The Next Generation Cyber Community Must Learn More Than How to Hack

By: Jaiz Anuar

20 July 2026 · Cybersecurity · Leadership · 10 min read

The next cyber generation must combine offensive curiosity with trust, resilience, responsibility and the ability to protect organisations.

For many years, Capture the Flag competitions have been among the most popular activities for developing future cybersecurity talent. Participants discover vulnerabilities, exploit weaknesses, analyse malicious code, investigate incidents and solve complex technical problems in a safe environment.

CTF competitions are valuable. They develop curiosity, persistence, technical confidence, teamwork and practical problem-solving skills. Learning how to think like an attacker remains an important part of cybersecurity education.

But the cybersecurity environment is evolving. Future cyber professionals will need to understand more than how to break into a system, bypass a control or capture a flag. They must also understand why the system trusted the wrong identity, instruction or transaction in the first place.

They must know how to detect compromise, limit its impact, maintain critical services and help an organisation recover safely.

This means the next generation cyber community must learn more than how to hack. It must learn how to question trust, design for failure and build resilience.

Finding a vulnerability demonstrates technical capability. Protecting an organisation requires something broader: judgment, responsibility, collaboration and an understanding of what the business and society depend upon.

A captured flag may end a competition. In the real world, it is often where the most important work begins.

Hacking teaches us how systems fail

An offensive security mindset is valuable because it challenges assumptions. A developer may believe an application is secure because it has passed testing. An administrator may believe an identity is legitimate because the correct credentials were used. An organisation may believe its environment is protected because multiple security products have been deployed.

A hacker asks different questions. What if the input is manipulated? What if the identity has been compromised? What if the control can be bypassed? What if the system behaves differently from what its designer intended?

These questions expose the difference between how a system is expected to operate and how it actually behaves when placed under pressure. This is why offensive security skills remain important: they help organisations discover weaknesses before real attackers do.

But the lesson should not end when the vulnerability is found. Why did the system trust that request? Why was abnormal behaviour not detected? Why could one compromised identity reach critical systems? Could the organisation continue operating and recover without restoring the same weakness?

These are no longer only questions about hacking. They are questions about architecture, governance, resilience and trust.

A captured flag is not the same as a protected organisation

In a competition, success is usually measured through points, speed and the number of challenges completed. In a real organisation, the outcome is measured differently.

A security team may successfully identify a vulnerability but still fail to protect the business. Sensitive information may already have been exposed, a critical service may remain unavailable, or an attacker may have established another route into the environment.

Real cybersecurity is not only about stopping an attacker from entering. It is also about limiting what happens after entry.

Future cyber professionals must understand how to:

Detect suspicious activity early.

Identify affected identities, devices and systems.

Contain the compromise and prevent lateral movement.

Protect critical services and information.

Maintain essential business operations.

Recover from a trusted and verified state.

Communicate clearly with business leaders.

Turn the incident into lasting improvement.

The best cyber professionals are not simply those who can break systems. They are those who can explain why the system failed, determine which trust decision was abused and design a safer way forward.

The next generation must learn to question trust

Almost every digital interaction involves a trust decision. A user trusts an application. An application trusts an identity provider. A server trusts a certificate. A system trusts information received through an API. An employee trusts an email, document or AI-generated response.

Many cyber incidents occur not because trust is absent, but because trust is granted too easily, maintained for too long or never verified again.

An identity may have been legitimate yesterday but compromised today. A managed device may have been compliant when it connected but become exposed later. A trusted application may begin behaving abnormally. A supplier that was previously secure may suffer a breach.

Trust cannot be treated as permanent merely because it was established once. The next generation cyber community must develop a culture of verified trust.

Who or what is requesting access? What evidence supports the identity? Is the device secure? Is the requested action consistent with the expected role? Does the behaviour match the context? Should access continue if conditions change?

The objective is not to remove trust from digital systems. It is to make trust deliberate, limited, observable and continuously verifiable.

Resilience must become part of cyber education

Security education often concentrates on stopping attacks. Prevention remains important, but prevention will never be perfect. Credentials will be compromised, applications will contain vulnerabilities, employees will make mistakes, trusted suppliers may be breached and controls may fail or be misconfigured.

The objective cannot be to create an environment in which nothing ever goes wrong. It should be to build systems and organisations that can withstand disruption, contain compromise and recover safely.

Future cyber professionals must understand that a control working today does not guarantee it will work tomorrow. A system operating normally does not necessarily mean it is resilient. An organisation that has not experienced a major incident is not necessarily secure.

Can the attack be detected? Can the affected component be isolated? Can the business continue operating? Are recovery systems separated and protected? Can services be restored from a known and trusted state? Has recovery actually been tested?

A resilient organisation does not assume every attack can be prevented. It ensures that one failed control does not become a complete business failure.

Future cyber exercises should evolve

CTF competitions should continue, but future exercises could evolve beyond capturing the flag. Participants could first find and exploit a vulnerability, then defend the affected service, investigate the incident and restore the environment.

Capture the flag: Discover and exploit the weakness.

Detect the attack: Identify the evidence left behind.

Contain the compromise: Prevent further movement and damage.

Recover the service: Restore operations from a trusted state.

Explain the lesson: Communicate what happened and recommend improvements.

The offensive mindset shows how a system can be broken. The defensive mindset shows how the attack can be detected and contained. The resilience mindset shows how the organisation can continue operating and recover. The trust mindset asks why the interaction was allowed. The leadership mindset explains what the incident means to the business.

The next generation will need all five.

Technical ability must be guided by responsibility

Cybersecurity knowledge creates power. The same capability used to test a system can be used to exploit it, and the same tool used for defence can be misused.

Young professionals must understand permission, boundaries, privacy and the consequences of their actions. Having the capability to perform an action does not automatically give them the authority to do it.

The question should not only be: Can I do this? It should also be: Am I authorised to do this, should I do it and who could be affected?

Ethics should be embedded into how cybersecurity professionals experiment, collaborate and make decisions. A strong cyber community must value integrity as highly as technical excellence.

Cybersecurity must become a learning community

Attackers share tools, techniques and knowledge quickly. Defenders cannot afford to work entirely in isolation.

Building the next generation cyber community requires stronger collaboration between students, universities, government agencies, technology companies, security practitioners and business leaders.

Experienced professionals should share more than successful implementations. They should share failed assumptions, difficult decisions, operational challenges and lessons from incidents. Young professionals should be encouraged to question established practices respectfully.

Knowledge should flow in both directions. Experienced practitioners provide context, judgment and lessons developed over time. The next generation brings new perspectives, curiosity and familiarity with emerging technologies. Both are needed.

We need more than a cybersecurity talent pipeline

We do not only need more people who know how to operate cybersecurity tools. We need architects who design for compromise, defenders who recognise weak signals, engineers who understand business continuity, incident responders who can contain an attack without unnecessarily stopping the organisation, and leaders who can make decisions under uncertainty.

Most importantly, we need people who recognise that cybersecurity is ultimately about protecting trust between individuals, organisations and technology.

The community we should build

The next generation cyber community should remain curious enough to explore how systems can be broken. But it must also be responsible enough to understand the consequences.

It should be technically capable, but never technically arrogant. It should question trust without becoming paralysed by distrust. It should recognise that controls can fail, while designing systems that can continue operating safely. It should compete to improve individual skills, but collaborate to protect the wider community.

Learning how to hack may open the door to cybersecurity. Learning how to protect trust, contain failure and strengthen resilience is what transforms that capability into a profession.

The future of cybersecurity will not be determined only by who can capture the flag fastest. It will be determined by who can help society remain secure, trusted and resilient after the flag has been captured.

Question assumptions. Share knowledge. Build trust.