

Cyber Security Trends and Careers Outlook for 2025

Amherst Security Group

February 20, 2025

Robert Hurlbut

RobertHurlbut.com • [@RobertHurlbut](https://twitter.com/RobertHurlbut)

Who am I?



X (Twitter): [@RobertHurlbut](https://twitter.com/RobertHurlbut)
BlueSky: [roberthurlbut.bsky.social](https://bsky.app/profile/roberthurlbut.bsky.social)
LinkedIn: [roberthurlbut](https://www.linkedin.com/in/roberthurlbut)
Discord: [robert.ct](https://discord.com/users/robert.ct) (robertct)

Robert Hurlbut

Principal Application Security Architect /
Threat Modeling Lead

@ Aquia, Inc. (<https://aquia.us>)



- Microsoft MVP – Dev Sec / Dev Tech
- (ISC2) CSSLP
- Boston Code Camp – Co-Organizer
- Boston .NET Architecture Group – Founder / Leader
- Amherst Security Group – Leader
- Application Security Podcast – Co-Host
- “Threat Modeling Manifesto” – Co-Author
- “Threat Modeling Capabilities” – Co-Author
- Threat Modeling Connect – Co-Founding Member
- Expert Witness (Threat Modeling, Cybersecurity)
- Ph.D. Student – Space Cybersecurity

Previous AmSec Group talks about Latest Trends in Cyber Security

- Latest trends in Cyber Security for 2023 (Robert Hurlbut)
– 1/19/2023
<https://www.meetup.com/amherstsec/events/290699032>

Notes and video links are in the comments for each session.

Previous AmSec Group talks about Careers in Cyber Security

- Associate to Architect – advance career Infosec (Marc French)
<https://www.meetup.com/amherstsec/events/270036447>
- Informal Chat about Careers in Cyber Security (Robert Hurlbut) - 12/8/2021
<https://www.meetup.com/amherstsec/events/wpvwxqyccqblb/>
- Shooting Your Shot: The Fallacy of Shooting Your Eye Out (Alyssa Miller) - 1/12/2022
<https://www.meetup.com/amherstsec/events/wpvwxqydccbqb/>
- Another Informal Chat about Careers in Cyber Security (Robert Hurlbut) – 3/16/2023
<https://www.meetup.com/amherstsec/events/291854444>

Notes and video links are in the comments for each session.

Cyber Security Trends

What do we mean by Cyber Security?

Cybersecurity is the practice of protecting critical systems and sensitive information from digital attacks. Also known as information technology (IT) security, cybersecurity measures are designed to combat threats against networked systems and applications, whether those threats originate from inside or outside of an organization.

*Definition from

<https://www.ibm.com/topics/cybersecurity>

Latest Trends *Work*

| January, 2023 | February, 2025 |
|--------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Covid-19 pandemic since early 2020 – still impacting the industry | Flu, Covid-19, and many others are still here but do not have as much of an impact (though many suffered over the holidays) |
| More returning to offices, many staying home | Many in offices now – more instances of hybrid work than remote work |
| Economic Recession? Microsoft, Facebook, Apple, Amazon, Twitter, etc. laying off 1000s of employees | <ul style="list-style-type: none">• Federal Government (since January 20) – return to office, layoffs/firings• Many other companies |

Latest Trends *Cyber Security*

| January, 2023 | February, 2025 |
|------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Internet of Things (IoT) – labeling devices | <ul style="list-style-type: none"> • IoT – increased spending (over \$3 trillion) • More AI-integration (and related threats) |
| Cloud Security – increased dependency, spending | It is still a concern, but also 5G and Edge (mobile) security risks |
| Zero Trust Adoption – increased spending | <ul style="list-style-type: none"> • More Zero Trust Architectures (recognizing it isn't a product but a long process) |
| SaaS security solutions – Security as a Service (SECaaS) | <ul style="list-style-type: none"> • Still on the rise |
| Security for Remote and Hybrid Workers- Multi-Factor Authentication (MFA), etc. | <ul style="list-style-type: none"> • Insider threats increased by hybrid work |
| Artificial Intelligence (AI) / Deep Learning / Machine Learning – ChatGPT (OpenAI), etc. | <ul style="list-style-type: none"> • AI-Driven Malware • “Bad/suspect” LLMs – DeepSeek (China), etc. • Agentic Threats • Social engineering / Deep Fakes |
| Protection against / remediation for Supply Chain Attacks, IoT Attacks, and Ransomware | <ul style="list-style-type: none"> • Supply chain attacks, IoT attacks • Ransomware events down • Quantum computing threats/concerns increasing |
| Security-aware Culture | <ul style="list-style-type: none"> • Convergence of IT (Information Technology) and OT (Operational Technology) security |

Latest Trends

Application Security

| January, 2023 | February, 2025 |
|------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cloud Security + Application Security | <ul style="list-style-type: none"> • Product Security (which includes Products, Cloud, and Application Security) |
| Tighter Security around Open-Source Software | <ul style="list-style-type: none"> • Vulnerability management • Automated code scanning • AI-powered security analysis/threat detection • Supply chain security |
| Code Factory Attack Surface will keep expanding | <ul style="list-style-type: none"> • Comprehensive Attack Surface Management (CASM) |
| Secure Software Compliance and SBOM | <ul style="list-style-type: none"> • SBOMs are still there, but not widespread adoption as hoped • Regulatory pressure for supply chain security |
| Smarter Prioritization through Security Issue Context | <ul style="list-style-type: none"> • “Zero Trust” – critical principle |
| Culture Change: Executive Demand for Application Release Governance (Security Champions, Shift Left) | <ul style="list-style-type: none"> • Security Champions - • Shift Left – became a “bad” word • Secure Development Practices • Secure-by-Design/Default (attestations) |

References

- “10 Cybersecurity Trends for 2025”
 - <https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-trends/>
- “Five Predictions for Application Security in 2025”
 - <https://www.ox.security/five-predictions-for-application-security-in-2025/>

Careers Outlook

Examples of day-to-day responsibilities in cybersecurity

The following are some of the typical responsibilities of cybersecurity professionals:

- **Monitoring for attacks across various systems**
- **Responding to successful attacks that breach a system or systems**
- **Assessing systems and people for security weaknesses (known as *vulnerabilities*)**
- **Tracking, validating, and reporting on the fixing of those vulnerabilities**
- **Working with developers on practices for developing secure software**
- **Designing and deploying security measures (also known as *controls*)**
- **Working with executive leaders to secure budgeting for security**
- **Providing evidence of security controls for auditors**
- **Maintaining various security systems (user accounts, firewalls, and so forth)**

*From Cybersecurity Career Guide (2022) by Alyssa Miller.

Top Cybersecurity Skills (2025)

- Networking and System Administration
- Knowledge of Operating Systems and Virtual Machines
- Network Security Control (firewalls, VPNs, etc.)
- Coding
 - Low-level: C, C++ - even better, Rust
 - Scripting: Python
 - Websites: JavaScript, HTML, PHP, ASP.NET, others
 - Cryptography: Go lang
 - Databases: SQL
 - Reverse Engineering: Assembly Language
- Cloud Security
- IoT Security
- Blockchain Security
- Internet of Things (IoT) Security
- Artificial Intelligence (AI)

Additional Cybersecurity Skills

- Risk Analysis (Governance, Risk, Compliance - GRC)
- Information Security
- Security Incident Handling and Response
- Security Audit
- Laws and Regulations

5 Phase Plan

John Strand's (Black Hills Information Security) 5-Phase Plan for Starting in Computer Security

Phase 1

- Learn core operating systems – Windows, Linux, Networking, Coding, Security Standards

Phase 2

- Start projects
 - Start a security group (work, school)
 - Learn PowerShell
 - Follow security news
 - Eliminate distractions

Phase 3

- Web Apps – PHP, ASP.NET – Develop something (even if it sucks!)

5 Phase Plan

John Strand's (Black Hills Information Security) 5-Phase Plan for Starting in Computer Security

Phase 4

- Hack stuff
 - Learn IDA and Immunity Debugger
 - Pick a protocol and understand that protocol
 - Online challenges
 - Learn ZAP from OWASP
 - Use/learn: ATT&CK for Enterprise Matrix, SANS Ultimate Pentest Poster

Phase 5

- Give talks everywhere and anywhere
- Present on things you have learned
- Take advantage of cons/events/webcasts as a speaker
- Put.Yourself.Out.There!

5 Phase Plan

John Strand's (Black Hills Information Security) 5-Phase Plan for Starting in Computer Security

Feel free to:

- Indulge in distractions
- Stick to this plan
- Ignore this plan
- Develop your own plan
- Get good at just one thing
- Get a degree
- Don't get a degree
- Get certifications
- Don't get certified

Do NOT do the following:

- Sink into video games
- Waste your time figuring out the cube
- Binge watch shows on Netflix
- Use Bing for anything
- Just barely learn Metasploit to impress people
- Spend more time on the hacker "look" than learning
- Get angry
- Blame others

Resources - Books

- Cybersecurity Leadership: Powering the Modern Organization (2015) by Dr. Mansur Hasib
<https://www.amazon.com/Cybersecurity-Leadership-audiobook/dp/B00U0EXIQE>
- Bring Inner Greatness Out: Personal Brand (2021) by Dr. Mansur Hasib
<https://www.amazon.com/Bring-Inner-Greatness-Out-Personal/dp/B08V97M76H>
- Cybersecurity Career Guide (2022) by Alyssa Miller
<https://www.amazon.com/Cybersecurity-Career-Guide-Alyssa-Miller-ebook/dp/B0B2XRMS9T>
- Confident Cyber Security: How to Get Started in Cyber Security and Futureproof Your Career (2020) by Dr. Jessica Barker
<https://www.amazon.com/Confident-Cyber-Security-Started-Futureproof/dp/1789663407>

Resources - Articles

- Top 8 Cybersecurity Skills You Must Have (Feb 17, 2025)
<https://www.simplilearn.com/tutorials/cyber-security-tutorial/cyber-security-skills>
- John Strand's 5 Phase Plan for Starting in Computer Security
<https://www.blackhillsinfosec.com/john-strands-5-phase-plan/>
- Your 2025 Guide to Cybersecurity Careers
<https://www.coursera.org/articles/cybersecurity-career-guide>

Resources - Training

- Wild West Hacking
<https://wildwesthackinfest.com/>
- Antisyphon InfoSec Training
<https://www.antsyphontraining.com/>
- HackerOne
<https://www.hackerone.com/hackers/hacker101>
- Pluralsight (<https://www.pluralsight.com/>), LinkedIn Learning (<https://www.linkedin.com/learning>)
- Boot Camps
- Bachelor's, Master's, and Doctoral / PhD Cybersecurity-related degree programs
Various universities – many becoming available as hybrid or online-only
In post-Covid era, there may be less of stigma about online vs. in-person degrees

Resources - Jobs

- LinkedIn
<https://linkedin.com> (consider Premium service while job hunting)
- Glassdoor
<https://glassdoor.com> (review salaries, experiences of companies)

Resources - Certifications

- Consider what certs are important to your industry
 - Government: Many agencies require certifications
 - Finance, Healthcare: May be required or recommended
 - Other: May not be as important – but could help you stand out
- (ISC2) CISSP, etc.
Certs requiring experience - showing you have actively participated in security activities can help
- CompTIA, CompTIA Security+
- When thinking about certs, determine a strategy based on cost, time to study, time to renew

Other Considerations

- Cover letter - write one
- Resumes - customize, be mindful of keywords / AI scanning, consider getting a review or help with rewriting
- GitHub account - shows active work – add to the resume!
- Courses with certificates – Coursera, LinkedIn Learning – add to the resume!
- Starting a blog?
<https://javvadmalik.com/2021/12/03/november-blog-a-day-reflections/>
- Find a professional mentor
 - Tanya Janca (@shehackspurple) makes calls each Monday for [#cybermentoringmonday](#) on Twitter
- Be a professional mentor – pay it forward!

Keeping Up To Date

- LinkedIn (<https://linkedin.com>)
- Dark Reading (<https://darkreading.com>)
- CSO Online (<https://www.csoonline.com>)
- Discord and/or Slack workspaces and channels
- Podcasts: DarkNet Diaries, others
(<https://www.sans.org/blog/cybersecurity-podcast-roundup/>)

Upcoming Local Events

- NERD Summit 2025 at UMass Amherst – canceled for this year
- NH Cybersecurity Symposium 2025 at Manchester Community College, Manchester, NH – probably canceled for this year
- Boston Code Camp 38 at Microsoft Offices, Burlington, MA (3/29) – FREE
 - <https://www.bostoncodecamp.com>
- OWASP Boston Application Security Conference (BASC) 2025 at Microsoft Offices, Burlington, MA (4/5) - FREE
 - <https://www.basconf.org/>

Questions?



Contacts

X (Twitter): [@RobertHurlbut](https://twitter.com/RobertHurlbut)

BlueSky: roberthurlbut.bsky.social

LinkedIn: [roberthurlbut](https://www.linkedin.com/in/roberthurlbut)

Discord: `robert.ct (robertct)`