cisco SECURE

SECURITY

study

Poised for Success: Proven Factors for Your Security Program

The 2021 Security Outcomes Study

Appendix B: Full Listing of Security Outcomes

Enabling Business	
EB1	Keeping up with the demands and growth of the business
	Example and Evidence of Success: The security program responds well to changing business needs and doesn't impede new lines of revenue. In some cases, security may provide competitive advantage or even be a net revenue generator. If security is viewed purely as a cost center or the "Department of 'No!'" by business execs, it's a sign of struggling to meet this goal.
EB2	Gaining the confidence and trust of executive leadership
	Example and Evidence of Success: Security leaders meet regularly – and favorably – with top executives and the Board of Directors. The relationship between business and security leaders is one of mutual respect and collaboration. If security is often in the hot seat with executives or regularly denied reasonable requests for support, it's a sign of struggling to meet this goal.
EB3	Obtaining buy-in from peers and other organizational units
	Example and Evidence of Success: Security enlists other divisions in building a cooperative defense of the organization. Communication and collaboration is strong with a fair sense of "give and take" for the greater good. Non-security leaders or divisions may have security-related performance measures. A culture of inter-departmental complaints and contention is a sign of struggling to meet this goal.
EB4	Creating a security culture embraced by all employees
	Example and Evidence of Success: Employees are treated as part of the security solution rather than the problem. Security isn't a negative theme in employee satisfaction surveys or exit interviews. Non-security staff regularly report phishing attempts, potential malware, and other incidents. Frequent security policy violations and workarounds are a sign of struggling to meet this goal.
Managing Risk	
MR1	Managing the top cyber risks to the organization
	Example and Evidence of Success: Top risk scenarios have been agreed upon by executives and security leaders and mitigation plans exist for those risks (or they've been accepted). Potential cyber risk exposure is currently within the risk appetite established by leadership. There's no evidence that risk management capabilities are failing (e.g., frequent near misses, control deviations, response/recovery testing failures, etc.).
MR2	Meeting regulatory compliance requirements
	Example and Evidence of Success: There's an absence of avoidable security findings from auditors and regulators. The organization is diligently tracking and addressing changing regulatory requirements. There's evidence that the organization understands what's required, acknowledges any findings and deficiencies, and is spending/working to mitigate them.
MR3	Avoiding major security incidents and losses
	Example and Evidence of Success: We expect that an organization that's highly successful in achieving this goal has not had a major security incident (of high internal and/or external visibility) in the last couple years. Furthermore, there's no reason to suspect that it's merely a matter of time until a major data loss event occurs. Minor and even moderate incidents are expected, but the question here is whether the organization has and will continue to stay out of the headlines.
Operating Efficiently	
OP1	Running a cost-effective security program
	Example and Evidence of Success: Executive leaders view the security program as having a good return on investment (ROI). There are no recurring rumblings about the overly high costs of security. There's a low rate of shelfware purchases. Staffing is lean but sufficient. A plan among executives and security leaders to reduce the security budget without increasing risk would be a good sign of success here.

OP2	Minimizing unplanned work and wasted effort
	Example and Evidence of Success: Strategy execution proceeds without frequent setbacks and deviations. Security budget is spent proactively rather than reactively. Employees spend their time on higher-level, more valuable tasks rather than being mired in the mundane. Constant firefighting mode or a program that "can't get out of its own way" is a sign of struggling to meet this goal.
OP3	Recruiting and retaining talented security personnel
	Example and Evidence of Success: The organization has a positive reputation in the security community as being a good place to work. Open security positions are generally filled quickly and without undue incentives. Talented staff move up instead of move out and attrition rates remain low. Employee satisfaction is consistently high.
OP4	Streamlining incident detection and response processes
	Example and Evidence of Success: There's a general sense that security operations run efficiently. Triaging security events isn't a guessing game and doesn't take forever. Responding to and remediating incidents is well-organized rather than chaotic. Metrics like time-to-detection and time-to-remediation are tracked and are trending down over time.

Appendix C: Full Listing of Security Practices

Business and Governance	
BG1	I have a clear understanding of how the security initiatives I'm involved in support my organization's business needs and objectives
BG2	I have good reason to believe that my organization's top executives view security as important to business objectives
BG3	My organization's top executives receive clear reporting on the activities and effectiveness of the security program
BG4	All employees in my organization receive effective security awareness education on threats, policies, and procedures relevant to their duties
BG5	I know what my organization considers to be our top cyber risks and believe that we've accurately assessed those risks
BG6	Someone in my organization is responsible for managing security and privacy compliance requirements
BG7	I'm confident that the security practices of vendors in my organization's value/supply chain are in line with our standards OR that we manage them accordingly
BG8	My organization maintains an accurate inventory of key systems and data and classifies those assets based on their security requirements and business criticality
Strategy and Spending	
SS1	Our security program maintains and communicates a sound overall strategy to successfully achieve its mission
SS2	Our security program has the financial budget needed to successfully achieve its mission
SS3	Our security program has the personnel needed to successfully achieve its mission
SS4	Our security personnel receive the role-specific training needed to successfully perform their duties
SS5	Our security program has the technology and tools needed to successfully achieve its mission
SS6	My organization has a proactive tech refresh strategy of frequent upgrades to best available IT and security technologies
Architecture and Operations	
AO1	Our security technologies are well integrated and work effectively together
AO2	Our security program uses performance metrics to drive operational decisions and actions
AO3	My organization's IT, development, and security operations personnel work effectively together

AO4	We use automation effectively to improve the efficiency of security operations and personnel
AO5	My organization meets established SLAs or deadlines for remediating disclosed vulnerabilities in systems and software
AO6	My organization takes a rigorous approach to developing and continually maintaining the security of our internal applications
AO7	Our security measures are actively monitored and regularly reviewed to verify and maintain their effectiveness
AO8	Our threat detection capabilities provide accurate awareness of potential security events without significant blind spots
AO9	Our incident response capabilities enable timely and effective investigation and remediation of security events
AO10	Our recovery capabilities minimize impact and ensure prompt restoration of assets affected by security incidents
AO11	We make a special effort to identify lessons learned from responding to incidents and use them to improve security measures for future events

CISCO

SECURE

The bridge to possible