: Capture recurring lessons and maintain playbook consistency.
  - *Structured prompt:*
    - "From the last 10 resolved tickets, extract common remediation patterns and update the knowledge base entry for 'Phishing Response Playbook.' Present findings in table format with fields for symptom, cause, fix, and prevention."
  - *Analyst prompt:*
    - "Summarize recurring lessons from recent incidents. Recommend one new entry or update to the SOC playbook that captures best practices and prevents similar issues."
- **Executive / Board Reporting**
  Goal: Communicate technical outcomes in clear business terms.
  - *Structured prompt:*
    - "Convert this technical incident report into a two-paragraph executive summary. Use business language, quantify impact (financial or operational), and highlight mitigation status and next steps."
  - *Analyst prompt:*
    - "Draft a 'Cybersecurity Monthly Snapshot' summarizing top 3 threats, key metrics (MTTR, false positive rate, incidents prevented), and one major improvement area. Keep it under 200 words and audience-ready."
- **Threat Communication Clarity**
  Goal: Deliver the right information to the right audience.
  - *Structured prompt:*
    - "Translate this security bulletin into a non-technical summary suitable for IT and HR teams. Explain what's at risk, recommended action, and urgency level in under 150 words."
  - *Analyst prompt:*
    - "Given this detected vulnerability and internal memo, create two tailored communications: one for technical staff (implementation guidance) and one for executives (risk and business impact). Highlight tone and key differences."

Note: *Since AI hallucinations are common, always verify with human review.*

Technology Stack Rehab – TCO & Tool Sprawl

Jeremy Williams, Chief Operating Officer, Logically
https://www.linkedin.com/in/jeremy-williams-0091536b/

Session Recording: https://vimeo.com/1133854293/5071cb888d?share=copy&fl=sv&fe=ci

Presentation Materials: https://go.logically.com/hubfs/LogicON25/Session-PDFs/Technology%20Stack%20Rehab%20%E2%80%93%20TCO%20&%20Tool%20Sprawl.pdf

Tool sprawl has become one of the most expensive and inefficient problems in IT and cybersecurity. This session focuses on how to consolidate and rationalize your tech stack—while improving outcomes. Learn how to measure tool overlap, eliminate shelfware, and integrate platforms for visibility, cost control, and operational efficiency.

Learning Outcomes:

- Audit and assess your current toolset.
- Identify redundancy and inefficiency in the technology stack.
- Build a plan for consolidation that aligns with business risk.

Notes:

Technology Stack Rehab – Post-Session Action Guide

Session Summary

As technology teams face increased pressure to deliver outcomes faster, cheaper, and with more intelligence, many organizations fall into the trap of 'tool sprawl'—overlapping systems, unused software, and ballooning costs. This guide helps you identify and eliminate redundancy in your stack, with special attention to AI tools promising transformational change.

Key Takeaways

- Audit tools based on specific business problems they solve.
- Identify overlap, shelfware, and inefficiencies.
- Measure true TCO—beyond licensing fees.
- Rationalize tools and prioritize platform consolidation.
- Align AI tools with strategic business outcomes, not hype.

Tool Audit Template

Use this worksheet to assess your entire stack. Focus on how each tool contributes to a measurable business goal. If there's overlap, explore consolidation opportunities.

Tool Name	Business Challenge Solved	Annual Cost	Utilization (%)	Overlap? (Y/N)	AI Integration (Low/Med/High)

Next Steps Checklist

1. Inventory all tools across business units and functions.
2. Map each to a core business problem or goal.
3. Eliminate shelfware and duplicates—prioritize essential tools.
4. Reinvest in platforms that integrate well and reduce complexity.
5. Document your decisions and communicate the 'why' to leadership.

AI in the Stack – Strategic Opportunity or Sprawl Risk?

AI is the buzzword of the year—but it's also a major contributor to renewed tool sprawl. Many vendors are pitching AI-powered solutions that often duplicate existing functionality found in your CRM, ERP, or business intelligence platforms.

Ask these questions when evaluating any new AI tool:

- What business problem does this solve better than existing systems?
- Is this a standalone AI product, or part of an extensible platform?
- What is the real cost to integrate this with my environment?
- Can I achieve this functionality by enabling features I already license?

AI Consolidation Strategy

- Commit to 1–2 anchor platforms (e.g., Microsoft, Google, or an ERP suite).
- Build on those platforms with native integrations or extensions.
- Resist point solutions unless they solve a niche, critical need.
- Review your AI stack annually for redundancy and alignment with business goals.

Exercise: Evaluating AI in Your Stack

Use the following exercise to review your current or planned AI tools. The goal is to determine if these solutions add unique value, or if they risk contributing to tool sprawl.

Instructions:

- List any current or proposed AI tools.
- Identify the specific business challenge it addresses.
- Evaluate whether this capability exists in other platforms you already use.
- Determine if this AI tool should be kept, consolidated, or avoided.

AI Tool Name	Business Challenge Solved	Already Exists in Platform? (Y/N)	Integration Needed? (Y/N)	Action (Keep/Consolidate/ Avoid)

Born with a Bot: Educating the AI-Native Generation

Colin Carhart, Technical Account Manager, Logically
https://www.linkedin.com/in/colin-carhart/
Chris Morton, Chief Information Officer, Logically
https://www.linkedin.com/in/christopher-morton-b10b4313/
Suzanne Bryan, Project Manager, Logically
https://www.linkedin.com/in/suzanne-bryan-4b73041/
Randy Hall, Vice President of Delivery Operations, Logically
https://www.linkedin.com/in/randyhall3/
Maddie Nemcik, Executive Assistant, Logically
https://www.linkedin.com/in/maddie-nemcik/

Session Recording: https://vimeo.com/1134687837/70871473af?share=copy&fl=sv&fe=ci

Presentation Materials: https://go.logically.com/hubfs/LogicON25/Session-PDFs/Born%20with%20a%20Bot%20-%20Educating%20the%20AI-Native%20Generation.pdf

Today's young professionals are growing up with AI as a default. What does that mean for leadership, learning, and security? This session explores how the next generation of IT and cybersecurity professionals approach knowledge, trust, and decision-making in an AI-saturated world. Attendees will leave with ideas for adapting training, mentorship, and talent development programs to this new AI-native mindset.

Learning Outcomes:

- Explore how AI is shaping the worldview of early-career professionals.
- Adapt leadership and learning to modern generational expectations.
- Anticipate future trends in recruitment and workforce evolution.

Notes:

Leading in the AI-Native Era

1. Reflection: How Is Your Organization Learning Today?

Use the prompts below to reflect on how AI is currently shaping your organization's approach to learning, decision-making, and operational efficiency.

- How are employees using AI to learn and solve problems in real time?

  _____

  _____

- Do we train for verification and critical thinking, or just tool usage?

  _____

  _____

- Who governs AI use internally, and do we have any current blind spots?

  _____

  _____

2. Checklist: Trust & Verification Readiness

Review your current practices and mark your level of maturity.

- ❑ We have a written AI acceptable use policy.
- ❑ Our teams are trained to verify AI-generated content before acting on it.
- ❑ We've seen or experienced hallucinations or overconfidence from AI outputs.
- ❑ We've identified where AI could impact cybersecurity or compliance.
- ❑ We reinforce critical thinking in all AI-augmented processes.

3. Leadership Action Framework

Use the table below to define how you will lead smarter in the AI-native era.

Leadership Action	What It Means	Your First Step
Normalize Verification Culture	Reward double-checking. Shift mindset from 'AI is always right' to 'AI is a first draft.'	
Rethink Training & Onboarding	Teach when to trust AI, when to slow down, and how to verify output.	
Build AI Fluency Into Strategy	Create governance and responsible AI use across all teams and functions.	

Cyber-First. Future Ready.

Who Are We

Logically is the trusted managed security and IT solutions partner for more than 3,000 organizations globally.

At Logically, we believe technology should empower—not endanger—your business. Since 1999, we've built our reputation on delivering cyber-first IT solutions that don't just keep systems running—they keep them resilient, responsive, and ready for growth. From multi-location healthcare organizations to fast-scaling retailers and financial institutions, Logically brings together deep technical expertise with a people-first mindset to secure your digital future.

Our Philosophy

We lead with security because trust is everything. Every system we touch is hardened against threats. Every solution we build is designed for longevity and performance. And every client relationship we build is rooted in accountability, transparency, and measurable results.

Our Core Values

- **Customer-Centric** — Service beyond expectation
- **Accountable** — Always own the outcome
- **Nimble** — Adapt fast, lead faster
- **Positive** — Optimism powers results
- **Relationship-Driven** — Trust is our currency
- **Do the Right Thing** — Even when it's hard

Snapshot of Success

- Founded: **1999**
- Employees: **350+** across the U.S
- Clients Served: **3,000+**
- Certifications: **650+**
- 24/7/365: **SOC & NOC Coverage**
- Global Support: **Yes**

> Logically focuses on your technology so you can take care of business. Fully Managed or Comanaged—Either Way, We've Got Your Back
>
> **Logically Team Ethos**

Awards & Recognition

Industry Awards

- GTIA North America Spotlight Awards - MSP/Solution Provider Award
- Sonicwall Enterprise Partner of the Year
- Cloudtango MSP Select
- CRN Solution Provider 500
- CRN Tech Elite 250
- CRN MSP 500
- Channel Futures MSP 500
- MSSP Alert Top 250 MSSPs

Innovation Awards

- The Communicator Awards - Emerging Tech - Best Immersive Game
- Channel Futures Digital Innovator of the Year Award
- Fortress Cybersecurity Award – SentryXDR 360

People Awards

- CRN's Women of the Channel Power 80
- CRN Women of the Channel
- CRN NextGen Leaders
- Women in Security Forum Power 100
- CompTIA Diversity in Leadership Award
- Comparably's Best Company for Women

Let's work together to protect what matters most.

Visit Logically.com | Call 866-946-9638

What We Do

Logically
CYBER FIRST. FUTURE READY.

Cyber-First Services That Let You Focus on Business, Not Back-End

Today's business environment demands more than just uptime—it demands uptime without compromise. That's why Logically delivers cyber-first IT services built for **resilience, compliance, and velocity**. Whether you need a fully managed solution or a partner to co-manage your stack, we bring clarity and confidence to even the most complex environments.

Service Overview

Each offering is built with security at its core and tailored to your organization's size, industry, and goals.

Cybersecurity Services

We don't layer on cybersecurity—we build with it.

- 24/7/365 SOC + NOC Coverage
- Managed Detection & Response (MDR + XDR)
- Vulnerability & Risk Assessments
- Penetration Testing
- Compliance & Cyber Insurance Support
- Endpoint Security, SIEM, Firewall & EDR

Cloud Solutions

Build flexibility and resilience in every environment.

- Public, Private, and Hybrid Cloud Management
- Cloud Migration & Architecture
- Cloud-Based Data Protection
- Disaster Recovery as a Service (DRaaS)
- Microsoft 365 & AWS Optimization

Data Center & Infrastructure

Optimize your IT backbone—secure, scalable, and reliable.

- Server & Storage Management
- Backup & Disaster Recovery
- Colocation Services
- Virtual Desktop Infrastructure (VDI)
- Performance & Security Assessments

Network Services

Smart, secure connectivity across locations and teams.

- LAN/WAN Design & Management
- SD-WAN & Load Balancing
- Wireless Design & Implementation
- Secure Remote Access
- NOC-as-a-Service (NOCaaS)

Collaboration & Communications

Unified, secure tools to empower hybrid and remote teams.

- UCaaS & VoIP
- Call Center & Help Desk Services
- Visual Collaboration Tools
- Mobile Device Management (MDM)
- Endpoint Monitoring & Support

Compliance Services

Reduce liability and meet your audit with confidence.

- HIPAA, PCI, SOX, CMMC, GDPR
- Risk Assessments & Gap Analysis
- Remediation Planning
- Cyber Insurance Readiness

LOGICON

Adapting IT & security for an AI-powered future.