The Frugal CISO:

Running Cybersecurity on a shoestring Budget

Anand Thangaraju
Field CISO, ePlus Inc.

Sep 2024

About Me

Fractional Chief Information Security Officer (vCISO)

- Cyber Risk & Fintech Leader
- Board Advisor & Angel for Startups. Scout and Advisor for VCs
- Corporate roles at Cognizant, JPMC, EY, SVB, Zelle, ePlus
- ISACA SV Board Member (Volunteer Member of many)
- AI Evangelist
- Certified ORM, CERP, CISA, CISSP, CIPM, SCR Professional

Anand Thangaraju

Field CISO, ePlus Inc.

ePlus Inc.

Cybersecurity on a Budget

Why It's More Relevant Than Ever

Businesses all over the world realise the importance of Cybersecurity - as threats emerging from cyber attacks are on a steep rise and they realise that even a single attack can cost them a fortune.

Last year, **over eight billion data** records were breached worldwide, according to IT Governance.

On the other side, companies are squeezing budgets to free up resources for funding growth projects like for innovation, sustainability, and other critical projects.

Thus the era of having a **Frugal Cybersecurity strategy** is upon us!

The Age of a Frugal CISO!!!

The global cost of cyberattacks will be about

$10.5 Trillion

Annually By 2025

Ransomware payments in 2023 hit a record

$1.1 Billion

What Does It Mean to Be a Frugal CISO?

In the above said scenario, security professionals must respond to the all growing security issues but at the same time keep a level headed budget.

This is where a Frugal CISO should take charge!

Actually, implementing a comprehensive, cost-resilient security strategy can improve an organization's risk profile. How?

When optimizing the cyber budget, a CISO will review people, processes, and technology to identify gaps and inefficiencies. Addressing these will automatically reduce risks while spending is held steady.

For this, companies need well-crafted cybersecurity strategies. And the first step is Understanding your Cybersecurity Budget.

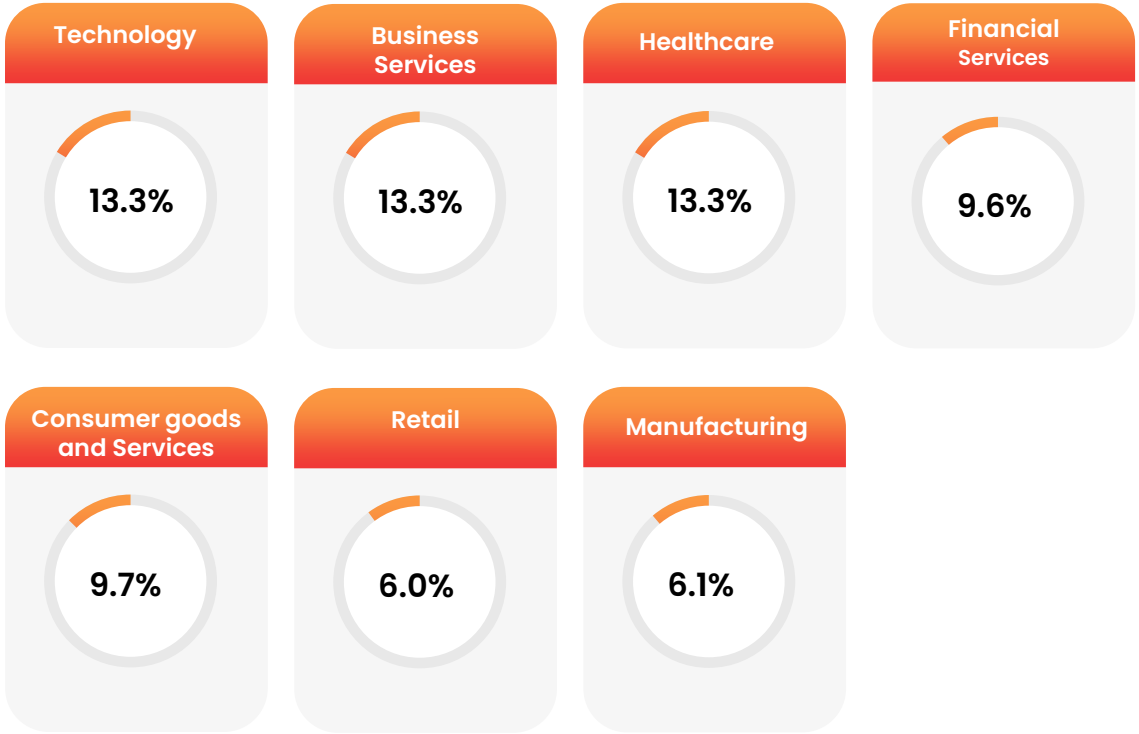
Understanding Your Cybersecurity Budget

On an average, businesses **spend approximately 11%** of their IT budgets on security.

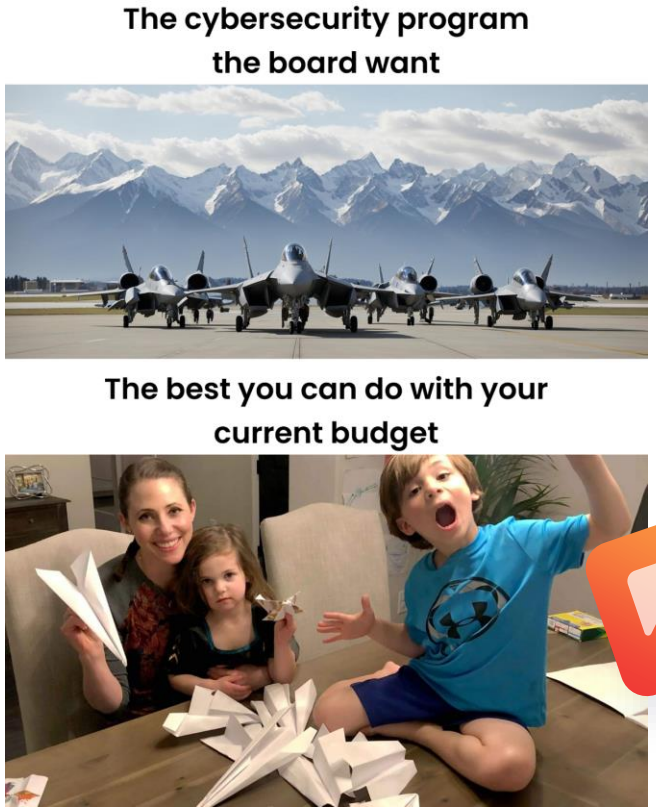
This can vary across industries, based on sector-specific data and technological and regulatory requirements.

First analyze your cybersecurity budget decisions based on what your sector is generally spending on security and considering opportunities for savings. Here are the average cybersecurity annual spending as a percentage of their IT budget by industry:

Percentage of budgets spent on security by industry



Prioritizing Cybersecurity Spending



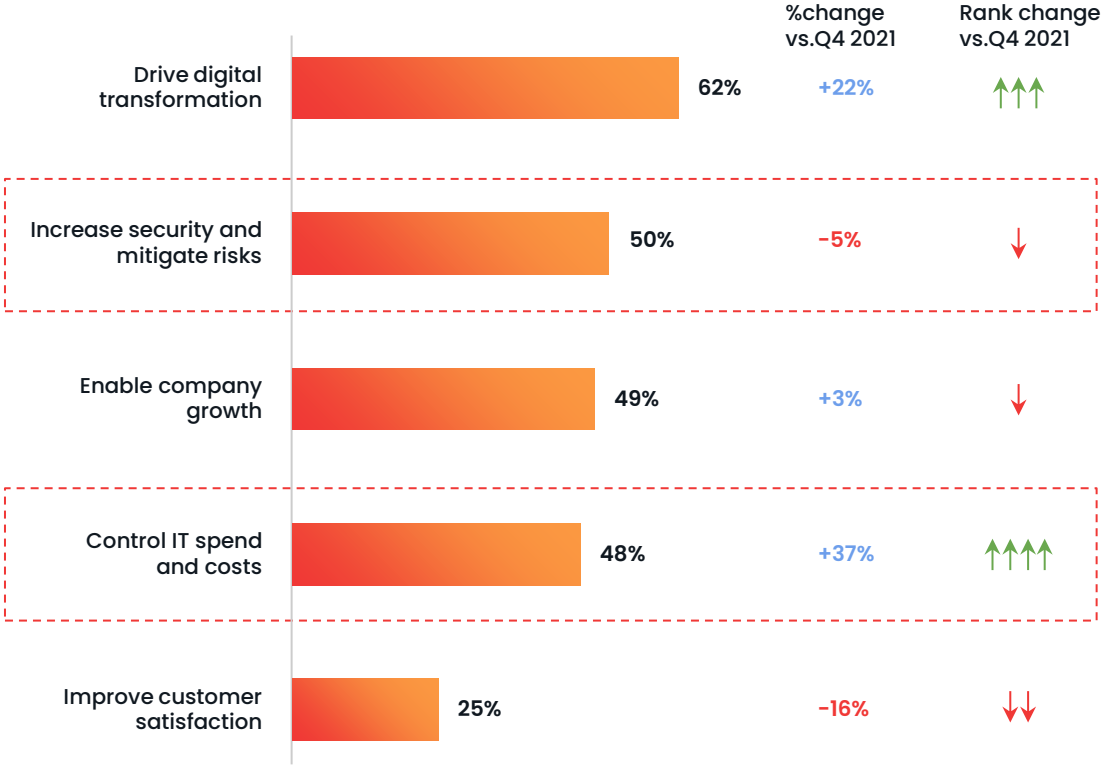
Prioritizing Cybersecurity Spending

Many companies are squeezing budgets to free up resources for growth.

For the Chief Information Security Officer (CISO), this may mean a new era. Increasingly, they are being asked to improve cybersecurity with historically small budget increases.

Exhibit 1 - While Security Remains a Top Priority, IT Professionals Must Now Control Costs

Respondents naming each issue as a Top 3 priority



Sources : IT Buyer Pulse Check 5.0 (December 2022), N = 450; IT Buyer Pulse Check 3.0 (October 2021),N = 676(APAC excluded).

Budget Levers at your disposal

Budget Levers at your disposal

01 Prioritize Spending on Critical Assets

02 Leverage What You Already Have

03 Create a Lean Cybersecurity Strategy

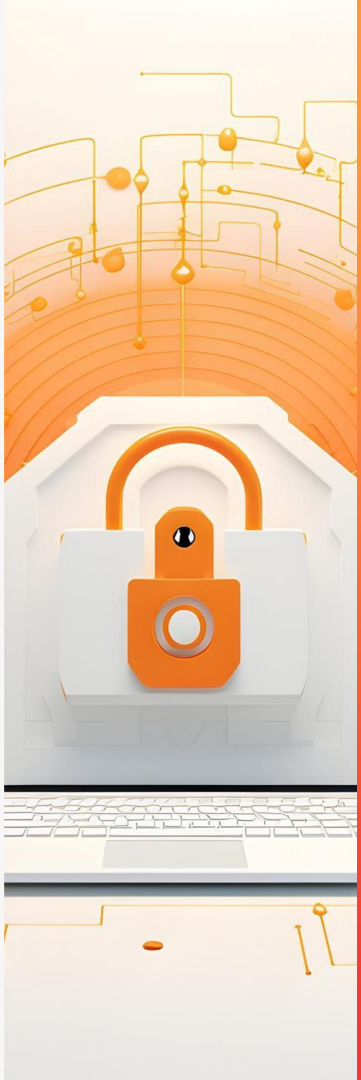
04 Utilize Open-Source / Free Tools

05 Automate to Save Time and Money

06 Outsource Smartly: Managed Security Services

07 Master the art of Negotiating Better Deals with Vendors

08 Humans contribute to More than 50% of cyber risk. Leverage Trainings and Awareness



01

Prioritize Spending on Critical Assets

- Use frameworks like NIST Cybersecurity Framework (CSF) or ISO/IEC 27001 to categorize assets based on their criticality to business operations. Prioritize securing high-value assets to ensure your budget is spent on the most impactful areas.
- The Cyber Defense Matrix builds on the above frameworks to organize your security data and identify your cybersecurity gaps.
- Utilize free tools like OWASP Risk Assessment Framework or Microsoft's Security Assessment Tool (MSAT) to assess vulnerabilities and rank them based on the likelihood of exploitation and the potential impact on the business.
- Leverage CIS Controls to implement basic but effective security measures, such as multi-factor authentication (MFA) and endpoint detection, for high-priority threats. Start with the most impactful controls from CIS Top 20 to get the best ROI on limited resources.
- Align your cybersecurity efforts with both regulatory compliance and business priorities. Use free tools like Cyber Risk Quantification from FAIR (Factor Analysis of Information Risk) to measure risk in financial terms and justify spending.

02 Leverage What You Already Have

Focus on ways to maximize current tools, talent, and processes first, before looking at new purchases.

Skip Tech Tools with Little ROI

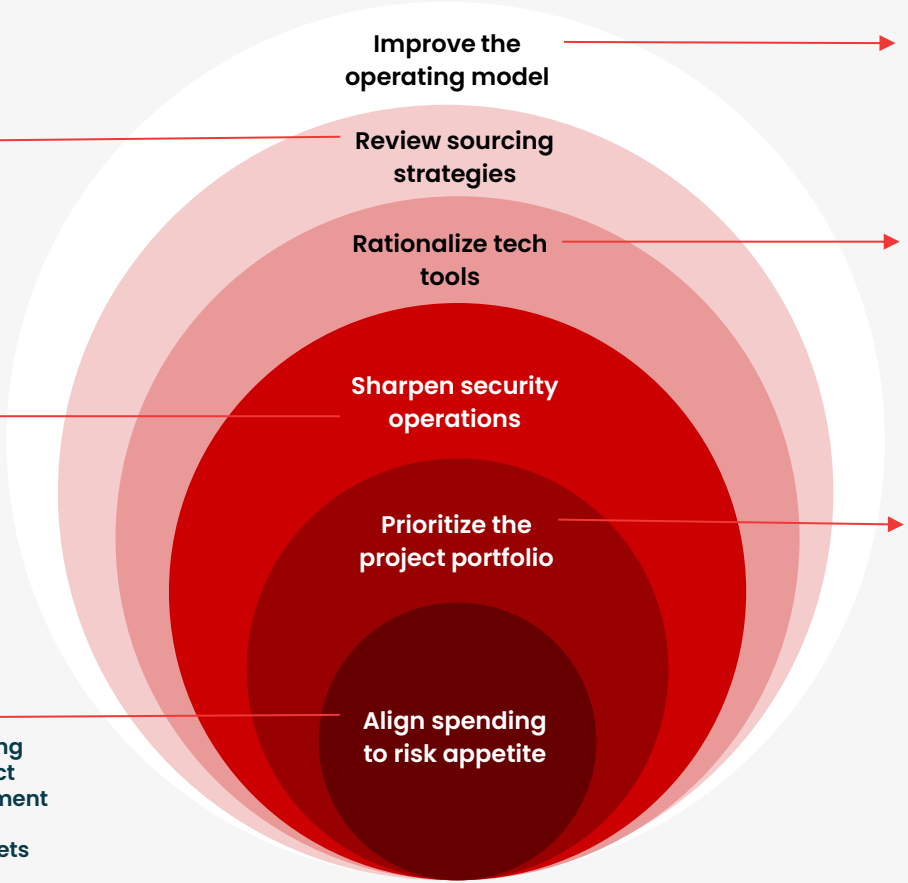
Consolidate vendors and tools to eliminate redundancy and inefficiency. Ensure every tool demonstrates a clear ROI. The ROI might manifest as labor savings, threat mitigation, or operational impact.

Consider minimizing or avoiding investment in the following areas:

- Consider cloud migration and hybrid work models instead of on-premises security appliances.
- Eliminate low-value consulting engagements, such as redundant penetration tests and costly audit preparations.
- Reduce spending on standalone governance, risk, and compliance (GRC) tools with overlapping capabilities.
- Shift from less effective technology, like runtime application self-protection (RASP), to posture management or modern application protection solutions.
- Essentially, you should assess the functionality of your standalone security controls and reduce overlap with other deployed platforms.

03

Create a Lean Cybersecurity Strategy



Improve the operating model
Optimize staffing and duplicative processes. Ensure that staff are spending time on the tasks that drive the biggest risk reductions.

Review sourcing strategies
Once tools and requirements are identified, optimize the purchase process. SLAs and in/outsourcing decisions should be reviewed to identify ways to maximize cost efficiency while meeting performance expectations.

Rationalize tech tools
Buying tools in packages can lead to duplication and waste. Look to consolidating vendors, seeking reduced costs and better security outcomes through improved tool integrations.

Sharpen security operations
Review all security operations with an eye to improving operational efficiency. What can be automated? Can costs be reduced by changing service level agreements etc.

Prioritize the project portfolio
Challenge ongoing investment - Ongoing projects must be evaluated, conflicts and overlaps resolved, and priorities decided on a balance of cost and risk reduction.

Align spending to risk appetite
Define cybersecurity risk appetite, working with business units to quantify the impact of incidents. Identify areas where investment exceeds what is necessary to meet the required risk profile and reallocate budgets accordingly.

04 Utilize Open-Source / Free Tools

CloudSploit

CloudSploit is a functional, open- source CSPM that is pretty low lift to get up and running to audit various public cloud providers

Bitwarden

Bitwarden is a capable password manager that is open source and can be deployed with minimal technical knowledge

Some commercial password vaulting and PAM solutions with far more capabilities, but most "have not" orgs should deploy the open-source version of Bitwarden and redirect limited funds to other areas like vulnerability management

- Utilize well-regarded open-source tools for tasks like intrusion detection (e.g., Snort, Suricata), vulnerability scanning (e.g., OpenVAS, Qualys FreeScan), and endpoint protection (e.g., OSSEC). This minimizes software costs without compromising effectiveness.
- Use free or low-cost threat intelligence services like **AlienVault Open Threat Exchange (OTX)** to stay updated on emerging threats and adjust your defense strategy accordingly. This allows you to focus spending where it's needed most.
- If you're willing to deploy a dedicated SIEM, consider **Wazuh** as an open-source solution

  (Side benefit: Wazuh also has endpoint agents that can serve as EDR if you can't afford a commercial agent)

05

Automate to Save Time and Money

SEC element	Capability	Tools
01 Automate Log Collection and Analysis with SIEM Tools	Automate the collection, analysis, and correlation of security event logs to detect threats in real time.	Leverage free or affordable tools like Elastic SIEM, Splunk Free, or Graylog to centralize log data from various systems and automate detection of anomalies without expensive manual monitoring.
02 Automate Patch Management	Automate the scanning and patching of vulnerabilities to keep systems updated without manual intervention.	Use free or low-cost tools like WSUS (Windows Server Update Services) for Windows environments or Automox for cross-platform automated patch management, which saves time and reduces human error.
03 Automated Vulnerability Scanning and Remediation	Automatically scan for vulnerabilities and provide actionable remediation steps on a regular schedule.	Utilize tools like OpenVAS or Nessus Essentials (free for small environments) to run continuous vulnerability scans and generate reports, reducing the need for manual assessments.

05

Automate to Save Time and Money

SEC element	Capability	Tools
04 Automate Phishing Detection and Response	Automate the detection of phishing attempts and the response process to minimize manual intervention.	Implement tools like Cofense Triage or PhishER, which can integrate with your email system to detect, report, and automatically respond to phishing threats without consuming human resources.
05 Automated Endpoint Detection and Response (EDR)	Automate threat detection and response on endpoints to identify and neutralize threats without manual monitoring.	Deploy budget-friendly or free solutions like OSSEC (open-source) or Cynet (offers free versions for small teams) to automate the detection and remediation of endpoint threats.
06 Automate Incident Response Playbooks	Implement automated workflows for incident response to standardize processes and reduce response time.	Use orchestration and automation platforms like TheHive or Shuffle (open-source SOAR) to automate incident response playbooks and alerting, which helps speed up response without relying on large teams.

06

Outsource Smartly: Managed Security Services

- SOC Monitoring: Outsource 24/7 threat monitoring and incident response to MSSPs, reducing the need for costly in-house infrastructure and expertise.
- Vulnerability Management & Pen Testing: External experts provide unbiased, up-to-date vulnerability assessments and penetration testing at lower costs.
- Incident Response & Forensics: Outsourcing ensures quick, specialized incident containment and recovery, without maintaining a full in-house team.
- Identity & Access Management (IAM): Cloud-based IAM services ensure consistent enforcement of access controls, reducing the internal management burden.
- Managed Detection & Response (MDR): Outsourced MDR offers advanced threat detection and response, leveraging cutting-edge tools and expertise.
- Compliance Management: External compliance experts ensure regulatory adherence and perform audits, saving internal resources and reducing risk.

07

Master the art of Negotiating Better Deals with Vendors

Do Thorough Market Research

- Understand the market rates, features, and competitors.
- Have alternative vendors and a clear knowledge of the pricing landscape.
- Tools like Gartner or G2 Crowd can help.

Bundle Multiple Solutions for Discounts

- If a vendor offers multiple products or services, try to bundle them together for a bulk discount.
- Additionally, explore longer-term contracts for lower pricing.

Ask for Flexibility in Pricing Models

- Negotiate for flexible payment plans, pay-as-you-go options, or user-based pricing
- Helps you avoid paying for services or features you don't need while scaling up when necessary.

Leverage Trials and Proof of Concept (PoC)

- Ask for free trials or PoCs before committing.
- Use the trial period to demonstrate the value to your organization.
- Positive PoC results can give better negotiate terms, as vendors want to convert trials into long-term contracts.

Highlight Long-Term Partnership Opportunities

- Position your organization as a potential long-term partner.
- Vendors are often more willing to negotiate if they see opportunities for upsell, referrals, or long-term collaboration.

Negotiate Maintenance and Support Costs

- Negotiate lower or bundled maintenance and support costs, or explore a tiered support plan.
- Vendors are often open to reducing these costs, especially for high-priority customers.

08

Humans contribute to more than 50% of cyber risk. Leverage Trainings and Awareness

Training 101

The budgeting process should cover training programs to teach your teams about cybersecurity challenges and best practices for managing security. It's vital to customize training content for different audiences, including staff, management, and consultants, and to test its impact regularly. Given the shortage of skilled resources in the market, investments in training can help you stay ahead of cybersecurity threats.

Bonus Ideas!

Bonus Ideas!

a

Cyber Risk Assessment On a Budget

b

Expect Unexpected Expenses

c

Strategic Partnerships and Alliances

d

Cyber Insurance As a Risk Management tool

Cyber Risk Assessment on a Budget

Resolve conflicts, and set priorities that balance cost and risk reduction. Focus on specific areas:

01 API security to protect new business models and partnerships

02 Multi-factor and passwordless authentication to reduce exposure to phishing attacks

03 Zero trust network access (ZTNA) for secure remote access and fine-grained control over assets

04 Extended detection and response (XDR) platforms for advanced threat detection capabilities to support security teams

05 Security posture management (SPM) to monitor and protect critical cloud infrastructure and SaaS applications

06 Consent management software solutions to ensure compliance with privacy regulations

07 AI-generated synthetic data, if you're ready to experiment with AI analytics and model training while maintaining data privacy and security

08 The bottom line is that security leaders should focus investment on security measures that protect the systems that interact with your customers and that generate revenue.

09 Proactive CISOs must continually monitor the efficacy of security controls in their environments and calibrate that against prevalent attack vectors. If risks go above the previously agreed thresholds, CISOs will need to evaluate the threat and either discuss the risks with management to seek further budget or reallocate budget -- or agree to accept the higher risk levels. Tools and services to budget for in this category include cyber insurance, penetration testing, bug bounty initiatives and incident response.

b Expect Unexpected Expenses

Cybersecurity is no longer a mere technological concern but a critical business issue because of all the global conflicts and other major global threats. Thus, organizations must always be prepared to effectively navigate these challenges:

01 Prepare for the unexpected by maintaining a buffer security budget and developing a mindset of cyber resilience.

02 Cyber insurance must be actively considered, which 71% of global leaders purchase to protect against financial losses.

03 Treat cybersecurity as an ongoing process. Invest in continual security testing and improvement, incident response planning, and comprehensive training.

04 Make informed cybersecurity investment decisions, manage risk effectively, and maximize the impact of your spending by integrating these considerations and approaches, you can.

C Building Strategic Alliances for Shared Cybersecurity Resources

Discuss partnerships with industry groups or alliances that offer shared security resources.

d Cyber Insurance as a Risk Mitigation Tool

By combining cyber insurance with strategically selected security investments like, endpoint protection, backups, and employee training, businesses can build a cost-effective security program.

Instead of investing heavily in every possible defense, one can focus on risks with the highest potential impact and rely on insurance to mitigate rare, but financially devastating events.

Cyber insurance can play a good part in a budget-friendly cyber security strategy:

Coverage of Financial Losses like Breach Response costs, claims by third-parties and any interruptions caused to business operations due to breach.

Risk Transfer Strategy: Budget-conscious security initiatives often find it difficult to implement each and every security measure due to limited funds. In such cases, Cyber insurance helps transfer part of the financial risk to the insurer. Also, these insurers often require certain baseline security measures (e.g., firewalls, encryption, incident response plans) before offering coverage which can in turn drive organizations to improve security.

Cyber insurance should not be considered in place of effective and robust cyber risk management. All companies need to purchase cyber insurance but should only consider it to mitigate the damage caused by a potential cyber attack.

Strategic Investment Areas

Any money spent on cybersecurity should ensure one result - risk reduction, that too at the least cost. Strategy guides like Forrester's suggests that companies focus on the following areas:

01 API security to protect new business models and partnerships

02 Multi-factor and passwordless authentication to reduce exposure to phishing attacks

03 Zero trust network access (ZTNA) for secure remote access and fine-grained control over assets

04 Extended detection and response (XDR) platforms for advanced threat detection capabilities to support security teams

05 Security posture management (SPM) to monitor and protect critical cloud infrastructure and SaaS applications

06 Consent management software solutions to ensure compliance with privacy regulations

07 AI-generated synthetic data, if you're ready to experiment with AI analytics and model training while maintaining data privacy and security

08 Best investment on security measures are those that at the same time protect the systems and interact with your customers and generate revenue.

8 Tactical Measures to Protect digital infrastructure on a tight budget

If you took nothing else
from this presentation,
do the following
tactical measures
at the very least.

Protect digital infrastructure on a tight budget - 8 tactics

Tactic	What	How
01 Implement a Strong Access Control Policy (Zero Trust)	Adopt the principle of "least privilege" to ensure that employees only have access to systems and data necessary for their roles.	Use existing role-based access control (RBAC) features in current software, and require multi-factor authentication (MFA) for all sensitive applications.
02 Leverage Open-Source Security Tools	Take advantage of free or low-cost open-source tools for intrusion detection, vulnerability scanning, and log management.	Many open-source tools like Snort (IDS), OSSEC (SIEM), and OpenVAS (vulnerability scanner) provide enterprise-level functionality without heavy license fees. Ensure staff or external contractors effectively configure and maintain these tools.
03 Conduct Regular Cybersecurity Training and Phishing Simulations	Train employees to recognize phishing emails, social engineering tactics, and other common threats.	Use free platforms for phishing simulations (e.g., Cofense PhishMe Free, KnowBe4 offers affordable training).

Protect digital infrastructure on a tight budget

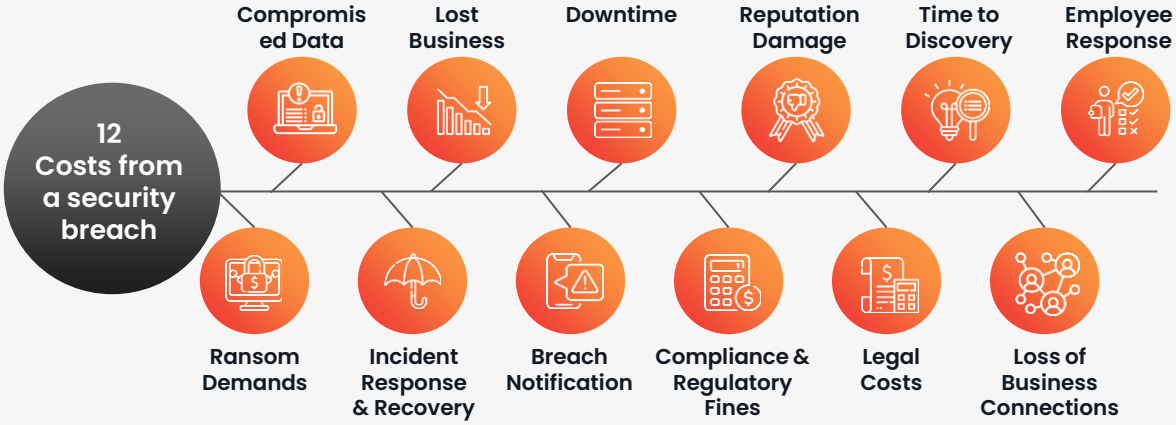
Tactic	What	How
04 Enable Logging and Monitor Logs Regularly	Set up detailed logging for critical systems and applications, and review those logs regularly for unusual activity.	Utilize built-in logging capabilities (e.g., Linux's syslog, Windows Event Viewer) and free SIEM platforms like Graylog or Elastic Stack.
05 Segment Your Network	Use network segmentation to isolate sensitive areas of the network from less critical systems (e.g., keep payment systems separate from email servers).	Most enterprise switches and routers already have VLAN capabilities. Implementing segmentation can be done without extra hardware.
06 Patch and Update Regularly	Prioritize regular patching and updating of software and operating systems to fix known vulnerabilities.	Automate updates and patching where possible using native OS update services (e.g., WSUS for Windows) or low-cost patch management tools.

Protect digital infrastructure on a tight budget

Tactic	What	How
07 Strengthen Endpoint Security	Ensure all endpoints (laptops, phones, IoT devices) are protected with basic security hygiene such as firewalls, antivirus, and encrypted storage.	Use built-in solutions (e.g., Windows Defender, macOS Gatekeeper), and consider lightweight, low-cost endpoint detection and response (EDR) solutions such as Crowdstrike or SentinelOne with flexible pricing models.
08 Utilize Cloud Security Features	If you're using cloud services (AWS, Azure, GCP), leverage their native security tools and best practices (e.g., IAM, security groups, monitoring).	Take advantage of tools like AWS GuardDuty, Azure Security Center, or Google Cloud Security Command Center, and use built-in logging and monitoring.

Quantifying ROI on Cybersecurity Investments

The True Costs of a Security Breach



A common formula is:

Cybersecurity ROI = (Benefits – Costs) / Costs x 100%

Benefits: Total value gained from cybersecurity initiatives - can include money saved from avoiding breaches, reduced risk levels, or any financial gains.

Costs: Total expenses incurred to implement cybersecurity strategies - including cost of software, hardware, training, and any other resources needed.

This percentage reflects the efficiency of cybersecurity investments, showing how much benefit is received for each dollar spent.

ROI of investing in cybersecurity: Comparing the cost of the said preventative measure against the cost of potential breaches it prevents.

Direct costs like fines, legal fees and indirect costs like reputational damage and loss of customer trust should also come while calculating potential damages.

Conclusion and Key Takeaways

A Frugal CISO can optimise a comprehensive, cost-resilient security strategy and at the same time improve an organization's risk profile by careful planning:

- Leverage What You Already Have
- Prioritize Spending on Critical Assets only
- Utilize Open-Source / Free Tools
- Leverage Talent Trainings and Awareness
- Strategic Partnerships and Alliances
- Cyber Insurance for Risk Mitigation

Questions ?


Trying to explain our current cyber risk to the board
Balbix


CYBER SECURITY BUDGET BEFORE A BREACH
CYBER SECURITY BUDGET AFTER A BREACH

Thank you

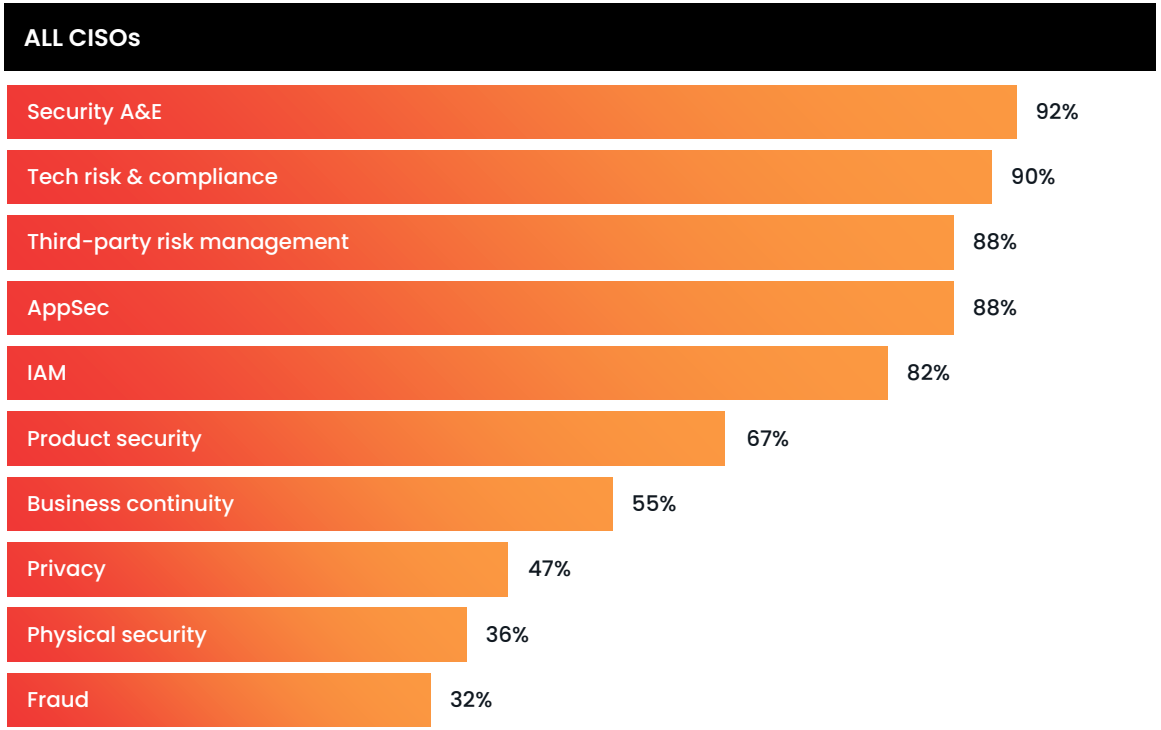
Anand Thangaraju

CISO, Board Director, Investor, Product GTM,
VC Catalyst, Mentor, Speaker

Scope Creep Continues

CISO's have a Broad Remit Including A&E, Tech Risk, AppSec and Third-Party Risk

What is included in your security ownership (multiple answers accepted)?



$1B+ firm C-level CISOs	Midsize firm C-level CISOs
+3pp	Same
Same	Same
+9pp	Same
+8pp	Same
Same	+7pp
+11pp	+13pp
Same	+16pp
+9pp	+16pp
Same	+21pp
+16pp	+11pp

Share of respondents (%)

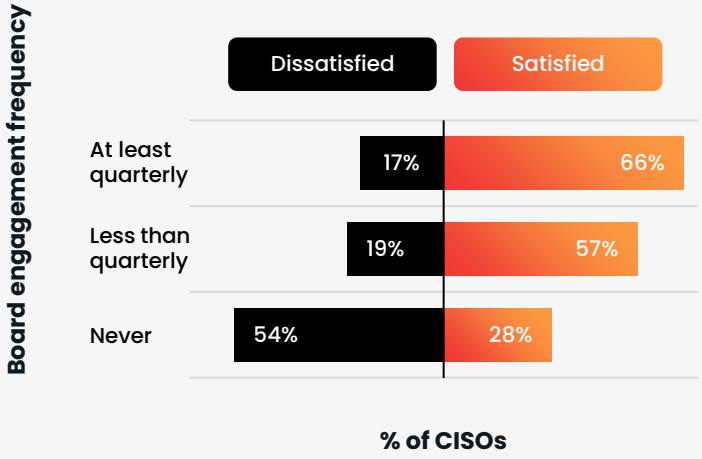
1pp = 1 percentage point

Board Reporting Critical In Driving Alignment

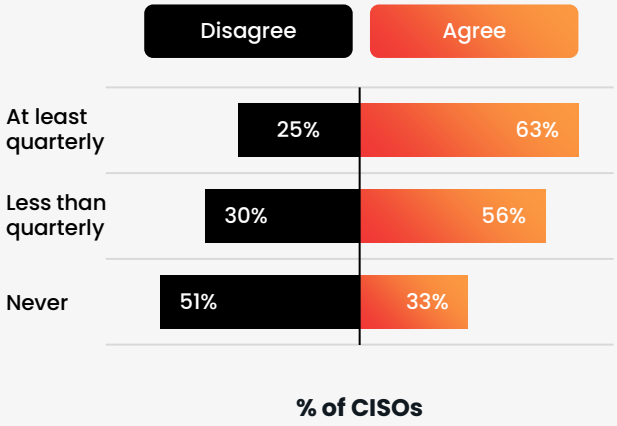
Regular CISO-Board Engagement Boosts Internal Alignment on Budgets and Risk

Board engagement frequency, and the impact on handling of budget requests and internal risk alignment

Satisfaction with the C-suite and board's handling of security budget requests (%)

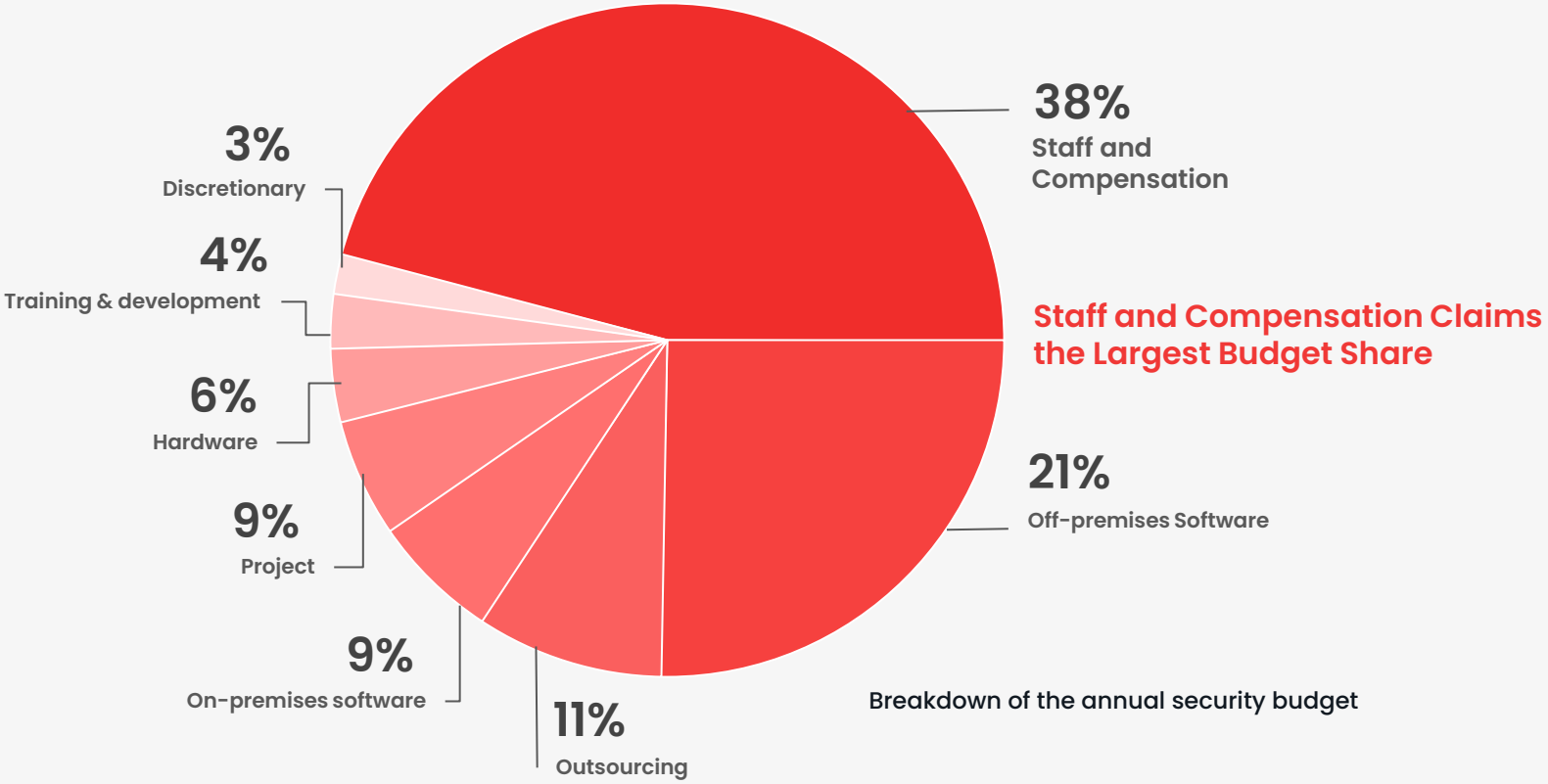


CISOs who agree the security budget and the Security mandate are in alignment (%)



Percentage do not add up to 100% because "neutral" responses have been excluded from the chart

Infosec Spend Priorities



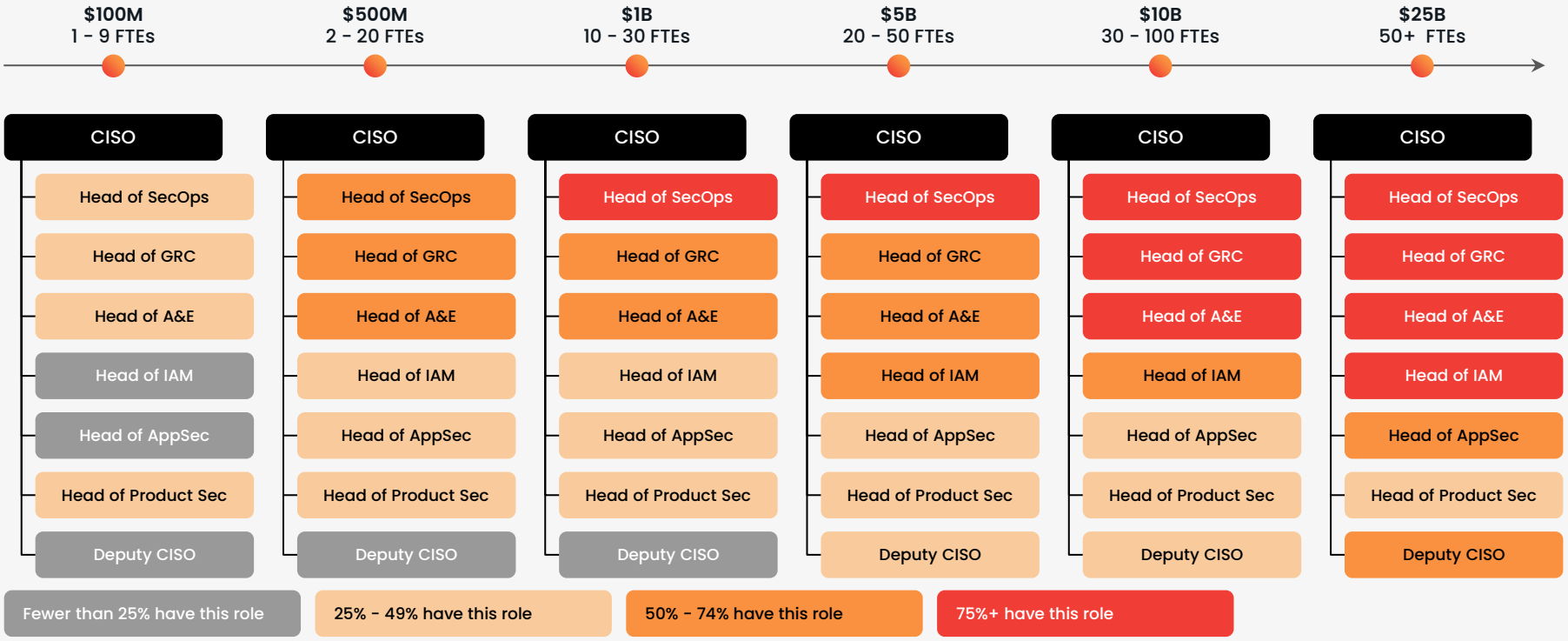
Staff and Compensation Claims the Largest Budget Share

Breakdown of the annual security budget

Typical Security Leadership Org Structure

Security Org Design at Different Revenue Milestones

Typical security leadership team structure in FTE for various revenue levels in USD

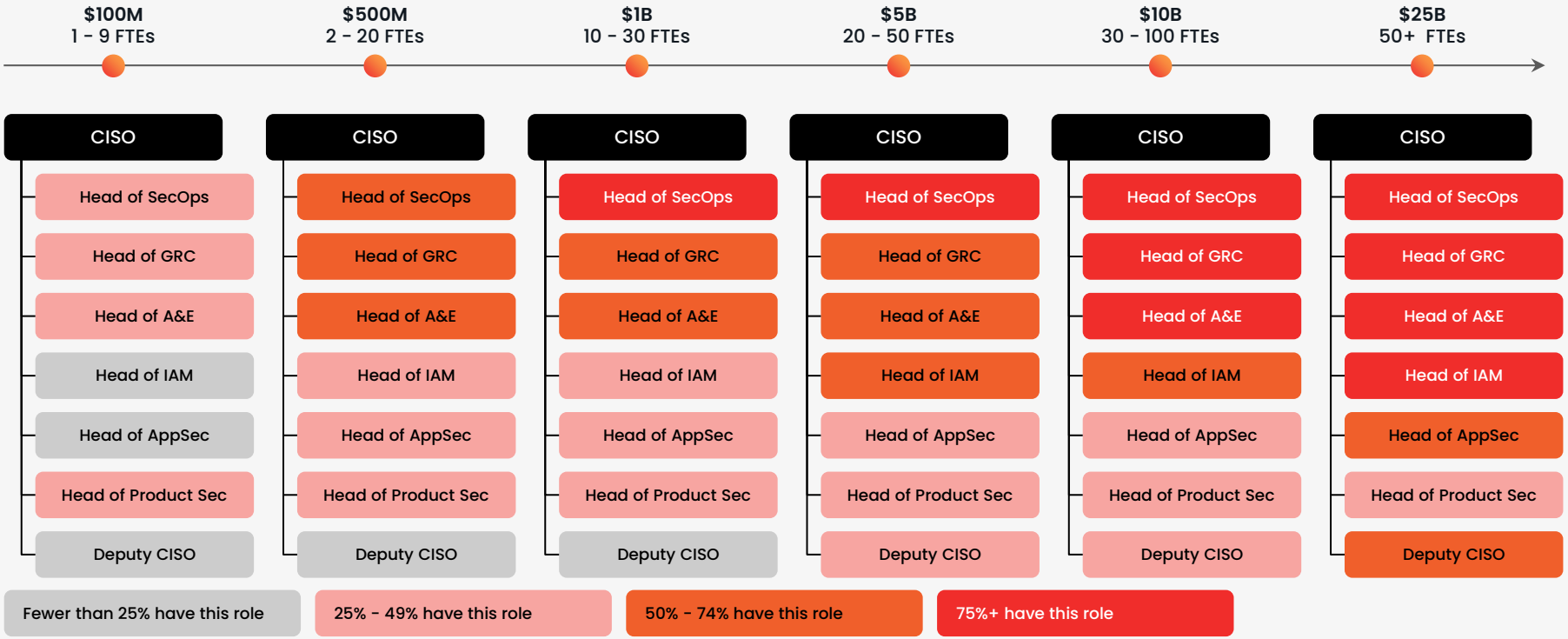


Revenue milestone and average security FTE range

Typical Security Leadership Org Structure

Security Org Design at Different Revenue Milestones

Typical security leadership team structure in FTE for various revenue levels in USD



Revenue milestone and average security FTE range

"Have Nots" Off Limits Solutions

Solutions most underfunded orgs shouldn't pursue:

01 Managed "threat hunting"

02 CTI feeds

03 Fancy "ransomware prevention" tools

04 Zero-trust solutions

05 AI-penetration testing

06 Commercial PAM solution

07 Phishing testing

08 Commercial security awareness training

09 Doubly so if it includes videos of Delta Force jumping out of vans

Best Practices Are Situational

Best practices depend entirely on your situation

When evaluating whether to apply a "best practice" make sure you understand how it applies to you.