CISCO
SECURE

5 Data-Backed Ways to Make a Cybersecurity Impact

Cybersecurity challenges aren't going anywhere. Every day, our world is becoming more connected and complex. And, for cybersecurity teams, more complexity equals more responsibility.

Luckily, companies can take concrete steps to improve security outcomes. In our Security Outcomes Study, Vol. 2, we gathered data from over 5,100 security and IT practitioners, across 27 countries. From that data, we've zeroed in on five key practices that are proven to drive cybersecurity program success. Leverage the checklist below:

Refresh Your Tech

39% of security technologies used by organizations are considered outdated.

Don't be reactive and evaluate your tech stack after an incident. Build a more proactive tech refresh strategy today.

> "With nearly 40% of in-use security technologies considered outdated, the issue of security debt is significant. But the good news is that organizations with modern consolidated cloud architectures achieve a high level of tech refresh by being proactive in their tech strategy. Problem plus solution."
>
> Richard Archdeacon, Advisory CISO, Cisco

Integrate for Better Visibility

77% of organizations would rather buy integrated solutions than build them.

Fortunately, with cloud-based solutions becoming more prominent, strong integrations are more accessible than ever, giving security teams broader visibility across their systems.

> "Modern, well-integrated security IT contributes to overall program success, more than any other security practice or control."
>
> Helen Patton, Advisory CISO, Cisco

Expand Your Team

Organizations with the highest staffing ratios are 20% more likely to report stronger threat detection and response.

Team expansion not an option? Consider strengthening the skills and proficiencies of existing staff. Training is always a smart investment.

> "Choose the best-skilled people for your SecOps teams because that matters more than just headcount. Automation can help you bridge the gap with your junior staff to get results that are just as strong as if you had more senior staff."
>
> Wendy Nather, Head of Advisory CISOs, Cisco

Work Smarter with Threat Intelligence

Organizations using threat intelligence are 2X as likely to report strong detection and response capabilities.

Whether or not team growth is an option, use every intelligence tool available to bridge that gap. Work smarter to yield stronger outcomes.

> "When enterprises combine strong people, processes, and technology, they achieve advanced threat detection and response capabilities, when rounded out with solid threat intelligence."
>
> Dave Lewis, Advisory CISO, Cisco

Break Things On Purpose

Companies that engage in chaos engineering are 2X as likely to see improved business continuity.

Regular and intentional IT disruption will prepare your organization for handling real threats. Embrace chaos to prepare for chaos.

> "Organizations who run regular and varied tests are 2.5 times more likely to maintain operations in the face of an emergency. This can be further bolstered by following chaos engineering practices."
>
> Wolfgang Goerlich, Advisory CISO, Cisco

Following these data-backed steps will put you on the path to a stronger cybersecurity posture. But don't just take our word for it. To see all the data behind our findings, check out the full report today.

Get the Report

CISCO The bridge to possible