CISO ToGo
Technology Risk Consulting

As Peter Drucker said, what gets measured, gets managed ... and cybersecurity is no different. If you can't measure your security efforts, you won't know how you're tracking.

Why are cybersecurity KPIs important?

Cybersecurity is not a one-time affair. Cyber threats are constantly evolving, and the processes and technology needed to prevent them are constantly changing. Having these measures in place will allow you to assess the effectiveness of your security investments.

This is important for two reasons:

1. Analysis of KPIs, key risk indicators (KRIs) and security postures provides a snapshot of how your security team is functioning over time. Helping you better understand what is working and what is worsening, improving decision making about future projects.
2. Metrics provide quantitative information that you can use to show management and board members you take the protection and integrity of sensitive information and information technology assets seriously.

Reporting and providing context on cybersecurity metrics is being an important part of the job for many Chief Information Security Officers (CISOs) and Chief Information Officers (CIOs), driven by increasing interest in reporting at the shareholder, regulatory and board levels. For many board members in sectors like financial services, they have a fiduciary or regulatory duty to manage cybersecurity risk and protect personally identifiable information (PII).

The best IT security professionals use metrics to tell a story, especially when giving a report to non-technical colleagues.

14 Cybersecurity KPIs to track ...

Below are examples of clear metrics you can track and present to your stakeholders:

1. **Level of preparedness:** How many devices on your network are fully patched and up to date? Vulnerability scans and vulnerability management is one of the 20 CIS Controls that can reduce the risk of vulnerability exploits.

2. **Unidentified devices on internal networks:** Employees can introduce malware and other cyber risks when they bring in their own devices, as can poorly configured Internet of Things (IoT) devices, which is why network intrusion detection systems are an important part of your organization's security.

3. **Intrusion attempts:** How many times have bad actors attempted to gain unauthorized access?

4. **Security incidents:** How many times has an attacker breached your information assets or networks?

5. **Mean Time to Detect (MTTD):** How long do security threats go unnoticed? MTTD measures how long it takes your team to become aware of indicators of compromise and other security threats.

6. **Mean Time to Resolve (MTTR):** What is the mean response time for your team to respond to a cyberattack once they are aware of it? A great measure of the quality of your incident response plan implementation.

7. **Mean Time to Contain (MTTC):** How long does it take to close identified attack vectors?

8. **First party security ratings:** Security ratings are often the easiest way to communicate metrics to non-technical colleagues through an easy-to-understand score. For instance, organizations can consider applying simple “A” through “F” ratings on such things as network security, phishing risk, DNSSEC, email spoofing, social engineering risk, DMARC, risk of man-in-the-middle attacks, data leaks and vulnerabilities. Security ratings can feed into your cybersecurity risk assessment process and help inform which information security metrics need attention.

9. **Average vendor security rating:** The threat landscape for your organization extends beyond your borders and your security performance metrics must do the same. This is why a robust third-party risk management framework is required. Traditional vendor management practices were limited to a snapshot of your vendor security ratings at a single point in time. Organizations should consider, however, using a commercially available tool to continuously monitor (and reduce) vendor risks.

10. **Patching cadence:** How long does it take your organization to implement security patches or mitigate high risk CVE-listed vulnerabilities? Cybercriminals often use threat intelligence tools and exploit the lag between patch releases and implementation. A great example of this is the widespread success of WannaCry, a ransomware computer worm. While WannaCry exploited a zero-day vulnerability called EternalBlue, it was quickly patched but many organizations fell victim anyway due to poor patching cadence.

11. **Access management:** How many users have administrative privileges? Access control and the principle of least privilege are simple, cost effective methods of reducing privilege escalation attacks.

12. **Company vs peer performance:** The topic 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. Organizations should consider using a commercially available tool to facilitate the ability to easily benchmark your org's security performance against industry peers over a pre-determined timeline.

13. **Vendor patching cadence:** This metric involves determining how many risks your vendor has and how many critical vulnerabilities are yet to be remediated. Accurately reporting this measure requires a solid and transparent relationship with your vendors.

14. **Mean time for vendors to respond to security incidents:** A security incident isn't just a successful cyberattack, as intrusion attempts to vendors can signify your organization as a potential target. The longer it takes vendors to respond to incidents, the higher the chance you will suffer from a third-party data breach. In fact, some of the biggest data breaches are result of poor vendor management.

Choosing the "right" cybersecurity KPIs ...

There is no hard and fast rule for choosing cybersecurity KPIs. These metrics will depend on your industry, organization's needs, regulations, guidelines, best practices and ultimately, you and your customer's appetite for risk.

That said, you will want to choose metrics that are clear to anyone, even non-technical stakeholders. A good rule of thumb is if your non-technical stakeholders can't understand them, you need to pick new metrics or do a better job of explaining them. Benchmarks and industry comparisons are an easy way to make even complex metrics understandable.

Keep in mind that one of the most important metrics is cost. Remember the goal of presenting to the executive team and board is to make a succinct point about how cybersecurity is saving the organization money or generating additional revenue. This shouldn't be too hard to justify, given that the average data breach costs organizations $3.92 million globally and $8.19 million in the United States.

Outside of the metrics outlined above, the CIS Controls provide a cost effective, prioritized list of security controls.

Final Thoughts ...

As presented previously in this document, the adoption of cybersecurity KPIs is an important part of implementing an overall cybersecurity program, as it will help to substantiate value to the organization. Moreover, however, these measurements can serve as a substantive yardstick to assess the maturing of the program and your ability to protect your organization.

Having trained and experienced cybersecurity professionals available to help to guide you through the necessary assessments, decisions, selection process, and implementation can prove critical to the success (of failure!) of this effort **... and this is exactly where CISO ToGo, LLC can help!**

Reach out today, to discuss exactly how we can help:

http://www.ciso-togo.com/

Providing services and support throughout the United States

Email: WRichmond@CISO-ToGo.com

Phone: 401-264-0880

CISO ToGo
Technology Risk Consulting

because security is everyone's concern ... but it's OUR business!