How to Use Cybersecurity KPIs

BARR ADVISORY

Table of Contents

What's a Cybersecurity Scorecard?

How can you tell if your cybersecurity program is effective? While audits give you a deep dive over your program at a point in time, cybersecurity needs to be continuously measured. Think of audits like an annual doctor's exam: you might get your annual exam and all of your vitals look good, but if a few days later you broke your leg falling down the stairs, you wouldn't wait until your next annual exam to get an X-ray and cast. Unfortunately, this is how we treat our cybersecurity programs. That's where cybersecurity scorecards and key performance indicators (KPIs) come into play.

A cybersecurity scorecard is an evaluation tool. It's a collection of metrics that can be used to measure the overall effectiveness of a cybersecurity program from a high level. Think of it as a cybersecurity report card that gives users a snapshot into their organization's security posture at any given time. Scorecards typically include several KPIs (but not too many), which provide a quantified measurable against a predetermined cybersecurity indicator.

Defining Cybersecurity KPIs

Cybersecurity KPIs give an organization's stakeholders and management a snapshot of the organization's cybersecurity performance. Think about it this way—**if you were vacationing on a beach somewhere and wanted to know the status of your organization's cybersecurity posture, what key metrics would you look at?**

Defining KPIs requires organizations to sit down and define what success looks like. It allows organizations to cut out the noise and focus on the most important measurables. When organizations have specific, defined measurables, it allows them to be most effective and take action whenever issues arise.

KPIs should be both digestible and actionable. Raw data alone isn't useful to organizations unless it's presented in a way that is widely comprehensible. For example, just measuring the number of open vulnerabilities doesn't provide much insight, but measuring the percent of issues closed on time or percent of issues that were elevated does.

KPIs should also be measurable. In the cybersecurity scorecard, there needs to be a clear definition of what success looks like for each KPI so that anyone could glance at it and understand whether any issues may arise.

Critical KPIs are highly specific to each organization depending on their industry, relevant laws and regulations, and appetite for risk. Organizations may also build their KPIs around customer commitments.

Cybersecurity KPIs should be:

- ***Digestible***
- ***Actionable***
- ***Measurable***

Six Key Cybersecurity KPIs

Let’s take a look at six KPIs that organizations should consider.

1. Percentage of devices on the organization’s network unpatched within your internal service level agreement (SLA)

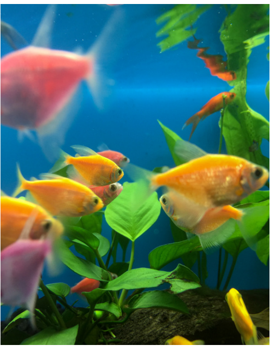
When a vulnerability is identified, it should be evaluated and treated accordingly through remediation or mitigation. Remediating or “patching” a vulnerability is an organization’s best option when a vulnerability is discovered. If fully patching a vulnerability is not an option, the risk posed by the vulnerability can be mitigated or accepted. Organizations may choose to measure the time it takes to patch a vulnerability or the percentage of devices on the organization's network unpatched within your internal SLA.

2. Eliminate unknown devices on an organization’s network

With the rapid growth of new technologies, Internet of Things (IoT) devices have been adopted by organizations of all sizes. From smart fridges to fish tank thermometers (yes, a smart fish tank thermostat caused a hack in 2018), these connected devices expand a network’s attack surface, increasing overall risk. Organizations should use network access control solutions to identify every device on their network and ensure each device has only appropriate access. Organizations can measure the number of unknown devices (with the goal clearly defined as zero) or measure the percent of known devices. Some organizations may have automated controls to prevent this occurrence. A bonus KPI might measure the percentage of resources exposed to the public internet. This is great not only as a KPI to monitor but is a good way to inform your threat modeling and risk assessment.

Did you know?

In 2018, cybercriminals exploited a vulnerability in an unnamed casino's fishtank thermostat and gained access to the casino's network, including a database of high profile casino clients.



Six Key Cybersecurity KPIs continued

3. Open security incidents with a severity measurement

The number of open security incidents, measured by level of severity, is a critical cybersecurity KPI. Incidents are inevitable, especially in organizations that are rapidly growing. Severity level can be measured by impact on business operations. Organizations may also choose to measure the time it takes to close open security incidents. The great thing about tracking something like this is eventually you can mature your program to see trends over time. This is helpful for measuring the effectiveness of not only closing incidents but also if your program is trending down, meaning you are fixing the root cause, or trending up, meaning you are just fixing the symptom and improvement is needed.

4. Percent of all accounts without multi-factor authentication (MFA) enabled

Time and time again, MFA has been proven to be an effective way of preventing attackers from using compromised credentials to gain unauthorized access to systems. MFA requires users to enter their password and a one-time code sent to their mobile device, email, or authenticator application. BARR recommends prioritizing systems that contain vital business data, but all systems benefit from MFA.

5. Number of users with privileged access to critical systems

The greater number of users with privileged access to critical systems, the larger the attack surface. Organizations should actively manage the number of users with privileged access to mitigate possible internal and external threats.

6. Reduce open risks from security assessments

The results of a security assessment give a company the information it needs to make improvements to their overall security posture. An open risk is one that is active (i.e., likely to occur and measures have not yet been taken to mitigate the risk). Organizations can measure the percent of open risks or the time it takes to close or mitigate those risks.

Continous Monitoring

Cybersecurity KPIs give an organization's management and key personnel a snapshot into the organization's cybersecurity performance. If designed appropriately, they should give an organization confidence that security practices are working effectively.

Establishing cybersecurity KPIs is a key first step—one that should not be treated as a "check the box" exercise. The real value comes from continuous monitoring, which is why it's important for organizations to automate KPIs using real time data where possible.

Organizations should establish internal service level agreements (SLAs) for response and remediation whenever issues arise that relate to critical KPIs. The SLA creates a process for resolving security issues on a regular, measurable basis, and defines the responsibilities of various internal and external parties in the event of a security issue.

Looking for Patterns

KPIs and cybersecurity scorecards allow organizations to track key metrics over time. With a cybersecurity scorecard in place, you can see dips of performance or periods of time where issues tend to pop up. That larger pattern can help organizations predict when issues may come up. By looking for patterns, it's easier to create processes and action items to resolve future issues.

Refreshing KPIs

If you have the right KPIs in place, reviewing those results will provide value. If someone tracking KPIs doesn't feel like the data provides them with value, that's a sign that your KPIs need to be updated.

Just like the water on your nightstand, KPIs can go stale if they are not regularly refreshed. KPIs should be evaluated and reassessed at least twice a year, and more frequently depending on the growth and complexity of the organization. Over time, organizations may recognize that they're no longer getting value from some metrics and choose to add new KPIs to their scorecard.

> ***KPIs should be evaluated and reassessed at least twice a year, and more frequently depending on the growth and complexity of the organization.***

Implementing a cybersecurity scorecard and beginning to track KPIs takes time upfront. Organizations are required to sit down and define their key metrics and what success looks like for their specific business. But once a scorecard is in place, it's an extremely valuable tool that will guide the organization throughout issues in the future.

About BARR Advisory

At BARR Advisory, we build trust through cyber resilience. We help protect the world's data, people, and information networks through a human-first approach to cybersecurity and compliance. Businesses looking for the accessibility of a boutique firm with the tools and expertise of a global consulting firm will find a partner in us.

Specializing in cybersecurity and compliance for companies with high-value information in cloud environments like AWS, Microsoft Azure, and Google Cloud, BARR has the global network of partners, the perspective, and deep expertise every thriving SaaS provider to world-class enterprise needs to stay secure and compliant at every stage.

Our Services

- **SOC Examinations**
  [SOC 1, SOC 2, SOC 3, SOC for Cybersecurity]
- **Healthcare Services**
  [HIPAA, HITRUST]
- **ISO 27001 Assessments**
- **FedRAMP Security Assessments**
- **PCI DSS Assessment Services**
- **Penetration Testing and Vulnerability Assessments**
- **Virtual CISO Services**
- **People & Culture Services**

Connect with BARR

Want to learn more about cybersecurity KPIs? Contact us today.