Cadre
information security

19 Cybersecurity KPIs
to Help Your Business Succeed

If you're like most businesses, you may not feel confident you're looking at the most effective KPIs. Here are the 19 we think every business needs to measure:

- □ **Preparedness ratio:** % of fully patched and up-to-date devices that touch the network on a weekly basis.
- □ **Unidentified devices on the internal network:** Your employees not only bring their devices to work, but your organization may be using unauthorized Internet of Things (IoT) devices without your knowledge. These are huge risks for your organization as these devices are probably not secure. How many of these devices are on your network?
- □ **Intrusion incidents:** How many times have bad actors tried to breach your networks?
- □ **Response times:**
  - □ **Mean time to detect (MTTD):** How long do security threats fly under the radar at your organization? MTTD measures the length of time until your team becomes aware of a potential security incident.
  - □ **Mean time to contain (MTTC):** Once your team is aware of a threat, how long does it take them to respond and mitigate its impact?
  - □ **Mean time to resolve (MTTR):** How long does it take your team to resolve a threat once your team is aware of it?
- □ **Patch lag:** What is the lag between your schedule for patches and implementation?
- □ **Cybersecurity awareness training results:** Who has taken (and completed) training? Did they understand the material?
- □ **Time to report cybersecurity incidents:** How much time passes before an incident is reported?
- □ **% of employees using preferred reporting method:** Once your employees are aware of a threat, do they report via approved channels?
- □ **Third party security ratings:** Security ratings are often the easiest way to communicate metrics to non-technical colleagues through an easy-to-understand score.
  - □ **Average vendor security rating:** The threat landscape for your organization extends beyond your borders and your security performance metrics must do the same.

- □ **Access management accuracy:** When users are audited, how many need to be removed or downgraded because their status has changed?
- □ **Company vs peer performance:** The topical metric for board level reporting today is how your organization's cybersecurity performance compares to the peers in your industry. This information is easily digestible, visually appealing, and highly compelling which makes it a top choice for board presentations. BitSight or Security ScoreCard's Executive Summary Report allows you to easily benchmark your security performance against four key industry peers over the last twelve months.
- □ **Vendor patching cadence:** How effective are your vendors in mitigating and managing vulnerabilities?
- □ **Volume of data transferred using the corporate network:** A sudden, unexplained uptick could indicate an issue.
- □ **Number of days to deactivate former employee credentials:** If this period of time is longer than it should be, disgruntled former employees have more of an opportunity to compromise your data.
- □ **Number of communication ports open during a period of time:** Keep tabs on outbound SSL, as well as any common ports that allow remote sessions.
- □ **Cost per incident:** According to CSO, the average cost per compromised record was $221.
- □ **Uptime:** An analysis of the reasons behind downtime can also highlight areas of concern.
- □ **Regulatory requirements compliance:** How compliant are your current systems compared to industry standards?
- □ **Phishing test success rate:** How susceptible are your employees, vendors, and customers to phishing attempts?
- □ **Customer impact:** Collaborate with your customer-facing teams to identify the impact of your cybersecurity results on customers.