BRANDED CONTENT

OCTOBER 27, 2025

CYBERSECURITY & Data Protection

A Roundtable Discussion

PERVEZ DELAWALLA
Founder and CEO
VegaNext

DAVID LAM
Partner, CISSP, CPP
Miller Kaplan

ALI MIRKARIMI
CEO
PM IT Services

GURJIT SINGH
Chief Information Officer
Prager Metis

In today's rapidly evolving digital landscape, cybersecurity is no longer just an IT concern—it's a critical business imperative. From ransomware attacks to data breaches and AI-driven threats, organizations of all sizes face unprecedented challenges in protecting their assets and reputations. This roundtable brings together leading local cybersecurity experts to discuss the latest trends shaping the industry, emerging threat vectors, and best practices for building resilient systems. Our panel generously share insights on proactive defense strategies, employee awareness, regulatory compliance, and how businesses can balance innovation with risk management in an increasingly complex cyber environment.

CYBERSECURITY & DATA PROTECTION ROUNDTABLE

What emerging cybersecurity threats should businesses be most concerned about heading into 2026?

DELAWALLA: There are several: #1) *AI-Powered Cyberattacks*. This is not just hype; it's a fundamental shift that will amplify existing threats and create new ones. #2) *Supply Chain & Third-Party Attacks*. Attacking a single, trusted vendor can compromise hundreds or thousands of their customers. This creates a massive attack surface that is difficult to manage. #3) *Advanced Phishing-as-a-Service (PhaaS) and Ransomware-as-a-Service (RaaS)*. Cybercrime has been professionalized. These platforms lower the barrier to entry, allowing less-skilled "affiliates" to launch sophisticated attacks in exchange for a cut of the profits. #4) *Weaponization of Legitimate Tools (Living-off-the-Land)*. Attackers are increasingly using built-in IT administration tools (like PowerShell, PsExec, and RMM software) and legitimate cloud services for their attacks. #5) *Critical Infrastructure Targeting*. Attacks on energy grids, water systems, transportation and healthcare are becoming more frequent and brazen. The motivation is often geopolitical disruption or large-scale extortion. #6) *The Quantum Computing Countdown*. While large-scale, cryptographically relevant quantum computers are still a few years away, the threat is already present. How Businesses Should Prepare: 1) Adopt a "Zero Trust" architecture; 2) prioritize security hygiene; 3) extend visibility and control; 4) develop an AI strategy; 5) begin post-quantum preparation; and 6) create and test incident response plans. In summary, the theme for 2026 is increased sophistication, scale, and systemic risk. Businesses must move beyond a reactive posture and build resilient, adaptive security programs that can withstand attacks targeting not just their own systems, but the entire ecosystem they operate in.

"Many businesses, especially small and mid-sized ones, make the critical mistake of assuming they're too small to be targeted."

– ALI MIRKARIMI

LAM: One of the most pressing threats heading into 2026 is the growing risk posed by third-party vendors and service providers. More often, cybercriminals are targeting external partners as an entry point into larger organizations — a tactic that bypasses stronger internal defenses. In 2025, we saw this play out with high-profile breaches at companies like Grubhub and Hertz, where attackers exploited vulnerabilities through third-party systems to access sensitive data. These incidents highlight a critical area many businesses overlook: third-party risk management. Ensuring vendors follow strong cybersecurity protocols while conducting ongoing vulnerability assessments are essential. If large, well-funded enterprises are falling short, it raises real concerns for small and midmarket companies, which often times lack the same level of security infrastructure.

What are the top three cybersecurity policies every business should have in place today?

SINGH: If a business could only start with three, I recommend those that address the human factor, the worst-case scenario, and the keys to the kingdom. A) *Identity and access management policy:* Think of this policy as a mandate to apply MFA or equivalent controls across all critical services. It also enforces the principle of least privilege access, ensuring that users only have the minimum permission necessary for their specific job. B) *Data backup and disaster recovery policy:* I call it the ultimate insurance against threats like ransomware and catastrophic/unplanned system failures. If you can quickly and reliably restore your data, a ransomware attack becomes a significant business interruption vs. a business-ending event. Also, it's critical to apply the 3-2-1 principle: have three copies of the data on two different media types, with one copy stored completely offline or in an immutable cloud backup. Don't forget to test your backups! C) *Lastly, an incident response plan:* Instead of treating this policy as a technical document (which it's not), make it a framework for business decision-making during a crisis. It will avoid panic and confusion, ensuring the response to an incident is organized and swift. Some elements of this response plan include those responsible for notifying legal, managing communications, and performing technical isolation. IAM stops the attack from starting, the Backup Policy ensures you survive the attack, and the Incident Response Plan ensures you manage the crisis effectively.

What are the most common mistakes businesses make regarding cybersecurity, and how can they avoid them?

MIRKARIMI: Many businesses, especially small and mid-sized ones, make the critical mistake of assuming they're too small to be targeted. Cybercriminals often prefer these organizations because they typically lack robust defenses. Another major vulnerability is the human factor: most breaches stem from phishing or user error. Without regular security awareness training, employees remain the weakest link. Weak passwords and the absence of multi-factor authentication (MFA) also leave systems exposed. Companies should enforce strong, unique passwords and enable MFA across all critical systems. Other common missteps include ignoring software updates, lacking a disaster recovery plan, and poor backup practices. Unpatched software is a goldmine for attackers, and without a tested incident response plan, breaches can cause chaos and costly downtime. Businesses often fail to monitor activity, underestimate third-party risks, and neglect network segmentation, allowing attackers to move freely once they are inside. Perhaps the most dangerous mindset is treating cybersecurity as a one-time project. Threats evolve daily, so security must be an ongoing program involving regular reviews, updates and training. By addressing these areas proactively, businesses can significantly reduce their exposure and build a resilient cybersecurity posture.

LAM: Not properly vetting your technology provider has become increasingly problematic. We are seeing more and more supply chain attacks coming through folks who have access to company systems based upon contractual relationships. We just saw in Verizon's 2025 Data Breach Investigations Report (DBIR) that almost a third of cyber breaches now involve third-party vendors or external platforms. Organizations need to (1) ensure strong guardrails are in place when relying on a third-party system, (2) review appropriate practices before aligning with the vendor and, most importantly, (3) ensure all parties are protected.

How is the rise of AI and machine learning shaping cybersecurity, both in terms of threats and defenses?

DELAWALLA: The rise of AI and ML is fundamentally reshaping the cybersecurity landscape, creating a powerful, automated arms race between attackers and defenders. Here's a breakdown of how it's shaping both threats and defense…AI/ML is empowering cyber (threats) in that attackers are leveraging AI to create more sophisticated, scalable and evasive attacks with: 1) hyper-realistic social engineering; 2) automated and adaptive malware; and 3) evasion of defense systems. On the defense side, AI/ML is fortifying cyber in that defenders are using AI to keep pace with the volume and sophistication of attacks, shifting from reactive to proactive and predictive security, utilizing: 1) threat detection and response; 2) vulnerability management; 3) fraud prevention; and 4) enhancing human analysts. With the emerging arms race and key challenges being faced, the impact of AI on cybersecurity is profound and dual-edged. The ultimate outcome in this new era will not be determined by who has the best AI, but by who can integrate AI most effectively into their strategy, learn and adapt the fastest, and maintain a skilled human workforce to guide

"We must remain ready to pivot to meet the needs of our patients who will continue to seek and demand care when and where they want it."

– GURJIT SINGH

MILLER KAPLAN

PROTECTING YOUR DATA IS CRITICAL

Your company has an obligation to protect its data and your clients are trusting you to get it right.

Our security experts help you safeguard sensitive information, reduce risk, and ensure compliance so you can stay secure, stay trusted, and stay focused on your business.

MILLERKAPLAN.COM
INFORMATION SECURITY & RISK ADVISORY SERVICES

CYBERSECURITY & DATA PROTECTION ROUNDTABLE

> One of the biggest financial risks that comes from cyberattacks is the downstream economic costs to business innovation."
>
> – DAVID LAM

and oversee the machines. The future of cybersecurity lies in a tight, synergistic partnership between human expertise and artificial intelligence.

How can businesses ensure their third-party vendors and partners comply with cybersecurity standards?

MIRKARIMI: Ensuring that third-party vendors and partners comply with cybersecurity standards is crucial for protecting sensitive data and maintaining a strong security posture. Businesses can start by conducting thorough due diligence before engaging with vendors, including assessing their security policies, practices, and history of breaches. Implementing contractual obligations that require vendors to adhere to specific cybersecurity standards and undergo regular security audits can help enforce compliance. Regularly monitoring and assessing the security practices of third-party vendors through audits, assessments, and continuous monitoring can identify potential risks and ensure ongoing compliance. Establishing clear communication channels and collaboration with vendors on security matters can also enhance the overall security posture. Additionally, businesses should require vendors to report any security incidents promptly and have a clear incident response plan in place. By taking these proactive measures, businesses can mitigate the risks associated with third-party vendors and ensure that their cybersecurity standards are consistently met.

SINGH: A check box is not simply enough. It is important to establish an internal rigorous vendor management program that determines the depth of security review. The vendor management platform should clearly list the Vendor's ability to access internal data and classify it with a risk score. For example, HIGH could mean PII/finance data, while LOW indicates general marketing information. A security questionnaire should be established to ask the vendor about their security controls, employee training, and patching procedures. It establishes a baseline of their security posture. Hold vendors that have access to sensitive data to high standards, ask them for their independent audits, such as a SOC 2 type 2 report. The report should cover all the criteria for trust services. However, it's equally important to bind vendors to your security standards legally. Should they experience an incident, they should immediately notify the clients where they have gateway access, if not within 24 hours. If you want to kick it up a notch, I encourage adding the right to audit — it allows you to verify their controls should a SOC2 or equivalent not be present. Compliance is not a one-time check; it must be monitored for the entire life of the contract.

What role does geopolitical instability play in the current cybersecurity landscape?

DELAWALLA: Geopolitical instability is not just a background factor in cybersecurity; it is a primary driver and amplifier of cyber threats. It has fundamentally reshaped the motivations, tactics, and targets of malicious cyber activity. Nation-states increasingly use cyber capabilities as a primary tool to achieve geopolitical goals without resorting to open kinetic warfare. This is often described as "hybrid warfare" or "gray zone conflict." Geopolitical conflicts often create a "proxy" environment in cyberspace. Instability directly changes who gets targeted and why. Geopolitical risks force nations and organizations to rethink their cybersecurity strategies. Some key examples linking geopolitics to cyberattacks include the Russia-Ukraine War. This is the most potent contemporary example. It has featured pre-invasion wiper malware (e.g., WhisperGate) to destabilize Ukrainian systems; sustained cyberattacks on critical infrastructure; global spillover with attacks like the Viasat KA-SAT incident, which disrupted internet service across Europe; and rise of volunteer "IT armies" on both sides. US-China tensions have also been characterized by: long-term intellectual property theft from American companies by Chinese state-sponsored groups and pre-positioning malware in critical infrastructure networks (as highlighted by the US FBI/CISA warnings about Volt Typhoon). Iranian and North Korean Activity are other examples. These nations use cyber operations for espionage, disruption and revenue generation (through ransomware and cryptocurrency theft) to counter international sanctions and pressure. In essence, geopolitical instability has weaponized cyberspace. It has transformed it from a domain of individual hackers and criminals into a theater for ongoing, state-level conflict. For any organization, understanding the geopolitical landscape is no longer a matter for policy experts alone; it is a crucial component of risk management and cybersecurity strategy. The firewalls of a business are now, in a very real sense, part of the new front lines of international conflict.

How has the increasing adoption of cloud services changed the approach to securing business data?

SINGH: This gets right to the heart of the modern security challenge. The fundamental shift is that the security perimeter has dissolved, and it's forcing us to stop relying on network location for trust. Traditional security focused on building a strong castle wall, securing the network itself with firewalls and VPNs. Once inside that wall, you were largely trusted. Now, with remote access, distributed resources, and an erosion of the corporate network boundary, that model is obsolete. The focus is on verifying the user, device, and application every time access is requested, regardless of their location. The new security perimeter resembles least privilege access and strong MFA controls. There's also confusion about where the cloud service provider's responsibility ends and where the customers begin; it is one of the leading causes of cloud data breaches, often due to misconfigurations. In a nutshell, the CSP (AWS or Azure) out of the box is responsible for the security of the cloud, so think of the Physical infrastructure, hardware, and global network. The customer is responsible for the security IN the cloud (data and configurations).

> Employee training is not just a "nice-to- have" IT policy; it is a fundamental layer of an organization's cybersecurity defense."
>
> – PERVEZ DELAWALLA

LAM: In today's AI- and SaaS-powered business environment, securing business data has become a two-fold challenge. While organizations are investing more time and resources into cloud platforms — which benefits both customers and end users — this shift also introduces new vulnerabilities, reshaping company strategies in securing business data. For instance, we've seen greater emphasis on Identity Access Management (IAM) and role-based access controls to minimize risk. As demand for cloud-based solutions continues to rise, we'll continue to see more focus on shared security responsibilities between the cloud service provider and the business along with the continuation of identity centered access.

Are small- and mid-sized businesses still the most vulnerable, or are attackers increasingly targeting larger enterprises and critical infrastructure?

MIRKARIMI: Cybercriminals actively target both small and large organizations, but for different reasons and with different tactics. Small and mid-sized businesses (SMBs) often believe they're too insignificant to be attacked. However, limited budgets, lack of dedicated security staff, and reliance on third-party tools make them easy prey. Attackers use automated tools to find vulnerabilities, and ransomware gangs frequently target SMBs, knowing they're more likely to pay quickly to restore operations. Studies show SMBs account for over 40–50% of

ransomware victims, with many unable to recover from major breaches. Large enterprises and critical infrastructure, on the other hand, are strategic targets. These organizations hold vast amounts of sensitive data and intellectual property, and their disruption can have a widespread societal impact. Sophisticated threats, such as Advanced Persistent Threats (APTs), supply chain attacks, and large-scale ransomware campaigns, are increasingly common. High-profile breaches, such as those involving SolarWinds, Colonial Pipeline, and MOVEit, illustrate the stakes. Attackers now divide their efforts: fast, opportunistic attacks against SMBs for quick wins, and stealthy, prolonged campaigns against enterprises for high-value gains. Ultimately, both groups are vulnerable. SMBs often serve as entry points into larger ecosystems, while enterprises are targeted for their data, influence, and financial resources.

How can businesses balance compliance with innovation in their cybersecurity strategies?

LAM: Ultimately, to balance compliance and innovation, any business — regardless of size — needs to make cybersecurity part of the early conversations as they build out their products and services. Cybersecurity investment should never be an afterthought. Unfortunately, it too often is. It's better to include cybersecurity expertise upfront because in the end it saves you money on both your tech stack and resolving information security issues later.

How can businesses test their readiness for potential cybersecurity incidents?

SINGH: Plain and simple, make sure the documented plan works under pressure. It's the same philosophy as a backup; it's only as good as a working backup. The starting point should be to identify critical assets in the organization, think about the applications you use, data storage points, and what happens

"The rise of AI and ML is fundamentally reshaping the cybersecurity landscape, creating a powerful, automated arms race between attackers and defenders."

– PERVEZ DELAWALLA

if they're suddenly not accessible/available? Craft a table-top exercise where a guided discussion takes place to walk through a hypothetical crisis scenario. I would say executive leadership needs to be involved, and a member or two from the IT/Security, legal, HR, communications, and finance teams. Once you have this documented, focus on building the plan.

What role does employee training play in preventing cyberattacks, and how can businesses improve it?

LAM: Humans remain the weakest link in any organization's cybersecurity program — which is why effective training is essential. Unfortunately, most training today is ineffective. Computer-based modules that lack interactivity or discussion often fail to make a lasting impact, leaving organizations vulnerable. A more effective approach is multipronged. Start with small, discussion-based training sessions of fewer than 10 people to encourage engagement. Follow up with phishing simulations tailored to your organization and provide one-on-one coaching for employees who click on malicious links to reinforce the risks. Finally, ensure leadership is involved — executives should hold individuals accountable when their actions lead to cybersecurity incidents. This hands-on, personalized method is the only way we've seen real, lasting behavior change.

MIRKARIMI: Employee training is a critical component in preventing cyberattacks, as human error is often the weakest link in cybersecurity. Many cyberattacks, such as phishing and social engineering, exploit the lack of awareness and training among employees. Regular security awareness training helps employees recognize and respond to potential threats, reducing the likelihood of successful attacks. Businesses can improve employee training by incorporating interactive and engaging methods, such as simulations and role-playing exercises, to reinforce learning. Additionally, creating a culture of cybersecurity within the organization, where employees understand the importance of their role in protecting company data, is essential. Providing ongoing training and updates on the latest threats and best practices ensures that employees stay informed and vigilant. Encouraging employees to report suspicious activities without fear of repercussions can also help with early detection and mitigation of threats. By investing in comprehensive and continuous employee training, businesses can significantly enhance their overall cybersecurity posture and reduce the risk of cyberattacks.

"Craft a table-top exercise where a guided discussion takes place to walk through a hypothetical crisis scenario."

– GURJIT SINGH

CYBERSECURITY & DATA PROTECTION ROUNDTABLE

"Cybercriminals actively target both small and large organizations, but for different reasons and with different tactics."

– ALI MIRKARIMI

DELAWALLA: Employee training is not just a "nice-to-have" IT policy; it is a fundamental layer of an organization's cybersecurity defense. Think of it as the "human firewall." While technology (firewalls, antivirus, intrusion detection) can stop automated and known threats, it is often powerless against attacks that exploit human psychology and error. Elements to consider: 1) *Mitigating the Human Factor:* The vast majority of security breaches (over 80-90% by some estimates) involve a human element, such as phishing, pretexting, or simple mistakes. Training directly targets this primary vulnerability. 2) *First Line of Defense Against Social Engineering:* Attacks like phishing, spear-phishing, and business email compromise (BEC) rely on tricking employees into revealing credentials, transferring money, or installing malware. A well-trained employee can recognize and report these attempts, stopping an attack before it starts. 3) *Promoting Secure Behaviors:* Training goes beyond attack recognition. It instills good "cyber hygiene" habits, such as: creating strong, unique passwords and using a password manager; enabling multi-factor authentication (MFA) wherever possible; recognizing and using secure networks (e.g., avoiding public Wi-Fi for work); and safely handling and disposing of sensitive data. 4) *Fostering a Security-Conscious Culture:* When training is continuous and supported by leadership, it creates a culture where security is everyone's responsibility. Employees become proactive, asking "is this safe?" rather than just following orders. 5) *Ensuring Regulatory Compliance:* Many industries (like healthcare, finance, and government) have strict data protection regulations (e.g., GDPR, HIPAA, CCPA). Training employees on how to handle data is often a mandatory requirement to avoid heavy fines and legal repercussions.

What should a comprehensive cyber incident response plan look like?

LAM: The first 24 hours after a cyber incident are critical. How the team initially responds and the actions that follow can dictate your organization's short-term recovery and long-term viability. When you are responding to something as complex as a cyber incident, a comprehensive response plan is simple and effective. Organizations should: have an incident playbook in place; define the response team's roles and responsibilities; and create a communication map and timeline that identifies when to contact cyber counsel, vendors and other stakeholders.

MIRKARIMI: A comprehensive cyber incident response plan is essential for minimizing damage and ensuring a swift recovery during a cyberattack. The plan should include several key components: preparation, detection, containment, eradication, recovery, and lessons learned. Preparation involves establishing a dedicated incident response team, defining roles and responsibilities, and conducting regular training and simulations. Detection focuses on identifying potential threats through continuous monitoring and alert systems. Containment aims to limit the spread of the attack by isolating affected systems and networks. Eradication involves removing the threat from the environment, such as deleting malware or closing vulnerabilities. Recovery focuses on restoring normal operations, including data restoration from backups and system repairs. Finally, the lessons learned phase involves analyzing the incident to identify weaknesses and improve future response efforts. Regularly updating and testing the incident response plan ensures that it remains effective and relevant. By having a well-defined and practiced incident response plan, businesses can minimize the impact of cyberattacks and recover more quickly.

What new technologies hold the most promise for improving cybersecurity in the near future?

SINGH: There are a few that focus on detection and response; however, I say for me, it's anything in the marketplace of Defensive AI and Behavioral Analytics. We've heard so many times that attackers are using AI to craft more convincing phishing emails and malware, and as a response, defensive teams/solutions are using AI and Machine learning to counter at scale. AI systems can learn what is "normal" network and user behavior (so, for example, how quickly someone types vs. a bot speeding through a large # of commands to login times, why is someone suddenly logging in at 3 am when the work hours are 9 to 5. If a system can automatically flag a compromised account because the user is suddenly accessing data they never touch or a machine is now running a script at an unusual time, I would like to be notified to begin isolation immediately. This is yet another layer of advanced intelligence that organizations can add to their repertoire for defense.

Are there any industries more vulnerable to cyberattacks currently, and why?

DELAWALLA: Several industries are currently more vulnerable to cyberattacks due to the nature of their data, their reliance on interconnected systems, and sometimes slower adoption of security measures. Here are some of the most targeted sectors: healthcare; financial services (banks, credit unions, insurance); critical infrastructure (energy, utilities, transportation); education (universities and K-12 schools); government and public sector; and small and medium-sized businesses (SMBs). Common vulnerabilities across these sectors includes: a) The Human Element: Phishing remains the #1 attack vector. A single employee clicking a malicious link can compromise an entire network; b) Supply Chain Attacks: Breaching one software vendor (like the SolarWinds attack) can give attackers access to all of its customers; and c) Rapid Digital Transformation: The shift to cloud services and remote work has expanded the attack surface faster than many organizations can secure it. In summary, the most vulnerable industries are those that possess highly valuable data, operate critical systems with real-world consequences, and have characteristics (like legacy tech or open networks) that make them easier to exploit.

How can small and medium-sized businesses implement robust cybersecurity measures on limited budgets?

MIRKARIMI: Small and mid-sized businesses can build robust cybersecurity defenses without the need for enterprise-level budgets by focusing on key areas. First, strengthen the "human firewall" through affordable training and phishing simulations. Most breaches begin with human error, so incorporating cybersecurity into company culture is essential. Updates are authentication using password managers and multi-factor authentication (MFA), particularly for critical systems such as email, finance, and HR. Keeping systems patched and updated is vital; automated updates and low-cost patch management tools can help close known vulnerabilities. Robust backups are another cornerstone of resilience. Follow the 3-2-1 rule (three copies, two media types, one offsite/offline) and test restore procedures regularly. Limit access using the principle of least privilege and segment networks to prevent lateral movement. Basic monitoring is achievable with the built-in tools in Microsoft 365 or Google Workspace. Affordable Endpoint Detection & Response (EDR) or Managed Detection & Response (MDR) solutions also offer 24/7 visibility. Establish clear policies and incident response plans to avoid chaos during breaches. Free or low-cost tools, such as Windows Defender, vulnerability scanners, and MFA apps, can cover many needs. By focusing on people, passwords, patching, and planning, SMBs can eliminate common attack vectors and build a resilient cybersecurity posture.

What are the biggest financial risks from cyberattacks—beyond immediate breach costs (e.g., reputational harm, regulatory fines, shareholder lawsuits)?

LAM: One of the biggest financial risks that comes from cyberattacks is the downstream economic costs to business innovation. Cyberattacks have long-term consequences that are hard to predict, especially for small and mid-sized businesses. While larger companies often can absorb the impact, smaller firms may not survive due to limited financial resources. SMBs are disproportionately impacted by cyberattacks, accounting for 43% of all total cybercrimes with an average cost of over two million dollars. Considering that small and midsize businesses represent nearly 46% of the U.S. workforce (about 59 million people) and are driven by entrepreneurs and innovators—cyberattacks on these businesses can put jobs, intellectual property, and future innovation at risk. Which can then lead to broader implications for the entire innovator economy—stifling entrepreneurship and slowing market competition. This is why it is essential that (all companies, but especially) SMBs should invest in cybersecurity from the beginning.

If you could give one piece of advice to organizations for the next 12–24 months to stay ahead of cyber threats, what would it be?

SINGH: I always tout education. The weakest link in the security chain, as we have all said, is human error. Cybersecurity training shouldn't be an annual exercise; it should be done at least quarterly, with shorter programs, and users need to be aware of sophisticated phishing attacks. Email is given; the trend has shifted to Microsoft Teams and other external chat-enabled applications. I would recommend hiring an ethical hacking organization to understand which systems are at risk, both externally and internally. It's amazing what these folks will discover that goes unnoticed. Think of your conference room and the technology it has. Even though the VOIP conference room unit is equipped with an IP address (typically on the same LAN as your endpoints), it still serves as another gateway into your network. On the other side of education are the tools that are in place. Don't be afraid to consider a change. Demo products in the marketplace may offer a competitive advantage over your existing tools and further diversify the security layers in your organization.

"The first 24 hours after a cyber incident are critical. How the team responds and the actions that follow can dictate your organization's short-term recovery and long- term viability."

– DAVID LAM