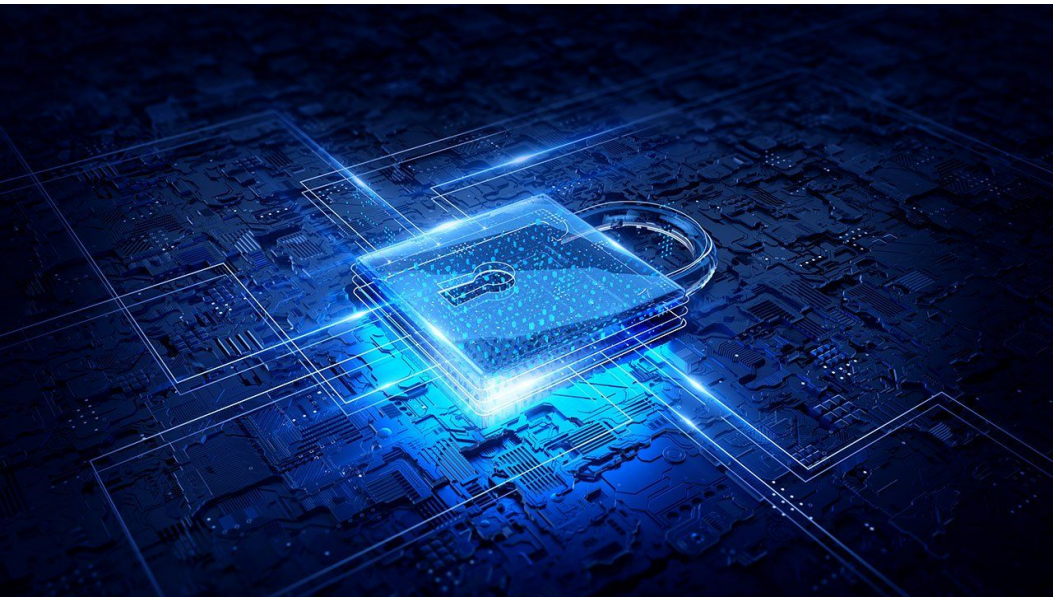
AUSTIN FORUM

ON TECHNOLOGY & SOCIETY



Cybersecurity 2025: Risks & Strategies

February 4, 2025

Welcome to the

Austin Forum on Technology & Society!

We cover emerging, disruptive, and pervasive technologies to help you understand how these technologies will influence and impact society,

and how you can be a positive contributor to that!

Welcome to the
Austin Forum on Technology & Society!

Jay Boisseau

Austin Forum Executive Director & Founder
(and Vizias CEO, Austin AI Alliance Founder & board member)

email: jay@austinforum.org

Welcome to ACC Rio Grande!

Bryan Port

Director

Center for Government & Civic Service

Austin Community College

bryan.port@austincc.edu

We have **6** ways to learn, share, connect!

Live monthly events	Online content
Presentation + Networking events • Expert presenter-focused • In-person and online—hybrid • Recording and slides posted online	**Workshops** • Offered by Austin Forum partners and friends • Free, or with special discounts for AF attendees • Designed to accelerate technical understanding, expertise
Meetup discussion events • Participatory for everyone • In-person ***only*** • Never recorded—speak freely!	**Slack Community, Website, Newsletter** • Get updates and register for events • Learn more about the Austin Forum • Ask questions, share, etc. (Slack)
Book discussion events • Participatory for everyone • Online ***only*** • Never recorded—speak freely!	**Podcasts: Austin Forum Upload (hiatus)** • Audio only • Conversation formats • Hosted in all major podcast stores, AF website

Our Partners Make Austin Forum Possible!

AMD

arm

SXSW

GOOD SYSTEMS
A UT Grand Challenge

The University of Texas at Austin
McCombs School of Business
MASTER OF SCIENCE IN TECHNOLOGY COMMERCIALIZATION

Please contact us if you want to become an annual partner!

Welcome, Abilitie and Bjorn Billhardt!

abilitie

THE 12-WEEK MBA

BJORN BILLHARDT & NATHAN KRACKLAUER

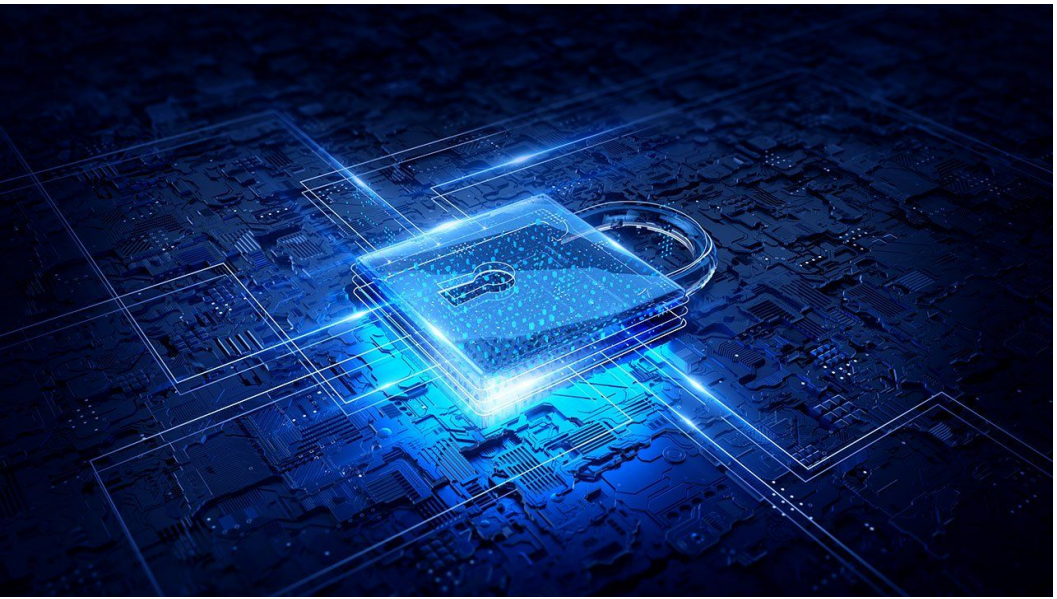
Before we get started, join our slack

1. Go to: www.austinforum.org/slack
2. Click “Join the Austin Forum Slack Workspace”
3. Enter your email address
4. Check your email to confirm Slack invitation
5. Enter your name and click “Create Account”
6. You’re in! You can use the Slack mobile app now, too.
7. Add channels to your view using **+ Add channels.**
   Make sure to add the #event-questions channel!

And now, our featured presentation…

Please:

- ✔ ***Respect our speakers & audience***
- ✔ ***Ask questions*** in the AF Slack in the **#event-questions** channel. The question of the night will win a SXSW 2025 badge! (must be present to win)
- ✔ ***Learn, think, and enjoy!***



Cybersecurity 2025: Risks & Strategies

February 4, 2025

Cybersecurity 2025: Risks & Strategies

Tod Beardsley
Hacker Dilettante
todb@packetfu.com

Robert “RSnake” Hansen
Managing Director
rsnake@rsnake.com

Anastasia Uglova
Specialist Leader
Cyber & Strategic Risk
auglova@deloitte.com

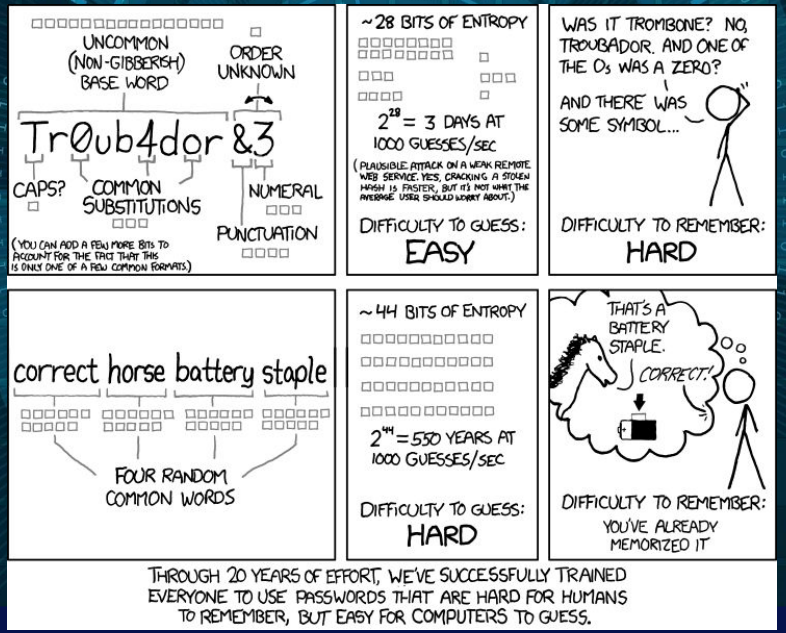
It's the Basics

There are lots and lots and LOTS of things you can do to secure yourself, your enterprise, and your life.

And yet, the vast majority of successful compromises boil down to failing at one of three things. Sometimes two of three things. Rarely, four of three things.

#1: Complex, Unique Passwords

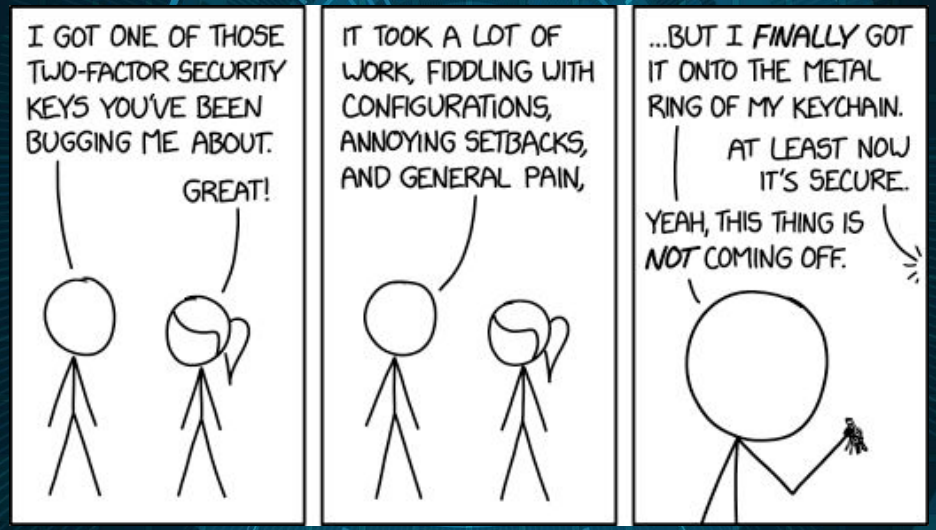
1) Pick a password manager
2) Use the password manager
3) Multi-platform & IT-managed
4) All eggs in one basket



XKCD: https://xkcd.com/936/

#2: Multi-Factor Auth (MFA)

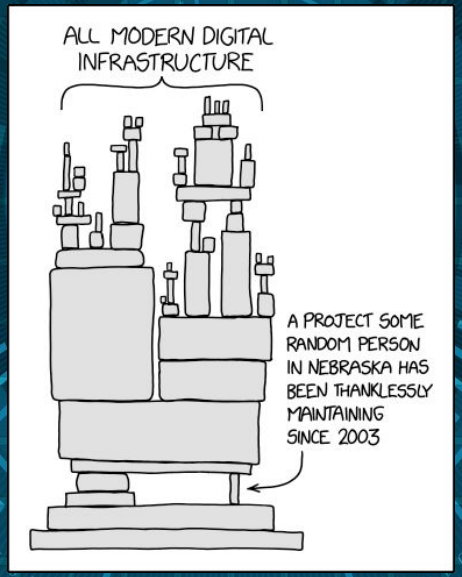
1) All MFA is better than no MFA
2) Even SMS-based MFA
3) TOTP is much, much better
4) FIDO2/PKI is even better, but...



XKCD: https://xkcd.com/2522/

#3: Keep Up On Patches

1) It's harder than it sounds
2) Regular maintenance windows
3) Actually, it's asset management
4) Prefer honest vendors/suppliers



XKCD: https://xkcd.com/2347/

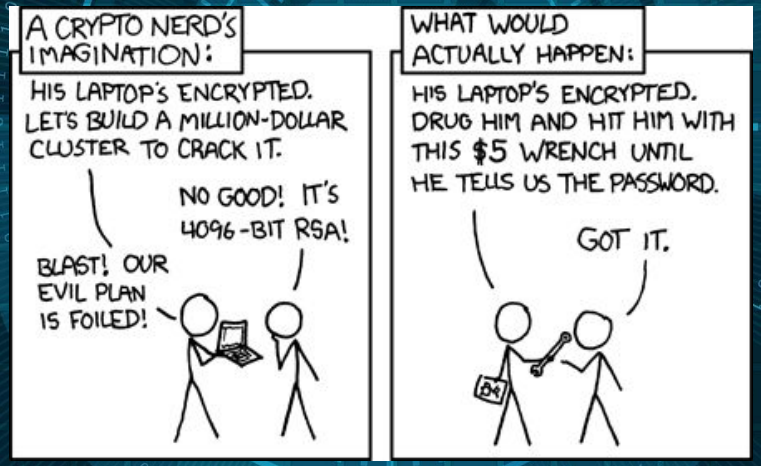
#4 - #512: Everything Else

1) Good enough is good enough.

2) 0days happen. Expect them.

3) Actually, it's log management

4) Practice DR, IDR



XKCD: https://xkcd.com/538/

Would You Like to Know More?

https://cisa.gov/KEV *(almost the shortest URL in CISA!)*

https://cisa.gov/secure-our-world/use-strong-passwords

https://cisa.gov/resources-tools/resources/multi-factor-authentication-mfa

This talk was not produced, edited, managed, nor approved by CISA.

I just like the agency.

qr.link/ovgsDL

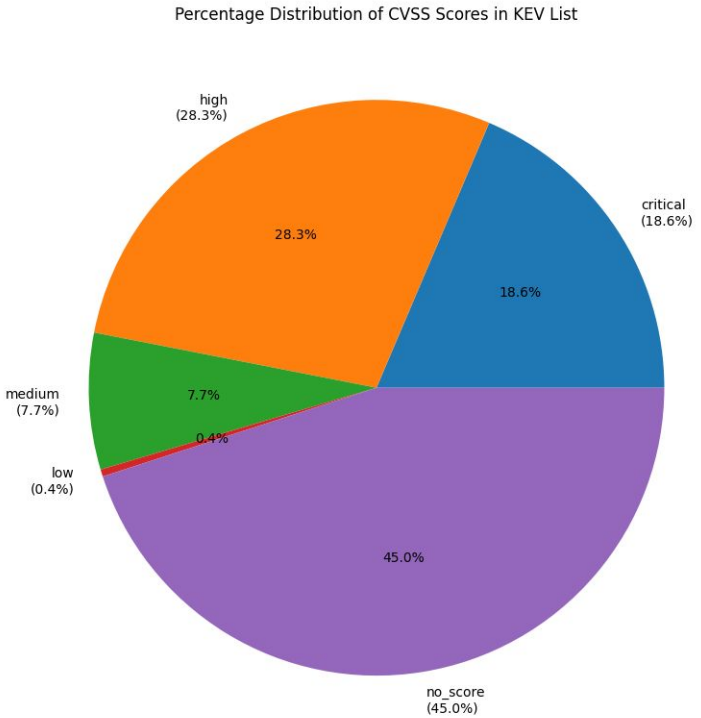
The Current Situation

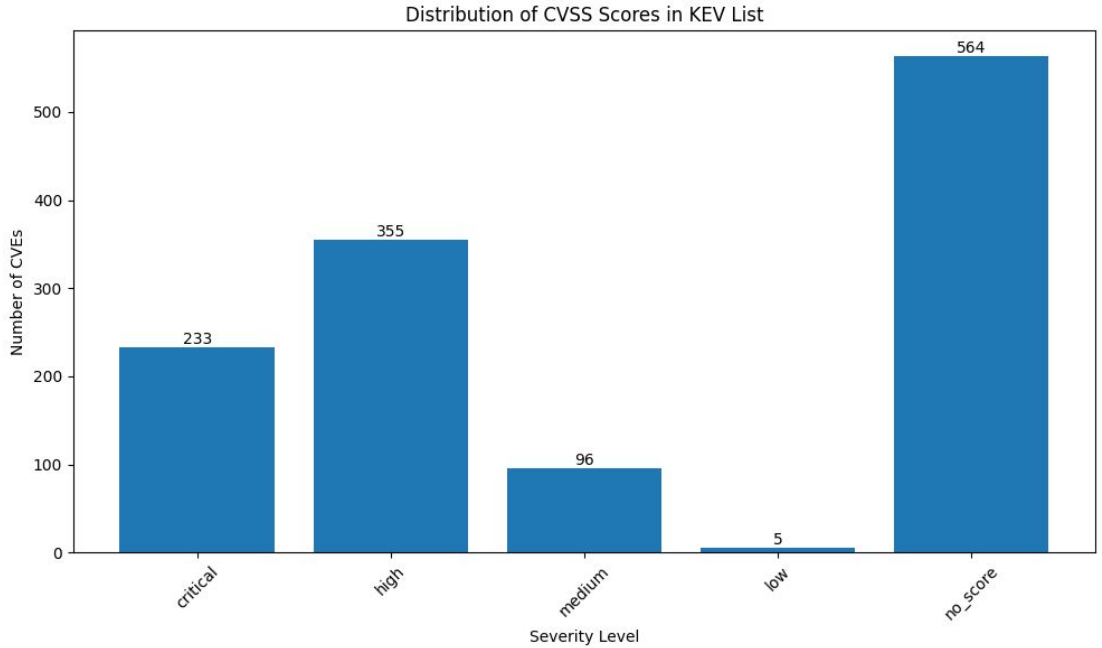
- Orgs *don't want* to scan everything because it's expensive and noisy.
- Orgs end up doing *manual prioritizing* which makes every company unique in a bad way.
- Orgs *waste untold amount of time/money* searching for and fixing the wrong issues.
- *CISOs do not understand and cannot explain the cost/benefit* to the board/CFO.

State of CVE and KEV at a Glance

Total CVEs (as of today): 280,049

- Scored CVEs: 85,834 (30.65%)
- Unscored CVEs: 194,215 (69.35%)
- Out of 280k CVEs only 0.45% make it on KEV.
  - 99.55% of CVEs don't currently matter according to KEV.
- Of the CVE 9.0 or greater, only 2.96% matter.
  - 97.04% of vulns 9.0 or greater don't currently matter according to KEV.





Only 18% of KEV are critical, most don’t even have a CVSS score

It’s Time We Start Addressing ROSI

- A CVSS of 9.0 or greater does not mean it’s actually exploitable in your environment, and it definitely doesn’t mean it will lead to loss. The insurance companies are getting wise to this.
- A CVSS of 10 is not 10x worse than a CVSS of 1.
- Prioritization doesn’t address ROSI. At all.
- Better things do exist like vulncheck and EPSS, but they still aren’t great, IMHO (for another talk). But overall, the security community has done an awful job of fixing this issue and finding common ground with the CFO.

Key themes for 2025

1. Emphasis: **Secure AI** ⬆️ **Trustworthy AI** ⬇️

   Proactive measures ⬆️ **Passive** compliance ⬇️

2. **Cyber**security 🤝 **physical** security
3. **Dual-use tech:** more AI capabilities = **more risk surface**
4. Agentic AI + Systems of Systems = **more complexity**
5. Secure AI talent gap. I've got news for you: There's work for you in AI! You are **NOT OBSOLETE!**

Secure AI ⬆️ **Trustworthy** AI ⬇️

Proactive measures ⬆️ **Passive** compliance ⬇️

Key Regulatory Shift

🆕 EO 14179: Removing Barriers to American Leadership in AI

Previous

❌ EO 14110: Safe, Secure, and Trustworthy Development and Use of AI

✅ EO 14144: Strengthening and Promoting Innovation in the Nation's Cybersecurity

✅ EO 14141: Advancing U.S. Leadership in AI Infrastructure

Implications

- Cyber teams take center stage in business strategy and risk mitigation
- Agencies moving from a framework-driven approach to proactive measures to safeguard national security, data integrity, and public trust

Key takeaway:

In 2025, cybersecurity **shifts waaaaay to the left**.

Cybersecurity 🤝 physical security

- **AI** + compute **infra** ($500B Stargate Project) + reopening **Small Modular Reactors** (Big Tech investing in small nuclear) + **physical OT**
  - Cyber no longer confined to software and networks – now: hardware / chips, data centers, OT, IoT, smart cities, energy grids
  - More focus on physical chips, verifiable compute, TEEs, etc.
- **Tradeoffs of more efficient chips and cheaper models**…
  - Reduced redundancy in chip functions?
  - Skipping security layers (less encryption to save on compute?
  - Supply chain risks from custom chip production
  - Smaller models leading to potential backdoors
- **Rapid digitization of legacy systems** (Fortran, for real)


The New York Times

Hungry for Energy, Amazon, Google and Microsoft Turn to Nuclear Power

Large technology companies are investing billions of dollars in nuclear energy as an emissions-free source of electricity for artificial intelligence and other businesses.


The Telegraph

Google buys world's first private mini-nuclear reactors


WIRED SECURITY POLITICS GEAR THE BIG STORY BUSINESS SCIENCE CULTURE IDEAS MERCH SIGN IN | SUBSCRIBE

BY MATT REYNOLDS BUSINESS SEP 24, 2024 1:26 PM

The AI Boom Is Raising Hopes of a Nuclear Comeback

Microsoft's deal to bring back a Three Mile Island nuclear reactor is just one part of Big Tech's quid pro quo with nuclear power.

1 Cybersecurity 🤝 physical security

Tradeoffs of compute optimization: Squeezing more performance out of chips = vulnerabilities at hardware / firmware level

➡️ Fancy things like dynamic resource allocation and overclocking can mean:

- Reduced redundancy in chip functions, making systems less resilient
- Skipping security layers (deprioritizing encryption to save compute power)
- Supply chain risks from custom efficient chip production (not NVIDIA, say) and smaller, cheaper models, increasing potential backdoors

➡️ Security teams have to protect digital ecosystems against highly capable AI that requires far fewer resources

➡️ More focus on physical chips, verifiable compute, TEEs, etc.

2 Cybersecurity 🤝 physical security

Data center security and AI infrastructure expansion (Stargate, Small Modular Reactors)

➡️ Insider threats, unauthorized access, and state-sponsored attack

➡️ Complexity of infra supply chains: hardware, software, and vendor dependencies

➡️ Data center resilience depends on multi-layered security: access control, real-time monitoring, and threat intel

3 Cybersecurity 🤝 physical security

Legacy systems in modern solutions

- Integrating outdated systems = exposure to cyber threats and interop issues
- Legacy infra lacks built-in security measures to handle AI-driven automation securely

Need more energy, more compute, more BUILDINGS

- AI-managed energy grids and nuclear reactors are new attack surfaces for adversaries

Interconnected OT / IoT / Smart Cities

- Exposure to data interception, manipulation, cascade failures
- Standardized security frameworks are needed but lacking

Complexity of data types makes cybersecurity really hard!

- Processing diverse data sources = risks of data poisoning + integrity breaches
- Cross-system data exchange between AI, IoT, and industrial networks creates new attack vectors

Dual-use tech: New capabilities always introduce new risks – when we have something shiny, adversaries have it, too!

Zero-trust: assume breach, trust nothing, verify everything

- Component authentication to protect interaction with AI models, APIs, and data pipelines
- Least privilege access to training data, inference, components based on role and necessity
- Dynamic access control to adjust real-time permissions based on risk assessments and anomalous behavior

Mitigation strategies

- Proactive threat intel to continuously monitor for emerging risks
- AI-specific security to protect the parts of the tech stack not covered in “trad cyber”
- Microsegmentation to divide systems into smaller zones to limit blast radius

Agentic AI + Systems of Systems = **more complexity**

- The rise autonomous systems capable of making decisions and taking actions without direct human oversight complicates security: **keep HITL & carry on!**
- Agentic AI can self-modify, communicate, and execute tasks autonomously
- Concerns about:
  - hijacking, excessive agency, and unintended escalation of actions
  - interconnected systems and networks vulnerable to adversarial manipulation, model poisoning, and prompt injection attacks
  - **more connection points** (APIs, data flows, protocols) can cause **cascade failures**
  - **unpredictable behavior in complex environments** with heterogeneous data sources make containment difficult
  - lack of explainability complicates incident response

Cybersecurity Talent Gap

WEF cybersecurity outlook

- Since 2024, the cyber skills gap has increased by 8%
- 67% of orgs report moderate-to-critical skills gaps
- Only 14% of orgs are confident that they have the people and skills they need today

Turn that frown upside down!

- **Multidisciplinary teams**
  - Integrate AI expertise with cybersecurity knowledge to build robust defenses
  - AI security not just about software – it's hardware, procurement, supply chain…
- **Investment in workforce training**
  - Red teaming, resilience testing, and secure AI development are essential
  - Upskilling and AI-focused security education key to continuous adaptation

Recommendations for 2025

1. To understand cyber in 2025, learn about the differences between **cyber AI vs. traditional cybersecurity** – they are many!
2. Get smart on Operational Technology
3. Get smart on dual-use tech: for 2 hours on ChatGPT, spend 2 minutes studying the OWASP Top 10 for LLMs
4. Be the Zero Trust Hero!
5. **Cybersecurity in 2025 is no longer hackers in hoodies**. It's supply chain analysts, procurement specialists, and the ENTIRE CROSS-FUNCTIONAL TEAM! **To wit: it's YOU!**

Resources

1 First of all, me and my Secure AI team at Deloitte and are a resource: **auglova@deloitte.com**

AI Governance Alliance

2 WORLD ECONOMIC FORUM

In collaboration with the Global Cyber Security Capacity Centre, University of Oxford

Transformation of Industries in the Age of AI

Artificial Intelligence and Cybersecurity: Balancing Risks and Rewards

WHITE PAPER

JANUARY 2025

www.weforum.org/publications

Open Web Application Security Project is the wasp's knees!

genai.owasp.org

3

Q&A for Cybersecurity 2025: Risks & Strategies

Bjorn Billhardt
CEO, Abilitie
bjorn@abilitie.com

Tod Beardsley
todb@packetfu.com

Robert “RSnake” Hansen
rsnake@rsnake.com

Anastasia Uglova
auglova@deloitte.com

What was the most important/interesting thing you learned tonight? (30 sec)

1 2 3 4 5 6 7 8 9 10

11 12 13 14 15 16 17 18 19 20

21 22 23 24 25 26 27 28 29

Join Us for More Great!

Upcoming **presentation** topics include:

- Future of Human Workers
- AI
- Gaming tech
- Neurotech
- Quantum computing
- Sustainability tech
- More AI
- and much more!!!

Plus:

- In-person **meetups** & **workshops**
- Online **book discussions**
- **Podcasts**

Donate Your Unused Tech

- If you have computers, tablets, or smartphones no longer being used, please help those in need
- Bring your devices to any in-person event, and we'll donate to our worthy charities!

Be an Austin Forum Friend—or Champion!

BE A ***CHAMPION*** OF THE FORUM!

www.austinforum.org/support

Champions help us program and provide great educational programming and informative experts ($1000+)

- Offer advice on programming topics, invited speakers, podcasts & events
- Attend the annual meeting & VIP reception
- Get a nice tax deduction!
- Get cool AF swag
- 100% of your gift goes to executing the Forum

BE A ***FRIEND*** OF THE FORUM!

Or be a Friend of the Forum—*forever*! ($100+)

- Get cool AF swag
- Get a tax deduction!
- 100% of your gift goes to executing the Forum
- Listed on our Friends page *forever*!

Join us to learn, share, discuss!!

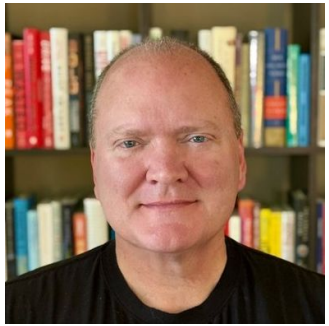
Please share the upcoming events with your friends and colleagues!

Networking

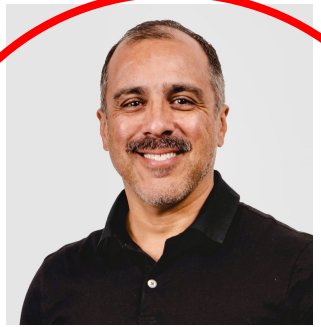
Network here until 8:15pm, then head to Remedy* (3rd & Nueces) if you want to continue conversations! First drinks and snacks are courtesy of our annual partners and champions!

**The Austin Forum advisory board has approved Remedy as our networking bar for cost, proximity, and support contribution reasons*

Austin Forum Team!



Jay Boisseau
Executive Director



Derek Castillo
Managing Director

Mary Garza
Web/UX Designer

Welcome!

Allison Boisseau
Administration

Chris Ashton
Streaming Support

John Lockman
Podcast Engineer

Our Partners Make Austin Forum Possible!

Please contact us if you want to become an annual partner!

AUSTIN FORUM

ON TECHNOLOGY & SOCIETY

Connect. Collaborate. Contribute.™