

CYBERSECURITY & Data Protection

A ROUNDTABLE DISCUSSION



POUYAN ESLAMI, PH.D.

Program Director, MS in Cybersecurity
and AI Governance;
Associate Professor of Information Systems
David Nazarian College of Business
and Economics, California State
University, Northridge

CSUN NAZARIAN
COLLEGE OF BUSINESS & ECONOMICS



**SANDEEP
KRISHNAMURTHY, PH.D.**

Dean, College of Business &
Singelyn Graduate School of Business
Cal Poly Pomona


**Cal Poly
Pomona**
College of Business
Administration
SINGELYN GRADUATE SCHOOL
OF BUSINESS



NICK MANCINI

President
The Tech Consultants

 **THE TECH
CONSULTANTS**



JASON THOMPSON

Advanced Security Specialist
Comcast Business

**COMCAST
BUSINESS**

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

What emerging cybersecurity threats should businesses be most concerned about in the next 12 months?

KRISHNAMURTHY: The dimensionality of cybersecurity is changing. It is not the specific types of threats (e.g., phishing, ransomware, data theft) that matter. Instead, it is that there is a broader orchestration that combines different types of threats in novel ways, leading to complex risks. Simply reciting a list of new threats is meaningless and serves to mislead, since what is new is that each type of threat is now multi-dimensional, AI-enabled, synchronized, and involves multiple actors.

ESLAMI: Three threats deserve the most attention. First, AI-enabled social engineering. Voice cloning and video deep-fakes now make a convincing call from the CEO achievable with a few minutes of public audio, and finance teams are the primary target. Second, attacks on the AI systems businesses are rapidly deploying. Prompt injection, poisoned data, and over-permissioned AI agents create paths into internal systems that most security teams have not yet mapped. Third, supply chain compromise. Attackers increasingly target the software vendors, managed service providers, and identity platforms many companies share, so one breach can cascade across hundreds of customers. Ransomware remains the costliest day-to-day threat, but it is increasingly delivered through these newer routes. The common thread is identity and trust. Verify people, verify software, and verify what your AI systems are allowed to do.

THOMPSON: It's the speed everything is moving at now. We analyzed 79.3 billion cybersecurity events this past year, and what stood out wasn't a brand-new threat, it was how automated and industrialized the old ones have become. Attackers are scanning constantly, around the clock, looking for any crack they can exploit, and the tools to do it are now rented through underground marketplaces instead of built from scratch. The common thread is scale. Attacks that used to take real skill and real time now take a few clicks and a few minutes, and businesses need to plan their defenses around that shift instead of the slower pace we used to expect. The old assumption that a security team had time to investigate before damage was done simply does not hold anymore, and that is the mindset shift businesses need to make heading into next year.

What is an overlooked cybersecurity improvement that can deliver significant value at relatively low cost?

MANCINI: Email authentication. SPF identifies authorized sending systems, DKIM adds a verifiable digital signature, and DMARC tells receiving systems how to handle messages that fail its authentication and domain-alignment checks. Publishing records is only the beginning. Identify legitimate sending services, review reports and move DMARC from monitoring to quarantine or rejection without disrupting business email. Have the sending provider verify reverse DNS, or PTR records, as well. These controls help reduce domain spoofing and support reliable delivery; they do not eliminate phishing. The value comes from correct configuration, clear ownership and ongoing maintenance—not just having records in place.



The dimensionality of cybersecurity is changing.

There is a broader orchestration that combines different types of threats in novel ways, leading to complex risks."

— SANDEEP KRISHNAMURTHY, PH.D.



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

KRISHNAMURTHY: Artificial Intelligence is rewriting the nature of cybersecurity for both the adversarial actor as well as the corporation with much to lose. For the corporate side, AI is now able to help with significant cybersecurity functions including enabling advanced threat detection, automation, and predictive analytics. Adversarial AI is now a reality that companies must contend with- the malicious actor is weaponizing AI to gain further advantage. Specifically, this includes allowing attackers to overcome or bypass security protocols, increased sophistication of cyber-attacks and corruption of organizational software and data. Given the dual nature of the impact of AI, on the one hand, we see that companies can use AI to improve threat detection while the sophistication of the attacks continues to rise.

MANCINI: Criminals can use AI to make impersonation more convincing, while employees can expose sensitive information through unapproved tools. Autonomous agents add another risk: they can take actions, not just produce answers. An agent with excessive access could be manipulated into sending data, changing records, or triggering transactions. Businesses should approve tools based on how they handle data, limit each agent's permissions, log its actions, and require human approval for consequential decisions. Every agent needs an accountable owner and a way to revoke access. Treat AI adoption as an access-control decision, not simply a software purchase.

THOMPSON: It's a two-way street, and that's really the story of this year's Comcast Business Cybersecurity Threat Report. On the attacker side, AI is compressing the time between a vulnerability being discovered and it getting exploited, sometimes before a patch even exists, and it is making phishing lures sharper and harder to spot. We are also seeing new angles like prompt injection and model poisoning that simply did not exist a few years ago. But it cuts both ways. Our own team is using AI assisted testing to find vulnerabilities in our own environment before anyone else does, and it has already turned up real findings we would not have caught otherwise. AI is raising the bar for attackers and defenders at the same time, and the businesses that win are the ones using it to move faster on defense too. To download the Cybersecurity Threat Report visit business.comcast.com.



A good incident response plan assumes something will eventually get through because it will."

— JASON THOMPSON

As AI becomes more integrated into business, what skills will future business leaders need to understand and manage cybersecurity and data protection risks?

ESLAMI: Future leaders will not need to write code, but they will need to ask better questions. Where does this model get its data? Who can change it? What happens when it is wrong, and how would we know? Three skills matter most. Risk literacy: the ability to tier AI and data systems by potential harm and allocate oversight accordingly. Accountability design: knowing how to assign ownership for systems that span vendors, cloud providers, and internal teams. And evidence-based judgment: the discipline to verify AI outputs before acting on them, especially when they are fluent and confident. Leaders who delegate too much to AI lose the expertise needed to supervise it. The strongest executives I see treat AI as a capable junior analyst, valuable but requiring review, and they invest in keeping their own judgment sharp.

How should organizations evaluate the cybersecurity practices of vendors, suppliers, and other third parties before giving them access to sensitive systems or data?

MANCINI: Evaluate vendors based on their access level and ask for evidence, not just assurances. Request evidence appropriate to the vendor's access and risk, such as a SOC 2 report or equivalent independent assessment, a penetration-test summary and documentation showing how significant findings were addressed. Review cyber insurance coverage separately.

Powering 90% of the Fortune 500—ready to power what's next.

Comcast Business delivers secure AI-backed networking in more than 100 countries, helping businesses stay connected, scale quickly, and grow with confidence. With cybersecurity solutions providing 24/7 threat hunting, businesses can stay ahead of emerging cyberthreats and rely on thousands of experts ready to respond at 2am like it's 2pm. It's no wonder Comcast Business is recognized as the fastest-growing enterprise provider, now powering over 90% of the Fortune 500.

When you add it all up, no one does business like Comcast Business.

Visit comcastbusiness.com to learn more.



COMCAST
BUSINESS

Fastest growing enterprise provider based on publicly disclosed revenue of leading providers from Q3'24 to Q3'25. © 2026 Comcast.

CYBERSECURITY & DATA PROTECTION



Businesses should approve tools based on how they handle data, limit each agent’s permissions, log its actions, and require human approval for consequential decisions.”

— NICK MANCINI

Put security obligations, incident notification expectations and exit arrangements in writing. Then ask the question most companies skip: Who has standing access to your systems? For many, the answer is their IT provider. Vet that partner hard- est. Ask how their technicians authenticate, whether access is logged, and how they would detect a compromise on their end. Outsourcing a service does not outsource management’s responsibility to understand and govern the risk.

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

KRISHNAMURTHY: Malicious nation states have long been a foundational element of cybersecurity. Whenever there is a physical war (e.g., Ukraine, Iran), there is an analogous rise in the cyber warfare with nation states seeking to maim, minimize or eliminate digital infrastructure- both in the public and private sector. With the rise of geopolitical instability, the number of fronts on which the war is waged tends to increase- it is not just about one state now, but a long list of malicious state actors. There is also collusion across states as well as the weaponization of AI to various extents. Add other factors to the geopolitical mix (e.g., violent regime change, economic collapse, political protests), and the chessboard grows even more complex.

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

THOMPSON: The data keeps pointing back to the same thing every year: basic hygiene gets overlooked. The over- whelming majority of what we detected traced back to phish- ing and drive by compromise, meaning someone clicked a link or approved something they should not have. That is not a sophisticated nation state problem, that is an employee read- ing email in a hurry. The fix isn’t complicated either. It starts with treating your people as your first line of defense rather than your weakest link and making sure reporting a suspicious email is a one click habit instead of a hassle. Patching on a consistent schedule matters just as much. None of this requires cutting edge technology, it requires discipline. The businesses that struggle most usually are not missing tools, they are miss- ing follow through on the fundamentals.

MANCINI: The biggest mistake is treating cybersecurity as a product you buy once instead of a process you run every day. Companies buy a firewall or antivirus software and consider the matter closed. Nobody is watching the alerts, verifying



Artificial Intelligence is rewriting the nature of cybersecurity for both the adversarial actor as well as the corporation with much to lose.”

— SANDEEP KRISHNAMURTHY, PH.D.

that backups actually restore, or removing accounts of employ- ees who left two years ago. The second is assuming someone else has the basics covered. Business owners assume their IT provider has security covered, while the actual agreement covers support, not ongoing security management. Nobody has made the gap explicit. Finally, making exceptions for leadership, such as owners and CFOs skipping multifactor authentication, creates unnecessary exposure. The people with the greatest financial authority should not receive the weakest security controls. The greatest exposure is not always a missing security product; it is an important control nobody is actually managing.

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

KRISHNAMURTHY: Industries must be ranked based on- 1) Proportionality- larger industries are more likely to be attacked, 2) Mission-criticality- if cybersecurity attacks can lead to large-scale economic damage, service outages or loss of human life, they will be prioritized, and, 3) Poor systems and training- enterprises whose employees are not well trained are more vulnerable.

ESLAMI: Healthcare, education, manufacturing, and pro- fessional services stand out, for different reasons. Healthcare holds highly sensitive data and cannot tolerate downtime, which makes ransom payments more likely. Education runs on thin budgets with open networks and large populations of transient users. Manufacturing has connected decades-old operational technology to the internet without built-in cyber- security. Professional services firms, including law and account- ing, hold their clients’ most valuable information while often operating with small IT teams. Across all of them, the shared vulnerability is a gap between how much the organization depends on technology and how much it invests in governing it. Attackers do not target industries so much as target weak controls at scale. Any organization with unpatched systems, weak identity management, and no rehearsed recovery plan is vulnerable, regardless of sector.

How can small and medium-sized businesses implement robust cybersecurity measures on limited budgets? Or are they less vulnerable because attackers are increasingly focused on larger enterprises and critical infrastructure?

MANCINI: Small and mid-sized businesses remain vulner- able. Being small is not a security control. Criminals look for opportunities such as weak credentials, exposed systems and outdated software; your company does not have to be a house- hold name to be a target. A 40-person law firm can receive the same phishing campaign as a Fortune 500 company. The dif- ference is what happens next. The larger company may have a dedicated security team; the smaller firm may have nobody watching, or an IT provider engaged only to fix what breaks. The important question is not whether your company is inter- esting enough to attack. It is whether someone is responsible for detecting an intrusion, responding and getting the business operating again.

What role should cybersecurity and data literacy play in business education, even for students who are not pursuing careers specifically in technology or cybersecurity?

ESLAMI: It should be foundational, the way financial literacy is. Every marketing manager handles customer data. Every operations leader depends on systems that can be disrupted. Every finance professional is a target for business email com- promise. Treating cybersecurity as a specialist topic leaves most future decision-makers unprepared for the risks they will face on their first day of work. Business schools should teach every student how data moves through an organization, what obli- gations attach to it, how attacks typically unfold, and how to recognize when an AI tool is being trusted beyond its reliabili- ty. This does not require technical depth. It requires a mindset: data is an asset with liabilities attached, and protecting it is part of running a business well. Graduates who carry that mindset

into any function make their organizations safer.

What should a comprehensive cyber incident response plan look like?

THOMPSON: A good incident response plan assumes something will eventually get through because it will. It needs three things working together: continuous monitoring that does not rely only on known bad signatures, a team that can quickly confirm what is actually happening rather than just reacting to an alert, and the authority to contain it imme- diately instead of escalating through layers of approval. One of our Comcast Business case studies shows this in practice. One of our managed security customers had a compromised software package pull malicious code onto an employee’s machine through a routine update. Our SOC caught the unusual behavior, matched it to a known attack pattern, and quarantined the machine before it spread further. That is the model working as intended. Speed and clear ownership are what separate a contained incident from a headline.



AI-driven detection and response can investigate alerts and contain threats faster than human teams, which matters most for organizations that cannot staff around the clock.”

— POUYAN ESLAMI, PH.D.

For small and mid-sized businesses with limited budgets and IT resources, where should cybersecurity investment be prioritized first?

MANCINI: Start with the controls that prevent compromise and limit the damage when prevention fails: (a) Multifactor Authentication (MFA) -- Require MFA wherever supported, prioritize phishing-resistant methods, and make no exceptions for executives; (b) Endpoint Protection -- Deploy modern endpoint protection backed by 24/7 monitoring and response. An unread alert is worthless; (c) Protected Backups – Main- tain backups separated from your network that are protected from deletion and regularly tested by performing actual restores; (d) Managed Email Authentication – Properly con- figure SPF, DKIM, and DMARC, with DMARC enforcement, to help reduce spoofing of your domain; and (e) Patching and Updates -- Promptly address exploited vulnerabilities and keep supported systems updated. Do not spend the entire budget on software licenses while leaving nothing for implementation, monitoring, or maintenance. A smaller set of well-run controls is far more effective than a large collection nobody manages.

How can businesses recover quickly and minimize damage after a cybersecurity breach?

THOMPSON: Recovery speed comes down to how fast you can detect and isolate the problem before it spreads. One of the cases in our report involved an attacker who got into a network using stolen VPN credentials on a Friday evening, then started moving laterally and pulling more credentials, activity that typically precedes a ransomware deployment. Our SOC caught that behavior in progress and shut it down before encryption ever started, stopping what could have been a companywide shutdown right before the weekend. That is the difference detection speed makes. On the flip side, our data shows supply chain compromises take an average of 258 days to identify and contain when that visibility is not in place, which is an enor- mous window for damage to spread. Recovery is not a separate



THE TECH
CONSULTANTS

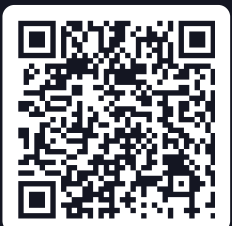
20

YEARS
keeping
businesses safe.

MORE THAN CYBERSECURITY
WE'RE YOUR COMPLETE I.T. PARTNER.



Google rating
5.0 ★★★★★



Talk to an Expert

Peace of mind is closer than you think.

(818) 225-5000 · info@ttcmssp.com · ttcmssp.com



SERVING L.A. COUNTY SINCE 2006

CYBERSECURITY & DATA PROTECTION

phase from prevention; it is what happens when detection and containment work the way they are supposed to.

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

ESLAMI: My research on AI governance and software delivery suggests the tension between compliance and innovation is largely a design problem. Organizations that bolt governance on at the end of a project experience it as friction. Organizations that build it into their pipelines experience it as speed, because teams stop waiting for late-stage approvals. Practically, that means automated security checks in development, model and data documentation generated as part of normal work, and risk tiers that reserve heavy review for high-impact systems. Frameworks such as the NIST Cybersecurity Framework and the NIST AI Risk Management Framework are flexible enough to support this. Compliance becomes a floor rather than a ceiling. The companies that innovate fastest with AI



The strongest executives I see treat AI as a capable junior analyst, valuable but requiring review, and they invest in keeping their own judgment sharp."

— POUYAN ESLAMI, PH.D.

are usually the ones whose guardrails are clear enough that people can move confidently within them.

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

ESLAMI: Several technologies are maturing at the right time. AI-driven detection and response can investigate alerts and contain threats faster than human teams, which matters most for organizations that cannot staff around the clock. Passwordless authentication using passkeys removes the credential that attackers steal most often. Zero-trust architectures, which verify every request rather than trusting the network, are finally practical for mid-sized companies through cloud identity platforms. Post-quantum cryptography is moving from research to deployment, and organizations with long-lived sensitive data should begin planning migration now. Confidential computing and privacy-preserving techniques let organizations analyze data without exposing it. My caution is that none of these replace governance. A powerful detection tool with no one assigned to act on its findings improves nothing. Technology multiplies the effect of good management; it cannot substitute for it.

THOMPSON: Orchestration is the shift that matters most right now, not any single point solution. Our Threat Report points to bringing network, endpoint, and identity signals together as the biggest lever businesses have, because attackers today chain several small techniques together rather than relying on one big exploit. Behavioral detection is becoming essential too, since attackers are good at disguising themselves as legitimate traffic, which means static blocklists alone miss them. Visibility that does not stop at the perimeter is the common denominator across all of it.



Recovery speed comes down to how fast you can detect and isolate the problem before it spreads."

— JASON THOMPSON

How should executives and boards evaluate cybersecurity risk, and what questions should they be asking their technology and security leaders?

MANCINI: Stop asking "Are we secure?" as though security were a yes-or-no condition. Ask what could fail, what has been tested and which risks remain. Executives should ask questions that connect security work to operational performance: (a) Which of our accounts do not have multifactor authentication, and why? (b) When did we last restore from backup, and how long did it take? (c) Who owns unresolved risks, and who has administrator access? (d) Does what we actually do match what we told our cyber insurance carrier? Require leaders to "show the work"—produce backup reports, patch logs, and recovery test results. Management does not need to configure every control, but it must make risk decisions deliberately rather than relying on a feeling.

How do you see the role of cybersecurity evolving as businesses continue to digitize?



College of Business Administration
SINGELYN GRADUATE SCHOOL OF BUSINESS



BECOME A LEADER AT
SOCAL'S POLYTECHNIC
BUSINESS SCHOOL

High-quality, affordable education
Designed for working professionals

Master's Degrees: Accountancy, Business Administration (MBA),
Business Analytics, Digital Marketing, Digital Supply Chain
Management, Human Resources Leadership, Information Security,
Financial Analytics



NO. 2

Top Public University in the West
U.S. News & World Report

TOP 5

MBA Program
Los Angeles Business Journal



Become By Doing
at Cal Poly Pomona

Learn more:
cpp.edu/business

CYBERSECURITY & DATA PROTECTION

ESLAMI: Cybersecurity is moving from a technical function to a core management discipline, as financial control did a century ago. As every product, process, and customer relationship becomes digital, security decisions are business decisions about trust, continuity, and reputation. Boards are being held accountable, regulators expect named owners, and customers choose partners partly on their security posture. The arrival of AI accelerates this. Companies are now deploying systems that make decisions, act, and learn from data, so security must extend beyond protecting information to governing machine behavior. I expect the chief information security officer role to converge with risk, privacy, and AI governance into a single accountability for digital trust. The organizations that thrive will treat security as an enabler of digital strategy rather than a cost of doing business.

How should companies manage the cybersecurity risks created by employees using AI tools, cloud applications, and other technologies outside of approved IT environments?

MANCINI: Start by accepting that it is already happening. Your people are pasting contracts, client data, and financials into free AI tools because those tools are useful and nobody gave them a sanctioned option. A ban alone is not a strategy. Give employees an approved tool with appropriate data-protection terms and administrative controls. Write a short, plain-English policy defining what can and cannot go into it, and turn on the controls that enforce it. Use appropriately licensed and configured controls to restrict unapproved applications and detect sensitive-data sharing. Policy without enforcement is a suggestion; enforcement without a usable alternative invites workarounds.

How should universities and businesses work together to prepare the next generation of professionals for an increasingly complex cybersecurity landscape?

ESLAMI: The talent gap in cybersecurity is partly a translation gap. Businesses need people who understand both the technology and the organizational context in which risk decisions are made. Universities can produce them only if industry is in the room. At California State University, Northridge, we designed our new MS in Cybersecurity and AI Governance in conversation with practitioners, and we deliberately opened it to students without technical backgrounds. Companies can help in three ways. Share real, anonymized problems for capstone projects. Offer practitioners as guest instructors and mentors. Hire for aptitude and governance literacy, not just certifications. In return, universities should keep curricula current, teach frameworks that employers actually use, and emphasize communication and ethical reasoning alongside technical skill. The next generation will manage AI systems and human teams at once. Preparing them is a shared responsibility.

What advice would you give to businesses looking to future-proof their cybersecurity strategy?

THOMPSON: Stop thinking about this as a perimeter problem. The businesses best positioned treat identity as the real control plane, verifying continuously rather than just at login, because attackers today are logging in with stolen credentials far more often than they are breaking through a firewall. Pair that with behavioral threat hunting instead of relying only on known bad indicators, since so much of what we see today is designed to look like normal business activity. Take stock of what AI tools and integrations are running in your environ-

ment, because you cannot secure what you do not know exists. And build in the assumption that some attacks will get through so your team is just as focused on containment as prevention. The businesses that treat this as a continuous program are the ones still standing when the next wave hits.

KRISHNAMURTHY: Work with universities that emphasize experiential learning rather than textbook assignments. At Cal Poly Pomona's College of Business Administration, we offer world-class cybersecurity programs that prepare our students to compete in nationally ranked competitions at the highest levels. Students are required to operate a Security Operations Center (SOC) and student-run data center. We also host the National Security Agency's (NSA) Center for Academic Excellence along with a vital set of corporate partnerships. The master's degree in information security at the Singelyn Graduate School of Business is taught by exceptional faculty and is aligned with nationally recognized standards. We are preparing students to excel in ways that only doing can enable. Partner with us to create the talent pool that will take on the challenges of cybersecurity.



Criminals look for opportunities such as weak credentials, exposed systems and outdated software; your company does not have to be a household name to be a target."

— NICK MANCINI

Master of Science in Cybersecurity and AI Governance



Prepare for one of today's fastest-growing fields with Nazarian College's new Master of Science in Cybersecurity and AI Governance. Applications now open for the inaugural 2027 Fall cohort. Scan to learn more and apply.

CSUN NAZARIAN
COLLEGE OF BUSINESS & ECONOMICS