



This Top 25 Metrics document is provided to you and your organization as a starting point or maturity checkpoint for the existing Security Metrics program. It is brought to you by Jim McConnell, Principal Owner, and Ask McConnell, LLC – A Converged Security Services Provider. The content is not meant to cover every circumstance, industry, law, regulation, contractual requirement, threat, environment, or risk, but it provides an easy, defendable, highly accountable starting point for any organization. Please consult with your legal counsel and insurance provider about added requirements. If you know of peers that you think would find value in these resources, please have them contact us. These are simply a chapter from our book on the topic, and you are welcome to use them; we just ask for credit, shout-outs, and referrals if you find them helpful. If you have recommended updates, we are all ears. And if you need Converged Security Consulting and Training, please reach out; we would be honored to serve you and your organization.

Jim McConnell

info@askmcconnell.com

Ask McConnell, LLC

<https://askmcconnell.com>

Top 25 Security Metrics – A Starting Point

	The Metric	Best Score
1	Percentage of our organization's technology assets that will be EOL/EOS by end of the fiscal year	0%
2	Percentage of our organization's buildings that have vulnerabilities that cannot be mitigated by end of the fiscal year	0%
3	Percentage of our organization's suppliers that have contractual non-compliance that will not be mitigated by end of the fiscal year	0%
4	Percentage of our business customers' that have security requirements that we have not met and verified by the customer or their designated third-party	0%
5	Percentage of breaches, regardless of size and type, that have been reported to the BoD each quarter	100%
6	Percentage of BoD members that have signed off on the definition and scope of security, vulnerability, breach, fraud, material, reportable, etc.	100%
7	Percentage of fraud losses, regardless of size and type, which have been reported to the BoD each quarter	100%
8	Percentage of investigations that have involved director or higher that have been reported to the BoD within 72 hours of the accusation	100%
9	Percentage of M&A, divestiture, sales, rebadges that involve sign off by the CSO and CISO at due diligence, transition planning, Go-No-Go close and full integration	100%
10	Percentage of BoD members' that have a document explaining all the security (physical, personnel, cyber, etc.) protecting the BoD member, that the organization's security team is responsible for	100%
11	Percentage of organization's security operations reporting metrics, KPIs, CPIs, NPS to the CSO and/or CISO daily	100%
12	Percentage of organization's security governed by the CSO and/or CISO	100%
13	Percentage of M&A, divestiture, sales, rebadges that fully funded CSO and CISO requirements	100%
14	Percentage of supply chain (prime and subs), regardless of whether there is a contract, has been through a business risk, corruption, and financial due diligence within the last year.	100%

	The Metric	Best Score
15	Percentage of supply chain investigations, affecting the organization, which have been reported to the CSO and/or CISO	100%
16	Percentage of BoD reportable audits that checked for data integrity issues	100%
17	Percentage of BoD reportable audits that cover both whether an asset is secure, not just compliant	100%
18	Percentage of BoD reportable audits where the scope and testing specifically includes breach and fraud discovery	100%
19	Percentage of audit and investigations after-action findings that have an assigned owner and funding	100%
20	Percentage of BoD, while performing duties for our organization, have personal protection duties that are performed by trained, equipped, and audited personal protection professionals	100%
21	Percentage of BoD meetings that include facility “bug sweeps” and results provided to the BoD before the meetings	100%
22	Percentage of Annual meeting and BoD meetings covered by a social media threat monitoring capability before, during and after the meetings with reports going to the BoD members	100%
23	Percentage of breaches, vulnerabilities, threats that have an attribution nexus to known terrorist countries	100%
24	Percentage of BoD members that have taken part in threat exercises/tabletop exercises in last 12 months	100%
25	Percentage of BoD primary employer’s security teams that have met with our organization’s security team in last 12 months	100%
	Extra Credit: Percentage of meeting resorts/event locations/golf courses/etc., used for BoD meetings/retreats, that have been pre-meeting audited for security vulnerabilities and threats along with BoD briefings	100%